INFORME DE AUDITORÍA TI-05-06

29 de noviembre de 2004

Autoridad de los Puertos de Puerto Rico

Oficina de Tecnología de Informática

(Unidad 5160)

Período auditado: 9 de abril de 2003 al 31 de enero de 2004

CONTENIDO

Estado Libre Asociado de Puerto Rico

OFICINA DEL CONTRALOR

San Juan, Puerto Rico

29 de noviembre de 2004

A la Gobernadora y a los presidentes del Senado
y de la Cámara de Representantes

Realizamos una auditoría de las operaciones de la Oficina de Tecnología de Informática (OTI) de la Autoridad de los Puertos de 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 se nos confiere en la **Sección 22 del Artículo III 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 varios informes de dicha auditoría. Este es el primer informe y contiene el resultado de nuestro examen de los controles generales establecidos en la OTI, el uso y los controles establecidos para las microcomputadoras, y el acceso a la Internet.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Autoridad fue creada por la **Ley Núm. 17 del 19 de abril de 1955**, según enmendada. En dicho estatuto se delegó en el Administrador de Fomento Económico las facultades y los poderes de la Junta de Directores de la Autoridad.

Mediante el **Plan de Reorganización Núm. 6 de 1971** la Autoridad quedó adscrita al Departamento de Transportación y Obras Públicas efectivo el 1 de enero de 1973 y continúa

adscrita a éste. Conforme a dicho **Plan**, las facultades, los poderes y las responsabilidades de la Autoridad, que hasta esa fecha las ejercía el Administrador de Fomento Económico, fueron transferidas al Secretario del Departamento de Transportación y Obras Públicas (Secretario). Posteriormente, por la **Ley Núm. 6 del 28 de junio de 1973**, se creó una Junta de Directores para regir la Autoridad y sustituir al Secretario. Esta **Ley** fue derogada por la **Ley Núm. 74 del 22 de junio de 1975** para transferir nuevamente al Secretario las facultades, los poderes y las responsabilidades que ejercía dicha Junta. Finalmente, mediante la **Ley Núm. 65 del 17 de agosto de 1989** se enmendó la **Ley Núm. 17** con el propósito de volver a crear la Junta de Directores de la Autoridad (Junta de Directores), la cual quedó constituida el 2 de enero de 1990.

Los propósitos principales de la Autoridad son desarrollar, mejorar, poseer, funcionar y administrar cualquier tipo de instalaciones de transporte y servicios aéreos y marítimos. Además, establecer y administrar sistemas de transportación colectiva marítima por sí sola o en coordinación con otras entidades gubernamentales.

Los poderes de la Autoridad son ejercidos por la Junta de Directores integrada por el Secretario del Departamento de Transportación y Obras Públicas, quien es su Presidente, el Director Ejecutivo de la Compañía de Fomento Industrial, el Secretario del Departamento de Desarrollo Económico y Comercio, el Director Ejecutivo de la Compañía de Turismo y un ciudadano particular en representación del interés público designado por el Gobernador, con el consejo y consentimiento del Senado. Las funciones de la administración y dirección de la Autoridad las ejerce un Director Ejecutivo nombrado por la Junta de Directores.

La Oficina del Director Ejecutivo en el desempeño de su responsabilidad cuenta con un Subdirector Ejecutivo, un Coordinador Ejecutivo, cuatro directores ejecutivos auxiliares y los negociados Marítimo y de Aviación que dirigen la fase operacional de la Autoridad. El Director Ejecutivo Auxiliar en Finanzas tiene a su cargo las oficinas del Contralor y de Presupuesto, el Negociado de Finanzas, las secciones de Crédito y Cobro y de Facturación y la División de Desembolsos y Nóminas. El Director Ejecutivo Auxiliar en Administración está a cargo de las oficinas de Personal, de Compras, de Servicios Generales y de Seguridad Industrial. El Director

Ejecutivo Auxiliar en Ingeniería dirige los negociados de Ingeniería, de Construcción, de Desarrollo y Planificación y de Fondos Federales. El Director Ejecutivo Auxiliar en Transportación Marítima[1] está a cargo del servicio de lanchas de Vieques, Culebra, Fajardo, Cataño y Acuaexpreso. Además, a la Oficina del Director Ejecutivo están adscritas las oficinas de Auditoría Interna, de Tecnología de Informática, del Coordinador Ejecutivo, de Comunicaciones y Prensa, de Asuntos Tarifarios y del Asesor Legal.

A la fecha de nuestra auditoría, la OTI tenía en operación las siguientes computadoras principales:

- una computadora marca Sun, modelo Enterprises 3500. Dicha computadora tenía instalado el sistema financiero **Oracle** y el sistema **Airport Business Tools (ABT)**.

- una computadora marca Compaq, modelo Proliant 1600 identificada como **Puertos_APPL** utilizada por los usuarios para acceder los sistemas **Oracle** y **ABT**

- una computadora marca DELL, modelo 2550, identificada como **APPR PORTAL** y configurada como *Web Server*

- cuatro computadoras marca DELL, modelo 2550, identificadas como **PRPA06SRV**, **PRPA02SRV**, **PRPA03SRV** y **PRPA04SRV** utilizadas para el registro electrónico de la asistencia mediante la aplicación **Timekeeper de Interboro Systems**, para el recibo y envío de correo electrónico mediante la aplicación **MS Exchange**, para la aplicación **SMS**, y para la aplicación **Track-it**, respectivamente. La computadora **PRPA04SRV** estaba configurada como *File Server*.

[1] En enero de 2000 se creó la Autoridad de Transporte Marítimo de Puerto Rico (ATM) para, entre otras cosas, desarrollar, mejorar, poseer, operar y manejar todo tipo de facilidades de tránsito marítimo y servicios de transportación marítima. La ATM está adscrita al Departamento de Transportación y Obras Públicas. No obstante, la Autoridad realiza las funciones administrativas y operacionales de la ATM.

- una computadora marca Compaq, modelo Proliant ML350, identificada como **PRPA01ISA** y configurada como *ISA Server*

- tres computadoras marca Avant, modelo New Gate, identificadas como **PRPA-22649**, **PRPA-SKNET SRV** y **APPRLEX**. Las **PRPA-22649** y **PRPA-SKNET SRV** eran utilizadas para monitorear las cámaras de los cuartos de máquinas ubicados en el primer y segundo piso y para manejar el sistema de las tarjetas de acceso, respectivamente. La **APPRLEX** estaba configurada como *Printer Server*.

- una computadora marca Compaq, modelo Proliant ML370, identificada como **PRPA01SRV** y configurada como *Primary Domain Comptroller (PDC).*

La Autoridad también cuenta con una página de Internet, la cual puede accederse mediante la siguiente dirección: *http://www.prpa.gobierno.pr*. Esta página provee información de la entidad y de los servicios que presta.

El presupuesto operacional de la OTI para el año fiscal 2002-03 ascendió a $7,877,620.

RESPONSABILIDAD DE LA GERENCIA

Con el propósito de lograr una administración eficaz, regida por principios de calidad, la gerencia de todo organismo gubernamental, entre otras cosas, es responsable de:

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**, lo cual incluye divulgar sus disposiciones a todo el personal

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 9 de abril de 2003 al 31 de enero de 2004. En algunos aspectos examinamos 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.

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
- Análisis de información suministrada por fuentes externas
- Pruebas y análisis de información financiera, de procedimientos de control interno y de otros procesos
- Confirmaciones de otra información pertinente

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OTI en lo que concierne a los controles generales, al uso y los controles establecidos para las microcomputadoras, y al acceso a la Internet se realizaron sustancialmente conforme a las normas generales aceptadas en este campo, excepto por los **hallazgos 1 y 2**, clasificados como principales, y los **hallazgos 3 al 7**, clasificados como secundarios.

Nuestro examen de los controles internos no necesariamente reveló todas las faltas existentes. En la parte de este informe titulada **RELACIÓN DETALLADA DE HALLAZGOS** se comentan los **hallazgos 1 al 7**.

RECOMENDACIONES

A LA JUNTA DE DIRECTORES DE LA AUTORIDAD DE LOS PUERTOS DE PUERTO RICO

1. Ver que el Director Ejecutivo de la Autoridad cumpla con las **recomendaciones 3 a la 5** de este informe. **[Hallazgos 1 al 7]**

2. Ver que el Director de la Oficina de Auditoría Interna de la Autoridad efectúe las inspecciones periódicas necesarias para verificar el cumplimiento de las normas y los procedimientos relacionados con los sistemas de información. **[Hallazgo 1]**

AL DIRECTOR EJECUTIVO DE LA AUTORIDAD DE LOS PUERTOS DE PUERTO RICO

3. Ejercer una supervisión eficaz de las funciones del Oficial Principal de Informática para asegurarse que:

    a. Colabore con la Oficina de Auditoría Interna de la Autoridad durante las inspecciones periódicas necesarias para verificar el uso adecuado de las microcomputadoras y las cuentas de acceso a la Internet y durante las orientaciones a los usuarios sobre las normas y los procedimientos de los sistemas computadorizados. **[Hallazgo 1]**

b. Establezca los controles necesarios para asegurar el uso oficial de los sistemas computadorizados y las cuentas de acceso a la Internet. **[Hallazgo 1]**

c. Examine las condiciones de uso del equipo almacenado en la OTI para que prepare y someta al Jefe de la Oficina de Servicios Generales la lista del equipo inservible, obsoleto y sin uso alterno para las medidas que correspondan. **[Hallazgo 3]**

d. Considere asignar, de ser necesario, aquellos equipos computadorizados en almacén que están en buenas condiciones y no se utilizan o tomar las medidas que correspondan con dichos equipos, en beneficio del interés público, en caso de que éstos no tengan utilidad para la Autoridad. **[Hallazgo 3]**

e. Restrinja los derechos y privilegios para que solamente personal clave de la Autoridad pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis que sea realizado por la gerencia. **[Hallazgo 4]**

f. Identifique las necesidades de adiestramiento sobre el uso de los equipos y programas computadorizados y planificar, coordinar e implantar un plan de adiestramiento, sobre el particular, para los empleados y funcionarios de la Autoridad. **[Hallazgo 5-a.1) y 2)]**

g. Se asegure que se utilice una contraseña al iniciar el uso de las microcomputadoras y se establezca un procedimiento que permita acceder a la opción para instalar programas o remover programas ya instalados al personal autorizado solamente. **[Hallazgo 5-a.3) y 4)]**

h. Establezca un plan de actualización de antivirus para que se aseguren que los usuarios con máquinas que no están conectadas a la red de comunicación local instalen la versión más reciente de los programas antivirus a las referidas microcomputadoras. **[Hallazgo 5-a.5)]**

i. Efectúe las gestiones necesarias para que se instalen un falso piso y detectores de humedad en el Centro de Cómputos. **[Hallazgo 6]**

j. El Administrador de la Base de Datos y la Coordinadora de Seguridad revisen diariamente los eventos registrados por los archivos del sistema **Oracle** y **Windows NT**, respectivamente, para detectar posibles violaciones de seguridad. Además, documenten la acción tomada en los eventos inusuales y de importancia detectados. **[Hallazgo 7]**

4. Establecer un **Plan de Contingencias** en el que se incluyan los procedimientos para proteger el equipo, los archivos, los programas y la documentación de los sistemas de información, según las directrices establecidas al respecto. **[Hallazgo 2-a.]**

5. Formalizar acuerdos por escrito con un Centro Alterno que acepte la utilización de sus respectivos equipos en caso de desastres o emergencias para restaurar las operaciones computadorizadas de la Autoridad. **[Hallazgo 2-b.]**

6. Realizar un análisis para determinar el personal clave de la Autoridad que requiera tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. **[Hallazgo 4]**

CARTAS A LA GERENCIA

Las situaciones comentadas en la parte de este informe titulada **RELACIÓN DETALLADA DE HALLAZGOS** se le informaron al Director Ejecutivo de la Autoridad, Sr. Miguel Soto Lacourt (Director Ejecutivo), en cartas de nuestra auditora del 30 de enero y 29 de abril de 2004.

El borrador de este informe se sometió al Director Ejecutivo para comentarios en carta del 2 de septiembre de 2004.

COMENTARIOS DE LA GERENCIA

En cartas del 12 de febrero y 19 de mayo de 2004 el Director Ejecutivo informó sobre las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en las cartas de nuestra auditora. Además, el Director Ejecutivo contestó el borrador del informe en carta del 24 de septiembre de 2004. Sus observaciones fueron consideradas en la redacción final del informe y se incluyen en la parte de este informe titulada **RELACIÓN DETALLADA DE HALLAZGOS EN LA OFICINA DE TECNOLOGÍA DE INFORMÁTICA DE LA AUTORIDAD DE LOS PUERTOS DE PUERTO RICO**.

AGRADECIMIENTO

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

Oficina del Contralor

Por: [redacted]

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, reglamento, carta circular, memorando, procedimiento, norma de control interno, norma de sana administración, principio de contabilidad generalmente aceptado, opinión de un experto o 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, irregularidades o 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 los hallazgos incluidos en el borrador 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 TECNOLOGÍA DE INFORMÁTICA DE LA AUTORIDAD DE LOS PUERTOS DE 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 TECNOLOGÍA DE INFORMÁTICA DE LA AUTORIDAD DE LOS PUERTOS DE PUERTO RICO

Los **hallazgos 1 y 2** se clasifican como principales y los **hallazgos 3 al 7** como secundarios.

Hallazgo 1 - Utilización de equipos computadorizados para fines ajenos a la gestión pública

a. Al 14 de agosto de 2003 la Autoridad tenía 543 microcomputadoras. El examen realizado entre agosto y octubre de 2003 del uso de 45 de éstas reveló que durante el 1999 y el 2003 se utilizaron 11 microcomputadoras, identificadas con los números de propiedad 22646, 23020, 23286, 25296, 26003, 26082, 26104, 26176, 26199, 26823 y 27447, y cuentas de acceso a la Internet pertenecientes a la Autoridad para procesar varios documentos y examinar varias páginas de Internet con contenidos ajenos a los intereses y a la gestión pública.

   En la **Sección 9 del Artículo VI de la Constitución del Estado Libre Asociado de Puerto Rico** se establece que sólo se dispondrá de las propiedades y de los fondos públicos para fines públicos y para el sostenimiento y funcionamiento de las instituciones del Estado y en todo caso por autoridad de ley.

En el **Artículo 3.2 de la Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental**, 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.

En la **Guía Núm. 8 - Utilización del Internet de la Carta Circular Núm. 96-01** promulgada por el Comité del Gobernador sobre Sistemas de Información[2] el 25 de septiembre de 1995 se establece que cada jefe de agencia es responsable de establecer los procedimientos y la política administrativa para el uso de la Internet. Además, se prohíbe el uso de ésta para actividades de lucro, de impacto negativo o para actos maliciosos.

En la **Orden Administrativa Núm. 120 - Política para Establecer el Uso de los Equipos Computadorizados y sus Programas** emitido por el Director Ejecutivo el 14 de mayo de 2003 se establece que el equipo computadorizado, los programas, el correo electrónico y el servicio de Internet son para uso oficial solamente.

El uso de microcomputadoras y las cuentas de acceso a la Internet pertenecientes a la Autoridad para procesar documentos y examinar archivos de carácter privado es contrario al interés público y desvirtúa los propósitos para los cuales fueron adquiridos. Además, provee al funcionario o empleado que indebidamente los utiliza unas ventajas, beneficios y privilegios que no están permitidos por ley.

Las situaciones señaladas se debían a falta de:

- inspecciones periódicas por parte de la Oficina de Auditoría Interna como elemento disuasivo y preventivo para verificar el cumplimiento de las normas establecidas por

[2] Creado en virtud del **Artículo 7 de la Ley Núm. 110 del 3 de agosto de 1995** para, entre otras cosas, adoptar la política a seguir y las guías que regirán la adquisición e implantación de los sistemas, del equipo y de los programas de información tecnológica para los organismos de la Rama Ejecutiva del Gobierno del Estado Libre Asociado de Puerto Rico.

los usuarios sobre el uso oficial de las microcomputadoras y de las cuentas para acceder a la Internet.

- orientación periódica a todos los usuarios de los equipos computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de los equipos computadorizados, y las cuentas para acceder a la Internet y a la red de la Autoridad.

El Director Ejecutivo, en la carta que nos envió, informó lo siguiente:

> No estamos de acuerdo con la causa presentada en dicho borrador. Podemos aceptar una recomendación para que la Oficina de Auditoría Interna efectúe inspecciones periódicas a las microcomputadoras, pero no haberlo hecho no es la causa para que los empleados hagan mal uso de las mismas. Cada empleado es responsable del uso de su equipo y cada computadora tiene en la pantalla de entrada las reglas de uso requeridas. Para utilizar la misma el empleado tiene que aceptar dichas reglas diariamente. La Oficina de Tecnología Informática envía notificaciones electrónicas constantemente a los usuarios sobre el uso de las microcomputadoras, los correos electrónicos, entre otras cosas. Nuestra Oficina de Auditoría Interna ha ofrecido orientaciones sobre el uso de cualquier equipo de la Agencia, incluyendo las disposiciones de la Ley de Ética Gubernamental sobre este asunto. Continuaremos con nuestro esfuerzo para evitar el mal uso de estos equipos al igual que de cualquier otro.

Consideramos las alegaciones del Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece.

Véanse las recomendaciones 1, 2 y 3.a. y b.

Hallazgo 2 - Necesidad de establecer un Plan de Contingencias y falta de acuerdos por escrito para mantener un centro alterno de sistemas de información

a. La Autoridad carecía de un **Plan de Contingencias** para las operaciones de los sistemas computadorizados en el que se establecieran las medidas a considerarse en caso de ocurrir algún desastre o circunstancia que afectara sus operaciones normales.

Una situación similar se comentó en el **Informe 03-04-(E)-09** emitido por la Oficina de Auditoría Interna de la Autoridad el 24 de noviembre de 2003.

b. Al 13 de enero de 2004 la Autoridad no había formalizado acuerdos por escrito con alguna entidad pública o privada para mantener un centro alterno de recuperación de sistemas de información. Esto, para la restauración de sus operaciones computadorizadas en casos de desastres o de emergencias.

En la **Resolución Núm. 89-01-A** del **By-Laws of the Puerto Rico Ports Authority** aprobado el 11 de diciembre de 1989 se establece lo siguiente:

> The Executive Director may prescribe and adopt such rules, regulations, and directives as shall be necessary and proper, and authorized by law for the administration and the operation of the Authority, and for exercising the powers delegated to or vested in him by law, by these By-Laws, or by any and all resolutions or other actions of the Governing Board.

En la **Guía Núm. 6 - Plan de Contingencia de la Carta Circular Núm. 96-01** se establece como política pública, que las entidades gubernamentales deberán desarrollar, preparar y ejecutar un **Plan de Contingencias** para los centros de sistemas de información, con el propósito de confrontar un desastre y poder continuar rindiendo la misión de la agencia por un tiempo indeterminado. En dicha **Guía** se requiere que el **Plan de Contingencias** incluya, entre otras cosas, lo siguiente:

- Cinco grupos de recuperación que asuman las funciones de decisiones gerenciales, coordinación, restauración en el centro primario, activación del centro alterno y operación del centro alterno. Para cada grupo se deben especificar sus respectivos miembros y una lista detallada con todos los medios de comunicación con éstos.

- Convenios escritos con proveedores de equipo donde se estipulen las necesidades, el equipo mínimo necesario y los servicios requeridos para afrontar la emergencia. Estos convenios podrían ser con una entidad pública o privada de similar configuración y tamaño.

- Itinerario de restauración debidamente identificado por grupos y tareas, y especificado de manera secuencial. Cada tarea debe ser detallada, con todos los procesos que conlleve y las funciones de cada uno de los miembros del grupo. Además, el personal asignado a cada proceso deberá utilizar una identificación de participante del **Plan de Contingencias**.

- Sección de aplicaciones que provea un detalle del orden de las prioridades de las aplicaciones a restaurar.

- Detalle de todos los sistemas operativos utilizados en los centros primario y alterno, y las correspondientes especificaciones.

- Evidencia de los simulacros efectuados dos veces al año en el centro alterno.

De ocurrir un desastre o emergencia, la falta de un **Plan de Contingencias** podría dar lugar a que el equipo no se proteja adecuadamente y sufra daños materiales, así como la pérdida de información importante. Además, la falta de acuerdos por escrito con un centro alterno podría afectar las funciones de la Autoridad y los servicios de la OTI, ya que no tendrían disponible una instalación para continuar operando después de la emergencia o evento que afectara su funcionamiento. Esto podría atrasar, dificultar o impedir el proceso de restauración de archivos y de programas, y el pronto restablecimiento de las operaciones normales de la Autoridad y de la OTI.

Las situaciones que se comentan se atribuyen a que el Director Ejecutivo no había establecido un **Plan de Contingencias** donde se detallaran los pasos a seguir en situaciones de emergencia. Tampoco había formalizado acuerdos por escrito con un centro alterno para la recuperación de sus sistemas de información en casos de desastres o emergencia.

El Director Ejecutivo, en la carta que nos envió informó, que en abril de 2004 se enviaron solicitudes de propuestas a varias compañías que ofrecen ese servicio. El 28 de mayo

de 2004 dos compañías sometieron sus propuestas y realizaron presentaciones mostrando en forma gráfica el alcance de las mismas. Seleccionaron una de esas compañías y refirieron la información a la División Legal para la preparación del contrato.

Véanse las recomendaciones 1, 4 y 5.

Hallazgo 3 - Equipo de computadoras sin uso, dañado u obsoleto

a. El 12 de diciembre de 2003 realizamos un inventario físico del equipo de computadoras que se mantenía en el almacén de la OTI. Encontramos las siguientes 170 unidades que no eran utilizadas, de las cuales 98 tenían un costo de $65,042[3] en el **Informe de Inventario de Propiedad** preparado el 14 de enero de 2004.

EQUIPOS ALMACENADOS	CANTIDAD
Microcomputadoras	23
Monitores	21
Battery Backups	3
Discos externos	74
Impresora	1
Accesorios	48
Totales	170

El examen efectuado de la utilidad y obsolescencia de dichos equipos reveló que:

1) Setenta y tres unidades de discos externos (*tape drive 8 GB*) adquiridos entre septiembre y diciembre de 2002 a un costo de $29,200 no se utilizaban ni habían sido asignadas, a pesar de que tenían utilidad.

[3] El **Informe de Inventario de Propiedad** no contenía el costo en inventario de los restantes 72 equipos.

2) Noventa y seis equipos (23 microcomputadoras, 21 monitores, 3 *battery backups,* 1 impresora y 48 accesorios de computadora) estaban obsoletos o sin uso alterno. Veinticuatro de dichos equipos habían sido adquiridos por $35,442.[4]

3) un *tape drive* de 8 *GB* adquirido por $400 estaba dañado.

En la **Guía Núm. 20 - Disposición de Equipo Electrónico de la Carta Circular Núm. 96-01** se establece como política pública que las dependencias y entidades gubernamentales utilicen el equipo computadorizado hasta que el mismo ya no tenga vida útil. Ello implica que, como norma de sana administración, la gerencia de toda entidad gubernamental debe maximizar la inversión de los fondos públicos mediante la utilización de la propiedad pública.

En el **Artículo 500.15, Sección (A) del Manual de la Propiedad**, aprobado por el Director Ejecutivo el 29 de mayo de 1990 se establece, entre otras cosas, que las áreas operacionales administrativas que necesitan declarar excedente materiales o equipo (propiedad mueble) deberán preparar un listado con una descripción clara de los mismos y la enviarán al Jefe de la Oficina de Servicios Generales quien hará las gestiones necesarias para la transferencia física del equipo.

Las situaciones que se comentan ocasionaban que los registros de la propiedad de la Autoridad estuviesen sobre valorados al incluir equipos inservibles u obsoletos. Esto pudiera propiciar el pago innecesario de las pólizas de seguro de dichos equipos. Además, el no asignar a los usuarios equipo útil impide obtener un rendimiento o beneficio de la inversión realizada.

Las mismas se atribuyen, en parte, a que el Oficial Principal de Informática no había evaluado las condiciones de los equipos almacenados para someter el listado de la

[4] El **Informe de Inventario de Propiedad** del 14 de enero de 2004 no contenía el costo de 72 de los equipos.

propiedad dañada u obsoleta al Jefe de la Oficina de Servicios Generales, de manera que éste transfiera el equipo. Tampoco había considerado un uso alterno para el equipo útil.

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, las medidas que han implantado para corregir las situaciones señaladas.

Véanse las recomendaciones 1 y 3.c. y d.

Hallazgo 4 - Falta de controles de los mensajes de correo electrónico recibidos y enviados a la Autoridad de fuentes externas

a. Al 9 de diciembre de 2003 el archivo de las cuentas de correo electrónico del sistema **MS Exchange** contenía 386 cuentas activas. Seleccionamos para examen 45 de dichas cuentas mediante un muestreo aleatorio simple. El examen efectuado de los controles establecidos para el uso del correo electrónico reveló que los usuarios de las 45 cuentas examinadas podían enviar y recibir mensajes de correo electrónico de fuentes externas a la Autoridad sin ningún tipo de restricción. Esto, conforme a las necesidades de la Autoridad y a los deberes y las responsabilidades de los usuarios.

En la **Guía Núm. 5 - Administración y Seguridad de Información Computadorizada de la Carta Circular Núm. 96-01** se establece como política pública que las dependencias y entidades gubernamentales deberán garantizar el buen uso, integridad, exactitud y preservación de la información del gobierno y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental. Dicha norma se instrumenta, en parte, mediante la configuración correcta para el manejo y envío de mensajes mediante las cuentas de correo electrónico conforme a las funciones, los deberes y las responsabilidades de los usuarios y a las necesidades de la entidad.

La situación que se comenta impide a la Autoridad mantener un control efectivo de los mensajes de correo electrónico que se reciben y se envían a la Autoridad de fuentes externas. La ausencia de dichos controles provocaron que el 4 de diciembre de 2003 se

recibieran en la Autoridad, provenientes de fuentes externas, cuatro mensajes de correo electrónico con información de carácter ofensivo hacia los funcionarios de la Autoridad y de alusiones político-partidistas.[5] Estos mensajes fueron enviados a la cuenta de correo electrónico de la Autoridad conocida como **PRPA-USERS@prpa.gobierno.pr**, la cual enviaba automáticamente los mensajes a todos los usuarios de correo electrónico de la Autoridad.

La situación señalada se debía a que los jefes de las distintas áreas que autorizaban las solicitudes de cuentas de correo electrónico a los usuarios no habían realizado un análisis para determinar los funcionarios y empleados a quienes debían otorgarse los privilegios para recibir y enviar mensajes de correo electrónico de fuentes externas, de acuerdo con las necesidades de la Autoridad y a los deberes y las responsabilidades de sus puestos. Esto, para que la Coordinadora de Seguridad configure las cuentas de los usuarios a quienes debían otorgarse.

El Director Ejecutivo, en la carta que nos envió informó lo siguiente:

> El grupo llamado **PRPA-USERS@prpa.gobierno.pr** fue eliminado de nuestra configuración de correo electrónico. No existe otro grupo definido en nuestro programa de correo electrónico que pueda afectar a todos los usuarios desde el exterior con el envío de estos mensajes en cadena.

Consideramos las alegaciones del Director Ejecutivo, pero determinamos que el **Hallazgo** prevalece.

Véanse las recomendaciones 1, 3.e. y 6.

[5] Los mensajes de correo electrónico provenían de correos externos, tales como: **Hotmail**, **Yahoo Mail** y **Lycos Mail**.

Hallazgo 5 - Falta de adiestramientos y otras deficiencias relacionadas con el uso y la seguridad de los sistemas computadorizados

a. El examen realizado, mediante pruebas, sobre el uso y la seguridad de las 45 microcomputadoras seleccionadas y las entrevistas a los usuarios de éstas reveló las siguientes deficiencias:

1) Diez usuarios de microcomputadoras (22 por ciento) no habían recibido adiestramientos sobre los programas computadorizados **MS Word**, **MS Outlook**, **MS Excel** y **MS PowerPoint**. Un usuario (2 por ciento) del Negociado de Ingeniería no había recibido adiestramiento del programa computadorizado **AutoCad** que utilizaba como herramienta de trabajo.

2) Diecisiete usuarios (37 por ciento) no producían resguardos periódicos de la información contenida en sus microcomputadoras.

3) Las microcomputadoras utilizadas por 9 usuarios (20 por ciento) no les requerían a éstos la utilización de contraseñas[6] para acceder los recursos de las mismas.

4) A seis de las microcomputadoras (13 por ciento) no se les había controlado el acceso a la opción *Add/Remove Programs* del sistema operativo para impedir a los usuarios que pudieran instalar programas no autorizados o remover programas ya instalados. Esta opción debe estar disponible únicamente al personal autorizado de la OTI.

5) Seis de las microcomputadoras (13 por ciento) examinadas e identificadas con los números de propiedad 22667, 22679, 23077, 23083, 23091 y 23685 no tenían instalada la última versión del programa **Norton Antivirus** correspondiente al 11 de agosto de 2003. Las fechas de actualización **(virus definition date)** de los programas antivirus instalados en las referidas microcomputadoras eran las siguientes: 7/13/00, 3/14/03, 8/08/01, 8/08/01, 8/16/02 y 9/25/02, respectivamente.

[6] Siete de dichas microcomputadoras no tenían conexión a la red de comunicaciones de la Autoridad.

Además, la microcomputadora identificada con el número de propiedad 21189 no tenía instalado programa antivirus alguno. Las siete microcomputadoras utilizadas por dichos usuarios no estaban conectadas a la red de comunicaciones de la Autoridad.

En la **Guía Núm. 5 de la Carta Circular Núm. 96-01** se establece como política pública que las dependencias y entidades gubernamentales deberán garantizar el buen uso, manejo, integridad, exactitud y preservación de la información del gobierno y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental. También se establece que las agencias mantendrán al día un programa de concientización sobre seguridad de información dirigida a todos los usuarios en todos los niveles. Dicha política se instrumenta, en parte, mediante el adiestramiento ordenado y continuo a los usuarios sobre:

- el uso de las microcomputadoras y sus programas
- la reproducción de resguardos periódicos de la información almacenada en las microcomputadoras
- la utilización de contraseñas, y
- la actualización constante de los programas antivirus.

Las situaciones que se comentan pueden propiciar que no se utilicen al máximo los equipos y programas computadorizados, se pierda información almacenada en las microcomputadoras, se utilicen equipos y programas computadorizados sin la debida autorización, y se instalen programas que no estén debidamente autorizados por la Autoridad. Además, que se propaguen virus a otras microcomputadoras.

Las situaciones que se comentan en el **Apartado a.1) y 2)** se debieron a que el Oficial Principal de Informática no había identificado las necesidades de adiestramiento a los

usuarios sobre el uso de los sistemas computadorizados a los fines de planificar, coordinar e implantar un plan de adiestramiento para los empleados de la Autoridad.

La situación que se comenta en el **Apartado a.3)** se debió a que las referidas microcomputadoras no fueron configuradas con la opción de requerir la utilización de una contraseña. Por otro lado, cuando se configuraron las microcomputadoras mencionadas en el **Apartado a.4)** no seleccionaron la opción para restringir a los usuarios el privilegio de instalar programas o remover programas ya instalados.

La que se comenta en el **Apartado a.5)** se debió a falta de supervisión efectiva por parte del Oficial Principal de Informática sobre los técnicos de Comunicación para asegurarse que todas las microcomputadoras tuvieran instaladas la última versión del programa **Norton Antivirus**.

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir las situaciones señaladas en el **Apartado a.1)** y **2)**. También informó lo siguiente:

- La Oficina de Desarrollo y Mantenimiento de Sistemas estableció el uso de contraseñas con las máquinas que están conectadas a nuestra red. En los lugares o áreas remotas como Aguadilla, Ponce, Mayagüez y otros, los equipos son utilizados por varios usuarios y están independientes. No hay forma de que esos usuarios puedan conectarse a nuestra red y alteren nuestro sistema. **[Apartado a.3)]**

- Entendemos que esta situación se refiere a máquinas que no están conectadas a la red de información. Estos equipos están instalados “standalone” en las facilidades remotas y sus sistemas operativos están muy limitados. El equipo ya está obsoleto y comenzamos con el proceso de identificarlos para reemplazarlos por equipo nuevo para corregir la situación. **[Apartado a.4)]**

- Las máquinas a las que se refiere el auditor no están conectadas a la red. Por lo tanto, cuando se actualiza el antivirus de la red las mismas no son actualizadas. Al usuario se le ha indicado en varias ocasiones que si su máquina no está conectada a la red debe notificar a la División de Tecnología Informática a través de una solicitud de trabajo para la actualización del antivirus. **[Apartado a.5)]**

Consideramos las alegaciones del Director Ejecutivo, pero determinamos que el **Apartado a.3) al 5) del Hallazgo** prevalece.

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

Hallazgo 6 - Faltas relacionadas con la seguridad física del Centro de Cómputos

a. Al 25 de noviembre de 2003 la Autoridad invirtió $675,051 para la instalación de los servidores marca Sun Enterprises, modelo 3500 en el Centro de Cómputos, para procesar las aplicaciones financieras de la Autoridad. Sin embargo, dicho Centro no estaba protegido contra inundaciones y del acumulamiento de agua. Éste carecía de un falso piso y de un detector de agua.

En la **Guía Núm. 5 de la Carta Circular Núm. 96-01** se establecen las normas para la administración y seguridad de información computadorizada. El propósito es asegurar la integridad y exactitud de la información y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar razonablemente la seguridad de los equipos y sistemas computadorizados, es necesario tener un salón de computadoras que reúna condiciones de seguridad adecuadas, como es la instalación de un falso piso y de los equipos de detección y protección necesarios.

Las situaciones que se comentan pueden poner en riesgo la seguridad de los empleados y de los equipos computadorizados y podrían contribuir a que ocurran daños a la propiedad.

El Oficial Principal de Informática no había implantado las referidas medidas de seguridad.

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, las medidas que están implantando para corregir las situaciones señaladas.

Véanse las recomendaciones 1 y 3.i.

Hallazgo 7 - Falta de revisiones periódicas a los registros de violaciones de seguridad provistos por los sistemas Windows NT y Oracle

a. A diciembre de 2003 el Supervisor de Sistemas de Información, cuyos deberes y responsabilidades estaban relacionados con la supervisión del funcionamiento de la red de comunicaciones de la Autoridad, no examinaba diariamente los registros de violaciones de seguridad provistos por los sistemas **Windows NT** y **Oracle**. Esto para conocer las posibles violaciones de seguridad que pudieran ocurrir en el servidor, en la red de comunicaciones o en los diferentes módulos de las aplicaciones financieras y tomar prontamente las medidas preventivas y correctivas necesarias.

En la **Guía Núm. 5 de la Carta Circular Núm. 96-01** se establece como política pública que las agencias deben garantizar el buen uso, manejo, integridad, exactitud y preservación de la información del gobierno y protegerla contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental. Dicha norma se instrumenta, en parte, mediante la impresión y el examen continuo de los informes que detallan los eventos inusuales del sistema para su pronta corrección.

La situación que se comenta impide la detección temprana de posibles violaciones de seguridad en el acceso lógico a los sistemas computadorizados que permitan tomar las medidas preventivas y correctivas de inmediato.

La misma se debía a falta de supervisión efectiva a la Coordinadora de Seguridad por parte del Oficial Principal de Informática.

El Director Ejecutivo, en la carta que nos envió informó, entre otras cosas, las medidas implantadas para corregir la situación señalada.

Véanse las recomendaciones 1 y 3.j.

ANEJO 1

AUTORIDAD DE LOS PUERTOS DE PUERTO RICO
OFICINA DE TECNOLOGÍA DE INFORMÁTICA

**MIEMBROS DE LA JUNTA DE DIRECTORES
QUE ACTUARON DURANTE EL PERÍODO AUDITADO**

		PERÍODO	
NOMBRE	**CARGO**	**DESDE**	**HASTA**
Hon. Fernando Fagundo Fagundo	Presidente	9 abr. 03	31 ene. 04
Sr. José M. Suárez Corujo	Miembro y Secretario de la Junta	9 abr. 03	31 ene. 04
Hon. Milton Segarra Pancorbo	Miembro	9 abr. 03	31 ene. 04
Dr. Hiram Ramírez Rancel	"	1 ene. 04	31 ene. 04
Vacante	"	9 abr. 03	31 dic. 03
Vacante	Miembro Representante del Interés Público	9 abr. 03	31 ene. 04

ANEJO 2

AUTORIDAD DE LOS PUERTOS DE PUERTO RICO
OFICINA DE TECNOLOGÍA DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES DEL NIVEL EJECUTIVO QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO**	**DESDE**	**HASTA**
Sr. Miguel Soto Lacourt	Director Ejecutivo	22 abr. 03	31 ene. 04
Lic. José G. Baquero Tirado	"	9 abr. 03	21 abr. 03
Lic. Carlos Ramírez Hernández	Subdirector Ejecutivo[7]	3 jun. 03	31 ene. 04
Sra. Elaine Maymí Naiz	Directora Ejecutiva Auxiliar en Administración[8]	9 abr. 03	31 mayo 03
Ing. Francisco E. Rosario Robles	Oficial Principal de Informática	9 abr. 03	31 ene. 04
Sra. Mariné Ortiz Espinell	Gerente Centro Sistemas de Información	9 abr. 03	31 ene. 04
Sr. Juan Agosto Pérez	Director de Auditoría y Controles Administrativos	9 abr. 03	31 ene. 04
Sra. Giselle L. Rodríguez González	Jefa de Auditoría Interna[9]	9 abr. 03	18 jul. 03

[7] Mediante la **Resolución Núm. 2002-54** la Junta de Directores autorizó al Director Ejecutivo a enmendar el organigrama para crear el puesto de Subdirector Ejecutivo efectivo el 2 de junio de 2003. Anteriormente dicho puesto se incluía en el organigrama como Asesor Financiero.

[8] Puesto vacante del 1 de junio de 2003 al 31 de enero de 2004.

[9] Puesto vacante del 19 de julio de 2003 al 31 de enero de 2004.