INFORME DE AUDITORIA TI-03-05

3 de abril de 2003

Autoridad de Edificios Públicos

Oficina de Sistemas de Información

(Unidad 5120)

Período auditado: 16 de octubre de 2001 al 28 de junio de 2002

CONTENIDO

Estado Libre Asociado de Puerto Rico

OFICINA DEL CONTRALOR

San Juan, Puerto Rico

3 de abril de 2003

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 Sistemas de Información (OSI) de la Autoridad de Edificios Públicos (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 OSI, el uso y los controles establecidos para las microcomputadoras, el acceso a la Internet y a las redes de comunicación de la Autoridad.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Autoridad fue creada por la **Ley Núm. 56 del 19 de junio de 1958 (Ley Núm. 56)**, según enmendada. Su propósito principal es satisfacer las necesidades de estructuras e instalaciones físicas de las agencias gubernamentales que tienen a su cargo la educación, la seguridad y el bienestar de los ciudadanos; y conservar y mantener en óptimas condiciones los edificios que ésta administra. Ello mediante el diseño, la preparación de planos, la construcción

de edificios y la conservación de éstos. El desarrollo de estos proyectos se determina a base de las necesidades establecidas por las agencias.

Los poderes de la Autoridad son ejercidos por una Junta de Gobierno (Junta) compuesta por el Secretario del Departamento de Transportación y Obras Públicas, el Presidente del Banco Gubernamental de Fomento para Puerto Rico, el Secretario del Departamento de Educación y otros cuatro miembros nombrados por el Gobernador, con el consejo y consentimiento del Senado de Puerto Rico, por un término de seis años. El Presidente de la Junta es elegido entre los miembros de ésta. La Junta, además nombra al Director Ejecutivo, quien tiene la responsabilidad de dirigir y administrar la Autoridad.

A la fecha de nuestra auditoría, la OSI tenía en operación dos computadoras marca Digital, modelo Alpha 4100 que operaban con un sistema operativo **UNIX 4.0E** y una red de comunicación compuesta por 12 servidores con un sistema operativo **Windows NT** y 330 microcomputadoras con sus respectivos equipos periferales. Dicha red permitía la comunicación de los usuarios de la Oficina Central a las Aplicaciones Financieras **ORACLE**, Correo Electrónico y Acceso a la Internet.

Además, como parte de un proyecto para el desarrollo e instalación de un Sistema Computadorizado Integrado para la Autoridad y sus oficinas en la Isla **(Island Wide)**, se habían instalado redes de comunicación local en ocho de las nueve oficinas regionales de la Autoridad.[1] Cada una de estas redes estaba compuesta por un servidor marca IBM, modelo Netfinity 3500, con un sistema operativo **Windows NT** y sus equipos periferales correspondientes.

El presupuesto de la Autoridad para el año fiscal 2001-02 ascendió a $726,609,144, del cual se asignaron $1,034,570 para las operaciones de la OSI.

---

[1] A la fecha de nuestra auditoría la red de comunicación local de la Oficina Regional de Caguas no estaba instalada.

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 información pertinente

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a los controles generales establecidos en la OSI, el uso y los controles establecidos para las microcomputadoras, el acceso a la Internet y a las redes de comunicación de la Autoridad se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo; y que el sistema de control interno establecido era razonablemente adecuado, excepto por el **Hallazgo 1** clasificado como principal.

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 el hallazgo principal y los hallazgos clasificados como secundarios enumerados del 2 al 8.

RECOMENDACIONES

A LA JUNTA DE GOBIERNO DE LA AUTORIDAD DE EDIFICIOS PÚBLICOS

1. Ver que la Directora Ejecutiva de la Autoridad cumpla con las **recomendaciones 2 a la 5** de este informe. **[Hallazgos 1 al 8]**

2. Ejercer una supervisión efectiva sobre las funciones de la Directora de la Oficina de Auditoría Interna para asegurarse que:

   a. Realice inspecciones periódicas para verificar el uso oficial de las microcomputadoras y de las cuentas de acceso a la Internet. **[Hallazgo 1]**

   b. Realice auditorías periódicas de los controles y las operaciones de los sistemas de información computadorizados de la Autoridad, y participe en el desarrollo y en la implantación de dichos sistemas. **[Hallazgo 8]**

A LA DIRECTORA EJECUTIVA DE LA AUTORIDAD DE EDIFICIOS PÚBLICOS

3. Ejercer una supervisión eficaz sobre el Director de la OSI para asegurarse que:

   a. Oriente a los funcionarios y empleados de la Autoridad en cuanto a las normas y a los procedimientos que rigen el uso del equipo y de los sistemas computadorizados. **[Hallazgo 1]**

   b. Prepare, para su revisión y aprobación, las normas y los procedimientos escritos necesarios para controlar el acceso a las páginas de la Internet. En las normas se deben incluir disposiciones sobre las medidas disciplinarias a aplicarse por cualquier violación a las mismas. **[Hallazgo 1]**

   c. Cumpla con las disposiciones del **Reglamento para Uso y Control de Datos, Manejo y Preservación de Licencias y Derechos de Programas en Computadoras y Sistemas de Información** de la Autoridad aprobado el 19 de octubre de 1999. **[Hallazgo 2-a.2)]**

   d. Realice las gestiones necesarias para que a las microcomputadoras y a los equipos de interconexión de las redes de comunicación de la Autoridad, se les instalen los equipos de protección contra fluctuaciones en la energía eléctrica. **[Hallazgo 2-b. y 4-c.2)]**

e. Prepare, para su revisión y aprobación, las normas y los procedimientos para el control de las redes de comunicación de la Autoridad y el mantenimiento de éstas. **[Hallazgo 4-a.1)]**

f. Diseñe un formulario para controlar el proceso de asignación de cuentas de acceso a las redes de comunicación. **[Hallazgo 4-a.2)]**

g. Active la opción de seguridad de acceso lógico que provee el sistema operativo **Windows NT** para restringir los días y el horario de acceso a las redes de comunicación. Además, que prepare para su revisión y aprobación normas de seguridad para el control de acceso a las redes de comunicación conforme a las políticas de seguridad que provee el sistema operativo **Windows NT**. Estas normas deben incluir procedimientos sobre la disponibilidad del sistema computadorizado fuera de horas laborables, cuando la necesidad del servicio lo amerite. **[Hallazgo 4-b.]**

h. Prepare un plan de visitas periódicas a las oficinas regionales para verificar si las computadoras utilizadas como servidores de las redes de comunicación están ubicadas en áreas con las condiciones ambientales y de seguridad adecuadas, y para verificar el funcionamiento de las mismas. **[Hallazgo 4-c.1) y 3)]**

i. Se asegure que la instalación, la reparación, el movimiento, la sustitución o la eliminación de equipos computadorizados se realice conforme a las guías establecidas en la **Carta Circular Núm. 96-01**. **[Hallazgo 4-d.]**

j. Prepare un programa de orientación a los usuarios de las microcomputadoras sobre los procedimientos para la preparación de resguardos de la información almacenada en dichos equipos, y vea que se cumpla con la reglamentación. **[Hallazgo 5]**

k. Prepare, para su revisión y aprobación, las normas y los procedimientos para el control de acceso a la OSI. **[Hallazgo 6-a.1)]**

l. Produzca los informes del Sistema **WinPass** y realice las verificaciones correspondientes. **[Hallazgo 6-a.2)]**

m. Coordine con la Oficina de Seguridad Interna la preparación de los procedimientos relacionados con la administración y conservación de los vídeos que se producían mediante el sistema de cámaras de seguridad. **[Hallazgo 6-a.3)]**

n. Prepare para su revisión y aprobación las medidas de seguridad necesarias para las oficinas administrativas y el salón de las computadoras principales. **[Hallazgo 7-a.1) al 6)]**

o. Coordine adiestramientos relacionados con las medidas a tomar en caso de emergencia para el personal de la OSI. **[Hallazgo 7-a.7)]**

4. Tomar las medidas necesarias para asegurarse de que el Director de Administración:

a. Ejerza una supervisión efectiva sobre la Encargada de la Propiedad, de manera que:

1) Actualice el **Registro de la Propiedad Mueble** y lo concilie periódicamente con la lista de inventario que mantiene el Director de la OSI, realice un inventario físico y le notifique sobre cualquier diferencia en inventario para las medidas correspondientes. **[Hallazgo 2-a.1)]**

2) Cumpla con las disposiciones del **Reglamento de Propiedad Mueble** que requiere que se le asigne y se marque con un número de propiedad todos los equipos computadorizados de la Autoridad. **[Hallazgo 2-a.3)]**

b. Cumpla con las disposiciones del **Reglamento para Uso y Control de Datos, Manejo y Preservación de Licencias y Derechos de Programas en Computadoras y Sistemas de Información** de la Autoridad aprobado el 19 de octubre de 1999. Además, vea que se concilie el **Informe de Activos Adquiridos General**

con el **Desglose de Licencias** periódicamente y que se le informe sobre cualquier diferencia para las medidas correspondientes. **[Hallazgo 2-a.2)]**

5. Ejercer una supervisión eficaz sobre las funciones del Director de la Oficina de Contraloría para asegurarse que cumpla con las disposiciones del **Procedimiento para el Recibo, Control y Entrega de Cheques** aprobado el 21 de marzo de 1994. **[Hallazgo 3]**

CARTAS A LA GERENCIA

Las situaciones comentadas en la parte de este informe titulada **RELACIÓN DETALLADA DE HALLAZGOS** se le informaron a la Directora Ejecutiva de la Autoridad, Arq. Lilliam Rivera Correa, mediante carta de nuestro auditor del 9 de abril de 2002.

El borrador de este informe fue sometido a la Directora Ejecutiva de la Autoridad para sus comentarios, por carta del 27 de enero de 2003.

COMENTARIOS DE LA GERENCIA

En carta del 22 de abril de 2002 la Directora Ejecutiva de la Autoridad informó las medidas adoptadas o que se proponía adoptar para corregir las situaciones comentadas en la carta de nuestro auditor. Dicha funcionaria contestó el borrador del informe mediante carta del 10 de febrero de 2003. Sus observaciones fueron consideradas en la redacción final del informe. Al final de los **hallazgos 1 al 8** se incluye parte de sus comentarios.

AGRADECIMIENTO

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

Por:

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 SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD DE EDIFICIOS PÚBLICOS, 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 EDIFICIOS PÚBLICOS

El **Hallazgo 1** se clasifica como principal y los **hallazgos 2 al 8** como secundarios.

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

a. El examen realizado entre febrero y marzo de 2002 sobre el uso de 28 computadoras reveló que en las computadoras con los números de propiedad AEP 58588, AEP 48991 y AEP 48918 se utilizaron cuentas de acceso a la Internet pertenecientes a la Autoridad para examinar, en varias ocasiones, archivos con información ajena a la gestión pública.

   Una situación similar se comentó en el informe de auditoría anterior.

   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 las guías incluidas en 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.

En el memorando sobre el **Uso del Equipo de Computadoras** emitido por la Directora Ejecutiva el 2 de abril de 2001 se establece, entre otras cosas, que las computadoras de la Autoridad son para realizar trabajos oficiales no personales. Además, se establece que se realizaran auditorías periódicas a los equipos de computadoras para garantizar que se estén cumpliendo con las normas establecidas en dicho memorando.

El uso de las microcomputadoras y de 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, en parte, a que:

- La Oficina de Auditoría Interna no realizaba inspecciones periódicas necesarias para verificar el uso oficial de las microcomputadoras y de las cuentas de acceso a la Internet.

- No se habían establecido las normas necesarias para controlar el uso de la Internet.

---

[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.

La Directora Ejecutiva, en la carta que nos envió informó, entre otras cosas, sobre las medidas implantadas para corregir las situaciones señaladas.

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

Hallazgo 2 - Faltas de controles de las microcomputadoras y los programas de computadoras

a. El examen del control que se ejercía de las microcomputadoras y los programas de la Autoridad reveló las siguientes faltas de control:

1) Existía una diferencia de 69 microcomputadoras entre el inventario de equipos de computadoras provisto por el Director de la OSI a nuestros auditores (330 microcomputadoras) y el **Registro de la Propiedad Mueble** certificado por la Supervisora de la División de Propiedad (261 microcomputadoras).

En la **Sección III del Reglamento de Propiedad Mueble** de la Autoridad aprobado el 19 de octubre de 1999 se establece, entre otras cosas, que el Encargado de la Propiedad debe mantener registros actualizados de la propiedad por unidad de trabajo, localización física y custodio. Además, como norma de control, se deben realizar conciliaciones de los registros periódicamente, investigar cualquier diferencia y tomar las medidas correspondientes.

2) La Oficina de Administración y la OSI no mantenían un registro completo y actualizado de los programas de computadoras y sus correspondientes licencias. Al 6 de marzo de 2002 el **Desglose de Licencias** que mantenía la OSI contenía 27 programas, mientras que el **Informe de Activos Adquiridos General** que mantenía la División de Propiedad de la Oficina de Administración contenía 16 programas. Ambos registros no contenían toda la información requerida por la reglamentación interna vigente. El **Desglose de Licencias** sólo contenía el nombre del programa, la cantidad de licencias y la cantidad de usuarios. El **Informe**

de Activos Adquiridos General no contenía el número de licencia, proveedor, dueño de la licencia, equipo donde está instalado, ubicación de la licencia, disquetes y manuales, y el nombre del usuario a quien se le asignó el programa.

En la **Sección VI del Reglamento para Uso y Control de Datos, Manejo y Preservación de Licencias y Derechos de Programas en Computadoras y Sistemas de Información** de la Autoridad aprobado el 19 de octubre de 1999, se establece que la Oficina de Administración en conjunto con la OSI mantendrán un registro de todo programa adquirido inmediatamente de ser recibido. En el registro se indicará lo siguiente:

- Número de licencia
- Suplidor
- Dueño de la licencia
- Fecha de adquisición
- Propósito y justificación de la compra
- Equipo donde será instalada (número de serie/propiedad)
- Ubicación física de la licencia, disquetes y manuales
- Nombre del usuario a quien se le asignó
- Número de propiedad asignado al programa
- Lista de inventario (licencia, disquete, manuales, equipo)

Se establece, además, que la Oficina de Administración realizará inventario de los programas adquiridos por la Autoridad anualmente y lo certificará la OSI.

Como norma de control, se deben realizar conciliaciones de los registros periódicamente, investigar cualquier diferencia y tomar las medidas correspondientes.

3) Un examen efectuado entre febrero y marzo de 2002 a 36 microcomputadoras y sus equipos periferales reveló que cinco microcomputadoras (14 por ciento), dos **Uninterruptible Power Supply (UPS)** y dos impresoras no tenían adherido el número de propiedad correspondiente.

En la **Sección VI del Reglamento de Propiedad Mueble** se establece que toda propiedad será registrada en el Archivo de Propiedad, se le asignará un número correlativo en orden ascendente, se ubicará por unidad de trabajo y se describirá en términos generales, haciendo uso de la **Forma de Entrada de Datos**. Además, se establece que se mantendrá la propiedad con una placa metálica o marcador especial que no pueda ser borrado (cuando así lo permita el equipo) en la que se insertará el número de propiedad y se identificará a la Autoridad.

Las situaciones comentadas impiden ejercer un control eficaz de las microcomputadoras, los programas y las licencias de éstos. Además, pueden dar lugar a que se incurra en irregularidades y dificultan que éstas se puedan detectar a tiempo para tomar las medidas correspondientes.

Las situaciones comentadas se atribuyen a que el Director de Administración y el Director de la OSI no cumplieron con la reglamentación vigente.

b. Identificamos 11 microcomputadoras que no estaban conectadas a un **UPS** o a un equipo para proteger las mismas contra cambios repentinos en la energía eléctrica.

En las guías incluidas en la **Carta Circular Núm. 96-01** se establece que la agencia debe mantener un plan de contingencia, que le permita reaccionar ante un evento que afecte las operaciones parcial o totalmente. Ello incluye, entre otras medidas, mantener fuentes de energía disponibles y listas para utilizarse durante el evento que interrumpa las operaciones. Además, que se tomen los cuidados necesarios para proteger los equipos, mantenerlos en óptimas condiciones y evitar daños y averías.

Esta situación podría ocasionar que se afecten las funciones de los usuarios y la información almacenada en las microcomputadoras de surgir interrupciones prolongadas en el servicio eléctrico o daños al equipo computadorizado por las fluctuaciones en la energía eléctrica.

Esta situación se atribuye a que el Director de la OSI no se había percatado de la falta de estos equipos para proteger dichas microcomputadoras. Denota, además, que no se ejercía una supervisión adecuada de dichas funciones por parte de la Directora Ejecutiva.

La Directora Ejecutiva, en la carta que nos envió, informó entre otras cosas, sobre las medidas a implantarse para corregir las situaciones comentadas en los **apartados a.1), 3),** y **b.** Además, nos indicó que la OSI mantiene un registro de todos los programas adquiridos y sus licencias. **[Apartado a.2)]**

Consideramos las alegaciones de la Directora Ejecutiva, pero determinamos que el hallazgo prevalece.

Véanse las recomendaciones 1, 3.c. y d. y 4.

Hallazgo 3 - Faltas de control de los cheques en blanco

a. Al 24 de octubre de 2001, en el salón de las computadoras principales se mantenía una caja de los cheques en blanco que son utilizados para efectuar los pagos a los proveedores u otras cuentas a pagar de la Autoridad.

En el **Procedimiento para el Recibo, Control y Entrega de Cheques** aprobado el 21 de marzo de 1994, se establece que los cheques en blanco se mantendrán en la caja fuerte de la Oficina de Contraloría. Como norma de control interno el personal de la OSI no debe ser custodio de los cheques en blanco.

La situación comentada podría propiciar el uso indebido de los cheques en blanco. Además, al no mantener un control adecuado de la utilización de éstos se haría difícil detectar cualquier irregularidad que surja con los mismos y fijar responsabilidades.

La situación comentada denota que el Director de la Oficina de Contraloría no había cumplido con el procedimiento establecido para el control de los cheques en blanco.

La Directora Ejecutiva, en la carta que nos envió, informó que el nuevo diseño de cheques permitirá que el personal de tesorería imprima los cheques desde sus facilidades y no tenga que intervenir en el Centro de Cómputos, razón por la cual debían mantenerlos en la impresora de cheques ubicada allí. Además, indicó que se hicieron recomendaciones a la Oficina de Contraloría para lograr estos objetivos.

Véanse las recomendaciones 1 y 5.

Hallazgo 4 - Faltas en la administración de las redes de comunicación

a. Nuestro examen realizado entre febrero y marzo de 2002 de la operación de las redes de comunicación de la Autoridad reveló lo siguiente:

1) No se habían adoptado las normas y los procedimientos para la administración, la utilización y el mantenimiento de las redes de comunicación.

2) No se había diseñado un formulario para la solicitud, aprobación, modificación y cancelación de las cuentas de acceso de los usuarios de las redes de comunicación.

En las guías incluidas en la **Carta Circular Núm. 96-01** se establece que 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. Ello requiere, entre

otras cosas, que se establezcan por escrito normas y procedimientos específicos para reglamentar el uso de sus redes, según los siguientes parámetros:

- Documentación de las especificaciones de la red que incluya la instalación de sus servidores y demás componentes

- Modificaciones a la composición de la red

- Configuración actualizada de la red

- Protección del área del cableado y la rotulación de los cables

- Lista de los programas, las aplicaciones y los usuarios de la red

- Controles de acceso rigurosos a la programación y a los archivos, que incluya el uso de formularios para solicitar la creación, modificación o eliminación de cuentas de acceso, según las necesidades y las condiciones de la entidad

- Protección de los archivos con información confidencial y los informes relacionados con éstos, así como la disposición de los mismos

- Renovación periódica de la contraseña de cada usuario, según las necesidades de la agencia y los procedimientos establecidos

- Prohibición de conexiones simultáneas para los usuarios

- Controles para prevenir y detectar los virus de computadoras

- Producción periódica de copias de reserva de los archivos de información y almacenamiento de los mismos

- Protección de los servidores de las redes, sus estaciones o microcomputadoras y los archivos de información en casos de desastre

- Restauración de programas y datos

- Procedimientos para verificar que el uso de los equipos de la red sea estrictamente oficial

La ausencia de las normas y los procedimientos mencionados podría ocasionar que las operaciones de la red no se efectúen uniformemente, lo que reduciría su eficacia. Además, la falta de controles expondría los datos procesados en ésta a riesgos innecesarios. También, podría afectar la toma de decisiones al momento de modificar la red o alguno de sus componentes.

b. Identificamos las siguientes deficiencias en los parámetros de controles de acceso y de seguridad definidos en el sistema operativo **Windows NT**:

1) En 271 (89 por ciento) de 304 cuentas de acceso no se había activado la instrucción para restringir el tiempo de acceso (**Logon Hours**) a la red según las responsabilidades y la necesidad de servicio de los usuarios.

2) Los usuarios de la red tenían acceso a los archivos de los discos duros de las computadoras de cinco usuarios cuyo uso debía estar restricto a éstos únicamente.

En la **Guía Núm. 5 - Administración y Seguridad de Información Computadorizada de la Carta Circular Núm. 96-01**, se establece como política pública, que cada agencia establecerá los controles de solicitud y nivel de acceso a sus sistemas electrónicos, de acuerdo con sus necesidades. En consonancia con dicha política pública, la gerencia de todo sistema computadorizado es responsable de delinear las medidas de control interno que permitan proteger los datos almacenados en sus sistemas de información contra la modificación, divulgación, manipulación o destrucción no autorizada o accidental.

La falta de controles de acceso lógico adecuados propicia que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de ésta. Además, propicia la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

Las situaciones comentadas en el **Apartado a.** se debían a que el Director de la OSI no había preparado para la aprobación de la Directora Ejecutiva y de la Junta de Directores de la Autoridad las normas, los procedimientos y el formulario que indicamos. La Directora Ejecutiva tampoco cumplió con su responsabilidad al respecto.

Las situaciones comentadas en el **Apartado b.** se debían a que el Director de la OSI no había activado la opción de seguridad de acceso lógico que provee el sistema operativo **Windows NT**. Además, a que el Director de la OSI no había preparado para la aprobación de la Directora Ejecutiva y de la Junta de Directores de la Autoridad instrucciones específicas en las políticas, normas y procedimientos de las operaciones de la OSI.

c. El examen efectuado de los controles de las redes de comunicación de las oficinas regionales de Mayagüez, Aguadilla, Arecibo y Carolina reveló lo siguiente:

1) Las computadoras utilizadas como servidores estaban ubicadas en áreas donde no se restringía el acceso a las mismas.

2) Los equipos de interconexión (**Superstack II Switch 1100**) de las redes de comunicación local no estaban conectados a un equipo para protegerlos contra cambios repentinos en la energía eléctrica.

3) No se realizaban revisiones periódicas del funcionamiento de las redes de comunicación de dichas oficinas.

En las guías incluidas en 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 la seguridad de los equipos y de los sistemas computadorizados, es necesario que:

- Se controle adecuadamente el acceso de personas a dichas áreas.

- Se utilice equipo y tecnología adecuada para proteger los sistemas.

- Se realicen revisiones periódicas sobre el funcionamiento de la red.

La situación comentada en el **Apartado c.1)** propicia que personas no autorizadas tengan acceso a los servidores de las redes de comunicación y que se ocasionen daños a los mismos o a los datos procesados en ellos, sin que se puedan fijar responsabilidades. Además, ponen en riesgo la seguridad de la propiedad y la información almacenada.

Las situaciones comentadas en el **Apartado c.2)** y **3)** ponen en riesgo los equipos de las redes de comunicación y la información almacenada.

Las situaciones comentadas se atribuyen a que el Director de la OSI no había preparado un plan de visitas periódicas a las oficinas regionales para verificar las condiciones ambientales y de seguridad de los equipos de las redes de comunicación, y para verificar el funcionamiento de las mismas.

d. En enero de 2001 las instalaciones de la Oficina Regional de Caguas fueron relocalizadas dentro del mismo edificio donde se encontraban. Las computadoras y los equipos periferales de la red de comunicación de dicha oficina no fueron reubicados por personal de la OSI.

En las guías incluidas en la **Carta Circular Núm. 96-01** se establece que toda solicitud de instalación, reparación, movimiento, sustitución o eliminación de equipos tales como: terminales, impresoras, computadoras personales, líneas de comunicación, deberá dirigirse por escrito a la unidad responsable por el funcionamiento de la red. Todas las solicitudes deben ser originadas por el director del área solicitante. Ningún empleado por su propia iniciativa está autorizado a realizar tareas de instalación y reparación a los equipos asociados a la red de telecomunicaciones.

Esta situación pudo provocar averías en los equipos de la red de comunicación. Además, puso en riesgo la seguridad de dichos equipos y de la información almacenada en las microcomputadoras.

Esta situación se atribuye a que el Director de la Oficina Regional de Caguas no solicitó al Director de la OSI la relocalización de los equipos de la red de comunicación.

La Directora Ejecutiva, en la carta que nos envió informó, entre otras cosas, sobre las medidas a implantarse para corregir las situaciones comentadas en los **apartados a., b.2), c.** y **d.** Con relación al **Apartado b.1)** indicó que en muchas oficinas surgen trabajos de emergencia fuera de horas laborables y no tendrían acceso al sistema, lo que se convierte en un impedimento en lugar de un control saludable.

Consideramos las alegaciones de la Directora Ejecutiva, pero determinamos que el hallazgo prevalece.

Véanse las recomendaciones 1 y 3.d. a la i.

Hallazgo 5 - Deficiencias en la preparación de los resguardos de información en las microcomputadoras

a. En un examen realizado a 25 microcomputadoras se determinó que los usuarios de 20 (80 por ciento) de éstas no efectuaban resguardos de la información almacenada en dichas microcomputadoras.

En el **Reglamento para Uso y Control de Datos, Manejo y Preservación de Licencias y Derechos de Programas en Computadoras y Sistemas de Información** de la Autoridad aprobado el 19 de octubre de 1999, se establece que es responsabilidad de cada usuario preparar periódicamente (diario, semanal, mensual) resguardos de los archivos.

No producir ni mantener copias de reserva de los datos procesados podría ocasionar la pérdida permanente de información importante sin la posibilidad de poder restaurarla.

Esta situación se atribuye a que el Director de la OSI no había orientado a los usuarios de las microcomputadoras sobre los procedimientos para la preparación de los resguardos de la información almacenada en las microcomputadoras. Denota, además, que la Directora Ejecutiva no ejerció una supervisión adecuada en lo concerniente.

La Directora Ejecutiva, en la carta que nos envió, informó que actualmente se hacen copias de todos los documentos de las oficinas que manejan documentos sensitivos. Además, que se está adquiriendo un servidor de mayor capacidad para hacer extensivo este proceso a todas las computadoras.

Véanse las recomendaciones 1 y 3.j.

Hallazgo 6 - Faltas en los controles de acceso físico de la OSI

a. El examen de los controles de acceso físico de la OSI reveló las siguientes faltas de control:

1) Un Programador, una Analista de Sistemas y un consultor tenían acceso al salón de las computadoras principales mediante tarjetas electromagnéticas. Además, dos supervisores interinos de la División de Tesorería y la Secretaria Administrativa del Director de la OSI tenían acceso a dicho salón. Dichos funcionarios de acuerdo con las funciones que desempeñaban no deberían tener acceso al referido salón.

2) No se producían los informes que proveía el Sistema **WinPass**[3] para verificar el acceso a la OSI y al salón de computadoras.

3) En la OSI se había instalado un sistema de cámaras de seguridad, cuyos monitores estaban ubicados en la Oficina del Director de la OSI. Sin embargo, no se habían promulgado procedimientos escritos para la administración y conservación de los vídeos que se producían mediante el sistema de cámaras de seguridad.

En las guías incluidas en la **Carta Circular Núm. 96-01** se establecen normas para la administración y la seguridad de la información computadorizada. El propósito es asegurar la integridad y exactitud de la información del gobierno y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- se controle adecuadamente el acceso de personas a dichas áreas.

- se controlen los vídeos que producen el sistema de cámaras de seguridad.

La situación comentada en el **Apartado a.1)** podría propiciar la comisión de irregularidades, y de éstas ocurrir se dificultaría fijar responsabilidades con prontitud.

Las situaciones comentadas en el **Apartado a.2)** y **3)** podrían facilitar que personas no autorizadas tuvieran acceso a la OSI y al salón de las computadoras principales, y ocasionaran daños a la computadora o a los datos procesados en ellas, sin que se pudieran fijar responsabilidades.

Las situaciones comentadas se debían, en parte, a que el Director de la OSI no había preparado para la aprobación de la Directora Ejecutiva y de la Junta de Directores de la Autoridad las normas y los procedimientos para el control del acceso físico a la OSI.

---

[3] Sistema computadorizado de cerraduras electromagnéticas utilizado para restringir mediante tarjetas magnéticas el acceso a la OSI y al salón de las computadoras principales.

Dicho funcionario tampoco cumplió con su obligación de producir los informes del Sistema **WinPass** para las verificaciones correspondientes. La Directora Ejecutiva tampoco cumplió con su responsabilidad al respecto.

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

- Los supervisores interinos de la División de Tesorería tenían la necesidad de entrar a las facilidades del centro de cómputos, en donde se mantenía una impresora de cheques, en lo que terminaba el proceso de cambio de programación. Además, que es su obligación imprimir y mantener la seguridad de los procesos de pago y no podían delegarlo en otra persona. La secretaria administrativa tiene necesidad de acceso disponible al centro, para cuando viene personal externo a dar mantenimiento a los equipos y resolver situaciones de emergencia. **[Apartado a.1)]**

- El sistema **WinPass** permite monitorear los accesos otorgados a través del monitor, lo que les permite hacer búsquedas por tipo de evento. Se creó una tabla de incidencias las cuales son investigadas para tomar la acción que corresponda. **[Apartado a.2)]**

- Los procedimientos escritos para la administración y el monitoreo de los accesos a OSI se encuentran en proceso de aprobación. **[Apartado a.3)]**

Consideramos las alegaciones de la Directora Ejecutiva relacionadas con el **Apartado a.1)**, pero determinamos que el mismo prevalece.

Véanse las recomendaciones 1 y 3.k. a la m.

Hallazgo 7 - Faltas relacionadas con la seguridad física de la OSI

a. El examen de la seguridad física de la OSI reveló las siguientes faltas de control:

1) La OSI y el salón de las computadoras principales no tenían salidas de emergencia.

2) Las áreas administrativas de la OSI no tenían detectores de humo.

3) No había detectores de agua bajo el falso piso del salón de las computadoras principales.

4) El salón de las computadoras principales no contaba con equipo para controlar la humedad y temperatura.

5) No se había instalado un interruptor de energía eléctrica fuera del salón de las computadoras principales.

6) En el salón de las computadoras principales no se había marcado o identificado la ubicación de los dispositivos o detectores de humo colocados debajo del falso piso.

7) El personal de la OSI no había participado en adiestramientos sobre las medidas a tomar en caso de una emergencia.

En las guías incluidas en 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 las condiciones de seguridad y los equipos de detección y protección adecuados. También, se deben ofrecer conferencias periódicas sobre las medidas a tomar en caso de una emergencia. Ambas prácticas tienen el objetivo de proteger tanto al personal como al equipo y otras propiedades.

Las situaciones comentadas pueden poner en riesgo la seguridad de los empleados y podría contribuir a que ocurran daños a la propiedad.

El Director de la OSI no había implantado las medidas de control que se comentan.

La Directora Ejecutiva, en la carta que nos envió, informó que están realizando las gestiones para corregir estas deficiencias.

Véanse las recomendaciones 1 y 3.n. y o.

Hallazgo 8 - Necesidad de que la Oficina de Auditoría Interna participe en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas computadorizados

a. La Oficina de Auditoría Interna de la Autoridad no había efectuado auditorías de los procedimientos, los controles y el funcionamiento de los sistemas computadorizados de la Autoridad desde el 17 de febrero de 1999. Tampoco había participado en el desarrollo y en la implantación de los sistemas de información computadorizados.

En la **Sección VII del Reglamento Para Uso y Control de Datos, Manejo y Preservación de Licencias y Derechos de Programas en Computadoras y Sistemas de Información** de la Autoridad aprobado el 19 de octubre de 1999 se establece que la Oficina de Auditoría Interna implementará un Programa de Auditoría Interna para salvaguardar el uso e instalación de programas en las computadoras de la Autoridad. La auditoría debe llevarse a cabo rutinariamente cotejando el inventario de los programas aceptados para residir en cada computadora.

En las guías incluidas en la **Carta Circular Núm. 96-01** se establece como política pública que las agencias deberán implementar un programa de auditorías internas rutinarias para salvaguardar el uso y la instalación de programas en sus microcomputadoras. Además, como norma generalmente aceptada en el campo de los sistemas de información computadorizados, los auditores internos deben participar en las diferentes etapas del desarrollo y la operación de los sistemas. Esta norma se fundamenta en la aportación que puedan hacer éstos en el desarrollo y en la implantación de los controles necesarios para una operación adecuada de dichos sistemas, y en la verificación continua del funcionamiento eficaz de los mismos.

Resulta difícil incorporar controles en los sistemas computadorizados luego que han sido implantados. Además, la ausencia de fiscalización y de recomendaciones por parte de los auditores internos puede propiciar que se cometan errores e irregularidades y que los mismos no se detecten a tiempo para fijar responsabilidades. También, priva a la gerencia de información necesaria sobre el funcionamiento de los sistemas, los controles y las demás operaciones.

Esta situación se atribuye a que la Directora de Auditoría Interna no había cumplido con las disposiciones reglamentarias. Además, la Junta de Gobierno no se había percatado de la importancia de que la Oficina de Auditoría Interna participara en el desarrollo y en la implantación de los sistemas de información computadorizados.

La Directora Ejecutiva, en la carta que nos envió, informó que luego del cambio de administración, la Oficina de Auditoría Interna tuvo una nueva dirección en febrero de 2001. Entre sus primeras encomiendas, dicha Oficina participó en la auditoría que promoviera la Oficina de Gerencia y Presupuesto, que incluía sistemas de información, y en la auditoría independiente de los sistemas realizada por una firma de auditores independientes. También, indicó que una de las razones por las que se pospuso realizar las auditorías programadas fue evitar la duplicidad de funciones e interferir con la auditoría del Contralor, que precisamente fue anunciada cuando el programa de auditoría estaba en progreso. Entendía que era su deber y responsabilidad distribuir adecuadamente el trabajo a realizar, ya que la Oficina cuenta con poco personal y ha sido señalada por otros informes del Contralor, que debe auditar las áreas administrativas y de construcción, con mayor presupuesto.

Consideramos las alegaciones de la Directora Ejecutiva, pero determinamos que el hallazgo prevalece.

Véanse las recomendaciones 1 y 2.b.

ANEJO 1

AUTORIDAD DE EDIFICIOS PÚBLICOS
OFICINA DE SISTEMAS DE INFORMACIÓN

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

NOMBRE	CARGO	PERÍODO DESDE	PERÍODO HASTA
CPA Juan Agosto Alicea	Presidente	13 nov. 01	28 jun. 02
CPA Carlos Nieves Marrero	"	16 oct. 01	12 nov. 01
Ing. Miguel P. Vélez Rodríguez	Vicepresidente	16 oct. 01	28 jun. 02
Hon. José M. Izquierdo Encarnación	Miembro	16 oct. 01	28 jun. 02
Lic. Roberto Montalvo Carbia	"	16 oct. 01	28 jun. 02
Hon. César A. Rey Hernández	"	13 nov. 01	28 jun. 02
Lic. Carmen Candelaria Peña	"	26 nov. 01	13 mayo 02
Lic. Teodoro Muñiz Jiménez	"	16 oct. 01	12 nov. 01
Sr. Manuel Feliciano Parilla	"	16 oct. 01	12 nov. 01
Sr. Franco Chinea Rivera	"	16 oct. 01	12 nov. 01

ANEJO 2

AUTORIDAD DE EDIFICIOS PÚBLICOS

OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES DEL NIVEL EJECUTIVO QUE ACTUARON DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO	PERÍODO DESDE	PERÍODO HASTA
Arq. Lilliam Rivera Correa	Directora Ejecutiva	16 oct. 01	28 jun. 02
Sra. Robin G. Garland Cansobre	Subdirectora Ejecutiva de Administración	1 mar. 02	28 jun. 02
Lic. Claudio Ocasio Rojas	Subdirector Ejecutivo de Administración	16 oct. 01	31 ene. 02
Lic. Lénidas Ramírez Piñeiro	Directora de la Oficina de Servicios Legales	16 oct. 01	28 jun. 02
Sra. Sara Indira Luciano Delgado	Directora de la Oficina de Recursos Humanos	16 nov. 01	28 jun. 02
Sra. Nadya Morales Cátala	"	16 oct. 01	15 nov. 01
Sr. Oscar Hernández Nevárez	Director de la Oficina de Contraloría	16 oct. 01	28 jun. 02
Sr. Carlos Corraliza Torres	Director de la Oficina de Administración	16 oct. 01	28 jun. 02
Sr. Jaime Belgodere Marietti	Director de la Oficina de Sistemas de Información	16 oct. 01	28 jun. 02
Sra. Rosana Medina Peraza	Directora de la Oficina de Auditoría Interna	16 oct. 01	28 jun. 02