INFORME DE AUDITORÍA TI-12-07

13 de febrero de 2012

Departamento del Trabajo y Recursos Humanos

Administración del Derecho al Trabajo

Oficina de Informática

(Unidad 5020 - Auditoría 13290)

Período auditado: 13 de abril al 15 de septiembre de 2009

CONTENIDO

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

13 de febrero de 2012

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 Informática de la Administración del Derecho al Trabajo (ADT), adscrita al Departamento del Trabajo y Recursos Humanos, 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 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.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La ADT fue creada por virtud de la *Ley Núm. 115 del 21 de junio de 1968*. Esta se creó como una corporación pública y su misión es fomentar la creación, por parte de otras entidades públicas y privadas, de oportunidades adicionales de empleo, adiestramiento o readiestramiento.

En la *Ley Núm. 100 del 23 de junio de 1977*, se redenominó al Departamento del Trabajo como Departamento del Trabajo y Recursos Humanos (Departamento). Mediante dicha *Ley*, la ADT quedó adscrita al Departamento. Esto, con el propósito de integrar los esfuerzos existentes encaminados a combatir el desempleo y lograr una mayor utilización de los recursos humanos del país. Por virtud de la *Ley Núm. 100*, se le transfirieron al Secretario del Trabajo y Recursos Humanos (Secretario) los poderes, las funciones y las obligaciones conferidos

al Gobernador por la *Ley Núm. 115*, en lo que respecta al funcionamiento de la ADT. Mediante el *Plan de Reorganización Núm. 2* aprobado por el Gobernador el 4 de mayo de 1994, la ADT pasó a ser un componente operacional del Departamento. Las funciones ejecutivas de la ADT son ejercidas por un Administrador[1] nombrado por el Gobernador, previa recomendación del Secretario.

La ADT brindaba sus servicios a través de 12 oficinas, compartidas con el Departamento, las cuales se encontraban localizadas en Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Fajardo, Guayama, Manatí, Mayagüez, Ponce, San Germán y San Juan. El Administrador contaba para el desempeño de sus funciones con las siguientes unidades de asesoramiento que le respondían directamente: Área de Administración; Área de Adiestramiento y Empleo; Oficina de Recursos Humanos; Oficina de Asuntos Legales; Oficina de Monitoría y Auditoría Interna; Oficina de Planificación, Sistemas y Procedimientos; Oficina de Comunicaciones; y Oficina de Informática.

A la fecha de nuestra auditoría, el puesto de Director de Informática se encontraba vacante, por lo que se le asignó al Subadministrador la función de supervisión del personal de la Oficina de Informática. Esta contaba con una Administradora de Sistemas de Oficina, cuatro operadores de equipo de procesar información, tres programadores de sistemas de información, dos técnicos de red de computadoras y una Bibliotecaria de Sistemas de Información.

Mediante el *Plan de Reorganización Núm. 4* del 9 de diciembre de 2011 se reorganizó el Departamento mediante la consolidación y la transferencia a dicha agencia de las operaciones, el personal, los activos, las funciones y los poderes de la ADT.

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

La ADT tenía un computador principal que operaba en plataforma *mainframe* para procesar la nómina de participantes, la nómina administrativa y la contabilidad. A la fecha de nuestra auditoría, el computador principal contaba con aproximadamente 169 usuarios.

[1] A la fecha de nuestra auditoría, el Secretario también ejercía las funciones de Administrador.

El usuario principal de este sistema era el Área de Administración, el cual era dirigido por una Administradora Auxiliar. A su vez, el Área de Administración era apoyada tecnológicamente por la Oficina de Informática, la cual respondía al Administrador. Además, la ADT contaba con una red de comunicaciones, compuesta por 14 servidores y 183 computadoras, que proveía a los usuarios acceso a Internet y al correo electrónico, y la interconexión a 11 de sus oficinas locales.

El presupuesto de la ADT se componía de resoluciones conjuntas del presupuesto general, asignaciones especiales y fondos federales. Para los años fiscales 2008-09 y 2009-10, el presupuesto ascendió a $17,687,000 y $11,545,000, respectivamente.

RESPONSABILIDAD DE LA GERENCIA

La gerencia de todo organismo gubernamental debe considerar los siguientes *Diez Principios para Lograr una Administración Pública de Excelencia*. Estos 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 13 de abril al 15 de septiembre de 2009. 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 información financiera, de procedimientos de control interno y de otros procesos
- confirmaciones de información pertinente.

OPINIÓN

Las pruebas efectuadas revelaron que las operaciones de la Oficina de Informática de la ADT, en lo que concierne a los controles internos relacionados con el acceso lógico y físico, la administración del programa de seguridad, la segregación de deberes, la evaluación de la continuidad de servicio, los controles sobre las aplicaciones y el mantenimiento a los sistemas operativos, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 14**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

INFORME DE AUDITORÍA ANTERIOR

En el *Informe de Auditoría CPED-97-9* del 30 de junio de 1997 fueron objeto de recomendaciones tres situaciones similares a las comentadas en los **hallazgos 7-a., 11 y 12-a.** No obstante, dichas recomendaciones no fueron atendidas.

RECOMENDACIONES

AL SECRETARIO DEL TRABAJO Y RECURSOS HUMANOS

1. Ver que en contrataciones futuras se protejan los mejores intereses del Departamento, y tomar las medidas correctivas que procedan para evitar que ocurran situaciones como la comentada en el **Hallazgo 1**.

2. Ver que se realice un análisis de riesgos que considere los sistemas computadorizados que operaban en la ADT, según se establece en la *Política Núm. TIG-003, Seguridad de los Sistemas de Información 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, y según se sugieren en las mejores prácticas en el campo de la tecnología. El informe, producto de este análisis de riesgos, debe ser remitido para su revisión y aprobación. **[Hallazgo 2]**

3. Realizar las gestiones pertinentes para asegurarse de que se prepare un *Plan para la Continuidad de Negocios*, que incluya un *Plan para la Recuperación de Desastres* y un *Plan para la Continuidad de las Operaciones*, que considere los sistemas computadorizados que operaban en la ADT, y que los mismos se remitan para su revisión y aprobación. Una vez estos sean aprobados, tomar las medidas necesarias para asegurarse de que se mantengan actualizados y se conserve una copia en un lugar seguro fuera de los

predios del Departamento. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados concernientes, y que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 4-a.]**

4. Ejercer una supervisión efectiva sobre el Director de Cómputos y Sistemas de Información para asegurarse de que:

   a. Prepare y remita, para su consideración y aprobación, un plan de seguridad en el que se establezcan los proyectos, las tareas y las actividades requeridos para proteger al personal y a los activos de los sistemas de información que operaban en la ADT. Una vez aprobado, asegurarse de que se divulgue a los funcionarios y a los empleados concernientes, y se realicen pruebas periódicas del mismo. **[Hallazgo 3-a.]**

   b. Prepare y remita, para su consideración y aprobación, las normas y los procedimientos escritos para el manejo de incidentes que incluya los requisitos indicados en el **Hallazgo 3-c.**

   c. Prepare y remita, para su consideración y aprobación, el *Plan de Contingencias* que considere los sistemas computadorizados que operaban en la ADT y los aspectos comentados en el **Hallazgo 4-b.**

   d. Establezca procedimientos para preparar y mantener los respaldos (*backups*) de los datos, la documentación de los programas y las aplicaciones que operaban en la ADT. Además, se asegure de que dicho procedimiento incluya el mantener los respaldos en un lugar seguro fuera de los predios del Departamento. **[Hallazgo 5-a.1) y 2)]**

   e. Mantenga un registro de los respaldos que le permita controlar y documentar adecuadamente la preparación de estos. Además, se asegure de que el registro contenga la información que se indica en el **Hallazgo 5-a.3)**.

f. Mantenga copias de los manuales de operación de los sistemas de información que operaban en la ADT y de la documentación de las aplicaciones, los servidores, los programas y las bases de datos, en un lugar seguro fuera de los predios del Departamento, para poder utilizarlos en caso de una emergencia. **[Hallazgo 5-b.]**

g. Ejerza una supervisión eficaz sobre el personal encargado de la administración de la red para que:

1) Evalúe las opciones correspondientes a las políticas de auditorías (*Audit Policy*), los parámetros de seguridad (*Security Options*) y los privilegios a los usuarios (*User Rights Assignment*), y active las que considere necesarias de acuerdo con los riesgos y las amenazas de la entidad. **[Hallazgo del 6-a.1) al 3)]**

2) Relacionado con el **Hallazgo 6-a.4)**, configure los registros (*logs*) de los eventos de seguridad, aplicación y sistema del servidor principal para:

a) Definir el tamaño adecuado de los registros según la criticidad de los datos, la frecuencia de revisión de los registros y el espacio disponible en el disco de los servidores. Una vez se alcance el tamaño definido, realice un respaldo de los mismos.

b) Restringir el acceso a los registros a personas autorizadas.

c) Examinar periódicamente los eventos o los incidentes grabados en los registros provistos por el sistema operativo del servidor principal para conocer las posibles violaciones de seguridad que pudieran ocurrir en los sistemas de información de la red y tomar prontamente las medidas preventivas y correctivas necesarias.

d) Revisar periódicamente los eventos registrados en el servidor principal y, de ser necesario, tomar de inmediato las medidas preventivas y correctivas.

3) Prepare y remita para su aprobación, el diagrama esquemático de la red e incluya en el mismo la configuración de los cuartos de comunicación y la descripción del equipo que utiliza como respaldo, en caso de que la comunicación con los servidores se interrumpa. **[Hallazgo 9]**

h. Desarrolle y remita, para su consideración y aprobación, los procedimientos que se comentan en el **Hallazgo 7-a. y b.1)**. Una vez aprobados, se asegure de que se oriente al personal sobre las disposiciones de los mismos.

i. Revise y remita, para su consideración y aprobación, el *Procedimiento Clave de Acceso Usuarios*, el *Procedimiento Tarjetas de Acceso a la Oficina de Informática*, y el *Procedimiento para la Producción y Protección de Cintas Magnéticas y/o Cartuchos de Reserva*, para que incluyan los aspectos comentados en el **Hallazgo del 7-b.2) al 4)**. Una vez aprobados, se asegure de que se distribuyan al personal que llevará a cabo los procesos establecidos en los mismos.

j. Establezca las medidas de control necesarias para corregir las situaciones, relacionadas con la protección ambiental y física de los equipos computadorizados, comentadas en el **Hallazgo 8**.

k. Cumpla con lo establecido en el *Procedimiento Clave de Acceso Usuarios* y en la *Carta Circular Núm. 01-001, Utilización del Correo Electrónico e Internet* para la autorización del acceso a la red e Internet, respectivamente. **[Hallazgo 10-a. y b.]**

l. Verifique que los formularios para solicitar acceso a la red de comunicaciones, Internet y correo electrónico, sean completados debidamente antes de crear cuentas de acceso para consultores externos. **[Hallazgo 10-b.]**

m. Prepare y remita, para su consideración y aprobación, un procedimiento para el control de los cambios que establezca, entre otras cosas, un formulario oficial y uniforme para solicitar los cambios en las aplicaciones instaladas en el computador principal (*mainframe*), que incluya la información mencionada en el **Hallazgo 10-c.** y que se mantenga como parte de la documentación permanente del sistema.

n. Mantenga una segregación adecuada de las funciones conflictivas realizadas por la Bibliotecaria de Sistemas de Información y por la Programadora de Sistemas de Información III, o establezca controles compensatorios que mitiguen el riesgo resultante de una falta de segregación de funciones adecuada. **[Hallazgo 12-a.]**

o. Establezca, en coordinación con la Directora de Recursos Humanos, un plan para ofrecer adiestramientos técnicos y periódicos al personal que laboraba en la Oficina de Informática de la ADT y un programa de adiestramiento escrito para ofrecer orientaciones periódicas a los empleados que laboraban en la ADT sobre la seguridad de los sistemas de información. En el mismo se debe ofrecer información sobre la seguridad de acceso lógico y físico, el manejo y el control de las contraseñas, la producción de respaldos, y las normas de uso de los equipos y sistemas de información computadorizados. Además, se deben ofrecer orientaciones periódicas a todo el personal que laboraba en la ADT sobre los planes establecidos de seguridad y de contingencias. **[Hallazgo 14]**

5. Ejercer una supervisión eficaz sobre la Directora de Recursos Humanos para asegurarse de que:

a. Prepare acuerdos de confidencialidad escritos, dirigidos a los empleados que trabajen con datos confidenciales y activos sensitivos. Estos acuerdos deben establecer el período de no divulgación posterior a la fecha de terminación del empleo. **[Hallazgo 3-b.]**

b. Prepare y remita, para su consideración y aprobación, las normas y los procedimientos necesarios para el traslado y la separación del personal que tiene acceso a los sistemas de información. **[Hallazgo 13]**

6. Realizar las gestiones necesarias para crear el puesto de Administrador de Red, y evaluar la posibilidad de reclasificar en este puesto a la Programadora de Sistemas de Información III, que realiza las funciones del mismo. **[Hallazgo 12-b.]**

AL DIRECTOR DE LA OFICINA DEL INSPECTOR GENERAL DEL GOBIERNO DE PUERTO RICO

7. Evaluar la situación comentada en el **Hallazgo 11** y tomar las medidas que correspondan.

CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos del 1 al 14**, incluidos en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**, se informaron al Hon. Miguel A. Romero Lugo, Secretario del Trabajo y Recursos Humanos, y al Sr. Ángel A. Santiago Torres, entonces Administrador Interino de la ADT[2], en carta de nuestros auditores del 10 de noviembre de 2009. Con la referida carta se incluyeron anejos que especifican detalles sobre las situaciones comentadas.

El borrador de los **hallazgos** de este *Informe* se remitió al Secretario y al señor Santiago Torres, entonces Administrador de la ADT, para comentarios, en cartas del 10 de febrero de 2011.

COMENTARIOS DE LA GERENCIA

El 30 de noviembre de 2009, el Secretario y el entonces Administrador Interino remitieron sus comentarios sobre los **hallazgos** incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador del *Informe*.

El Administrador de la ADT contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 24 de febrero de 2011. El Secretario contestó el borrador de los **hallazgos** de este *Informe* en carta del 25 de febrero de 2011, la cual se recibió en nuestra Oficina el 7 de marzo de 2011. 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

[2] El Hon. Miguel A. Romero Lugo fue Administrador de la ADT hasta el 21 de octubre de 2009. El 22 de octubre de 2009, se nombró como Administrador Interino al Sr. Ángel A. Santiago Torres, quien ocupaba el puesto de Subadministrador.

RELACION DETALLADA DE HALLAZGOS, bajo la sección HALLAZGOS EN LA OFICINA DE INFORMÁTICA DE LA ADMINISTRACIÓN DEL DERECHO AL TRABAJO, ADSCRITA AL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS.

AGRADECIMIENTO

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

Por: Oficina del Contralor
Yasmin M Valdivieso

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. Estos 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.

En la sección sobre los **COMENTARIOS DE LA GERENCIA** se indica si el funcionario principal de la unidad auditada efectuó comentarios sobre el borrador de los hallazgos del informe, que le 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 INFORMÁTICA DE LA ADMINISTRACIÓN DEL DERECHO AL TRABAJO, ADSCRITA AL DEPARTAMENTO DEL TRABAJO Y

RECURSOS HUMANOS., 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, este 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 INFORMÁTICA DE LA ADMINISTRACIÓN DEL DERECHO AL TRABAJO, ADSCRITA AL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

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

Hallazgo 1 - Gastos innecesarios incurridos en la contratación de servicios de almacenamiento en bóveda para mantener los respaldos de la ADT

a. Del 1 de julio de 1999 al 30 de junio de 2009, la ADT formalizó dos contratos con la Compañía A: el Contrato Núm. 2000-023, cuya vigencia era del 1 de julio de 1999 al 30 de junio de 2004, y el Contrato Núm. 2005-00048, cuya vigencia era del 1 de julio de 2004 al 30 de junio de 2009. El costo de cada uno de estos contratos fue de $118,080. Mediante estos contratos la compañía contratada acordó ofrecer a la ADT un centro de respaldo de desastres y contingencias para llevar a cabo el procesamiento de información, en caso de que condiciones imprevistas ocasionaran que el equipo de la Oficina de Informática no se pudiera utilizar.

   Como parte de dichos contratos, la ADT tenía a su disposición el servicio de almacenamiento en bóveda, el cual estaba incluido en el costo del contrato para mantener los respaldos y la documentación necesaria fuera de sus predios, y poder procesar la información en caso de ocurrir una emergencia. A pesar de esto, durante el mismo período en el que estuvieron vigentes estos contratos, la ADT formalizó otros 10 contratos[3], con la Compañía B para los servicios de almacenamiento en bóveda[4]. Estos contratos ascendieron a $8,900.

[3] Una relación de los contratos de la Compañía B se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al Administrador de la ADT.

[4] A la fecha de nuestra auditoría los respaldos se mantenían en la Compañía B.

En el Artículo 2.(e) de la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, se establece como política pública que exista un control previo de todas las operaciones del Gobierno; que sirva en el desarrollo de los programas encomendados a cada dependencia o entidad corporativa. En consonancia con dicha disposición, y como norma de sana administración, los funcionarios a cargo de administrar los fondos de las agencias deben tomar las medidas necesarias para proteger adecuadamente los intereses de estas, por lo que la ADT debió asegurarse de que los servicios que se contrataron eran necesarios y se realizaran de forma tal que se protegieran sus mejores intereses.

Además, en el Artículo 2.(f) y (g) de la *Ley Núm. 230* se establece que, independientemente del control previo general que se establezca para todas las operaciones de cada rama del Gobierno, los jefes de dependencia, entidades corporativas y cuerpos legislativos serán, en primera instancia, responsables de la legalidad, la corrección, la exactitud, la necesidad y la propiedad de las operaciones fiscales que sean necesarias para llevar a cabo sus respectivos programas, y de que los gastos del Gobierno se hagan dentro de un marco de utilidad y austeridad.

La situación comentada provocó que la ADT realizara pagos por $8,900 por servicios de almacenamiento de respaldos, que estaban incluidos en los contratos núms. 2000-023 y 2005-00048.

La situación comentada se debió a que los funcionarios que actuaron como Administrador, y los funcionarios que tuvieron a su cargo la formalización de los contratos, no protegieron adecuadamente los intereses de la ADT.

El Administrador informó en la carta que nos envió, entre otras cosas, la medida implantada para corregir la situación comentada en el **Hallazgo**.

Hallazgo 2 - Falta de un informe de avalúo de riesgos

a. Un avalúo de riesgos es un método para identificar las vulnerabilidades y las amenazas a los recursos de sistemas de información. Además, evalúa los posibles daños para determinar dónde implantar las medidas de seguridad para poder alcanzar y cumplir con los objetivos de la entidad gubernamental. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.
- Identificar las vulnerabilidades y las amenazas de los recursos de sistemas de información.
- Cuantificar la probabilidad y el impacto de las amenazas potenciales en las operaciones de la entidad gubernamental.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 5 de mayo de 2009, en la ADT no se había realizado un avalúo de riesgos sobre los sistemas de información computadorizados.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, que cada agencia deberá implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Para esto, deberá llevar a cabo un análisis de riesgos que incluya:

- Un inventario de los activos de sistemas de información, incluidos el equipo, los programas y los datos. Todos los activos deberán ser clasificados de acuerdo con el

nivel de importancia para la continuidad de las operaciones. En particular, los datos electrónicos deberán ser clasificados de acuerdo con su nivel de confidencialidad. Esto permitirá establecer qué es lo que se va a proteger.

- Las posibles amenazas contra los sistemas de información (robos, desastres naturales, fallas, virus y acceso indebido a los datos, entre otras), junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

La situación comentada impidió a la ADT evaluar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de esta, y de considerar cómo protegerlos para reducir los riesgos de daños materiales y de pérdida de información. Además, impidió el desarrollo de un plan de continuidad de negocios donde se establezcan las medidas de control que minimicen los riesgos previamente identificados a un nivel aceptable, y los pasos a seguir para restablecer las operaciones de la ADT, en caso de que surja alguna eventualidad. **[Véase el Hallazgo 4]**

La situación comentada se atribuye a que el Administrador no había promulgado una directriz para la preparación y la documentación del avalúo de riesgos de los sistemas de información de la ADT, según establecido en la *Carta Circular Núm. 77-05*.

Hallazgo 3 - Falta de un plan de seguridad y de acuerdos de confidencialidad, y deficiencias relacionadas con el plan para el manejo de incidentes

a. Al 8 de julio de 2009, la ADT no tenía un plan de seguridad aprobado por el Administrador, que incluyera, entre otras cosas, disposiciones en cuanto a:

- La documentación de la validación de las normas de seguridad[5]

- La evidencia de un análisis de riesgos actualizado, que sea la base del plan

[5] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y vulnerabilidades detectadas en el avalúo de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

- La responsabilidad de la gerencia y de los demás componentes de la unidad

- Un programa de adiestramiento especializado al equipo clave de seguridad

- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, los contratistas, el personal de sistemas de información y los usuarios, y el cual permita mantener los conocimientos actualizados

- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros)

- La documentación de la interconexión de los sistemas.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. También se establece que las entidades gubernamentales son responsables de:

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

- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones para que se les transmitan los conocimientos actualizados sobre los aspectos de seguridad de sus áreas.

- Crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que les apliquen.

Las mejores prácticas en el campo de tecnología de información sugieren que las entidades deben mantener un plan escrito que describa claramente el programa de seguridad y los procedimientos relacionados con este. El mismo debe considerar los sistemas y las

instalaciones principales e identificar los deberes de los dueños y de los usuarios de los sistemas de información de la entidad, y de los empleados responsables de velar por la seguridad de dichos sistemas.

La falta de un plan de seguridad podría provocar la inversión de recursos en medidas de control inadecuadas, el desconocimiento y la falta de entendimiento de las responsabilidades relacionadas con la seguridad, y la protección inadecuada de los recursos críticos.

La situación comentada se atribuye a que el Administrador no había promulgado una directriz para la preparación del plan de seguridad.

b. Al 26 de mayo de 2009, la ADT no había establecido acuerdos escritos de confidencialidad con los empleados antes de exponerlos a información confidencial u otros activos sensitivos.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, que las agencias establecerán controles en el reclutamiento del personal de sistemas de información, especialmente en el área de seguridad, que requieran que este firme acuerdos de no divulgación antes de exponerlo a información confidencial o a otros activos sensitivos como los programas y los equipos.

Esta situación podría dar lugar al uso indebido de información privilegiada y a que, de ocurrir, se dificulte fijar responsabilidades. Esto, a su vez, resultaría en otras consecuencias adversas para la ADT.

La situación comentada obedece, principalmente, a que el Administrador no le había requerido a la Directora de la Oficina de Recursos Humanos desarrollar y remitir, para su consideración y aprobación, acuerdos de confidencialidad escritos, dirigidos a los empleados que tienen acceso a datos confidenciales y a activos sensitivos.

c. El procedimiento *Documentación del Sistema del Control de Llamadas de Servicio*, que nos fue provisto como plan para el manejo de incidentes, no incluía los siguientes requisitos que son necesarios para atender incidentes:

- Clasificación de los incidentes por niveles, ya sea, incidentes sin importancia, eventos menores, incidentes mayores o crisis, y establecimiento de un nivel de impacto sobre las operaciones.
- Especificación del término máximo y mínimo de respuesta.
- Establecimiento de un protocolo a seguir para notificar y documentar los incidentes.
- Notificación al personal con funciones de seguridad en el área de servidores y en el *mainframe*.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, que las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad, incluidos límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta. Además, se establece que todos los empleados y los contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes.

La situación comentada le impide a la Oficina de Informática tener un control eficaz y documentado sobre el manejo de incidentes. Además, puede provocar duplicidad de esfuerzo y tiempo ante situaciones inesperadas, lo que afectaría el restablecimiento de los sistemas con prontitud y aumentaría la extensión de los daños, si alguno.

La situación comentada se atribuye a que el Subadministrador[6] no había requerido que se incluyera en la *Documentación del Sistema de Control de Llamadas de Servicio* los requisitos esenciales que debe tener un plan de manejo de incidentes.

[6] Durante el período de la auditoría el puesto de Director de Informática estuvo vacante, por lo que se le asignó al Subadministrador la función de supervisión del personal de la Oficina de Informática.

Hallazgo 4 - Falta de un plan de continuidad de negocios, y deficiencias en el plan de contingencias para los sistemas de información de la ADT

a. Al 8 de julio de 2009, la ADT carecía de un plan de continuidad de negocios que incluyera los planes específicos, completos y actualizados de la Oficina de Informática. Esto era necesario para lograr el pronto funcionamiento de los sistemas de información computadorizados y restaurar las operaciones de la Oficina de Informática en caso de riesgos, tales como: inundaciones, variaciones de voltaje o virus de computadoras, entre otros.

   En la *Política Núm. TIG-003* de la *Carta Circular 77-05* se establece que las entidades gubernamentales deberán desarrollar un *Plan de Continuidad de Negocios* que incluya un *Plan para la Recuperación de Desastres* y un *Plan para la Continuidad de las Operaciones*.

b. El examen efectuado al *Plan de Contingencias para el Control de Desastres y/o Emergencias de la Oficina de Informática* (*Plan*) provisto a nuestros auditores el 13 de abril de 2009, reveló las siguientes deficiencias:

   1) No estaba aprobado por el Administrador de la ADT.

   2) No estaba actualizado. El mismo incluía áreas y puestos que ya no existen en la Oficina de Informática.

   3) No incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:

      - las estrategias a utilizarse para efectuar y documentar las pruebas o los simulacros, que certifiquen la efectividad del *Plan*

      - el nombre del encargado de activar el *Plan* y del personal de reserva, de forma tal que pueda ser ejecutado sin depender de individuos específicos

      - el plan general de acción identificado por grupo y tareas de forma secuencial

- el inventario de equipos, sistemas operativos y aplicaciones
- el detalle de la configuración de los equipos críticos (*mainframe*, equipos de comunicaciones y servidores) y del contenido de los respaldos, así como los nombres de las librerías
- el detalle de la configuración de los sistemas y de los equipos de comunicación utilizados en la Oficina de Informática requeridos para el centro alterno
- un itinerario de restauración que incluya el orden de las aplicaciones a restaurar y los procedimientos para restaurar los respaldos
- los procedimientos a seguir cuando el centro de cómputos no puede recibir ni transmitir información
- una hoja de cotejo para verificar los daños ocasionados por la contingencia.

Las mejores prácticas en el campo de la tecnología utilizadas para garantizar la confiabilidad, la integridad y la disponibilidad de los sistemas de información computadorizados sugieren que como parte del *Plan de Continuidad de Negocios* se deberá preparar un *Plan de Contingencias*. Este es una guía que asegura la continuidad de las operaciones normales de los sistemas de información computadorizados cuando se presentan eventualidades inesperadas que afectan su funcionamiento. El mismo deberá estar aprobado por el funcionario de máxima autoridad de la agencia y deberá incluir todos los procesos necesarios para recuperar cualquier segmento de la operación del centro de cómputos o, si fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable.

De ocurrir una emergencia, las situaciones comentadas podrían dar lugar a que el equipo no se proteja adecuadamente y sufra daños materiales, así como a la pérdida de información importante. Además, se podría atrasar el proceso de reconstrucción de archivos y programas, y el pronto restablecimiento y la continuidad de las operaciones normales de los sistemas de información.

Las situaciones comentadas se atribuyen a que el Administrador no había requerido que se efectuara un avalúo de riesgos **[Véase el Hallazgo 2]** que sirviera de base para el desarrollo, la aprobación y la implantación de un plan de continuidad de negocios, que provea las herramientas para responder ante cualquier desastre que ocurra.

Además, las situaciones comentadas en el **apartado b.** se debían, en parte, a que el Administrador no había promulgado una directriz para la implantación y la continua actualización del *Plan*. Además, no se aseguró de que se incluyeran en el *Plan* los requisitos mencionados.

El Administrador, en carta que nos envió, informó lo siguiente:

> Actualmente la operación del Centro de Cómputos de la Agencia se va a ejecutar a través del Departamento del Trabajo, por lo tanto ellos serán responsables de la continuidad del Plan en el área de Informática. [*sic*]

Hallazgo 5 - Deficiencias relacionadas con el almacenamiento de los respaldos de información, y falta de almacenamiento de los manuales de operación y de la documentación de las aplicaciones, los programas y las bases de datos en un lugar seguro fuera de los predios de la ADT

a. Al 11 de mayo de 2009, la Bibliotecaria de Sistemas de Información realizaba los respaldos de la información mantenida en el computador principal que incluía las transacciones de nómina del Sistema de Participantes y del Sistema Administrativo, y las de contabilidad de la Aplicación Global. Estos respaldos se realizaban todos los martes y jueves y eran llevados a la Compañía B, el viernes de cada semana.

   Además, una de las programadoras de sistemas de información realizaba los respaldos de los 10 servidores[7] administrados por la Oficina de Informática. Los respaldos de dichos servidores se realizaban durante distintos días de la semana y eran guardados en el Área de la Biblioteca, dentro de una bóveda. Por otro lado, el Especialista de Adiestramiento y Servicio de Empleo y Desempleo II del Área de Programas de Empleo, Adiestramientos y

[7] Los nombres de los servidores se incluyeron en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al Administrador de la ADT.

Propuestas, realizaba el respaldo diario de un servidor[7], el cual era administrado por personal de esta área, y en el que se mantenía la base de datos de los participantes del Programa WIA 167.

El examen realizado sobre la preparación y el control de los respaldos de información reveló las siguientes deficiencias:

1) El respaldo diario del servidor ubicado en el Área de Programas de Empleo se almacenaba en el mismo servidor, en lugar de mantenerse en un lugar fuera del área donde este se encontraba.

2) No se mantenía una copia de los respaldos realizados a los servidores administrados por la Oficina de Informática y al servidor ubicado en el Área de Programas de Empleo, en un lugar seguro fuera de los predios de la ADT. Esto, a pesar de que la ADT mantenía un contrato con la Compañía A y otro con la Compañía B, mediante los cuales se proveía el servicio de bóveda para almacenar las copias de los respaldos en un lugar fuera de los predios de la entidad. **[Véase el Hallazgo 1]**

3) No se mantenía un registro de los respaldos preparados de los servidores en el cual se detallara la descripción de los archivos respaldados, el nombre del servidor donde se mantenían estos archivos, la última fecha de actualización de la información y la explicación de fallas o de situaciones especiales que ocurrieron, si alguna, durante la preparación de los respaldos.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que deberán existir procedimientos para tener y mantener una copia de respaldo (*backup*) recurrente de la información y de los programas de aplicación y de sistemas, esenciales e importantes, para las operaciones de la agencia. En consonancia con dicha política pública es necesario, entre otras cosas, que toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar fuera de los predios de la entidad. Esto, con el propósito de poder recuperar la mayor cantidad de información posible en caso de una emergencia o desastre. Además, es

necesario mantener un inventario detallado de los cartuchos de respaldos para facilitar su localización y para sustituir periódicamente, por cartuchos nuevos, los utilizados para los respaldos, y que permita, además, documentar el cumplimiento con las normas y con los procedimientos establecidos.

Las situaciones comentadas en el **apartado a.1) y 2)** podría ocasionar la pérdida permanente de información importante, sin la posibilidad de poder recuperarla, lo que afectaría adversamente las operaciones de la ADT.

La situación comentada en el **apartado a.3)** limitó el alcance de nuestro examen para determinar si los respaldos se habían preparado con la regularidad requerida. Además, puede dar lugar a que no se detecte a tiempo la pérdida de los cartuchos almacenados en la Oficina de Informática y dificulta la localización e identificación del contenido de las cintas de respaldos en caso de que se requiera reconstruir la información en forma efectiva.

Las situaciones comentadas se debían a que en el *Procedimiento para la Producción y Protección de Cintas Magnéticas y/o Cartuchos de Reserva* no se establecían directrices para producir los respaldos de la información y de los programas de los servidores, ni para mantener una copia de estos en un lugar fuera de los predios de la ADT. **[Véase el Hallazgo 7-b.4)]**

b. No se mantenían copias de los manuales de operación de los sistemas de información ni de la documentación de las aplicaciones, de los servidores, de los programas y de las bases de datos, en un lugar seguro fuera de los predios de la ADT.

Como norma de sana administración y de control interno se requiere que las entidades gubernamentales mantengan copias actualizadas de los manuales de operación de los sistemas de información y de la documentación de las aplicaciones, de los programas y de las bases de datos, en un lugar seguro fuera del edificio donde radica el centro. Esto es necesario para garantizar la continuidad de las operaciones en caso de que ocurra un evento inesperado.

La situación comentada podría afectar la continuidad de las operaciones normales de la Oficina de Informática si ocurriera alguna eventualidad que afectara las instalaciones de esta, y destruyera toda la documentación y los manuales que allí se almacenan. Además, la ADT no tendría acceso para iniciar el proceso de reconstrucción de archivos y programas, y el restablecimiento y la continuidad de las operaciones normales de los sistemas de información en un tiempo razonable.

La situación comentada se debía a que el Subadministrador de la ADT no había realizado las gestiones necesarias para mantener copia de la documentación mencionada en un lugar seguro fuera de los predios de la entidad.

El Administrador informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en los **apartados a.1) y 2), y b.** del **Hallazgo**.

Hallazgo 6 - Deficiencias relacionadas con los parámetros de seguridad del servidor principal de la ADT

a. El examen realizado el 15 de septiembre de 2009 de los parámetros de seguridad establecidos en el sistema operativo del servidor configurado como *Primary Domain Controller*, reveló las siguientes deficiencias:

1) No se había definido la política de auditoría (*Audit Policy*) para que el sistema produjera un registro cuando ocurrieran los siguientes eventos:

- las solicitudes al servidor para validar una cuenta de usuario (*Audit account logon events*)

- la creación, la modificación o la eliminación de una cuenta o grupo de usuarios, el cambio de nombre o contraseña y la activación o desactivación de una cuenta o grupo de usuarios (*Audit account management*)

- el acceso a los directorios de servicios (*Audit directory service access*)

- la conexión o desconexión de las cuentas de los usuarios (*Audit logon and logoff events*)
- los accesos a los archivos, cartapacios (*folders*) e impresoras (*Audit object access*)
- los cambios efectuados a las opciones de seguridad, a los privilegios de usuarios y a las políticas de auditoría (*Audit policy change*)
- el uso de los privilegios de los usuarios (*Audit priviledge use*)
- el seguimiento de los procesos (*Audit process tracking*)
- el reinicio, el apagado y los eventos que afectan al sistema de seguridad (*Audit system events*).

2) En la pantalla *Security Option* no se habían configurado 51 políticas de seguridad (*Security Options*)[8] de acuerdo con la recomendación de la industria.

3) No se habían definido cinco opciones para asignarles a los usuarios los siguientes privilegios (*User Rights Assignment*):

- Permitir la conexión a través del *Terminal Services*. Este privilegio debe ser otorgado a los administradores.
- Depurar programas (*Debug programs*). Este privilegio debe ser otorgado a los administradores.
- Prohibir el acceso a la computadora desde la red (*Deny access to this computer from network*). Este acceso se le debe prohibir a las cuentas de acceso anónimas, de visitantes (*Guests*) y de servicio no asociadas con el sistema operativo.

[8] Una relación de las políticas de seguridad se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al Administrador de la ADT.

- Prohibir la conexión de procedimiento en grupo (*Deny logon as a batch job*). Esta conexión se le debe prohibir a las cuentas de visitantes (*Guests*).

- Prohibir la conexión a través del *Terminal Services.* Esta conexión se le debe prohibir a las cuentas de acceso de visitantes (*Guests*).

4) No se habían configurado las políticas del registro de eventos (*Event Logs*) para lo siguiente:

- Definir el tamaño máximo de los registros de aplicación (*Maximum application log size*), de seguridad (*Maximun security log size*) y del sistema (*Maximum system log size*).

- Restringir el acceso de las cuentas de invitados a los registros de aplicación (*Restrict guest access to application log*), de seguridad (*Restrict guest access to security log*) y del sistema (*Restrict guest access to system log*).

- Establecer el método de retención de los registros de aplicación (*Retention method for application log*), de seguridad (*Retention method for security log*) y del sistema (*Retention method for system log*).

En la *Política General sobre la Administración, Manejo y Seguridad de Información Computadorizada, Internet y Mensajería Electrónica*, aprobada el 4 de marzo de 2008 por el Secretario (*Política General*), se establece como objetivo el asegurar la integridad y la exactitud de la información de las agencias, y protegerla contra su modificación, divulgación, manipulación o destrucción no autorizada o accidental. Además, se dispone que la Oficina de Informática debe mantener documentación (en forma de *log* o de bitácora) de cambios, problemas, servicios, mantenimientos, pruebas, modificaciones en programación, violaciones y atentados contra la seguridad de los sistemas.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que las agencias son responsables de desarrollar procedimientos para detectar, informar y responder a incidentes de seguridad, incluidos límites para esos incidentes en términos de tiempo

máximo y mínimo de respuesta. Esta política se implementa, en parte, mediante la activación de todas las opciones para registrar los eventos de seguridad, de las aplicaciones y del sistema, y mediante la revisión continua, por el personal técnico especializado, de los registros computadorizados producidos por el servidor principal.

Las situaciones comentadas en el **apartado a.1)** impiden la detección temprana de errores críticos o problemas con los servidores que permitan tomar de inmediato las medidas preventivas y correctivas necesarias. Además, privan a la gerencia de los medios necesarios para supervisar eficazmente el desempeño de los usuarios, y detectar el acceso y uso indebido de los sistemas computadorizados.

Las situaciones comentadas en el **apartado del a.2) al 4)** propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información, sin que puedan ser detectados a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían, principalmente, a que el Subadministrador no había preparado, para la aprobación del Administrador, los procedimientos necesarios para la administración de la red. **[Véase el Hallazgo 7-a.]** En estos deben incluirse, entre otras cosas, las instrucciones para que el personal encargado de administrar la red active las opciones de seguridad que proveen los sistemas operativos, limite el acceso a los archivos de datos de los usuarios y establezca los controles adecuados para evaluar periódicamente los registros de seguridad.

El Administrador informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Hallazgo 7 - Falta de normas y de procedimientos para reglamentar la administración, la seguridad y el uso de los sistemas computadorizados

a. A julio de 2009, la ADT no había promulgado las normas ni los procedimientos necesarios para reglamentar los siguientes procesos de la Oficina de Informática:

- la instalación, configuración y administración de la red
- la configuración, producción y revisión de los registros de eventos de los servidores
- la autorización del acceso a las aplicaciones del sistema operativo
- el uso y la revisión de los programas de utilerías
- la solicitud, autorización y aprobación de los cambios a las aplicaciones instaladas en el *mainframe*.
- la identificación, selección, instalación y modificación del sistema operativo de las computadoras
- la identificación y documentación de los problemas con las aplicaciones de sistema operativo
- el control de los cambios de emergencia a la configuración de las aplicaciones de sistema operativo.

Una situación similar se comentó en el *Informe de Auditoría CPED-97-9*.

b. Al 13 de abril de 2009, nos suministraron los procedimientos de los sistemas de información computadorizados mantenidos por la Oficina de Informática de la ADT. El examen de esta documentación reveló las siguientes deficiencias:

1) Al 15 de abril de 2009, la Oficina de Planificación, Sistemas y Procedimientos había preparado 26 procedimientos operacionales para la Oficina de Informática. Sin embargo, 24 de estos (92 por ciento) no habían sido aprobados por el Administrador[9].

2) En el *Procedimiento Clave de Acceso Usuarios* no se establecían directrices para:

- Requerir que las contraseñas utilizadas fueran combinaciones alfanuméricas.
- Requerir un mínimo de cinco contraseñas diferentes antes de volver a utilizar la misma.
- Requerir un mínimo de seis caracteres para el establecimiento de las contraseñas.
- Establecer que las contraseñas sean cambiadas periódicamente.
- Documentar la solicitud, la aprobación, la creación, la modificación y la cancelación de las cuentas de los usuarios que requieren acceso remoto a la red.

3) En el *Procedimiento Tarjetas de Acceso a la Oficina de Informática* no se establecían directrices para:

- Codificar el acceso para el Área de Red y el Área de Técnicos.
- Mantener un registro e inventario de las tarjetas utilizadas para dar acceso a la Oficina de Informática y sus áreas.
- Mantener una lista del personal autorizado para entrar a la Oficina de Informática.

[9] Una relación de los procedimientos se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Secretario y al Administrador de la ADT.

- Configurar las tarjetas de acceso para que estén de acuerdo con las funciones y el horario establecido para cada empleado.

- Prohibir que presten o compartan las tarjetas de acceso con otros empleados, y notificar la pérdida de las mismas.

- Establecer un mínimo de tiempo para que los códigos de acceso se cambien periódicamente.

- Cancelar los accesos físicos de los exempleados de la Oficina de Informática.

4) En el *Procedimiento para la Producción y Protección de Cintas Magnéticas y/o Cartuchos de Reserva* no se establecían directrices para:

- Identificar los servidores a los que se les debe realizar el respaldo de la información.

- Definir las especificaciones de respaldo, el método, la frecuencia de ejecución, los directorios y los archivos, y establecer períodos de retención para los respaldos.

- Verificar y registrar los respaldos.

- Manejar los errores.

- Archivar los cartuchos de respaldos.

- Restaurar la información respaldada.

- Producir los respaldos de información y programas de los servidores, y mantener una copia de estos en un lugar fuera de los predios de la ADT.

- Implantar las medidas de seguridad y los controles de acceso para la administración de los respaldos.

- Establecer que se realicen inventarios de los cartuchos en la bóveda y el centro alterno.

En la Sección 8 de la *Ley Núm. 115* se establece que la ADT tiene el derecho y el poder de establecer las normas y las reglamentaciones internas necesarias para su operación y funcionamiento. Esto implica que se adopten, revisen y aprueben normas y procedimientos escritos y específicos para reglamentar todas las operaciones de los equipos computadorizados.

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. Será responsabilidad de cada entidad gubernamental desarrollar normas específicas que consideren las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. Esto implica que, como norma de sana administración, se deben establecer políticas, normas y procedimientos de control interno escritos que reglamenten las operaciones computadorizadas, y que estén aprobados por la alta gerencia. Mediante los mismos se logran definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia, y facilitan la labor de adiestramiento.

Además, en la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de dicha *Carta Circular* se dispone que cada agencia debe establecer las políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y de las herramientas de trabajo que estos proveen.

Las situaciones comentadas podrían ocasionar que las operaciones de los sistemas de información computadorizados no se realicen de manera uniforme. Esto puede dar lugar a la comisión de errores e irregularidades sin que se puedan detectar a tiempo para fijar responsabilidades, y tomar las medidas correctivas necesarias. Además, podría exponer al personal de la Oficina de Informática, a los equipos y a la información de la ADT a riesgos innecesarios que pudieran afectar la continuidad de las operaciones.

La situación comentada en el **apartado b.2)** ocasionó, entre otras cosas, que los usuarios utilizaran contraseñas no alfanuméricas y de tres a cinco caracteres, y que los consultores y el personal de la Oficina de Informática tuvieran cuentas de acceso remoto a la red sin mantener la evidencia requerida para otorgar o cancelar el mismo.

La situación comentada en el **apartado b.3)** ocasionó, entre otras cosas, que no exista un control o inventario de las tarjetas de acceso utilizadas, y que los empleados de la Oficina de Informática tengan un acceso ilimitado y no restringido por sus funciones y horario de trabajo.

La situación comentada en el **apartado b.4)** ocasionó, entre otras cosas, que no exista un inventario de los cartuchos que se encuentran en el Área de Biblioteca.

La situación comentada en los **apartados a. y b.1)** obedecen, principalmente, a que el Administrador no le había requerido al Subadministrador que desarrollara y remitiera para su consideración y aprobación las normas y los procedimientos escritos necesarios para regular los procesos antes mencionados.

Las situaciones mencionadas en el **apartado del b.2) al 4)** se deben a que el Subadministrador no incluyó las directrices mencionadas en los procedimientos indicados.

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

> Esto no se ha podido implantar, ya que esa área no cuenta con Director y Administrador de Redes. Actualmente, tenemos un Director Interino, quien estará trabajando con esto. [*sic*]

Hallazgo 8 - Falta de controles ambientales y físicos en el computador principal y en el área de los servidores

a. En la Oficina de Informática de la ADT había un centro de cómputos en el cual se mantenía el computador principal y una oficina habilitada con 13 servidores[10]. En 10 de estos servidores, los cuales eran administrados por la Oficina de Informática, se procesaban los servicios de correo electrónico e Internet, entre otros, y se permitía la conexión de las

[10] Véase la nota al calce 7.

oficinas locales con el Sistema de Participantes. En los otros 3 servidores, los cuales eran administrados por personal del Área de Programas de Empleo, Adiestramientos y Propuestas, se mantenía información relacionada con el Programa WIA 167. Además, la ADT tenía en el Área de Programas de Empleo, Adiestramientos y Propuestas un servidor[11] en el cual se mantenía la aplicación del Programa WIA 167.

El examen efectuado entre el 25 de mayo de 2009 y el 9 de junio de 2009, sobre los controles ambientales[12] y físicos[13] existentes en el centro de cómputos y en las áreas en las que se mantenían los servidores, reveló que no se habían establecido las condiciones de seguridad física[14] adecuadas para proteger los sistemas de información computadorizados, según se indica:

1) Relacionado con los controles ambientales:

   a) En el centro de cómputos no se prohibía el consumo de alimentos para prevenir daños a los equipos computadorizados.

   b) En el centro de cómputos no tenían dispositivos de detección de agua y líneas redundantes de acondicionadores de aire.

---

[11] Véase la nota al calce 7.

[12] Controles diseñados para proteger las instalaciones y los equipos de eventos inesperados que ocurren naturalmente o son ocasionados por el hombre. Entre estos, tormentas, inundaciones, huracanes, terremotos, ataques terroristas, vandalismo, descargas eléctricas, tsunami y fallas de equipo.

[13] Controles diseñados para proteger la organización y sus instalaciones contra accesos no autorizados por medio de sistemas de cerraduras, remoción de discos innecesarios y sistemas de protección del perímetro, entre otros.

[14] Incluye los controles y los procedimientos establecidos para proteger a las personas, la información, los equipos, los sistemas y las instalaciones, al utilizar los mecanismos de seguridad que incluyen el diseño y la ubicación de las instalaciones, los componentes ambientales, las medidas de respuesta de emergencia, el control de acceso, la detección de intrusos y la protección contra fuego y pérdida de energía.

c) El lugar donde se encontraban los servidores en la Oficina de Informática y en el Área de Programas de Empleo, Adiestramiento y Propuesta, no contaban con líneas redundantes de acondicionadores de aires para la protección de los sistemas de información computadorizados. En el caso del área habilitada para los servidores de la Oficina de Informática, la temperatura no era adecuada debido al calor que generaban los servidores y al sol que entraba por la ventana. Además, el conducto de aire del área no funcionaba.

2) Relacionados con los controles físicos:

a) No se habían rotulado todos los puertos de los equipos de comunicaciones ubicados en el centro de cómputos ni los cables conectados a estos, para identificar la ruta de conectividad.

b) La puerta que daba acceso a la oficina habilitada para los servidores permanecía abierta a pesar de que la misma estaba programada para abrir con tarjeta magnética.

c) El servidor que se encontraba en el Área de Programas de Empleo, Adiestramientos y Propuestas se mantenía en un cubículo en donde no existían controles físicos para su seguridad.

En la Sección IV, Utilización de Recursos y Servicios, de la *Política General* se establece, entre otras cosas, que:

- El Departamento y sus componentes establecerán un control de acceso para el personal en los lugares donde se encuentran las máquinas principales.

- Se restringirá el acceso a toda persona ajena a las operaciones y al mantenimiento del sistema, y la Oficina de Informática deberá proveer control de acceso físico adicional, el cual deberá ser conocido y utilizado únicamente por los empleados que trabajan en el área.

- El personal de las agencias utilizará equipos electrónicos para facilitar y agilizar el flujo de tareas. Las agencias exigirán que su personal utilice estos equipos correctamente y que tome los cuidados necesarios para protegerlos y mantenerlos funcionando en óptimas condiciones y evitar daños y averías.

- Los usuarios no deberán llevar alimentos o bebidas a las áreas de trabajo donde existan equipos periféricos.

En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece que el acceso a las instalaciones de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas. Además, se establece que cada agencia será responsable de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas críticos. Esto implica que, como norma de sana administración, las agencias deberán tomar los cuidados necesarios para proteger y mantener funcionando en óptimas condiciones los equipos electrónicos para evitar daños y averías. El propósito es asegurar la integridad, la exactitud y la disponibilidad 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 que:

- se controle adecuadamente el acceso de personas a dichas áreas

- se utilice equipo y tecnología adecuada para proteger los sistemas, tales como: detectores de humo, alarmas, sistemas de supresión de incendio, extintores portátiles inspeccionados anualmente, detectores de agua, sistemas de enfriamiento redundante, cerraduras y cámaras de seguridad

- se mantenga la temperatura y la humedad requerida para el buen funcionamiento de los equipos

- se supervise al personal y se les oriente sobre las normas establecidas para prohibir consumir alimentos y mantener líquidos en estas instalaciones.

Las situaciones comentadas en el **apartado a.1)** pueden propiciar daños a las instalaciones y a los equipos, y provocar eventos de interrupción de servicios que afectarían la continuidad de las operaciones de los sistemas de información computadorizados de la ADT. Además, pueden aumentar los costos de mantenimiento debido al deterioro prematuro de los equipos.

Las situaciones comentadas en el **apartado a.2)a)** podrían dificultar la labor de mantenimiento que efectuaban los técnicos para resolver los problemas de comunicación e interrupciones de servicio, con los consiguientes efectos adversos como el retraso en las labores y el aumento en los costos relacionados.

Las situaciones comentadas en el **apartado a.2)b) y c)** pueden propiciar que personas no autorizadas o ajenas a la Oficina de Informática, por error o intencionalmente, causen daños al equipo o accedan indebidamente la información mantenida en los sistemas de información. Esto, a su vez, disminuye la confiabilidad de la información computadorizada, aumenta el riesgo de destrucción y divulgación indebida de la misma, dificulta la adjudicación de responsabilidades a las personas que cometan estos actos, y afecta adversamente el funcionamiento de la red y la continuidad de las operaciones.

Las situaciones comentadas se debían, en parte, a que el Subadministrador de la ADT no había tomado las medidas de control necesarias para la protección ambiental y física de los equipos computadorizados.

El Administrador informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Hallazgo 9 - Deficiencias relacionadas con el diagrama esquemático de la red de la ADT

a. El examen del diagrama esquemático (diagrama físico) de la infraestructura de la red de la ADT, suministrado para examen el 13 de abril de 2009, reveló las siguientes deficiencias:

- no estaba aprobado por la alta gerencia

- no incluía el detalle de las computadoras, las conexiones del equipo ni el cableado vertical (*backbone*)[15] instalados en 2 pisos de la ADT, y en 8 oficinas locales[16]

- no incluía tres *routers*[17] inalámbricos que son utilizados como respaldo en caso de que se interrumpa la comunicación con los servidores.

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica*, de la *Carta Circular Núm. 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 eficiente de servicios.

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

La situación comentada impide a la ADT tener una compresión clara y precisa sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento a la misma. Además, dificulta la atención de problemas de conexión en un tiempo razonable, y que se planifiquen efectivamente las mejoras a la red, según el crecimiento de sus sistemas.

---

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

[16] Las oficinas locales estaban localizadas en Aguadilla, Arecibo, Bayamón, Caguas, Carolina, Guayama, Mayagüez y Ponce.

[17] Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar los datos se realiza a base de la información de nivel de red y tablas de direccionamiento.

La situación comentada obedece, principalmente, a que el Subadministrador no había realizado las gestiones para desarrollar y remitir, para consideración y aprobación del Administrador, un diagrama esquemático representativo de la configuración de la red que incluya la descripción de los equipos instalados en la misma.

El Administrador informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Hallazgo 10 - Deficiencias encontradas en el proceso de solicitud de acceso a la red e Internet, y en los formularios de cambios en las aplicaciones

a. Al 13 de abril de 2009, la ADT tenía 130 usuarios con acceso a la red de los cuales 117 tenían acceso a Internet. La solicitud para la creación de una cuenta de acceso a la red se hacía mediante memorando en papel timbrado. En este memorando se indicaba el tipo de acceso deseado, la vigencia de la contraseña, los cambios de posición o de las responsabilidades del usuario y cualquier otra información pertinente al acceso solicitado. El acceso a Internet se solicitaba mediante el *Formulario ADT-AO-16, Solicitud de Acceso al Sistema de Correo Electrónico e Internet*. En este se indicaba el nombre del empleado, el puesto, el área o la división de trabajo y el propósito de la solicitud. El formulario lo firmaba el empleado y su supervisor.

El examen realizado el 14 de octubre del 2009 sobre la solicitud de acceso de los 130 y 117 usuarios con acceso a la red e Internet, respectivamente, reveló lo siguiente:

1) La solicitud de acceso a la red para 101 usuarios (78 por ciento) no se realizó mediante memorando en papel timbrado. El acceso a la red de estos usuarios se otorgó mediante correos electrónicos y memorandos escritos de los supervisores y directores de cada unidad, en los que solamente se solicitaba acceso al correo electrónico e Internet.

2) No se encontró evidencia de la solicitud de acceso a la red para siete usuarios (5 por ciento).

3) La solicitud de acceso a Internet para 83 usuarios (71 por ciento) no se realizó mediante el *Formulario ADT-AO-16*. La misma se hizo mediante correo electrónico o memorando escrito.

4) No se encontró evidencia de la solicitud de acceso a Internet para tres usuarios (3 por ciento).

b. Al 13 de abril de 2009, la ADT tenía dos consultores externos con acceso a la red, uno de los cuales también tenía acceso a Internet. Para dichos accesos no se documentó la solicitud, la justificación ni la aprobación de los mismos por parte del Subadministrador de la ADT. La solicitud y la autorización de estos accesos se realizó informalmente mediante una comunicación verbal.

En la Sección IV de la *Política General* se establece lo siguiente:

- La Oficina de Informática establecerá los controles de acceso a sus sistemas electrónicos de acuerdo con las necesidades de las agencias. La solicitud de acceso deberá indicar el nivel necesario para llevar a cabo la tarea, y será autorizada por el supervisor del usuario y enviada al encargado de los sistemas de información.

- La Oficina de Informática será responsable de crear y mantener un documento oficial que describa la asignación, el uso, el cambio y el control de las contraseñas. El documento debe permanecer guardado y ser utilizado solamente por el personal autorizado. El documento debe indicar, como mínimo, los medios de seguridad y el uso de las contraseñas para las maquinas; los nombres de las personas con acceso a cada máquina; el período de uso de las contraseñas; y la lista de contraseñas por máquina. Además, debe establecer las instrucciones para los cambios de una contraseña inmediatamente después de haber sido utilizada por personal de mantenimiento o servicio cuando se sospecha que se ha divulgado a personas ajenas, o cuando alguna persona en la lista de acceso termina su empleo en la agencia (por traslado o separación de cualquier índole).

- El encargado de los sistemas de información o su representante proveerá la solicitud de contraseña, asignándola de acuerdo con los estándares establecidos por la agencia. Las contraseñas pueden ser asignadas en varias etapas de la seguridad: acceso a la computadora (antes de acceder a la red); acceso a la red; acceso a los productos, aplicaciones o programas; y acceso específico a leer, escribir, borrar, ejecutar o editar archivos. Estas medidas se implementarán de acuerdo con las necesidades del Departamento y sus componentes operacionales.

En el *Procedimiento Clave de Acceso Usuarios*, aprobado por el Director de la Oficina de Informática, con fecha de efectividad del 1 de diciembre de 2000, se establece que el personal autorizado de cada unidad notificará al Director de la Oficina de Sistemas de Información, mediante memorando en papel timbrado, cuando desee que un usuario acceda al sistema computadorizado.

En la *Carta Circular Núm. 01-001, Utilización del Correo Electrónico e Internet*, aprobada el 15 de marzo de 2001 por la Administradora de la ADT, se establece que toda solicitud de acceso a los sistemas de Internet y al correo electrónico se hará por escrito mediante el *Formulario ADT-AO-16*.

Las situaciones comentadas impiden mantener la evidencia requerida para otorgar o cancelar los accesos y los privilegios a los usuarios. También propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en el Sistema, sin que puedan ser detectadas a tiempo para fijar responsabilidades.

Las situaciones comentadas se debían, principalmente, a que el Subadministrador de la ADT no había requerido que los supervisores inmediatos redactaran los memorandos para solicitar acceso a la red, según lo establecido en el *Procedimiento Clave de Acceso Usuarios*, y la utilización del *Formulario ADT-AO-06, Solicitud de Accesos al Sistema de Correo Electrónico e Internet*, para la autorización del acceso a Internet, según lo establece la *Carta Circular Núm. 01-001*. Además, no había requerido, antes de aprobar el acceso,

que la persona responsable de administrar la red cumpliera con la reglamentación interna, descrita anteriormente, para asegurar que los accesos a la red y a Internet estén debidamente documentados y autorizados por las partes correspondientes.

c. Al 11 de mayo de 2009, la ADT utilizaba diferentes versiones de formularios para añadir, corregir y realizar cambios a las aplicaciones instaladas en el *mainframe*. El examen realizado sobre los formularios para la solicitud de cambios a las aplicaciones reveló las siguientes deficiencias:

1) No se utilizaba un formulario oficial y uniforme para la solicitud de cambios a las aplicaciones, donde se asignara un número único de control para cada solicitud.

2) Los formularios utilizados no proveían para lo siguiente:

- Identificar si el cambio era estándar o de emergencia.
- Indicar el nombre del usuario que emite la solicitud.
- Indicar la fecha en que se emite la solicitud.
- Documentar el beneficio esperado.
- Documentar las actividades que se realizaron para la implementación del cambio.
- Aprobar o rechazar al usuario.
- Documentar la revisión posterior a la implementación.
- Indicar el nombre de la persona responsable de la revisión posterior a la implementación.

En la *Política Núm. TIG-011* de la *Carta Circular Núm. 77-05* se indica que se debe establecer una política del componente de datos e información mediante la cual las agencias mantengan uniformidad de los datos utilizados en sus sistemas. Los datos e información que las agencias mantienen son vitales para la toma de decisiones tanto para la agencia

como para el desarrollo de estrategias que benefician los servicios ofrecidos por el Gobierno del Estado Libre Asociado de Puerto Rico. Las agencias deben establecer metodologías para asegurar la integridad y la confiabilidad de los datos producidos y almacenados. También se indica que toda aplicación comercial o personalizada implantada debe ser documentada mediante metodologías de desarrollo y documentación estándares o de uso común.

Esta norma se instrumenta, en parte, mediante, lo siguiente:

- El desarrollo y la actualización de la documentación de los sistemas y el establecimiento de un proceso uniforme para realizar y documentar los cambios a los sistemas. Este proceso debe incluir los pasos para asegurar que los cambios al sistema estén de acuerdo con las necesidades de la organización, y debidamente autorizados, documentados, probados y aprobados por la gerencia.

- El establecimiento de algún tipo de correspondencia formal, como por ejemplo un formulario estándar que asegure que todos los cambios sean considerados para llevar a cabo una acción y que permita al personal correspondiente dar seguimiento a la solicitud con facilidad.

- La solicitud de cambio iniciada por el usuario final, así como por el personal operativo y el equipo de desarrollo y mantenimiento del sistema, debe incluir como mínimo el nombre del solicitante, la fecha de la solicitud, la fecha en que se necesita el cambio, la prioridad de la solicitud, una descripción minuciosa del cambio que se solicita y una descripción de cualquier efecto o efectos anticipados sobre otros sistemas o programas.

La situación comentada propicia, entre otras cosas, que:

- no se consideren todos los cambios a realizarse, y que se dificulte el seguimiento del estado de la solicitud por parte del personal responsable

- el usuario responsable de la aplicación no tenga conocimiento del cambio

- no se documente de forma adecuada el proceso de cambios a las aplicaciones instaladas en el *mainframe*.

La situación comentada se debía principalmente a que el Subadministrador de la ADT no había requerido que se preparara un procedimiento para el control de cambios en el que, entre otras cosas, se establezca la importancia de asegurar que los mismos sean documentados en un formulario oficial y uniforme. **[Véase el Hallazgo 7-a.]**

El Administrador informó en la carta que nos envió, entre otras cosas, las medidas implantadas para corregir las situaciones comentadas en el **Hallazgo**.

Hallazgo 11 - Falta de participación de la Oficina de Auditoría Interna y Monitoría en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información

a. Al 21 de abril de 2009[18], la Oficina de Auditoría Interna y Monitoría de la ADT no había efectuado auditorías de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados de la ADT.

Una situación similar se comentó en el *Informe de Auditoría CPED-97-9.*

En la Sección IV de la *Política General*, se establece que la Oficina de Informática y la Oficina de Auditoría Interna se reservan el derecho de vigilar, auditar y fiscalizar los servicios computadorizados para garantizar que se utilicen para propósitos y gestiones oficiales. Se realizarán auditorías internas, periódicas o al azar, como medida de prevención.

En las normas para la práctica profesional de la auditoría interna se establece, entre otras cosas, que la actividad de auditoría interna debe asistir a la organización mediante la identificación y la evaluación de las exposiciones de los riesgos, y contribuir al

[18] A esta fecha, la Oficina de Auditoría Interna y Monitoría de la ADT contaba con dos auditores y dos oficiales de monitoría.

mejoramiento de los sistemas de gestión de riesgos y control. También se establece que la actividad de auditoría interna debe evaluar las exposiciones de riesgo referidas a gobierno, las operaciones y los sistemas de información con relación a lo siguiente:

- confiabilidad e integridad de la información financiera y operativa
- eficacia y eficiencia de las operaciones
- protección de activos
- cumplimiento de las leyes, los reglamentos y los contratos.

La falta de fiscalización y de recomendaciones sobre los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados por parte de los auditores internos puede propiciar que se cometan errores e irregularidades sin que se puedan detectar 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 de la ADT. Además, existe la posibilidad de que no se incluyan en los sistemas de información los controles básicos necesarios para evitar incurrir en errores, irregularidades y otras situaciones adversas.

Esta situación se debía a que la Oficina de Auditoría Interna y Monitoría de la ADT no contaba con personal suficiente y adiestrado en el área de auditoría de sistemas de información.

El Administrador, en carta que nos envió, informó lo siguiente:

> Reconocemos el hallazgo, pero la Administración nunca asignó un Monitor a nuestra área, y en estos momentos con las cesantías y transferencia de personal, no contamos con Monitores, solamente el Director de la Oficina. [*sic*]

Hallazgo 12 - Funciones conflictivas realizadas por la Bibliotecaria de Sistemas de Información y por una programadora de la Oficina de Informática, y falta de un puesto de Administrador de Red

a. En el examen realizado el 5 y 11 de mayo de 2009, determinamos que algunas funciones asignadas a empleados de la Oficina de Informática resultaban conflictivas al ser realizadas por un mismo empleado, según se indica:

1) La Bibliotecaria de Sistemas de Información, como parte de las funciones de su puesto, estaba a cargo de registrar, suministrar, recibir y custodiar los archivos de programas; administrar las librerías en producción; mantener el control de cintas y discos magnéticos; y producir los respaldos diarios y semanales del *mainframe*. Además de estas funciones, la Bibliotecaria realizaba las funciones relacionadas con la administración de la seguridad lógica, tales como: crear, modificar y eliminar las cuentas de acceso y los privilegios asignados a los usuarios en el *mainframe*. Las funciones de administración de seguridad lógica son incompatibles con las de Bibliotecaria de Sistemas de Información. Esto, porque al realizar funciones de administración de seguridad lógica, la Bibliotecaria podría otorgarse accesos y privilegios de ver, escribir y borrar información en el sistema, que no estuviesen autorizados.

2) Una Programadora de Sistemas de Información III de la Oficina de Informática, como parte de las funciones de su puesto, estaba a cargo de realizar los cambios en la programación del Sistema de Participantes y del Sistema Administrativo. Además de estas funciones, realizaba las de Administradora de Seguridad, lo que le permitía, entre otras cosas, otorgar el acceso físico a los empleados de la Oficina de Informática. También realizaba las funciones de la Bibliotecaria de Sistemas de Información cuando esta se encontraba de vacaciones o estaba ausente, entre las que se encontraban el otorgar acceso a usuarios al *mainframe* y a la administración de las librerías en producción. Las funciones de Administradora de Seguridad y de Bibliotecaria de Sistemas de Información son incompatibles con las de Programadora de Sistemas. Esto, porque al realizar funciones de Administradora de Seguridad y de Bibliotecaria de

Sistemas de Información, la Programadora podría otorgarse accesos lógicos y privilegios dentro de las librerías de producción, y realizar cambios que no estén autorizados.

Una situación similar se comentó en el *Informe de Auditoría CPED-97-9*.

b. Al 29 de abril de 2009, la ADT tenía instalado 14 servidores mediante los cuales se conectaban 174 computadoras que proveían a los usuarios acceso a Internet y al correo electrónico, entre otros servicios. Además, mediante uno de estos servidores se le proveía la conexión con el *mainframe* a 11 de las oficinas locales de la ADT para ingresar al Sistema de Participantes la información de los integrantes de los programas de adiestramiento y empleo. Durante el 2008, la ADT emitió cheques por $11,207,771 a 11,788 participantes de estos programas.

A la fecha de nuestro examen, la ADT no contaba con un puesto de Administrador de Red. Las funciones correspondientes a este puesto las ejercía, desde principio del 1998, una Programadora de Sistemas de Información III.

En la Sección 6.2 de la *Ley 184-2004, Ley para la Administración de los Recursos Humanos en el Servicio Público del Estado Libre Asociado de Puerto Rico*, según enmendada, se establece que como instrumento eficaz para la consecución de los programas de Gobierno, cada Autoridad Nominadora será responsable de establecer y mantener una estructura racional de funciones que tenga la mayor uniformidad posible y que sirva de base para las acciones de personal. Para lograr este propósito, las agencias podrán utilizar el método de análisis de trabajo y evaluación de puesto más adecuado para sus funciones operacionales y realidad organizacional.

En la Sección IV de la *Política General* se establece que la Autoridad Nominadora designará a las personas autorizadas a adquirir, instalar, modificar, sustituir o utilizar los servicios y los recursos disponibles en las agencias; y así constará en la *Descripción de Puesto (DTRH-16)* de cada funcionario o empleado. Cada una de las unidades de trabajo

debe distribuir las tareas de acuerdo con las funciones que realiza cada sección. Antes de autorizar el uso de un acceso de información, el Supervisor del usuario debe asegurarse de que no existe apariencia de conflicto de intereses de los usuarios.

En la *Política Núm. TIG-011* de la *Carta Circular Núm. 77-05* se establece que las agencias deben adquirir e implementar una infraestructura de red segura basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución eficiente de servicios. Esta *Política* se implementa, en parte, mediante la creación de un puesto de Administrador de Red a cargo, entre otras funciones, de supervisar la instalación y la administración de las operaciones, y el mantenimiento de la red; analizar, evaluar y establecer los niveles de seguridad y los requisitos de los archivos; y supervisar la instalación y la configuración de los componentes de la red.

Las normas generalmente aceptadas en el campo de la tecnología de información sugieren que para fortalecer los controles establecidos sobre la información de la entidad es necesario que se segreguen las tareas relacionadas con las operaciones de la Oficina de Informática de manera que no recaiga en la misma persona el control de una o varias transacciones. El objetivo primordial de dichos controles es disminuir la probabilidad de que se cometan errores o irregularidades y que estos no se detecten a tiempo para fijar responsabilidades.

Las situaciones comentadas pueden propiciar que se incurran en errores o en irregularidades, sin que se puedan fijar responsabilidades y tomar las medidas correctivas necesarias con prontitud, con los consiguientes efectos adversos para la entidad.

La situación comentada en el **apartado a.** se atribuye, en parte, a que el Subadministrador de la ADT no había considerado el conflicto en las funciones que realizaban la Bibliotecaria de Sistemas de Información y la Programadora de Sistemas de Información III.

La situación comentada en el **apartado b.** se debía, en parte, a que, a pesar de las gestiones realizadas por el Subadministrador, el Administrador no había requerido que se efectuaran las gestiones necesarias para crear el puesto de Administrador de Red.

Hallazgo 13 - Falta de procedimientos para el traslado y la separación del personal con acceso a los sistemas de información de la ADT

a. Al 26 de mayo de 2009, la ADT no había establecido procedimientos escritos para el manejo del traslado y la separación del personal que tiene acceso a los sistemas de información. Estos procedimientos deben considerar, entre otras cosas, los procesos a realizarse para la entrevista final, la devolución de la propiedad y de las tarjeta de identificación, la notificación al personal que trabaja con la seguridad de los servidores y el *mainframe*, con el fin de que se efectúe el cambio correspondiente o la revocación inmediata de las cuentas de acceso, y la identificación del período durante el cual los acuerdos de no divulgación son efectivos.

   En la *Política Núm. TIG-003* de la *Carta Circular Núm. 77-05* se establece, entre otras cosas, que cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de manera que estas circunstancias no afecten la seguridad de la información ni de los sistemas. Para esto, deberán establecerse procedimientos que incluyan una comunicación efectiva entre el área de Recursos Humanos, el área en que trabaja el empleado y el área de Sistemas de Información.

   La situación comentada propicia que no existan mecanismos de control para evitar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta. Esto puede propiciar la comisión de irregularidades sin que puedan ser detectadas a tiempo para fijar responsabilidades.

   La situación comentada se debía a que el Administrador no le había requerido a la Directora de Recursos Humanos que desarrollara y remitiera, para su consideración y aprobación, las normas y los procedimientos escritos necesarios para el traslado y la separación del personal que tiene acceso a los sistemas de información de la ADT.

Hallazgo 14 - Falta de adiestramientos periódicos al personal de la Oficina de Informática sobre sus funciones y la seguridad de los sistemas, y a los funcionarios y empleados sobre el uso y el control de los equipos y sistemas computadorizados

a. Al 5 de mayo de 2009, la Técnica de Red de Computadora, el Operador de Equipo de Procesar Información III y la Bibliotecaria de Sistemas de Información de la ADT, no habían recibido adiestramientos sobre los temas relacionados con sus funciones, tales como:

- análisis de problemas
- novedades, actualizaciones o mejoras en los sistemas
- fundamentos de seguridad para los sistemas de información
- nuevas amenazas y posibles soluciones
- plan de contingencias y plan de seguridad
- seguridad de los sistemas operativos
- configuración de computadoras.

b. La ADT no ofrecía adiestramientos sobre el uso y el control de los equipos y los sistemas de información. Esto, para orientar a los funcionarios y a los empleados en cuanto a la seguridad de acceso lógico y físico, el manejo y el control de las contraseñas, y las normas de uso de los equipos y de los sistemas computadorizados, entre otros.

En la Sección 6.5 de la *Ley 184-2004* se establece, entre otras cosas, como concepto básico en administración, que para que una agencia cumpla a cabalidad su misión debe desarrollar al máximo sus recursos humanos y proveer los instrumentos administrativos para su mejor utilización. Además, se indica que cada agencia mantendrá un historial por cada empleado de los adiestramientos recibidos, de modo que puedan utilizarse para tomar decisiones relativas a ascensos, traslados, asignaciones de trabajo, evaluaciones y otras acciones de personal compatibles con el principio de mérito.

En la Sección IV de la *Política General* se establece que será política pública del Departamento y de sus componentes mantener al día un programa de concientización, educación y orientación sobre seguridad de información. El período durante el cual se ofrecerán conferencias a los usuarios será establecido por el Director de la Oficina en coordinación con la División de Adiestramiento. Estas conferencias deben ofrecerse a todo nuevo empleado dentro de un lapso no mayor de 30 días desde su comienzo en el trabajo, y a todos los usuarios en todos los niveles por lo menos anualmente, o según las necesidades de la agencia.

La situación comentada en el **apartado a.** podría reducir la efectividad de los sistemas computadorizados y exponer los datos y el personal a riesgos innecesarios que afecten la continuidad de las operaciones de la ADT.

Las situación comentada en el **apartado b.** puede propiciar que no se utilicen al máximo los equipos y los programas computadorizados, se pierda información almacenada en las computadoras, se utilicen equipos y programas computadorizados sin la debida autorización, y se instalen programas que no estén debidamente autorizados por la ADT. Además, que se propaguen virus a los equipos computadorizados.

Las situaciones comentadas se atribuyen a que el Subadministrador no cumplió con su deber de informar a la Oficina de Recursos Humanos sobre las necesidades de adiestramientos para la Técnica de Red de Computadora, el Operador de Equipo de Procesar Información III y la Bibliotecaria de Sistemas de Información, a los fines de mantenerse al día en los conocimientos relacionados con sus funciones y en el manejo de la seguridad de los sistemas a su cargo. Además, no había identificado las necesidades de adiestramiento de los usuarios sobre el uso de los sistemas computadorizados a los fines de planificar y coordinar adiestramientos y orientaciones sobre la seguridad de la información para los empleados de la ADT.

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

> Nunca ha habido un presupuesto para adiestramiento y la Oficina de Gerencia y Presupuesto (OGP) tampoco asignó para este año. [*sic*]

ANEJO

DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

ADMINISTRACIÓN DEL DERECHO AL TRABAJO

OFICINA DE INFORMÁTICA

FUNCIONARIOS PRINCIPALES DEL NIVEL EJECUTIVO QUE ACTUARON DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Miguel A. Romero Lugo	Secretario del Trabajo y Recursos Humanos y Administrador[19]	13 abr. 09	15 sep. 09
Sr. Ángel A. Santiago Torres	Subadministrador[20]	13 abr. 09	15 sep. 09
Vacante	Director de Informática	13 abr. 09	15 sep. 09
Sra. Práxedes Navedo Rosado	Directora de Recursos Humanos	13 abr. 09	15 sep. 09
Sr. David Morales De Jesús	Auditor Principal	13 abr. 09	15 sep. 09

[19] Véase la nota al calce 1.

[20] Véase la nota al calce 6.