INFORME DE AUDITORÍA TI-12-03

29 de septiembre de 2011

Departamento del Trabajo y Recursos Humanos

Administración para el Adiestramiento de Futuros Empresarios y Trabajadores

Oficina de Sistemas de Información

(Unidad 5235 - Auditoría 13243)

Período auditado: 8 de diciembre de 2008 al 27 de mayo de 2009

CONTENIDO

Página

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

29 de septiembre de 2011

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información (OSI) de la Administración para el Adiestramiento de Futuros Empresarios y Trabajadores (AAFET), adscrita al Departamento del Trabajo y Recursos Humanos (Departamento), 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 *Ley Núm. 1 del 23 de julio de 1985*, según enmendada, creó el Cuerpo de Voluntarios al Servicio de Puerto Rico (Cuerpo de Voluntarios). Además, creó un programa de oportunidades de estudio, adaptación, adiestramiento, trabajo y desarrollo personal a jóvenes entre las edades de 16 a 28 años que, debido a la falta de recursos de naturaleza económica o familiar, presentan una pobre adaptación al sistema escolar y a la vida comunitaria en general. El *Plan de Reorganización Núm. 2* del 4 de mayo de 1994, según enmendado, adscribe el Cuerpo de Voluntarios al Departamento como un componente operacional.

Mediante la *Ley Núm. 224 del 6 de agosto de 1999* se creó la AAFET en sustitución del Cuerpo de Voluntarios. La AAFET, como sucesora del Cuerpo de Voluntarios, está adscrita al Departamento como un componente operacional.

La misión de la AAFET es fomentar el desarrollo humano, la capacitación técnico-vocacional, y la creación de microempresas y empleos a jóvenes, entre las edades de 14 a 29 años, que estén fuera del sistema de educación formal y de trabajadores desplazados que se puedan integrar a la fuerza laboral. Para cumplir con su misión, la AAFET brinda sus servicios mediante los siguientes programas:

- Adiestramientos en Operación y Administración de Negocios - Está constituido por el Subprograma de Autoempresas y la Propuesta de Desarrollo Empresarial de la *Workforce Investment Act of 1998, Ley de Inversión para el Desarrollo de la Fuerza Trabajadora* (Ley *WIA*). El Subprograma de Autoempresas desarrolla varias actividades encaminadas a viabilizar su meta de contribuir a reducir el desempleo de los jóvenes entre las edades de 18 a 29 años. Además, adiestra a jóvenes que interesen adquirir las destrezas para iniciar un proyecto empresarial en producción o servicios. Por su parte, a través del Subprograma de Autoempresas y de la Propuesta de Desarrollo Empresarial de la Ley *WIA*, se atiende en forma directa y a corto plazo el problema del desempleo en el País; se fomenta el desarrollo de nuevos empresarios; y se adiestra intensivamente al participante en lo relacionado con la administración de negocios, el énfasis en las áreas de venta, el mercadeo, la gerencia y la contabilidad. Una vez finalizado el adiestramiento, el participante completa un plan de negocio, el cual elabora de forma concurrente con el curso para establecer su propia microempresa. Además, el Programa le brinda apoyo y sirve de enlace para el financiamiento que necesita, y le ofrece asesoramiento técnico empresarial una vez establecido el negocio. Los servicios se prestan a través de las regiones de la AAFET: Noreste-San Juan, Central-Ponce y Oeste-Mayagüez.

- Educación Tecnológica Vocacional a Jóvenes - Está orientado en el desarrollo de competencias vocacionales, técnicas, sociales y de desarrollo humano que capaciten al participante para obtener o retener un empleo y que faciliten su inserción en la sociedad como un ciudadano productivo. El aspecto vocacional es completado por experiencias de acción comunal y de desarrollo humano en un enfoque de formación integral. Además, ofrece servicios de tutorías para dirigir a los participantes hacia el

mejoramiento de su escolaridad o lograr la equivalencia del diploma de Escuela Superior. Los servicios se ofrecen en 14 institutos vocacionales localizados en: Aguadilla, Aibonito, Barceloneta, Camuy, Coamo, Dorado, Guánica, Juana Díaz, Las Piedras, Mayagüez, Naranjito, San Germán, San Juan y Yabucoa.

- Servicios Integrados a Comunidades - Este atrae e incentiva a los jóvenes de los residenciales públicos y de las comunidades especiales para que ingresen a los programas de adiestramiento y empleo de la AAFET. Esto es posible a través de las diversas alianzas estratégicas con sectores públicos y privados que convierten a la agencia en un ente facilitador de servicios, con especial énfasis en la población desaventajada. Además, fomenta el desarrollo del autoempleo y de la autogestión en las comunidades identificadas como de mayor necesidad.

La Dirección y Administración General de la AAFET tiene a su cargo la planificación y la coordinación de las operaciones de los programas para que se cumplan las metas trazadas por la Agencia, en relación con la erradicación del desempleo entre la juventud y los trabajadores desplazados. Las funciones administrativas y ejecutivas de la AAFET las realiza un Administrador[1] nombrado por el Gobernador por un término de cuatro años, con la recomendación del Secretario del Trabajo y Recursos Humanos, y el consejo y consentimiento del Senado de Puerto Rico.

La AAFET se compone de las siguientes oficinas: Oficina del Administrador, de Adquisiciones y Subastas, de Asesoramiento Legal, de Auditoría Interna e Inspectoría, de Desarrollo Económico, de Planificación y Registraduría, de Prensa y Comunicaciones, de Recursos Humanos, de Seguridad y Salud, y de Sistemas de Información. Además, cuenta con dos negociados: de Finanzas y de Servicios Generales, y un Área de Tecnológica Vocacional.

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

---

[1] En el Artículo 6 de la *Ley Núm. 224* se establece, entre otras, que el Administrador responderá directamente al Secretario del Trabajo y Recursos Humanos y estará sujeto a la política pública establecida, y a las directrices y normas que promulgue el Secretario.

La OSI cuenta con los siguientes puestos: 1 Director de Sistemas, 1 Analista de Sistema Electrónicos, 1 Programador de Sistemas Electrónicos, 1 Oficinista II, 4 operadores de equipo de procesar datos, 1 Funcionario Ejecutivo V, 1 Secretaria V, 1 Supervisor y 1 Funcionario Ejecutivo I. Al 27 de mayo de 2009, estaban vacantes los puestos de Secretaria V, Supervisor y Funcionario Ejecutivo I.

Los gastos operacionales de la OSI eran sufragados del presupuesto operacional de la AAFET que para el año fiscal 2008-09 ascendió a $13,779,000.

La AAFET cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.aafet.gobierno.pr. Esta página provee información acerca de la entidad y de los servicios que presta.

RESPONSABILIDAD DE LA GERENCIA

La gerencia de todo organismo gubernamental debe considerar los siguientes *Diez Principios para Lograr una Administración Pública de Excelencia*. 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 8 de diciembre de 2008 al 27 de mayo 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 procedimientos de control interno y de otros procesos
- confirmaciones de información pertinente.

OPINIÓN

Las pruebas efectuadas demostraron que las operaciones de la OSI en lo que concierne a los controles internos relacionados con la administración del programa de seguridad, la evaluación de la continuidad de servicio, y la participación de la Oficina de Auditoría Interna en la evaluación de los controles y las operaciones de los sistemas de información de la AAFET, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 5**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

INFORME DE AUDITORÍA ANTERIOR

Situaciones similares a las comentadas en los **hallazgos 2-a.2) y 4), y 5** de este *Informe* fueron objeto de recomendaciones en el *Informe de Auditoría CPED-95-6* del 30 de junio de 1995. Estas no fueron atendidas.

El no atender, sin justa causa, las recomendaciones de los informes de auditoría de esta Oficina puede constituir una violación al Artículo 3.2(b) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, según enmendada. A estos efectos, el 30 de enero de 1987, el Director Ejecutivo de la Oficina de Ética Gubernamental de Puerto Rico emitió la *Carta Circular Núm. 86-4*, mediante la cual exhortó a los alcaldes y a los funcionarios de la Rama Ejecutiva del Gobierno a cumplir con las mismas.

RECOMENDACIONES

AL SECRETARIO DEL TRABAJO Y RECURSOS HUMANOS

1. Se asegure de que la Administradora de la AAFET cumpla con las **recomendaciones de la 4 a la 9** de este *Informe*. **[Hallazgos del 1 al 5]**

2. Evalúe y apruebe los procedimientos necesarios para corregir las deficiencias comentadas en los **hallazgos 2-a.3) y 4), y 4-b.**

3. Efectúe las gestiones necesarias para que en la *Política sobre la Administración y Seguridad de Información Computadorizada, Internet y Mensajería Electrónica*, aprobada el 4 de marzo de 2008 por el Secretario del Trabajo y Recursos Humanos, se incluyan disposiciones para la protección de la información sensitiva y de las licencias de los programas durante los procesos para decomisar o transferir los equipos. **[Hallazgo 4-a.3)]**

A LA ADMINISTRADORA DE LA ADMINISTRACIÓN PARA EL ADIESTRAMIENTO DE FUTUROS EMPRESARIOS Y TRABAJADORES

4. Asegurarse de que se realice y se documente el análisis de riesgos 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 sugiere en las mejores prácticas en el campo de la tecnología. El informe, producto de este análisis de riesgos, debe ser remitido para la aprobación del Secretario del Trabajo y Recursos Humanos. Una vez aprobado, ver que se revise anualmente para asegurarse de que se mantiene actualizado. **[Hallazgo 1]**

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

   a. Revise el *Manual de Seguridad y Plan de Contingencias* para que se incluya la información comentada en el **Hallazgo 2-a.3)**. Una vez revisado, tomar las medidas necesarias para que se remita para la aprobación del Secretario del Trabajo y Recursos Humanos, y vea que se mantenga actualizado y que se divulgue a los funcionarios y a los empleados concernientes. **[Hallazgo 2-a.1) y 2)]**

   b. Mantenga una copia de los respaldos de la información de los sistemas computadorizados en un lugar seguro fuera de los predios de la AAFET. **[Hallazgo 3]**

6. Asegurarse de que se prepare un *Plan de Continuidad de Negocios* que cumpla con lo requerido en la *Política Núm. TIG-003*, y vea que se remita para la aprobación del Secretario del Trabajo y Recursos Humanos. Una vez este sea aprobado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se asegure 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 2-a.4)]**

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

   a. Mantenga un programa de capacitación para orientar a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la agencia y dar a conocer las reglamentaciones y las políticas relacionadas con la seguridad de la información. **[Hallazgo 4-a.1)]**

   b. Requiera acuerdos de confidencialidad a los empleados de la AAFET que trabajan con información confidencial. **[Hallazgo 4-a.2)]**

8. Remitir el *Procedimiento de Respaldo* para la aprobación del Secretario del Trabajo y Recursos Humanos. Una vez aprobado, 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-b.]**

9. Establezca un programa de adiestramiento continuo para capacitar a los auditores internos de la AAFET en las técnicas de auditoría de los sistemas de información computadorizados. Una vez adiestrados, se asegure de que la Directora de Auditoría Interna incluya en su plan de auditoría exámenes periódicos sobre los controles y las operaciones de los sistemas de información computadorizados de la AAFET. **[Hallazgo 5]**

CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos del 1 al 5**, incluidos en la parte de este *Informe* titulada **RELACION DETALLADA DE HALLAZGOS**, se informaron a la Dra. Iris N. López Sánchez, Administradora, en carta de nuestros auditores del 27 de mayo de 2009.

El borrador de los **hallazgos** de este *Informe* se remitió al Hon. Miguel A. Romero Lugo, Secretario del Trabajo y Recursos Humanos y a la Administradora de la AAFET, para comentarios, en cartas del 7 de octubre de 2010. Con el mismo propósito, remitimos el borrador

de los **hallazgos** de este *Informe* al Sr. Román M. Velasco González, ex-Secretario del Trabajo y Recursos Humanos, y al Sr. Eduardo J. Vergara Agostini, ex-Administrador de la AAFET, en cartas de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por la AAFET.

COMENTARIOS DE LA GERENCIA

El 3 de julio de 2009, la Administradora remitió sus comentarios sobre los **hallazgos** incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador de *Informe*.

En carta del 27 de octubre de 2010 el Secretario del Trabajo y Recursos Humanos indicó que se suscribía a la contestación y a los comentarios provistos por la Administradora de la AAFET relacionados con los hallazgos de este *Informe*. La Administradora de la AAFET remitió sus comentarios al borrador de los **hallazgos** de este *Informe* en carta del 19 de octubre de 2010. Además, el ex-Administrador remitió sus comentarios al borrador de los **hallazgos del 1 al 4** de este *Informe* en carta del 3 de noviembre de 2010. Los comentarios de dichos funcionarios fueron considerados en la redacción final de este Informe; y se incluyen en la segunda parte de este *Informe*, titulada **RELACIÓN DETALLADA DE HALLAZGOS**, bajo la sección de HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN PARA EL ADIESTRAMIENTO DE FUTUROS EMPRESARIOS Y TRABAJADORES, ADSCRITA AL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS.

El ex-Secretario del Trabajo y Recursos Humanos no contestó el borrador de los hallazgos de este *Informe* que le fuera remitido para comentarios en nuestra carta del 7 de octubre de 2010, y en carta de seguimiento del 26 de octubre de 2010.

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yermin 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 y los exfuncionarios de la unidad auditada efectuaron comentarios sobre el borrador de los hallazgos del informe, que les envía nuestra Oficina. Dichos comentarios se consideran al revisar el borrador del informe; y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN LA OFICINA DE SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN PARA EL ADIESTRAMIENTO DE FUTUROS EMPRESARIOS Y TRABAJADORES, 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 SISTEMAS DE INFORMACIÓN DE LA ADMINISTRACIÓN PARA EL ADIESTRAMIENTO DE FUTUROS EMPRESARIOS Y TRABAJADORES, ADSCRITA AL DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

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

Hallazgo 1 - Falta de un Informe de Avalúo de Riesgos de los sistemas de información computadorizados

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 proteger dichos recursos de manera que no se afecten adversamente las operaciones. 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 de gobierno.
- Proveer un balance económico entre el impacto de las amenazas y el costo de las medidas de seguridad a implantarse.

Al 8 de diciembre de 2008, en la AAFET no se había realizado un avalúo de riesgos de los sistemas de información.

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 realizar un análisis de riesgos que incluya:

- Un inventario de activos de sistemas de información que incluya 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 impide a la AAFET evaluar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y pérdida de información. Además, impide 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 AAFET en caso de que surja alguna eventualidad.

La situación comentada se atribuye a que los funcionarios que actuaron como Secretario del Trabajo y Recursos Humanos durante el período auditado no habían promulgado una directriz para que los administradores de la AAFET prepararan y remitieran para aprobación un avalúo de riesgos de los sistemas de información, según lo establecido en la *Carta Circular Núm. 77-05*.

En la carta de la Administradora de la AAFET, esta nos indicó, entre otras cosas, lo siguiente:

> Posterior a la Auditoría, la Agencia corrigió y actualizó en dos ocasiones el Plan para la Continuidad del Negocio y Preparación para Desastres el cual incluye una sección del análisis de riesgo y un inventario de todos los activos de Sistemas de Información de la Agencia. [*sic*]

En la carta del ex-Administrador de la AAFET, este nos indicó, entre otras cosas, lo siguiente:

> Conscientes de la importancia de los sistemas de información computadorizados, para el año 2003, en la Oficina de Sistemas de Información de la AAFET, se preparó un documento titulado Manual de Seguridad y Plan de Contingencia en el cual se incluyeron las diferentes potenciales amenazas como fuego, terremoto, inundación, robo y sabotaje para identificar los posibles daños, los métodos preventivos y posibles medidas que podrían implantarse de ocurrir alguna de las situaciones identificadas. [*sic*]

Hallazgo 2 - Deficiencias relacionadas con el Plan de Seguridad y el Plan de Continuidad de Negocios de la AAFET

a. El 8 de diciembre de 2008, el Oficial de Seguridad de la AAFET nos entregó el *Manual de Seguridad y Plan de Contingencias* como el *Plan de Seguridad* y el *Plan de Continuidad de Negocios* de la AAFET. El examen del *Manual* reveló las siguientes deficiencias:

1) No estaba aprobado por el Secretario del Trabajo y Recursos Humanos.

2) No había sido revisado desde el 22 de abril de 2003.

3) Carecía de la siguiente información, que debe ser parte esencial de un plan de seguridad:

- La documentación de la validación de las normas de seguridad[2]

[2] La validación de las normas de seguridad se efectúa mediante la prueba de los controles para eliminar o mitigar las amenazas y las 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 evidencia de un análisis de riesgos actualizado, que sea la base 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 y los usuarios, y que permita mantener los conocimientos actualizados

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

- La documentación de la interconexión de los sistemas.

4) Carecía de la siguiente información, que debe ser parte esencial de un plan de continuidad de negocios:

- Un inventario actualizado de los equipos, los sistemas operativos, las aplicaciones y los archivos críticos de la AAFET. El *Plan de Contingencias* incluido en el *Manual* hacía referencia a sistemas operativos que no eran utilizados por la AAFET.

- Una lista de amenazas basada en el avalúo de riesgos con sus correspondientes procedimientos para prevenir los daños y restaurar las operaciones.

- Una lista actualizada de los empleados de la OSI con sus roles y nivel de autoridad para ejecutar los procedimientos asignados. El *Plan* incluía a un empleado que renunció el 21 de marzo de 2008 como el encargado de los respaldos de información de la AAFET.

- Una lista actualizada de los proveedores de servicio principales. El *Plan* hacía referencia a consultores que no mantenían contratos con la AAFET.

- Un itinerario de restauración que incluya el orden de las aplicaciones a restaurar, y los procedimientos para restaurar los respaldos.

- Copias de los acuerdos establecidos con centros alternos de procesamiento y de respaldos de datos.

- El detalle de la configuración de los sistemas utilizados en la OSI.

- Las políticas y los procedimientos aprobados para el registro de los problemas de los equipos.

- Información sobre los resultados de las pruebas y las revisiones efectuadas al *Plan* y los adiestramientos ofrecidos al personal responsable de la continuidad de las operaciones.

Una situación similar se comentó en el *Informe de Auditoría CPED-95-6*.

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 entidad gubernamental para que estén al tanto de los controles de seguridad y de los beneficios correspondientes.

- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones, y de que se le transmitan 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 le apliquen.

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

Las situaciones comentadas se atribuyen a que los administradores de la AAFET no se habían asegurado de que los directores de la OSI revisaran el *Manual* para que incluyeran lo que se indica en este **Hallazgo** y lo remitieran para su revisión. Además, los funcionarios que actuaron como Secretario del Trabajo y Recursos Humanos durante el período auditado no le habían requerido a los administradores de la AAFET que prepararan un *Plan de Seguridad* y un *Plan de Continuidad de Negocios*, que incluya un *Plan para la Recuperación de Desastres* y un *Plan para la Continuidad de las Operaciones* y que los mismos se remitieran para su revisión y aprobación.

En la carta de la Administradora de la AAFET, esta nos indicó, entre otras cosas, lo siguiente:

> Posterior a la auditoría la Agencia corrigió y actualizó el Plan para la Continuidad del Negocio y Preparación para Desastres, el cual incluye los aspectos relacionados a la seguridad de los sistemas, así como los procesos a seguir luego de situaciones de emergencias a fin de continuar las operaciones de la Agencia. El nuevo plan responde a las necesidades de la agencia y corrige las deficiencias encontradas en el plan original. [*sic*] **[Apartado a.1), 2) y 4)]**

En la carta del ex-Administrador de la AAFET, este nos indicó, entre otras cosas, lo siguiente:

> Conscientes de la importancia de los sistemas de información computadorizados, al comienzo de mi gestión como Administrador de la AAFET, se preparó el Manual de Seguridad y Plan de Contingencia en el cual se identificaban las potenciales amenazas, los posibles daños, las medidas de seguridad y los pasos para continuar las operaciones. Además, como parte del Grupo Operacional del Plan Operacional de Emergencias,

> esta unidad tenía y realizaba la responsabilidad de proteger los sistemas computadorizados y minimizar los riesgos de daños de forma tal, que se pudiera dar continuidad a los servicios. [*sic*] **[Apartado del a.1) al 4)]**

Hallazgo 3 - Falta de almacenamiento de los respaldos de la información de los sistemas computadorizados de la AAFET en un lugar seguro fuera de los predios de esta

a. Al 30 de enero de 2009, no se mantenían copias de los respaldos realizados a la información de los sistemas computadorizados de la AAFET en un lugar seguro fuera de los predios de esta. Los respaldos se almacenaban en la OSI, por lo que estaban expuestos a las mismas posibles amenazas de desastres que la información almacenada en los servidores.

   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 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 se requiere mantener copias de los respaldos almacenadas en un lugar seguro fuera del edificio donde están instalados los servidores y que sea una localidad que ofrezca las condiciones ambientales y de seguridad necesarias.

   La situación comentada podría ocasionar la pérdida permanente de información importante, sin la posibilidad de poder recuperarla, lo que afectaría adversamente las operaciones de la AAFET.

   La situación comentada se debía a que el Director de la OSI no había efectuado las gestiones para mantener copias de los respaldos en un lugar seguro fuera de los predios de la AAFET.

   En la carta de la Administradora de la AAFET, esta nos indicó, entre otras cosas, lo siguiente:

> En la revisión del Plan para la Continuidad del Negocio y Preparación para Desastres, se incluyó la sección 17 que detalla el proceso para cumplir con

> la exigencia de disponer de alternativas fuera de la agencia para almacenar los respaldos y para garantizar la continuidad de las operaciones en caso de emergencias. El Proyecto se puso en marcha en diciembre de 2009. [*sic*]

En la carta del ex-Administrador de la AAFET, este nos indicó, entre otras cosas, lo siguiente:

> La Oficina de Sistemas de Información de la AAFET, realizaba resguardos de la información mantenida en los servidores y se almacenaba en el armario contra fuegos. Como parte de los esfuerzos para minimizar riesgos, el 18 de junio de 2007, mediante comunicación al […], Secretario del Departamento del Trabajo y Recursos Humanos, se le solicitó autorización para utilizar un espacio en la bóveda del Centro de Cómputos del Departamento, para almacenar las unidades magnéticas de resguardo. Estas gestiones se realizaban en el mencionado Departamento, por la falta de presupuesto para contratar un espacio en un lugar privado. [*sic*]

Hallazgo 4 - Deficiencias en la implantación y en el contenido de la Política sobre la Administración y Seguridad de Información Computadorizada, Internet y Mensajería Electrónica, y en el Procedimiento de Respaldos no aprobado

a. Al 8 de diciembre de 2008, los aspectos relacionados con los sistemas de información de la AAFET se regían mediante la *Política sobre la Administración y Seguridad*. El examen sobre la implantación y el contenido de esta *Política* reveló las siguientes deficiencias:

   1) La AAFET no mantenía un programa de capacitación para orientar a los usuarios sobre la importancia de salvaguardar y utilizar correctamente la información de la agencia y dar a conocer la reglamentación y la política pública relacionadas con la seguridad de la misma.

   2) La AAFET no había establecido acuerdos de confidencialidad con sus empleados antes de exponerlos a información confidencial.

   3) La *Política sobre la Administración y Seguridad* no incluía disposiciones en cuanto a la disposición de la información sensitiva y de los programas antes de transferir o dar de baja los equipos computadorizados y los medios de almacenamiento de información.

b. Al 8 de diciembre de 2008, el Administrador no había remitido el *Procedimiento de Respaldo* utilizado por la OSI para la aprobación del Secretario del Trabajo y Recursos Humanos. Además, en este *Procedimiento* se hacía referencia, entre otras cosas, a un acuerdo que la AAFET había establecido con el Departamento para utilizar su bóveda para guardar copias de los respaldos. Sin embargo, el examen del almacenamiento de los respaldos reveló que los mismos se mantenían en la OSI de la AAFET. **[Véase el Hallazgo 3]**

En el Artículo 4 (8) del *Plan de Reorganización Núm. 2* se dispone que los directores de los componentes del Departamento deberán preparar y remitir para la aprobación del Secretario del Trabajo y Recursos Humanos los reglamentos necesarios, incluidas las enmiendas o las derogaciones de los mismos.

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 crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

Como norma de sana administración, se deben establecer por escrito normas, procedimientos y políticas de control interno eficaces que reglamenten las operaciones computadorizadas, que estén aprobados por la alta gerencia y que sean uniformes. Mediante los mismos, se logra definir los niveles de control que deben existir en las distintas áreas. Además, contribuyen a mantener la continuidad de las operaciones en casos de renuncias o ausencias del personal de mayor experiencia y facilita la labor de adiestramiento.

En la *Política sobre Administración y Seguridad* se establece, entre otras cosas, que el Departamento y sus componentes operacionales mantendrán al día un programa de concienciación, educación y orientación sobre la seguridad de información. También se establece que la información contenida en los sistemas de archivo electrónicos del Departamento y sus componentes operacionales, será utilizada con el único propósito de

realizar las operaciones propias del servicio público y de las agencias. Por esto, ningún usuario podrá divulgar información, sin importar el medio en que se encuentre, sin autorización previa. En consonancia con dicha política pública se deben establecer acuerdos de confidencialidad escritos con los usuarios en los cuales se establezcan claramente las responsabilidades y las restricciones sobre el uso y la divulgación de la información mantenida en los sistemas de información de la AAFET.

Las situaciones comentadas podrían ocasionar, entre otras cosas, que la AAFET:

- No cuente con personal capacitado para efectuar las labores asignadas y que los empleados utilicen su propio criterio para realizar sus trabajos, lo que podría llevar a la comisión de errores, faltas e irregularidades. **[Apartados a.1) y b.]**

- Carezca de medidas de control necesarias para proteger la confidencialidad y la divulgación de su información, lo que podría ocasionar que personas no autorizadas utilicen esta información para propósitos ajenos a la gestión pública. **[Apartado a.2) y 3)]**

- No invierta eficientemente sus recursos para establecer medidas de control y prioridades de procesamiento en las instalaciones, los equipos y los sistemas relacionados con las operaciones críticas de la AAFET. **[Apartado a.3)]** Esto, a su vez, podría afectar la continuidad de dichas operaciones.

Las situaciones comentadas en el **apartado a.1) y 2)** se debían a que los administradores que actuaron durante el período auditado no se habían asegurado de requerir a la Directora de Recursos Humanos en funciones que estableciera un programa de capacitación sobre lo establecido en la *Política*, y requiriera a los empleados la firma de acuerdos de confidencialidad. Además, los administradores no habían efectuado las gestiones necesarias para que el Secretario del Trabajo y Recursos Humanos evaluara y aprobara el *Procedimiento de Respaldo.* **[Apartado b.]**

La situación comentada en el **apartado a.3)** se debía a que el Secretario del Trabajo y Recursos Humanos no se había asegurado de que se incluyera en la *Política*, las disposiciones para la protección de la información sensitiva y de las licencias de los programas durante los procesos para decomisar o transferir los equipos.

En la carta de la Administradora de la AAFET, esta nos indicó, entre otras cosas, lo siguiente:

> El Comité de Reglamentación está en el proceso de actualizar las normas y medidas disciplinarias de la Agencia para entre otras cosas, incluir normas sobre el acuerdo de confidencialidad en el uso de los sistemas de información. **[Apartado a.2)]**
>
> Por otro lado se ha propuesto la inclusión de normas para la disposición de información sensitiva en las Políticas sobre la Administración y Seguridad de Información Computadorizada, Internet y Mensajería Electrónica. Al momento el Departamento se encuentra en el proceso de enmendar las mismas. [*sic*] **[Apartado a.3)]**

En la carta del ex-Administrador de la AAFET, este nos indicó, entre otras cosas, lo siguiente:

> […] durante mi incumbencia en la AAFET y como norma de sana administración se desarrollaron políticas y controles de seguridad sobre los sistemas computadorizados. Estas fueron divulgadas a todos los usuarios de la red mediante varias comunicaciones en las cuales se orientaba sobre la seguridad en el uso de la contraseña, confidencialidad en los sistemas, información computadorizada, internet y mensajería electrónica. Además, se requería la aceptación de estas políticas por parte del usuario al iniciar sus labores en el sistema. [*sic*] **[Apartado a.]**

Hallazgo 5 - Falta de participación de la Oficina de Auditoría Interna e Inspectoría en la evaluación de la seguridad, los controles y las operaciones de los sistemas de información

a. Al 19 de marzo de 2009, la Oficina de Auditoría Interna e Inspectoría de la AAFET no había efectuado auditorías de los controles y las operaciones de los sistemas de información, y de la seguridad de las aplicaciones más importantes de la AAFET.

Una situación similar se comentó en el *Informe de Auditoría CPED-95-6*.

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 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 al 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 demás operaciones de la AAFET. Además, existe la posibilidad de que en los sistemas de información no se incluyan 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 e Inspectoría no contaba con personal suficiente y adiestrado en el área de auditoría de sistemas de información.

En la carta de la Administradora de la AAFET, esta nos indicó, entre otras cosas, lo siguiente:

> Actualmente la Oficina de Auditoría Interna cuenta con dos auditores incluyendo la Directora de la oficina. Estas personas no tienen el expertis necesarios para realizar auditorías a los sistemas de información.

Reconocemos que la agencia no cuenta con los recursos económicos para atender de inmediato esta situación. No obstante, estaremos buscando alternativas de manera que podamos implementar las recomendaciones a estos efectos. [*sic*]

ANEJO

DEPARTAMENTO DEL TRABAJO Y RECURSOS HUMANOS

ADMINISTRACIÓN PARA EL ADIESTRAMIENTO DE FUTUROS EMPRESARIOS Y TRABAJADORES

OFICINA DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Hon. Miguel A. Romero Lugo	Secretario del Trabajo y Recursos Humanos	2 en. 09	27 m. 09
Sr. Román M. Velasco González	"	8 dic. 08	31 dic. 08
Dra. Iris N. López Sánchez	Administradora	2 en. 09	27 m. 09
Sr. Eduardo J. Vergara Agostini	Administrador	8 dic. 08	31 dic. 08
Srta. Ivelisse Sánchez Collazo	Directora de Recursos Humanos	7 en. 09	27 m. 09
Sra. Thelma Cabrera Delgado	"	8 dic. 08	31 dic. 08
Sra. Sonia Berríos López	Directora de Finanzas	2 feb. 09	27 m. 09
Sra. Mirna J. Purcell Salgado	"	8 dic. 08	31 dic. 08
Sr. Daniel Santiago Berríos	Director de Sistemas de Información	16 en. 09	27 m. 09
Sr. Salvador Méndez Torres	"	8 dic. 08	31 dic. 08
Sra. Luz H. Morales Rosario	Directora de Auditoría Interna e Inspectoría	16 en. 09	27 m. 09
Sra. Yaniz Jiménez Borrero	"	8 dic. 08	31 dic. 08