Secretaría

MANUEL A. TORRES NIEVES
SECRETARIO DEL SENADO

- [x] Ver al dorso
- [ ] Para su información
- [ ] Notas
- [ ] Para mantenerle al día
- [x] Expediente
- [ ] Dar Cuenta
- [ ] Registrar y Procesar

Senado
DE PUERTO RICO

EL CAPITOLIO
PO Box 9023431
San Juan, Puerto Rico
00902-3431

T: 787.722.3460
787.722.4012
F: 787.723.5413
E: mantorres@senadopr.us
W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

- [ ] Hacienda
- [ ] Gobierno
- [x] Seguridad Pública y Judicatura
- [ ] Salud
- [ ] Educación y Asuntos de la Familia
- [ ] Desarrollo Eonómico y Planificación
- [ ] Urbanismo e Infraestructura
- [ ] Jurídico Penal
- [ ] Jurídico Civil
- [ ] Agricultura
- [ ] Recursos Naturales y Ambientales
- [ ] Comercio y Cooperativismo
- [ ] Turismo y Cultura
- [ ] Trabajo, Asuntos del Veterano y Recursos Humanos
- [ ] Bienestar Social
- [ ] Asuntos Municipales
- [ ] Recreación y Deportes
- [ ] Banca, Asuntos del Consumidor y Corporaciones Públicas
- [ ] Desarrollo de la Región del Oeste
- [ ] Asuntos de la Mujer
- [ ] Asuntos Internos
- [ ] Reglas y Calendario
- [ ] Asuntos Federales
- [ ] De la Montaña
- [ ] Ética

COMISIONES ESPECIALES

- [ ] Puerto de las Américas
- [ ] Derecho de Autodeterminación del Pueblo de Puerto Ricc
- [ ] Sobre Reforma Gubernamental

COMISIONES CONJUNTAS

- [ ] Informes Especiales del Contralor
- [ ] Donativos Legislativos de Puerto Rico
- [ ] Internado Córdova-Fernós
- [ ] Internado Pilar Barbosa
- [ ] Internado Ramos Comas
- [ ] Código Penal
- [ ] Revisión y Reforma del Código Civil
- [ ] Alianzas Público Privadas
- [ ] Auditoría Fiscal y Manejo Fondos Públicos
- [ ] Revisión Continua Código Penal y Reforma de las Leyes

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

RECIBIDO
SENADO DE PUERTO RICO
SECRETARIA
2010 FEB 18 PM 3:31

Manuel Díaz Saldaña
Contralor

18 de febrero de 2010

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Thomas Rivera Schatz
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-10-12* del Centro de Sistemas de Información de la Agencia Estatal para el Manejo de Emergencias y Administración de Desastres de Puerto Rico aprobado por esta Oficina el 16 de febrero de 2010. Publicaremos dicho *Informe* en nuestra página en Internet: http://www.ocpr.gov.pr para conocimiento de los medios de comunicación y de otras partes interesadas.

Estamos a sus órdenes para ofrecerle cualquier información adicional que estime necesaria.

Contamos con su cooperación para mejorar la fiscalización y la administración de la propiedad y de los fondos públicos.

Cordialmente,

Manuel Díaz Saldaña

Anejo

PO BOX 366069 SAN JUAN, PUERTO RICO 00936-6069
105 AVENIDA PONCE DE LEÓN, HATO REY, PUERTO RICO 00917-1136
TEL. (787) 754-3030 FAX (787) 751-6768
E-MAIL: ocpr@ocpr.gov.pr INTERNET: http://www.ocpr.gov.pr

PO_8325

INFORME DE AUDITORÍA TI-10-12

16 de febrero de 2010

Agencia Estatal para el Manejo de Emergencias y Administración de Desastres de Puerto Rico

Centro de Sistemas de Información

(Unidad 5249 - Auditoría 13157)

Período auditado: 17 de marzo al 28 de octubre de 2008

CONTENIDO

Página

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

RESPONSABILIDAD DE LA GERENCIA **5**

ALCANCE Y METODOLOGÍA **6**

OPINIÓN **6**

RECOMENDACIONES **7**

AL DIRECTOR EJECUTIVO DE LA AGENCIA ESTATAL PARA EL MANEJO DE EMERGENCIAS Y ADMINISTRACIÓN DE DESASTRES DE PUERTO RICO 7

CARTAS A LA GERENCIA **11**

COMENTARIOS DE LA GERENCIA **12**

AGRADECIMIENTO **12**

RELACIÓN DETALLADA DE HALLAZGOS **13**

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO 13

HALLAZGOS EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DE LA AGENCIA ESTATAL PARA EL MANEJO DE EMERGENCIAS Y ADMINISTRACIÓN DE DESASTRES DE PUERTO RICO 14

1 - Computadoras y cuentas para acceder a Internet utilizadas para fines ajenos a la gestión pública, y falta de controles para prevenir y detectar la instalación de programas no autorizados y la remoción de programas autorizados, de actualización de las definiciones del programa antivirus instalado en las computadoras y de pantallas de advertencias sobre el uso de éstas 14

2 - Desviaciones de ley y de reglamentación relacionadas con la desaparición de propiedad pública 19

3 - Falta de inventarios físicos de la propiedad de los sistemas de información computadorizados y de un registro de programas instalados en cada computadora 21

4 - Falta de normas y de procedimientos escritos para la instalación y la configuración de la red, para la preparación y la actualización del inventario de los equipos de la red y para la disposición de la información sensitiva 23

5 - Deficiencias relacionadas con la seguridad y el acceso físico a los cuartos de distribución del cableado (*wiring closets*), en el mantenimiento de los equipos y en el diagrama esquemático de la red 25

6 - Deficiencias relacionadas con la configuración y la estructura de seguridad para acceder a la red, falta de actualización del programa antivirus y de producción de respaldos de la información almacenada en la red 29

7 - Deficiencias en los parámetros de seguridad de los servidores de la AEMEAD para controlar las cuentas de acceso a los recursos de la red 31

8 - Equipos de comunicación sin uso 34

9 - Falta de documentación de la justificación para la otorgación de privilegios de conexión remota y de configuración para controlar los accesos remotos 35

10 - Falta de adiestramientos periódicos al Gerente de Sistemas de Información 37

ANEJO - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO 39

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

16 de febrero de 2010

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

Realizamos una auditoría de las operaciones del Centro de Sistemas de Información (CSI) de la Agencia Estatal para el Manejo de Emergencias y Administración de Desastres de Puerto Rico (AEMEAD) 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.

Determinamos emitir dos informes de esta auditoría. Este es el último informe y contiene el resultado de nuestro examen de los controles internos establecidos para el uso de las computadoras, Internet y el correo electrónico, para la red de comunicaciones (red), y para el acceso lógico a los sistemas de información computadorizados. El primer informe se emitió el 4 de febrero de 2009 y contiene el resultado de nuestro examen de los controles internos relacionados con la evaluación de riesgos y el plan de seguridad y, los controles de acceso físico y de sistemas operativos establecidos en el CSI (*Informe de Auditoría TI-09-13*).

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La AEMEAD se creó mediante la *Ley Núm. 211 del 2 de agosto de 1999, Ley de la Agencia Estatal para el Manejo de Emergencias y Administración de Desastres de Puerto Rico*, según enmendada, adscrita a la Comisión de Seguridad y Protección Pública de

Puerto Rico[1]. Se creó con el objetivo de establecer la política pública del Gobierno de Puerto Rico en relación con situaciones de emergencia que afecten a la Isla. Además, por virtud de dicha *Ley* y del *Boletín Administrativo Núm. OE-2001-26* del 25 de junio de 2001 emitido por la Gobernadora, la AEMEAD es responsable de coordinar las cuatro fases de manejo de emergencias, a saber: preparación, mitigación, respuesta y recuperación. Por virtud de la *Ley Núm. 211*, se derogó la ley creadora de la Defensa Civil de Puerto Rico[2] y las funciones de ésta le fueron transferidas a la AEMEAD.

La administración de las operaciones de la AEMEAD está a cargo de un Director Ejecutivo nombrado por el Comisionado de Seguridad y Protección Pública[3], en consulta con el Gobernador[4]. El Director Ejecutivo ejerce sus funciones a través de sus oficinas de Información y Prensa, Programas Federales y las áreas de Administración y Operación. La AEMEAD cuenta, además, con 11 zonas regionales a través de toda la Isla ubicadas en: Aguadilla, Arecibo, Carolina, Fajardo, Guayama, Gurabo, Humacao, Mayagüez, Orocovis, Ponce y San Juan. En estas zonas se ofrecen los servicios necesarios a la ciudadanía en caso de emergencias. En el **ANEJO** se incluye una lista de los funcionarios principales que actuaron durante el período auditado.

El CSI está adscrito a la División de Administración y cuenta con un Gerente de Sistemas de Información, un Oficial Ejecutivo I y un Operador de Equipo Electrónico de Información.

---

[1] El propósito principal de la Comisión es coordinar las actividades de varios organismos que realizan funciones en el Área de Seguridad y Protección Pública.

[2] *Ley Núm. 22 del 23 de junio de 1976, Ley de la Defensa Civil de Puerto Rico*, según enmendada.

[3] La Comisión está constituida por el Superintendente de la Policía (Comisionado), el Jefe del Cuerpo de Bomberos, el Director del Cuerpo de Emergencias Médicas y el Ayudante de la Guardia Nacional de Puerto Rico.

[4] Los directores ejecutivos que se desempeñaron del 8 de noviembre de 2007 al 14 de marzo de 2008 fueron nombrados por el Gobernador, ya que la Comisión estaba administrativamente inoperante, aunque la *Ley* no había sido derogada ni enmendada.

Los gastos operacionales del CSI eran sufragados del presupuesto operacional de la AEMEAD, que para los años fiscales 2007-08 y 2008-09 ascendió a $11,043,000 y $14,817,900, respectivamente.

Al 28 de octubre de 2008, estaba pendiente de resolución por los tribunales una demanda civil presentada contra la AEMEAD por $6,800,000. Esta demanda era por daños y perjuicios. En dicha demanda se alega que se utilizó una computadora portátil para fines ajenos a la gestión pública.

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

RESPONSABILIDAD DE LA GERENCIA

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

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

10. Cumplir con la *Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, lo cual incluye divulgar sus disposiciones a todo el personal.

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

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 17 de marzo al 28 de octubre de 2008. 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 y a empleados
- 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 del CSI en lo que concierne a los controles internos establecidos para el uso de las computadoras, Internet y el correo electrónico, para la red, y para el acceso lógico a los sistemas de información computadorizados, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 10**, clasificados como principales, se comentan en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**.

RECOMENDACIONES

AL DIRECTOR EJECUTIVO DE LA AGENCIA ESTATAL PARA EL MANEJO DE EMERGENCIAS Y ADMINISTRACIÓN DE DESASTRES DE PUERTO RICO

1. Ejercer una supervisión efectiva sobre el Director del Área de Administración para que se asegure de que:

   a. El Gerente de Sistemas de Información del CSI:

      1) Oriente a los funcionarios y a los empleados de la AEMEAD sobre el uso adecuado, las restricciones y el manejo correcto de las computadoras y de las cuentas para acceder a Internet, y conserve evidencia de dicha orientación. **[Hallazgo 1-a.1) y 2), y b.]**

      2) Establezca por escrito los controles necesarios para asegurarse de que los sistemas computadorizados se utilizan para asuntos oficiales. Además, vea que se cumpla con dichos controles. **[Hallazgo del 1-a.1) al 3) y b.]**

      3) Realice inspecciones periódicas para asegurarse de que los usuarios cumplan con las normas establecidas sobre el uso de las computadoras y de las cuentas para acceder a Internet. **[Hallazgo del 1-a.1) al 3) y b.]**

      4) Establezca los controles necesarios para restringir el acceso de los usuarios de las computadoras a la opción *Add/Remove Programs* del sistema operativo. Esto, para que los usuarios no puedan instalar ni remover programas. **[Hallazgo 1-a.3) y 5)]**

      5) Mantenga un registro de los programas adquiridos por la AEMEAD e instalados en las computadoras de ésta que contenga, entre otra información, el número de la licencia y el costo de los programas instalados, el nombre del usuario, el número de propiedad y la descripción de la computadora donde están instalados los mismos. Esto, con el fin de mantener un inventario de los mismos y detectar la instalación de programas no autorizados. **[Hallazgos 1-a.3) y 3-b.]**

6) Establezca un plan de actualización del programa antivirus para que se asegure de que los equipos computadorizados de la AEMEAD tengan instalada la versión más reciente de éste. Además, efectúe inspecciones periódicas para asegurarse del cumplimiento del mismo. **[Hallazgos 1-a.4) y 6-b.]**

7) Incluya una advertencia en la pantalla inicial de todas las computadoras para que se notifique a los usuarios sobre las normas principales para el uso de las mismas y éstos se comprometan a observarlas, y conozcan las medidas aplicables en caso de violación a las mismas. **[Hallazgo 1-a.6)]**

8) Prepare y remita para la consideración y la aprobación del Director Ejecutivo:

   a) Las normas y los procedimientos necesarios para reglamentar los procesos que se comentan en el **Hallazgo 4**.

   b) Los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. **[Hallazgo 9-a.1)]**

9) Establezca las medidas necesarias para la protección física de los equipos de la red, de manera que no estén accesibles al personal ajeno a las operaciones de ésta. **[Hallazgo 5-a.1) y 4)]**

10) Prepare un diagrama de los *drops* e incluya copia de éste en un área visible en los cuartos de distribución del cableado. **[Hallazgo 5-a.2)]**

11) Instale los equipos para controlar la temperatura y detectar humo en los cuartos de distribución del cableado de la AEMEAD. **[Hallazgo 5-a.3)]**

12) Establezca un plan para el mantenimiento preventivo de los equipos computadorizados conectados a la red y que el mismo incluya un itinerario de limpieza rutinario. **[Hallazgo 5-b.]**

13) Establezca un registro de servicios de los programas y los equipos de la red que presentan problemas. **[Hallazgo 5-c.]**

14) Prepare un diagrama de la red que incluya la información descrita en el **Hallazgo 5-d.**

15) Establezca una configuración que incluya una Zona Desmilitarizada (*DMZ,* por sus siglas en inglés)[5] que limite el acceso desde Internet a los servidores de la red de la AEMEAD y viceversa. Esto es necesario para proteger la red de ataques cibernéticos, y para evitar que personas externas y no autorizadas puedan acceder a ésta y comprometer la seguridad de sus sistemas. **[Hallazgo 6-a.]**

16) Prepare los respaldos (*backups*) de la información almacenada en los servidores y que los mismos se mantengan en un lugar seguro fuera de los predios de la AEMEAD. **[Hallazgo 6-c.]**

17) Efectúe las modificaciones en los parámetros de seguridad del sistema operativo de los servidores de la red para:

    a) Requerir un mínimo de 10 días antes que el sistema permita al usuario cambiar la contraseña nuevamente. **[Hallazgo 7-a.1)a)]**

    b) Establecer un mínimo de ocho caracteres para la utilización de las contraseñas. **[Hallazgo 7-a.1)b)]**

    c) Restringir el horario de acceso a los recursos de la red, según las funciones y las responsabilidades de cada usuario, y activar en los servidores la opción para desconectar automáticamente las cuentas de acceso cuando éstas son utilizadas para acceder los recursos de la red fuera de horas laborables. **[Hallazgo 7-a.1)c)]**

---

[5] En seguridad informática, una zona desmilitarizada (*DMZ*, por sus siglas en inglés) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una *DMZ* es que las conexiones desde la red interna y la externa a la *DMZ* estén permitidas, mientras que las conexiones desde la *DMZ* sólo se permitan a la red externa. La *DMZ* se utiliza para ubicar servidores que son necesarios que sean accedidos desde fuera, como servidores de *E-mail*, *Web* y *DNS* (*Domain Name Service*).

d) Restringir que los usuarios puedan repetir las últimas cinco contraseñas utilizadas anteriormente. **[Hallazgo 7-a.1)d)]**

e) Establecer que las contraseñas sean combinaciones de letras y números. **[Hallazgo 7-a.1)e)]**

f) Activar la opción de *Lockout after __ bad logon attempts* para deshabilitar las cuentas de acceso luego de tres intentos fallidos de conexión al sistema. **[Hallazgo 7-a.1)f)]**

18) Active las políticas de auditoría (*Audit Policy*) que provee el sistema operativo, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la AEMEAD. **[Hallazgo 7-a.2)]**

19) Establezca un término fijo de, por lo menos, una vez al año para que el sistema requiera cambiar la contraseña de la cuenta de Administrador. **[Hallazgo 7-a.3)]**

20) Elimine prontamente las cuentas de acceso de los empleados que cesaron en sus funciones y vea que, en lo sucesivo, las cuentas se eliminen en el momento en que el empleado cesa. Esto, de manera que se corrija y no se repita la situación comentada en el **Hallazgo 7-a.4)**.

21) Prepare un plan para terminar la instalación del cableado, de manera que los equipos de comunicación mencionados en el **Hallazgo 8** se puedan utilizar eficazmente.

22) Se configuren las opciones de seguridad en el sistema operativo para controlar los accesos mediante procedimientos de *call back*[6]. **[Hallazgo 9-a.2)]**

---

[6] Es un control de acceso mediante el cual la computadora verifica que el número recibido está autorizado a conectarse remotamente para acceder a los sistemas de información computadorizados de la entidad.

b. El Encargado de la Propiedad:

1) Notifique a la Oficina del Contralor de Puerto Rico y a las demás entidades gubernamentales concernientes, dentro del término establecido, cualquier irregularidad relacionada con la propiedad y los fondos públicos. **[Hallazgo 2]**

2) Cumpla con la *Ley Núm. 230 del 23 de julio de 1974, Ley de Contabilidad del Gobierno de Puerto Rico*, según enmendada, y con el *Reglamento Núm. 11, Normas Básicas para el Control y la Contabilidad de los Activos Fijos*, aprobado el 29 de diciembre de 2005 por el Secretario de Hacienda, relacionado con la custodia y el control de la propiedad. **[Hallazgo 3-a.]**

c. El Director de la División de Recursos Humanos, en coordinación con el Gerente de Sistemas de Información, establezca un procedimiento para que se notifique a tiempo al CSI el cese de un usuario en sus funciones para la cancelación de la cuenta de acceso de éste. **[Hallazgo 7-a.4)]**

d. Establezca, en coordinación con el Director de la División de Recursos Humanos, un programa de adiestramiento continuo para el Gerente de Sistemas de Información. **[Hallazgo 10]**

CARTAS A LA GERENCIA

El borrador de los **hallazgos** de este *Informe* se remitió al Sr. Heriberto Saurí Santiago, Director Ejecutivo, para comentarios, en carta del 16 de noviembre de 2009. Con el mismo propósito, remitimos el borrador de los **hallazgos** de este *Informe* a la Sra. Karilyn Bonilla Colón, ex Directora Ejecutiva, en carta de esa misma fecha, por correo certificado con acuse de recibo, a una dirección provista por la AEMEAD. Con los referidos borradores se incluyeron anejos que especifican detalles sobre los **hallazgos**.

COMENTARIOS DE LA GERENCIA

El Director Ejecutivo contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 30 de noviembre de 2009. En dicha carta nos indicó que no tenía observaciones relacionadas con los hallazgos de este *Informe*.

El 1 de diciembre de 2009, la ex Directora Ejecutiva solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. En esa misma fecha le concedimos la prórroga hasta el 16 de diciembre de 2009. La ex Directora Ejecutiva contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 15 de diciembre de 2009 y nos indicó que no tenía acceso a información administrativa de la agencia ni evidencia que pudiera sustentar sus argumentos.

AGRADECIMIENTO

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

Oficina del Contralor

Por:

RELACIÓN DETALLADA DE HALLAZGOS

CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO

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

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

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

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

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

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

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

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

consideran al revisar el borrador del informe y se incluyen al final del hallazgo correspondiente en la sección de HALLAZGOS EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DE LA AGENCIA ESTATAL PARA EL MANEJO DE EMERGENCIAS Y ADMINISTRACIÓN DE DESASTRES DE PUERTO RICO, de forma objetiva y conforme a las normas de nuestra Oficina. Cuando la gerencia no provee evidencia competente, suficiente y relevante para refutar un hallazgo, éste prevalece y se añade al final del mismo la siguiente aseveración: Consideramos las alegaciones de la gerencia, pero determinamos que el hallazgo prevalece.

HALLAZGOS EN EL CENTRO DE SISTEMAS DE INFORMACIÓN DE LA AGENCIA ESTATAL PARA EL MANEJO DE EMERGENCIAS Y ADMINISTRACIÓN DE DESASTRES DE PUERTO RICO

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

Hallazgo 1 - Computadoras y cuentas para acceder a Internet utilizadas para fines ajenos a la gestión pública, y falta de controles para prevenir y detectar la instalación de programas no autorizados y la remoción de programas autorizados, de actualización de las definiciones del programa antivirus instalado en las computadoras y de pantallas de advertencias sobre el uso de éstas

a. El *Inventario de Equipos de Computadoras* de la AEMEAD del 16 de junio de 2008, provisto por el Encargado de la Propiedad, contenía 106 computadoras localizadas en la Oficina Central de la AEMEAD. Las certificaciones provistas por los directores de las 11 zonas regionales de la AEMEAD del 23 de abril al 29 de junio de 2008 de los equipos computadorizados localizado en las mismas contenían 72 computadoras. Dichos inventarios fueron realizados a solicitud de nuestros auditores. **[Véase el Hallazgo 3]**

El examen del uso de 24 computadoras, reveló lo siguiente:

1) Siete computadoras[7] (29 por ciento) contenían documentos ajenos a la gestión pública.

2) Tres computadoras[7] (13 por ciento) se utilizaron para examinar páginas en Internet cuyo contenido era ajeno a la gestión pública.

[7] Una relación de las computadoras se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

3) Dieciséis computadoras[8] (67 por ciento) tenían instalados programas que no guardaban relación con los trabajos que se realizaban en la AEMEAD.

4) Once computadoras[8] (46 por ciento) no tenían actualizadas las definiciones[9] (*virus definitions file*) del programa antivirus instalado en las referidas computadoras. Esto, para la prevención y la detección de programas no deseados.

5) Las 24 computadoras[8] no tenían controles para impedir el acceso a la opción *Add/Remove Programs* del sistema operativo. Esto, para imposibilitar que los usuarios instalen programas no autorizados o remuevan programas autorizados. El acceso a dicha opción solamente debe estar disponible para el Encargado del Sistema.

6) Diecinueve computadoras[8] (79 por ciento) no incluían una advertencia en la pantalla inicial para notificar a los usuarios sobre las normas principales para el uso de las mismas.

b. La AEMEAD tenía un servidor[10] en la red que permitía acceso a Internet a los usuarios autorizados. Dicho servidor producía diariamente un archivo en el cual se registraban todas las páginas de direcciones de Internet (*Log* del *ISA Server*) que fueron accedidas por las cuentas de usuarios. El examen del registro de direcciones de Internet del mencionado servidor correspondiente al 12 de agosto de 2008 reveló que ese día se había utilizado este servicio para acceder 22 páginas de Internet con contenido ajeno a la gestión pública[11]. No se pudieron determinar las cuentas de acceso de los usuarios que visitaron las mismas porque el servidor no estaba configurado para que se registrara el nombre del usuario que accedía a las páginas de Internet.

---

[8] Véase la nota al calce 7.

[9] Archivos que contienen información sobre las características y el comportamiento de los virus que afectan los sistemas computadorizados.

[10] El nombre del servidor se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

[11] Una relación de las páginas visitadas ajenas a la gestión pública se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

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

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

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

- Los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que sólo pueden utilizarse para fines estrictamente oficiales y legales.

- Los programas y los recursos utilizados en los sistemas de información de las entidades gubernamentales sólo podrán ser instalados por personal autorizado a tales efectos. Además, no podrán instalarse programas sin la previa autorización del Departamento de Sistemas de Información, aunque sean programas libres de costo.

- Los sistemas de comunicación y el acceso a Internet son propiedad de la entidad gubernamental y deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las normas que rigen el comportamiento del personal de la entidad y nunca con fines no oficiales o para actividades personales o con fines de lucro.

- Cada entidad gubernamental será responsable de verificar que la Internet y el correo electrónico funcionen adecuadamente. También se asegurarán que la información contenida en dichos sistemas esté protegida de accesos no autorizados. La agencia utilizará sistemas de protección contra virus y sistemas de protección contra accesos no autorizados (*firewall*).

- Cada entidad gubernamental debe colocar un aviso que indique al usuario o a quien acceda a su sistema de información que el mismo es propiedad de esa entidad del Estado Libre Asociado de Puerto Rico y que se compromete a utilizarlo conforme a las normas establecidas.

En la *Política Núm. TIG-003, Seguridad de los Sistemas de Información de la Carta Circular Núm. 77-05*, se establece que las agencias deberán instalar controles automáticos para la prevención y detección de programas no deseados, tales como: virus, *spyware*[12], *adware*[13] y *updates* automáticos. Esto implica que, como norma de sana administración, dichos programas deberán estar actualizados, de manera que los mismos puedan detectar y eliminar nuevas amenazas.

En la *Carta Circular OC-98-11, Sugerencias sobre normas y controles para el uso de los sistemas computadorizados*, promulgada el 18 de mayo de 1998 por el Contralor de Puerto Rico, se recomienda incluir una advertencia en la pantalla inicial del sistema para que se notifique al usuario sobre las normas principales para el uso del mismo y se comprometa a observarlas. Además, para que conozca sobre las medidas aplicables en caso de la violación a las mismas. En la *Carta Circular OC-06-13, Sugerencias sobre Normas y Controles para el Uso de los Sistemas Computadorizados*, promulgada el 28 de noviembre de 2005 por el Contralor de Puerto Rico, se incluye copia del programa y el texto de las normas que mantenemos en nuestros sistemas computadorizados.

---

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

[13] Programa que se instala inadvertidamente en una computadora y su principal propósito es desplegar ante el usuario anuncios y propaganda.

El uso de las computadoras pertenecientes a la AEMEAD para procesar documentos y examinar archivos de carácter privado es contrario al interés público y desvirtúa los propósitos para los cuales fueron adquiridas. Además, provee al funcionario o empleado que indebidamente las utiliza ventajas, beneficios y privilegios que no están permitidos por ley. Por otro lado, los programas no autorizados y los archivos ajenos a la gestión pública ocupan espacio y capacidad en los sistemas de información, lo que afecta el rendimiento de los mismos. Además, proliferan la transmisión de los virus de computadoras, lo que podría destruir información importante almacenada en las mismas. **[Apartados del a.1) al 3) y b.]**

La situación comentada en el **Apartado a.4)** impide la prevención y la detección de programas no deseados, y da lugar a que éstos se propaguen a los sistemas de información, lo que podría afectar la integridad, la confidencialidad y la disponibilidad de éstos.

La situación comentada en el **Apartado a.5)** propicia la instalación y el uso de programas no autorizados, y la remoción de programas autorizados, con los consiguientes efectos adversos.

La falta de las advertencias de uso en las computadoras asignadas a los usuarios podría causar que éstos no observen las normas principales para el uso de los sistemas de información, que se dificulte imponer sanciones por la violación a las mismas, y que se incurra en irregularidades y otras situaciones adversas. **[Apartado a.6)]**

Las situaciones comentadas se debían a la falta de:

- Adiestramientos y orientaciones periódicas a los usuarios de los equipos computadorizados sobre las leyes, las normas y los procedimientos que reglamentan el uso de las computadoras e Internet. **[Apartados a.1) y 2), y b.]**

- Controles efectivos para asegurarse del uso oficial de los sistemas computadorizados y de las cuentas de acceso a Internet, y para la detección, el control y la corrección de virus o programas no deseados. **[Apartados del a.1) al 6) y b.]**

- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento por los usuarios de las normas establecidas sobre el uso oficial de las computadoras y de las cuentas para acceder a Internet. **[Apartados del a.1) al 3) y b.]**

- Controles efectivos que limiten el acceso a la opción de *Add/Remove Programs* del sistema operativo en las computadoras. **[Apartado a.3)]**

- Planes de actualización del programa antivirus que asegurara que los equipos computadorizados de la AEMEAD tuvieran instalada la versión más reciente de éste. **[Apartado a.4)]**

Véase la Recomendación de la 1.a.1) a la 7).

Hallazgo 2 - Desviaciones de ley y de reglamentación relacionadas con la desaparición de propiedad pública

a. Según información obtenida por nuestros auditores, el 23 de mayo de 2008 se desapareció una computadora portátil[14] adquirida por $2,158. Dicha computadora estaba asignada al Director de la Zona de Aguadilla de la AEMEAD. El 24 de mayo de 2008, el Director de la Zona de Aguadilla notificó la desaparición de la computadora a la Policía de Puerto Rico y el 27 de mayo de 2008 al Director del Área de Administración de la AEMEAD. El examen realizado reveló lo siguiente:

   1) El 18 de julio de 2008, el Supervisor de la División de Servicios Generales, quien funge como Encargado de la Propiedad, notificó a la Oficina del Contralor de Puerto Rico la desaparición de dicha computadora con 25 días de dilación.

   2) Al 11 de julio de 2008, no se había informado la desaparición de la computadora al Área de Seguros Públicos del Departamento de Hacienda.

[14] La marca y el número de propiedad de la computadora portátil se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

En la *Ley Núm. 96 del 26 de junio de 1964*, según enmendada, se dispone que toda agencia que determine cualquier pérdida de fondos o bienes públicos bajo su dominio, control o custodia deberá notificarlo prontamente al Contralor de Puerto Rico para la acción que corresponda.

En el Artículo 4-a. del *Reglamento Núm. 41, Notificación de Irregularidades en el Manejo de la Propiedad y los Fondos Públicos a la Oficina del Contralor de Puerto Rico*[15], aprobado el 10 de noviembre de 1999 por el Contralor de Puerto Rico, se dispone, entre otras cosas, que las agencias serán responsables de notificar a la Oficina del Contralor de Puerto Rico las irregularidades en el manejo de fondos y bienes públicos que surjan, dentro de un término de 30 días contados a partir de la fecha en que se descubrió la irregularidad. En el Artículo 6-a. de dicho *Reglamento* se establece que las agencias serán responsables de notificar las irregularidades, además, al Departamento de Justicia, al Departamento de Hacienda y a cualquier otro organismo que por ley se le requiera, conforme se disponga por ley o reglamento.

Las situaciones comentadas le impidieron al Contralor de Puerto Rico y al Director del Área de Seguros Públicos del Departamento de Hacienda tener conocimiento de los hechos mencionados para tomar las medidas correspondientes prontamente.

Las situaciones comentadas se debieron a que el Encargado de la Propiedad se apartó de las disposiciones reglamentarias mencionadas. Además, a que el Director del Área de Administración no supervisó adecuadamente dichas operaciones.

Véase la Recomendación 1.b.1).

---

[15] Este *Reglamento* fue derogado por el *Reglamento Núm. 43, Reglamento Derogatorio*, del 16 de julio de 2008. El 20 de junio de 2008 el Contralor de Puerto Rico aprobó el *Reglamento Núm. 41, Notificación de Pérdidas o Irregularidades en el Manejo de Fondos o Bienes Públicos a la Oficina del Contralor de Puerto Rico*, el cual contiene disposiciones similares.

Hallazgo 3 - Falta de inventarios físicos de la propiedad de los sistemas de información computadorizados y de un registro de programas instalados en cada computadora

a. El Encargado de la Propiedad es responsable de la custodia, el control y la contabilidad de la propiedad mueble de ésta. El examen realizado reveló que el Encargado de la Propiedad no había realizado un inventario de la propiedad de los sistemas de información computadorizados que incluyera, entre otras cosas, la descripción, el número de propiedad, la fecha de adquisición, el precio unitario y la localización. **[Véase el Hallazgo 1]**

En la *Ley Núm. 230* 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. Como parte de esto y como norma de sana administración y de control interno, las entidades deben mantener registros de la propiedad confiables y actualizados para ejercer un control eficaz de los activos y asegurar que los mismos existan. Esto, para tener información confiable y poder fijar responsabilidades a los empleados que tienen a su cargo la custodia de la propiedad en caso de alguna situación irregular, y se pueda ejercer un control adecuado de tales transacciones.

En el Artículo XIV del *Reglamento Núm. 11* se establece, entre otras cosas, lo siguiente:

- Los registros internos de las dependencias de inventario tienen que estar respaldados por los inventarios físicos.

- Las agencias prepararán el inventario de forma mecanizada con el *Modelo SC 795, Inventario Físico de Activo Fijo*. El inventario debe incluir los siguientes datos: el número de propiedad, el costo, la clase de propiedad, la descripción, la fecha de adquisición y el código de fondo que se cargó para adquirir la propiedad.

La situación comentada impide a la AEMEAD mantener un control adecuado de los equipos de los sistemas computadorizados bajo su custodia. Además, propicia el ambiente para el uso indebido o la desaparición de la misma y otras situaciones adversas sin que se puedan detectar a tiempo para fijar responsabilidades.

La situación comentada es indicativa de que el Encargado de la Propiedad y el Director del Área de Administración no cumplieron con sus responsabilidades ni velaron por el cumplimiento de las disposiciones citadas.

b. Al 8 de agosto de 2008, el CSI no mantenía un registro de los programas adquiridos e instalados en cada computadora que incluyera, entre otras cosas, el número de licencia de los programas instalados, el nombre del usuario, el número de propiedad y la descripción de la computadora donde estaban instalados los programas, y el costo de los mismos.

En la *Política TIG-008 de la Carta Circular Núm. 77-05* se establece que los sistemas de información de las entidades gubernamentales, incluidos los programas, las aplicaciones y los archivos electrónicos, son propiedad del Estado Libre Asociado de Puerto Rico, por lo que deben constar en el inventario de las respectivas agencias y sólo pueden utilizarse para fines estrictamente oficiales y legales. Además, los programas y los recursos utilizados en los sistemas de información de las entidades gubernamentales deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas sólo podrán ser instalados por el personal autorizado. Además, no podrán instalarse programas sin la autorización previa del Departamento de Sistemas de Información, aunque sean programas libres de costo.

No cumplir con la disposición mencionada impide ejercer un control eficaz de los programas y las licencias correspondientes. Además, propicia la instalación y el uso de programas no autorizados, sin que se pueda detectar esta situación a tiempo para fijar responsabilidades, con los consiguientes efectos adversos para la AEMEAD. También limitó el alcance de nuestro examen sobre los programas instalados en las computadoras examinadas.

La situación comentada se debía a que el Director del Área de Administración no le había impartido instrucciones al Gerente de Sistemas de Información para mantener un registro y un control adecuado de los programas adquiridos e instalados en las computadoras de la AEMEAD.

Véase la Recomendación 1.a.5) y b.2).

Hallazgo 4 - Falta de normas y de procedimientos escritos para la instalación y la configuración de la red, para la preparación y la actualización del inventario de los equipos de la red y para la disposición de la información sensitiva

a. Al 22 de agosto de 2008, no se habían promulgado las normas ni los procedimientos escritos necesarios para reglamentar los siguientes procesos:

- La instalación y la configuración de la red que permita mantener la uniformidad de las mismas
- La preparación y la actualización del inventario de los equipos de la red
- La disposición de la información sensitiva y de los programas antes de transferir o disponer 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. Se indica que cada entidad gubernamental tiene la responsabilidad de desarrollar normas específicas de seguridad que consideren las características propias de los ambientes de tecnología de ésta, particularmente, sus sistemas de misión crítica.

En la *Política Núm. TIG-008* de dicha *Carta Circular* se establece que cada agencia debe establecer políticas necesarias para garantizar el uso adecuado, efectivo y seguro de los sistemas de información y las herramientas de trabajo que éstos proveen. Esto implica que, como norma de sana administración, se deben establecer por escrito políticas, normas y procedimientos de control interno eficaces que reglamenten las operaciones computadorizadas y estén 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 caso de renuncias o ausencias del personal de mayor experiencia, y facilitan la labor de adiestramiento.

La situación comentada propicia que los mecanismos de control y 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, a los equipos y a la información de la AEMEAD a riesgos innecesarios que pudieran afectar la continuidad de las operaciones. También la falta de procedimientos escritos para borrar información sensitiva y programas antes de transferir o disponer de un equipo puede propiciar que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de la misma.

La situación comentada se atribuye, principalmente, a que el Director del Área de Administración no le había impartido instrucciones al Gerente de Sistemas de Información para que desarrollara y remitiera para la aprobación de la Directora Ejecutiva, las normas y los procedimientos necesarios para reglamentar los referidos procesos.

Véase la Recomendación 1.a.8)a).

Hallazgo 5 - Deficiencias relacionadas con la seguridad y el acceso físico a los cuartos de distribución del cableado (*wiring closets*), en el mantenimiento de los equipos y en el diagrama esquemático de la red

a. El examen efectuado en agosto de 2008 sobre la seguridad y el acceso físico a los cuartos de distribución del cableado (*wiring closets*) de la red de la AEMEAD reveló que no se mantenían las condiciones de seguridad adecuadas para proteger los equipos de comunicación, según se indica:

1) El Departamento de Servicios Generales era el custodio de las llaves de los cuartos de distribución del cableado de la AEMEAD. Por esto, el personal del CSI no tenía control ni el libre acceso a los mismos para atender cualquier eventualidad que afectara las operaciones de la red.

2) Ninguno de los cuartos de distribución del cableado tenía un diagrama de los *drops*[16]. Los cables no estaban amarrados ni organizados. Tampoco estaban identificados al ser conectados a los *switches*[17] desde el panel de distribución (*Patch Panel*).

3) Los cuartos de distribución del cableado de la AEMEAD no contaban con mecanismos para controlar la temperatura ni con detectores de humo.

4) El cableado del panel del servicio telefónico se encontraba en el cuarto de distribución del cableado de uno de los pisos.

En la *Política Núm. TIG-011, Mejores Prácticas de Infraestructura Tecnológica de la Carta Circular Núm. 77-05*, se establece que las agencias tendrán la responsabilidad de adquirir e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. También se establece que las redes en las agencias deben proveer la

[16] Conector de pared para las instalaciones de redes.

[17] Dispositivo de comunicación central para líneas de comunicaciones de red que permite que ocurran transmisiones simultáneas, y aumenta el ancho de banda de la red.

infraestructura necesaria para implementar y mantener los procesos de negocio de la agencia, y ser operacionales y confiables.

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. Para garantizar la seguridad en los sistemas de información y la de los equipos computadorizados, es necesario que:

- Se controle adecuadamente el acceso a las áreas donde están ubicados los equipos de comunicaciones
- Se mantengan los equipos de comunicaciones en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas
- Se mantenga la documentación e identificación adecuada del cableado de conexión a la red de forma que permita corregir a tiempo problemas de comunicación y detectar cualquier conexión no autorizada.

Las situaciones comentadas en el **Apartado a.1) y 4)** pueden propiciar que personas ajenas a las operaciones de la red tengan acceso a los equipos, lo que representa un riesgo para la continuidad de los servicios que ofrece la AEMEAD, así como la confidencialidad de la información. Además, pudieran ocasionar daños a los equipos de comunicación y dificultarían fijar responsabilidades.

La situación comentada en el **Apartado a.2)** impide a la AEMEAD obtener una comprensión clara sobre los componentes de la red, de manera que se mantenga un control eficiente y efectivo al administrar y efectuar el mantenimiento de la misma. Además, dificulta atender los problemas de conexión en un tiempo razonable y planificar eficazmente las mejoras a la red, según el crecimiento de sus sistemas.

La situación comentada en el **Apartado a.3)** pudiera ocasionar daños y deterioros prematuros a los equipos de la red y a los equipos de computadoras, lo que dificultaría obtener el rendimiento máximo en términos de los servicios que ofrecen estos equipos.

b. El examen realizado sobre el mantenimiento a los equipos conectados a la red de la AEMEAD reveló que en el CSI no se había implantado un itinerario para el mantenimiento y la limpieza rutinaria de los equipos conectados a la misma. Tampoco se había implantado un registro del tiempo que los recursos de la red no se encontraban disponibles para los usuarios.

c. El CSI no mantenía un registro de servicios de los programas y los equipos de la red que presentan problemas a los usuarios de la AEMEAD.

En la *Política Núm. TIG-004 de la Carta Circular Núm. 77-05* se establece que el personal de la oficina de tecnología de información de la agencia será el responsable de proveer apoyo a sus usuarios, así como del mantenimiento de sus sistemas internos. Además, revisará regularmente sus sistemas para verificar que funcionen adecuadamente.

La situación comentada en el **Apartado b.** podría propiciar que fallas en los equipos que componen la red no sean detectadas a tiempo. Esto, a su vez, puede resultar en una falla mayor en la que se interrumpan las operaciones de la AEMEAD.

La situación comentada en el **Apartado c.** impide a la AEMEAD detectar fallas en los programas y equipos de la red sin que éstas puedan ser corregidas a tiempo.

d. El CSI no tenía documentación en la AEMEAD a nivel central ni tampoco en sus 11 zonas sobre:

- Las instalaciones, las interconexiones y las configuraciones de los equipos de comunicación conectados a la red
- La estructura de la red
- La instalación y la configuración del sistema operativo de cada computadora principal de la unidad y sus correspondientes servicios
- Las instalaciones y las configuraciones de los cuartos de distribución de cableado

- Las instalaciones y las configuraciones de interconexiones externas.

En la *Política Núm. TIG-011 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 de servicios eficientemente. Además, incluye como política que el diseño de la red debe estar documentado.

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

La situación comentada impide a la AEMEAD tener una comprensión 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.

Las situaciones comentadas se debían a que la Directora Ejecutiva no había impartido instrucciones para que se implantaran medidas de control para la seguridad y el acceso físico de las instalaciones de la red, la identificación y actualización de la documentación de la red, y para mantener un plan para el mantenimiento preventivo de los equipos computadorizados conectados a la red y un registro de los servicios a los programas y equipos que presentan problemas a los usuarios.

Véase la Recomendación de la 1.a.9) a la 14).

Hallazgo 6 - Deficiencias relacionadas con la configuración y la estructura de seguridad para acceder a la red, falta de actualización del programa antivirus y de producción de respaldos de la información almacenada en la red

a. El examen realizado el 8 de agosto de 2008 a la configuración y a la estructura de seguridad establecida para acceder a la red de la AEMEAD, a través de Internet, reveló que no se había establecido como medida de seguridad una zona desmilitarizada (*DMZ*, por sus siglas en inglés). Esto, para brindar a la red interna de la AEMEAD una protección que minimice los riesgos de que la información sea accedida de forma no autorizada.

   En la *Política Núm. TIG-011 de la Carta Circular 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución de servicios eficientemente. Además, en la *Política Núm. TIG-003* de dicha *Carta Circular* 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.

   La situación comentada propicia que personas no autorizadas puedan lograr acceso mediante Internet a información confidencial y, a la vez, comprometan la seguridad de los equipos de la red por el uso indebido de ésta.

b. El examen realizado el 9 de septiembre de 2008 al servidor principal[18] de la red de la AEMEAD reveló que éste no tenía actualizadas las definiciones (*virus definitions file*) del programa antivirus.

[18] Véase la nota al calce 10.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las agencias deberán instalar controles automáticos para la prevención y la detección de programas no deseados, tales como: virus, *spyware*[19], *adware*[20] y *updates* automáticos. Esto implica que, como norma de sana administración, dichos programas deberán estar actualizados, de manera que los mismos puedan detectar y eliminar nuevas amenazas.

La situación comentada puede impedir la prevención y la detección de programas no deseados y permitir que éstos puedan propagarse a los sistemas de información, lo que afectaría la integridad, la confidencialidad y la disponibilidad de los sistemas de información de la AEMEAD.

c. El examen realizado el 12 de septiembre de 2008 relacionado con los procedimientos utilizados para la producción y el almacenamiento de los respaldos de la información almacenada en dos servidores[21] reveló que el Gerente de Sistemas de Información no había realizado los respaldos desde el 17 de abril de 2008. Tampoco se guardaban los que se habían producido en un lugar seguro fuera de los predios de la AEMEAD.

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 sistema esenciales e importantes para las operaciones de la agencia. En consonancia con dicha política pública se requiere, 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 seguro 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.

---

[19] Véase la nota al calce 12.

[20] Véase la nota al calce 13.

[21] El nombre de los servidores se incluyeron en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

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 AEMEAD.

La situación comentada en el **Apartado a.** se debía a que el Gerente de Sistemas de Información no había configurado la red de la AEMEAD con los criterios básicos de una arquitectura de seguridad.

La situación comentada en el **Apartado b.** se debía, en parte, a que el Gerente de Sistemas de Información no revisaba periódicamente si el proceso automatizado de actualización del programa antivirus en los servidores se efectuaba correctamente.

La situación comentada en el **Apartado c.** se debía a que el Gerente de Sistemas de Información no había preparado directrices específicas y detalladas para producir y preparar las copias de respaldo, y mantener las mismas en un lugar seguro fuera de los predios de la AEMEAD.

Véase la Recomendación 1.a.6), 15) y 16).

Hallazgo 7 - Deficiencias en los parámetros de seguridad de los servidores de la AEMEAD para controlar las cuentas de acceso a los recursos de la red

a. El examen realizado el 18 de julio de 2008 sobre los parámetros de control de acceso y de seguridad (*Account Policies*, *Password Policy* y *Account Lockout Policy*) definidos en el sistema operativo de dos servidores[22] de la AEMEAD, reveló las siguientes deficiencias:

1) En los dos servidores no se habían activado los siguientes parámetros para:

a) Requerir un mínimo de 10 días para que el sistema le permita al usuario cambiar la contraseña nuevamente (*Minimum Password Age*).

[22] Véase la nota al calce 21.

b) Requerir un mínimo de ocho caracteres en la contraseña de los usuarios. El mínimo de caracteres requeridos para la utilización de las contraseñas se había establecido a 0 (*Min password len: 0 chrs*).

c) Restringir el tiempo de acceso a la red para todas las cuentas conforme a las responsabilidades y las necesidades de servicios de cada usuario (*Do not force logoff when logon hours expire*). El sistema les permitía a los usuarios tener acceso las 24 horas y los 7 días de la semana.

d) Requerir un mínimo de cinco contraseñas diferentes antes de volver a utilizar la misma (*Enforce Password History*).

e) Requerir que las contraseñas fueran combinaciones de letras y números (*Password must meet complexity requirements*).

f) Definir un término fijo de intentos de acceso sin éxito a los recursos de la red para que el sistema deshabilitara automáticamente las cuentas de acceso (*Lockout after __ bad logon attempts*).

2) En los dos servidores no se había definido la política de auditoría (*Audit Policy*) para que el sistema produzca un registro cuando ocurran los siguientes eventos:

- El encendido y apagado de la computadora (*Restart and Shutdown*)
- El acceso a archivos y objetos (*File/Object Access*)
- Los cambios a las políticas de seguridad (*Security Policy Changes*)
- La administración de usuarios o grupos (*User/Group Management*)
- El acceso a los directorios de servicios (*Directory Service Access*).

3) La contraseña de cuenta de acceso con privilegios de administrador no se había cambiado en 884 días.

4) No se habían eliminado de los servidores cuatro cuentas de acceso[23] de ex empleados que cesaron sus funciones del 1 de enero de 2007 al 1 de agosto de 2008. A la fecha del examen dichas cuentas permanecían activas.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales deberán 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. También se establece que cada entidad gubernamental deberá establecer controles para el manejo de la terminación de empleados en la agencia, de tal 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. Esta norma se instrumenta, en parte, mediante lo siguiente:

- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos

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

- La notificación inmediata al encargado de la seguridad de los sistemas de información del cese de un usuario en sus funciones o de la modificación de las mismas para la acción correspondiente.

En la *Carta Circular Núm. OC-98-11* se establece, que para tener acceso al sistema, el usuario deberá registrar una contraseña (*password*), de por lo menos ocho caracteres, deberá ser una combinación de caracteres alfanuméricos (letras, números y símbolos) en cualquier proporción y arreglo y que sólo será de su conocimiento.

---

[23] Las cuentas de acceso se incluyeron en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

Las situaciones comentadas en el **Apartado a.1), 3) y 4)** propician que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de ésta. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en dichos sistemas sin que puedan ser detectados a tiempo para fijar responsabilidades.

La situación comentada en el **Apartado a.2)** impide a la AEMEAD mantener un registro de los eventos inusuales o problemas ocurridos en la red que le permitiera al Gerente de Sistemas de Información tomar a tiempo las medidas correctivas o preventivas necesarias.

Las situaciones comentadas en el **Apartado del a.1) al 3)** se debían a que el Gerente de Sistemas de Información no había puesto en vigor las opciones de seguridad de acceso lógico que provee el sistema operativo ni había establecido controles adecuados para el mantenimiento de las cuentas de acceso a la red.

La situación comentada en el **Apartado a.4)** se debe a que no existían procedimientos escritos que les requirieran a los empleados de la División de Recursos Humanos informarle al Gerente de Sistemas de Información el cese de un usuario en sus funciones por motivo de renuncia, separación o traslado para proceder con la cancelación de su cuenta de acceso.

Véase la Recomendación de la 1.a.17) a la 20) y c.

Hallazgo 8 - Equipos de comunicación sin uso

a. Del 22 al 25 de agosto de 2008, realizamos un inventario físico de los equipos de comunicación que se mantenían en el Área del Almacén de la AEMEAD y encontramos dos equipos de comunicación[24] que no se habían utilizado. Dichos equipos fueron

[24] La descripción de los equipos de comunicación se incluyó en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

adquiridos para proveer seguridad en la red entre la Zona de Gurabo y la Oficina Central de la AEMEAD mediante la Orden de Compra Núm. 0630440240 del 29 de septiembre de 2005 (Subasta Núm. 06-72-230-93) por $21,303.

En la *Ley Núm. 230* se establece como política pública que los gastos del gobierno se hagan dentro de un marco de utilidad y austeridad. En consonancia con ésta, las mejores prácticas en el campo de la tecnología sugieren que la gerencia de toda entidad gubernamental debe estudiar, planificar y supervisar adecuadamente la adquisición e instalación de los equipos para garantizar la inversión de fondos y la utilización eficaz de éstos.

Como consecuencia de la situación comentada, no se había obtenido un rendimiento razonable de la inversión de $21,303 realizada en la adquisición de dichos equipos. Además, los equipos que no se utilizaban pueden deteriorarse, dañarse o convertirse en obsoletos sin haberse obtenido rendimiento alguno de éstos.

La situación comentada se debió, en parte, a que los directores ejecutivos de la AEMEAD no habían dado las instrucciones para realizar la instalación del cableado necesario para utilizar los equipos mencionados.

Véase la Recomendación 1.a.21).

Hallazgo 9 - Falta de documentación de la justificación para la otorgación de privilegios de conexión remota y de configuración para controlar los accesos remotos

a. El examen efectuado a tres cuentas de acceso[25] que tenían privilegio de conexión remota reveló lo siguiente:

1) No le fueron suministrados a nuestros auditores los documentos justificantes para la otorgación del privilegio de conexión remota para las tres cuentas de acceso.

2) Dichas cuentas no se habían configurado para controlar los accesos remotos mediante procedimientos de *call back.*

[25] Los nombres de las cuentas de acceso se incluyeron en el borrador de los **hallazgos** del *Informe* remitido para comentarios al Director Ejecutivo y a la ex Directora Ejecutiva de la AEMEAD.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que, si existe la necesidad de acceder a la red interna desde afuera de las instalaciones de la entidad gubernamental (por ejemplo, para que un empleado realice un trabajo en un programa de aplicación desde Internet), deberán existir los controles de autenticación, confidencialidad, integridad y monitoreo necesarios para proteger los sistemas y la información. Esta norma se instrumenta, en parte, mediante:

- El uso de las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos

- El establecimiento de normas y procedimientos específicos para la asignación del privilegio de acceso remoto a los usuarios, donde se incluya, entre otras cosas, la justificación para la otorgación de dicho privilegio.

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

Las situaciones comentadas se debían, en parte, a que el Gerente de Sistemas de Información no había preparado ni remitido a la Directora Ejecutiva, para aprobación, los procedimientos para la asignación de privilegio de acceso remoto a los usuarios. Tampoco había puesto en vigor las opciones de seguridad que provee el sistema operativo para controlar los accesos remotos.

Véase la Recomendación 1.a.8)b) y 22).

Hallazgo 10 - Falta de adiestramientos periódicos al Gerente de Sistemas de Información

a. Al 17 de septiembre de 2008, el Gerente de Sistemas de Información, quien funge como Administrador de la Red, no recibía adiestramientos continuos sobre los temas relacionados con sus funciones, tales como:

- Programas para el diseño de la red
- Fundamentos de redes de comunicaciones
- Diseño, instalación y configuración del cableado
- Instalación y configuración de equipos de telecomunicaciones (*router* y *hub*, entre otros)
- Problemas (*trouble shooting*) en la red, servidores y estaciones de trabajo
- Seguridad y confidencialidad de la información, y de las leyes de derechos de autor de los programas computadorizados.

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

- La agencia es responsable de proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.
- El personal de sistemas de información y telecomunicaciones deberá estar adiestrado y con conocimiento actualizado sobre los aspectos de seguridad de sus áreas.
- La agencia es responsable de crear mecanismos de capacitación para que todos los empleados conozcan los procedimientos de seguridad que le apliquen.

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

La situación comentada se debe a que el Director del Área de Administración no había identificado las necesidades de adiestramiento sobre el uso y la seguridad de los sistemas de información del Gerente de Sistemas de Información a los fines de informar al Director de la División de Recursos Humanos para que éste planifique y desarrolle un plan de adiestramiento.

Véase la Recomendación 1.d.

ANEJO

AGENCIA ESTATAL PARA EL MANEJO DE EMERGENCIAS
Y ADMINISTRACIÓN DE DESASTRE DE PUERTO RICO

CENTRO DE SISTEMAS DE INFORMACIÓN

FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO

		PERÍODO	
NOMBRE	**CARGO O PUESTO**	**DESDE**	**HASTA**
Sra. Karilyn Bonilla Colón	Directora Ejecutiva	17 mar. 08	28 oct. 08
Sr. Xavier González Calderón	Subdirector Ejecutivo[26]	1 ag. 08	28 oct. 08
Sr. Carlos D. Salgado Calzada	Director del Área de Administración	16 jul. 08	28 oct. 08
Sr. Emanuel Cantres Carmona	"	17 mar. 08	15 jun. 08
Sr. Frank R. Vázquez Madera	Director de Finanzas	1 ag. 08	28 oct. 08
Sra. Nydia Rivera Rivera	Directora de Finanzas	17 mar. 08	15 jun. 08
Sr. Emanuel Cantres Carmona	Director de la División de Recursos Humanos	18 jul. 08	28 oct. 08
Sr. Carlos D. Salgado Calzada	"	17 mar. 08	16 jul. 08
Sr. Luis O. Cruz Ramírez	Supervisor de la División de Servicios Generales	17 mar. 08	28 oct. 08
Sr. Marco Rodríguez Vázquez	Oficial Ejecutivo I[27]	17 mar. 08	28 oct. 08
Sr. Tomás Cabrera Ramírez	Gerente de Sistemas de Información	16 abr. 08	28 oct. 08

[26] Este puesto estuvo vacante desde el 17 de marzo hasta el 31 de julio de 2008.

[27] Este funcionario realizó las funciones del Director del CSI durante el período auditado.