

Madeline De



Secretaria

- Ver al dorso
- Para su información
- Notas
- Para mantenerle al día
- 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

W: www.senadopr.us

REFERIDO A:

COMISIONES PERMANENTES

- Hacienda
- Gobierno
- Seguridad Pública y Judicatura
- Salud
- Educación y Asuntos de la Familia
- Desarrollo Económico 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 Rico
- 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 Leves

15499

INFORME DE AUDITORÍA TI-12-09

19 de marzo de 2012

Comisión para la Seguridad en el Tránsito

Sistemas de Información Computadorizados

(Unidad 5198 - Auditoría 13358)

Período auditado: 9 de septiembre de 2009 al 30 de abril de 2010

CONTENIDO

Página

INFORMACIÓN SOBRE LA UNIDAD AUDITADA.....	3
RESPONSABILIDAD DE LA GERENCIA.....	6
ALCANCE Y METODOLOGÍA.....	6
OPINIÓN.....	7
INFORME DE AUDITORÍA ANTERIOR.....	7
RECOMENDACIONES.....	8
AL SECRETARIO DE TRANSPORTACIÓN Y OBRAS PÚBLICAS Y PRESIDENTE DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO.....	8
AL DIRECTOR EJECUTIVO DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO.....	8
CARTAS A LA GERENCIA.....	12
COMENTARIOS DE LA GERENCIA.....	12
AGRADECIMIENTO.....	13
RELACIÓN DETALLADA DE HALLAZGOS.....	14
CLASIFICACIÓN Y CONTENIDO DE UN HALLAZGO.....	14
HALLAZGOS EN LOS SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO.....	15
1 - Uso de los servicios de Internet para fines ajenos a la gestión pública, y falta de controles de los mensajes de correo electrónico recibidos y enviados de fuentes externas a la Comisión.....	15
2 - Falta de un informe de avalúo de riesgos sobre los sistemas de información computadorizados.....	19
3 - Falta de un plan de seguridad y de un plan de manejo de incidentes.....	21

4 - Falta de un Plan de Continuidad de Negocios, deficiencias relacionadas con el Plan de Respuestas de Emergencias y de Recuperación, y falta de acuerdos escritos para mantener un centro altemo de recuperación de sistemas de información	23
5 - Deficiencias relacionadas con los parámetros de seguridad y con los controles de acceso lógico de los servidores de la red, y falta de un formulario para la solicitud, la aprobación, la creación y la cancelación de las cuentas para acceder al correo electrónico y a Internet.....	27
6 - Deficiencias relacionadas con la seguridad y el acceso físico al cuarto de servidores, y falta de documentación de la configuración de los servidores y del diagrama esquemático de la red	30
7 - Deficiencias relacionadas con la preparación y el almacenamiento de los respaldos de los archivos computadorizados de información	32
8 - Deficiencias relacionadas con el Inventario de Equipo Computadorizado y el control del equipo, y falta de un registro de los programas instalados en la red y en las computadoras de la Comisión	35
ANEJO - FUNCIONARIOS PRINCIPALES QUE ACTUARON DURANTE EL PERÍODO AUDITADO	38

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

19 de marzo de 2012

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

Realizamos una auditoría de las operaciones de los Sistemas de Información Computadorizados de la Comisión para la Seguridad en el Tránsito (Comisión) 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

En la *Ley Núm. 33 del 25 de mayo de 1972*, según enmendada, se faculta al Gobernador para establecer un programa de prevención de accidentes de tránsito. Además, lo faculta para concertar y tramitar los convenios necesarios para que el Estado pueda recibir los fondos y los beneficios que correspondan bajo las disposiciones de la *Ley Pública del Congreso Núm. 89-564 del 1966*, actualmente conocida como *Highway Safety Act for 21st Century (Ley Pública)*.

Bajo la disposición de la *Ley Núm. 33* se creó un comité de coordinación conocido como la Comisión para la Seguridad en el Tránsito. En dicha *Ley* se dispone que la Comisión es presidida por el Gobernador o la persona en quien él delegue. La Comisión está compuesta

por 13 miembros de los cuales 11 son funcionarios de la Rama Ejecutiva¹, 1 es representante del interés público y el otro es representante de la juventud². El Gobernador delegó en el Secretario de Transportación y Obras Públicas para que actúe como Presidente de la Comisión. La *Ley Núm. 33* faculta a la Comisión para nombrar un Director Ejecutivo y todo el personal necesario para sus operaciones y el cumplimiento de los objetivos. Además, la faculta para adoptar, promulgar y enmendar las reglas y los reglamentos necesarios para cumplir con las disposiciones de esta *Ley*, en asuntos que no estén en conflicto con otras leyes ni con la autoridad concedida por ley a otras agencias.

La Comisión tiene a su cargo la planificación, la coordinación, la administración y la divulgación del programa de prevención de choques de tránsito a nivel estatal. A su vez, tramita y administra los fondos y los beneficios federales bajo la *Ley Pública*. La Comisión está autorizada a utilizar recursos de las agencias y de las corporaciones públicas que se integran a la misma para realizar sus programas de seguridad en el tránsito. Dichas agencias y corporaciones, particularmente la Administración de Compensaciones por Accidentes de Automóviles (ACCAA), fueron autorizadas para poner recursos a la disposición de la Comisión.

La ACCAA asigna y provee a la Comisión los fondos para parte de sus gastos de funcionamiento y queda facultada para solicitar y aceptar la cooperación financiera, a esos fines, de cualquier otro programa o institución interesada. Los fondos que la ACCAA asigna a la Comisión, así como los fondos que aporte el Gobierno Federal, permanecen bajo su custodia en una partida independiente creada para ese propósito. Los desembolsos los efectúa la ACCAA, previa certificación de la Comisión y con cargo a dicha partida.

¹ Los funcionarios miembros de la Comisión son el Gobernador, los secretarios de Justicia, de Transportación y Obras Públicas, de Educación y de Salud, la Administradora de la Administración de Servicios de Salud Mental y Contra la Adicción, el Superintendente de la Policía, el Director Ejecutivo de la Autoridad de Carreteras y Transportación, la Directora Administrativa de los Tribunales, el Director Ejecutivo de la ACCAA y el Presidente de la Comisión de Servicio Público.

² Al 30 de abril de 2010, no se había nombrado al representante de la juventud.

Para llevar a cabo sus funciones, la Comisión cuenta con la siguiente estructura organizacional: Oficina del Director Ejecutivo³, Oficina del Director Auxiliar de Operaciones, Oficina del Director Auxiliar de Administración, y Oficina del Auditor Interno. Además, existe una Oficina de Relaciones Públicas que está a cargo de la Oficial de Comunicaciones y Relaciones Públicas.

La Comisión tiene un cuarto donde se ubican sus seis servidores. A la fecha de nuestra auditoría, la Comisión no contaba con personal para administrar sus servidores, por lo que mantenía un contrato con una compañía (Compañía A) para obtener asesoría en el área de sistemas de información. La Compañía A ofrecía apoyo técnico a los usuarios y mantenimiento a los servidores y a la red, y realizaba los procesos de respaldos a la información. Las tareas realizadas por la Compañía A eran supervisadas por el Director Auxiliar de Operaciones.

La Comisión no cuenta con una estructura fiscal independiente, ya que sus desembolsos se realizan a través de la Oficina de Finanzas de la ACAA. Durante los años fiscales del 2007-08 al 2009-10, la Comisión recibió asignaciones de la ACAA y fondos federales, por \$34,655,000, según se indica a continuación:

AÑO FISCAL	ASIGNACIONES ACAA	FONDOS FEDERALES	TOTAL
2007-08	\$1,304,000	\$10,677,000	\$11,981,000
2008-09	1,285,000	11,190,000	12,475,000
2009-10	<u>1,386,000</u>	<u>8,813,000</u>	<u>10,199,000</u>
TOTAL	<u>\$3,975,000</u>	<u>\$30,680,000</u>	<u>\$34,655,000</u>

El ANEJO contiene una relación de los funcionarios principales de la Comisión que actuaron durante el periodo auditado.

La Comisión cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: <http://www.comisionparalaseguridadeneltransito.com>. Esta página provee información acerca de la entidad y de los servicios que presta.

³ Durante el periodo de nuestra auditoría, el puesto del Director Ejecutivo lo ocupaba un funcionario en destaque de la Autoridad de Carreteras y Transportación.

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 9 de septiembre de 2009 al 30 de abril de 2010. En algunos aspectos examinamos transacciones de fechas anteriores. El examen lo efectuamos de acuerdo

con las normas de auditoría del Contralor de Puerto Rico en lo que concierne a los sistemas de información computadorizados. Realizamos las pruebas que consideramos necesarias, a base de muestras y de acuerdo con las circunstancias.

Para efectuar la auditoría utilizamos la siguiente metodología:

- entrevistas a funcionarios, a empleados y a particulares
- inspecciones físicas
- examen y análisis de informes y de documentos generados por la unidad auditada
- 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 los Sistemas de Información Computadorizados de la Comisión, en lo que concierne a los controles internos relacionados con la administración del programa de seguridad, la evaluación de la continuidad del servicio, y el control de acceso lógico y físico a los sistemas de información computadorizados, no se realizaron conforme a las normas generalmente aceptadas en este campo.

Los **hallazgos del 1 al 8**, 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 4-b., y 8-a.3)** y **b.** de este *Informe* fueron objeto de recomendaciones en el *Informe de Auditoría CPED-95-13* del 30 de junio de 1995. Estas no fueron atendidas.

RECOMENDACIONES

AL SECRETARIO DE TRANSPORTACIÓN Y OBRAS PÚBLICAS Y PRESIDENTE DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO

1. Ver que el Director Ejecutivo de la Comisión cumpla con las **recomendaciones de la 2 a la 7 de este Informe. [Hallazgos del 1 al 8]**

AL DIRECTOR EJECUTIVO DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO

2. Asegurarse de que se realice un análisis para determinar las páginas electrónicas que son necesarias, según los deberes y las responsabilidades del personal autorizado, para acceder a Internet. Luego de efectuado el análisis, remitir la lista de las páginas autorizadas al Director Auxiliar de Operaciones. **[Hallazgo 1-a.]**
3. Asegurarse de que se realice un análisis para determinar el personal clave de la Comisión que requiera tener privilegios para enviar y recibir mensajes de correo electrónico de fuentes externas. Luego de efectuado el análisis, remitir la lista del personal clave al Director Auxiliar de Operaciones. **[Hallazgo 1-b.]**
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, Equipo 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 que se sugiere en las mejores prácticas en el campo de la tecnología. Además, que se incluyan en el avalúo de riesgos los elementos mencionados en el **Hallazgo 2**, y que el informe producto de este análisis de riesgos se remita para su revisión y aprobación.

5. Ejercer una supervisión eficaz sobre el Director Auxiliar de Operaciones para que se asegure de que:
 - a. Oriente a los funcionarios y a los empleados de la Comisión sobre las leyes, las normas y los procedimientos que reglamentan el uso y el manejo de las cuentas para acceder a Internet y al correo electrónico y conserve evidencia de dicha orientación. **[Hallazgo 1]**
 - b. Realice inspecciones periódicas para asegurarse de que los usuarios cumplan con las normas establecidas sobre el uso del correo electrónico e Internet. **[Hallazgo 1]**
 - c. Se limite el acceso a Internet para que el personal autorizado solo pueda acceder las páginas electrónicas que son necesarias para cumplir con sus deberes y responsabilidades, según el análisis realizado por la gerencia. **[Hallazgo 1-a.]**
 - d. Se restrinjan los derechos y los privilegios para que solamente el personal clave de la Comisión pueda enviar y recibir mensajes de correo electrónico de fuentes externas, según el análisis realizado por la gerencia. **[Hallazgo 1-b.]**
 - e. Se prepare y se remita para aprobación:
 - 1) El plan de seguridad en el que se establezcan los proyectos, las tareas y las actividades, requeridos para proteger al personal y a los activos del sistema de información. **[Hallazgo 3-a.]**
 - 2) El procedimiento para el manejo de incidentes no esperados. Como parte del procedimiento, se debe requerir que se documenten todos los incidentes y cómo se resolvieron, de manera que cuando estos se repitan, se puedan resolver en el menor tiempo posible, sin afectar los sistemas de información y la continuidad de las operaciones. **[Hallazgo 3-b.]**
- 3) El *Plan de Continuidad de Negocios*, que incluya un *Plan para la Recuperación de Desastres* y un *Plan para la Continuidad de las Operaciones*. Una vez este

- sea aprobado, tomar las medidas necesarias para asegurarse de que el mismo se mantenga actualizado y se conserve copia en un lugar seguro fuera de los predios de la Comisión. Además, asegurarse de que sea distribuido a los funcionarios y a los empleados concernientes, y de que se realicen pruebas periódicas para garantizar la efectividad del mismo. **[Hallazgo 4-a.]**
- f. Se revise y se actualice el *Procedimiento Núm. CST-P-10, Plan de Respuestas de Emergencias y de Recuperación* aprobado el 28 de diciembre de 2007 por el Director Ejecutivo, considerando los aspectos comentados en el **Hallazgo 4-b.1), 2) y 4)**, y lo remita para su aprobación. Una vez aprobado, asegurarse de que se distribuya al personal que llevará a cabo los procesos del mismo y de que se mantenga copia en un lugar seguro fuera de las instalaciones de la Comisión.
- g. Se efectúen pruebas o simulacros para certificar la efectividad del *Plan de Respuestas de Emergencias y de Recuperación*, y mantenga la documentación de las estrategias utilizadas y los resultados de las pruebas. **[Hallazgo 4-b.3)]**
- h. Se efectúen las modificaciones en los parámetros de seguridad de los servidores de la red para:
- 1) 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 estas son utilizadas para acceder los recursos de la red fuera de horas laborables. **[Hallazgo 5-a.1)a)]**
 - 2) Desconectar automáticamente las cuentas de acceso de aquellos usuarios que realizan tres intentos sin éxito para acceder los recursos de la red. **[Hallazgo 5-a.1)b)]**
 - 3) Establecer un mínimo de ocho caracteres para la utilización de las contraseñas. **[Hallazgo 5-a.1)c)]**

- 4) Activar las opciones correspondientes en la pantalla de políticas de auditoría (*Audit Policies*) que se mencionan en el **Hallazgo 5-a.2)**, de manera que se pueda mantener un rastro de las actividades realizadas en los servidores de la Comisión.
 - i. Se prepare y se remita para aprobación un procedimiento para la creación, el mantenimiento y el control de las cuentas de acceso a la red y a Internet. En este se debe establecer la utilización de un formulario para la solicitud, la aprobación, la creación y la cancelación de las cuentas de acceso de los usuarios. [**Hallazgo 5-b.1**]
 - j. Se desarrollen y se implanten las medidas de control necesarias para corregir las situaciones comentadas en el **Hallazgo 6-a.**, y se asegure de que estas se incluyan en el *Plan de Seguridad*.
 - k. Se prepare un diagrama esquemático de la red y se documente la configuración de los servidores y de la red de comunicaciones. [**Hallazgo 6-b.1**]
 - l. Se mantenga un registro de los respaldos preparados y de los entregados a la Compañía B que permita controlar y proteger los mismos. [**Hallazgo 7-a.1) y 2)**]
 - m. Se envíen mensualmente las cintas de los respaldos a la bóveda externa. [**Hallazgo 7-a.3) y b.1)**]
 - n. Se obtenga una llave de acceso a la bóveda externa donde se guardan las cintas de los respaldos. [**Hallazgo 7-b.2)**]
6. Formalizar un acuerdo escrito con un centro externo que acepte la utilización de sus equipos en caso de desastres o emergencias en la Comisión, y que no esté expuesto a los mismos riesgos que el lugar donde se encuentra el cuarto de servidores. El centro externo podría ser en un lugar como el Parque Educativo para la Seguridad en el Tránsito en Arecibo o en una de las agencias que forman parte de la Comisión y que no se encuentre en el Centro Gubernamental de Minillas. [**Hallazgo 4-c.1**]

7. Ejercer una supervisión eficaz sobre la persona encargada de la propiedad para asegurarse de que:
- a. 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 8-a.**]
 - b. Se guarde la documentación de toda compra o adquisición de equipos computadorizados, se mantenga un registro de estos equipos y se corrijan las situaciones mencionadas. [**Hallazgo 8-a. y b.**]
 - c. Mantenga un registro de los programas adquiridos por la Comisión, que contenga, entre otros datos, el número de la licencia y el costo de los programas instalados en las computadoras y en la red. Esto, con el fin de mantener un inventario de los mismos y detectar la instalación de programas no autorizados. [**Hallazgo 8-c.**]

CARTAS A LA GERENCIA

Las situaciones comentadas en los **hallazgos del 2 al 8**, incluidos en la parte de este *Informe* titulada **RELACIÓN DETALLADA DE HALLAZGOS**, se informaron al Sr. Miguel A. Santini Padilla, Director Ejecutivo, por carta de nuestros auditores del 30 de abril de 2010.

El borrador de los **hallazgos** de este *Informe* se remitió al Director Ejecutivo, para comentarios, por carta del 31 de marzo de 2011.

COMENTARIOS DE LA GERENCIA

Mediante carta del 6 de mayo de 2010, el Director Ejecutivo, remitió sus comentarios sobre los **hallazgos** incluidos en la carta de nuestros auditores. Sus observaciones fueron consideradas en la redacción del borrador del *Informe*.

El Director Ejecutivo contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 14 de abril de 2011. En esta nos indicó que se sostiene en los comentarios previamente emitidos, en la contestación a la carta de nuestros auditores, y que se presentarán las medidas tomadas para corregir los **hallazgos** de este *Informe*, mediante el *Plan de Acción Correctiva*, una vez reciba el informe final.

AGRADECIMIENTO

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

Por:
Agencia del Contralor
Samir M. Velazquez

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 LOS SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO,**

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 LOS SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS DE LA COMISIÓN PARA LA SEGURIDAD EN EL TRÁNSITO

Hallazgo 1 - Uso de los servicios de Internet para fines ajenos a la gestión pública, y falta de controles de los mensajes de correo electrónico recibidos y enviados de fuentes externas a la Comisión

- a. La Comisión mantenía un servidor⁴ que permitía acceso a Internet a los usuarios autorizados. El examen del registro de direcciones de Internet visitadas por los usuarios de la Comisión del 26 de febrero al 4 de marzo de 2010, reveló que en dicho periodo se había utilizado este servicio para acceder 250 páginas en Internet. De estas, 239 (96 por ciento) eran páginas con contenido ajeno a la gestión pública⁵. No se pudieron determinar las cuentas de acceso de los usuarios que visitaron las mismas porque el servidor no estaba debidamente configurado para que se registrara el nombre del usuario que accedía a las páginas en Internet.
- b. La Comisión mantenía un servidor⁴ en la red que permitía a los empleados el envío y el recibo de mensajes de correo electrónico. Dicho servidor producía diariamente un archivo en el cual se registraban todos los mensajes enviados y recibidos por las cuentas de usuarios (*message tracking logs*). El examen del registro del correo electrónico del 26 de febrero de 2010 reveló que los usuarios podían recibir y enviar mensajes de correo electrónico de fuentes externas a la Comisión sin ningún tipo de restricción.

⁴ El nombre del servidor se incluyó en el borrador de los hallazgos de este *Informe* remitido al Director Ejecutivo para comentarios.

⁵ Una relación de las páginas se incluyó en el borrador de los hallazgos de este *Informe* remitido al Director Ejecutivo para comentarios.

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

En el Artículo 3.2(c) de la *Ley Núm. 12* 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. CST-POL-02, Política sobre el Uso de Sistemas de Información, de la Internet y Correos Electrónicos*, aprobada el 25 de junio de 2007 por el Director Ejecutivo, se establece que:

- Los sistemas de comunicación y acceso a Internet deberán ser utilizados exclusivamente como herramienta de trabajo conforme a las normas que rigen el comportamiento personal de la entidad y nunca con fines no oficiales o personales o con fines de lucro.
- El correo electrónico podrá utilizarse únicamente para propósitos relativos a las funciones de la Comisión. Se prohíbe el uso de asuntos no oficiales o actividades personales con fines de lucro. No deberán utilizarse para uso personal; ni para transmitir, acceder o almacenar comunicados que sean discriminatorias, ofensivos, profanos, obscenos, o que vayan en contra de las buenas costumbres o de las leyes.
- Durante horas laborables, los usuarios no podrán utilizar o acceder a cuentas de correo electrónico distintas a las cuentas oficiales de la Comisión, a menos que estén autorizados por escrito a tal uso.

En la *Norma Núm. CST-N-01, Normas sobre el Uso de Sistemas Electrónicos*, aprobada el 28 de diciembre de 2007 por el Director Ejecutivo, se establece, entre otras cosas, que:

- El sistema de correspondencia interna (*e-mail*) y la Internet solo podrán utilizarse para propósitos lícitos, prudentes, responsables y dentro de las funciones y los poderes de la Comisión.
- Los mensajes de correspondencia electrónica (*e-mail*) y la Internet no podrán utilizarse para fines ajenos a las funciones y los poderes de la Comisión.
- Se prohíbe el uso de los sistemas de computadoras y comunicaciones de la Comisión para propósitos personales, de recreo, para manejo de un negocio o asunto privado del usuario o para la utilización y el envío de mensajes de cadena. De igual forma, el usuario no podrá utilizar los recursos electrónicos de la Comisión para tener acceso a compras, juegos, concursos, encuestas, páginas de entretenimiento, o cualquier otro servicio ajeno a las funciones de la Comisión.
- Se prohíbe que los usuarios utilicen durante horas laborables cuentas de correo electrónico distintas a las cuentas oficiales provistas por la agencia.

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

Por otro lado, el acceso a páginas en Internet ajenas al fin público expone a los equipos y a la información sensible almacenada en los sistemas, a riesgos innecesarios como son la

propagación de virus, *spyware*⁶, *phishing*⁷, *spoofing*⁸, *spamming*⁹ y ataques de negación de servicios¹⁰, entre otros, que pudieran afectar la continuidad de las operaciones de la Comisión.

Las situaciones comentadas se debían, en parte, a la falta de:

- Orientaciones periódicas a los usuarios de los sistemas de información computarizados sobre las leyes, las normas y los procedimientos que reglamentan el uso y el manejo de las cuentas para acceder a Internet y al correo electrónico
- Inspecciones periódicas como elemento disuasivo y preventivo para verificar el cumplimiento de las normas establecidas para el uso oficial de los equipos computarizados y de las cuentas para acceder a Internet
- Análisis para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado a acceder a Internet
- Análisis para determinar los funcionarios y los empleados a quienes debían otorgarse los privilegios para recibir y enviar mensajes de correo electrónico de fuentes externas, de acuerdo con las necesidades de la Comisión, y con los deberes y las responsabilidades de sus puestos.

⁶ Es un 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.

⁷ Es un tipo de ataque de correo electrónico que trata de convencer a un usuario de que el originador es auténtico, pero con la intención de obtener información.

⁸ Es un ataque activo en el que el intruso presenta una identidad que no es la identidad original. En este ataque, el propósito es obtener acceso a los datos sensibles o a los recursos de los sistemas de información computarizados a los que no se permite el acceso bajo la identidad original.

⁹ Es el envío de correspondencia electrónica a cientos o a miles de usuarios.

¹⁰ Ocurren cuando una computadora conectada a Internet es inundada con datos y solicitudes que deben ser atendidas. La computadora se dedica exclusivamente a atender estos mensajes y queda imposibilitada de realizar otras actividades.

Hallazgo 2 - Falta de un informe de avalúo de riesgos sobre 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 poder alcanzar y cumplir con los objetivos de la entidad gubernamental. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas, pertinentes a las operaciones de la entidad gubernamental y respondan a las posibles amenazas identificadas. El avalúo de riesgos tiene cuatro objetivos:

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

Al 25 de febrero de 2010, en la Comisión no se había preparado por escrito, un informe de avalúo de riesgos sobre los sistemas de información.

Una situación similar fue comentada en el *Informe C-08-001* del 10 de marzo de 2008, emitido por la Oficina de Auditoría Interna de la Comisión.

En la *Política Num. TIG-003 de la Carta Circular Num. 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 los 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 datos, entre otros), junto con un análisis del impacto en las operaciones y la probabilidad de que ocurran esas amenazas. Esto permitirá establecer cómo se van a proteger los activos identificados anteriormente.

La situación comentada impidió a la Comisión estimar el impacto que los elementos de riesgos tendrían sobre las áreas y los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y de pérdida de información. Además, dificulta desarrollar 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 Comisión, en caso de que surja alguna eventualidad. [Véase el Hallazgo 4-a.]

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

Hallazgo 3 - Falta de un plan de seguridad y de un plan de manejo de incidentes

- a. Al 9 de marzo de 2010, la Comisión no tenía un plan de seguridad aprobado por el Director Ejecutivo que incluyera, entre otras cosas, disposiciones en cuanto a:
- La documentación de la validación de las normas de seguridad¹¹
 - La evidencia de un análisis de riesgos actualizado, como base del *Plan*
 - 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, contratistas y usuarios, y que permita mantener los conocimientos actualizados
 - La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros)
 - La documentación de la interconexión de los sistemas.
- Una situación similar fue comentada en el *Informe C-08-001*.
- En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas de misión crítica. También se establece que las entidades gubernamentales son responsables de:
- Proveer adiestramientos a toda la gerencia y a los supervisores de la agencia para que estén al tanto de los controles de seguridad y los beneficios correspondientes.

¹¹ La validación de las normas de seguridad se efectúan mediante la prueba de los controles para eliminar o mitigar las amenazas y las vulnerabilidades detectadas en el avaiño de riesgos. Además, se valida mediante los resultados de los simulacros efectuados para probar la efectividad del plan de seguridad.

- Proveer adiestramientos al personal de sistemas de información y telecomunicaciones para que se actualicen los conocimientos 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.

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

- b. Al 21 de abril de 2010, la Comisión no tenía un procedimiento o plan para el manejo de incidentes que estableciera, entre otras cosas, una estrategia documentada para el manejo de los incidentes, un equipo de respuesta y la documentación de las actividades relacionadas con los mismos.

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

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

Las situaciones comentadas se atribuyen a que el Director Ejecutivo no había promulgado una directriz para:

- La preparación de un *Plan de Seguridad*, basado en un avalúo de riesgos de los sistemas de información, y para la implantación y la actualización continua del mismo, según se establece en la *Carta Circular Num. 77-05*. [Apartado a.]
- El desarrollo y la aprobación de normas y de procedimientos escritos para el manejo de incidentes. [Apartado b.]

Hallazgo 4 - Falta de un Plan de Continuidad de Negocios, deficiencias relacionadas con el Plan de Respuestas de Emergencias y de Recuperación, y falta de acuerdos escritos para mantener un centro alternativo de recuperación de sistemas de información

a. Al 21 de abril de 2010, la Comisión carecía de un *Plan de Continuidad de Negocios* que incluyera los planes específicos, completos y actualizados de la misma. Esto era necesario para lograr un pronto funcionamiento de los sistemas de información computarizados y restaurar las operaciones de la Comisión en caso de riesgos como: variaciones de voltaje, virus de computadoras, ataques maliciosos a la red, desastres naturales, entre otros.

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

b. El *Plan de Respuestas de Emergencias y de Recuperación (Plan)* tiene como propósito establecer una guía eficaz a seguir para tener y mantener un *Plan de Emergencia* para los sistemas que se encuentran en sus servidores. El examen realizado el 8 de abril de 2010, reveló las siguientes deficiencias:

- 1) El *Plan* no incluía los siguientes requisitos que son necesarios para atender situaciones de emergencia:
 - Identificación de los procesos y archivos críticos de la Comisión

- Una asignación clara de responsabilidades para la recuperación
 - Identificación de los recursos que darán apoyo a las operaciones críticas de la Comisión en caso de emergencia
 - Personal de reserva de forma tal que el *Plan* pueda ser ejecutado sin depender de individuos específicos
 - Los procedimientos a seguir cuando el cuarto de servidores no puede recibir ni transmitir información
 - Inventario de equipos, sistemas operativos, de aplicaciones y archivos críticos de la Comisión
 - Itinerario de restauración que incluya los procedimientos para restaurar los respaldos.
- 2) El *Plan* no estaba actualizado. En el mismo se hacía referencia al puesto de Oficial Principal de Informática que ya no existía en la Comisión y a la aplicación FASGOV que ya no se utilizaba.
- 3) La Comisión no había realizado pruebas o simulacros que certificaran la efectividad del *Plan*. Además, no había realizado las pruebas semestrales de recuperación de cintas de respaldos para asegurarse de que el proceso de respaldo estaba funcionando correctamente.
- 4) Se desconocía si se mantenía una copia del *Plan* fuera de las instalaciones de la Comisión.

Situaciones similares a las indicadas en el **apartado b.** fueron comentadas en el informe de auditoría anterior *CPEP-95-13*, y en el *Informe C-08-001*.

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

Las situaciones comentadas podrían propiciar la improvisación y que, en casos de emergencia, se tomen medidas inapropiadas y sin orden alguno. Esto representa un alto riesgo de incurrir en gastos excesivos e innecesarios de recursos e interrupciones prolongadas de los servicios a los usuarios y clientes de la Comisión.

Las situaciones comentadas se atribuyen a que el Director Ejecutivo no había promulgado una directriz para:

- La preparación de un informe de avalúo de riesgos sobre los sistemas de información que sirviera de base para el desarrollo, la aprobación y la implantación de un *Plan de Continuidad de Negocios*. Este debe contener un *Plan para la Continuidad de las Operaciones* y un *Plan para la Recuperación de Desastres*, con el fin de que sirvan como herramientas para responder ante cualquier incidente o desastre que ocurra.

[Apartado a.]

- La preparación e implantación de un *Plan de Contingencias* para la Comisión con el propósito de garantizar la continuidad de las operaciones en caso de surgir algún desastre o emergencia. **[Apartado b.]**

- c. Al 25 de febrero de 2010, la Comisión no contaba con un centro alternativo de los sistemas de información para restaurar las operaciones críticas computarizadas en casos de emergencia. Tampoco había formalizado acuerdos con otra entidad para establecer un centro alternativo en las instalaciones de esta.

Las mejores prácticas en el campo de la tecnología de información sugieren que, como parte integral del *Plan de Continuidad de Negocio*, deben existir convenios con otras entidades donde se estipulen las necesidades y los servicios requeridos para afrontar una emergencia. Debe incluirse, además, una cláusula que especifique el lugar o los lugares donde podrían ser requeridos dichos servicios. Estos lugares, de acuerdo con la capacidad de la agencia, podrían ser los siguientes:

- Una entidad pública o privada de similar configuración y tamaño
- Una compañía dedicada a servicios de restauración
- Un centro alternativo de la propia entidad.

La situación comentada podría afectar las funciones de la Comisión, ya que no tendrían disponibles unas instalaciones para operar después de una emergencia o de un evento que afectara su funcionamiento. Esto podría atrasar o impedir el proceso de restauración de archivos y el pronto restablecimiento de las operaciones de la Comisión.

La situación comentada se atribuye a que el Director Auxiliar de Operaciones no había coordinado la identificación de un lugar disponible y adecuado como centro alternativo, de manera que el Director Ejecutivo pudiera formalizar los acuerdos escritos necesarios para la utilización del mismo en casos de emergencia.

Hallazgo 5 - Deficiencias relacionadas con los parámetros de seguridad y con los controles de acceso lógico de los servidores de la red, y falta de un formulario para la solicitud, la aprobación, la creación y la cancelación de las cuentas para acceder al correo electrónico y a Internet

a. La Comisión tenía seis servidores¹² en los cuales se procesaban las transacciones de contabilidad y de nómina, mediante el sistema MIP, y las de correo electrónico e Internet. El examen efectuado el 25 de marzo de 2010 sobre los parámetros de seguridad y control de acceso definidos en el sistema operativo de estos seis servidores, reveló las siguientes deficiencias:

- 1) En los seis servidores no se habían activado los siguientes parámetros, relacionados con las cuentas de acceso (*Account Policies*), para:
 - a) Restringir el tiempo de acceso a la red para todas las cuentas de acceso de acuerdo con las funciones de cada usuario (*Do not force logoff when logon hours expire*). El sistema les permitía a los usuarios tener acceso los 7 días de la semana y las 24 horas.
 - b) Definir un término fijo de intentos de acceso sin éxito a los recursos de la red para que el sistema inhabilitara automáticamente las cuentas de acceso de los usuarios (*No account lockout*).
 - c) Requerir, al menos, un mínimo de ocho caracteres para la utilización de las contraseñas. El mínimo de caracteres requeridos para la utilización de las contraseñas se había establecido a siete (*Minimum password length*).

¹² Véase la nota al calce 4.

2) Identificamos las siguientes deficiencias en la definición de los parámetros relacionados con las políticas de auditoría (*Audit Policies*):

- a) En cinco servidores¹³ no se habían activado las opciones correspondientes al encendido y apagado de la computadora (*Restart and Shutdown*).
- b) En un servidor¹³ no se había activado la opción correspondiente a la apertura y al cierre de sesión (*Logon and Logoff*).

b. La Comisión no había establecido un formulario para la solicitud, la aprobación, la creación, la modificación y la cancelación de las cuentas para acceder al correo electrónico y a Internet, ni documentaba por escrito estas solicitudes.

En la *Política Num. TIG-003 de la Carta Circular Num. 77-05*, se establece lo siguiente:

- 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.
- La información y los programas de aplicación utilizados en las operaciones de la entidad gubernamental deberán tener controles de acceso para su utilización, de tal manera que solamente el personal autorizado pueda ver los datos que necesita, o usar las aplicaciones (o parte de las aplicaciones) que necesita utilizar. Estos controles deberán incluir mecanismos de autenticación y autorización.
- Los privilegios de acceso de los usuarios deberán ser reevaluados regularmente.

¹³ Véase la nota al calce 4.

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

- El uso de las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos.
- La limitación del tiempo de acceso para todas las cuentas de acceso de acuerdo con las funciones de cada usuario.
- El establecimiento de controles de acceso rigurosos a la red, a los programas y a los archivos, incluido el uso de formularios para solicitar la creación, la modificación o la eliminación de cuentas de acceso para cada usuario.
- El mantenimiento de registros confiables y actualizados de las cuentas solicitadas y autorizadas.

Las situaciones comentadas en el **apartado a.** propician que personas no autorizadas puedan lograr acceso a información confidencial y hacer uso indebido de esta.

La situación comentada en el **apartado b.** impide mantener la evidencia requerida para otorgar o cancelar los accesos y los privilegios a los usuarios. Esto puede dificultar que se fijen responsabilidades por el uso indebido de los sistemas computarizados. Además, puede afectar la integridad de la información registrada en estos.

Las situaciones comentadas en el **apartado a.** se debían, en parte, a que el Director Auxiliar de Operaciones no veló por que la Compañía A, pusiera en vigor las opciones de seguridad de acceso lógico que proveen los sistemas operativos, y estableciera controles adecuados para las cuentas de acceso a la red.

La situación comentada en el **apartado b.** se debía a que el Director Ejecutivo no le había requerido al Director Auxiliar de Operaciones que desarrollara y le remitiera para aprobación, un procedimiento para la creación, el mantenimiento y el control de las cuentas

de acceso a la red de la Comisión y a Internet que incluyera, entre otras cosas, la utilización y el control de un formulario para la solicitud, la autorización, la creación, la aprobación y la cancelación de las cuentas de acceso de los usuarios.

Hallazgo 6 - Deficiencias relacionadas con la seguridad y el acceso físico al cuarto de servidores, y falta de documentación de la configuración de los servidores y del diagrama esquemático de la red

a. Los 6 servidores¹⁴ de la Comisión estaban ubicados en el cuarto de servidores y mediante estos se ofrecía servicios a 41 usuarios de la red de comunicaciones. El examen efectuado el 10 de marzo de 2010 sobre la seguridad y el acceso físico en el cuarto de servidores, reveló las siguientes faltas de control:

- 1) La Comisión no estaba utilizando el *Registro de Visitantes* para el cuarto de servidores donde se encontraban instalados los servidores y los equipos que componen la red.
- 2) La construcción de las paredes del cuarto de servidores no era desde el piso hasta el techo, por lo que quedaba un espacio que permitía el acceso al lugar.
- 3) Las puertas de los gabinetes, en los que estaban ubicados los servidores, se mantenían abiertas y con las llaves colgadas de las mismas.
- 4) El cableado de los gabinetes de los servidores no estaba organizado ni identificado. Además, había cables eléctricos, junto a los cables de comunicaciones, y no estaban protegidos dentro de tubos flexibles para entrar al gabinete de cableado.

En la *Política Ním. TIG-003 de la Carta Circular Ním. 77-05* se establece que el acceso a las instalaciones de sistemas de información deberá estar controlado para que solamente el personal autorizado pueda utilizarlas. Además, se establece que cada agencia será responsable de desarrollar políticas específicas de seguridad de acuerdo con las características propias de los ambientes de tecnología de la agencia, particularmente sus sistemas críticos. Esto implica que, como norma de sana administración, las agencias

¹⁴ Véase la nota al calce 4.

deberán tomar los cuidados necesarios para evitar daños y averías. El propósito es asegurar la confiabilidad, la integridad y la disponibilidad de la información, y protegerla contra la destrucción accidental, entre otras cosas. Para garantizar razonablemente la seguridad de los equipos y sistemas computarizados, es necesario tener un salón de computadoras que reúna las condiciones de seguridad, y los equipos de detección y protección adecuados.

b. Al 4 de noviembre de 2009, la Comisión no mantenía la documentación de la configuración de la red ni la de los servidores conectados a esta. Tampoco contaban con un diagrama esquemático de la red.

Situaciones similares a las indicadas en este **Hallazgo** fueron comentadas en el *Informe C-08-001*.

En la *Política Núm. TIG-011, Mejores Prácticas De Infraestructura Tecnológica, de la Carta Circular Núm. 77-05* se establece que las entidades gubernamentales tendrán la responsabilidad de adquirir, desarrollar e implantar una infraestructura de red segura, basada en estándares de dominio en la industria, la cual provea la comunicación necesaria para la distribución 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 sobre 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.

Las situaciones comentadas en el **apartado del a.1) al 3)** podrían 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 Comisión, así como para la confidencialidad de la información. Además, pudieran ocasionar daños a los equipos de comunicación y dificultarían fijar responsabilidades.

Las situaciones comentadas en los **apartados a.4) y b.** impiden a la Comisión 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.

Las situaciones comentadas se debían a que el Director Auxiliar de Operaciones no había tomado las medidas necesarias para asegurarse de que la Compañía A implantara controles para la seguridad y el acceso físico de las instalaciones de la red, para la identificación y la actualización de la documentación de la red, y para mantener un control de los equipos del cuarto de los servidores de la Comisión.

Hallazgo 7 - Deficiencias relacionadas con la preparación y el almacenamiento de los respaldos de los archivos computarizados de información

- a. La Compañía A realizaba diariamente un respaldo incremental de los archivos computarizados que se mantenían en los servidores. Estos respaldos diarios se guardaban en un servidor¹⁵, al igual que un respaldo completo que se preparaba semanalmente. También se preparaba mensualmente un respaldo completo que se grababa en cintas.

La Comisión mantenía dos contratos con la Compañía B, uno para los servicios de acarreo de cintas y otro para el arrendamiento de gabinetes (bóveda externa), con el objetivo de salvaguardar los respaldos de información. El personal de la Compañía B recogía en la Comisión las cintas de los respaldos y las llevaba a la bóveda externa que se encontraba en la misma compañía.

¹⁵ Véase la nota al calce 4.

El examen realizado el 4 de marzo de 2010 de los procedimientos utilizados para la preparación y el almacenamiento de los respaldos, reveló lo siguiente:

- 1) La Comisión no mantenía un registro de los respaldos preparados, en el cual se detallara la descripción de los archivos respaldados; el nombre del servidor donde se mantenían, la última fecha de actualización de la información y la explicación de fallas o situaciones especiales que ocurrieron, si alguna, durante la preparación de los respaldos.
 - 2) La Comisión no mantenía un registro de los respaldos entregados al personal de la Compañía B. Dependían de una hoja de trámite que preparaba el personal de esta compañía cuando venía a recoger los mismos.
 - 3) Los respaldos de octubre a diciembre de 2008 se entregaron a la Compañía B en enero de 2009.
- b. El examen efectuado relacionado con los servicios prestados por la Compañía B, reveló lo siguiente:
- 1) No se encontró evidencia de que se hayan prestado los servicios de acarreo para llevar los respaldos a la Compañía B, correspondientes al período de noviembre de 2009 a febrero de 2010.
 - 2) La Comisión no contaba con la llave del gabinete localizado en la Compañía B, donde se mantenían los respaldos de los datos de sus sistemas de información.

Situaciones similares a las indicadas en este **Hallazgo** fueron comentadas en el *Informe C-08-001*.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece que las agencias deben establecer controles adecuados en sus sistemas de información para garantizar la confidencialidad, la integridad y la disponibilidad de la información que manejan. Además, 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 es necesario, entre otras cosas, que toda información almacenada en medios electrónicos que se utilice como parte de la operación normal de la entidad, sea duplicada periódicamente y guardada en un lugar 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. Además, es necesario mantener un inventario detallado de las cintas de respaldos para facilitar su localización y para sustituir periódicamente, por cintas nuevas, las utilizadas para los respaldos y que permita, además, documentar el cumplimiento con las normas y los procedimientos establecidos.

En la Sección VII A. del *Plan de Respuestas de Emergencias y de Recuperación*, se establece que las cintas que se envían fuera de la agencia tienen que estar detalladas en el *Registro Resguardos Mensuales y Diarias* de cintas que se envían a la Compañía B.

Las situaciones comentadas limitaron el alcance de nuestro examen para determinar si los respaldos se habían preparado y enviado a la bóveda externa con la regularidad requerida. Además, privan a la Comisión de mantener un control adecuado de los respaldos almacenados en el servidor¹⁶, ubicado en el cuarto de servidores de la Comisión, y dificulta la localización e identificación del contenido de las cintas de respaldo enviados a la bóveda externa, en caso de que se requiera reconstruir la información en forma efectiva. Esto, a su vez, podría afectar el proceso de restauración de los sistemas afectados en casos de contingencia o emergencia.

Las situaciones comentadas se debían a que el Director Auxiliar de Operaciones:

- No le requirió al personal de la Compañía A que mantuviera un registro de los respaldos preparados, y de los enviados a la bóveda externa, para documentar la preparación y controlar los mismos. [Apartado a.1) y 2)]

¹⁶ Véase la nota al calce 4.

- No veló por que los respaldos fueran llevados consistentemente a la bóveda externa. **[Apartados a.3) y b.1)]**

La situación comentada en el **apartado b.2)** se debió a que la llave para acceder la bóveda externa donde se guardaban las cintas de los respaldos se había extraviado y no se solicitó una nueva.

Hallazgo 8 - Deficiencias relacionadas con el Inventario de Equipo Computadorizado y el control del equipo, y falta de un registro de los programas instalados en la red y en las computadoras de la Comisión

- a. El 22 de septiembre de 2009, se nos proveyó el *Inventario de Computadoras e Impresoras* de la Comisión. El examen realizado por nuestros auditores sobre este inventario reveló que el mismo no incluía la siguiente información:
 - 1) La localización, la fecha de adquisición y la descripción del equipo de la Comisión
 - 2) El costo para tres computadoras y dos servidores¹⁷
 - 3) Una computadora de escritorio, un monitor y una impresora, localizados en el Parque Educativo para la Seguridad en el Tránsito en Arecibo. Estos equipos tampoco tenían asignado un número de propiedad.
- b. En una visita realizada el 10 de marzo de 2010 al cuarto de servidores de la Comisión, encontramos tres *switches* y tres servidores sin número de propiedad.
- c. No se mantenía un registro de los programas adquiridos e instalados en la red y en las computadoras de la Comisión 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.

¹⁷ Una relación del equipo se incluyó en el borrador de los hallazgos de este Informe remitido al Director Ejecutivo para comentarios.

Situaciones similares a las indicadas en los **apartados a.3) y b.** fueron comentadas en el informe de auditoría anterior *CPED-95-13*.

En la *Ley Núm. 230* se establece que la custodia, el cuidado y el control físico de la propiedad pública será responsabilidad del jefe de la propia dependencia o su representante autorizado. 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. Esto permite ejercer un control eficaz de los activos, asegurar que los mismos existan y fijar responsabilidades a los empleados que tienen a su cargo la custodia de la propiedad, en caso de alguna situación irregular.

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

- El Encargado de la Propiedad es responsable de numerar y marcar todos los activos fijos que se reciban en su dependencia de inventario.
- 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.

En la *Política Núm. TIG-003 de la Carta Circular Núm. 77-05* se establece, entre otras cosas, que será necesario un inventario de activos de sistemas de información que incluya el equipo, los programas y los datos. Además, en la *Política Núm. TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico*, de dicha *Carta Circular* 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 solo pueden utilizarse para fines estrictamente oficiales y legales.

Las situaciones comentadas en los **apartados a. y b.** le impiden a la Comisión mantener un control efectivo sobre el equipo y la propiedad bajo su custodia. Además, propician 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 en el **apartado c.** 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 Comisión.

Las situaciones comentadas en los **apartados a. y b.** son indicativas de que el Ayudante Especial del Área de Administración¹⁸, quien, entre otras funciones, realizaba las de Encargado de la Propiedad, no cumplió con sus responsabilidades ni veló por el cumplimiento de las disposiciones citadas. Además, la situación comentada en el **apartado a.2)**, relacionada con dos computadoras de escritorio¹⁹ se debía a que este funcionario desconocía cómo fueron adquiridas las computadoras. Las mismas fueron encontradas guardadas dentro de sus cajas en la oficina del Director Auxiliar de Operaciones.

La situación comentada en el **apartado c.** se debía a que el Director Auxiliar de Operaciones no había tomado las medidas necesarias para mantener un registro y un control adecuado de los programas adquiridos e instalados en la red y en las computadoras de la Comisión.

¹⁸ El puesto de Director Auxiliar de Administración estuvo vacante durante el periodo de nuestra auditoría. El Ayudante Especial del Área de Administración estaba a cargo de las secciones de Contabilidad, Finanzas, Compras y Recursos Humanos.

¹⁹ Véase la nota al calce 17.

ANEXO

**COMISIÓN DE SEGURIDAD EN EL TRÁNSITO
SISTEMAS DE INFORMACIÓN COMPUTADORIZADOS
FUNCIONARIOS PRINCIPALES QUE ACTUARON
DURANTE EL PERÍODO AUDITADO**

		PERÍODO	
NOMBRE	CARGO O PUESTO	DESDE	HASTA
Hon. Rubén Hernández Gregorat	Secretario de Transportación y Obras Públicas y Presidente de la Comisión	9 sep. 09	30 abr. 10
Sr. Miguel A. Santini Padilla	Director Ejecutivo	9 sep. 09	30 abr. 10
Sr. Carlos E. Torres Rodríguez	Director Auxiliar de Operaciones	9 sep. 09	30 abr. 10
Sr. Pedro Colón Torres	Ayudante Especial Área de Administración ²⁰	9 sep. 09	12 abr. 10
Sra. Vanessa Resto Feliciano	Auditora Principal ²¹	16 feb. 10	30 abr. 10
Sr. Ángel Díaz Marrero	Auditor Interno	9 sep. 09	30 abr. 10
Sra. Marilú Díaz Rosado ²²	Directora de Recursos Humanos	1 en. 10	30 abr. 10

²⁰ Véase la nota al calce 18.

²¹ Este puesto fue ocupado a partir del 16 de febrero de 2010.

²² Durante el periodo del 9 de septiembre al 31 de diciembre de 2009, ocupaba el puesto de Oficial Administrativo de Recursos Humanos, pero fungió como Directora de Recursos Humanos.