Secretaría

Lcda. Tania Barbarossa Ortiz

- ☐ Ver al dorso
- ☐ Para su información
- ☐ Notas
- ☐ Para mantenerle al día
- ☐ Expediente
- ☑ Dar Cuenta
- ☐ Registrar y Procesar
- ☐ Archivar
- ☐ Preparar Carta

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 Públic
- ☐ 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 R
- ☐ 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 Leye

#862

Estado Libre Asociado de Puerto Rico
Oficina del Contralor

Yesmín M. Valdivieso
Contralora

RECIBIDO SECRETARIA SENADO DE P.R. 2013 AUG -1 AM 9:58

15 de mayo de 2013

A LA MANO

PRIVILEGIADA Y CONFIDENCIAL

Hon. Eduardo A. Bhatia Gautier
Presidente
Senado de Puerto Rico
San Juan, Puerto Rico

Estimado señor Presidente:

Le incluimos copia del *Informe de Auditoría TI-13-19* del Centro de Sistemas de Información de la Comisión de Servicio Público de Puerto Rico, aprobado por esta Oficina el 30 de abril de 2013. 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.

Mejorar la fiscalización y la administración de la propiedad y de los fondos públicos es un compromiso de todos.

Cordialmente,

Yesmín M. Valdivieso

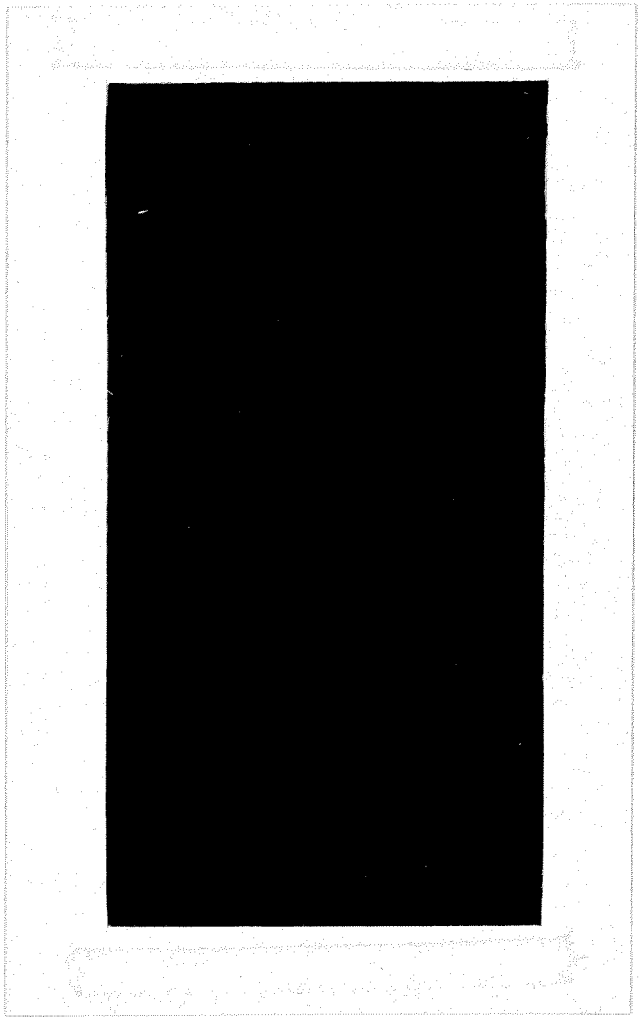
Anejo

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

#862.

[redacted]

Estado Libre Asociado de Puerto Rico
Oficina del Contralor
San Juan, Puerto Rico



INFORME DE AUDITORÍA TI-13-19

30 de abril de 2013

Comisión de Servicio Público de Puerto Rico

Centro de Sistemas de Información

(Unidad 5196 - Auditoría 13510)

Período auditado: 17 de septiembre de 2010 al 16 de mayo de 2011

CONTENIDO

Página

ALCANCE Y METODOLOGÍA **2**

CONTENIDO DEL INFORME **2**

INFORMACIÓN SOBRE LA UNIDAD AUDITADA **3**

COMUNICACIÓN CON LA GERENCIA **4**

OPINIÓN Y HALLAZGOS **5**

1 - Deficiencias relacionadas con la Evaluación de Riesgo 5

2 - Deficiencias relacionadas con el Plan de Seguridad y con el aviso que aparecía al encender las computadoras de los usuarios, y falta de un procedimiento para el manejo de incidentes de seguridad sobre los sistemas de información 7

3 - Deficiencia relacionada con el Plan de Contingencias y falta de pruebas o simulacros que certificaran la efectividad del Plan 10

4 - Deficiencia relacionada con los parámetros de seguridad sobre el control de acceso lógico a un servidor de la red, y falta de revisiones periódicas de los registros de eventos de los sistemas operativos de los servidores de la Comisión 11

5 - Deficiencias relacionadas con el contenido del formulario para la solicitud y el otorgamiento de las cuentas de acceso a los sistemas de información computadorizados de la Comisión 14

6 - Deficiencias relacionadas con el inventario de las licencias de los programas instalados, y discrepancias entre las licencias instaladas y las otorgadas a la Comisión 15

RECOMENDACIONES **17**

AGRADECIMIENTO **18**

ANEJO - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO **19**

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

30 de abril de 2013

Al Gobernador, y a los presidentes del Senado
y de la Cámara de Representantes

Realizamos una auditoría de las operaciones del Centro de Sistemas de Información (CSI) de la Comisión de Servicio Público de Puerto Rico (Comisión) para determinar si las mismas se efectuaron 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. Hicimos 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.

ALCANCE Y METODOLOGÍA

La auditoría cubrió del 17 de septiembre de 2010 al 16 de mayo de 2011. 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, tales como: entrevistas; inspecciones físicas; examen y análisis de informes y de documentos generados por la unidad auditada o suministrados por fuentes externas; pruebas y análisis de procedimientos de control interno y de otros procesos; y confirmaciones de información pertinente.

CONTENIDO DEL INFORME

Este *Informe* contiene seis hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para la administración del programa de seguridad, el acceso lógico y la continuidad del servicio. El mismo está disponible en nuestra página en Internet: http://www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La Comisión fue creada mediante la *Ley Núm. 109 del 28 de junio de 1962, Ley de Servicio Público de Puerto Rico*, según enmendada. La Comisión tiene, entre sus facultades, otorgar toda autorización de carácter público para cuyo otorgamiento no se haya fijado otro procedimiento de ley, reglamentar las compañías de servicio público y los porteadores por contrato, así como las empresas de vehículos privados dedicados al comercio. Cualquier reglamentación que se establezca sobre estas cubrirá sólo el aspecto relacionado con la seguridad de los vehículos. La Comisión está, además, facultada para imponer multas y otras sanciones administrativas; conducir investigaciones e intervenciones; y exigir cualquier clase de información que sea necesaria para el cumplimiento de sus facultades, entre otras. La Comisión está compuesta por siete comisionados, uno de los cuales será su Presidente, nombrados todos por el Gobernador con el consejo y consentimiento del Senado.

Para llevar a cabo sus funciones, la Comisión cuenta con las siguientes 15 oficinas: Presidente, Secretaría, Asesor Jurídico, Preparación y Revisión de Reglamentos, Auditoría Interna, Ayuda al Ciudadano, Planificación y Evaluación, Sistemas y Procedimientos Estratégicos, Recursos Humanos, Asesoramiento Técnico, Administración, Abogados Examinadores, Abogados del Interés Público, Coordinación de Regiones y para el Manejo de Emergencias, y Sistemas de Contabilidad y Estudios Tarifarios. Además, cuenta con 2 centros y 2 divisiones: Centro de Coordinación de Trabajos de Excavaciones y Demoliciones, Centro de Sistemas de Información, División de Estudios, Autorizaciones y Ruta Fija y División de Seguridad en el Transporte.

La Comisión presta sus servicios públicos a todos los municipios a través de seis oficinas regionales localizadas en Arecibo, Bayamón, Caguas, Mayagüez, Ponce y San Juan. Además, mantiene una División de Inspección en el Transporte en el Aeropuerto Internacional Luis Muñoz Marín.

El CSI es dirigido por un Director y cuenta con dos analistas programadores, un Ejecutivo I y un Inspector de Servicio Público III.

A la fecha de nuestra auditoría, el CSI tenía en operación una red de comunicaciones (red) de área local (*LAN*, por sus siglas en inglés) y de área amplia[1] (*WAN*, por sus siglas en inglés). La red de área local permite el acceso a los usuarios de la Oficina Central y la red de área amplia a las oficinas regionales de la Comisión.

Los gastos operacionales del CSI eran sufragados del presupuesto operacional de la Comisión, que para los años fiscales 2009-10 y 2010-11 ascendió a $11,192,000 y $9,650,000.

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

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

COMUNICACIÓN CON LA GERENCIA

Las situaciones comentadas en los **hallazgos** de este *Informe* y varias situaciones determinadas durante la auditoría, relacionadas con los controles internos establecidos para la administración del programa de seguridad, el acceso físico y lógico y la continuidad del servicio, fueron remitidas al Lcdo. José H. Banuchi Hernández, entonces Presidente, mediante cartas de nuestros auditores del 16 de mayo y del 6 y 15 de junio de 2011. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante cartas del 1, 14 y 21 de junio de 2011 el entonces Presidente remitió sus comentarios a los **hallazgos** incluidos en las cartas de nuestros auditores. Dichos comentarios fueron considerados en la redacción del borrador de este *Informe*.

---

[1] Es una red de comunicación que se conecta con diferentes lugares remotos que puede incluir desde distancias cortas, como por ejemplo un piso o un edificio, hasta transmisiones extremadamente largas que abarcan una región grande o varios países.

El borrador de los **hallazgos** de este *Informe* se remitió al entonces Presidente para comentarios, por carta del 14 de noviembre de 2012.

El entonces Presidente contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 17 de diciembre de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe*, y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**. Luego de evaluar dichos comentarios y la evidencia suministrada, determinamos que la Comisión tomó las acciones correctivas pertinentes, excepto por los **hallazgos** que se incluyen en este *Informe*.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas demostraron que las operaciones del CSI, en lo que concierne a los controles internos establecidos para la administración del programa de seguridad, el acceso físico y lógico, y la continuidad del servicio se realizaron sustancialmente conforme a las normas generalmente aceptadas en este campo, excepto por los **hallazgos del 1 al 6** que se comentan a continuación.

Hallazgo 1 - Deficiencias relacionadas con la Evaluación de Riesgo

Situación

a. Un análisis de riesgos[2] de los sistemas de información computadorizados es un método para identificar las vulnerabilidades y las amenazas a los recursos de dichos sistemas. Mediante este se identifican los posibles daños para determinar dónde implantar las medidas de seguridad para proteger dichos recursos, de manera que no se afecten adversamente las operaciones. Este método se utiliza para asegurar que las medidas de seguridad a ser implantadas sean costo-efectivas y pertinentes a las operaciones de la entidad gubernamental, y respondan a las posibles amenazas identificadas. El análisis de riesgos tiene cuatro objetivos:

- Identificar los activos y el valor monetario asignado a los mismos.

[2] Al análisis de riesgos también se le conoce como avalúo de riesgos.

- 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.

El examen realizado a la *Evaluación de Riesgo de la Comisión de Servicio Público Año Fiscal 2010-2011* (*Evaluación de Riesgo*), aprobada el 29 de junio de 2010 por la Presidenta de la Comisión, reveló las siguientes deficiencias:

- No incluía un inventario de todos los activos de los sistemas de información que detallara los equipos, programas y datos; y su valoración y clasificación de acuerdo con la misión y los servicios de la Comisión.
- No se realizó un análisis del impacto sobre las operaciones de la Comisión en caso de que se materialice alguna de las amenazas identificadas.
- No se implantaron las actividades de control sugeridas para atender las amenazas identificadas.

Criterio

Esta situación es contraria a lo establecido en la *Política TIG-003, Seguridad de los Sistemas de Información* de la *Carta Circular 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 (OGP).

Efecto

La situación comentada impide a la Comisión estimar el impacto que los elementos de riesgos tendrían en las áreas y en los sistemas críticos de esta, y considerar cómo protegerlos para reducir los riesgos de daños materiales y la pérdida de información.

Causa

La situación comentada se debió a que la Presidenta de la Comisión no había requerido que se documentara la *Evaluación de Riesgo*, según lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

Comentarios de la Gerencia

En la carta del entonces Presidente, este nos indicó las medidas implantadas y las que estaban en proceso para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 1.

Hallazgo 2 - Deficiencias relacionadas con el Plan de Seguridad y con el aviso que aparecía al encender las computadoras de los usuarios, y falta de un procedimiento para el manejo de incidentes de seguridad sobre los sistemas de información

Situaciones

a. El examen realizado al *Plan de Seguridad* (*Plan*) de la Comisión reveló que carecía de la siguiente información:

- La aprobación del Presidente
- La documentación de la validación de las normas de seguridad[3]
- La evidencia de que el Plan se basó en el análisis de riesgo
- La responsabilidad de la gerencia y de los demás componentes de la unidad relacionados con dicho plan
- Un programa de adiestramiento especializado al equipo clave de seguridad

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

- Un programa de adiestramiento continuo sobre seguridad que incluya a los nuevos empleados, los contratistas y los usuarios, y que permita mantener los conocimientos actualizados
- La documentación de los controles administrativos, técnicos y físicos de los activos de información (datos, programación, equipos y personal, entre otros)
- La documentación de la interconexión de los sistemas
- La estructura para la administración de la seguridad que requiriera la independencia adecuada, autoridad y conocimiento técnico del personal a cargo de implementar el Plan de Seguridad
- Las responsabilidades de seguridad de los administradores de los sistemas de información.

b. En la Comisión se había establecido un aviso que aparecía al encender las computadoras de la Comisión. Sin embargo, no incluía las *Normas para el Uso de las Computadoras de la CSP* ni las medidas aplicables en casos de violación a las mismas.

c. Al 25 de enero de 2011, el CSI 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.

Criterios

Las situaciones comentadas en los **apartados a. y c.** se apartan de lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*.

La situación comentada en el **apartado b.** es contraria a lo establecido en la *Política TIG-008, Uso de Sistemas de Información, de la Internet y del Correo Electrónico* de la *Carta Circular 77-05*.

Efectos

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

La situación comentada en el **apartado b.** podría dar lugar a que los usuarios no observen las normas principales para el uso de los sistemas de información, y a que se dificulte imponer sanciones por violación a las mismas. Además, pueden provocar la comisión de irregularidades y otras situaciones adversas.

La situación comentada en el **apartado c.** le impide al CSI 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.

Causas

Las situaciones comentadas se debían a que el Director del CSI no incluyó los aspectos mencionados en el *Plan de Seguridad* **[Apartado a.]** y no cumplió con lo establecido en la *Política TIG-008* de la *Carta Circular 77-05*. **[Apartado b.]**

La situación comentada en el **apartado c.** obedece, principalmente, a que no se le había requerido al Director del CSI que desarrollara y remitiera para consideración y aprobación del Presidente, las normas y los procedimientos escritos necesarios para establecer el procedimiento o plan para el manejo de incidentes.

Comentarios de la Gerencia

En la carta del entonces Presidente, este nos indicó, entre otras cosas, lo siguiente:

> [...] estará trabajando con cada una de las situaciones para subsanar cualquier deficiencia observada.

Véase la Recomendación 2 de la a. a la c.

Hallazgo 3 - Deficiencia relacionada con el Plan de Contingencias y falta de pruebas o simulacros que certificaran la efectividad del Plan

Situaciones

a. La Comisión tenía el *Plan Operacional de Emergencias Plan Multiriesgo* (*Plan Operacional de Emergencias*), aprobado el 16 de junio de 2010 por la Presidenta de la Comisión. El *Plan de Contingencias* estaba incluido en el *Plan Operacional de Emergencias*. El examen realizado al *Plan de Contingencias* reveló que no incluía el detalle del contenido de los respaldos, así como los nombres de las librerías y de los archivos.

b. El CSI no había realizado pruebas o simulacros que certificaran la efectividad del *Plan de Contingencias*.

Criterio

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 garantiza 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 fuera necesario, relocalizar las operaciones en el menor tiempo posible y de la forma más ordenada y confiable. **[Apartado a.]** Además, se deben efectuar pruebas o simulacros, por lo menos una vez al año, para comprobar la efectividad del mismo. **[Apartado b.]**

Efectos

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 y de interrupciones prolongadas de los servicios a los usuarios de la Comisión.

Causas

La situación comentada en el **apartado a.** se debía a que el Director del CSI no había recibido instrucciones por parte del entonces Presidente para incluir en el *Plan* los requisitos mencionados.

La situación comentada en el **apartado b.** se debía a que el Director del CSI no había realizado las gestiones de efectuar y documentar los simulacros como parte del *Plan*.

Comentarios de la Gerencia

En la carta del entonces Presidente, este nos indicó las medidas implantadas y las que estaban en proceso para corregir las situaciones comentadas en el **Hallazgo**.

Véanse las recomendaciones 2.d. y 3.

Hallazgo 4 - Deficiencia relacionada con los parámetros de seguridad sobre el control de acceso lógico a un servidor de la red, y falta de revisiones periódicas de los registros de eventos de los sistemas operativos de los servidores de la Comisión

Situaciones

a. La Comisión tenía en operación un servidor configurado como *Domain Controller* (*DC*) con 173 cuentas de usuarios para acceder a la red. El examen realizado sobre los parámetros de los controles de acceso y de seguridad definidos en el sistema operativo de dicho servidor reveló que no se había restringido el tiempo de acceso a la red a 97 cuentas de usuarios conforme a las responsabilidades y las necesidades de servicio de estos. Los mismos tenían acceso a la red las 24 horas y los 7 días a la semana.

b. Al 17 de marzo de 2011, el personal del CSI no examinaba periódicamente los registros de violaciones de seguridad provistos por el sistema operativo de los servidores de la Comisión. Esto, para

conocer las posibles violaciones de seguridad que pudieran ocurrir en el servidor y en la red, y tomar prontamente las medidas preventivas y correctivas necesarias.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta se establece, entre otras cosas, que las agencias 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. Además, se establece que las agencias deberán desarrollar procedimientos para detectar, reportar y responder a incidentes de seguridad, incluidos los límites para esos incidentes en términos de tiempo máximo y mínimo de respuesta. También se establece que todos los empleados y contratistas deberán conocer los procedimientos para informar los diferentes tipos de incidentes. Esta política se implementa, en parte, mediante la revisión continua, por el personal técnico especializado, de los registros computadorizados de eventos e incidentes de seguridad, producidos por los servidores principales.

Efectos

La situación comentada en el **apartado a.** propicia que personas no autorizadas puedan lograr acceso a información confidencial mantenida en los sistemas computadorizados y hacer uso indebido de esta. Además, propicia el ambiente para la comisión de errores e irregularidades sin que los mismos se puedan detectar a tiempo para fijar responsabilidades.

La situación comentada en el **apartado b.** priva al CSI de información sobre errores en el sistema y posibles violaciones de seguridad que pudieran ocurrir en la red, que le permita tomar prontamente las medidas preventivas y correctivas necesarias.

Causas

La situación comentada en el **apartado a.** se debió a que el Director del CSI entendía que el restringir el tiempo de acceso a los usuarios por las funciones que realizan es una carga administrativa para el empleado que realiza las funciones de Administrador de Seguridad.

La situación comentada en el **apartado b.** se atribuye a que el Director del CSI no se había asegurado de que se revisaran periódicamente los registros de violaciones de seguridad provistos por el sistema operativo de los servidores de la Comisión.

Comentarios de la Gerencia

En la carta del entonces Presidente este nos indicó, entre otras cosas, lo siguiente:

> La CSP ha implementado controles en torno al acceso físico a sus facilidades. Solo dos personas están autorizadas a entrar fuera de horas laborables incluyendo el Presidente. Cualquier otra persona que desee acceso al edificio y a sus recursos tiene que ser autorizadas directamente por el presidente de la CSP. Entendemos que esto es control suficiente para este propósito. El problema de mantener otros tipos de controles supone una carga adicional en tiempo y esfuerzo al ya atareado y escaso personal de sistemas. [...] [*sic*] **[Apartado a.]**
>
> Se ha encomendado esta tarea al [...], su labor es la de monitorear semanalmente a través de un programa de inventario de equipos y aplicaciones adquirido por la CSP. Este programa permite de manera centralizada la auditoria de las bitácoras de eventos de todos los servidores incluyendo aquellos eventos que se relacionan con la seguridad. [...] [*sic*] **[Apartado b.]**

Consideramos las alegaciones del entonces Presidente, pero determinamos que el **apartado a.** del **Hallazgo** prevalece porque los controles establecidos por la Comisión no son efectivos para asegurar la prevención y la detección oportuna de accesos no autorizados a los sistemas de información computadorizados.

Véase la Recomendación 2.e. y f.

Hallazgo 5 - Deficiencias relacionadas con el contenido del formulario para la solicitud y el otorgamiento de las cuentas de acceso a los sistemas de información computadorizados de la Comisión

Situación

a. Desde finales de 2010, en la Comisión se utiliza el formulario *Acceso y Registro de Usuario* para solicitar acceso a la red, a Internet y a las diferentes aplicaciones con los privilegios de acceso en cada una de estas. En dicho formulario se requiere, entre otras cosas, el tipo de solicitud, el nombre del empleado, el tipo de usuario, el horario para el uso del sistema, la fecha de la solicitud y el nombre del supervisor. Sin embargo, en este formulario no se requiere la firma del supervisor como aprobación del acceso solicitado ni la firma del empleado del CSI que otorgaba el acceso a los sistemas de información computadorizados.

Criterios

La situación comentada es contraria a lo establecido en el Artículo X del *Procedimiento para la Adquisición, Uso y Administración de las Tecnologías de Información de la Comisión de Servicio Público*, aprobado el 16 de junio 2006 por el Presidente de la Comisión, y en la *Política TIG-003* de la *Carta Circular 77-05*.

Efecto

La situación comentada impide mantener un control de los usuarios autorizados a acceder los sistemas de información computadorizados y de los privilegios asignados para fijar responsabilidades en caso de errores o irregularidades.

Causa

La situación comentada se debía a que el Director de la CSI no se aseguró de que se incluyera en el formulario *Acceso y Registro de Usuario* un espacio para la firma del supervisor del empleado que solicitaba el acceso y del empleado del CSI que otorgaba el mismo.

Comentarios de la Gerencia

En la carta del entonces Presidente, este nos indicó las medidas implantadas y las que estaban en proceso para corregir las situaciones comentadas en el **Hallazgo**.

Véase la Recomendación 2.g.

Hallazgo 6 - Deficiencias relacionadas con el inventario de las licencias de los programas instalados, y discrepancias entre las licencias instaladas y las otorgadas a la Comisión

Situaciones

a. La Comisión utiliza diferentes programas en sus sistemas de información. El uso de estos programas está restringido a la cantidad de licencias adquiridas. El examen realizado del inventario entregado el 25 de marzo de 2011 reveló que este no incluía, entre otras cosas, el número de licencia del programa, la fecha de adquisición, el número de propiedad asignado, el equipo donde está instalado el programa y la ubicación física de la licencia.

b. El inventario contenía una discrepancia entre las licencias otorgadas por la OGP y las licencias que fueron instaladas en las computadoras de los usuarios de la Comisión. La OGP le había otorgado 230 licencias de un programa antivirus[4] y la Comisión tenía instalado 236 de esta, lo que representa que 6 fueron instaladas sin tener la licencia requerida.

Criterios

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-008* de la *Carta Circular 77-05*.

Las mejores prácticas en el campo de la tecnología sugieren que se mantenga un registro de todos los programas en el cual se indique lo siguiente: el número de la licencia, el nombre del proveedor, el dueño de la licencia, la fecha de adquisición, el propósito y la justificación de la compra, el equipo donde está instalado (número de propiedad o de serie),

[4] El nombre del programa de antivirus se incluyó en el borrador de los **hallazgos** de este *Informe* remitido al Presidente de la Comisión para comentarios.

la ubicación física de la licencia, los disquetes y los manuales, el nombre del usuario, el número de propiedad asignado, la lista de inventario (licencia, disquetes, manuales, equipo) y el costo.

Efectos

Las situaciones comentadas impiden ejercer un control eficaz de los programas y de 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.

Causas

Las situaciones comentadas se debieron a que el Director del CSI:

- no se aseguró de incluir la información indicada en el inventario de las licencias de los programas instalados **[Apartado a.]**
- no mantuvo un control de las licencias otorgadas por la OGP y las instaladas en las computadoras. **[Apartado b.]**

Comentarios de la Gerencia

En la carta del entonces Presidente este nos indicó, entre otras cosas, lo siguiente:

> La comisión adquirió una aplicación cuyo propósito, entre otras cosas, es el tener una herramienta para auditar el cumplimiento y la utilización de las licencias que poseemos. [*sic*] **[Apartado a.]**
>
> La razón para esto es que una gran cantidad de esas maquinas no están en funcionamiento a consecuencia de la cantidad de empleados que ya no trabajan en la CSP. [...] Aunque el inventario refleja la totalidad de las maquinas lo cierto es que hay una diferencia significativa entre las que están siendo utilizadas en el día a día y las 236 en cuestión. Alguna de esas maquinas están almacenadas esperando ser decomisadas y otras se les está utilizando como remplazo de partes por lo que no deben ser contabilizadas. [*sic*]. **[Apartado b.]**

Véase la Recomendación 2.h.

RECOMENDACIONES

Al Presidente de la Comisión de Servicio Público de Puerto Rico

1. Asegurarse de que se realice y se documente el análisis de riesgos de los sistemas de información computadorizados, según se establece en la *Política TIG-003* de la *Carta Circular 77-05* y que se incluyan los elementos mencionados en el **Hallazgo 1**. El informe producto de este análisis de riesgos debe ser remitido para su revisión y aprobación.

2. Ejercer una supervisión eficaz sobre el Director del CSI para asegurarse de que:

   a. Revise el *Plan de Seguridad* para que incluya los criterios descritos en el **Hallazgo 2-a.** y luego lo remita para su aprobación. Una vez aprobado, vea que se divulgue a los funcionarios y a los empleados concernientes, y que se realicen pruebas periódicas del mismo para asegurar su funcionamiento.

   b. Revise el aviso que aparecía al encender las computadoras de la Comisión para que incluya las *Normas para el Uso de los sistemas electrónicos de la CSP* y las medidas aplicables en casos de violación a las mismas. **[Hallazgo 2-b.]**

   c. Prepare y remita para su aprobación un procedimiento para el manejo de incidentes. En el mismo 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 2-c.]**

   d. Revise el *Plan de Contingencias* para que incluya los aspectos comentados en el **Hallazgo 3-a.** y lo remita para aprobación.

   e. 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 4-a.]**

f. Revise, periódicamente, los eventos registrados en el servidor principal de la red y, de ser necesario, tome de inmediato las medidas preventivas y correctivas necesarias. **[Hallazgo 4-b.]**

g. Enmiende el formulario *Acceso y Registro de Usuarios* para que contenga la información que se indica en el **Hallazgo 5**.

h. Mantenga un inventario actualizado de los programas adquiridos por la Comisión y los instalados en las computadoras de esta. El inventario debe contener, 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. **[Hallazgo 6]**

3. Ejercer una supervisión eficaz sobre la Coordinadora Interagencial para el Manejo de Emergencias para asegurarse de que coordine y efectúe, junto al Director del CSI, las pruebas o simulacros para certificar la efectividad del *Plan de Contingencias*. **[Hallazgo 3-b.]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yesmin Valdivieso

ANEJO

COMISIÓN DE SERVICIO PÚBLICO DE PUERTO RICO
CENTRO DE SISTEMAS DE INFORMACIÓN
FUNCIONARIOS PRINCIPALES DE LA ENTIDAD
DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Lcdo. José H. Banuchi Hernández	Presidente	9 mar. 11	16 may. 11
"	Presidente Interino	1 feb. 11	8 mar. 11
Lcda. María T. Fullana Hernández	Presidenta	17 sep. 10	31 ene. 11
Sra. Ana I. Delgado Santiago	Auditora Principal	17 sep. 10	16 may. 11
Sra. Cynthia Z. Zambrana Crespo	Directora de Finanzas Interina	17 sep. 10	16 may. 11
Sr. Alexander Rodríguez Sánchez	Director del Centro de Sistemas de Información	17 sep. 10	16 may. 11
Sra. Wilmaris Báez Morales	Directora de Recursos Humanos	16 dic. 10	16 may. 11
"	Directora de Recursos Humanos Interina	17 sep. 10	15 dic. 10
Sr. José R. Fernández Rodríguez	Ejecutivo II a cargo de Administración	17 sep. 10	16 may. 11

MISIÓN

Fiscalizar las transacciones de la propiedad y de los fondos públicos, con independencia y objetividad, para determinar si se han realizado de acuerdo con la ley, y atender otros asuntos encomendados.

Promover el uso efectivo, económico, eficiente y ético de los recursos del Gobierno en beneficio de nuestro Pueblo.

PRINCIPIOS PARA LOGRAR UNA ADMINISTRACIÓN PÚBLICA DE EXCELENCIA

La Oficina del Contralor, a través de los años, ha identificado principios que ayudan a mejorar la administración pública. Dichos principios se incluyen en la *Carta Circular OC-08-32* del 27 de junio de 2008, disponible en nuestra página en Internet.

QUERELLAS

Las querellas sobre el mal uso de la propiedad y de los fondos públicos pueden presentarse, de manera confidencial, personalmente o por teléfono al (787) 754-3030, extensión 1106, o al 1-877-771-3133 (sin cargo). También se pueden presentar mediante el correo electrónico Querellas@ocpr.gov.pr o mediante la página en Internet de la Oficina.

INFORMACIÓN SOBRE LOS INFORMES DE AUDITORÍA

En los informes de auditoría se incluyen los hallazgos significativos determinados en las auditorías. En nuestra página en Internet se incluye información sobre el contenido de dichos hallazgos.

La manera más rápida y sencilla de obtener copias libres de costo de los informes es mediante la página en Internet de la Oficina.

También se pueden emitir copias de los mismos, previo el pago de sellos de rentas internas, requeridos por ley. Las personas interesadas pueden comunicarse con el Administrador de Documentos al (787) 754-3030, extensión 3400.

INFORMACIÓN DE CONTACTO

Dirección física:

105 Avenida Ponce de León

Hato Rey, Puerto Rico

Teléfono: (787) 754-3030

Fax: (787) 751-6768

Dirección postal:

PO Box 366069

San Juan, Puerto Rico 00936-6069

Internet:

http://www.ocpr.gov.pr

Correo electrónico:

ocpr@ocpr.gov.pr