Secretaría

Lcda. Tania Barbarossa Ortíz

- ☐ 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 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 Leyes

#857

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

28 de febrero 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-13-14* de la Oficina de Sistemas de Información y Procesamiento Electrónico de la Comisión Estatal de Elecciones, aprobado por esta Oficina el 11 de febrero 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

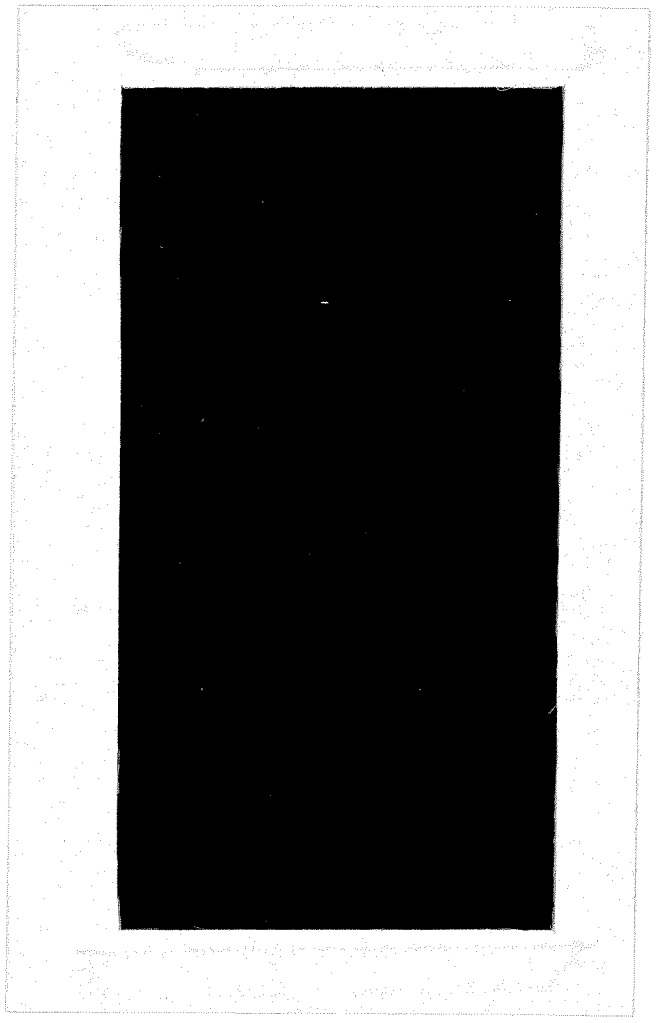
Anejo

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

#957

[redacted]

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



INFORME DE AUDITORÍA TI-13-14

11 de febrero de 2013

Comisión Estatal de Elecciones

Oficina de Sistemas de Información y Procesamiento Electrónico

(Unidad 5220 - Auditoría 13415)

Período auditado: 25 de enero de 2010 al 31 de enero de 2011

CONTENIDO

Página

ALCANCE Y METODOLOGÍA 2

CONTENIDO DEL INFORME 2

INFORMACIÓN SOBRE LA UNIDAD AUDITADA 3

COMUNICACIÓN CON LA GERENCIA 5

OPINIÓN Y HALLAZGOS 5

1 - Cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública, y falta de restricciones para enviar y recibir mensajes de correo electrónico de fuentes externas a la CEE 6

2 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de la red, y falta de revisiones periódicas de las bitácoras (*logs*) de eventos de estos servidores 9

3 - Falta de instalación y actualización del programa de antivirus, de actualización del sistema operativo, y de un registro sobre las implantaciones y actualizaciones de este 15

4 - Deficiencias relacionadas con el contenido y el uso del formulario para otorgar los accesos a la red 17

5 - Falta de controles físicos y ambientales en las áreas donde se mantenían los servidores y en los cuartos de distribución del cableado de la red 20

RECOMENDACIONES 23

AGRADECIMIENTO 27

ANEJO 1 - INFORME PUBLICADO 28

ANEJO 2 - MIEMBROS DE LA COMISIÓN ESTATAL DE ELECCIONES DURANTE EL PERÍODO AUDITADO 29

ANEJO 3 - FUNCIONARIOS PRINCIPALES DE LA ENTIDAD DURANTE EL PERÍODO AUDITADO 30

ANEJO 4 - MIEMBROS DE LA JUNTA DE ASESORES TÉCNICOS DURANTE EL PERÍODO AUDITADO 31

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

11 de febrero de 2013

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

Realizamos una auditoría de las operaciones de la Oficina de Sistemas de Información y Procesamiento Electrónico (OSIPE) de la Comisión Estatal de Elecciones (CEE) 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 25 de enero de 2010 al 31 de enero de 2011. 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, 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 es el segundo informe, y contiene cinco hallazgos sobre el resultado del examen que realizamos de los controles internos establecidos para el acceso físico y lógico a la red de comunicaciones, y del uso y el control de los equipos computadorizados. En el **ANEJO 1** presentamos información sobre el primer informe emitido sobre los controles internos establecidos para la administración del programa de seguridad, la continuidad del

servicio, y la función de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados. Ambos están disponibles en nuestra página en Internet: http://www.ocpr.gov.pr.

INFORMACIÓN SOBRE LA UNIDAD AUDITADA

La CEE se creó por virtud de la *Ley Núm. 4 del 20 de diciembre de 1977*[1], *Ley Electoral de Puerto Rico*, según enmendada. Su misión es planificar, organizar, dirigir y supervisar el organismo electoral y todos los procedimientos de naturaleza electoral que conforme a esta *Ley* y sus reglamentos, rijan en cualquier elección a celebrarse en Puerto Rico. Además, garantizar el derecho a ejercer el voto a todos los electores en los procesos eleccionarios democráticos, según dicta y dispone la Constitución.

La CEE está integrada por un Presidente, quien es el Oficial Ejecutivo, y un Comisionado Electoral en representación de cada uno de los partidos políticos principales. Además, son miembros de la CEE, pero sin voto, un Primer, un Segundo y un Tercer Vicepresidente. El Presidente es responsable de llevar a cabo y supervisar los procesos electorales en un ambiente de absoluta pureza e imparcialidad. Además, redacta y remite a la consideración y aprobación de la CEE las reglas y los reglamentos que fueran necesarios para cumplir con las disposiciones de la ley bajo su jurisdicción.

Mediante la *Resolución CEE-RS-01-05, Funciones, deberes y responsabilidades de la Junta Administrativa y la Junta de Asesores Técnicos en la Oficina de Sistemas de Información y Procesamiento Electrónico de la Comisión Estatal de Elecciones*, aprobada el 26 de junio de 2001 por la CEE, se creó la Junta Administrativa de OSIPE, la cual está integrada por un Director y dos subdirectores de distintos partidos políticos. Además, mediante dicha *Resolución*, la Junta de Técnicos creada en virtud de la *Ley Núm. 4*, fue nombrada como Junta de Asesores Técnicos (JAT). La misma está integrada por un representante de cada

[1] Esta *Ley* fue derogada por la *Ley 78-2011, Código Electoral de Puerto Rico para el Siglo XXI.*

Comisionado Electoral de los partidos principales, todos con igual rango, funciones y acceso a los procesos de la OSIPE, y quienes actúan de manera colegiada ante el Director en todos los procedimientos de esta.

La OSIPE es dirigida por la Junta Administrativa y por la JAT. Además de contar con los miembros de la Junta Administrativa, la OSIPE tiene 1 Gerente de Operaciones de Sistemas de Informática, 1 Administrador de Redes de Comunicación, 1 Administrador de Base de Datos, 3 gerentes de proyectos, 1 Gerente para el Desarrollo de Sistemas de Informática, 5 desarrolladores de sistemas de informática, 5 operadores de computadoras, 12 operadores de equipo y validación de datos, 1 Supervisor de Telecomunicaciones, 6 técnicos de comunicaciones y 2 oficinistas de proyectos especiales.

A la fecha de nuestra auditoría, la OSIPE tenía en operación una red de comunicaciones de área amplia[2] (*WAN*, por sus siglas en inglés). Dicha red permite el acceso a los usuarios del Edificio Administrativo (Oficina Central), del Edificio de Operaciones Electorales y de las juntas de inscripción permanente (JIP)[3], a los sistemas de información computadorizados.

Los recursos para financiar las actividades operacionales de la CEE provienen de resoluciones conjuntas del Presupuesto General y de fondos federales. Para los años fiscales del 2008-09 al 2010-11, el presupuesto de la CEE ascendió a $64,965,017, $36,236,489 y $37,089,550.

Los **anejos del 2 al 4** contienen una relación de los miembros de la CEE, de los funcionarios principales del nivel ejecutivo y de los miembros de la JAT que actuaron durante el período auditado, respectivamente.

---

[2] 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.

[3] En estas juntas se desarrolla un programa permanente de inscripción, expedición de tarjetas de identificación electoral, transferencias, reubicaciones y otras correcciones del registro electoral. La CEE contaba con 102 JIP ubicadas en los 78 municipios.

La CEE cuenta con una página en Internet, a la cual se puede acceder mediante la siguiente dirección: http://www.ceepur.org. 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* fueron remitidas al Hon. Héctor J. Conty Pérez, Presidente de la CEE, mediante cartas de nuestros auditores, del 22 de octubre de 2010 y del 1 de marzo de 2011. En las referidas cartas se incluyeron anejos con detalles sobre las situaciones comentadas.

Mediante cartas del 18 de noviembre de 2010 y del 24 de marzo de 2011, el Presidente remitió sus comentarios a los **hallazgos** incluidos en las cartas de nuestros auditores. Sus comentarios se consideraron al redactar el borrador de este *Informe*.

El borrador de los **hallazgos** de este *Informe* se remitió al Presidente para comentarios, por carta del 26 de septiembre de 2012. En este se indicaron datos específicos como nombres, cuentas de acceso y localizaciones, entre otros; que como medida de seguridad no se incluyeron en este *Informe*. El 2 de octubre de 2012 el Presidente solicitó una prórroga para remitir sus comentarios al borrador de los **hallazgos** de este *Informe*. El 4 de octubre de 2012 le concedimos la prórroga para remitir sus comentarios hasta el 26 de octubre de 2012. El 24 de octubre de 2012 el Presidente solicitó una prórroga adicional. El 25 de octubre de 2012 le concedimos la prórroga solicitada hasta el 13 de noviembre de 2012. El Presidente contestó el borrador de los **hallazgos** de este *Informe* mediante carta del 13 de noviembre de 2012. Sus comentarios fueron considerados en la redacción final de este *Informe* y se incluyen en la sección titulada **OPINIÓN Y HALLAZGOS**.

OPINIÓN Y HALLAZGOS

Las pruebas efectuadas revelaron que las operaciones de la OSIPE, en lo que concierne a los controles internos establecidos para el acceso físico y lógico a la red de comunicaciones, y al uso y el control de los equipos

computadorizados, no se realizaron de acuerdo con la ley y la reglamentación, aplicables en este campo. A continuación se comentan los **hallazgos del 1 al 5**.

Hallazgo 1 - Cuentas para acceder a Internet y al correo electrónico utilizadas para fines ajenos a la gestión pública, y falta de restricciones para enviar y recibir mensajes de correo electrónico de fuentes externas a la CEE

Situaciones

a. La CEE mantiene un servidor que permite el acceso a Internet a los usuarios autorizados. Dicho servidor produce diariamente un archivo en el cual se registran todas las páginas de direcciones de Internet (*web logs*) que son accedidas por las cuentas de usuarios. El examen del registro de direcciones de Internet visitadas por los usuarios de la CEE del 2 al 6 de agosto de 2010, reveló que 91 cuentas se utilizaron para examinar páginas en Internet con contenidos ajenos a la gestión pública.

b. La CEE mantiene un servidor que permite a los empleados el envío y el recibo de mensajes de correo electrónico. Dicho servidor produce diariamente un archivo en el cual se registran todos los mensajes enviados y recibidos por las cuentas de usuarios (*message tracking logs*). El examen de los registros de correo electrónico correspondientes al período del 1 al 8 de agosto de 2010, reveló que los usuarios podían enviar y recibir mensajes de correo electrónico de fuentes externas a la CEE sin ningún tipo de restricción. Además, identificamos 27 cuentas que se utilizaron para enviar mensajes de correo electrónico con contenidos ajenos a la gestión pública.

Criterios

Las situaciones comentadas son contrarias a lo establecido en el Artículo VI, Sección 9 de la Constitución. En esta se establece que sólo 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. Además, son contrarias a lo establecido

en el Artículo 3.2(c) de la *Ley Núm. 12 del 24 de julio de 1985, Ley de Ética Gubernamental del Estado Libre Asociado de Puerto Rico*, según enmendada[4].

Por otro lado, estas situaciones son contrarias a lo establecido en los artículos III y VII-c) de las *Normas Generales para el Uso de los Sistemas Computadorizados de Información de la Comisión Estatal de Elecciones*, aprobadas el 6 de noviembre de 2002 por la CEE. En estas se establece lo siguiente:

> El sistema que la CEE provee al personal de la agencia, es una herramienta de trabajo para que se realicen funciones que han sido encomendadas. El sistema incluye computadoras personales (PC), equipo electrónico, accesorios, sistema operativo, aplicaciones, correo electrónico, Internet (a los que se les autorice), utilidades y otros programas, archivos, imágenes y gráficas que son propiedad de, o cuyas licencias pertenecen a la agencia. La Comisión autoriza su uso con propósitos estrictamente oficiales. [*sic*] **[Artículo III]**
>
> [...] El servicio de correo electrónico será exclusivo para uso oficial, así como el uso de los recursos del internet y el Intranet. [*sic*] **[Artículo VII-c]**

Efectos

El uso de las cuentas para acceder a Internet y al correo electrónico, pertenecientes a la CEE, 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 y a mensajes de correo electrónico ajenos al fin público expone a los equipos y a la información sensitiva almacenada en los sistemas a riesgos innecesarios como son la

---

[4] Esta *Ley* fue derogada por la *Ley 1-2012, Ley de Ética Gubernamental de Puerto Rico de 2011*, la cual en el Artículo 4.2(b) contiene disposiciones similares.

propagación de virus, *spyware*[5], *phishing*[6], *spoofing*[7], *spamming*[8] y ataques de negación de servicios[9], entre otros, que pudieran afectar la continuidad de las operaciones de la CEE.

Causas

Las situaciones comentadas se atribuyen a la falta de:

- Orientaciones periódicas a los usuarios de los sistemas de información computadorizados 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 las cuentas para acceder a Internet y al correo electrónico.
- Evaluaciones periódicas para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado a acceder a Internet. Esto, para que el Administrador de Redes de Comunicación limite el acceso a las páginas autorizadas.
- Análisis para determinar los funcionarios y los empleados a quienes deben otorgarse los privilegios para recibir y enviar mensajes de correo electrónico de fuentes externas, de acuerdo con las necesidades de la CEE, y con los deberes y las responsabilidades de sus puestos. Esto, para que el Administrador de Redes de Comunicación configure las cuentas de los usuarios.

---

[5] 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.

[6] 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.

[7] Es un ataque activo en el que el intruso presenta una identidad que no es la original. En este ataque el propósito es obtener acceso a los datos sensitivos o a los recursos de los sistemas de información computadorizados a los que no se permite el acceso bajo la identidad original.

[8] Es el envío de correspondencia electrónica a cientos o a miles de usuarios.

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

Comentarios de la Gerencia

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

> La CEE reconoce la importancia de la utilización adecuada de los sistemas de información, por lo cual ordenó una investigación.
>
> [...] Se circuló las Normas Generales para el Uso de Sistemas Computadorizados de Información a todos los empleados de la CEE. [*sic*]

Véanse las recomendaciones de la 1 a la 3.a.3) y 4.

Hallazgo 2 - Deficiencias en los parámetros de seguridad y en los controles de acceso lógico de los servidores de la red, y falta de revisiones periódicas de las bitácoras (*logs*) de eventos de estos servidores

Situaciones

a. El examen efectuado el 12 de agosto y el 28 de septiembre de 2010 sobre los parámetros de seguridad (*Account Policies*, *Password Policy* y *Account Lockout Policy*) y los controles de acceso establecidos en el sistema operativo de seis de los servidores, reveló lo siguiente:

    1) En los seis servidores no se habían definido las políticas de contraseñas para establecer lo siguiente:

        a) La cantidad de veces que la contraseña podía ser reutilizada (*Enforce password history*)

        b) El mínimo de días para que el sistema le requiriera al usuario cambiar la contraseña (*Minimum password age*)

        c) El mínimo de caracteres requeridos para establecer las contraseñas de las cuentas de acceso de los usuarios (*Minimun password lenght*)

        d) La opción de requisitos de complejidad para la contraseña (*Password must meet complexity requirements*).

2) En los seis servidores no se habían definido las políticas de control de cuentas para establecer lo siguiente:

   a) Al menos cinco intentos fallidos antes de desactivar la cuenta (*Account lockout threshold*)

   b) El tiempo que debía permanecer la cuenta desactivada en casos de desactivarse la misma por intentos de acceso fallidos (*Account lockout duration*)

   c) El tiempo de la instrucción para reiniciar el conteo de intentos para acceder a los recursos de la red sin éxito (*Reset account lockout counter after*).

3) En tres servidores no estaba definida la política de seguridad para requerir al usuario entrar una contraseña para continuar con el uso de la red, luego de un período de inactividad (*Idle time before suspending sesión*).

4) En los seis servidores identificamos las siguientes deficiencias en la definición de los parámetros relacionados con las políticas de auditoría (*Audit Policies*):

   a) En tres servidores no se habían definido las políticas de auditoría para que el sistema produjera un registro cuando ocurrieran los siguientes eventos:

      - Un registro de solicitudes al servidor para validar las cuentas de usuario (*Audit account logon events*)

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

      - Un registro de servicios en los objetos del *Active Directory* (*Audit directory services access*)

- Un registro de eventos del sistema relacionados con la activación y desactivación en las cuentas (*Audit logon events*)
- Los accesos a los archivos, cartapacios (*folders*) e impresoras (*Audit object access*)
- Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit policy change*)
- El uso de los privilegios de los usuarios (*Audit privileged use*)
- Las acciones ejecutadas de los procesos (*Audit process tracking*)
- El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit system events*).

b) En dos servidores las políticas de auditoría estaban configuradas para que no se produjera un registro (*no auditing*) de los eventos que se describen a continuación:

- La creación, modificación o eliminación de una cuenta o grupo de usuarios, el cambio de nombre o contraseña y la activación o desactivación de una cuenta o grupo de usuarios (*Audit account management*)
- Los cambios efectuados a las opciones de seguridad, los privilegios de usuarios y las políticas de auditoría (*Audit policy change*)
- El reinicio y apagado, y los eventos que afectan al sistema de seguridad (*Audit system events*).

c) En un servidor las políticas de auditoría estaban configuradas para que no se produjera un registro (*no auditing*) de los eventos que se describen a continuación:

- Un registro de solicitudes al servidor para validar las cuentas de usuario (*Audit account logon events*)
- Un registro de eventos del sistema relacionados con la activación y desactivación en las cuentas (*Audit logon events*).

b. Al 12 de agosto de 2010, un servidor contenía 445 cuentas para acceder a la red. El examen efectuado sobre el control y el mantenimiento de estas cuentas reveló las siguientes deficiencias:

1) Existían 42 cuentas inactivas y no habían sido eliminadas del sistema. Estas cuentas nunca se habían utilizado.

2) Con relación a las 403 cuentas activas, identificamos lo siguiente:

a) Para 402 cuentas (99%) no se había restringido el tiempo de acceso a la red de la CEE conforme a las responsabilidades y a las necesidades de servicio de los usuarios. Los mismos tenían acceso a la red las 24 horas y los 7 días de la semana.

b) Doscientas setenta y cinco cuentas (68%) estaban configuradas para que la contraseña no expirara.

c) Existían 46 cuentas (11%) que nunca se habían utilizado.

3) Trece cuentas tenían privilegios de administración. Diez de estas tenían sus contraseñas expiradas por un período entre 189 y 1,178 días, y a 1 nunca se le había cambiado la contraseña.

c. Al 14 de octubre de 2010, el personal encargado de administrar los sistemas no examinaba periódicamente los registros de violaciones de seguridad provistos por el sistema operativo. 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.

Situaciones similares a las de los **apartados a.1)b) y 2), y b.2)a)** se comentaron en el *Informe de Auditoría TI-98-11* del 13 de mayo de 1998.

Criterio

Las situaciones comentadas son contrarias 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. En esta se establece, entre otras cosas, que las entidades gubernamentales deberán implantar controles que minimicen los riesgos de que los sistemas de información dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Esta norma se instrumenta, en parte, mediante lo siguiente:

- La renovación periódica de la contraseña de cada usuario, según las necesidades de la entidad y los procedimientos establecidos
- El uso de todas las opciones para restringir y controlar los accesos que proveen los distintos sistemas operativos
- La activación de todas las opciones para registrar los eventos de seguridad de las aplicaciones y del sistema operativo
- La limitación del tiempo de acceso para todas las cuentas de acceso de acuerdo con las funciones de cada usuario
- La impresión y el examen continuo de los informes que detallan los eventos inusuales del sistema.

Efectos

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

Las situaciones comentadas en el **apartado a.4)** impiden a la CEE mantener registros de los eventos inusuales o problemas ocurridos en la red que le permitan al Administrador de Redes de Comunicación tomar a tiempo las medidas correctivas o preventivas necesarias. Además, impiden la detección temprana de errores críticos o problemas en los servidores y en las computadoras, de accesos no autorizados y del uso indebido de los sistemas computadorizados.

Causa

Las situaciones comentadas se debían, en parte, a que el Administrador de Redes de Comunicación no realizaba todas las funciones designadas en su especificación de clase, entre las que se encontraban administrar, monitorear y mantener la seguridad e integridad de la red de comunicaciones de la CEE.

Comentarios de la Gerencia

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

> La Junta Administrativa y la Junta de Asesores Técnicos estudió y evalúo los parámetros de seguridad, los controles de acceso lógico de los servidores y los atemperó a las mejores prácticas disponibles y particularidades de la Agencia y los servicios que esta presta. [*sic*]

Véanse las recomendaciones 3.a. de la 4) a la 11), b. y c.

Hallazgo 3 - Falta de instalación y actualización del programa de antivirus, de actualización del sistema operativo, y de un registro sobre las implantaciones y actualizaciones de este

Situaciones

a. El examen realizado entre el 8 de marzo y el 30 de abril de 2010 sobre el uso y el control del programa antivirus, en 19 computadoras instaladas en 12 JIP visitadas, reveló que:

   1) Una computadora no tenía instalado un programa antivirus, que permitiera prevenir y detectar los programas no deseados.

   2) Tres computadoras no tenían actualizadas las definiciones[10] (*virus definitions file*) del programa antivirus instalado en estas.

b. En 10 de las 19 computadoras (53%) examinadas en las JIP no se había instalado la última actualización del sistema operativo, provista por el proveedor.

c. En dos servidores no se habían instalado las actualizaciones (*services packs*) correspondientes al sistema operativo. Además, en un servidor no se había instalado la última actualización del sistema operativo ni de la aplicación.

d. Al 7 de junio de 2010, la CEE no contaba con un registro de la implantación y las actualizaciones al sistema operativo de la red.

Criterios

Las situaciones comentadas en el **apartado a.** 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 instalar controles automáticos para la prevención y la detección de programas no deseados, tales como: virus, *spyware*, *adware*[11] y actualizaciones (*updates*)

---

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

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

automáticas. Esto implica que, como norma de sana administración, dichos programas deben estar actualizados, de manera que los mismos puedan detectar y eliminar nuevas amenazas.

Las mejores prácticas en el campo de la tecnología de información sugieren que se deben implantar controles que minimicen los riesgos de que los sistemas computadorizados dejen de funcionar correctamente y de que la información sea accedida de forma no autorizada. Estos controles se establecen, en parte, mediante: **[Apartados del b. al d.]**

- La activación de todas las opciones para registrar los eventos de seguridad de las aplicaciones y del sistema operativo
- La instalación de las actualizaciones de seguridad, de manera que se puedan atender las vulnerabilidades descubiertas en los sistemas y evitar nuevas amenazas a los mismos
- El registro de las actualizaciones realizadas a los sistemas operativos.

Efectos

Las situaciones comentadas en el **apartado a.** pueden impedir la prevención y la detección de programas no deseados, y permitir que estos puedan propagarse a los sistemas de información. Esto afectaría la integridad, la confidencialidad y la disponibilidad de los sistemas de información de la CEE.

Las situaciones comentadas en los **apartados del b. al d.** no permiten que la CEE tenga un control efectivo y documentado, dirigido a mantener actualizado y en óptimas condiciones el sistema operativo instalado en las computadoras y en los servidores. Esto mantiene a la CEE al margen de los avances tecnológicos y no le permite tener a su disposición mejores herramientas que promuevan una administración más efectiva y eficiente de los recursos de la red de comunicaciones.

Causas

La situación comentada en el **apartado a.** se debío, en parte, a que el Administrador de Redes de Comunicación no revisaba periódicamente si el proceso de actualización del programa de antivirus en las computadoras, se efectuaba correctamente. Este proceso estaba automatizado.

Las situaciones comentadas en los **apartados del b. al d.** se debieron, en parte, a que la Junta Administrativa de OSIPE no se aseguró de que:

- El Gerente de Operaciones de Sistemas de Informática instalara en las computadoras de las JIP, las últimas actualizaciones de los sistemas operativos emitidas por el proveedor. **[Apartado b.]**

- El Administrador de Redes de Comunicación mantuviera actualizados los servidores y las aplicaciones **[Apartado c.]** y un registro de las implantaciones y de las actualizaciones realizadas al sistema operativo de la red. **[Apartado d.]**

Comentarios de la Gerencia

En la carta del Presidente, este nos indicó, entre otras cosas, las medidas establecidas para corregir y evitar las situaciones comentadas.

Véase la Recomendación 3.a.12) y 13) y d.

Hallazgo 4 - Deficiencias relacionadas con el contenido y el uso del formulario para otorgar los accesos a la red

Situaciones

a. Al 12 de agosto de 2010, en la CEE se utiliza el formulario *Hoja de Trámite sobre el Acceso a la Red* para solicitar la creación y la modificación de las cuentas de acceso de los usuarios. En este formulario se requiere, entre otra información, el nombre y puesto del usuario, la fecha de solicitud para la creación de la cuenta de acceso, la fecha de autorización y de procesamiento de la solicitud, y las

opciones para solicitar el acceso a las aplicaciones, el correo electrónico e Internet. El examen realizado sobre el contenido y el uso de dicho formulario reveló las siguientes deficiencias:

1) El formulario no requería:

   a) La justificación del otorgamiento del acceso basado en las responsabilidades del usuario

   b) La justificación del cambio en los accesos de las cuentas de los usuarios.

2) El formulario no era utilizado para solicitar la cancelación de las cuentas de acceso de los usuarios. Esto, a pesar de que el mismo contaba con un apartado para este propósito.

3) El formulario no se utilizaba para autorizar y justificar la creación de las cuentas con privilegios de administración y las cuentas de mantenimiento.

b. En el examen de 26 cuentas de acceso a la red de la CEE, creadas entre el 5 de diciembre de 2002 y el 29 de febrero de 2009, determinamos lo siguiente:

   1) No se encontró, ni le fue suministrada a nuestros auditores, evidencia de que se hubiera utilizado algún documento o formulario para la solicitud y la aprobación de 19 (73%) de las 26 cuentas de acceso.

   2) De los formularios examinados, correspondientes a las restantes 7 cuentas de acceso, 6 (86%) no tenían la firma del solicitante, y 1 (14%) no indicaba el acceso otorgado.

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 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. Además, se establece que la información y los

programas de aplicación utilizados en las operaciones de la agencia 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. Esta norma se instrumenta, en parte, mediante:

- El establecimiento de controles de acceso rigurosos a la red, a las aplicaciones y a los archivos, incluido el uso de formularios para solicitar la creación, la modificación y la eliminación de cuentas de acceso a los diferentes recursos disponibles a través de la red, para cada usuario
- El mantenimiento de registros confiables y actualizados de las cuentas solicitadas, autorizadas, modificadas y canceladas.

Efectos

Las situaciones que se comentan impiden mantener la evidencia requerida de las autorizaciones para otorgar o cancelar los accesos y los privilegios a los usuarios. Esto, a su vez, puede propiciar que personas no autorizadas accedan a información confidencial y la utilicen indebidamente. Además, propician la comisión de irregularidades y la alteración, por error o deliberadamente, de los datos contenidos en los sistemas de información, sin que puedan ser detectados a tiempo para fijar responsabilidades.

Causas

Las situaciones comentadas se debían principalmente a que la Junta Administrativa de la OSIPE no mantenía un control adecuado de los accesos otorgados, cancelados y modificados, para documentar claramente la justificación de los mismos. Además, se debía a la falta de evaluación detallada previo a la autorización, para asegurarse de que los formularios estuvieran debidamente completados por los usuarios y sus supervisores.

Comentarios de la Gerencia

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

> Se revisó los formularios: "Documento para solicitud y entrega de tokens para acceso al Sistema de la TIE desde la JIP" y "Hoja de Trámite sobre el Acceso a la Red" con el fin de que las situaciones presentadas no se vuelvan a repetir. [*sic*]

Véase la Recomendación 3.a.8), e. y f.

Hallazgo 5 - Falta de controles físicos y ambientales en las áreas donde se mantenían los servidores y en los cuartos de distribución del cableado de la red

Situaciones

a. Al 22 de febrero de 2010, el Centro de Cómputos de la CEE estaba dividido en el Área de Operaciones, que contaba con 13 servidores, y en el Área de Servidores, que contaba con 18. Además, la CEE tenía un cuarto de distribución de cableado en cada uno de los 10 pisos del edificio principal, y un gabinete con los equipos de comunicaciones, en cada una de las JIP.

   El examen efectuado en el Área de Servidores, en los 10 cuartos de distribución de cableado y en las 12 JIP visitadas, reveló lo siguiente:

   1) Relacionado con los controles físicos:

      a) Un cuarto de distribución de cableado permanecía abierto, lo que permitía el acceso a personal ajeno a las operaciones de la red.

      b) En 9 (75%) de las 12 JIP visitadas, los gabinetes donde se ubicaban los equipos de comunicaciones se encontraban sin seguro. Además, en 1 JIP la puerta del gabinete tenía las llaves puestas en la cerradura.

      c) En 2 (17%) de las 12 JIP visitadas, el cableado y los equipos de comunicaciones se instalaron en áreas donde estaban accesibles a los empleados y a los visitantes.

2) Relacionado con los controles ambientales:

a) El cableado y los equipos de comunicaciones en los cuartos de distribución del edificio principal de la CEE y los equipos de comunicaciones de 4 (33%) de las 12 JIP visitadas tenían polvo acumulado.

b) En 7 (58%) de las 12 JIP visitadas, el área donde se encontraban instalados los equipos de comunicaciones no cumplían con las condiciones ambientales adecuadas para proteger los mismos. En dichas áreas encontramos almacenados materiales inflamables, tales como, cajas de cartón, estufas, equipos de cocina y alimentos.

Criterio

Las situaciones comentadas son contrarias a lo establecido en la *Política TIG-003* de la *Carta Circular 77-05*. En esta 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. Esto implica que, para garantizar la seguridad en los sistemas de información y de los equipos computadorizados, es necesario que:

- Se controle adecuadamente el acceso a las áreas donde están ubicados los servidores y los equipos de comunicaciones. **[Apartado a.1)]**
- Se mantengan los equipos de comunicaciones en un lugar seguro que provea las condiciones ambientales y de seguridad adecuadas. **[Apartado a.2)]**
- No se almacenen materiales que entorpezcan el libre movimiento en las referidas áreas y puedan causar daños a los equipos de comunicación. **[Apartado a.2)b)]**

Efectos

Las situaciones comentadas en el **apartado a.1)** pueden ocasionar que personal ajeno a las operaciones de la red tengan acceso a los equipos de comunicaciones, lo que pone en riesgo la continuidad de los servicios que ofrece la CEE, así como la confidencialidad de la información.

Las situaciones comentadas en el **apartado a.2)** pueden ocasionar daños y deterioros prematuros a los servidores y a los equipos de comunicaciones de la CEE, y provocar eventos de interrupción de servicios.

Causas

Las situaciones comentadas se debían a que la Junta Administrativa de la OSIPE no se había asegurado de que:

- Los servidores y los equipos de comunicaciones estuvieran ubicados en lugares adecuados y seguros, en los que existieran los correspondientes controles físicos y ambientales. **[Apartado a.]**

- Se proveyera mantenimiento preventivo al cableado y a los equipos conectados a la red, de manera que estos se mantengan libres de polvo, y se garantice la existencia de controles ambientales adecuados. **[Apartado a.2)]**

Además, la situación comentada en el **apartado a.2)a)** se debía, en parte, a que la Junta Administrativa de la OSIPE no se había asegurado de que se estableciera un itinerario para el mantenimiento y la limpieza rutinaria de los equipos conectados a la red.

Comentarios de la Gerencia

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

> Se fortaleció la seguridad en los cuartos de distribución de cableado en todos los pisos de la CEE y se realizaron mejoras al edificio.
>
> Aceptamos la situación y se tomaran medidas correctivas mediante comunicación para impartir instrucciones a las JIP para que la situación no se repita.

Véase la Recomendación 3.g.

RECOMENDACIONES

Al Presidente de la Comisión Estatal de Elecciones

1. Impartir instrucciones para que se realicen evaluaciones periódicas para determinar las páginas electrónicas que son necesarias según los deberes y las responsabilidades del personal autorizado para acceder a Internet. Luego de efectuada cada evaluación, remitir la lista de las páginas autorizadas a la OSIPE. **[Hallazgo 1-a.]**

2. Impartir instrucciones para que se realicen evaluaciones periódicas del personal que debe tener el privilegio de envío y recibo de correo electrónico de fuentes externas, de acuerdo con los deberes y las responsabilidades de sus puestos. Luego de efectuada cada evaluación, remitir la lista de los usuarios a la OSIPE para que se limiten los privilegios de acceso del correo electrónico. **[Hallazgo 1-b.]**

3. Ejercer una supervisión efectiva para asegurarse de que la Junta Administrativa de la OSIPE:

    a. Imparta instrucciones al Administrador de Redes de Comunicación para que:

        1) Realice las inspecciones periódicas necesarias para verificar el uso adecuado de las cuentas de acceso a Internet y correo electrónico. **[Hallazgo 1]**

        2) Conforme a la lista de páginas autorizadas, limite el acceso a las páginas electrónicas para que sólo se puedan acceder aquellas que son necesarias para cumplir con los deberes y las responsabilidades del personal autorizado para acceder a Internet. **[Hallazgo 1-a.]**

        3) De acuerdo con las evaluaciones periódicas realizadas por la gerencia, limite los derechos y los privilegios para que solamente pueda enviar y recibir mensajes de correo electrónico de fuentes externas el personal que lo necesita para cumplir con los deberes y las responsabilidades de su puesto. **[Hallazgo 1-b.]**

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

   a) Restringir que los usuarios puedan repetir las últimas cinco contraseñas utilizadas anteriormente. **[Hallazgo 2-a.1)a)]**

   b) Requerir un mínimo de 10 días antes que el sistema permita al usuario cambiar la contraseña nuevamente. **[Hallazgo 2-a.1)b)]**

   c) Establecer un mínimo de ocho caracteres para la utilización de las contraseñas y que sean elaboradas con una combinación de caracteres alfanuméricos (letras, símbolos y números). **[Hallazgo 2-a.1)c) y d)]**

   d) Establecer un mínimo de al menos 30 días para los cambios de contraseña de cuentas con privilegio de administrador. **[Hallazgo 2-b.3)]**

5) Desconecte automáticamente las cuentas de acceso de aquellos usuarios que realizan cinco intentos sin éxito para acceder los recursos de la red (*Account Lockout Duration*) y establezca un tiempo definido para reiniciar el conteo de intentos para acceder a la red (*Reset Account Lockout Counter After*) y el tiempo que debe permanecer la cuenta desactivada en casos de desactivarse la misma por intentos de acceso fallidos (*Account Lockout Threshold*). **[Hallazgo 2-a.2)]**

6) Active la opción correspondiente en la pantalla de política de seguridad, de manera que le requiera a los usuarios entrar una contraseña para continuar con el uso de la red luego de un período de inactividad (*Idle Time Before Suspending Session*). **[Hallazgo 2-a.3)]**

7) Active las opciones correspondientes en la pantalla de políticas de auditoría (*Audit Policy*), de manera que se pueda mantener un rastro de los eventos exitosos realizados en los sistemas. **[Hallazgo 2-a.4)]**

8) Examine periódicamente los registros y las cancelaciones de accesos a la red y utilice el apartado destinado a cancelación de cuentas en el formulario *Hoja de Trámite sobre el Acceso a la Red* para llevar mejor control de las cuentas canceladas. **[Hallazgos 2-b.1) y 4-a.2)]**

9) Analice periódicamente el sistema para detectar la falta de contraseñas o la creación de contraseñas débiles y fáciles de corromper. **[Hallazgo 2-b.2)b) y c)]**

10) Restrinja el horario de acceso a los recursos de la red, según las funciones y las responsabilidades de cada usuario, y active 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 2-b.2)a)]**

11) Revise periódicamente el registro de eventos que produce el servidor principal y los intentos de acceso a la red de la CEE y, de ser necesario, tome de inmediato las medidas preventivas y correctivas. **[Hallazgo 2-c.]**

12) Revise periódicamente las actualizaciones del programa de antivirus en los servidores de la red. **[Hallazgo 3-a.]**

13) Realice y registre las implantaciones y actualizaciones a los sistemas operativos y las aplicaciones. **[Hallazgo 3-c. y d.]**

b. Establezca políticas para la elaboración, el uso, el cambio y la cancelación de las contraseñas para los usuarios de la red, aplicaciones críticas y usuarios con cuentas con privilegios de administrador y las remita para aprobación de la CEE.

Las mismas deben establecer, entre otras cosas, el prohibir compartir las contraseñas y el concientizar al personal sobre dichas políticas. **[Hallazgo 2-a.1) y 2-b.3)]**

c. Evalúe herramientas de monitoreo y análisis, de manera que mejoren los procesos de administración de seguridad y actualizaciones de los sistemas computadorizados y someta a la JAT para su aprobación. **[Hallazgo 2-c.]**

d. Imparta instrucciones para que el personal técnico evalúe e instale el programa de antivirus, las actualizaciones de seguridad y los *Service Packs* emitidos por el proveedor de los sistemas para mantener los mismos actualizados, y así asegurar un funcionamiento más efectivo y eficaz de los sistemas de información. Además, se asegure de que se mantenga un registro de las implantaciones y las actualizaciones realizadas a los sistemas operativos y a las aplicaciones de los equipos computadorizados. **[Hallazgo 3]**

e. Enmiende el formulario *Hoja de Trámite sobre el Acceso a la Red* para que contenga la información que se indica en el **Hallazgo 4-a.**

f. Se asegure de que el personal a cargo de recibir el formulario *Hoja de Trámite sobre el Acceso a la Red* verifique que este se complete en todas sus partes por los usuarios, antes de entregarlo al personal encargado de crear, modificar o cancelar la cuenta de acceso a la red. Además, que el personal de la OSIPE complete el referido formulario una vez brinde el servicio. **[Hallazgo 4-b.]**

g. Establezca las medidas de control necesarias para corregir las situaciones indicadas en el **Hallazgo 5**. Esto, de manera que se asegure de que los servidores y los equipos de comunicación se mantengan en lugares donde estén debidamente protegidos contra accesos no autorizados y contra posibles daños causados por condiciones físicas y ambientales, que puedan afectar la

continuidad de los servicios de la CEE, la confidencialidad de la información, y la disponibilidad y el rendimiento de estos equipos.

4. Ejercer una supervisión efectiva para que la Directora de Recursos Humanos establezca en coordinación con el encargado de la seguridad un programa de concienciación al personal sobre las normas y los procedimientos relacionados con el uso y la seguridad del Internet y del correo electrónico. **[Hallazgo 1]**

AGRADECIMIENTO

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

Oficina del Contralor

Por: Yesmín M. Valdivieso

ANEJO 1

COMISIÓN ESTATAL DE ELECCIONES

OFICINA DE SISTEMAS DE INFORMACIÓN Y PROCESAMIENTO ELECTRÓNICO

INFORME PUBLICADO

INFORME	FECHA	CONTENIDO DEL INFORME
TI-13-11	28 nov. 12	Examen de los controles internos establecidos para la administración del programa de seguridad, la continuidad del servicio, y la función de la Oficina de Auditoría Interna en la evaluación de los procedimientos, los controles y el funcionamiento de los sistemas de información computadorizados.

ANEJO 2

COMISIÓN ESTATAL DE ELECCIONES

OFICINA DE SISTEMAS DE INFORMACIÓN Y PROCESAMIENTO ELECTRÓNICO

MIEMBROS DE LA COMISIÓN ESTATAL DE ELECCIONES

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Héctor J. Conty Pérez	Presidente	25 ene. 10	31 ene. 11
Lcdo. Nicolás Gautier Vega	Comisionado Electoral del Partido Popular Democrático	25 ene. 10	31 ene. 11
Ing. Héctor M. Morales Vargas	Comisionado Electoral del Partido Nuevo Progresista	8 sep. 10	31 ene. 11
Sr. Hugo L. Pérez Estrella	"	25 ene. 10	31 ago. 10
Lcdo. Juan M. Dalmau Ramírez	Comisionado Electoral del Partido Independentista Puertorriqueño	25 ene. 10	31 ene. 11
Sr. Walter Vélez Martínez	Secretario	25 ene. 10	31 ene. 11

ANEJO 3

COMISIÓN ESTATAL DE ELECCIONES

OFICINA DE SISTEMAS DE INFORMACIÓN Y PROCESAMIENTO ELECTRÓNICO

FUNCIONARIOS PRINCIPALES DE LA ENTIDAD

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Hon. Héctor J. Conty Pérez	Presidente	25 ene. 10	31 ene. 11
Sra. María D. Santiago Rodríguez	Primer Vicepresidente	25 ene. 10	31 ene. 11
Sr. Néstor Colón Berlingeri	Segundo Vicepresidente	25 ene. 10	31 ene. 11
Sr. José De Jesús Peña	Tercer Vicepresidente	19 ene. 11	31 ene. 11
Sr. Andrés Miranda Rosado	"	25 ene. 10	31 dic. 10
Sra. Miriam Vega Rodríguez[12]	Directora de la Oficina de Sistemas de Información y Procesamiento Electrónico	25 ene. 10	31 ene. 11
Sr. Luis R. Avilés Ramos[22]	Subdirector de la Oficina de Sistemas de Información y Procesamiento Electrónico	25 ene. 10	31 ene. 11
Sr. Juan A. Gutiérrez Rodríguez[22]	"	1 sep. 10	31 ene. 11
Vacante	"	25 ene. 10	31 ago. 10
Sra. Enid E. Rodríguez Román	Directora de la Oficina de Recursos Humanos	25 ene. 10	31 ene. 11

[12] Estos funcionarios integraban la Junta Administrativa de la OSIPE.

ANEJO 4

COMISIÓN ESTATAL DE ELECCIONES

OFICINA DE SISTEMAS DE INFORMACIÓN Y PROCESAMIENTO ELECTRÓNICO

MIEMBROS DE LA JUNTA DE ASESORES TÉCNICOS

DURANTE EL PERÍODO AUDITADO

NOMBRE	CARGO O PUESTO	PERÍODO	
		DESDE	HASTA
Sr. Eduardo Nieves Cartagena	Asesor Técnico del PNP	6 ago. 10	31 ene. 11
Vacante	"	1 jul. 10	5 ago. 10
Sr. Edgar R. Fermín Rivas	"	8 abr. 10	30 jun. 10
Vacante	"	1 abr. 10	7 abr. 10
Sr. Ángel F. Talavera Forty	"	25 ene. 10	31 mar. 10
Sr. Armando Lassus González	Asesor Técnico del PPD	25 ene. 10	31 ene. 11
Sr. Jorge I. Tirado González	Asesor Técnico del PIP	25 ene. 10	31 ene. 11
Sr. Adolfo J. Socorro Ramos	Asesor Técnico del Presidente	25 ene. 10	31 ene. 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 2124, 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) 294-0625 o (787) 200-7253, extensión 536.

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