EMPRESA ELÉCTRICA QUITO S.A.

Informe de Auditoría Interna
EMPRESA ELÉCTRICA QUITO S.A.

Auditoría Número: AI-002-2012

EXAMEN ESPECIAL A LA EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO RELACIONADO CON LA NORMA 410 – TECNOLOGÍA DE LA INFORMACIÓN

Período de Revisión: Febrero/23/2012 – Mayo/31/2012

Distribución del Informe de Auditoría

Para: Presidente del Directorio de la Empresa Eléctrica Quito S.A.
Gerente General de la Empresa Eléctrica Quito S.A.
Gerente de Planificación
Director de Tecnología de Información y Comunicaciones

EMPRESA ELÉCTRICA QUITO S.A.

INFORME DE AUDITORÍA INTERNA

EXAMEN ESPECIAL A LA EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO RELACIONADO CON LA NORMA 410 – TECNOLOGÍA DE LA INFORMACIÓN

Empresa Eléctrica Quito S.A.		Fecha de Emisión:	Agosto/14/2012
Auditor Responsable:	Ing. Nikolay Trujillo A.	Equipo de Auditoría:	Dr. Mauricio Borja, CPA, CISA Ing. Fernando Guevara

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

MOTIVO

El Examen Especial a la "Evaluación del Sistema de Control Interno relacionado con la Norma 410 – Tecnología de la Información", se realizó en atención a la Orden de Trabajo OT-04-2012 del 23 de febrero de 2012 suscrita por el Auditor General de la Empresa Eléctrica Quito S.A. ("EEQSA"). Este examen especial corresponde a la categoría de Auditorías Planificadas Nuevas que consta en el Plan de Auditoría Interna para el año 2012, dicho Plan fue aprobado por la Junta General de Accionistas mediante resolución 2012.009.J.A el 27 de junio de 2012.

OBJETIVO

Establecer si el Sistema de Control Interno implementado en la empresa en relación con los procesos de tecnología de la información, proporciona un grado de seguridad razonable, en cuanto a la consecución de objetivos relacionados con la eficiencia y eficacia de la gestión y cumplimiento de las disposiciones legales y demás normas aplicables.

ALCANCE

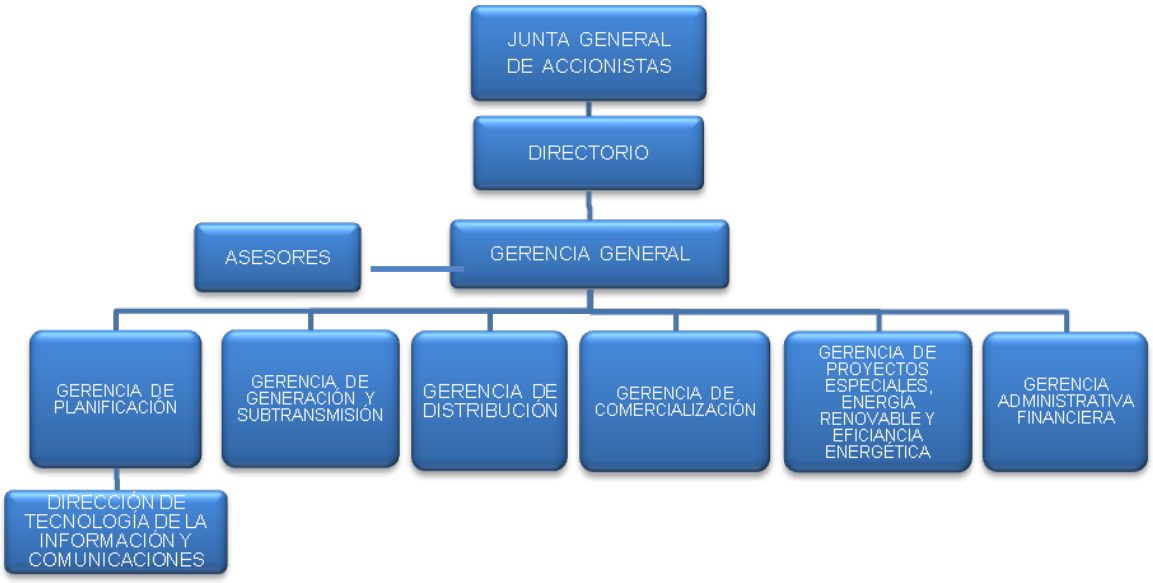
Esta auditoría cubrió la evaluación de la situación actual del Sistema de Control Interno en los procesos relacionados con Tecnología de la Información de la EEQSA, en base de la Norma de

Control Interno[1] NCI 410 – Tecnología de la Información; no incluyó el análisis de la propiedad, legalidad y veracidad de las operaciones administrativas y financieras.

ESTRUCTURA ORGÁNICA

- **Estructura Orgánica Actual**

  El Directorio de la EEQSA mediante Resolución 2011-004-D en sesión del 14 de abril de 2011, aprobó una nueva estructura organizacional que quedó de la siguiente manera:



OBJETIVOS DE LA INSTITUCIÓN

Los objetivos de la empresa que constan en el Plan Estratégico 2012-2015, son los siguientes:

- Incrementar la satisfacción de los consumidores en la calidad del producto y servicio.
- Incrementar la población con servicio.
- Incrementar el uso eficiente de los recursos.
- Incrementar la eficiencia institucional.
- Incrementar la eficiencia energética.
- Incrementar el uso de fuentes de energía alternativas.
- Incrementar la satisfacción de los grupos de actores con una gestión socialmente responsable.
- Incrementar el desarrollo del talento humano.
- Incrementar la innovación tecnológica que optimice la gestión.

[1] Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que dispongan de fondos del públicos, Acuerdo No. 39 - GG de la Contraloría General del Estado, promulgado el 1 de diciembre de 2009.

OBJETIVOS ESPECÍFICOS

Los objetivos a corto plazo relacionados con la gestión de la Dirección de Tecnología de la Información y Comunicaciones ("DTIC"), son:

- Incrementar la atención de solicitudes de TIC's en mesa de ayuda, hardware y software de estaciones de trabajo.
- Reducir el tiempo de indisponibilidad del servicio en Servidores y B/D, Aplicaciones.
- Reducir el tiempo de indisponibilidad del servicio en Redes y Comunicaciones.
- Incrementar el cumplimiento de avances de proyectos de desarrollo de Aplicaciones.
- Incrementar el nivel de actualización el Sistema de Información Geográfica.

MONTO DE RECURSOS EXAMINADOS

No aplica por el alcance y naturaleza de la evaluación realizada.

SERVIDORES RELACIONADOS

Cargo	Nombres y Apellidos
Gerente de Planificación	Eco. Justo Tobar
Director de Tecnología de Información y Comunicaciones	Ing. Jorge Morales
Jefe de Departamento de Administración de Sistemas Estratégicos (Data Center)	Ing. Alberto Belalcázar
Jefe de Departamento de Desarrollo de Sistemas Administrativos	Ing. Francisco Mena
Jefe de Departamento de Desarrollo Tecnológico de Sistemas Técnicos	Ing. Francisco Calderón
Jefe de Departamento de Comunicaciones y Soporte	Ing. Miguel Araujo
Jefe de Departamento Sistema GIS (Enc) – Dibujante 4	Ing. Francisco Bermúdez
Jefe de Sección de Desarrollo Tecnológico de Sistemas Administrativos	Ing. Susana Benalcázar
Jefe de Sección de Mesa de Ayuda (Help Desk)	Ing. Jaime Raza
Jefe de Sección de Desarrollo Tecnológico de Sistemas Técnicos	Ing. Patricia Cerón
Jefe de Sección de Administración de Seguridad Informática	Ing. Walter Carrera
Jefe de Sección de Soporte de Hardware de Estaciones de Trabajo	Ing. Bolívar Ortiz
Jefe de Sección de Soporte de Software de Estaciones de Trabajo	Ing. Wilson Castro
Ingeniero de Sistemas 2	Ing. Carlos Benavides

CONCLUSIÓN GENERAL:

Calificación del Informe: Satisfactorio (Estándar)
La Evaluación del Sistema de Control Interno relacionado con la Norma 410 – Tecnología de la Información, nos permitió determinar que la mayoría de controles internos son adecuados y están operando como es la intención. Sin embargo, existen recomendaciones para mejorar controles en relación con los siguientes asuntos: La creación del Comité Informático; el registro de software como propiedad intelectual; la ausencia de una política que regule el "acceso remoto" de computadoras personales que están en la red; la compartición del perfil de usuario de Administrador en el Sistema de Inventarios y Avalúos (SIA); la falta de políticas que regulen el uso del perfil de Administrador de computadoras personales en la red y las revisiones regulares formales de todas las cuentas de usuarios y los privilegios asociados; la implementación inconclusa de los procedimientos y medios técnicos para el uso de firmas electrónicas; no haber actualizado las políticas y procedimientos tecnológicos de retención de información respecto a la perpetuidad y recuperación de los datos; la falta de documentación de los procedimientos de seguridad para el ingreso al *Data Center* por la noche o en fin de semana; la falta de actualización de los procedimientos existentes para la administración de servicios de internet, intranet, correo electrónico ya que no regulan la gestión de sitios WEB de la empresa; la inexistencia de un procedimiento explícito respecto a la dependencia sobre personal clave; y la desactualización de los procedimientos de desarrollo de software que contemplen los casos relacionados a cambios en las disposiciones legales y normativas. Las recomendaciones para mejorar los controles internos en relación con la Norma 410 – Tecnología de la Información, requieren una pronta atención por la parte de la Gerencia.

Durante nuestro trabajo de auditoría, el personal inmerso en los procesos de Tecnología de la Información de la Empresa Eléctrica Quito S.A., nos proporcionó su apoyo total. Nos gustaría agradecer a las áreas mencionadas por su valiosa cooperación.

A continuación encontrará el informe detallado de Auditoría Interna que contiene todas nuestras observaciones, conclusiones y recomendaciones, para que se tomen las acciones pertinentes.

Atentamente,

ORIGINAL FIRMADO POR NIKOLAY TRUJILLO A.

Ing. Nikolay Trujillo A., MBA, CIA, CRMA, CPA
AUDITOR GENERAL

EMPRESA ELÉCTRICA QUITO S.A.

VISIÓN GENERAL DE LAS OBSERVACIONES DE AUDITORÍA

No.	Título	Personas Responsables de Implementar la Recomendación	Fecha Tope
1.	El Comité Informático no ha sido creado. (410-16)	Gerente General.	31/12/2012
2.	Registro de software como propiedad intelectual. (410-07,15)	Gerente de Planificación, Director de TIC.	31/12/2013
3.	No existe una política que regule el "acceso remoto" de computadoras personales en la red. (410-12,4)	Gerente de Planificación, Director de TIC.	31/12/2012
4.	En el sistema SIA el perfil de usuario de Administrador está siendo compartido (410-12 y 410-02)	Gerente de Planificación, Director de TIC.	31/10/2012
5.	No existen políticas que regulen el uso del perfil de administrador de computadoras personales en la red y para revisiones regulares formales de todas las cuentas de usuarios y los privilegios asociados. (410-12,4)	Gerente de Planificación, Director de TIC.	31/10/2012
6.	La implementación de los procedimientos y medios técnicos para el uso de Firmas Electrónicas no se ha concluido. (410-17)	Gerente de Planificación.	31/12/2012
7.	Las políticas y procedimientos tecnológicos de retención de información respecto a la perpetuidad y recuperación de los datos no han sido actualizados. (410-10,3)	Gerente de Planificación, Director de TIC.	30/07/2013
8.	Los procedimientos de seguridad para el ingreso al Data Center por la noche o en fin de semana no han sido documentados. (410-10,8)	Gerente de Planificación, Director de TIC.	31/12/2012
9.	Los procedimientos existentes para la administración de servicios de internet, intranet, correo electrónico, no están	Gerente de Planificación, Director de TIC.	31/12/2012

No.	Título	Personas Responsables de Implementar la Recomendación	Fecha Tope
	actualizados ya que no especifican la gestión de sitios WEB de la entidad. (410-14,1)		
10.	Falta un procedimiento explícito respecto a la dependencia sobre personal clave. (410-02,5)	Gerente de Planificación, Director de TIC.	31/12/2012
11.	Los procedimientos de desarrollo de software no han sido actualizados para contemplar los casos relacionados a cambios en las disposiciones legales y normativas. (410-09,1)	Gerente de Planificación, Director de TIC.	31/08/2012

CAPÍTULO II

RESULTADOS DE LA EVALUACIÓN

Auditoría Interna realizó la Evaluación de Control Interno de la Norma 410 – Tecnología de la Información, que forma parte de las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que disponen de Recursos Públicos, que fueron emitidas por la Contraloría General del Estado mediante Acuerdo No. 39-CG del 16 de noviembre del 2009 y promulgadas en el Registro Oficial No. 78 de 1 de diciembre de 2009.

El Procurador de la EEQSA en memorando No. 1418 del 9 de agosto del 2011, dirigido al Auditor General respecto a la "Consulta sobre Aplicación Acuerdo No. 39 Contraloría General del Estado" en la EEQSA, indicó lo siguiente:

> "*… Procuraduría considera que las Normas de Control Interno para las Entidades, Organismos del Sector Público y Personas Jurídicas de Derecho Privado que disponen de Recursos Públicos, son de aplicación obligatoria en la Empresa Eléctrica Quito S.A., para lo cual, la Unidad de Auditoría Interna, se encargará de realizar el control previo y concurrente, tal como lo señala la Ley Orgánica de Empresas Públicas*".

A fin de realizar la Evaluación de Control Interno de Tecnología de la Información, Auditoría Interna tomó como criterios la Norma 410 – Tecnología de la Información y el Modelo COBIT (Objetivos de Control para la Información y Tecnologías Relacionadas - *Control Objetives for Information and Related Technologies*).

Las Normas que se evaluaron de la Norma 410 son las siguientes:

- Norma 410-01 Organización informática
- Norma 410-02 Segregación de funciones
- Norma 410-03 Plan informático estratégico de tecnología
- Norma 410-04 Políticas y procedimientos
- Norma 410-05 Modelo de información organizacional
- Norma 410-06 Administración de proyectos tecnológicos
- Norma 410-07 Desarrollo y aplicación de software aplicativo
- Norma 410-08 Adquisiciones de infraestructura tecnológica
- Norma 410-09 Mantenimiento y control de la infraestructura tecnológica
- Norma 410-10 Seguridad de tecnología de la información
- Norma 410-11 Plan de contingencias
- Norma 410-12 Administración de soporte de tecnología de información
- Norma 410-13 Monitoreo y evaluación de los procesos y servicios
- Norma 410-14 Sitio WEB, servicios de internet e intranet
- Norma 410-15 Capacitación Informática
- Norma 410-16 Comité informático
- Norma 410-17 Firmas electrónicas

De la evaluación a las normas descritas se determinaron las siguientes observaciones:

1. El Comité Informático no ha sido creado. (410-16).

La EEQSA no ha creado el Comité Informático. Actualmente, la Dirección de Tecnología de Información y Comunicaciones y los dueños de los procesos de cada área realizan reuniones en las cuales se toman las decisiones relacionadas con la tecnología de la información de sus respectivas áreas. Existe un documento denominado *"Creación Comité de Tecnología"*, generado por la DTIC, en el que se definen los siguientes aspectos: conformación, objetivo y funciones generales del Comité, sin embargo éste documento no ha sido revisado ni aprobado por los niveles jerárquicos correspondientes, por lo que tampoco se encuentra declarado en el Sistema de Gestión de la Calidad de la Empresa.

La Norma de Control Interno 410-16 referente a Comité Informático, determina que:

> *"Para la creación de un comité informático institucional, se considerarán los siguientes aspectos:*
>
> - *El tamaño y complejidad de la entidad y su interrelación con entidades adscritas"*
>
> - *La definición clara de los objetivos que persigue la creación de un comité de informática… tiene como propósito fundamental definir, conducir y evaluar las políticas internas para el crecimiento ordenado y progresivo de la tecnología de la información y la calidad de los servicios informáticos, así como apoyar en esta materia a las unidades administrativas que conforman la entidad."*

Según explicación verbal del Director de Tecnología de Información y Comunicaciones una de las causas para que hasta la presente fecha no se haya creado el Comité Informático de la EEQSA es que el documento denominado *"Creación Comité de Tecnología"* no ha sido sometido a los procesos de revisión y aprobación correspondientes.

La no creación del Comité Informático no permite asegurar el alineamiento entre el Plan Estratégico de la organización con las actividades que desarrolla el área de Tecnología ni la imputabilidad en la ejecución de las funciones y responsabilidades del Comité.

Conclusión

El no haber creado un Comité Informático para la Empresa no asegura el adecuado alineamiento entre el Plan estratégico de la organización y las actividades que realiza el área de Tecnología.

Recomendación

El Gerente General creará el Comité Informático para lo cual servirá de base el documento denominado "Creación Comité de Tecnología" desarrollado por la DTIC; también coordinará con las distintas gerencias la designación y las funciones de lo miembros de dicho Comité, y dispondrá su funcionamiento inmediato.

Responsable: Gerente General

Fecha tope de cumplimiento: 31 de diciembre de 2012.

2. Registro de software como propiedad intelectual. (410-07,15).

El software que ha sido desarrollado por la EEQSA no se encuentra registrado como propiedad intelectual, en el organismo competente.

La Norma de Control Interno 410-07 denominada "Desarrollo y Adquisición de Software Aplicativo" estipula que:

> *"La unidad de tecnología de información regulará los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos. Los aspectos a considerar son:*
>
> *9. Los derechos de autor del software desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente. Para el caso de software adquirido se obtendrá las respectivas licencias de uso."*

Lo comentado se debe a anteriormente no existió una norma que obligue a la EEQSA el registro como propiedad intelectual del software desarrollado por la Empresa, lo cual puede ocasionar el riesgo de que éste sea plagiado por otras organizaciones.

Conclusión

Al no estar registrado como propiedad intelectual el software desarrollado por la EEQ S.A. no se podría asegurar sus derechos sobre éste.

Recomendación

El Gerente General dispondrá al Gerente de Planificación, y éste a su vez al Director de Tecnología de la Información y Comunicaciones, que coordine con el Procurador de la EEQSA el asesoramiento legal respectivo para el registro en el organismo competente del software de la EEQSA, para lo cual realizará un análisis e identificación previa del software que cumpla con los requisitos correspondientes.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 de diciembre de 2013.

3. No existe una política que regule el "acceso remoto" de computadoras personales en la red. (410-12,4).

No existe una política que regule el "acceso remoto" cuando se usa herramientas como Virtual Network Computing (VNC) de computadoras personales en la red, lo que se pudo evidenciar en una muestra revisada a varios equipos del área de Auditoría, en los que no se encuentra configurada la opción de aceptación de inicio del monitoreo o notificación de conexión.

La Norma de Control Interno numeral 410-12 relacionada con "Administración de Soporte de Tecnología de Información" menciona que:

> *"La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.*
>
> *Los aspectos a considerar son:*
>
> *4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información."*

Lo comentado se debe a que no se consideró incluir una política que regule el "inicio de monitoreo" que incluya el parámetro de "notificar conexión" en las computadoras personales de la red, existiendo el riesgo de que la seguridad de los computadoras personales sean vulneradas y la confidencialidad quede comprometida, en el caso de que los usuarios de la red sean monitoreados sin saberlo.

Conclusión

El que no exista una política que regule el "acceso remoto" cuando se usa herramientas Virtual Network Computing (VNC), compromete la confidencialidad y seguridad de la información de las computadoras personales.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de la Información y Comunicaciones que establezca políticas y procedimientos que regulen el "acceso remoto" cuando se usa herramientas de monitoreo, para computadoras personales en la red.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 de diciembre de 2012.

4. En el sistema SIA el perfil de usuario de Administrador está siendo compartido (410-12 y 410-02).

En el Sistema de Inventarios y Avalúos (SIA) el perfil del usuario de Administrador y su contraseña están siendo compartidos por los Operadores, lo cual no garantiza una adecuada segregación de funciones.

La Norma de Control Interno 410-12 denominada Administración de Soporte de Tecnología de la Información, en su numeral 2 estipula lo siguiente:

> *"Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad."*

Adicionalmente, la Norma de Control Interno 410-02 referente a Segregación de funciones menciona que:

> *"Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo.*
>
> *La asignación de funciones y sus respectivas responsabilidades garantizarán una adecuada segregación, evitando funciones incompatibles. Se debe realizar dentro de la unidad de tecnología de información la supervisión de roles y funciones del personal dentro de cada una de las áreas, para gestionar un adecuado rendimiento y evaluar las posibilidades de reubicación e incorporación de nuevo personal."*

La situación descrita se debe a que desde que se adquirió e implementó el sistema SIA, el responsable del sistema no consideró el mantener una adecuada segregación de funciones, mediante la asignación de diferentes perfiles de usuario para los operadores sin que se otorguen los permisos de administrador; esta situación conlleva el riesgo de un inadecuado uso del sistema, luego del cual no se pueda imputar al responsable específico.

Conclusión

El que se esté compartiendo el perfil de usuario de administrador y su contraseña del sistema SIA no permite una adecuada segregación de funciones existiendo el riesgo que pueda darse un uso inadecuado al sistema.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de Información y Comunicaciones, que se definan en el sistema SIA los diferentes perfiles de usuario, de acuerdo a los requerimientos del dueño del proceso.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones.

Fecha tope de cumplimiento: 31 de octubre de 2012.

5. No existen políticas que regulen el uso del perfil de administrador de computadoras personales en la red y para revisiones regulares formales de todas las cuentas de usuarios y los privilegios asociados. (410-12,4).

No existe una política que regule el uso del perfil de administrador para los usuarios de computadoras personales en la red, lo cual se evidenció al verificar los perfiles de usuario de algunos computadores personales de la red. La Dirección de Tecnología de la Información y Comunicaciones ha estado otorgando dicho perfil, según los requerimientos de los usuarios.

Adicionalmente no se ha definido una política para revisiones regulares formales de todas las cuentas de usuarios y los privilegios asociados, a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información. Actualmente la Dirección de Tecnología de la Información y Comunicaciones, realiza revisiones ocasionales e informales de las cuentas de los usuarios y privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información, pero no se ha establecido un procedimiento escrito que obligue a realizar estas revisiones de manera formal y periódica por parte de los administradores responsables de cada uno de los sistemas.

La Norma de Control Interno 410-12 denominada "Administración de soporte de tecnología de información" estipula que:

> *"La unidad de tecnología de información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.*
>
> *Los aspectos a considerar son:*
>
> *4. Revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.*
>
> *5. Medidas de prevención, detección y corrección que protejan a los sistemas de información y a la tecnología de la organización de software malicioso y virus informáticos."*

Lo comentado se debe a que no se ha considerado la inclusión de políticas que regulen el uso del perfil de administrador y para revisiones regulares de todas las cuentas de usuarios y privilegios asociados, existiendo el riesgo de que se instale software no autorizado, malware o que se altere indebidamente la configuración del computador personal; así también existe el riesgo de que se presenten brechas entre los permisos y accesos

autorizados por los dueños de los procesos y los permisos y accesos actuales que tengan los usuarios de los sistemas de información.

Conclusión

El no contar con políticas que regulen el uso del perfil de administrador para los usuarios de computadoras personales en la red y para revisiones regulares de todas las cuentas de usuarios y los privilegios asociados, puede ocasionar la instalación de software no autorizado, malware o que se altere a la configuración del computador personal y que se presenten brechas entre los permisos y accesos autorizados por los dueños de los procesos y los permisos y accesos actuales que tengan los usuarios de los sistemas de información.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de la Información y Comunicaciones que establezca políticas y procedimientos escritos que regulen: a) el uso del perfil de administrador para los usuarios de computadoras personales en la red y b) las revisiones regulares de todas las cuentas de usuarios y los privilegios asociados, a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 de octubre de 2012.

6. La implementación de los procedimientos y medios técnicos para el uso de Firmas Electrónicas no se ha concluido. (410-17).

La EEQSA ha buscado los mecanismos para la implementación de los procedimientos y medios técnicos necesarios para permitir el uso de Firmas Electrónicas, sin embargo la implementación de esta herramienta tecnológica no ha concluido.

La Norma de Control Interno 410-17 referente a Firmas Electrónicas estipula que:

> *"Las entidades, organismos y dependencias del sector público, así como las personas jurídicas que actúen en virtud de una potestad estatal, ajustarán sus procedimientos y operaciones e incorporarán los medios técnicos necesarios, para permitir el uso de la firma electrónica de conformidad con la Ley de Comercio Electrónico, Firmas y Mensajes de Datos y su Reglamento"*

El Gerente de Planificación de la EEQSA con e-mail del 26-jul-12 informó a Auditoría lo siguiente:

"La Gerencia de Planificación ha realizado acciones con personeros de la Secretaría Nacional de la Administración Pública SNAP, a efecto de lograr nuestra incorporación al Proyecto Gobierno por Resultados – GpR, quienes nos manifestaron que eso solo será posible cuando la EEQ termine la fase de transición de S. A. a Empresa Pública."

"Así también con el Sistema de Gestión Documental, que tiene a cargo la gestión del sistema documental denominado QUIPUX, y el cual se gestiona con el uso de firma electrónica a ciertos niveles, respecto de lo cual y por alineamiento institucional que los sustenta, también demanda de que la EEQ sea una Empresa Pública."

Esta situación no ha permitido generar las condiciones interinstitucionales que hagan posible la implantación de la Firma Electrónica en la EEQSA; por lo que existe el riesgo que no se facilite el intercambio de documentos firmados por este medio con otras entidades públicas, así como tampoco permite que se agilite con la debida celeridad la tramitación formal de documentos.

Conclusión

El no haber concluido con la implementación de los procedimientos y medios técnicos necesarios para permitir el uso de Firmas Electrónicas, no facilita el intercambio de documentos firmados por este medio con otras entidades públicas, así como tampoco la celeridad en la tramitación formal de documentos.

Recomendación

El Gerente General dispondrá al Gerente de Planificación que en coordinación con todas las Gerencias de la empresa, continúen el desarrollo de las acciones administrativas necesarias para procurar la implementación del uso de la firma electrónica en la entidad.

Responsable: Gerente de Planificación

Fecha tope de cumplimiento: 31 de diciembre de 2012

7. Las políticas y procedimientos tecnológicos de retención de información respecto a la perpetuidad y recuperación de los datos no han sido actualizados. (410-10,3).

La Dirección de Tecnología de la Información y Comunicaciones cuenta con mecanismos para asegurar el respaldo de la información histórica, pero las políticas y procedimientos tecnológicos de retención de información respecto a la perpetuidad y recuperación de los datos, no han sido actualizados documentadamente para asegurar su migración a diferentes tipos de medios y tecnologías actuales.

La Norma de Control Interno 410-10 referente a Seguridad de Tecnología de Información menciona:

"La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

3. En los casos de actualización de tecnologías de soporte se migrará la información a los medios físicos adecuados y con estándares abiertos para garantizar la perpetuidad de los datos y su recuperación;"

Lo comentado se debe a la desactualización de las políticas y procedimientos tecnológicos relacionados con la retención de información que aseguren la perpetuidad y recuperación de los datos de la Empresa, lo cual genera el riesgo de que no se puedan recuperar los datos guardados en algunos medios de almacenamiento, debido a su deterioro físico y a los cambios de tecnología.

Conclusión

La Dirección de Tecnología de la Información y Comunicaciones no ha actualizado por escrito las políticas y procedimientos tecnológicos de retención de información en lo relacionado a la perpetuidad y recuperación de los datos definidos por la Empresa, por lo que algunos datos guardados en ciertos medios de almacenamiento podrían no ser accesibles cuando se necesiten, debido al deterioro físico de los medios y a los cambios de tecnología.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de la Información y Comunicaciones, que se incorpore políticas y procedimientos tecnológicos referentes a la conservación de información que aseguren la perpetuidad y recuperación de los datos definidos por la Empresa, tomando en cuenta un análisis de costo/beneficio.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 30 de julio de 2013.

8. Los procedimientos de seguridad para el ingreso al *Data Center* por la noche o en fin de semana no han sido documentados. (410-10,8).

Debido a las necesidades operativas del *Data Center*, existen funcionarios autorizados que ingresan a este sitio en las noches o fines de semana, para solucionar problemas que se presentan en el mismo; sin embargo no existen procedimientos de seguridad escritos que regulen este ingreso.

La Norma de Control Interno 410-10 de "Seguridad de Tecnología de Información" numeral 8 estipula que:

"La unidad de tecnología de información, establecerá mecanismos que protejan y salvaguarden contra pérdidas y fugas los medios físicos y la información que se procesa mediante sistemas informáticos, para ello se aplicarán al menos las siguientes medidas:

8. Definición de procedimientos de seguridad a observarse por parte del personal que trabaja en turnos por la noche o en fin de semana."

Lo comentado se debe a que las políticas y procedimientos de seguridad que regulan el ingreso al *Data Center* no han sido documentados para los casos en que se necesite ingresar por la noche o en fines de semana, lo que puede generar incidentes de seguridad.

Conclusión

La Dirección de Tecnología de la Información y Comunicaciones no dispone de procedimientos de seguridad escritos a observarse por parte del personal que necesita ingresar por la noche o en fin de semana, por lo que eventualmente podrían producirse incidentes de la seguridad en el *Data Center*.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de la Información y Comunicaciones que se incorporen procedimientos de seguridad escritos a observarse por parte del personal que necesita ingresar por la noche o en fines de semana.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 diciembre de 2012.

9. Los procedimientos existentes para la administración de servicios de internet, intranet, correo electrónico, no están actualizados ya que no especifican la gestión de sitios WEB de la entidad. (410-14,1).

El *Procedimiento de Administración de servicios de internet y correo electrónico"* código DS.ASBD.423.PRO.06 existente que regula la administración de estos servicios no especifica la gestión de sitios WEB de la entidad; y tampoco se encuentra actualizado, tal es así que en el caso del correo electrónico se hace referencia a la herramienta Lotus Notes y no a la herramienta actual (RoundCube/ Thunderbird).

La Norma de Control Interno 410-14 referente a "Sitio Web, Servicios de Internet e Intranet", establece que:

"Es responsabilidad de la unidad de tecnología de información elaborar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB de la entidad, a base de las disposiciones legales y normativas y los requerimientos de los usuarios externos e internos."

Esto se debe a que cuando se desarrolló este procedimiento la DTIC no consideró incorporar políticas y procedimientos relacionados con la gestión de sitios WEB, lo cual puede dar lugar a una eventual mala utilización de los mencionados servicios y posibles incidentes de seguridad.

Conclusión

El no actualizar las normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB para la EEQSA puede ocasionar que se generen incidentes de seguridad.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de Información y Comunicaciones, que actualice la normativa relacionada con la instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio WEB, basados en las disposiciones legales y normativas y los requerimientos actuales de los usuarios externos e internos.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 de diciembre de 2012.

10. Falta un procedimiento explícito respecto a la dependencia sobre personal clave. (410-02,5).

La Dirección de Tecnología de Información y Comunicaciones ha desarrollado una tabla denominada "Remplazos por Competencias" en la que se han identificado los cargos claves y candidatos que remplazarían a los titulares de éstos, así como también se han valorado las competencias, sin embargo ésta no ha sido complementada con un procedimiento que instrumente la aplicabilidad de estos remplazos.

La Norma de Control Interno 410-02 referente a Segregación de Funciones menciona lo siguiente:

"Las funciones y responsabilidades del personal de tecnología de información y de los usuarios de los sistemas de información serán claramente definidas y formalmente comunicadas para permitir que los roles y responsabilidades asignados se ejerzan con suficiente autoridad y respaldo."

"La descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de tecnología de información, contemplará los deberes y responsabilidades, así como las habilidades y experiencia necesarias en cada posición, a base de las cuales se realizará la evaluación del desempeño. Dicha descripción considerará procedimientos que eliminen la dependencia de personal clave."

Cuando DTIC realizó la tabla denominada "Remplazos por Competencias" no se consideró la incorporación de un procedimiento que instrumente la aplicabilidad de estos remplazos, por lo que hay el riesgo que exista personal sobre quienes haya una excesiva dependencia por ser los únicos en tener ciertos conocimientos; exponiendo de esta manera a la organización a un vacío de estos conocimientos en caso de ausencia temporal o definitiva de ese personal.

Conclusión

No se consideró la incorporación de un procedimiento que complemente e instrumente la aplicabilidad de la tabla denominada "Remplazos por Competencias" por lo que no está asegurado que todos los puestos clave de Dirección de Tecnología de la Información y Comunicaciones cuenten con personal alterno en caso de contingencia.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste a su vez al Director de Tecnología de la Información y Comunicaciones que se complemente de manera explícita la tabla denominada "*Remplazos por Competencias*" con: a) un procedimiento que instrumente la aplicabilidad de estos remplazos y b) la denominación de los cargos de los remplazantes.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 de diciembre de 2012

11. Los procedimientos de desarrollo de software no han sido actualizados para contemplar los casos relacionados a cambios en las disposiciones legales y normativas. (410-09,1).

Actualmente existen los siguientes documentos para cuando se realizan cambios a los programas: *Procedimiento de Ingeniería del Software – Código DS.IS.751.PRO.01* y la *Metodología de Desarrollo de Sistemas*; pero éstos no han sido actualizados con procedimientos escritos relacionados al mantenimiento y liberación de software de aplicación para los casos en que ocurran cambios a las disposiciones legales y normativas.

La Norma de Control Interno 410-09 relacionada con el Mantenimiento y Control de la Infraestructura Tecnológica establece que:

"La unidad de tecnología de información de cada organización definirá y regulará los procedimientos *que garanticen el mantenimiento y uso adecuado de la infraestructura tecnológica de las entidades. Los temas a considerar son:*

1. Definición de procedimientos para mantenimiento y liberación de software de aplicación por planeación, por cambios a las disposiciones legales y normativas, por corrección y mejoramiento de los mismos o por requerimientos de los usuarios."

Cuando se realizaron los documentos anteriormente mencionados, no se contempló la incorporación de procedimientos específicos para estos casos, lo cual puede ocasionar que se generen incidentes de seguridad e incumplimiento de leyes y normas.

Conclusión

El no contar con procedimientos específicos para mantenimiento y liberación de software de aplicación para los casos en que ocurran cambios a las disposiciones legales y normativas puede ocasionar que se presenten incidentes de seguridad e incumplimiento de leyes y normas.

Recomendación

El Gerente General dispondrá al Gerente de Planificación y éste al Director de Tecnología de la Información y Comunicaciones que se actualicen los procedimientos de desarrollo de software existentes, para contemplar los casos en que por nuevas disposiciones legales y cambios a las normas se deban modificar los programas, y se incluya en los requisitos la documentación legal que respaldan los cambios.

Responsables: Gerente de Planificación, Director de Tecnología de Información y Comunicaciones

Fecha tope de cumplimiento: 31 de agosto de 2012.