TRIBUNAL SUPREMO DE ELECCIONES
AUDITORÍA INTERNA

INFORME DE SEGUIMIENTO SOBRE EL CUMPLIMIENTO DE RECOMENDACIONES DEL INFORME IC-01/06 RELACIONADO CON EL DESARROLLO DE LOS PROGRAMAS ELECTORALES REDISEÑADOS A SISTEMAS ABIERTOS

Mayo, 2007

Tabla Contenido

"INFORME DE SEGUIMIENTO SOBRE EL CUMPLIMIENTO DE RECOMENDACIONES DEL INFORME IC-01/06 RELACIONADO CON EL DESARROLLO DE LOS PROGRAMAS ELECTORALES REDISEÑADOS A SISTEMAS ABIERTOS"

1. INTRODUCCIÓN

1.1 Origen del Estudio

El presente estudio se efectuó de acuerdo con el Plan Anual de Auditoría Interna del presente año y en cumplimiento de lo dispuesto en el artículo Nº 17 de La Ley Nº 8292, Ley General de Control Interno y el aparte 2.6 del Manual de Normas para el Ejercicio de la Auditoría Interna en el Sector Público.

1.2 Objetivo del Estudio

Determinar el grado de ejecución de las recomendaciones del Informe Nº ICI-01/2006 del 20 de enero del 2006, denominado "Informe de Control Interno Relativo a la Evaluación del Cumplimiento de la Normativa Legal y Técnica Vigente en el Desarrollo de los Programas Electorales Rediseñados a Sistemas Abiertos con Énfasis en Pistas de Auditoría".

1.3 Alcance del Estudio

El seguimiento incluyó el examen de la documentación relacionada con los aspectos evaluados, mediante la aplicación de cuestionarios, entrevistas, así como pruebas sustantivas y de cumplimiento, que se llevaron a cabo en conjunto con los funcionarios desarrolladores y encargados del mantenimiento de los sistemas de información objeto de seguimiento.

Por otro lado, esta Auditoría solicitó al Lic. Fernando Víquez Jiménez, Coordinador del Programa de Transmisión de Datos y al Lic. Gerardo Hernández Granda, Jefe a.i. del Departamento de Informática y Comunicaciones, información sobre aspectos relacionados al tema.

El análisis comprendió el período que va entre el 10 de diciembre del 2006 y el 21 de marzo del 2007 y se efectuó de conformidad con lo establecido en el Manual sobre Normas Técnicas de Auditoría para la Contraloría General de la República y las Entidades y Órganos Sujetos a su Fiscalización, Ley General de Control Interno, Manual de Normas Generales de Auditoría para el Sector Público, Normas Generales de Control Interno, y Manual Sobre Normas y Técnicas de Control Interno Relativas a los Sistemas de Información Computarizados y demás normativa aplicable.

1.4 Generalidades del Estudio

La Auditoría Interna elaboró el informe de Control Interno ICI-01/2006, denominado ***"INFORME DE CONTROL INTERNO RELATIVO A LA EVALUACIÓN DEL CUMPLIMIENTO DE LA NORMATIVA LEGAL Y TÉCNICA VIGENTE EN EL DESARROLLO DE LOS PROGRAMAS ELECTORALES REDISEÑADOS A SISTEMAS ABIERTOS"*.**

El referido informe fue remitido al Tribunal el 12 de enero de 2006, mediante oficio Nº 10-A.I.-2006 y versó sobre problemas que se detectaron en la gestión de las bases de datos y riesgos de seguridad y control de los sistemas de elecciones, utilizados en los comicios del 5 de febrero del 2006 y que constituían serias debilidades en el sistema de control interno, en aspectos como los siguientes:

a. *Necesidad de establecer estatus, políticas generales, estándares y procedimientos de seguridad informática para la asignación de roles y perfiles de acceso a la bases de datos.*
b. *Necesidad de habilitar recursos y mejorar la gestión operativa y de seguridad del ambiente del sistema gestor de la bases de datos. (catalogado como punto critico de éxito para el desarrollo del proyecto).*
c. *Necesidad de implementar Pistas de Auditoría en Oracle, y*
d. *La necesidad de evaluar los riesgos y planes de continuidad.*

El informe fue acogido por el Superior en sesión ordinaria Nº 71-2006, celebrada el 7 de marzo del 2006.

Para mejor comprensión por parte del lector, se ha procurado identificar el grado de cumplimiento de las recomendaciones, de acuerdo con la siguiente denominación:

- **Ejecución Satisfactoria (E.S.)**: Significa que se alcanzó el propósito de la recomendación.

- **Ejecución Aceptable (E.A.):** Significa que se hizo lo posible por alcanzar el propósito de la recomendación, pero no se logró en forma total, por factores externos.

- **Ejecución Insatisfactoria (E.I.):** Significa que no se ha alcanzado el propósito de la recomendación.

- **Pendiente (P):** Significa que no se ha ejecutado la recomendación.

1.5 Labor de seguimiento realizada por la Auditoría Interna

Esta Auditoría Interna emprendió algunas acciones, entre ellas la remisión de oficios con el propósito de verificar avances de proceso, se llevaron a cabo reuniones con el personal del DTIC, por medio de trabajo de campo que consistió en evaluar los sistemas de elecciones, entrevistas a los programadores y diseñadores, así como personal de gestión de las diferentes áreas del DTIC.

Lo anterior, con el propósito de monitorear y dar seguimiento oportuno de las acciones que debería estar emprendiendo la Administración en su labor de cumplir con las recomendaciones objeto de estudio.

Algunas de las acciones e iniciativas de esta Auditoría Interna están materializadas en los siguientes documentos:

- Oficio Nº 46-A.I.-2006 de fecha 23 de febrero del 2006, en donde se le brinda un amplio informe a los señores Magistrados sobre el cumplimiento oportuno de las recomendaciones del informe ICI-01/06, dando énfasis a la estimación de daños y perjuicios por los incumplimientos y por otro lado sobre la oportunidad de confirmar la congruencia que debe existir en los informes sobre el avance de los cumplimientos que el DTIC brindó en su oficio Nº 111 DTIC del 25 de enero del 2006.

- Oficio Nº 87-A.I.-2006 de 27 de marzo del 2006, en respuesta a la Señora y Señores Magistrados sobre el supuesto desacato por parte de esta Auditoría Interna para elaborar el Plan de Acción, por cuanto las competencias de la auditoría en este aspecto están reguladas por el ente Contralor.

- Correo electrónico enviado al Lic. Gerardo Hernández Granda Jefe a.i. del DTIC de fecha 4 de septiembre del año 2006, con copia al Lic. Fernando Víquez Jiménez, Director Ejecutivo, mediante el cual se solicitó información sobre el resultado de las acciones de mejora a los programas electorales.

- Oficio Nº 18-A.I.-2007 de 12 de febrero del 2007, con el cual se le solicita al Lic. Hernández Granda, la entrega del Plan de Acción actualizado y que informe sobre las recomendaciones que no incluyo en su pasado plan.

1.6 Comunicación verbal de resultados

En reunión celebrada el día 17 de Mayo del 2007, en la sala de juntas del DTIC, se comunicaron los resultados del presente informe a la Licda Patricia Chacón Jiménez Sub-Jefe a.i. del DTIC y el Lic. Erick Sánchez Del Valle, encargado del Área de Sistemas DTIC.

2 RESULTADOS

2.1 Grado de ejecución de las recomendaciones

De conformidad con la evaluación, el estado de cumplimiento de las recomendaciones es el siguiente:

- De las recomendaciones referidas a los puntos Nos. 4.1.2, 4.1.3, 4.1.4, 4.1.8, 4.1.9, 4.2.1., 4.2.2, 4.2.3, 4.3.1, 4.3.2, 4.3.3, 4.3.4, 4.4.3 (para un total de 13), se determinó que éstas fueron ejecutadas en forma satisfactoria.

- Las que corresponden a los puntos Nos 4.1.5, 4.4.2 y 4.4.4 (para un total de 3), se determinó un grado de ejecución aceptable.

- La recomendación 4.1.7 presenta un grado de ejecución insatisfactorio.

- Las recomendaciones expuestas en los puntos Nos 4.1.1, 4.1.6, 4.1.10 y 4.4.1 (para un total de 4), se determinó que se encuentran pendientes de ejecución.

En el Anexo Nº 1 se presenta un detalle de las recomendaciones antes indicadas, así como el respectivo comentario de esta Auditoría, con el propósito de dejar constancia de las razones que justifican el grado de cumplimiento que se da a cada una de las recomendaciones.

2.2 Análisis cuantitativo sobre el grado de cumplimiento de las recomendaciones.

Como resultado del seguimiento de las recomendaciones cumplidas del informe de cita, se puede apreciar lo siguiente:

a. De la totalidad de las recomendaciones, trece presentan en estado de Ejecución Satisfactorio (E.S), lo que representa un 61% de cumplimiento.

b. En estado de Ejecución Aceptable (E.A.) tres recomendaciones s encuentran en esa condición, lo que en función del total de las recomendaciones representan un 14%.

c. Las recomendaciones en estado de Ejecución Insatisfactorio (E.I.) representan un 6% de todas las recomendaciones emitidas.

d. En Estado Pendiente (P) aún se presentan cuatro recomendaciones, las cuales representan un 19% del total.

2.3 Recomendaciones pendientes de ejecución

Con el propósito de establecer la relación que existe entre el total de recomendaciones que se encuentran pendientes de ejecución (8) con respecto a cada uno de los puntos citados en este anexo, obtenemos los siguientes resultados:

- En Ejecución Aceptable (E.A.) se encuentran tres recomendaciones las cuales significan un 37.5%.
- En Ejecución Insatisfactoria (E.I.) se presenta una recomendación, para un 12.5%.
- Dentro de las recomendaciones pendientes (P) existen cuatro, lo que representan un 50%.

Los detalles sobre lo expuesto en este aparte, así como en los apartes 2.2 y 2.3 se pueden apreciar en el Anexo Nº 2 del presente informe.

2.4 Acciones adoptadas por el Departamento de Tecnologías de Información y Comunicaciones.

En el Anexo Nº 3 se detallan las Recomendaciones sujetas a cumplimiento, una descripción del tema central, así como el comentario sobre cada una de éstas, de

conformidad con el criterio del DTIC (excepto en lo que se refiere a la recomendación 4.1.6., debido a que por un error del informe del DTIC se omitió).

2.5 Valoración de Riesgo

Al efecto se realizó una valoración de riesgo del Sistema de Transmisión de Datos, para lo cual se utilizó la herramienta de entrevista preliminar y cuestionario con preguntas a los encargados del DTIC. Los resultados al efecto se presentan en el Anexo Nº 4.

2.6 Resultados del Seguimiento de Auditoría

2.6.1 Falta de procesos de gestión y valoración de riesgos en tecnologías de información

Esta recomendación se encuentra pendiente de ejecución, por cuanto no se evidenció el cumplimiento sobre la necesidad de realizar una valoración del riesgo en TI, principalmente por las debilidades detectadas en el tratamiento de errores, en la asignación de perfiles y roles y en la documentación sobre aspectos de seguridad en las Bases de Datos.

En el oficio Nº DTIC-266-2007 de 12 de febrero del 2007, página Nº 7, se expresa en relación con este punto lo siguiente:

> *"Valoración de riesgo de los procesos implementada (con copia de la metodología usada y su resultado). En cuanto a este aspecto se reitera lo expuesto en los objetivos departamentales sobre lo planeado a ejecutar por este Departamento en cuento a la aplicación del SIVAR en el segundo semestre del presente año y, posiblemente, primer semestre del año 2008, dependiendo obviamente de las disponibilidad del tiempo del recurso profesional - técnico de este Departamento".*

Es importante valorar la necesidad de implantar un sistema de valoración de riesgo en los sistemas electorales o en cualquier sistema que se implante, tal y como se formuló en el informe de control interno No. ICI-01/2006 que nos ocupa, el cual fue aprobado en su oportunidad por el Tribunal en sesión ordinaria Nº 71-2006, celebrada el 7 de marzo del 2006.

Lo que se busca es minimizar el riesgo y aumentar la eficiencia de los sistemas de información. Una adecuada valoración de riesgos debería involucrar la comparación de los costos en que podría incurrir la institución ante la ocurrencia de un evento desfavorable, contra los costos de implantar los controles requeridos para minimizar la posibilidad de que ocurra tal evento, o para minimizar los costos resultantes del impacto de la ocurrencia de una situación adversa.

Este proceso puede abarcar todas las actividades relacionadas con tecnologías y sistemas de información, así como sus riesgos asociados.

Al respecto, es preciso indicar que el DTIC no cuenta con los procesos preventivos, sistemáticos de gestión, estudio y análisis de riesgos, que permitan identificar tales hechos y sus consecuencias perjudiciales ante un evento de naturaleza desfavorable. Asimismo, se carece de controles que permitan controlar y minimizar los efectos negativos.

Cabe mencionar que en su oportunidad, cuando se expuso a los funcionarios del DTIC el informe de control interno original, se les mostró y proporcionó una metodología de riesgos como herramienta para cumplir con esta recomendación.

2.6.2 Necesidad de incrementar las medidas de seguridad en los procesos basados en tecnologías de información

Se evidenció, mediante el análisis de las pistas de auditoría del sistema Sinóptico, que el perfil de usuario del Lic. Gilberto Gómez Guillén, usuario encargado del sistema, ha sido usado en forma incorrecta. Según se constató en las bitácoras, este perfil se uso en forma simultánea en dos equipos o terminales ubicadas en diferentes oficinas, sin existir restricción alguna.

Al respecto, se determinó que para ingresar al sistema se usa como perfil de usuario el número de cédula del Sr. Gómez y que la clave de acceso (password), también es el número de cédula.

Además, se comprobó que los técnicos desarrolladores de la aplicación del sistema, realizan operaciones como carga de datos y consultas con el perfil del Sr. Gómez Guillén. Sobre el particular ver copias de las bitácoras en el Anexo Nº 5.

Ante esta situación, esta Auditoría Interna solicitó al DTIC información que validara el cumplimiento de la recomendación Nº 4.1.6 sobre la definición de la política de seguridad con oficio Nº 18-A.I.-2007 de 22 de enero del 2007. Sin embargo, la respuesta brindada[1] para cumplir con este extremo no reúne las condiciones propias de una política debidamente documentada, aprobada y comunicada a los funcionarios de la institución que tienen a cargo algún tipo de acceso a sistemas institucionales.

[1] Nota DTIC-266-2007 de fecha 12 de febrero del 2007, del Licda. Armenia Masís Soto. DTIC. Página No. 10.

Cabe señalar que respecto al uso de las claves de acceso a los sistemas de información la Ley de Administración Financiera de la República y Presupuestos Públicos en el Artículo 111- Delito informático indica:

> *"…Cometerán delito informático, sancionado…….c) Facilitar a terceras personas el uso del código personal y la clave de acceso asignados para acceder a los sistemas…"*

Esta problemática podría originarse por la falta de una directriz o control automático para obligar al cambio periódico de las contraseñas de los usuarios, una política que responsabilice al usuario de garantizar la confidencialidad de las claves de acceso a los sistemas institucionales, la política o directriz de que todo sistema tenga habilitada una función que permita asignar un período de vigencia y caducidad que inhabilite automáticamente las contraseñas.

Lo anterior eventualmente puede atribuirse a una problemática de gestión y debilidad en el ejercicio del control interno informático.

Asimismo, eventualmente se podrían vulnerar los procesos de control interno informático, provocando el riesgo de que personas no autorizadas tengan acceso a los archivos de datos y a los programas de los SIC puestos en operación para el procesamiento de datos y efectuar cambios no autorizados a los datos o información procesada. A esto hay que agregar que si el usuario permite el uso de su perfil y claves de acceso a personas ajenas a él, está vulnerando el sistema de control interno y permitiendo un eventual uso indebido del sistema que es responsable.

Por lo anteriormente indicado, es de suma importancia definir una adecuada política de seguridad sobre el uso de las claves de acceso a los sistemas, ésta no sólo debe estar por escrito, sino que debe ser aplicada por el personal del DTIC.

2.6.3 Definir una política sobre el Control de los perfiles para que sea administrado por el usuario dueño de los datos

El punto al que se refiere esta condición es el 4.1.10 del informe de marras. Ante esta recomendación el DTIC no aportó una solución alterna a la recomendación que satisfaga lo requerido por esta Auditoría Interna. En oficio Nº 266-2007 de fecha 12 de febrero del año en curso, indica:

> *"En relación con esta recomendación se considera que el Control de los Perfiles no debe ser administrado en su totalidad por el dueño de los datos."*

Si bien es cierto el control de los perfiles no puede ser administrado en su totalidad, como es lo deseado el DTIC debería establecer las pautas sobre las cuales debería ser "administrado en parte", siempre y cuando se reúnan las condiciones requeridas por el Área de Seguridad TIC.

Para conseguir una seguridad efectiva y completa de los recursos informáticos y activos de información, es imprescindible delimitar las funciones y definir las responsabilidades de quienes lo utilizan.

Hay que tomar en consideración que recursos informáticos y activos de información son propiedad de la institución, pero es necesario delegar en los actores que desempeñan las distintas funciones en la protección y asignar a cada uno de ellos sus responsabilidades. Este proceso es de extrema importancia, ya que de él dependerán todas las Políticas y Normas de Seguridad desarrolladas por la institución.

Según la normativa estándar de seguridad ISO 17799 cada uno de los recursos informáticos y activos de información han de tener asignado un propietario que

actuará siempre por delegación de la dirección de la institución y será responsable de su protección.

En términos de seguridad, el propietario es el único que organizativamente tiene la responsabilidad de mantener operativos sus recursos informáticos y activos de información, determinar su criticidad y clasificación, establecer los requerimientos de protección y conceder o eliminar derechos de acceso a los usuarios.

2.6.4 Ausencia de un adecuado cronograma de pruebas y simulacros, que incluya las técnicas, integración y simulacros del un plan de contingencias

No se aportó documentación sobre el cumplimiento del cronograma de pruebas y simulacros (excepto del sistema de Transmisión de Datos) de la recomendación 4.4.1., del informe de control interno original.

Es conveniente que se considere la normativa que le atribuye al DTIC, entre otras cosas; dictar políticas para la priorización en el desarrollo de los sistemas.[2] Estas debían incluir las técnicas, integración y simulacros (Plan de contingencia).

Al respecto, el DTIC aduce en oficio Nº 266, de 12 de febrero del 2007, que esta tarea fue responsabilidad de los diferentes programas de elecciones.

> *"(…) el guión de pruebas y los datos a utilizar en las mismas fue responsabilidad de cada uno de los programas electorales,.."*

[2] Declaración interpretativa de la norma 302.04 Políticas relativas al SIG, del Manual de Normas técnicas de Control Interno Relativas a los SIC, CGR.

Es pertinente manifestar que, la inexistencia de dichos planes constituye un riesgo potencial para la continuidad de la operación normal de la institución en cuanto a los procesos y sistemas de elecciones, ya que en caso de producirse una contingencia en el suministro normal de energía, o la ocurrencia de cualquier otro tipo de siniestro, que podría ocasionar no sólo problemas de perjuicio económico para la institución, sino alguno de carácter legal, debido a la importante función que cumple esa entidad en el control del proceso electoral, por mandato constitucional.

3 CONCLUSIÓN

Como resultado del estudio de seguimiento de las principales operaciones y seguridad de la información de los sistemas de elecciones, contenidas en el informe ICI-01/06, esta Auditoría estima que las situaciones que se derivan de las recomendaciones pendientes de implementación evidencian fallas en los controles generales de las facilidades informáticas, violación de criterios de confidencialidad, integridad y disponibilidad del servicio, como lo es el caso de las claves de acceso del perfil del Lic. Gómez Guillén, en el sistema Sinóptico y la falta de habilitación de controles del sistema de base, que aunque se ha avanzado mucho en su documentación, evidencia falta de acciones importantes, como por ejemplo la divulgación y ejecución de las mismas.

Merece especial atención el hecho de que el Encargado de Seguridad TIC, sólo estuviera a cargo de las políticas y supervisión de la seguridad informática en el programa o sistema de Transmisión de Datos y no en los demás, según lo manifestó en la entrevista llevada a cabo. Ver Anexo No. 6 (Entrevista con funcionarios del DTIC).

Esto significa un alto riesgo para la institución, porque no propicia o facilita la implantación de políticas de seguridad informática, procedimientos uniformes de asignación de derechos de acceso, y contar con mecanismos para evitar ingresos no autorizados al sistema de base y aplicaciones.

La ausencia de una valoración de riesgo (recomendación 4.1.1), la definición de políticas de seguridad (4.1.6) y la documentación de cronogramas de pruebas y simulacros (4.4.1), implican un alto riesgo y deficiencias, de un sistema adecuado de control interno que permita regular las operaciones y la seguridad informática tal como lo establece el ordenamiento jurídico y las sanas prácticas administrativas.

Es importante que el DTIC, disponga de estudios para implantar una metodología de evaluación y valoración de riesgos a nivel organizacional, principalmente en materia de tecnologías y sistemas de información, para coadyuvar al fortalecimiento y la optimización del sistema de control interno de la institución.

Como parte de la responsabilidad de la administración activa con respecto al sistema de control interno y en particular, en cuanto al componente de valoración del riesgo, ésta debe emprender las acciones necesarias a efectos de establecer, mantener, perfeccionar y evaluar el sistema específico de valoración del riesgo regulado en la Ley General de Control Interno. Dicho sistema; entre otros objetivos, debe propiciar el cumplimiento de los deberes del jerarca y el titular subordinado, con respecto a la valoración del riesgo y demás componentes del sistema de control interno, y proporcionar información sobre el nivel de riesgo institucional, o por áreas, sectores, actividades, tareas u otros componentes, según la conformación del sistema.

4 RECOMENDACIÓN

Con fundamento en lo anteriormente expuesto, esta Auditoría Interna se permite recomendar se tomen las medidas pertinentes con el propósito de que a la mayor brevedad posible el Departamento de Tecnologías de Información y Comunicaciones (DTIC) implemente las recomendaciones del informe ICI-01/06 del 12 de enero de 2006 que a la fecha se encuentran pendientes, así como de aquellas que alcanzan un grado de cumplimiento aceptable e insatisfactorio, todo de conformidad con los antecedentes que al efecto se suministran en el presente.

Con el propósito de cumplir con lo dispuesto por el artículo N° 36 de la Ley General de Control Interno, N° 8292, respecto del plazo en el cual deben ser analizados los informes que remite la Auditoría a los titulares subordinados, respetuosamente se les solicita llevar a cabo el análisis del presente documento, en el curso de los próximos diez días hábiles, a partir de su recibo.

Hecho por	Asistido por
Lic. Allan Acevedo Rodríguez	Lic. Andres Blanco Chavez
Auditor de Sistemas	Auditor de fiscalizador

Auditoría Interna
Mayo, 2007