# N° ICI-01/2006

# 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 INTRODUCCIÓN

### 1.1 ORIGEN DEL ESTUDIO

En virtud de que la inversión en proyectos informáticos es cuantiosa, delicada y critica, se deben evaluar estos a la luz de la normativa vigente.

La institución enfrenta una problemática entorno al computador central A14-521, que afecta su giro de negocio y que provoca preocupación con respecto a la viabilidad de efectuar el proceso electoral del año 2006, aparte de la situación crítica de obsolescencia que enfrenta dicho equipo.

Debido a ello, la institución ha generado algunas experiencias de rediseño y desarrollo en ambientes fuera de esa plataforma. El Departamento de Tecnologías de Información y Comunicaciones, en adelante DTIC, ha generado varios esfuerzos de migración. Dicha experiencia originó una iniciativa por parte de los analistas y desarrolladores de este departamento, para el desarrollo de una *"Solución Emergente Informática para el Traslado del Sistema de Elecciones"*.

## 1.2 OBJETIVO

Evaluar el cumplimiento de la normativa legal y técnica vigente, especialmente en relación con el diseño y modelaje de los programas electorales rediseñados a sistemas abiertos, con énfasis en las pistas de auditoría.

Además, se fijaron los siguientes específicos:

- Analizar la metodología de trazas auditables,
- Aplicar la metodología de valoración de riesgo,
- Valorar la práctica de procedimientos de seguridad lógica,
- Verificar la ejecución de controles de acceso,
- Revisar las políticas de administración de bases de datos Oracle y SQL Server,
- Valorar los procedimientos de respaldo y continuidad del negocio.

## 1.3 ALCANCE

El estudio comprendió la evaluación del sistema de control interno relacionado con la propuesta para la migración de los programas electorales denominado; *"Solución Emergente Informática para el Traslado del Sistema de Elecciones,"* desarrollado por el Departamento de Tecnologías de Información y Comunicaciones (DTIC), del Tribunal Supremo de Elecciones, como una contribución asesora de la Auditoría Interna[1], con el fin de aportar conocimiento técnico en la implementación de controles de seguridad y de pistas de auditoría, para dicha solución.

1 Solicitud realizada en oficio No. 109 DTIC de fecha 24 de enero del 2005.

Se realizó también un análisis de valoración del riesgo tomando en cuenta la metodología diseñada por la Auditoría Interna como herramienta de evaluación, proporcionada por la experiencia en el proceso del diseño de los SIC de la Contraloría General de la República. (Ver Anexo N° 1)

El examen consideró la gestión realizada entre el 10 de febrero y el 10 de noviembre del 2005**,** ampliándose en aquellos casos que se consideró necesario.

Se toma como referencia el marco normativo del "Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computarizados", emitido por la Contraloría General de la República, así como investigaciones en el entorno informático, sanas prácticas para la incorporación de pistas de auditoría en sistemas de producción y los resultados de la evaluación de riesgos aplicados a este proceso (Ver Anexo N° 2).

## 1.4 LIMITACIONES DEL ESTUDIO

El período del estudio se apoyó en los procesos de desarrollo y diseño de las aplicaciones de los sistemas electorales, así como la conceptualización de las relaciones de las tablas con las Bases de Datos de los sistemas rediseñados. Es importante señalar que ante solicitudes de documentación técnica, manuales de procedimientos y políticas la administración se tuvo problemas para suplir los requerimientos de información solicitados por esta Auditoría ya que no fueron entregados en el tiempo solicitado sino que se tuvo que ampliar en varios casos.

## 1.5 DISPOSICIONES DE LA LEY GENERAL DE CONTROL INTERNO

Por considerarse de importancia, se transcribe a continuación lo dispuesto por los artículos 36, 37 y 38, así como el primer párrafo del artículo 39 de la Ley General de Control Interno (LGCI) N° 8292, en relación con los informes que emiten las Auditorías Internas:

> *"Artículo 36.—**Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*
>
> *c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*
>
> *Artículo 37.—**Informes dirigidos al jerarca**. Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.*
>
> *Artículo 38.—**Planteamiento de conflictos ante la Contraloría General de la República**. Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.*

*La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de septiembre de 1994.*

*Artículo 39.—**Causales de responsabilidad administrativa.** El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios."*

## 1.6 COMUNICACIÓN VERBAL DE RESULTADOS

Los hallazgos del presente informe fueron presentados el 11 de noviembre del 2005 al Jefe y Subjefe del Departamento de Tecnologías de Información y Comunicaciones y al Encargado del Área de Sistemas del mismo Departamento.

Con motivo de la conferencia final, se efectuaron algunas observaciones al contenido de este documento, las cuales posteriormente fueron remitidas a la Auditoría por escrito con Oficios números 2030 y 2032 DTIC, ambos del 22 de noviembre del 2005, suscritos por el Lic. Gerardo Hernández Granda, Jefe del Departamento de Tecnologías de Información y Comunicaciones. El contenido de los citados oficios fue debidamente valorado por la Auditoría e incorporado a este documento lo que se consideró pertinente.

## 1.7 GENERALIDADES DEL ESTUDIO

En los primeros meses del presente año se llevaron a cabo reuniones y se conformaron grupos de trabajo para el proceso de modelaje, diseño y análisis de los sistemas de elecciones que residían bajo un lenguaje propietario denominado "Linc" en el A-14-521 y que por los motivos ampliamente conocidos fue necesario

considerar desarrollarlos bajo un modelo de sistemas abiertos, demostrándose la capacidad del personal técnico para asumir un desarrollo de tal magnitud.[2]

Esta Auditoría Interna realizó un análisis preliminar en febrero del año recién pasado, para implementar controles y pistas en los sistemas diseñados[3] (Ver Anexo N° 5) y como parte de una labor de seguimiento sobre el desarrollo de estos sistemas, se evaluó posteriormente por medio de un análisis FODA, la viabilidad técnica de su diseño e implementación, y brindar oportunamente mayores elementos de juicio al Superior para corregir los problemas de riesgo y control que eventualmente podría asumir[4]. (Ver Anexo N° 3).

Se establecieron reuniones de trabajo con el personal técnico responsable en el diseño de los módulos del sistema de elecciones, con el fin de analizar desde un ámbito técnico la metodología de registro y auditabilidad de los sistemas.

En efecto, en el transcurso de las reuniones llevadas a cabo con la Auditoría Interna, se enfatizó sobre la importancia de minimizar los riesgos en materia de dependencia tecnológica, así como la necesidad de fomentar la capacidad de apropiación de los sistemas por parte del personal técnico, para evitar situaciones como las que está enfrentando la institución a las puertas de los comicios del 2006. Se realizó una valoración de riesgo siguiendo la metodología establecida por esta Auditoría.

La Auditoría Interna dentro de su ámbito de competencia trabajó con los analistas y programadores del DTIC en la fase de implementación de pistas y

2 Valoración Técnica contemplada en el informe No. 69-A.I.-2005 denominado “Informe de Control Interno Relativo al Peritazgo de la plataforma Tecnológica del A14-521”.

3 Entregadas al DTIC, mediante oficio No. 68-A.I-2005 de fecha 25 de Febrero del 2005.

4 Resultados del análisis FODA realizado por medio de cuestionarios a los analistas y desarrolladores del DTIC, comunicado al Superior mediante oficio No. 317-A.I.-2005 de fecha 29 septiembre del 2005.

controles de auditoría para los sistemas desarrollados, dando énfasis en los que presentaban un avance importante en su diseño y modelaje, se valoró en conjunto las necesidades de implementación de trazas auditables para alcanzar un marco de control adecuado de conformidad con las limitantes técnicas que posee el DTIC en la administración y soporte de las bases de datos Oracle.

Es importante mencionar que, la solución evolucionó partiendo de una solución contingente hasta constituir un recurso efectivo para la implementación de programas en producción y que están trabajando directamente desde el inicio en el proceso de elecciones del 2006.

Como producto del informe de peritaje de la plataforma tecnológica del A-14, página No.15 y 16, se evidenció la experiencia en rediseño a sistemas abiertos.

> *"Estas aplicaciones se encuentran en un proceso avanzado de diseño lógico y conceptual en sistemas abiertos, por funcionarios del Departamento de Tecnologías de Información y Comunicación; de estos se evidenció que se han migrado a sistemas abiertos, en lenguaje VISUAL BASIC, las siguientes aplicaciones: Sistema de miembros de mesa, Sobres lacrados, Sorteo de posiciones de partidos políticos, Abstencionismo, Preparación y acomodo por ruta de envío del material electoral (sobrantes y faltantes), Recepción del material electoral, Carátulas del Padrón Fotográfico, Delegados (impresión de carnés), Telegramas de prueba, Etiquetas, Credenciales, Contribuciones a partidos políticos, Cociente y sub-cociente. También existe la aplicación del padrón fotográfico y el proyecto de voto electrónico."*

# 2 RESULTADOS

## 2.1 NECESIDAD DE ESTABLECER ESTATUTOS, POLÍTICAS GENERALES, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA ASIGNACIÓN DE ROLES Y PERFILES DE ACCESO EN LAS BASES DE DATOS

Se comprobó en la fase de diagnóstico que el DTIC no dispone de manuales de procedimientos, políticas para la asignación de la seguridad en bases de datos, así como ausencia de la función administrativa y organizacional dedicados exclusivamente a la gestión de la seguridad relacionada con la segregación de roles y perfiles de accesos en las Bases de Datos, aprobados por el Superior, tal como lo reflejó el análisis de riesgo efectuado en este contorno.

Consecuentemente, no se inició el proyecto con la existencia de un administrador de bases de datos que tuviera la responsabilidad de implementar los procedimientos de control de acceso a las Bases de Datos y su seguridad, situación que se corrigió al alcanzar un grado de avance significativo posterior al análisis FODA.

Los analistas señalaron durante el proceso de diagnóstico, como hecho relevante, que la solución desarrollada llevará la seguridad de accesos por medio de roles en las Bases de Datos y no en la aplicación. Ante esta situación, no se encontró evidencia de un plan ni de una propuesta de estatuto completo, integrado, actualizado y vigente que normalice el ambiente para el manejo de la seguridad de accesos, asignación de roles y la administración de la seguridad de las Bases de Datos Oracle y SQL Server.

Cabe señalar como se comprobó posteriormente, todos los procesos de control y accesos a las Bases de Datos fueron trasladados a la persona encargada.

El “Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computarizados”, emitido por la Contraloría General de la República, en su norma 305.02.02, declara que se mantendrán procedimientos y medidas efectivas para la protección del hardware, del software y de los datos de los SIC.

La norma 305.03 del mismo Manual menciona que la seguridad lógica es relevante en todo su contenido a la seguridad de acceso a los SIC y restringe el acceso a los archivos de datos y programas dentro del computador; sólo se permitirá al personal autorizado.

No se evidencia un cumplimiento efectivo de la norma 303.05.07 sobre el desarrollo de la documentación de los SIC, ya que constituye una etapa clave del CVDS en su parte de seguridad de accesos y delegación de perfiles.

La estructura organizacional de los sistemas de elecciones migrados constituye un elemento sustancial para determinar el grado de importancia de las políticas que deben establecerse para suministrar una seguridad razonable sobre el uso y manejo de estos sistemas de información.

Los procedimientos de seguridad de estos sistemas y de las bases de datos en las cuales va a sustentar su función, no están apoyados sobre un estatuto de políticas de seguridad, las cuales deben someterse a la aprobación de la Administración Superior.

Dichas políticas deben contar con el apoyo de la alta administración, para garantizar su efectividad y deben ser congruentes con las normas legales y de operación vigentes.

Los procedimientos que actualmente existen no alcanzan en forma colectiva los objetivos de seguridad informática de la institución y para su elaboración se deben considerar los niveles de aplicación, los procedimientos de seguridad específicos para cada aplicación o sistema, incorporar los respectivos manuales de usuario; y a nivel general no se han generado procedimientos que contemplen la seguridad de acceso electrónico, la seguridad física, la seguridad sobre respaldos y recuperación y la planificación sobre contingencias, entre otros asuntos.

Existe 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 efectúen cambios no autorizados a los datos o información procesada.

Estos riesgos se enfocan al inadecuado acceso a sistemas, datos e información, en los que se incluyen riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información, lo que puede valorarse como un riesgo de operación.

Es necesario aclarar que no es en el sentido de incapacidad del equipo de trabajo para diseñar y programar los sistemas, sino como sinónimo de riesgo por ejercer labores que por inopia le competen a otra especialidad de las ciencias informáticas.

## 2.2 NECESIDAD DE HABILITAR RECURSOS Y MEJORAR LA GESTIÓN OPERATIVA Y DE SEGURIDAD DEL AMBIENTE DEL SISTEMA GESTOR DE BASE DE DATOS "SGBD"

Se evidenció una deficiencia en la segregación de funciones relacionada con los procesos de Administración de las Bases de Datos, tal como se refleja en el análisis de riesgos (Ver Anexo N°.2 -Valoración de Riesgo).

Los procesos de segregación de funciones, documentación para la asignación de responsabilidades y los procedimientos para el Administrador de Bases de Datos, han arrojado porcentajes críticos de riesgo, por cuanto no se han establecido en forma escrita con políticas y procedimientos, debidamente integrados en manuales formalizados por los niveles administrativos pertinentes, en relación con el acceso, aspectos de control interno sobre la confidencialidad, integridad y disponibilidad de la información; el diseño y mantenimiento de la estructura de la base de datos, incluyendo el esquema y el respectivo afinamiento; el mantenimiento de la documentación sobre el esquema lógico de la base de datos y su debida actualización.

La norma 302.08 del referido Manual sobre Normas Técnicas de Control Interno, delimita la segregación de funciones de análisis y diseño de sistemas, programación a la operación del equipo y el control de los datos.

El objetivo básico es mantener la integridad de los SIC, tal como lo establecen las normas en sus secciones 304 y 305 del respectivo manual de cita.

Puesto que no se cuenta con una función organizacional, específicamente designada para la administración de la base de datos, pese a que existe un funcionario que puede apoyar el uso del software de gestión de base de datos, se

carece de la figura administrativa formalmente designada con las funciones y responsabilidades que competen a esa tarea, específicamente para este proyecto.

Al respecto mediante nota N° 2032 DTIC de fecha 22 de noviembre del 2005, el Lic. Gerardo Hernández Granda indica:

> *"(…) que dicha funcionaria no cuenta con el tiempo necesario, para dedicarse a tiempo completo al desarrollo de la "solución Emergente" y que le falta experiencia para la creación de una base de datos desde cero, al igual que en el área de Desarrollo de Sistemas de Información y Aplicaciones falta experiencia en la elaboración de "triggers", procedimientos almacenados, capturas Web."*

Efectivamente, se comprobó con el análisis FODA desarrollado en la etapa de diagnóstico, que el personal de análisis de sistemas llevó la carga no sólo del desarrollo de los sistemas, sino también de la creación, administración y soporte de las Bases de Datos.

En la nota de cita indica el Sr. Hernández Granda lo siguiente:

> *"(…) que la Administradora de Bases de Datos ha tenido a su cargo por mucho tiempo las bases de datos Oracle, donde se encuentran las aplicaciones SICI y TIM, lo que indica que la labor se ha realizado de la mejor manera evitando ante todo posibles problemas en las bases de datos; actualmente tiene a su cargo la administración de la base de datos en producción denominada "Solución emergente", para lo cual se han realizado los procedimientos de respaldos necesarios"*

Uno de los puntos de mayor relevancia que se evidenciaron del análisis FODA y del trabajo realizado en conjunto, fue que al diseñar y desarrollar los sistemas de elecciones en una plataforma abierta, como lo es Visual Basic, Cristal

Report y con una interfase en Oracle para las Bases de Datos, estos procesos van de la mano con una adecuada administración de las tablas, mantenimiento de registros y objetos de las Bases de Datos, pero es en esta última fase donde no todos los esfuerzos están dirigidos hacia la atención de esas funciones.

Según los Técnicos entrevistados, la Administradora de Bases de Datos actual, realiza funciones y tareas que no corresponden a su perfil, situación que a nuestro criterio le resta tiempo valioso que se podría aprovechar para actualizar sus conocimientos y participar más activamente en los desarrollos.

Eventualmente se podría vulnerar los procedimientos que soporten debidamente la administración de las operaciones en la integridad de las Bases de Datos y su seguridad. La ausencia de documentación técnica hace que los recursos tecnológicos no funcionen en forma correcta y segura, con el propósito de minimizar el riesgo de fallas y proteger la estructura del software y de la información, riesgo que se incrementará conforme se acerca el período electoral.

Ante esta situación, los analistas han tenido que asumir labores fuera de su marco de acción. Las labores de administración de bases de datos son básicas y delicadas dentro del proceso de desarrollo, este riesgo eventualmente puede causar una debilidad en el manejo de las operaciones tramitadas en los sistemas, así como vulnerabilidad en el sistema de control interno.

## 2.3 NECESIDAD DE IMPLEMENTAR PISTAS DE AUDITORÍA EN ORACLE

Es necesario documentar todos los procesos de Administración de Bases de Datos con la herramienta Oracle, ya que es importante valorar todas las posibilidades "automáticas" de mantenimiento, afinamiento, monitoreo y control de las bases de datos, así como las distintas actividades que se pueden realizar en los procesos que están sujetos a ser auditados.

El "Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computarizados" emitido por la Contraloría General de la República, en su norma 303.07 delimita los procedimientos de control y rastros de las transacciones, por lo que deben incluirse en estos procedimientos.

> *"Durante el desarrollo de los sistemas de información computarizados, deberán considerarse especialmente los procedimientos y rutinas de control que sean necesarios, tanto manuales como automatizados, para que el sistema brinde información confiable para la planificación, el control y la toma de decisiones. Con tal propósito deberán incorporarse los controles establecidos en las normas de aplicación, normas adicionales y otros (…)*
> *Asimismo, los SIC deberán diseñarse de tal forma que se facilite el rastreo y la comprobación de una transacción original hacia delante a un total de resumen, o la inversa, para investigar un total resumen hacia la transacción original. (El subrayado es nuestro)."*

A partir del diagnóstico realizado del proceso de diseño de los sistemas de los programas electorales, que implementan el uso de motores de Bases de Datos Oracle y SQL Server, se comprobó como eventuales puntos críticos los controles de acceso, la captura de los datos, el control E/S, así como la necesidad de incorporar tablas "Históricas" y de "Inconsistencias" como elementos de valor actual, para generar las trazas auditables.

Si el registro de transacciones se lleva por medio de tablas históricas y no por medio del “Log” de transacciones de Oracle, es un asunto que resulta razonable debido a la falta de recursos de hardware. Es importante mencionar que existe un riesgo de llevar a cabo inadecuadas acciones a nivel de sistema sobre los objetos, dificultan las acciones de manejo de datos dirigidas a estos y la posibilidad de ser auditadas. Entre las acciones de control críticas a incluir para una eventual auditoria están las operaciones SELECT, INSERT, UPDATE, y DELETE sobre las tablas.

Es relevante entonces mencionar que si se eliminan los “Logs” (registro de transacciones en las bases de datos), estas acciones no podrían ser auditadas de forma muy similar a las auditorias de acción, por lo que generaría un riesgo eliminarlas de los procesos de producción en las Bases de Datos.

## 2.4 NECESIDAD DE EVALUAR LOS RIESGOS Y PLANES DE CONTINUIDAD

El DTIC carece de un plan de contingencias para el rediseño de los sistemas electorales, que sea completo, documentado, comunicado y que garantice la continuidad de la operación normal de los sistemas de información, especialmente cuando se presenten hechos inesperados que afecten su funcionamiento. No existe una política documental o escrita para el backup en cualquiera de las arquitecturas de hardware enmarcadas para este proyecto.

Sobre la importancia de integrar los procesos de planificación con una valoración de los riesgos que puedan obstaculizar el logro de los objetivos institucionales y la necesidad de contar con planes de continuidad del negocio, se remite a los numerales 14 de la Ley General de Control Interno, 3.1 y 3.2 del Manual de normas generales de control interno y 305.07 del Manual sobre normas técnicas de control interno relativas a los SIC.

La gestión informática debe estar enfocada al seguimiento de los procesos y el grado de cumplimiento de los planes. El artículo 110, inciso j) de la Ley de la Administración Financiera de la República y Presupuestos Públicos, establece entre los hechos que pueden generar responsabilidad administrativa, el incumplimiento total o parcial, gravemente injustificado, de las metas señaladas en los correspondientes proyectos, programas y presupuestos. La relación intrínseca que debe existir entre la planificación y el desarrollo en materia informática se sustenta en los numerales 302.03 y 303.01 del Manual sobre normas técnicas de control interno relativas a los SIC.

El DTIC no dispone de medidas formales para regular y realizar los respaldos de la información y programas de las aplicaciones computadorizadas para los sistemas rediseñados, pues se determinó la ausencia de un instructivo que establezca los procedimientos y la regularidad para realizar los respaldos, así como el detalle de las técnicas y dispositivos que deberían utilizarse y las responsabilidades sobre dichos respaldos y su custodia. (Ver comentario en página 5 de informe 2032 DTIC).

La institución puede eventualmente enfrentar el riesgo de una ruptura en los procesos internos o en el suministro de un producto/servicio. Y si no existen adecuados planes de recuperación de la información o de contingencia que establezcan un curso de acción, en el caso de que se produzcan rupturas en la provisión de servicios electrónicos, se puede incurrir en pérdida de información, en un encarecimiento de una pronta solución y en un atraso en la prestación de servicios.

# 3 CONCLUSIONES

## 3.1 SOBRE LA NECESIDAD DE ESTABLECER ESTATUTOS, POLÍTICAS GENERALES, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA ASIGNACIÓN DE ROLES Y PERFILES EN LAS BASES DE DATOS.

De los resultados de este aparte del informe se deriva que las principales operaciones de diseño, modelaje y desarrollo de los programas de elecciones rediseñados, evidencian deficiencias en cuanto a: controles generales de las facilidades informáticas, problemas de segregación de funciones y tareas incompatibles, desarrollo de transacciones sin normalización, eventual violación de criterios de confidencialidad, integridad y disponibilidad del servicio y falta de habilitación de controles del sistema gestor de Bases de Datos (SGBD), entre otras, debido a debilidades en los controles operativos y de seguridad.

Por otra parte, la evaluación del ambiente de control interno en los sistemas de información y procedimientos de registro observados, evidenció la falta de un adecuado control, documentación, asignación y registro de los roles de acceso a las bases de datos en los que se debe rastrear la fecha de creación o de ultima modificación de un registro, el responsable de la modificación, la fecha de baja lógica de un registro en general y sobre la posibilidad de rastrear todos los datos relevantes para poder llevar un seguimiento de las modificaciones efectuadas para promover su mejora y optimización.

Al momento del diagnóstico no se tenían delimitadas las responsabilidades, la propiedad y derechos de acceso por parte de los usuarios de la información y de otros activos. Se solicitó de manera formal desde el mes de marzo del 2005, una

matriz de roles y perfiles de usuario, la cual no fue remitida[5], así como información documental de relevancia para el establecimiento de estatutos, políticas, estándares y procedimientos de seguridad relativas a la asignación de roles y perfiles en las bases de datos, la cual no fue enviada a esta Auditoría.[6]

Si bien es cierto la documentación sobre los perfiles, usuarios, modelo relacional y glosario de términos fue entregada posteriormente, esta se entregó en forma incompleta mediante Oficio N°. 2030 DTIC del 22 de noviembre del 2005, (Ver Anexo N° 4), y se complementó con Oficio N° 2243 DTIC del 22 de diciembre del mismo año.

Por consiguiente, se evidenció durante el diseño y análisis de los sistemas electorales la ausencia de un marco de control de acceso y recursos de TI, sin haber establecido procedimientos de identificación y autenticación para el acceso a la información propiamente en las bases de datos, que defina el uso de niveles de acceso a la información contenida en éstas y que identifiquen ¿Quién?, ¿Qué? y ¿Cuándo?, utilizaron la información. Dicha situación se solucionó posteriormente y se comprobó con la entrevista realizada a la Administradora de Bases de Datos.

Sin embargo aún no se ha establecido un procedimiento para el uso de cuentas que contemple la requisición, establecimiento, emisión, aprobación, suspensión y eliminación de las cuentas de usuario, como mecanismos de mantenimiento de datos, según se desprende de la entrevista realizada a la DBA.

[5] Minuta No. 4, de las reuniones llevadas a cabo en el DTIC, el día 4 de marzo del presente.
[6] Oficio No.331-A.I.-2005 de fecha 24 de octubre del 2005.

### 3.2 SOBRE LA NECESIDAD DE HABILITAR RECURSOS Y MEJORAR LA GESTIÓN OPERATIVA Y DE SEGURIDAD DEL AMBIENTE DEL SISTEMA GESTOR DE BASE DE DATOS "SGBD"

El DTIC dispone de un DBA con funciones específicamente delimitadas en el manual descriptivo de puestos de dicho departamento, así como en el manual de perfiles de puestos del Departamento de Recursos Humanos. Además, la institución ha invertido grandes sumas de dinero en capacitación para solventar las necesidades en dicha especialidad.

De acuerdo con lo manifestado los técnicos en los cuestionarios elaborados como producto del análisis FODA, dicha funcionaria atiende otras funciones, lo que reduce considerablemente el tiempo que destina a esta importante labor y tampoco dispone de procedimientos escritos de operación y mantenimiento.

Al no existir la figura de un administrador de bases de datos en el equipo de trabajo, (aun teniendo una persona nombrada con ese perfil), los técnicos del DTIC han tenido que asumir funciones y actividades referentes a la administración y soporte de la Base de Datos, situación que desde el punto de vista de las sanas prácticas no es adecuada, puesto que no es posible que el personal que tiene las responsabilidades de análisis y diseño esté tomando gran tiempo para el mantenimiento de las Bases de Datos.

Por otra parte, en relación con asuntos técnicos y mediante análisis de las posibilidades el software de base de datos Oracle de los sistemas electorales, se determina que dicha herramienta posee una serie de comandos básicos para monitorear el ambiente en línea, por otro lado no se encuentra instalado un producto especializado para medir el rendimiento y apoyar el afinamiento y optimización del

funcionamiento de las bases de datos, así como para medir la degradación de las aplicaciones.

Asimismo, no se encuentran habilitadas algunas medidas de seguridad, tales como seguridad por actividad (aplicaciones), por categorías (tareas, programas), de base de datos y diccionarios de datos (en Oracle glosario de términos), cambio de clave por el usuario, vencimiento automático de claves, restricción de accesos por fecha y hora, acceso a recursos de "SGBD" desde el ambiente de lotes tanto en modo local como central, protección de programas del software, sistema operativo, programas ejecutables y fuentes de usuario.

### 3.3 SOBRE LAS PISTAS DE AUDITORÍA EN ORACLE

Debido a que las actividades a auditar se configuran de manera flexible y pueden modificarse fácilmente, la generación de pistas de auditoría debe mantener la historia de los cambios que se realizan a los datos e identificar: qué cambió, quién lo realizó y cuándo. En efecto, si estas acciones se lograran agrupar durante la auditoria, se reduce el esfuerzo administrativo necesario para establecer y mantener los valores de auditoría.

La implementación de las citadas trazas auditables, toman relevancia con la administración de las bases de datos en Oracle, de los sistemas rediseñados como motor de base, ya que no se evidenció el control de registros de modificaciones realizadas, con capacidad de grabar información necesaria para detectar incidencias o fallos, crear tablas “Históricas” y de “Inconsistencias” e incorporar un repositorio de los registros de movimiento en los procesos de objetos (como CREATE, ALTER y DROP), se obtiene gran relevancia para los procesos de control y registro de transacciones, precisos para garantizar la seguridad de los sistemas.

### 3.4 SOBRE LA EVALUACIÓN DE RIESGOS Y PLANES DE CONTINUIDAD

Esta Auditoría Interna siempre ha señalado en sus diferentes informes de control interno informático, la necesidad de disponer de una gestión integral de riesgos y planes de continuidad del negocio, lo que evita que la institución se exponga en mayor medida a los impactos que interrupciones severas en los procesos de tratamiento de la información que puedan ocasionar al margen de la plataforma tecnológica que exista.

Se debe minimizar el riesgo potencial involucrado para los sistemas electorales, con el propósito de llevar a los ciudadanos un proceso de elecciones, seguro, eficiente y eficaz, en donde se garantice la confidencialidad, integridad y disponibilidad de la información.

# 4 RECOMENDACIONES

## 4.1 PARA ESTABLECER ESTATUTOS, POLÍTICAS GENERALES, ESTÁNDARES Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA PARA LA ASIGNACIÓN DE ROLES Y PERFILES EN LAS BASES DE DATOS.

4.1.1 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.

4.1.2 Documentar la forma que tiene la base de datos de almacenar las contraseñas, porque añade nuevas opciones a la seguridad de la cuenta, por eso una de las obligaciones del DBA está en otorgar privilegios a los usuarios y clasificar los usuarios y los datos de acuerdo con la política de la organización. Las órdenes privilegiadas del DBA deberán incluir los siguientes tipos de acciones:

I. Creación de cuentas
II. Concesión de privilegios.
III. Revocación de privilegios.
IV. Asignación de niveles de seguridad.

4.1.3 Se debe ejercer el control de los movimientos para los procesos de Consulta (C), Inclusión (I), Modificación (M) y Borrado (B), mismos que deben ser valorados para el mantenimiento de las aplicaciones y su respectiva distribución a los perfiles que deberán trabajar en los sistemas de producción.

4.1.4 Implementar reglas de formato de contraseñas cifradas, ya que el resultado sería una cuenta a la que nunca se podría acceder y ninguna contraseña podría generar cifrado no válido. Considérese las cuentas y las contraseñas cifradas seleccionadas por las siguientes consultas, en los campos USERNAME y PASSWORD de la vista DBA_USER.

4.1.5 Implementar esquemas de seguridad en las Bases de Datos, así como crear una Matriz de Roles de usuarios con sus controles y permisos para generar reportes auditables.

4.1.6 Definir la política de seguridad: Es necesario definir una política de seguridad para este proyecto definido como un plan de seguridad de los sistemas de elecciones, el cual debe estar documentado y aprobado por el Superior. Cabe señalar que por más dispositivos de seguridad con que cuente la instalación, éstos no tendrán mayor utilidad si su uso no está acompañado por una política de seguridad adecuada.

La política de seguridad para este proyecto deberá especificar un conjunto de reglas de seguridad, como por ejemplo:

I. Definición de usuarios y roles.
II. Asignación de permisos por rol.
III. Usuarios administradores.
IV. Rotación de passwords

Es necesario hacer un balance entre las necesidades de nuestro negocio y los riesgos que vamos a correr en la implementación. En todas las aplicaciones Web, tenemos que focalizar gran parte del problema de seguridad en la red.

4.1.7 Establecer procedimientos de Seguridad de Red, en las siguientes áreas:

I. Identificación: proveer servicio básico de autenticación, con usuario y password.
II. Seguridad de acceso en los límites con otras redes externas, protección contra ataques de negación de servicio.
III. La necesidad de que toda red externa estará conectada a un Firewall, y en éste estarán definidas las políticas de acceso permitidas desde cada una de las redes externas.
IV. En la red perimetral se instalarán dispositivos de detección de intrusiones. Esto nos permite reaccionar en tiempo y forma a posibles ataques o mal funcionamiento de componentes de red del exterior.
V. Privacidad de datos. Aquellas transacciones que requieran mayor seguridad
VI. La implementación de políticas de monitoreo, análisis para reconocer vulnerabilidades, detectar y reaccionar ante intrusiones. Tanto los dispositivos de detección de intrusión, los scanners de vulnerabilidad y los firewalls que aplican y controlan que las políticas definidas se cumplan dan aviso, alertas y graban logs con la información necesaria para realizar el control y reaccionar en tiempo y forma ante problemas.
VII. Administración de las políticas de seguridad en forma sencilla y centralizada

4.1.8 Coordinar la auditoria de las bases de datos con la del sistema operativo, lo que facilitará la localización de problemas y la coordinación de las políticas de seguridad entre los dos entornos. Como es muy probable que los gestores del sistema no quieran ver excesivas entradas de seguimiento de auditoría,

también se propicia que el DBA analice exactamente qué acciones es más necesario auditar.

4.1.9 Documentar la metodología de certificados digitales que se ha de implantar tanto en los sistemas de elecciones como en el de transmisión de datos.

4.1.10 Que el control de los perfiles debería ser administrado por el usuario "dueño de los datos" y no por personal del DTIC.

## 4.2 ADMINISTRACIÓN DE BASES DE DATOS

4.2.1 Se recomienda implementar procedimientos y políticas granulares de control que permitan garantizar la integridad de los datos en los procesos de entrada, edición y validación de datos, que aseguren que todas las entradas se procesan a través de controles autorizados, tales como número de secuencia, totales de control, validación de la totalidad y exactitud de los datos transmitidos por vía Web, LAN o VLAN procesos críticos en las transacciones durante la transmisión de datos.

4.2.2 Se requiere de apoyo técnico experto en Bases de Datos Oracle, para minimizar los riesgos que puedan eventualmente asumirse debido a la carencia del soporte que debería proporcionar un DBA en labores como Tunning y monitoreo. Pero es esencial que si este apoyo especializado se da o se subcontrata, se debe generar una transferencia de conocimientos a la persona que se designe como capaz de seguir realizando esta labor de administración de Bases de Datos a los sistemas rediseñados. Esta medida toma mayor relevancia si se pretende migrar la parte civil.

4.2.3 Es preciso que la Administración disponga de un informe sobre las medidas que el DTIC ha considerado necesarias para mitigar este riesgo en cuanto al

desarrollo de aplicaciones con Designer, Web, creación de Triggers, procedimientos almacenados u otros objetos que se utilizan durante la programación. Por otro lado, aplicar la valoración para las labores de mantenimiento de las Bases de Datos Oracle de los programas electorales y SQL Server en el sistema de noche de elección.

## 4.3 PISTAS DE AUDITORÍA EN ORACLE

4.3.1 Implantar el cifrado de contraseñas en Oracle para evitar los riesgos de apoderarse de forma temporal de cualquier cuenta y devolverle después su contraseña original. Esta posibilidad permite convertirse en otro usuario. Si bien es cierto es especialmente útil durante la comprobación de las aplicaciones o la localización de problemas en Producción, es riesgosa para los procesos de seguridad y control.

4.3.2 En cuanto a las Bases de Datos de Oracle de todos los sistemas de elecciones, se requiere que éstas tengan la capacidad de auditar todas las acciones que tienen lugar dentro de ella.

En Oracle, los registros de auditoria deberán escribirse en una tabla denominada SYS.AUD$, de tal manera que si se realiza cualquier acción sobre la tabla SYS.AUD$ (sin contar las inserciones generadas por las auditorias de otras tablas como las Históricas y de Inconsistencias), se registrará dicha acción en el seguimiento de auditoría.

Por lo que estimamos importante que las acciones sobre SYS.AUD$, sólo pueden eliminarse por usuarios con capacidad CONNECT INTERNAL es decir, los del grupo DBA, para lo cual, para nuestros

efectos, requerimos se nos asigne un rol con este perfil, además de documentar este requerimiento para la administración de la seguridad en Oracle.

4.3.3 En cuanto a la necesidad intrínseca de generar políticas para la operación de Bases de Datos Oracle, se recomiendan los siguientes aspectos de relevancia:

I. Establecer políticas que limiten las funciones del DBA
II. Establecer políticas para el depósito de los archivos de la BD
III. Establecer políticas para evitar problemas de desempeño
IV. Establecer políticas para ejecutar actualizaciones en producción
V. Establecer políticas para evitar la Demanda Excesiva
    a. Número de conexiones
    b. Definición de controles
    c. Volumen de usuarios conectados
    d. Establecimiento de filosofías de conexión (call, open, new y report)
VI. Establecer un proceso para la depuración de controladoras
VII. Establecer procesos para el manejo adecuado de excepciones y cambios.
VIII. Diseñar procesos de escalabilidad
    a. Hardware al máximo
    b. Alto volumen de transacciones
    c. Problemas a nivel de redes
    d. Asignación de memoria
    e. Procesos excesivos de espacios temporales.
IX. Establecer una adecuada metodología de tunning

X. Establecer un proceso de verificación de password

XI. Evaluar la asignación de sentencias Hint (planes de optimización de tablas), Grant (usuarios system, Object y Rolls)[7]

4.3.4 Se recomienda que todas las acciones que se lleven a cabo mientras se esta conectado como INTERNAL se escribirán de forma automática en el seguimiento de auditoria, para lo cual solicitamos respetuosamente se adicione un usuario INTERNAL con el nombre de Sys_Audit.

### 4.4 EVALUACIÓN DE RIESGOS Y PLANES DE CONTINUIDAD

4.4.1 Para los efectos de las funciones que competen a esta Auditoría, requerimos que se nos suministre el cronograma de pruebas y simulacros. Este debe incluir: Técnicas, Integración y Simulacros (Plan de contingencia), tanto de los sistemas de elecciones como el de la noche de elección y transmisión de datos.

4.4.2 Establecer una política de Backup: Previamente a la realización de cualquiera de los tipos de backup de la base de datos, es recomendable tener un esquema de full backup del sistema operativo con el aplicativo de base de datos relacional instalado. El esquema es muy simple: luego de que se tiene el servidor con la base de datos instalada y funcionando, se realiza un full backup del server. Posteriormente, ante cualquier cambio de software de base en el servidor de base de datos, se debe realizar otro full backup.

4.4.3 Mantener el respaldo de los logs de transacciones: Almacenar en el servidor “Auditoría” (tipo Raid 5), mediante un “transfer” a las Bases de Datos los “logs” y que una vez ejecutado este proceso se limpien en los de

7 Políticas y procedimientos extraídos del Manual Oracle9i: SQL Tunning Workshop y Oracle9iAS: Basic Administration

producción, esto podría ser implementado por medio de un procedimiento almacenado el cual puede ser programado entre bases de datos o por medio de un archivo Bach. Otra posibilidad es que se respalden por medios magnéticos (cinta 4mm o DLT) las transacciones y se envíen a nuestra oficina, para lo cual necesitaríamos contar con este dispositivo en nuestro Servidor[8].

4.4.4 Que con la participación de la Oficina de Proyectos Tecnológicos (OPT), el Departamento de Tecnologías de información y Comunicación (DTIC), así como otras instancias o funcionarios que se estime pertinente, se proceda a analizar la posibilidad de que la evolución de la plataforma tecnológica del Tribunal pueda ser desarrollada internamente por programadores y analistas del DTIC, toda vez que se ha demostrado la capacidad técnica para el desarrollo interno de aplicaciones[9].

De esta manera se podría evitar la dependencia tecnológica en el aspecto de rediseño y mantenimiento en los sistemas de información, generar valor agregado sobre la inversión que en capacitación ha realizado la institución y analizar múltiples alternativas más consonantes con su orientación estratégica y que eventualmente pueden resultar más eficientes, efectivas y económicas.

**10 de enero del 2006**

**Lic. Allan Acevedo Rodríguez**
**Auditor Fiscalizador en TI**

[8] Propuesta realizada en oficio No.300-A.I.-2005 de fecha 09 de Septiembre del 2005.
[9] Tal como lo propone el Superior en Sesión Ordinaria No. 51-2005, celebrada el 24 de Mayo del 2005 y comunicado mediante oficio No. 3260-TSE-2005, específicamente el punto 3.b).