TRIBUNAL SUPREMO DE ELECCIONES
AUDITORÍA INTERNA

INFORME DE SEGUIMIENTO SOBRE EL CUMPLIMIENTO DE LAS DISPOSICIONES DEL INFORME DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA Nº DFOE-GU-16/2005 SOBRE EL ESQUEMA DE CERTIFICACIÓN CON BASES DE DATOS LOCALES (SBDL)

Junio, 2007

Tabla Contenido

SRCGR-10-2007

"INFORME DE SEGUIMIENTO SOBRE EL CUMPLIMIENTO DE LAS DISPOSICIONES DEL INFORME DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA Nº DFOE-GU-16/2005 SOBRE EL ESQUEMA DE CERTIFICACIÓN CON BASES DE DATOS LOCALES (SBDL)"

1. INTRODUCCIÓN

1.1 Origen del Estudio

El presente estudio se efectuó de conformidad con lo dispuesto por el Tribunal Supremo de Elecciones mediante acuerdo adoptado en Sesión Ordinaria Nº 32-2007, celebrada el 10 de abril del año en curso, comunicado mediante oficio Nº TSE-1723-2007, con motivo del **"INFORME ANUAL SOBRE EL ESTADO DE CUMPLIMIENTO DE LAS DISPOSICIONES GIRADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA AL TRIBUNAL SUPREMO DE ELECCIONES"**, correspondiente al año 2006, cuyos resultados fueron comunicados al Superior con oficio Nº AI-075-2007 del 30 de marzo del 2007.

Además de lo indicado, dicho seguimiento se efectuó en cumplimiento de la competencia que otorga a la Auditoría Interna el artículo Nº 22, inciso g) de la Ley General de Control Interno, Nº 8292, así como en la observancia de lo que establece el aparte No. 2.6 del Manual de Normas para el Ejercicio de la Auditoría Interna en el Sector Público, respecto de la supervisión del progreso sobre la implementación de las recomendaciones de los entes externos de fiscalización.

1.2 Objetivo del Estudio

Evaluar el grado de satisfacción respecto a la implementación de las disposiciones del Informe Nº DFOE-GU-16/2005, sobre el Esquema de Seguridad de la Base de Datos del "Sistema de Certificaciones con Bases de Datos Locales".

1.3 Alcance del Estudio

El seguimiento consistió en el examen de la documentación relacionada con las acciones tomadas por la Administración Activa en cuanto al tema objeto del seguimiento, así como la evaluación de los controles internos establecidos, mediante la realización de pruebas sustantivas y de cumplimiento en relación con la Bases de Datos Locales (BDL), en la Oficina de Certificaciones, ubicada en la Sede Central del Tribunal y en las siguientes Oficinas Regionales: Heredia, Alajuela, Grecia, San Ramón, Puriscal, Pérez Zeledón, Buenos Aires y Osa.

El análisis abarcó el período que comprendido entre el 7 de mayo y el 6 de junio 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

Mediante oficio No. 15837, el Lic. José Luis Alvarado Vargas, Gerente de Servicios de la División de Fiscalización Operativa y Evaluativa de la Contraloría General de la República, remitió al Tribunal Supremo de Elecciones el informe Nº DFOE-GU-16/2005 del 2 de diciembre del 2005, denominado **"INFORME DEL ESTUDIO REALIZADO EN EL TRIBUNAL SUPREMO DE ELECCIONES, SOBRE EL ESQUEMA DE SEGURIDAD DE LA BASE DE DATOS DEL SISTEMA DE CERTIFICACIONES CON BASES DE DATOS LOCALES".**

Sobre el particular, en Sesión Ordinaria No. 116-2005, celebrada el 6 de diciembre del 2005, acuerdo comunicado mediante oficio No. 7825-TSE-2005 de la misma fecha, el Tribunal acordó acoger integralmente las disposiciones giradas por el Órgano Contralor.

Al respecto y en cumplimiento de las competencias que otorga a esta Auditoría el artículo 22 inciso g) de la Ley General de Control Interno, mediante oficio No. AI-075-2007 del 30 de marzo del 2007 se remitió al Superior el informe N° SRCGR-09/2007, denominado **"INFORME ANUAL SOBRE EL ESTADO DE CUMPLIMIENTO DE LAS DISPOSICIONES GIRADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA AL TRIBUNAL SUPREMO DE ELECCIONES"** correspondiente al año 2007.

En dicho informe se establece el grado de cumplimiento de las recomendaciones emitidas por la Contraloría General de la República, definiéndose cinco disposiciones calificadas como "Seguimiento Pendiente", entre las cuales se identifican las ordenadas en el documento No. DFOE-GU-16/2005, arriba indicado.

En este orden de ideas y en atención a solicitud expresa del Tribunal al conocer el citado informe Nº SRCGR-09/2007 (oficio Nº TSE-1723-2007 citado en el aparte 1.1), con el propósito de validar el cumplimiento de las citadas disposiciones, esta Auditoría se dio a la tarea de establecer la programación y ejecución de una auditoría informática para llevar a cabo el seguimiento correspondiente.

1.5 Labor de seguimiento realizada por la Auditoría Interna

A efectos de conocer las acciones emprendidas por la Administración en torno al tema, esta Auditoría solicitó a las unidades administrativas designadas por el

Tribunal para implementar lo dispuesto por el órgano contralor, informar sobre las gestiones realizadas. Además, se llevaron a cabo reuniones con el personal del Departamento de Tecnologías de Información y Comunicaciones (DTIC), con el fin de conocer las mejoras realizadas al sistema objeto de estudio.

Mediante trabajo de campo en la Sede Central y algunas Oficinas Regionales, se evaluó la aplicación de Base de Datos Local, con el fin de comprobar los cambios efectuados, según lo recomendado. En el Anexo Nº 1 "Labor de Seguimiento de la Auditoría Interna", se muestran las iniciativas efectuadas por las referidas unidades administrativas.

1.6 Comunicación verbal de resultados

Los resultados del presente informe fueron comentados en reunión celebrada en el Salón de Expresidentes del Tribunal, el 27 de junio del año en curso, con la presencia de: Magistrada Eugenia María Zamora Chavarría y Magistrados Juan Antonio Casafont Odor y Fernando Del Castillo Riggioni, así como los funcionarios de la Administración: Lic. Fernando Víquez Jiménez, Director Ejecutivo, Lic. Rodrigo Fallas Vargas, Oficial Mayor Civil, Lic. Rodolfo Villalobos Orozco, Coordinador de Servicios Regionales y Lic. Gerardo Hernández Granda, Jefe a.i. del Departamento de Tecnologías de Información y Comunicaciones.

2. RESULTADOS

2.1 Disposición 4.a

En el aparte 4.a del referido informe se dispuso lo siguiente:

> ***"Ordenar al Departamento de Tecnologías de Información y Comunicaciones (DTIC), que efectúe en forma inmediata una revisión a fondo de la configuración de la seguridad de la base de datos utilizada por el "Sistema de Certificaciones con Bases de Datos Locales…".***

Mediante oficio Nº 2197 DTIC, de fecha 13 de diciembre del año 2005, el Jefe a.i. del DTIC, Lic. Gerardo Hernández Granda, informa al Superior las acciones a seguir con el fin de corregir los problemas presentados en cuanto al acceso de los datos a nivel de base de datos y a nivel de aplicación, Al respecto indicó:

> *"Se encriptan los password de los usuarios de la aplicación y se almacenan encriptados en la base de datos" /…/*

"Se llevó a cabo la revisión y prueba de entrada al sistema de certificaciones, en particular, a la base de datos del mismo, tal y como se solicitó, corroborándose que existe dificultad para el ingreso a los datos, sin embargo, el acceso no es imposible, por lo que se puede presentar el borrado físico de los datos, vía ambiente Windows…" (El subrayado no es del original)

Sobre el particular, en la investigación preliminar y entrevista llevada a cabo el día 21 de mayo del presente año con la Licda Pamela Garbanzo Valverde, Analista Encargada del Sistema de Certificaciones de Bases de Datos Local, nos indicó que el sistema había sido modificado para que el ingreso fuera más seguro, ya que se encriptó el usuario "root" del motor MySQL.

En la revisión llevada a cabo, tanto en Oficinas Centrales como en las Regionales, se constató que dichas modificaciones fueron realizadas efectivamente.

2.2 Disposición 4.b

En el aparte 4.b. del referido informe, se giró la siguiente disposición:

"**Disponer en forma inmediata al DTIC, realizar las valoraciones necesarias tendientes a mejorar el esquema de seguridad, a nivel de sistema operativo, de los equipos en que está instalado el "Sistema de Certificaciones con Bases de Datos Locales..."**"

Con oficio No. DITC-1040-2007 de fecha 1º de junio de 2007, remitido a este despacho por el Lic. Gerardo Hernández Granda, Jefe a.i. del DTIC, nos informó respecto a las pruebas de penetración realizadas por un funcionario de la empresa CESA al Sistema de Certificaciones con BDL lo siguiente:

"El especialista me informó que analizado el ambiente y dado que la base de datos estaba instalada en ambiente de microcomputadoras personal, se podía lograr violar la base de datos, pero era necesario cierto conocimiento técnico para concretar la violación requerida."

Además, mediante informe emitido por la Licda. Garbanzo Valverde Encargada del Sistema sujeto a estudio, remitido informe "sin número" al Lic. Gerardo Hernández Granda Jefe a.i. del DTIC, de fecha 14 de diciembre del 2005, el detalle de las modificaciones a la seguridad llevadas a cabo.

De acuerdo con lo anterior, esta Auditoría Interna determinó que las modificaciones realizadas por la encargada del Sistema de Certificaciones y el cambio de equipos con el Sistema Operativo XP, reportados por el Lic. Gerardo Hernández Granda jefe a.i. del DTIC, en el oficio Nº 445 DTIC de fecha 14 de marzo del 2006, satisfacen lo solicitado por el Órgano Contralor.

2.3 Disposición 4.c

Con la disposición 4.c. del referido informe, se requirió lo siguiente:

> ***"****Girar en forma inmediata al DTIC las instrucciones necesarias para que se realice una valoración de los mecanismos actuales de seguridad asociados al proceso de transporte y distribución de los datos que salen del computador central A-14 hacia las oficinas regionales y a la Unidad de Certificaciones, para realizar la actualización de la base de datos del Sistema de Certificaciones con Bases de Datos Locales..."*

Para dar cumplimento a esta disposición, la Administración realizó una serie de acciones, las cuales fueron informadas por la Dirección Ejecutiva al Superior, según consta en oficio No. 4800-DE de fecha 20 de diciembre del 2005.

En cuanto a lo recomendado para dar cumplimiento a la disposición de cita, concretamente en relación con el transporte y actualización de los discos compactos con las bases de datos locales a las Oficinas Regionales, se establecieron procedimientos que satisfacen lo requerido por la Contraloría, ya que se documentó y dictó como política un procedimiento para los funcionarios del "Rango de Operación."

No obstante, esta Auditoría Interna estima conveniente que tales procesos comprendan además la documentación de las etapas de: recibido, proceso y reenvío de la información de los discos compactos con la información de base de datos locales, una vez que son recibidas por el Jefe de la Sede Regional y la forma en que este debe tratar dicha información, por cuanto es necesario fijar responsabilidades a todos los participantes del procedimiento de transporte y distribución de la información.

2.4 Disposición 4.d

En el punto 4.d. del referido informe, se giró la siguiente disposición:

> ***"****Elaborar y divulgar las políticas que considere pertinentes sobre revisión periódica de los esquemas de seguridad instaurados en las bases de datos y aplicaciones disponibles en ese Tribunal..."*

Con oficio Nº 4800-D.E., de fecha 20 de diciembre del 2005, se generó un documento que contiene las políticas para la revisión periódica de los esquemas de seguridad instaurados en las bases de datos disponibles en el TSE.

Esta Auditoría Interna procedió a solicitar dicho documento y pudo constatar la emisión de las políticas conforme a lo dispuesto por la Contraloría.

2.5 Aspectos detectados mediante la evaluación realizada sobre las bases de datos locales de las Oficinas Regionales visitadas, que representan oportunidades de mejora

2.5.1 Problemas detectados en el uso de la clave de Administrador del Sistema de Certificaciones con BDL

Al respecto se detectó que en algunas sedes regionales se ha difundido el uso de la cuenta y la clave de Administrador. Dado que con esa cuenta los usuarios hacen su ingreso, dicha situación representa una importante debilidad de control y constituye un asunto grave en materia de autenticación y autorización de accesos, lo cual obedece a una incongruencia en el diseño y programación del módulo de seguridad de dicho sistema.

Por otra parte, en los equipos en los cuales está instalado el Sistema de Certificaciones con Bases de Datos Local, no se evidencia un uso eficiente y conciente de las medidas de seguridad, en aspectos tales como: seguridad por actividad (aplicaciones), y es omiso en cuanto a la seguridad por categorías (tareas, programas y registros), de la base de datos y diccionarios de datos.

Sobre el particular, durante las visitas se evidenció una vulnerabilidad de control de ingreso en algunas oficinas en relación con el password de administrador del sistema de certificaciones con BDL, el cual permite cierto nivel de acceso a la configuración y actualización de la Base de Datos de Certificaciones.

Se determinó que pese a las modificaciones realizadas en el sistema, éste no cuenta con los campos de control de fecha, ya que carece de una bitácora que registre adecuadamente las transacciones. Además, en los casos señalados, se evidenció que en algunos equipos se puede ingresar no solo al módulo de consulta e impresión, sino al de configuración y creación de usuarios.

Con el propósito de evitar situaciones como las comentadas, resulta fundamental incorporar procesos básicos de seguridad, tales como: el cambio de clave por usuario, vencimiento automático de claves, restricción de accesos por fecha y hora, bitácoras y pistas de auditoría que garanticen, la protección, supervisión y control de los registros de las acciones llevadas a cabo por cada uno de los usuarios del sistema y de la aplicación.

Asimismo, se carece de procedimientos que señalen la obligación de cerrar las terminales de trabajo durante ausencias y recesos del usuario, además las cuentas de usuario de varios sistemas (sistema operativo y la aplicación de certificaciones) no se deshabilitan durante ausencias prolongadas de sus titulares.

Por otra parte, se comprobó que las aplicaciones no muestran la fecha y otros detalles sobre el último acceso válido al sistema, como control de seguridad al inicio de cada sesión de un usuario autorizado.

Al respecto la Ley General de Control Interno, establece en su artículo Nº 16, en cuanto a la información y comunicación, los deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, sobre una adecuada gestión documental, al señalar que: "…Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos, corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada".

Los aspectos antes mencionados, contravienen lo que señalan las normas 302.07, 302.08, 303.07, 305.03, 305.04 y 305.06 del Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados.

La situación expuesta obedece a la ausencia de procedimientos para el desarrollo de aplicaciones y valoraciones de seguridad previos a su implantación, así como la comunicación de políticas que describan la manera y la forma en que los usuarios deben hacer un uso eficiente y pertinente de las claves de acceso, de lo cual se difiere que es necesario describir la forma de asignar roles y responsabilidades sobre la gestión de dicho recurso.

2.5.2 Problemas detectados a nivel de Sistema Operativo

En el estudio llevado a cabo se determinó que el ingreso al Sistema Operativo, así como a la aplicación del Sistema de Certificaciones con Bases de Datos Local, presenta debilidades en su sistema de seguridad y deficiencias en sus controles de ingreso, lo cual eventualmente podría vulnerar las bases de datos, esto por cuanto se evidenció que:

1. En los equipos ubicados en las Sedes Regionales visitadas (nueve en total), los usuarios ingresan al sistema operativo con un único usuario "tse" y una clave de acceso "tse". Dicha situación es generalizada en dichas sedes.

2. Las claves de acceso del perfil de administrador son conocidas por varios funcionarios, por lo que, con el perfil "admin." y clave "admin" se ingresa a los equipos que se muestran en el cuadro a continuación:

Cuadro No.1
Activos en los que corre la Base de Datos Local
y se conoce el perfil y la clave

Ubicación	No. Patrimonio	Perfil	Clave
Oficina Regional de Heredia	616691	admin	admin
	619007	admin	admin
	616597	admin	admin
	624082	admin	admin
	616620	admin	admin

Oficina Regional de Alajuela	616582	admin	admin
	624061	admin	admin
	616630	admin	admin
Oficina Regional de Grecia	616568	1/	1234
	616661	admin	1234

Fuente: Elaboración propia con base en las visitas realizadas.
1/ Pertenece al número de cédula del usuario.

Nótese además como el caso de la Oficina Regional de Grecia uno de los equipos se accesa con el número de cédula como perfil, con clave 1234, mientras que en el otro también se utiliza esta última con el perfil "admin".

3. Se tiene acceso a los módulos de "configuración y creación de usuarios", omitiendo el acceso por números de cédula y/o claves personalizadas que debió instaurarse, lo cual no limita a los usuarios a realizar únicamente las funciones de consulta e impresión de certificaciones de Nacimientos, Matrimonios y Defunciones. En el siguiente cuadro se detallan los activos en los que se comprobó dicha situación.

Cuadro No.2
Detalle de equipos que tienen acceso a módulos no autorizados

Ubicación	**No. Patrimonio**	**Se tiene acceso a los siguientes módulos**	
		Configuración	**Creación de Usuario**
Oficina Regional de Heredia	616691	SI	SI
	619007	SI	SI
	616597	SI	SI
	624082	SI	SI
	616620	SI	SI
Oficina Regional de Alajuela	616582	SI	SI
	624061	SI	SI
	616630	SI	SI
Oficina Regional de Grecia	616661	SI	SI
Pérez Zeledón	624056	SI	NO

Fuente: Elaboración propia con base en las visitas realizadas

4. Se presentan situaciones que comprometen la seguridad lógica y los derechos de acceso a la aplicación de Bases de Datos Local, ya que en algunos casos los usuarios no guardan el debido cuidado en cuanto a mantener la confidencialidad de su clave de acceso.

En ese sentido, se observó que los usuarios al estar activos en la aplicación, si son requeridos o requieren realizar otra diligencia, no hacen abandono de ésta por cuenta propia, ni son desconectados automáticamente del sistema cuando han transcurrido varios minutos, después de haber tecleado la más reciente instrucción, lo que permite que otras personas no autorizadas, puedan manipular la aplicación y realizar operaciones. Además, el sistema tampoco cuenta con una opción habilitada que permita asignar un periodo de vigencia y caducidad que inhabilite las contraseñas, es decir, que obligue al funcionario autorizado a cambiar periódicamente su clave de acceso.

En relación con los tres primeros aspectos, el Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados, emitido por la Contraloría General de la República, señala:

Numeral 305.02.02 "Se mantendrán procedimientos y medidas efectivas para la protección del hardware y del software y de los datos de los SIC"

Numeral 305.03 "El acceso a los archivos de datos y programas al computador, solo se permitirá al personal autorizado."

Con respecto al uso de las claves de acceso a los sistemas de información, el Manual de Normas Generales de Control Interno para la Contraloría General de la República y las Entidades y Órganos sujeto a su Fiscalización, en su aparte No. 5.4 "Controles sobre sistemas de información", define:

> *"…Los sistemas de información deberán contar con controles adecuados para garantizar la confiabilidad, seguridad y una clara administración de los niveles de acceso a la información y datos sensibles…"*

Por otra parte, la Ley de Administración Financiera de la República y Presupuestos Públicos, No. 8131, en su artículo No. 111 se refiere al delito informático en los siguientes términos:

> *"…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…"*

2.5.3 Ausencia de Políticas de Seguridad Informática en las Sedes Regionales

Durante las visitas a las Oficinas Regionales, no se obtuvo evidencia de que exista o funcione un manual de políticas de seguridad informática o documentación, sobre una propuesta de estatuto completo, integrado, actualizado y vigente que normalice el ambiente informático, así como el acceso a los recursos y a los sistemas de información computadorizados para estas oficinas.

Con oficio No. CSR-329-2007 suscrito por el Lic. Rodolfo Villalobos Orozco, del 4 de junio del presente año, brinda respuesta a la solicitud de esta Auditoría Interna

sobre las acciones llevadas a cabo, en su condición de responsable de las oficinas regionales, para dar cumplimiento a las disposiciones del ente Contralor. Al respecto nos informó lo siguiente:

> *"Según términos de referencia y de acuerdo a lo solicitado /…/ le comunico que a las regionales no se les remitió documento alguno para dicha situación, únicamente se les indicó que cualquier error lo informaran por medio del reporte que se envía al Departamento de Información y Comunicaciones, con copia a esta unidad administrativa."*

Es preciso indicar que el 29 de mayo del presente año, con motivo de un informe de seguimiento realizado por esta Auditoría sobre vulnerabilidades detectadas en los Sistemas de Elecciones, el Jefe a.i. del DTIC, Lic. Gerardo Hernández Granda, envío comunicado por medio de la circular No. DTIC-006-2007, sobre el uso de las claves de acceso a las diferentes aplicaciones informáticas. A la fecha este es el único documento del cual se tiene conocimiento que trate sobre el tema solicitado.

Sobre el particular el Manual sobre Normas Técnicas de Control Interno Relativas a los Sistemas de Información Computadorizados, en su norma Nº 302.04, establece que deben definirse políticas, como lineamientos o criterios generales dictados por la autoridad superior, ya que tienen como propósito orientar la acción para el cumplimiento de los objetivos y metas de la organización.

Lo anterior resulta básico para poder cumplir también con la norma Nº 305.03, en la que se señala que; los sistemas y programas deben estar apoyados por procedimientos detallados para cada actividad de seguridad. Agrega que; para mantener un control adecuado sobre los sistemas deben emplearse medidas de seguridad, delimitando el acceso a los datos, terminales, programas y sobre todo el control del sistema de claves de acceso.

2.5.4 Inconsistencias en los datos regístrales del Sistema de Certificaciones con BDL

Se evidenció a través de casos documentados en las Oficinas Regionales y suministrados a este Despacho, que algunos datos contenidos en la Base de Datos Local de Certificaciones, podrían contener errores, inconsistencias u omisiones, en detrimento de la eficacia del trámite, de los respectivos controles y de la confiabilidad de la información suministrada al usuario.

En relación con lo anterior, a continuación se detallan los siguientes hechos:

A. El 16 de mayo del 2007, mediante oficio No. ORAL-610-2007 el Lic. Walter Villalobos Zúñiga, Jefe de la Regional de Heredia, comunicó al Lic. Rodrigo Fallas Vargas Oficial Mayor Civil, lo que a la letra dicta:

"...Para lo que corresponda, me permito enviar adjuntos los siguientes documentos, ya que según mi humilde criterio presentan inconsistencias que podrían atentar contra la credibilidad de nuestra institución ante la opinión pública.

Certificación de matrimonio a nombre de VICTOR MANUEL DIAZ CASCANTE cedula emitida el día 16/05/2007 a las 09:45 horas. Con las citas de divorcio de Señor Juan Carlos Picado Viquez cedula 2-0499-0142.

Certificado de soltería a nombre del señor JUAN CARLOS PICADO VIQUEZ CEDULA 2-0499-0142, EMITIDO EL MISMO DIA A LAS 09:45 HORAS (NO APARECE NOTA DE DIVORCIO).

Certificado de matrimonio del señor JUAN CARLOS PICADO VIQUEZ CEDULA 2-0499-0142, emitido el mismo día a las 09:42 horas, no aparece divorcio..."

En relación con la situación comentada, la misma fue verificada por este Despacho el 30 de mayo del 2007, a las 01:17 p.m., al solicitarle al señor Carlos León Jiménez, Coordinador de la Unidad de Certificaciones, constatar por medio de la base de datos locales, la condición del Sr. Picado Víquez.

B. Mediante oficio No. ORPU-003-2006 del 05 de enero del 2007, el Sr. Wilfredo Molina Camacho, Jefe de la Región de Puriscal, informó al Lic. Rodolfo Villalobos Orozco, Coordinador Servicios Regional, lo siguiente:

"...la base de datos local (sic), del mes de diciembre no viene debidamente actualizada la de defunciones, por ejemplo aproximadamente de cada diez aparecen solamente dos y las otras no, se digita el mismo número de cédula en el nacimiento y aparece en el margen una leyenda que dice TIENE DEFUNCIÓN CON CITA: y no aparecen las citas.

Favor digitar estos números de cédulas 3-0064-0964, 1-0260-0678, 1-0260-0679 y 1-0110-7699, se hace la observación que antes si aparecía las defunciones..."

C. Con oficio No. ORPU-219-2007 del 18 de mayo del 2007, dirigido al Lic. Gerardo Hernández Granda, Jefe a.i. del DTIC, el Sr. Wilfredo Molina Camacho, Jefe de la Región de Puriscal, informa:

"...Para los fines que estime pertinentes, consultando la Base de Datos de esta Oficina Regional actualizada al 01 de mayo del 2007 y a solicitud del Lic. Róger Cordero, pide el estado civil de la señora MARIA ISABEL QUIROS VILLALOBOS, cédula No. 1-0729-0305, aparece matrimonio.

Por intuición, se consulta a la Coordinadora de Servicios Regionales dicho estado civil, aparece divorcio, por seguridad se llama a tomos y existe desde el 02 de mayo 2006 marginal en ese libro.

En virtud de lo anterior, para no incurrir en error por parte de lo funcionario de las Regionales, favor corregir este asunto, y un llamado vehemente para que revisen lo copiado en los CDs..." (El subrayado no es del original).

Lo comentado pone de manifiesto una situación de alto riesgo para el Tribunal, pues no se precisa si los hechos comentados representan casos asilados, o por el contrario, corresponden a situaciones que se presentan con frecuencia. Cabe señalar que según nos informó el Lic. Rodrigo Fallas Vargas, Oficial Mayor Civil, mediante oficio Nº OMC-3648-2007 de 11 de junio del año en curso, no se llevan estadísticas de reportes para poder cuantificar los casos que se presentan.

Sobre el particular, al presentarse condiciones similares en otras bases de datos del TSE, la Licda. Vilma Gamboa Bolaños, Gerente de Área, del Área de Seguimiento de Disposiciones de la División de Fiscalización Operativa y Evaluativa de la Contraloría General de la República, dentro del contexto del seguimiento al informe Nº DFOE-GU-13/2006 sobre el Modelo de Arquitectura de Información, con oficio No. 06-008 del 12 de junio del 2007, señaló:

"...También se deberá determinar si dicha situación constituye un caso aislado o existen otros casos que ameriten una corrección en forma integral..."

El artículo Nº 16 de la Ley General de Control Interno establece como deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:

a) Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna /.../

El sistema de Certificaciones con BDL no se encuentra integrado al Sistema de Información del TSE, situación que coadyuva a que la información registral no se actualice con la debida oportunidad, esto provoca que las sedes que dependen de dicho sistema para certificar a la ciudadanía los requerimientos, resulten insuficientes.

Eventualmente podrían existir problemas de calidad en la preparación y captura de los datos, así como la falta de actividades de conciliación, investigación y ajuste periódicos de las bases de datos, tanto del sistema principal como el usado para el Sistema de Certificaciones con Base de Datos Local.

2.5.5 Análisis de la gestión de DTIC con respecto a la Administración de las Bases de Datos institucionales.

El Administrador de Base de Datos institucional, no guarda relación ni ejerce control sobre la Base de Datos Local del Sistema de Certificaciones.

El Manual Descriptivo de Puestos del Tribunal define el cargo **"Administrador de Base de Datos"** y su relación con la bases de datos institucionales, siendo que mediante los apartes **"Naturaleza del Trabajo"** y **"Características Especiales"**, señala, en su orden:

> *"Ejecución de labores tendientes a organizar, brindar mantenimiento y seguridad a las bases de datos institucionales…"*
>
> *"…Es el responsable de administrar eficientemente las bases de datos institucionales*…" (Lo destacado no es del original).

Además, entre sus funciones el documento en mención, entre otras, le asigna: "…Organizar y brindar mantenimiento a las bases de datos institucionales…//…Administrar la base de datos institucionales…".

Sobre el particular, en consulta realizada al Lic. Gerardo Hernández Granda, Jefe a.i. del DTIC, sobre la relación del funcionario nombrado en dicho puesto con la Base de Datos Local, mediante oficio No. DTIC-1040-2007 del 1º de junio del 2007, señala que la persona que funge como Administradora de Bases de Datos, está encargada de los sistemas SICI y TIM, sea que no mantiene relación alguna con otras Bases de Datos.

Al respecto indicó:

> *"A la administradora de Bases de Datos no le fue asignada la tarea de la implementación de la base de datos de Certificaciones Local, que se envía a las Oficinas Regionales de la institución, debido a que la gestación de este aplicativo apareció como una aplicación informática de auxilio a la atención del ciudadano /…/*

Debido a lo anterior, se evidenció que los cambios en el Sistema de Certificaciones de repetida cita, realizados en atención a la disposición de la Contraloría mediante informe DFOE-GU-16/2005, estuvieron a cargo de la Licda. Pamela Garbanzo Valverde, quien se desempeña como profesional de apoyo.

Cabe señalar que con motivo de dicho trabajo, mediante oficio dirigido al Jefe a.i. del DTIC el día 14 de diciembre del año 2005 (sin número), la citada funcionaria informó sobre las modificaciones realizadas al sistema y además externa criterio sobre su posible vulnerabilidad, en los siguientes términos:

"…Para mi criterio, cualquier base de datos que se encuentre localmente instalada en una computadora, es vulnerable a no ser que se implementen los mecanismos de seguridad a nivel de sistema operativo que impidan tener libre acceso a todos los archivos del sistema operativo y de aplicaciones específicas que tengan cierto grado de confidencialidad"

No obstante, no se evidenció mediante dicho informe, ni en oficios posteriores, el traslado de ese documento para su validación y supervisión al Administrador de Bases de Datos institucional, en cuanto a ambiente de bases de datos se refiere, como parte de una labor de control interno, en el aparte que describe la **"Naturaleza del Trabajo"** y las **"Características Especiales"**.

Al respecto la normativa técnica vigente estipula:

302.07 Segregación de funciones incompatibles dentro de la organización: Se mantendrá una segregación efectiva de las funciones de iniciación, autorización, ejecución y registro de transacciones dentro de la organización.

302.08 Segregación de funciones dentro de la Unidad de Informática: Se segregarán las funciones de análisis y diseño de sistemas, programación, operación del equipo, control de los datos y manejo de la cintóteca.

En materia de segregación de funciones, la declaración interpretativa de esta última norma señala: ***"El control interno se verá fortalecido si dentro de la estructura de la organización de la Unidad de Informática, existe una segregación adecuada de funciones incompatibles, lo cual también dará como resultado, una mayor eficiencia operacional debido al diferente nivel de entrenamiento, conocimiento y habilidad requeridos en cada función".***

De conformidad con certificación expedida por el Lic. Ricardo Carias Mora, Jefe de Recursos Humanos, remitida a esta Auditoría mediante oficio RH-1233-2007 de 23 de mayo de 2007, señala en cuanto a las responsabilidades del Administrador de Bases de Datos, lo siguiente:

NATURALEZA DEL TRABAJO

"Ejecución de labores tendientes a organizar, brindar mantenimiento y seguridad a las bases de datos institucionales, a fin de alimentar los sistemas de información utilizados por las unidades administrativas mediante el empleo de diferentes tipos de software".

En cuanto a las tareas más relevantes y en lo que interesa, se definen así:

"Participa en el diseño, desarrollo e implementación de diversos sistemas institucionales…"

"Organiza y brinda mantenimiento a las bases de datos institucionales…"

Además, es de gran relevancia para lo que aquí se expone, que tiene como tarea diseñar e implantar la seguridad requerida para acceder las bases de datos, entre otras de similar importancia.

Oficio No. DTIC-1040-2007 de fecha 01 de junio del 2007, suscrita por el Jefe a.i. del DTIC

En cuanto a las responsabilidades del Administrador de Bases de Datos:

Objetivo

> *"Mantener un adecuado respaldo y administración de todas las bases de datos de la plataforma de acuerdo con los procedimientos y políticas correspondientes".*

Si partimos de la importancia de lo normado y estipulado sobre los procesos de segregación de funciones, podemos concluir que la asignación de responsabilidades y los procedimientos que competen al Administrador de Bases de Datos Institucional, son básicos y delicados dentro del proceso de desarrollo de cualquier sistema. Situación que no se dio en el desarrollo del sistema de Certificaciones con BDL. 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.

3. CONCLUSIONES

3.1 En relación con las disposiciones del informe de la Contraloría General de la República

De conformidad con los resultados del seguimiento realizado sobre las disposiciones 4.a, 4.b 4.c y 4.d del informe No. DFOE-GU-16/2005 de la Contraloría General de la República, se desprende que la Administración realizó las gestiones para su atención, situación que se constató mediante el análisis de diversos documentos que se gestionaron a partir de la presentación del informe ante el Tribunal Supremo de Elecciones y la posterior evaluación que al efecto llevó a cabo esta Auditoría.

3.2 En relación con los comentarios sobre los aspectos sujetos a mejora

3.2.1 Sobre el uso de la clave de Administrador del Sistema de Certificaciones con BDL

Los registros de movimientos en las tablas (en este caso el usuarios, tipo de consulta, y registro impresión), apoyados en un módulo de pistas de auditoría y bitácoras en la Base de Datos, son necesarios para ejercer un seguimiento y control sobre dichos movimientos. La debilidad detectada en cuanto al uso de la clave de administrador por parte de los usuarios, no garantiza los niveles de seguridad requeridos según las normas y estándares, lo que podría provocar un aumento significativo en el riesgo inherente y de control de las operaciones que se llevan a cabo en las sedes regionales visitadas.

3.2.2 Sobre los problemas detectados a nivel de Sistema Operativo

En relación con el uso de las claves de acceso, la situación expuesta obedece a que no se evidenció que el Departamento de Tecnologías de Información y Comunicaciones, siendo la dependencia técnica, comunicara las instrucciones, directrices y demás políticas en esta materia, lo cual constituye una falla significativa en relación con el control de accesos en la instalación del sistema.

Además, dicha situación representa un riesgo en el uso, divulgación o modificación no autorizados de las claves, lo que puede eventualmente ocasionar un daño o pérdida parcial o total de la información y del equipo.

3.2.3 Sobre la ausencia de Políticas de Seguridad Informática en las Sedes Regionales

La situación expuesta en cuanto a este tema, se presenta por la carencia de una política de seguridad aprobada y debidamente divulgada, sobre el uso de todos los sistemas y aplicaciones del Tribunal, lo cual podría eventualmente vulnerar los programas y datos de los SIC, o en el peor de los casos, que se haga un uso inadecuado de las claves y perfiles de usuario, tal como se evidenció en varias oficinas regionales.

Por otra parte, los costos asociados con algunas ocurrencias de riesgos se pueden incrementar por la dependencia de procesos computadorizados. En circunstancias extremas, una interrupción del servicio puede significar la afectación del principio del servicio que brinda el Tribunal, en especial en sus Oficinas Regionales y con mayor razón en cuanto a aquellas oficinas regionales no conectadas.

Lo anterior podría aumentar el riesgo de la integridad y confiabilidad de los datos consignados, los cuales se certifican como válidos en las sedes regionales.

3.2.4 Sobre las inconsistencias en los datos registrales del Sistema de Certificaciones con BDL

No obstante los esfuerzos que efectivamente la Administración realizó en cumplimiento de las disposiciones del informe emitido por la Contraloría General de la República, se evidenciaron aspectos que afectan la integridad de los datos, dado que ésta debe garantizar la calidad, la identificación de registros válidos de los datos y la corrección metodológica de estos en las bases de datos institucionales.

Desde el punto de vista técnico, el principal objetivo que la institución debe alcanzar con respecto a la integridad de los datos es garantizar que una entidad (fila o registro), siempre se relacione con otras entidades válidas, es decir, que existen en la base de datos, lo cual implica que en todo momento dichos datos sean correctos, sin repeticiones innecesarias, datos perdidos o relacionados en forma incorrecta.

Todas las bases de datos deben disponer de esta propiedad, es por esto que toma relevancia la incorporación de un Sistema Gestor de Base de Datos[1], el cual posee rutinas de control sobre el conjunto de dos o más tablas estructuradas en registros (líneas) y campos (columnas), que se vinculan entre sí por un campo en común, en ambos casos posee las mismas características. Por supuesto se debe tomar en cuenta que si estamos ante bases de datos jerárquicas, se requieren programadores que aseguren de mantener tal propiedad en sus programas.

La no atención de lo anterior podría aumentar el riesgo de la integridad y confiabilidad de los datos consignados, los cuales se certifican como válidos en las sedes regionales.

3.2.5 Sobre la Gestión del DTIC con respecto a la Administración de las Bases de Datos Institucionales.

A partir de de las características, naturaleza y funciones del puesto "Administrador de Base de Datos", contenidas en el Manual Descriptivo de Puesto de la institución –a la fecha vigente-, se desprende que la persona que se desempeña en esa función, es el funcionario técnico encargado de gestionar todo lo relacionado con las bases de datos institucionales, no obstante, en la práctica esa situación no se presenta tratándose de la base datos locales o cualquier otra, por cuanto el funcionario llamado a realizar esta función, esta limitado a la administración únicamente de las bases de datos SICI y TIM, lo cual representa una debilidad importante en la validación, supervisión y control del correcto cuidado profesional y metodológico de las Bases de Datos enmarcado en los Manuales que al respecto se han establecido.

3.2.6 Otras Conclusiones

La falta de conexión de algunas Sedes Regionales con los sistemas centrales del Tribunal Supremo de Elecciones, se ha visto aparentemente solventada con el uso del sistema de envío de CD´s con la copia de la BDL de Certificaciones, que se alimenta del SIIEC cada mes y que se aplica mensualmente, sin embargo esto ha originado que la información sobre hechos Civiles se encuentre desactualizada en dichas sedes.

El Sistema emite certificaciones "al día", pero la información de dicho documento se encuentra desactualizada. Dado que el proceso de certificación no puede validar la información respectiva sobre los hechos regístrales, existe la posibilidad de emitir una certificación inexacta.

---

[1] Sistema Gestor de Bases de Datos, recomendado en informe ICI-01-06 Sobre 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.

4. RECOMENDACIONES

4.1 Al Tribunal

4.1.1 En relación con los comentarios sobre los aspectos que representan oportunidades de mejora.

Solicitar al DTIC, en el plazo que se estime razonable, realizar las modificaciones necesarias sobre los aspectos citados, para lo cual se deberá formular un cronograma con las actividades, plazos y responsables de su ejecución.

Sobre este último aspecto, se solicita informar a esta Auditoría oportunamente.

4.1.2 En relación con la interconexión de las Sedes Regionales

Solicitar la elaboración de estudios necesarios con el propósito de elaborar un plan de interconexión de las sedes regionales que a la fecha no están conectadas por medios telemáticos.

Además, es conveniente que la institución inicie un proceso de depuración de las Bases de Datos Locales y de su fuente de alimentación, de manera que se pueda garantizar la confiabilidad de los datos.

4.1.3 En relación con las inconsistencias en los datos

Solicitar al DTIC conjuntamente con la Oficialía Mayor Civil, la realización de un análisis exhaustivo para determinar los problemas detectados en las inconsistencias de los datos y sus implicaciones formales y de contenido sobre el proceso de emisión de certificaciones con BDL, así como que se formulen directrices y procedimientos necesarios, con el fin de corregir los diversos problemas en el ámbito operativo y funcional de los sistemas computadorizados que se utilizan para emitir estos documentos.

4.2 Al Departamento de Tecnologías de Información y Comunicaciones (DTIC)

4.2.1 En relación con la necesidad de realizar un análisis integral sobre el SBDL

Que se definan las restricciones tecnológicas que presenta el motor de base de datos (MYSQL) en que está implementada dicha aplicación, a efecto que desde la perspectiva de funcionabilidad, relevancia y oportunidad que le significa al Tribunal mantener en operación la Base de Datos Locales, valore la migración de dicha base de datos a otras con mayor capacidad y que le permita a la institución, la implementación de mayores elementos de control, seguridad y eficiencia.

Realizar los estudios necesarios con el propósito de determinar la conveniencia y factibilidad técnica y operativa para que el Sistema de Certificaciones con BDL, cuente con un archivo maestro que registre históricamente las transacciones significativas, con el propósito de mantener a disposición de cualquier ente fiscalizador una bitácora de los movimientos en dicho sistema.

4.2.2 En relación con la seguridad de acceso al Sistema de Certificaciones BDL

Realizar las gestiones pertinentes para que en los equipos de cómputo de las Sedes Regionales, en los que opera el Sistema de Certificaciones con BDL, se restringa el uso de la clave “administrador” y se delegue el uso del perfil con acceso por medio del número de cédula y llave de paso (clave) con al menos ocho (8) caracteres. Asimismo, que se inste al cambio de claves mensuales y que se documente las políticas necesarias para llevar a cabo esta recomendación.

4.3 A la Dirección Ejecutiva

4.3.1 Evaluar la situación del Administrador de Base de Datos

Evaluar conjuntamente con el Departamento de Tecnologías de Información y Comunicaciones (DTIC), la situación del puesto “Administrador de Base de Datos”, con el fin que la persona nombrada en éste se dedique en su totalidad a las funciones que le corresponden de conformidad con el Manual Descriptivo de Puesto del Tribunal, o en su defecto, se valore la necesidad de nombrar a otro Administrador de Bases de Datos que apoye la administración de las demás bases de datos de la institución.

4.3.2 Documentar Políticas de Seguridad Informática

Solicitar a las instancias que corresponda, la elaboración y actualización de los respectivos manuales de documentación técnica, de operaciones y de usuario del Sistema de Certificaciones con BDL, para los encargados de las Sedes Regionales y oficina principal. Lo anterior en relación con el uso de las claves de acceso y seguridad informática.

Analizar la conveniencia de ampliar el procedimiento de traslado de información del sistema SIIEC a las sedes regionales, en las etapas de: recibido, proceso y reenvío de la información de los discos compactos con la información de base de datos locales, tal como se comentó en el aparte 2.3 del presente informe.

Auditoría Interna
Junio, 2007

Lic. Allan Acevedo Rodríguez
Auditor de Sistemas

Lic. Franklin Mora González
Auditor Fiscalizador