

**INFORME DEL AUDITOR INTERNO A LA JUNTA  
DIRECTIVA**

**AÑO 2009**

## Tabla de contenido

<b>1. OBJETO</b> .....	<b>3</b>
<b>2. INTRODUCCION</b> .....	<b>3</b>
<b>3. GESTION DE AUDITORIA INTERNA</b> .....	<b>3</b>
3.1 Auditoria Interna .....	3
3.2 Auditoria Externa de Sistemas. ....	8
<b>4. CONCLUSION</b> .....	<b>11</b>
<b>5. ANEXO DOMINIOS COBIT POR MACROPROCESO</b> .....	<b>12</b>

## **1. OBJETO**

El presente informe con destino al Comité de Auditoria y Riesgo de la Junta Directiva del Depósito Centralizado de Valores DECEVAL S.A. es elaborado por el Auditor General en cumplimiento a lo establecido por la Circular Externa 038 de 2009 emitida por la Superintendencia Financiera de Colombia en su numeral 7.7.1.4.2.2.7 literal xii y se refiere a los resultados de las funciones desarrollada por la Auditoria durante el año 2009.

## **2. INTRODUCCION**

El área de auditoria interna está compuesta por un staff de cuatro personas: Auditor General, Auditor Operativo, Auditor Financiero y Administrativo y un Auditor de TI. Las actividades en el año 2009 se adelantaron en cumplimiento al plan de auditoria aprobado por presidencia. Auditoria Interna coordina la ejecución del contrato de auditoria externa de informática la que para la vigencia 2008 - 2010 la que fue realizada por la firma ADVISORY SERVICES LTDA - KPMG.

## **3. GESTION DE AUDITORIA INTERNA**

### **3.1 Auditoria Interna**

La Auditoria Interna está alineada con el Sistema de Gestión de la Calidad de la compañía cuyo proceso se soporta en el Manual de Auditoria Interno que detalla los lineamientos generales del desarrollo de la actividad de la auditoria, en donde se incluyen las actividades de planeación, desempeño, discusión y presentación de informes a la administración y las actividades propias de supervisión, tal como lo establece la Circular Externa 038 de 2009 de la SFC. Es de notar que Auditoria Interna se encuentra en proceso de ajuste del Manual de Auditoria y procedimientos internos de acuerdo con el numeral 7.7.1.4 de la circular mencionada y demás numerales que de manera directa o indirecta le sean aplicables.

La planeación de las actividades a realizar en el año 2009 fue aprobada por la Gerencia General del Depósito y sobre la misma se realizaron reportes de avance periódicamente.

La actividad de la auditoria en el año 2009 se orientó principalmente a los siguientes aspectos:

- Desarrollo del plan de auditoria establecido para el año en lo relacionado con las áreas de Operaciones, Administrativa y Financiera y de Información Tecnológica;
- Acompañamiento especial al desarrollo de proyectos
- Fortalecimiento técnico de los procesos de auditoria.
- Acompañamiento al desarrollo del plan de Auditoria Externa de Informática

Parte importante de la gestión se centró en el acompañamiento de proyectos dentro de los cuales sobresale la participación en los proyectos de conversión tecnológica y su puesta en producción, traslado y puesta en marcha de los centros de cómputo, desarrollo de la Agencia Numeradora Nacional ANNA y el acompañamiento en el desarrollo y puesta en marcha de los proyectos de registro y pagarés. De igual forma, vale la pena mencionar el continuo monitoreo al sistema de riesgos, al cumplimiento de la circular 052 y el desarrollo e implementación de las circulares 014 y 038 relacionadas con control interno, en concordancia con lo establecido por la Superintendencia Financiera.

En el año 2009, se presentaron cincuenta y ocho (58) intervenciones que generaron al cierre del año 54 informes de auditoria emitidos y 4 informes en proceso de elaboración; y se emitieron 38 observaciones de auditoria para un total de 92 informes con recomendaciones.

En total durante el año 2009 se formularon 136 recomendaciones de las cuales 103 fueron adoptadas por la administración y 33 se encuentran con plan de acción y que se distribuyen al interior del Depósito de la siguiente forma:

<b>Informes de la Auditoría Interna emitidos en el 2009</b>				
<b>Clase de Informe</b>	<b>Número informes</b>	<b>Total Recomendaciones</b>	<b>Recomendaciones Cerradas</b>	<b>Recomendaciones Abiertas</b>
<b>OPERATIVOS</b>	<b>20</b>	<b>36</b>	<b>26</b>	<b>10</b>
<b>ADMINISTRATIVOS Y FINANCIEROS</b>	<b>6</b>	<b>20</b>	<b>10</b>	<b>10</b>
<b>TECNOLOGIA</b>	<b>26</b>	<b>23</b>	<b>16</b>	<b>7</b>
<b>ESPECIALES</b>	<b>2</b>	<b>7</b>	<b>7</b>	<b>0</b>
<b>OBSERVACIONES</b>	<b>38</b>	<b>50</b>	<b>44</b>	<b>6</b>
<b>TOTAL</b>	<b>92</b>	<b>136</b>	<b>103</b>	<b>33</b>

El acumulado de recomendaciones pendientes de implementación al cierre del año 2009 es de 57 clasificadas de la siguiente forma:

Clase de Informe	Recomendaciones Abiertas	Con plan de acción	Se cierra con proyecto o mejora SIIDJ	Recomendaciones pendientes de un plan de acción
OPERATIVOS	14	7	3	4
ADMINISTRATIVOS Y FINANCIEROS	30	15	13	2
TECNOLOGIA	7	7	0	0
ESPECIALES	0	0	0	0
OBSERVACIONES	6	4	0	2
<b>TOTAL</b>	<b>57</b>	<b>33</b>	<b>16</b>	<b>8</b>

La distribución por nivel de riesgo de las 57 recomendaciones abiertas a diciembre de 2009 es como sigue:

RECOMENDACIONES POR NIVEL DE RIESGO	Número de recomendaciones
RIESGO MUY ALTO	6
RIESGO ALTO	26
RIESGO MODERADO	21
RIESGO BAJO	4
<b>TOTAL</b>	<b>57</b>

Todas las recomendaciones de control fueron enviadas a la Gerencia General como a los responsables de procesos. A diciembre de 2009 la administración ha establecido plan de acción para 49 de ellas. De las 8 recomendaciones sin plan de acción, 4 corresponden a informes de auditoría emitidos en diciembre de 2009 y las restantes a la administración de los siguientes casos:

- Módulo de billing: Asignación y traspaso de la administración de la aplicación en producción al dueño del proceso
- Seguridad del sistema UNO: Mejoramiento en la administración de claves. Se observan limitaciones en la herramienta para el manejo de perfiles de seguridad.
- Decimales enajenación SIIDJ : Problema de manejo de los decimales en las constancias de enajenación, lo que implica ajustes a base de datos.
- Administración sobre claves de seguridad: Mejoramiento del ciclo de claves.

Al cierre del año 2009 el índice de gestión fue del 89% respecto de los informes de auditoría inicialmente planeados. Las intervenciones de auditoría planeadas y no realizadas corresponden a administración de acciones, usuarios del producto registro, PyG presupuesto, Compensación y Liquidación, perfiles de usuarios del producto pagarés, valoración del portafolio y página WEB. Las intervenciones no realizadas obedecen a iniciativas no desarrolladas por el Depósito, a falta de suficiencia de operaciones y usuarios en el caso de los proyectos y finalmente la realización de actividades no incorporadas en el plan como es el caso de las observaciones de auditoría que consumen un tiempo importante de horas presupuestadas.

Dentro de las intervenciones de auditoría más relevantes en el transcurso del año 2009 vale la pena mencionar:

- Gestión de Riesgos.
- Seguimiento SARO y la rendición del respectivo informe en términos de las normas vigentes.
- Auditoría a las áreas administrativa y Financiera y de Operaciones, particularmente en administración de la bóveda con orientación a títulos físicos, administración del portafolio de inversiones de DECEVAL, fraccionamientos, emisiones desmaterializadas con énfasis en TIDIS, BONOS PENSIONALES y emisión de bonos, cuentas exentas, derechos patrimoniales y sociales, operaciones entrega contra pago, actualización del valor diario de acciones, Gestión Humana, Gestión Documental y Compras.
- Auditoría al área de tecnología en donde vale la pena mencionar los seguimientos a la circular 052, proyectos ANNA, conversión del SIID, traslado de centros de cómputo, pagarés, registro, perfiles SIIDJ, administración de claves y auditoría al motor Oracle del core del negocio.
- Auditoría a la sucursal de Cali y Medellín.
- Auditoría del proceso de cierre anual de operaciones, lo que incluyó arqueo 100% tanto de títulos físicos como de macro títulos.
- Seguimiento a los hallazgos de auditoría interna, externa y de otros entes de vigilancia y control.

En el desarrollo de sus funciones la Auditoría obtuvo de la administración toda la información solicitada para el desarrollo de las intervenciones y en cumplimiento del proceso de auditoría y lo estipulado en el Manual de Auditoría, se realizaron las discusiones de los informes borrador y se realizó seguimiento a la implementación de las recomendaciones, con los resultados mencionados anteriormente.

En cumplimiento al desarrollo de la circular 014 y 038, Auditoría Interna presentó al Comité de Auditoría y Riesgos de la Junta Directiva en la sesión de diciembre la estructura del área, la gestión a noviembre de 2009, el análisis histórico de riesgo por macroproceso, involucrando hallazgos del área de calidad, de riesgo y de auditoría y presentó para aprobación el plan de auditoría para el año 2010 al igual que el presupuesto del área. La planeación para el año 2010 se centró en:

<b>MACROPROCESO</b>	<b>% PARTICIPACION TOTAL PROCESOS</b>
<b>Administración de Instrumentos Representativos de Derechos</b>	<b>22%</b>
<b>Gestión Tecnológica</b>	<b>18%</b>
<b>Administración de Recursos Físicos y Financieros</b>	<b>14%</b>
<b>Administración de Derechos Patrimoniales</b>	<b>11%</b>
<b>Mejoramiento Continuo</b>	<b>11%</b>
<b>Otros (Gestión Humana, Jurídico, Comercial, y otros sistemas de apoyo.)</b>	<b>24%</b>
<b>TOTAL PARTICIPACION</b>	<b>100%</b>

Del total de horas de auditoría aprobadas para el año 2010 el 50% se destinará a la auditoría de procesos, 24% a auditorías de verificación y monitoreo permanente, 11% a proyectos, 12% a seguimiento a la implementación de recomendaciones y 3% a otras actividades. De acuerdo con el número de horas planeadas de intervención la administración aprobó un recurso adicional para el área a partir del mes de marzo de 2010.

### 3.2 Auditoria Externa de Sistemas.

La Auditoria Externa Informática de DECEVAL S.A. fue realizada por la firma ADVISORY SERVICES LTDA, KPMG en cumplimiento al contrato firmado para la vigencia 2008-2010. Sus esfuerzos durante el año 2009 se enfocaron al cumplimiento al estándar COBIT con énfasis en los siguientes procesos:

- Plan de pruebas y marcha blanca en la conversión tecnológica del Sistema del SIID.
- Gobierno de TI.
- Definición de la arquitectura de información.
- Planeación estratégica de TI.
- Administración de proyectos.
- Administración de desempeño y capacidad
- Seguridad de los sistemas, seguridad de proyectos, matriz de riesgos de TI y pruebas de planes de contingencia.
- Además presentaron un informe especial frente a los procesos de administración de cambios, mesa de ayuda e incidentes, administración de datos, administración de problemas y gobierno de TI como base para que el área de TI mejorar el nivel de madurez de dichos procesos, en función del plan estratégico de tecnología.
- Frente a las circulares 014 y 038 de la superintendencia financiera, realizaron un informe del GAP entre lo mencionado en las circulares y lo establecido por COBIT.

Durante el año 2009 KPMG emitió 16 informes de auditoría que produjeron 120 recomendaciones, 21 de riesgo alto, 80 de riesgo moderado y 19 de riesgo bajo. De acuerdo con el plan de auditoria establecido se efectúan dos seguimientos anuales a la implementación de las recomendaciones por parte de la administración. De acuerdo al seguimiento provisional efectuado a Diciembre de 2009 las recomendaciones se encuentran en el siguiente estado:

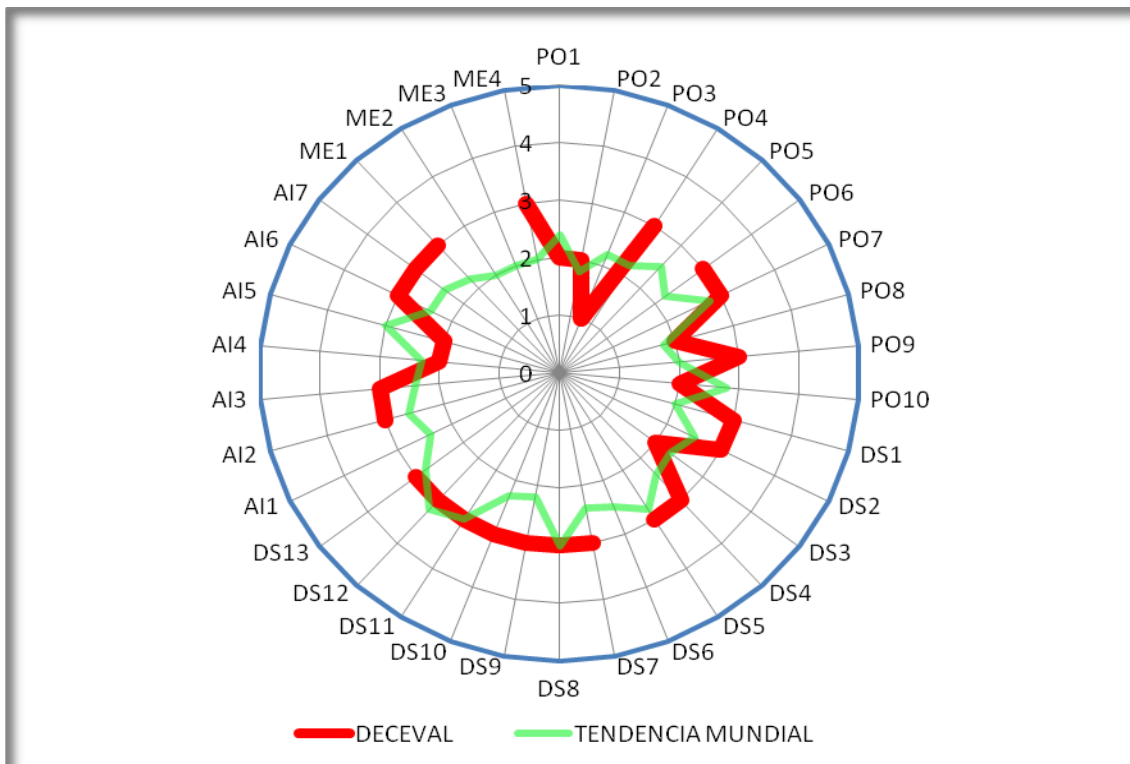
Nivel de Riesgo	Número de Recomendaciones	Recomendaciones. Cerradas	Recomendaciones Abiertas con Plan de Acción.	Recomendaciones Abiertas pendientes de un Plan de Acción
RIESGO ALTO	21	12	4	5
RIESGO MODERADO	80	30	43	7
RIESGO BAJO	19	13	3	3
TOTAL	120	55	50	15

Del total de las recomendaciones abiertas sin plan de acción 11 corresponden a informes recibidos por la administración en el último trimestre del año 2009.

Durante el presente año el Comité de Riesgo de JD recomendó evaluar y mejorar el nivel de madurez de los procesos COBIT Administración de Cambios, Administración Mesa de Ayuda e Incidentes, Administración de Problemas, Administración de Datos y Gobierno de TI lo que originó un informe de GAP de evaluación de dichos procesos por parte de KPMG recomendaciones que fueron dadas a conocer a la administración en Junio de 2009. De acuerdo con el informe presentado por KPMG al cierre de año, el nivel de madurez esperado por el Comité de Riesgo de la JD se alcanzó y en dos procesos COBIT se superó.

KPMG mantuvo de manera permanente la orientación de DECEVAL hacia la adopción de las mejores prácticas de control establecidas en el modelo COBIT. En el desarrollo de su ejercicio se apoyó en las herramientas provistas por KPMG internacional ITRMB para medir riesgos y evaluar controles y mantuvo la comparación de las prácticas del Depósito contra estándares internacionales como ITILL, BCP e ISSO 17799.

En noviembre de 2009 KPMG, tomando como referencia el artículo publicado en la revista ISACA Journal Volumen 3 de 2009 **“IT Governance and Process Maturity”** sobre el nivel de madurez COBIT de 51 entidades a nivel internacional , realizó una comparación para cada uno de los 34 procesos COBIT entre el promedio del nivel de madurez del estudio mencionado y el nivel de madurez de DECEVAL obteniendo como resultado que el Depósito se encuentra dentro del promedio de madurez y en ocasiones superando la madurez de algunos procesos, como se puede apreciar en la gráfica siguiente.



PO: Dominio PLANEACION Y ORGANIZACIÓN Contiene 10 procesos COBIT  
 DS: Dominio ENTREGA Y SOPORTE Contiene 13 procesos COBIT  
 AI : Dominio ADQUISICION E IMPLEMENTACION Contiene 7 procesos COBIT  
 ME: Dominio MONITOREO Y EVALUACION Contiene 4 procesos COBIT

Como resultado de la labor adelantada a Noviembre de 2009, KPMG recomendó mantener los esfuerzos en los procesos que mejoraron y centrar los esfuerzos de la gestión de la entidad en la optimización de los siguientes procesos de control a saber:

- Plan Estratégico de TI
- Arquitectura de la Información
- Administración de proyectos
- Definir procesos, organización y relaciones de TI
- Administrar la inversión de TI
- Comunicar las aspiraciones y dirección de la gerencia
- Administrar recursos humanos de Ti
- Definir y administrar niveles de servicio
- Administrar servicios de terceros
- Administrar desempeño y capacidad
- Garantizar la continuidad del servicio

- Garantizar la seguridad de los sistemas

La administración ha desarrollado un plan de trabajo para el año 2010 para adelantar mejoras en los siguientes frentes y procesos de TI, y ha asignado un presupuesto aprobado por la Junta Directiva para su ejecución:

- Plan Estratégico de TI
- Arquitectura de la Información
- Administración de proyectos
- Administración y estrategia de Backups
- Administración de BI, en especial el manejo de la administración de datos históricos.
- Administración del desempeño y capacidad, en particular con inversiones para fortalecer los ambientes de producción y prueba.
- Plan de trabajo para responder a las exigencias de definición de procesos tecnológicos contemplados en la Circular 14 y 38 de 2009 de la Superintendencia Financiera. Al respecto la administración ha planteado un esfuerzo de definición de GAP y de un plan de trabajo para cubrir las exigencias en los plazos establecidos por la Norma.

Debido a la proximidad de la terminación del contrato de Auditoría Externa establecida para enero de 2010, el Depósito elaboró los términos de referencia para la contratación del servicio de Auditoría Externa por dos años, para lo cual se extendió la invitación a las firmas Ernst and Young, BDO y KPMG con quienes se surtirá el proceso de selección durante el mes de enero de 2010.

#### **4. CONCLUSION**

Durante el año 2009, Auditoria Interna cumplió con las actividades y funciones exigidas en la Circular Externa 014 de 2009 de la SFC y la Circular Externa 038 de 2009 de la SFC en lo relacionado con el sistema de control interno. La gestión de auditoria durante el año mencionado alcanzó el 89% de la ejecución del plan y en adición a lo establecido en el mismo plan se emitieron 38 observaciones de auditoria. No se presentaron limitaciones al alcance y las recomendaciones de auditoria se presentaron a la administración de manera oportuna.

## 5. ANEXO DOMINIOS COBIT POR MACROPROCESO

Dominios COBIT	PROCESO COBIT 4.1
PO - Planeación y Organización	PO1 Definir el plan estratégico de TI.
	PO2 Definir la arquitectura de la información
	PO3 Determinar la dirección tecnológica.
	PO4 Definir procesos, organización y relaciones de TI.
	PO5 Administrar la inversión en TI.
	PO6 Comunicar las aspiraciones y la dirección de la gerencia.
	PO7 Administrar recursos humanos de TI.
	PO8 Administrar calidad
	PO9 Evaluar y administrar riesgos de TI
	PO10 Administrar proyectos.
AI - Adquirir e Implementar	AI1 Identificar soluciones automatizadas.
	AI2 Adquirir y mantener el software aplicativo.
	AI3 Adquirir y mantener la infraestructura tecnológica
	AI4 Facilitar la operación y el uso.
	AI5 Adquirir recursos de TI.
	AI6 Administrar cambios.
	AI7 Instalar y acreditar soluciones y cambios.
DS- Entrega y Soporte	DS1 Definir y administrar niveles de servicio.
	DS2 Administrar servicios de terceros.
	DS3 Administrar desempeño y capacidad.
	DS4 Garantizar la continuidad del servicio.
	DS5 Garantizar la seguridad de los sistemas.
	DS6 Identificar y asignar costos.
	DS7 Educar y entrenar a los usuarios.
	DS8 Administrar la mesa de servicio y los incidentes.
	DS9 Administrar la configuración.
	DS10 Administrar los problemas.
	DS11 Administrar los datos.
	DS12 Administrar el ambiente físico.
	DS13 Administrar las operaciones
ME - Monitorear y Evaluar	ME1 Monitorear y evaluar el desempeño de TI.
	ME2 Monitorear y evaluar el control interno
	ME3 Garantizar cumplimiento regulatorio.
	ME4 Proporcionar gobierno de TI.