

Aplicación de la norma COBIT en el monitoreo de transferencias electrónicas de datos contable-financieros

*Carolina Graterol Benavides *Aymara Hernández Arias

Recibido: 20 de Junio 2011, Aceptado:10 de Diciembre 2011

Resumen

Las organizaciones usan las tecnologías de información y comunicación (TICs) para facilitar la gestión y control de sus procesos internos, fijando como directriz principal la alineación con las estrategias empresariales establecidas. Partiendo de esta premisa, se fija como objetivo general del presente artículo: presentar los resultados de la aplicación de la norma COBIT (Control Objectives for Information and Related Technology) en el proceso de monitoreo de las transferencias electrónicas de datos contables, financieros y administrativos de la Unidad de Contraloría y Administración de la Región Occidente del Grupo Lácteos Los Andes. La organización considera que dicho proceso es crítico, lo cual se justifica gracias al valor de la información transferida en la elaboración de informes de gestión. Se trata de un proyecto factible, el cual involucra la aplicación de conocimiento, a través del uso de un modelo o marco de trabajo relacionado con la administración de recursos informáticos.

Palabras clave: Auditoría informática, COBIT, transferencia electrónica de datos, monitoreo de procesos.

Application of the COBIT framework in the monitoring process of the financial, countable data electronic interchange

Abstract

The information and communication technology (ICT's) are used by the organizations in order to facilitate the administration and control of their internal processes. The principal guideline is to achieve the linkage between business strategies and ICTs strategies. Taking this premise as our starting-point, the general objective of this article is to present the results of the application of the COBIT framework (Control Objectives for Information and Related Technology) in the monitoring process of the financial, countable and administrative data electronic interchange of the "Lácteos Los Andes" Western Region Controllershship and Administration Unit. The mentioned process is critical for the organization on account of the value of the information transfered for the preparation of management reports. This study is a feasible project, which takes into account the knowledge application through a framework related to ICTs resources management.

Keywords: Information and communication technology audit, COBIT, data electronic interchange, monitoring process.

Introducción

En la actualidad, para las organizaciones empresariales, es vital que se evalúen constante y regularmente todos los procesos que en ellas se llevan a cabo, con el fin de verificar su calidad y suficiencia en cuanto a los requerimientos de negocio para la información: control, integridad y confidencialidad. Por ello, los sistemas informáticos, como medios automatizados para soportar dichos procesos, permiten

*Decanato de Administración y Contaduría, Universidad Centroccidental "Lisandro Alvarado", Barquisimeto, Venezuela, caritograterol@gmail.com, ahernand@ucla.edu.ve

materializar uno de los recursos relevantes para cualquier organización empresarial: la información que cada día genera (Piattini y Del Peso, 1998; Ruiz, 1999; Echenique, 2001). En relación a la información, la gestión requiere un aumento en la calidad, funcionalidad y facilidad de uso; disminuyendo a la vez períodos de entrega; y mejorando continuamente los niveles de servicio (con la exigencia de que esto se lleve a cabo con costos más bajos (Ruiz, 1999:33). Se requiere de normas y/o programas que puedan ser utilizados en la evaluación del funcionamiento de los sistemas de información utilizados y en el análisis de la eficiencia del control interno, además de la verificación del cumplimiento de la normativa general de la empresa y la revisión de la gestión eficaz de los recursos materiales y humanos en el ámbito informático. Estos aspectos integran el dominio de estudio de la auditoría informática. Se parte de la revisión de normas de auditoría, disponibles y utilizadas a nivel internacional, tales como: COSO (Committee of Sponsoring Organizations of the Treadway Commission Internal Control-Integrated Framework, EEUU 1992), ITIL (Information Technology Infrastructure Library, Inglaterra 1990), ISO/IEC 17799:2000 (International Organization for Standardization/International Electrotechnical Commission, Inglaterra 2000) y COBIT (Control Objectives for Information and Related Technology IT, EEUU 1998).

Tomando en consideración la descripción, alcance y objetivos de las mismas, la norma COBIT surge como una alternativa factible para ser utilizada como una guía de acción al momento de garantizar la calidad de los procesos relacionados con el monitoreo, control, calidad y seguridad de los datos correspondientes a transacciones contables. COBIT es la fusión entre prácticas de informática (ITIL, ISO/IEC 17799) y prácticas de control (COSO), las cuales plantean tres tipos de requerimientos de negocio para la información: requerimientos de calidad (calidad, costo y entrega de servicio), requerimientos fiduciarios (efectividad y eficiencia de operaciones, confiabilidad de la información y cumplimiento de las leyes y regulaciones), y por último, requerimientos de Seguridad (confidencialidad, integridad y disponibilidad). Todo lo anterior bajo la auditoría o revisión de cuatro dominios de control, como lo son: planificación y organización, adquisición e implementación, entrega/soporte y monitoreo. Siendo una norma flexible para la auditoría de control, sus dominios pueden ser evaluados de manera aislada dependiendo de las necesidades de la gerencia. Cabe mencionar que un estudio completo de todos los dominios logrará mayor integración de las necesidades de la gerencia, en cuanto al control de la tecnología, la generación de información y ejecución de los procesos.

La toma de decisiones de toda organización depende principalmente de los resultados de sus operaciones. Sin embargo, los recursos y tecnologías, utilizados para ejecutar dichas operaciones, deben ser administrados para garantizar el control de riesgos, el cumplimiento de los parámetros de calidad y la adecuada implantación de medidas de seguridad. La necesidad de control, tanto en la información como en la tecnología de información, ha sido punta de lanza para la implementación de normas de aceptación general a nivel mundial, como lo son: COSO, ISO/IEC 17799:2000, ITIL, COBIT, entre otros. Dichos marcos de trabajo se han convertido en instrumentos gerenciales que ofrecen a los directivos, ejecutivos, gerentes y auditores un conjunto de prácticas que permiten aumentar el valor de la información y reducir los riesgos relacionados con los ámbitos informáticos, con la finalidad de suministrar información más efectiva, eficiente, íntegra y confiable. A pesar de que las ventajas ofrecidas por las tecnologías son numerosas, el procesamiento de datos automático y la incorporación de sistemas de información basados en red en las organizaciones, en forma específica, ha disminuido los niveles de seguridad de la data y ha aumentado la vulnerabilidad de los sistemas (Laudon y Laudon, 2000). Existen casos de empresas que no poseen cultura de controlar y asegurar la información que generan sus sistemas de información. Utilizan la tecnología de información y comunicación porque conocen sus ventajas, sin darse cuenta que la misma debe ser controlada y supervisada para un adecuado desarrollo de sus operaciones, garantizando así, la seguridad de la información¹. Se evita de esta manera, desde la fuga de información hasta manejos

¹como resultado de una creciente interconexión, los sistemas y las redes de información son más vulnerables, ya que están expuestos a un número creciente, así como a una mayor variedad, de amenazas y de vulnerabilidades. Esto hace que surjan nuevos retos que deben abordarse en materia de seguridad” (Organización para la Cooperación y el Desarrollo Económicos OECD , 2002: 6). Por estas razones, desde 1992, la OCDE, trabaja en conjunto con los países miembros en la elaboración de las Guías para la Seguridad de los Sistemas de Información y Redes. Dos de los propósitos principales de las guías mencionadas establecen la necesidad de promover una cultura de seguridad entre todos los participantes como medio de proteger los sistemas y redes de información e incrementar la concienciación sobre el riesgo de los sistemas y redes de

internos no adecuados, que de una u otra forma, modifiquen los resultados de los procesos de generación de información utilizada para la toma de decisiones. La situación señalada se manifiesta en el llamado despilfarro computacional, caracterizado por el uso inapropiado de la tecnología de información, el cual afecta el ejercicio del negocio por la carencia de una adecuada administración. De allí la importancia de controlar, supervisar, asegurar y monitorear las operaciones procesadas por estos medios tecnológicos; la auditoría informática puede proporcionar las herramientas necesarias para este fin, basándose en la utilización de normas internacionales de seguridad en información y de administración de las TIC's.

De acuerdo a lo antes planteado, el objetivo general de este artículo de investigación se enfoca en presentar los resultados de la aplicación de la norma COBIT (Control Objectives for Information and Related Technology) en el proceso de monitoreo de las transferencias electrónicas de datos contables, financieros y administrativos de la Unidad de Contraloría y Administración de la Región Occidente del Grupo Lácteos Los Andes. Cabe destacar, que la utilidad de este estudio viene dada por la formulación de normas de control, que permitirán corregir fallas, métodos o procedimientos inadecuados en las revisiones vía sistema de información (monitoreo), tomando como referencia estándares generalmente aceptados a nivel mundial. De esta manera, se estará en capacidad de establecer un sistema de control interno que permita garantizar calidad y suficiencia, en cuanto a los requerimientos de integridad, confiabilidad, seguridad y control de la información para la gerencia, los usuarios finales y los auditores. Se inicia con la síntesis de ciertos fundamentos teóricos relacionados con el área de interés como son: la auditoría de sistemas de información y el proceso de control interno en el ámbito informático. Posteriormente, se incluyen los aspectos metodológicos que guiaron el desarrollo del estudio y, por último, se presentan los resultados, conclusiones y recomendaciones.

Fundamentos teóricos

Auditoría de sistemas de información

Cada día es mayor el número de situaciones irregulares que se presentan, como consecuencia del uso y aplicación de las TIC's, en diversidad de organizaciones. Una auditoría de sistemas de información enmarca su ámbito desde el proceso de construcción del sistema, adecuación y uso del paquete computacional, hasta la calidad del producto terminado (producto computarizado). Todo esto enfocándose bajo la perspectiva de control interno del software y del entorno operativo. De acuerdo a lo antes expuesto, la firma Auditoría de Sistemas de Barcelona, España (2004), define como objetivos generales de la auditoría de sistemas informáticos, los siguientes: asegurar la integridad, confidencialidad y confiabilidad de la información, minimizar existencias de riesgos en el uso de tecnología de información, conocer la situación actual del área informática para lograr los objetivos, garantizando la seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático, así como también seguridad del personal, los datos, el hardware, el software y las instalaciones. Además de, buscar una mejor relación costo-beneficio de los sistemas automáticos y tomar decisiones en cuanto a inversiones para la tecnología de información. Así como incrementar la satisfacción de los usuarios de los sistemas informáticos, fomentando para ello, la capacitación y educación sobre controles en los sistemas de información.

El proceso de control interno en el ámbito informático

Un control interno es un proceso mediante el cual la administración, los directivos y/o la alta gerencia le proporcionan a sus actividades un grado razonable de confianza, que le garantice la consecución de sus objetivos, tomando en cuenta: la eficacia y eficiencia de las operaciones, fiabilidad de la información financiera y cumplimiento de las leyes y normas aplicables, con la finalidad de dotar a la organización medidas preventivas, detección y corrección de errores, fallos y fraudes o sabotajes (Governance Institute,

información; sobre las políticas, prácticas, medidas y procedimientos disponibles para poder afrontar estos riesgos; así como sobre la necesidad de adoptarlos y ejecutarlos (OECD, 2002).

2000a). Hoy en día, las tecnologías de la información están presentes en todas las áreas de las organizaciones. Según De la Fuente (2000), esta implantación generalizada de los sistemas de información se ha realizado en muchos casos sin la necesaria planificación, en parte porque los conceptos necesarios no estaban suficientemente desarrollados o porque la implantación de controles era muy costosa. Sin embargo, debido a la creciente dependencia de las TIC's en las organizaciones, existe desde la década de los noventa hasta la actualidad un movimiento internacional cuya misión es la de innovar en normas o códigos de controles de éstas con la finalidad de minimizar las brechas entre los riesgos y la adecuación de las TIC's. Surgen entonces numerosos modelos de control y administración de las mismas, según Datamation (2004), entre los más utilizados están: ISO/IEC 17799:2000 e ITIL. Estos marcos de referencias son utilizados a nivel internacional y su uso depende de los requerimientos de la organización auditada, sin embargo, las necesidades mundiales en controlar la tecnología y la información hizo posible la creación de un marco referencial que los integre y que cubra las exigencias actuales de las organizaciones. De manera aislada se pueden implantar estas herramientas pero atacan un solo aspecto. De allí, el nacimiento en 1996 de un nuevo modelo gerencial llamado COBIT, el cual fusiona prácticas de informática ya existentes como ISO/IEC 17799:2000 e ITIL con prácticas de control interno como COSO en Estados Unidos, CADBURY en Inglaterra, COCO en Canadá, entre otras. COBIT es una herramienta gerencial que le permite a las organizaciones grandes o pequeñas administrar la información de manera efectiva, eficiente, integra y confiable, bajo el estudio de los procesos y actividades, utilizando los recursos de la tecnología de información como los datos, las aplicaciones, tecnología y el recurso humano, con la finalidad de satisfacer los objetivos del negocio, en donde la información necesita cumplir con ciertos criterios, a los cuales COBIT le llama requerimientos de negocio para la información.

Aspectos metodológicos

La investigación origen del presente artículo se enmarcó en la modalidad de proyecto factible, puesto que se orientó a la implementación de un modelo operativo viable de revisión con la aplicación de una norma internacional como es COBIT. Esto con la finalidad de cubrir los requerimientos de proceso de revisión por monitoreo de las operaciones vía sistema de información, la cual utiliza la plataforma tecnológica del Grupo Lácteos Los Andes en la Unidad de Contraloría y Administración Región Occidente. Las fases desarrolladas fueron: Fase I. Diagnóstico de la situación. Se efectuó el diagnóstico de la situación real en forma objetiva; Fase II. Análisis de la normativa COBIT en el ámbito de monitoreo. En esta fase se analizaron los diferentes objetivos, lineamientos, alcances procedimientos, control interno en el monitoreo de las operaciones; Fase III. Levantamiento de la información para la ejecución de una prueba piloto, con la finalidad de determinar los posibles obstáculos que se pueden presentar con la implementación de la norma y así lograr adaptarla y Fase IV. Elaboración del Informe Final contentivo de los resultados y conclusiones.

Unidades de información objeto de estudio

Para la puesta en marcha de este trabajo, se escogieron tres (3) sistemas de información de las distribuidoras de la Región Occidente de los diez y seis (16) disponibles, para los cuales se contó con autorización para el acceso de información. Por tratarse de una selección intencional, se tuvo la potestad de decidir la muestra, sin necesidad de definir el número de casos que tiene posibilidad de ser escogido. Las muestras intencionales o no probabilísticas se utilizan en estudios de caso donde la medición no es tan importante como el análisis en profundidad (Bethencourt, 2004). La escogencia intencional de estos sistemas de información obedece a la experiencia de los usuarios de la información de la Unidad de Contraloría y Administración Región Occidente, ya que por el volumen de información, el uso del sistema de facturación a través de pocket, problemas de comunicación, fallas de luz eléctrica y los resultados de los informes de auditoría interna durante el año 2007-2008, fueron considerados como escenarios complejos que abarcan los intereses de estudio. De acuerdo a esta premisa, los sistemas a estudiar serían los utilizados por las Distribuidoras: Andilago y Andibarinas. La primera es considerada como la distribuidora

que mantiene el mayor número de Rutas Directas que utilizan la facturación móvil representando un 32% de rutas directas en toda la región occidente, y la segunda, por presentar problemas de fallas eléctricas que dañan archivos en el sistema de información para la emisión de información y errores en la transferencia electrónica de datos contable-financieros, y Andilara, por ser la primera distribuidora de la Región Occidente calificada por la Administración Tributaria como contribuyente especial, por lo cual debe emitir información veraz, oportuna y confiable para esta institución debido a que es fiscalizada con mayor frecuencia. Cada experiencia en la resolución de casos en estas distribuidoras servirá para abordar y atacar cualquier irregularidad que se presente en la emisión de información y/o procesamiento de datos en cualquier otro sistema de información, fortaleciendo el control interno en el monitoreo de las operaciones contable-financieras de la organización.

Técnicas e instrumentos de recolección de datos

Se utilizaron técnicas de recolección de datos, tales como: la observación directa, la revisión de materiales referenciales y las entrevistas no estructuradas. Además de los instrumentos y guías de diagnóstico y control COBIT. Uno de ellos fue el checklist de la Guía de Auditoría Genérica de COBIT (Governance Institute, 2000a). A través del mismo se garantizó la obtención de datos y opiniones relevantes, además de proporcionar fuentes adicionales orientadas a corroborar las evidencias de la auditoría. Así mismo, se realizaron sesiones con informantes claves basadas en los lineamientos de la norma o estándar utilizado, específicamente la ficha para el diagnóstico de conocimiento gerencial (Gueldentops, 2003). Se consideraron seis (7) informantes claves dentro de la organización, sobre la base de su conocimiento y experiencia en el proceso de transferencias electrónicas de datos: (a) Unidad de Contraloría y Administración Región Occidente (1 Contralor Principal y 2 Contralores Revisores), usuarios directos del proceso en estudio; (b) Coordinación General de Sistemas (1 Coordinador y 2 Analistas de Sistemas), quienes a su vez son usuarios y encargados de gestionar la plataforma tecnológica, administrar la seguridad de la misma y brindar soporte técnico a resto de los usuarios; y por último, (c) Auditoría (1 Auditor Interno), usuario del sistema y encargado de las evaluaciones de los controles y procesos administrativos.

Desarrollo y resultados de la investigación

El punto de partida se establece en función de las siguientes interrogantes: el proceso de monitoreo de las transacciones contables a través de la transferencia electrónica de datos (tomando en cuenta los datos, procesamiento y salida de la información para la Unidad de Contraloría y Administración de la Región Occidente) contará con un sistema de control que garantice a la organización requerimientos de calidad, reportes fiduciarios y de seguridad? Este proceso de monitoreo permitirá además, minimizar los riesgos de vulnerabilidad del sistema de información utilizado? Reconociendo que toda auditoría requiere de una adecuada planeación (Piattini y Del Peso, 1998), inicialmente se definieron los siguientes aspectos: (a) Objetivos y alcance del trabajo de auditoría informática: Asegurar que el proceso de transferencia de datos contable-financieros desde las estaciones de cada distribuidora hasta el servidor master del Staff, esté definido para el logro de los objetivos del negocio y proporcione seguridad respecto a las operaciones eficientes y efectivas además del cumplimiento de las leyes y regulaciones; (b) Técnicas y herramientas a utilizar: Lineamientos y conjunto de herramientas de implementación COBIT en el dominio específico de Monitoreo de Procesos (ME 1 y ME2); (c) Horas hombres a requerir para la ejecución de la revisión: 2 horas diarias de lunes a viernes en el período entre septiembre noviembre 2008 y (d) Recursos requeridos: portátil, impresora, disponibilidad de conexión a Internet, software de productividad (procesador de palabras, hoja electrónica de calculo, programa para la presentaciones multimedia), papeles de trabajo previos, informes de auditorías anteriores y espacio físico de trabajo. Dentro de la planeación también se incluye la actividad de comprensión del negocio y de su ambiente, a través de la cual el auditor logra una visión general de la organización y de los procesos internos en el área de estudio. De acuerdo a esto se ejecutaron tres etapas: (a) Conocimiento general de la organización: se describe la organización y su entorno. Esto con la finalidad de lograr una mayor comprensión de los

siguientes aspectos: requerimientos de negocio y riesgos asociados, estructura de la organización, roles y responsabilidades, políticas y procedimientos, leyes y regulaciones, indicadores de control establecidos y reportes gerenciales (Governance Institute, 2000a); (b) Conocimiento general de la Unidad responsable del proceso bajo estudio: en esta fase se describe la unidad en cuanto a su alcance, funciones, actividades que realiza y plataforma tecnológica disponible y (c) Conocimiento general del proceso en estudio y del Sistema de Información utilizado por la organización: aquí se expone el proceso de transferencia de datos contable-financieros desde los centros de distribución hasta el servidor master del Staff. Así como también, se describe el sistema de información utilizado por la organización. A continuación se detallan los resultados obtenidos al ejecutar cada una de las etapas mencionadas:

- a) **Conocimiento general de la organización:** a) El Grupo Lácteos Los Andes está constituido por tres plantas y sus distribuidoras exclusivas a nivel nacional. La misma nace el 15 de Diciembre de 1986 en Nueva Bolivia, Estado Mérida. En 1987 inicia su producción de suero pasteurizado y posteriormente amplía sus líneas de productos introduciendo al mercado yogurt líquido, yogurt firme, arroz con leche y gelatinas bajo la marca Los Andes. La comercialización de sus productos está distribuida por gerencias de cada zona (Oriente, Centro y Occidente). Para 1998, se adquieren una serie de centros de distribución: en la región oriental (Andioriente, C.A.), y en la región occidental (Andilara, C.A., Andilago, C.A., Andival, C.A., Lácteos Araure, C.A, entre otros). Para el año 1999 el Grupo Lácteos Los Andes ya se había consolidado como una de las marcas competitivas a nivel nacional en este ramo. Hoy en día el grupo posee un posicionamiento en el mercado nacional de distribución y comercialización de un 35 % ². La competencia esta representada por las marcas: Prolaca-Parmlat (31 % de participación), Carabobo-California (30 %), el resto Leche Táchira, Jugos Yaracuy e Inlaca, entre otras marcas. En cuanto a los elementos del mercadeo que aportan niveles de competitividad se pueden mencionar los planes de mercadeo y ventas, disminución de los tiempos de entrega y mejora en la calidad de servicio post-venta. El precio del producto no es considerado como factor de competitividad, por encontrarse este en el mismo rango de los de su competencia, aspecto que se compensa por la calidad y desempeño de los productos, amplia gama de productos ofrecidos para la venta y los servicios post-venta a los clientes. La necesidad de establecer políticas y directrices uniformes requirió de la conformación de un grupo de profesionales en las áreas de ventas, administración, recursos humanos como de sistemas. Más adelante, en el año 2000, se incorpora a éste equipo un auditor interno. Paralelamente al crecimiento y diversificación de productos, nace la Unidad de Staff, ya que para lograr mantenerse en el mercado se requería de una adecuada administración y control de las ventas, los recursos humanos, recursos económicos y financieros en cada región. Este notable crecimiento hace que la información financiera procesada por el sistema de información sea considerada como elemento fundamental para la toma de decisiones en el manejo del negocio, demandando un mayor control de las operaciones procesadas en el sistema de información. La organización cuenta con políticas establecidas para el procesamiento de la información, sin embargo, actualmente se está en un proceso de normalización con la finalidad de estandarizar los procesos contables, administrativos y operativos tanto de las distribuidoras como de las Plantas de producción, ya que los mismos no se encuentran formalmente descritos en un manual de cargos y funciones. En relación al párrafo anterior, además de poseer normas y políticas internas para su buen funcionamiento y mejoramiento continuo, sus operaciones e información están enmarcadas bajo una serie de leyes y regulaciones³, tales como:

- Constitución de la República Bolivariana de Venezuela
- Ley de Administración Financiera del Sector Público
- Ley Orgánica del Trabajo

²Estadísticas realizadas por las Gerencias de Comercialización de acuerdo al incremento de ventas a nivel nacional durante el año 2006-2008 publicado en la página <http://www.guia.com.ve/noticias/?id=19915> (Consulta: Febrero 2009).

³Disponibles en el portal del Centro Nacional de Tecnologías de Información y Comunicación (CNTI), institución adscrita al Ministerio del Poder Popular para Ciencia, Tecnologías e Industrias Intermedias de la República Bolivariana de Venezuela.

- Ley Orgánica de la Administración Pública
- Ley del Impuesto al Valor Agregado
- Principios de Contabilidad generalmente aceptados
- Código civil Venezolano
- Normas Internacionales de contabilidad
- Ley Orgánica de la contaduría
- Ley de Régimen Presupuestario
- Ley del Impuesto sobre la renta
- Impuesto municipales, tales como: publicidad comercial, patente de vehículo, inmuebles urbanos e impuestos sobre actividades económicas de industria, comercio, servicios o índole similar.

b) **Conocimiento general de la unidad responsable del proceso bajo estudio:** a) Debido su crecimiento económico, el Grupo Lácteos Los Andes ha creado una nueva unidad orgánica en su estructura organizativa: la Unidad de Contraloría y Administración en cada región, siendo una de sus funciones principales controlar, supervisar, normar, los procesos administrativos para el uso adecuado de los sistemas de información y las aplicaciones. La meta de ésta unidad es monitorear las operaciones a través del sistema de red. Esto con la finalidad de garantizarle a la gerencia resultados contable-financieros fidedignos y minimizar los riesgos inherentes al manejo y uso del sistema de información utilizado por la organización. En este caso los mayores riesgos informáticos se corren en el proceso de transferencia electrónica de datos contable-financieros desde el servidor de cada centro de distribución de la región occidente hasta el servidor de la Unidad de Contraloría y Administración ubicado en la ciudad de Barquisimeto estado Lara. Como toda organización, el Grupo Lácteos Los Andes está expuesto a que alguien con los conocimientos adecuados pueda modificar intencionalmente la información, genere transacciones falsas, incremente u oculte saldos en las cuentas, realice cuadros de inventarios, genere ventas ficticias, etc. Situaciones que pueden generar riesgos, tales como la emisión de información errada para la toma de decisiones y pérdidas millonarias en el control de las operaciones ⁴ Por otra parte, en la realización de los reversos de documentos de inventario a través de los pockets (computadoras de bolsillos), tales como facturas de ventas, notas de crédito o notas de devoluciones y los procesos de descarga de la data de los mismos al servidor master de cada distribuidora, se han detectado alteraciones significativas de datos de contabilidad de meses anteriores. Lo anterior ha generado, que al momento de comparar la información original con la información arrojada al final de los procesos de transmisión, se detecten diferencias, inconsistencias o desfases, producto de fallas en los sistemas. Estos problemas acarrear costos (horas-hombres) a la organización en corrección de los datos y de la correspondiente reconstrucción de la información generada. La Unidad de Contraloría y Administración Región Occidente está conformada por un (1) Contralor Principal, quien se encarga de supervisar el trabajo del personal a su cargo y establecer directrices, normas, políticas de control, revisión y de manejo adecuado del sistema contable-financiero; dos (2) contralores revisores, quienes son los responsables de realizar las revisiones vía sistema de información, reportar al Contralor Principal las conclusiones, recomendaciones, debilidades o fortalezas. Además tienen a su cargo los usuarios del sistema de información de cada centro de distribución, quienes son los que alimentan la data contable-financiera generada por toda la organización. Para la realización de sus actividades, la Unidad de Contraloría y Administración Región Occidente, cuenta con una plataforma informática, la cual incluye una

⁴...”los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas, que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles” (Pecantet, 2006).

red cliente-servidor la cual distribuye la información de toda la unidad de staff de la región.⁵ Para cumplir con las funciones de: normar, controlar, supervisar y monitorear los procesos administrativos realiza varias actividades a objeto de detectar, corregir y mejorar los controles internos. Dentro de las actividades relacionadas a su función, se tienen: (a) Revisión de las actualizaciones del sistema: Constantemente el sistema de información es actualizado a través de un enlace que se ejecuta por medio de la Intranet Orbisnet⁶ de la Organización. Se realizan las pruebas para validar que la actualización cumpla con las condiciones de control interno establecidas y no alteren o dañen la data, (b) Solución de casos: Se corrigen errores del sistema por pérdida de algún registro o archivo o por errores de usuario que afectan la data procesada. De no poder solventarlo, se crea un caso de soporte usuario a la Coordinación General de Sistemas a través de la Intranet Orbisnet; (c) Emisión de informes a la Gerencia: Se emiten informes a la gerencia con los resultados de la revisión de data contable-financiera. También se entrega un memorando de control interno, en el cual se evidencian los riesgos detectados, consecuencias, solución y oportunidades de mejora del sistema de información y (d) Ejecución, revisión y verificación de las transferencias electrónicas de datos al servidor: Puesto que la Unidad de Contraloría y Administración Región Occidente depende de los recursos TICs, se debe garantizar la calidad, confiabilidad y control de la información emitida por el sistema.

- c) **Conocimiento general del proceso de transferencia electrónica de datos y del sistema de información utilizado por la organización:** La alimentación de la data, a los servidores de las Unidades de Contraloría y Administración de las zonas (occidente, centro y oriente), se realiza a través de transferencias nocturnas de datos desde cada centro de distribución o descompresión de discos compactos de respaldo en el servidor. Para lograr la comunicación entre distribuidora y el Servidor Staff, la organización cuenta con una plataforma de comunicación de tecnología de red, que le proporciona un medio para aprovechar un canal público de Internet como si fuera un canal privado, esto es la VPN (Virtual Private Network). La organización cuenta con el servicio de Internet, el cual es prestado por dos proveedores nacionales. Los mismos ofrecen servicios de conexión banda ancha por medio de módem y a través de la transmisión de datos por tramas llamada Frame Relay utilizando un router. Ambos facilitan la comunicación y permiten compartir información desde la Distribuidora hacia el servidor de la Unidad de Contraloría y Administración y viceversa. La conexión vía remota se ejecuta mediante dos programas denominados Symantec pcAnywhere⁷ y/o UltraVNC⁸ La organización utiliza desde el año 1999 un sistema de información contable adaptado a sus requerimientos. La versión actual utiliza el manejador de base de datos Foxprox 2.6 de Microsoft. Dicho sistema está estructurado y programado con un método coherente que le permite una conceptualización modular bajo un esquema de integración. Está orientado al usuario, con submódulos de diseño y generación de reportes y consultas, totalmente probados para Arquitectura cliente-servidor, en redes Windows NT. Las actividades del proceso de transferencias contemplan la revisión de las transferencias de datos al servidor y la verificación de la data contable

⁵Los equipos de computación tienen instalado las siguientes versiones de software: Microsoft Windows XP Professional, con sesión para usuario limitado. Microsoft Office 2003, Roxio Inc Easy CD & DVD Version 6.0.0.0.209, Asistente para ajustar la seguridad de .NET, Microsoft Internet Security and Acceleration Server 2000 Version 3.0, Antivirus Norton, Symantec Corporation pcAnywhere Versión 11.0, UltraVNC Versión 1.0.0.18, WinZip Version 8.0., Foxprox. Versión 2.6, Orbisnet Backorbis respaldo. Copyright 1998. COMSISA, Intranet Orbisnet Versión 1.0.4. Copyright 2006.

⁶“Infraestructura basada en los estándares y tecnologías de Internet que soporta compartir información dentro de un grupo de usuarios bien definido y limitado, bajo un esquema de seguridad que provee la misma red local de la empresa. Es una herramienta que posibilita acumular, administrar, clasificar y presentar, en forma adecuada, la comunicación e información interna de una empresa” (COMSISA, 2007).

⁷Programa de acceso y manejo de computadores desde conexión remota, que le proporciona mayor seguridad, compatible con varias plataformas (Windows Vista, Linux, and Mac OS X Universal) para resolver cualquier problema a distancia, y poder transferir datos de una estación a otra. Fuente: eval.symantec.com/mktginfo/enterprise/factsheets/DS-00364-SLPCA12fs.pdf (Consulta: Octubre 2008).

⁸Programa de acceso rápido que puede exhibir la pantalla de otra computadora (vía Internet o red) en su propia pantalla. El programa permite que se utilice el ratón y el teclado para controlar otra PC remotamente, es decir que se puede trabajar en una computadora alejada, como si se sentara delante de ella. Fuente: www.uvnc.com (Consulta: Octubre 2008).

transferida. Esta última incluye: (a) chequeo del reporte de evidencia lógica que emite el programa de transferencia Symantec Pcanywhere. En el mismo se registran: la hora en que se transmitieron cada uno de los archivos, el nombre de los archivos transferidos y un mensaje indicativo si ocurrieron interrupciones. (b) Reindexación de tablas de datos: Como mecanismo preventivo, después de cada transferencia, se requiere ejecutar el programa Organiza para que internamente reindexe las tablas de datos y así evitar que el sistema de información emita mensajes de error por inconsistencia en los archivos. (c) Revisión de transferencias a través de la ejecución del programa de fechas: Este programa es utilizado con la finalidad de verificar si la data transferida pertenece a un mismo periodo. De no ser así, se corre el riesgo de que la información emitida sea inconsistente. (d) Verificación de la integración de la data generada y procesada entre los módulos: Para ello se utilizan las opciones disponibles en el módulo de inventario de productos: auditoria de asientos contables, auditoria de caja, auditoria de notas de débito y crédito. Dichas opciones, al detectar discrepancias en los resultados obtenidos entre los módulos (contabilidad y cuentas), emite mensajes: deberían estar y no están, están con diferencias y están y no deberían estar en la contabilidad. Ya sea que el error se genere antes o durante la transferencia, se contacta al administrador de la distribuidora para que ejecute las opciones de auditoria y verifique los mensajes de conciliación. De ser así, éste debe corregirlo inmediatamente en su base de datos. De no existir problemas de auditoría, se compara a través de conexión remota si los datos del servidor son exactos al de la distribuidora. (e) Revisiones contable-financieras: Apoyándose en los distintos reportes que emite el sistema de información se procede a revisar si los mismos están razonablemente presentados acorde con los principios de contabilidad generalmente aceptados. (f) Revisiones de control interno del sistema de información: Se realizan pruebas de control interno de seguridad lógica del funcionamiento de los módulos y procesamiento de datos del sistema de información. Si en la revisión se detecta que un procedimiento contable administrativo de alimentación de data al sistema puede ser mejorado o no existe, la Unidad de Contraloría y Administración establece normas formales. Se pueden sintetizar estas dos funciones, las cuales son el objeto de estudio de la siguiente manera:

Proceso	Datos-Insumos	Actividades	Resultado
Transferencia de Datos	Data de Caja Contabilidad Inventario y de Cuentas	Transferencia automática a través de conexión. Transferencia manual a través de descompresión de disco de respaldo	Datos transferidos: <ul style="list-style-type: none"> • Comprobantes Contables • Estados financieros • Reportes financieros
Verificación de data transferida	Datos transferidos	Revisión de transferencia. Ejecución del programa para la reindexación de archivos y de verificación de fechas de los registros y auditoría.	Datos verificados de acuerdo a los criterios de calidad, fiduciaros y de seguridad.
	Datos descargados	Prueba de revisión de data contable.	Reporte de revisión: debilidades, riesgos, oportunidades de mejoras de controles internos de seguridad y alimentación.

Cuadro 1: Sistematización del proceso de transferencia electrónica de datos

Determinación de riesgos y amenazas del proceso

Con base al conocimiento del proceso, se pueden identificar los riesgos y las amenazas a los que está expuesto. Qué factores intervienen para que una transferencia de datos no se realice bien? De acuerdo a esta pregunta se tiene lo siguiente:

- **Amenazas:** fallas en el servicio de luz eléctrica, en el servicio de Internet (problemas de comunicación), fallas imputables o no al sistema Backorbis de Administración de respaldo, errores provocados por los usuarios (intencionales o no), problemas de configuración o instalación, etc., programas de antivirus desactualizados, daño físico o fallas técnicas del CPU master de la distribuidora o de las unidades de respaldo y condiciones ambientales que afecten el desempeño de las líneas de comunicación.
- **Riesgos:** alta probabilidad de omisión de los pasos de respaldo por parte del usuario (máquinas apagadas, máquinas sin conexión VPN, postergar la ejecución del respaldo; usuario trabajando en el sistema en hora de ejecución del evento del respaldo, etc.), alta probabilidad de CD de respaldo contengan virus, estén dañados o mal grabados; en las distribuidoras, existe la posibilidad de que los usuarios alteren por error las fechas y las unidades de almacenamiento estipuladas para el respaldo a través del programa Backorbis, debido que no existe un mecanismo de acceso restringido.

Actividades de control del proceso de transferencia

Un sistema de control interno enmarca una serie de mecanismos de controles manuales y/o automáticos que permiten detectar cualquier irregularidad, corregir errores o prevenirlos y asegurar el logro de los objetivos previstos (Piattini y Del Peso, 1998). Tal es el caso del proceso en estudio, el cual posee tanto controles automáticos como manuales (preventivos, detectivos y correctivos). A continuación se muestran los controles específicos establecidos en el proceso bajo estudio:

- a) **Controles Preventivos** mensaje de alerta para la ejecución del respaldo de datos tanto en la unidad C como en CD (Backorbis Administrador de respaldo), procedimiento y normas de ejecución de respaldo y custodia, definición de actividades de ejecución de la transferencia nocturna y asignación de clave para descomprimir CD de respaldo a través de la intranet
- b) **Controles Detectivos** mensajes de culminación del respaldo indicando si el mismo se ejecutó correctamente o presentó problemas, de culminación de la transferencia automática indicando si la misma se ejecutó correctamente o presentó problemas, reporte de congruencias de fechas de transferencias de datos entre los distintos módulos mediante la ejecución del programa de verificación de fechas en el servidor del Staff y mensajes de advertencia en pantalla, los cuales indican si la transferencia de data presento problemas. Estos mensajes se generan al ejecutar el programa de auditoría
- c) **Controles Correctivos** respaldo de los datos transferidos, el cual permite su recuperación, ejecución del programa Organiza, reconstrucción de índice a solicitud del usuario, repetición del proceso de transferencia de datos a solicitud del usuario, uso de CD de respaldo, repetición del proceso de generación automática de comprobantes contables en los cuales se hayan presentado problemas y conexión remota para solventar pérdida de archivos o repetir el proceso de transferencia de la data de ser el caso.

La aplicación correcta y continua de los controles mencionados garantizaría que la información transferida al servidor de la Unidad de Contraloría y Administración de acuerdo a los criterios de calidad, fiduciarios y de seguridad. Además permitiría sistematizar el proceso por medio de una documentación detallada de la revisión vía sistema de información de la data transferida. A continuación se presenta de manera

gráfica el proceso de transferencia electrónica de data sobre la base del modelo de cubo de COBIT. La estructura del modelo de cubo COBIT, adaptada al proceso de transferencia electrónica de datos contable-financiero, permite reflejar tres perspectivas distintas que pueden ser asumidas al trabajar sobre la base de los criterios y objetivos de control COBIT correspondientes al dominio de monitoreo (ver Figura No.1):

- El proceso bajo estudio, para el cual se deben garantizar mecanismos de control adecuados (preventivos, detectivos y correctivos) a fin de alcanzar las metas de efectividad, eficiencia, confidencialidad, disponibilidad, cumplimiento y confiabilidad.
- Los recursos TI disponibles (datos, computadores, redes, sistemas de información, recursos humanos, instalaciones, entre otros), los cuales deben ser administrados por los encargados del proceso y especialistas para alcanzar los objetivos en respuesta a los requerimientos de negocio.
- Los tres tipos de requerimientos de negocio que debe reunir la información para ser considerada adecuada a las necesidades de la organización (Aguirre, 2006): requerimientos de calidad (calidad, costo y entrega de servicio), requerimientos fiduciarios (efectividad y eficiencia de operaciones, confiabilidad de la información y cumplimiento de las leyes y regulaciones), y por último, requerimientos de Seguridad (confidencialidad, integridad y disponibilidad).

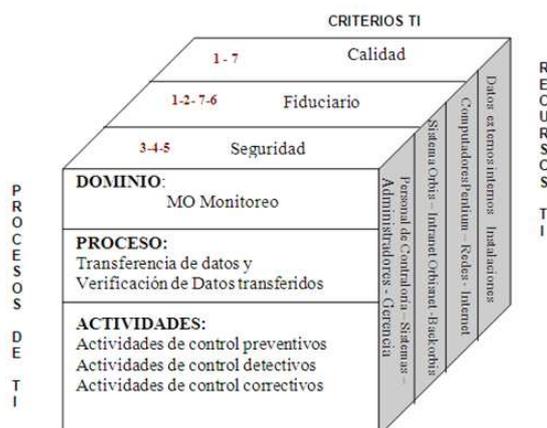
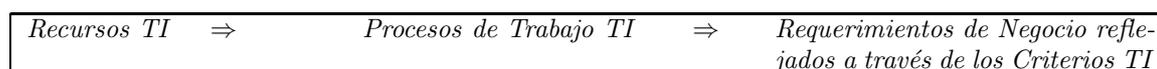


Figura 1: Modelo del cubo COBIT-Proceso de transferencia electrónica de datos contables financieros. Fuente: Governance Institute (2000a)

Al integrar dichas perspectivas se pueden sentar las bases para una gestión global del proceso bajo estudio, por parte de la gerencia de la empresa, de los encargados del proceso y de los especialistas TI (Aguirre, 2006). En líneas generales, las perspectivas representadas a través del cubo están relacionadas según se muestra en el cuadro 2:



Cuadro 2:

Aplicación de la guía genérica COBIT

El siguiente paso consistió en la aplicación de la guía genérica COBIT (Governance Institute, 2000a) en el proceso de interés. En este paso se pretende lograr lo siguiente: (1) Evaluar los controles. Evaluar la efectividad de los indicadores de control establecidos o el grado de alcance del objetivo de control. Básicamente decidir qué, por qué y cómo será controlado; (2) Evaluar la adecuación de los controles. Garantizar que los indicadores de control establecidos están trabajando de acuerdo a los objetivos previamente definidos, su consistencia y continuidad. Adecuación del ambiente general de control; (3) Corroborar los riesgos. Verificar cuáles son los riesgos potenciales en caso de que el objetivo de control no sea logrado usando técnicas analíticas y consultando fuentes adicionales. Siguiendo la guía genérica COBIT, se describen a continuación los pasos desarrollados:

- a) **Identificación/Documentación:** El objetivo de este paso “es permitir al auditor un mayor conocimiento de las tareas relacionadas con el objetivo de control e identificar si los gerentes TI creen que están controlando dicho objetivo. Incluye la identificación de los individuos que la ejecutan, proceso al cual pertenece y ubicación de la tarea, así como también los procedimientos establecidos para controlarla” (Governance Institute, 2000a). La primera actividad realizada fue la aplicación de entrevistas a nivel gerencial a los informantes claves para ganar una mayor comprensión del proceso de transferencia electrónica de los datos contable-financieros. Los resultados acerca de la percepción que poseen los entrevistados acerca del proceso se obtuvieron utilizando el instrumento de diagnóstico de conocimiento gerencial propuesto por Guldentops (2003), el cual contiene interrogantes tales como: El proceso es importante para el éxito de la empresa? Esta claro quien es el responsable de los resultados finales? El proceso es ejecutado de una manera formal? El proceso es ejecutado bien? Esta claro quien es el responsable del proceso? El proceso tiene objetivos y metas claros? El proceso es medido? El proceso es auditado? El proceso posee controles de debilidad conocidos? La tecnología utilizada tiene vulnerabilidades? Los entrevistados brindan su percepción indicando para cada interrogante el valor que ellos consideran apropiado basados en una escala específica (Status). Por ejemplo, para la interrogante: El proceso es importante para el éxito de la empresa? Se cuenta con la siguiente escala: 1 (Es crítico), 2 (Es muy significativo), 3 (Hace las cosas más fáciles), 4 (Se puede sobrevivir sin él) y 5 (No, en absoluto). La segunda actividad consistió en definir los responsables de las funciones del proceso. Para ello se utilizó una tabla RACI. Dicha tabla permite la documentación de quién es el responsable del proceso, quién debe rendir cuentas y quién debe ser consultado y/o informado. Todo con la finalidad de poder evaluar el grado de madurez (responsabilidad) del proceso de acuerdo a los objetivos de control detallado de COBIT. En este caso se puede decir que la estructura de responsables en el proceso es adecuada. Sin embargo, se propone involucrar a la auditoría interna en los objetivos de control, ya que ésta unidad le permitirá a futuro asegurar auditorías independientes, siendo uno de los objetivos de control del dominio de monitoreo (ME4).
- b) **Evaluación:** En este punto se utilizó el modelo de madurez COBIT para el control de procesos. Los mismos permiten a la Administración definir el punto donde la organización está hoy en relación con los estándares internacionales, así como determinar a donde se quiere llegar. A fin de definir el puntaje en la columna de grado de madurez de las tablas diseñadas para tal fin se utilizaron los índices o modelo de madurez indicados en el modelo COBIT. El objetivo de este paso es evaluar los procedimientos establecidos y determinar si los mismos proveen una estructura de control efectivo. Según el Programa de Auditoría COBIT, se deben identificar los procedimientos que permiten monitorear y evaluar la suficiencia del control interno asegurando que el proceso de las transferencias electrónicas de datos contable-financieros desde las estaciones de cada distribuidora hasta el servidor master del Staff, esté definido para el logro de los objetivos del negocio y proporcione seguridad respecto a las operaciones eficientes y efectivas además del cumplimiento de las leyes y regulaciones aplicables. Para ello se analizaron individualmente los objetivos de control de alto nivel correspondientes al dominio de monitoreo, específicamente los objetivos de control de alto

nivel ME1 y ME2, tomando algunos objetivos detallados de los mismos de acuerdo al alcance de la auditoría definida en el presente trabajo.

A continuación se describe el programa de auditoría desarrollado, específico para el dominio de Monitoreo, de acuerdo a los objetivos de control seleccionados para la revisión del proceso de transferencia y revisión de data contable-financiera (Governance Institute, 2000b):

- **Elementos de Revisión y prueba** Contempla las políticas y procedimientos del proceso de transferencia de datos contable-financieros desde las distribuidoras hasta el servidor del Staff, reportes de fallos, sistemas de controles, controles establecidos en el proceso en estudio, riesgos inherentes del proceso en estudio y la opinión de los involucrados en el proceso de transferencia de datos.
- **Papeles de Trabajo** Diagnóstico del conocimiento gerencial, Modelo de Madurez del Objetivo de control, Gráfica de RACI, Ficha de evaluación del control interno.
- **Objetivo de Negocio ME1** Monitorear el proceso.
 - **Efecto:** Evaluación del desempeño
 - **Objetivo de control de alto nivel:**
 - a) Recolectar datos de monitoreo. Garantizar el conocimiento del proceso.
 - b) Evaluar el desempeño. Realizar el análisis de la efectividad del proceso.
- **Objetivo de Negocio ME2** Evaluar la suficiencia del control interno.
 - **Efecto**
 - a) La definición de un sistema de control interno integrado en el marco de trabajo de los procesos de transferencia de datos.
 - b) Monitorear y reportar la efectividad de los controles internos existentes y propuestos para el mejoramiento continuo.
 - c) Reportar las excepciones de control a la gerencia para seleccionar las acciones pertinentes.
 - **Objetivo de control de alto nivel**
 - a) **Monitorear el marco de trabajo de control interno.** Se debe realizar la evaluación usando las mejores prácticas de la organización.
 - b) **Operación oportuna de los controles internos:** La confiabilidad en los controles internos requiere que operen rápidamente para detectar errores e inconsistencias y que éstos sean corregidos oportunamente.
 - c) **Reportes de nivel de control** Evaluar la complejidad y efectividad de los controles internos del proceso de transferencia de datos y la revisión de la data contable-financiera. Deberá llevarse a cabo acciones para identificar qué información es necesaria y a qué nivel en particular para facilitar la toma de decisiones.
 - d) **Aseguramiento de seguridad operacional y de control interno** Identificar medidas correctivas basadas en las evaluaciones y en los reportes de auto revisión. La actividad de Monitoreo por parte de la Unidad de Contraloría y Administración deberá revisar la existencia de puntos vulnerables y problemas de seguridad en el proceso de transferencia de datos contable-financieros y de revisión.

Una vez obtenidos resultados de la evaluación de acuerdo al modelo de madurez COBIT, se procedió a graficar los resultados e interpretar las evidencias obtenidas. Por último, se estructuró el Reporte final de Auditoría (ISACA, 2004), en el cual se plasmaron los siguientes aspectos: identificación de la organización, destinatarios del informe, restricciones de circulación, alcance de la auditoría, objetivos, periodo de cobertura, naturaleza de la labor de auditoría, plazo de la labor de auditoría y redacción

Informe Final con hallazgos, conclusiones y recomendaciones. Los hallazgos se sistematizaron en fichas de evaluación del Control Interno para cada uno de los objetivos de control del dominio bajo estudio, en las cuales se indicaban los siguientes aspectos: descripción del dominio, objetivo de control, responsable, nivel de relevancia, evaluación obtenida, responsable de la ejecución, nivel de importancia y riesgo, problemas detectados, opinión de la gerencia, recomendaciones, revisor y fecha. Para concluir, se presenta de manera gráfica el alcance de la prueba piloto de revisión y un resumen de los pasos desarrollados:

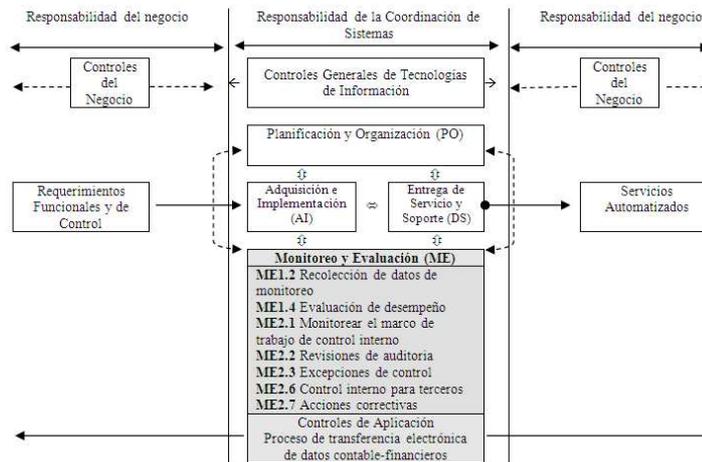


Figura 2: Alcance de la prueba piloto de revisión. Dominio de monitoreo(ME). Adaptación propia. Fuente: (IT Governance Institute (2007:16))

Conclusiones y recomendaciones

La ejecución de la revisión del proceso de monitoreo de las transferencias electrónicas de datos contable-financieros de la Unidad de Contraloría y Administración de la Región Occidente del Grupo Lácteos Los Andes aplicando las normas COBIT ha permitido, entre otros aspectos, evaluar la adecuación de los controles establecidos, detectar algunas debilidades y riesgos potenciales en el funcionamiento del mismo. A partir de la definición de los aspectos anteriores se puede estar en capacidad de realizar un análisis exhaustivo de los objetivos de control que son necesarios para garantizar el correcto funcionamiento, la operatividad continua y calidad de resultados. Siguiendo el modelo de madurez COBIT, el proceso está definido de manera formal por la Gerencia TICs y se han desarrollado políticas y procedimientos de evaluación y reportes, incluyendo programas de adiestramiento de usuarios responsables del proceso. Sin embargo, se requiere una mayor integración del sistema de control informático interno con el resto de los procesos relacionados con el área contable-financiera. En líneas generales se pueden plantear las siguientes recomendaciones: (a) Establecer una política de evaluación continua de monitoreo del proceso y de registro de indicadores de desempeño que permitan emitir información relevante para las actualizaciones de recursos tecnológicos (hardware y software); (b) Documentar los resultados de la evaluación de los controles de monitoreo con la finalidad de sistematizar el proceso de revisión, presentando así evidencias ante terceros para proveer auditorías independientes. El análisis de dichos reportes de control, por parte del equipo de trabajo, debe concretarse en el establecimiento de políticas que garanticen los criterios de calidad, fiduciaros y seguridad de la información y (c) Garantizar a futuro que los reportes de evaluación de control interno diseñados sean actualizados y utilizados por el equipo de trabajo encargado del monitoreo de procesos. Además, de formalizar el análisis de riesgos potenciales e impacto de manera de ejecutar oportunamente las acciones correctivas y mejorar el sistema de control informático.

Adicionalmente, es recomendable que la gerencia implante una política de evaluación del funcionamiento de los recursos TICs, a fin de definir programas y planes operativos de fortalecimiento y modernización de la plataforma informática, incluyendo mejoramiento del nivel servicio para los clientes internos, planes de contingencia y mitigación de riesgos. La idea es lograr un marco de trabajo que permita diseñar un sistema de control informático interno avalado y respaldado por la gerencia, con directrices de acción que sean seguidas cabalmente por la totalidad de usuarios de los sistemas informáticos de la empresa, tanto directos como indirectos. Para ello, se diseñó un programa de trabajo de auditoría y un cuestionario de control interno. El mismo podrá ser monitoreado, evaluado y analizado y actualizado por la gerencia, de manera de concretar a corto, mediano y largo plazo un programa de mejora continua basado en estándares que incorporen las mejores prácticas de gestión TICs reconocidas.

Referencias

- [1] Aguirre, Y. (2006). Propuesta de implantación del área de auditoría en informática en un órgano legislativo. Seminario de auditoría en informática, informe de titulación. Disponible en: <http://olea.org> (Consulta: Mayo 2009)
- [2] Auditoria de Sistemas de Barcelona Consultores, (2004). Auditoria de Sistemas. Home page. Disponible en: <http://www.auditoriasistemas.com> (Consulta: Noviembre 2006).
- [3] Bethencourt, L. (2004). Materiales de clase. Taller de Tesis. Trabajo no publicado. UCLA-CENDES. Barquisimeto. Venezuela.
- [4] Centro Nacional de Tecnologías de Información y Comunicación (2009). Gobierno en Línea. Legislación. Disponible en: <http://www.gobiernoenlinea.ve> (Consulta: Julio 2009).
- [5] Datamation Management and Technology, (2004). COBIT, el verdadero marco de referencia para el control en Tecnología de Información. Disponible en: <http://datamation.cubika.com> (Consulta Noviembre 2006).
- [6] De La Fuente, R. (2000). El carácter multidisciplinario de la Auditoría y el control en TI. Revista Percepciones N 3, Octubre 2000, Montevideo, Uruguay. Disponible en: <http://www.isaca.org.uy/> (Consulta: Noviembre 2006).
- [7] Echenique García, J. (2001). Auditoría en Informática. Segunda Edición. Mexico: McGraw Hill.
- [8] Governance Institute (2000a). Audit Guidelines COBIT. 3era. Edición. USA. Disponible en: <http://www.isaca.org> (Consulta: Octubre 2008).
- [9] Governance Institute (2000b). COBIT, conjunto de herramientas de implementación. 3era. Edición. USA.
- [10] Governance Institute (2007). COBIT 4.1, Excerpt. Executive Summary. Framework. USA.
- [11] Guldentops, E. (2003). Management Awareness Diagnostic. ISACA. IT Governance Institute. Disponible en: <http://www.itgi.org> (Consulta: Febrero 2009).
- [12] IBM (2007). IBM Training. Caracas.
- [13] Information Systems Audit and Control Association (1998). COBIT, marco referencial, objetivos de control para la información y tecnología a fines. Segunda Edición. Traducida al español por Gustavo A. Solís (CISA).
- [14] Information Systems Audit and Control Association (2004). Norma de Auditoría de SI. Reporte. Documento No. S7. Disponible en: <http://www.isaca.org>. (Consulta: Abril 2008).

- [15] Laudon, K. y J. P. Laudon (2000). Administración de los Sistemas de Información. Organización y Tecnología. 3ra Edición. México: Prentice Hall.
- [16] Organización para la Cooperación y el Desarrollo Económicos (2002). Directrices de la OCDE para la Seguridad de Sistemas y Redes de Información. Ministerio de Administraciones Públicas. España. Disponible en: <http://www.csae.map.es> (Consulta: Febrero 2009).
- [17] Piattini, M. y E. Del Peso (1998). Auditoría en Informática. Un enfoque práctico. España: Editorial RAMA.
- [18] Pecantet, J. E. 2006. La auditoría de seguridad en las empresas: puntos a tener en cuenta. Disponible en: <http://www.shellsec.net> (Consulta: Febrero 2009).
- [19] Ruiz González, F. (1999). Planificación y Gestión de Sistemas de Información. 2da. Edición. COBIT-Universidad de Castilla. España.