1. El papel de la auditoría en el ambiente PED.

La incorporación tecnológica a las empresas requiere de políticas de control y sistemas de evaluación que protejan la información empresarial. Ésta variedad de tendencias tecnológicas e información, deben estar acompañadas de un buen sistema de control interno PED que minimice los riegos informáticos, ya que estos se han convertido en una de las causas más graves y peligrosas dentro de una organización;[1] además de otros factores tales como: la resistencia al cambio, la mala definición de los requerimientos, el diseño inadecuado de estándares de seguridad, políticas de control y normatividad deficientes. Hoy en día, en el mercado se encuentran soluciones de Software Empresarial que incluyen base de datos middleware, infraestructura de hardware y servicios empaquetados y otros tipos de productos que ofrecen versiones ajustadas a las necesidades de los empresarios, como herramientas que realizan tareas financieras de rastrear cotizaciones y facturas para clientes, aceptar pagos y devoluciones, personalizar formas contables, centralización de la información de clientes, correos electrónicos y crear campañas de mercadotecnia por Internet.

Las tendencias tecnológicas y su relación con los procesos operativos y contables deben ubicar la auditoría en un lugar estratégico en la organización, donde el auditor debe apoyarse en la utilización de técnicas de auditoría a través del computador para poder llevar a cabo la evaluación del control PED. En concordancia con ésta nueva responsabilidad la auditoría exige un cambio conceptual, metodológico y de actitud profesional, donde su función genere de manera permanente un valor agregado en las organizaciones. Los nuevos enfoques permitirán plantear un marco de referencia para identificar el papel que podría tener la auditoría en este nuevo rol y la función de la auditoría informática como eje central del control interno en las empresas que llevan a cabo operaciones de procesamiento electrónico de datos e información, concepción que no es fácil.

[1] Situaciones en el ambiente informático que se pueden presentar, como pérdida de la información, sabotaje, manipulación de datos, entre otros.

En ese mismo sentido, Wand y Weber (1990:pp.87-107), consideran que los sistemas de procesamiento de datos que los auditores examinan y evalúan se modifican con frecuencia, por tanto, el auditor debe decidir, cuál es el efecto de los cambios que el sistema tiene en los controles necesarios para garantizar que el sistema sea confiable, y sobre la auditoría, los procedimientos utilizados en determinar si los controles están en el lugar de trabajo[2].

Entonces, los sistemas de control y procedimientos de auditoría, deben dejar una pista de auditoría, el diseño de un rastreo de auditoría para sistemas contables basados en computación no es tarea sencilla - Weber (1985), concluye además que "las capacidades operacionales de un sistema que soporta el rastro de auditoría debería proveer presuntamente la creación, supresión y las capacidades de recuperación dadas la necesidad del sistema. Este es un asunto que cobra mayor importancia en la implementación de sistemas avanzados por que se pueden generar más errores que atenten contra la integridad del rastro de auditoría. Diseñar un sistema que tenga la capacidad de ser modificado es una tarea compleja".

Usando un modelo entidad-relación, se puede describir el diseño de un sistema de rastreo de auditoría que provee un completo paquete de capacidades para las entradas de un rastro de auditoría: creación, supresión, recuperación y modificación. En particular una estrategia de modificación denominada reparación generativa es desarrollada permitiendo un historial de modificaciones para que el rastro de auditoría se mantenga intacto".

El rastro de auditoría en los sistemas de computación es una tarea principal en el papel de la auditoría, y la literatura sobre el diseño de rastro de auditoría para sistemas basados en computación podría dar la impresión de que el diseño es claramente delimitada y definida, Sin embargo, a pesar de las complejidades inherentes al concepto del rastro de auditoría su diseño e interacción funcional con la auditoría debe considerar el creciente número de sistemas avanzados como sistemas de transferencia electrónica de fondos, sistemas de administración de base de datos y sistemas distribuidos.

---

[2] Planteamiento que permitió establecer un modelo de control y procedimientos de auditoría en la evolución de sistemas de procesamiento de datos. El modelo en sí permite a los auditores en la estructura del proceso de búsqueda identificar los lugares donde los sistemas de control y procedimientos de auditoría deben ser modificados cuando ocurren cambios en el sistema.

Por lo anterior, se considera importante al estudiar el papel de la auditoría y mencionar aquellos aspectos teóricos que dan cuenta de la relación entre la auditoría y el control interno.

1.1. Conceptos generales entre auditoría y control interno.

La auditoría podría describirse como aquella actividad que a través de pasos, permite evaluar el control interno y obtener evidencia válida y suficiente para establecer el grado de confiabilidad de los procesos y la correlación entre la información y los criterios establecidos por la organización, el estado y el entorno.

Para Arenas y Loebbecke (1989), la auditoría es: "el proceso de acumular y evaluar evidencias, realizado por una persona independiente y competente acerca de la información cuantificable de una entidad económica específica, con el propósito de determinar e informar sobre el grado de correspondencia existente entre la información cuantificable y los criterios establecidos". El ejercicio de la profesión está soportado bajo unos esquemas normativos que generan confianza a los usuarios que ejercen control a la información contable y aún más si ésta se crea a través de procesos automatizados. La verificación, el aseguramiento, los sistemas de controles operativos y contables, que se dan en un ambiente PED constituyen un tema determinante en el proceso de transparencia de la información contable. La auditoría ha trascendido notoriamente y aquellas definiciones del término "Auditoría" que implícitamente traían consigo vocablos como de inspección, comprobación, intervención han permitido sintetizar en objetivos, principios de causalidad no muy contemporáneos que constituyen el fundamento del actuar del Contador Público; no obstante, los procesos de globalización de la información, el enfoque regulatorio nacional e internacional y los problemas de control que subyacen en la verificación de la información a través de medios informáticos como base de la confianza trae consigo un estudio crítico y evaluativo del modelo actual de ejercer la auditoría local y de la aplicación de las normas internacionales de auditoría.

Según Dorta (2005:p.13), desde la perspectiva organizativa, el concepto de control no es único y está supeditado a las diversas corrientes de pensamientos existentes[3], cita a Monllau (1997) la cual concluye, "en la literatura organizativa se produce una evolución del concepto de control: en la teoría clásica el control era considerado como sinónimo de autoridad; la escuela de Harvard ve el control como un conjunto de mecanismos que permiten conseguir la congruencia de los objetivos. La teoría de la agencia se limita a aplicar los principios y técnicas microeconómicas al concepto de control. La teoría de los sistemas abiertos considera el control como un sistema que tiene por finalidad establecer un feed-back entre el entorno en el que se mueve la empresa, y la propia empresa. La teoría contingente, partiendo de la teoría de los sistemas abiertos, considera que el diseño del control de la empresa depende de factores que caracterizan tanto el entorno de la empresa, como de los que caracterizan a la propia empresa".

Con la aparición de éstos marcos conceptuales no solo se ha logrado una mejor delimitación teórica del control interno, sino también una respuesta a las necesidades de gestión de las organizaciones actúales, ya que éstas pueden regirse exclusivamente por los principios que tradicionalmente han venido utilizándose en la doctrina contable y la auditoría. Es así, como en los trabajos de Jensen (1995), Marcella (1995) y Simons (1995), se establece la necesidad de un proceso de cambio que permita ajustar los sistemas de control interno al nuevo entorno que se da en las organizaciones empresariales de acuerdo a la globalidad de los mercados y las tecnologías de la información y comunicación. Se debe entonces tener en cuenta las fuertes implicaciones prácticas que estos cambios ejercen sobre los sistemas de control, en especial los controles que se dan en un ambiente PED, pues llevan consigo diversos aspectos que no pueden ser apoyados en la concepción tradicional de control y de auditoría.

Para el Committee of Sponsoring Organizations - COSO[4] (1997, p.16), el control interno es: "un proceso efectuado por el consejo de administración, la dirección y el resto del

[3] Dorta, Director de Control Económico de la Universidad de las Palmas de Gran Canaria, presenta a consideración las teorías organizativas y los sistemas de control interno un análisis de la perspectiva organizativa en cuanto a la visión Auditora-Contable y la del Control Organizacional.

[4] El comité fue creado sobre la base de una recomendación de la National Commission on Fraudulent Financial Reporting – generalmente conocida como Treadway commission. Patrocinada por cinco organizaciones: el American Institute of

personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías: eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, cumplimiento de las leyes y regulaciones aplicables", el reporte enfatiza que el sistema de control interno es una herramienta de la administración, pero no un sustituto para esta y que los controles deberán ser construidos dentro de las actividades de operación y no fuera de ellas. En este sentido el informe COSO propone cinco componentes[5], de los cuales se hará mención del componente "Información y Comunicación", al considerar que engloba el conjunto de procedimientos que, cuando se ejecutan, proporcionan información para la toma de decisiones y/o control de la organización. Igual, el término encierra el concepto de sistemas de información y se podría utilizar para denominar el procesamiento de datos generados internamente en la organización a las transacciones y operaciones internas resaltando el valor de la información como un activo estratégico en la empresas, el cual requiere una orientación en ese mismo sentido en que se deben integrar la planificación, el diseño y la implementación de los sistema de información en concordancia con un buen esquema de control.

Blanco (2001), sostiene que la definición de control interno refleja ciertos conceptos fundamentales entre ellos el de proceso. Es decir, es un medio hacia un fin, no un fin en si mismo. El Control Interno es efectuado por personas, no es meramente políticas, manuales y formatos, sino personas a niveles de una organización. Del control interno puede esperarse que provea solamente una razonable seguridad, no absoluta seguridad a la gerencia y a la junta Directiva de una entidad. El control interno es el mecanismo para el logro de objetivos de una o más categorías separadas o interrelacionadas.

Certified Public Accountants (AICPA), La American Accounting Association (AAA), el Financial Executives Institute (FEI), el Institute of Internal Auditors (IIA) y el Institute of Management Accountants (IMA)., con el propósito general de proporcionar criterios prácticos para el establecimiento y evaluación del sistema de control interno.

[5] El informe COSO propone cinco componentes, cuya evaluación integral permite establecer el grado de eficacia con el que está funcionando el sistema de control interno: a) Entorno de Control, b) Evaluación de los Riesgos, c) Actividades de Control, d) Información y Comunicación, e) Supervisión. Se plantea que el sistema de control interno debe cubrir todas las posibles áreas y facetas de la organización, estos componentes han de ser suficientemente amplios como para abarcar las categorías de los objetivos planteados por la comisión.

De otra parte, los modelos canadiense desarrollado por el Criteria of Control Committee,(CoCo), bajo el auspicio del Canadian Institute of Chartered Accountants (CICA)[6] y el modelo Austrialian Control Criteria (ACC) elaborado por el institute of Internal auditors (IIA)[7] de Australia, destacan la influencia que puede tener el sistema de información en la toma de decisión y establecen que en las actividades de control deben diseñarse como parte integral de la organización, tomando en consideración sus objetivos, riesgos y otros elementos de control.

En el contexto colombiano, el Sistema de Control Interno y de Gestión, para el sector público, es una herramienta dispuesta por la Constitución Política de Colombia, en sus artículos 209 y 269 interpretadas por la Ley 87 de 1.993, para modernizar las instituciones y llevarlas al perfeccionamiento mediante la evaluación y cambio permanente y continuo. En sentido amplio el Control se define como el conjunto de normas, procedimientos, técnicas, políticas por medio de los cuales se evalúan y corrige el ejercicio profesional.

Ante la rapidez de los cambios, los directores para evitar fallos de control significativos deben revaluar y reestructurar sus sistemas de control interno. Actuar de manera proactiva, tomando medidas eficaces para su propia tranquilidad, así como para garantizar a los directivos, accionistas, empleados y público en general que los controles internos de la empresa están adecuadamente diseñados para hacer frente a los retos del futuro y en consecuencia asegurar la integridad de los datos.

1.2. La Auditoría en el ambiente PED.

Los Estándares internacionales de Auditoría (ISAs), son para ser aplicados en la auditoría de estados financieros y pueden ser también aplicados, con las adaptaciones necesarias, a la auditoría de otra información y a servicios relacionados. La IFAC (2003), incluye en la

[6] Entre los pronunciamientos que configuran su marco conceptual destacan fundamentalmente dos, Guidance on Control (1995) y Guidance on Assessing Control – The CoCo Principles (1997), los cuales aportan un conjunto de criterios con connotaciones diferentes a los establecidos en el informe COSO.

[7] De acuerdo con Dorta (2005), este modelo no solo entra en contradicción con los conceptos generalmente aceptados por los auditores internos sino que, por el contrario, se propone integrarlos con los marcos conceptuales que se están imponiendo en el ámbito internacional.

página web los estándares internacionales y con respecto a este marco estructura se deben considerar los ISAs, 120- estructura conceptual de los ISAs, 220 – control de calidad del trabajo de auditoría, 400 – valoración de riesgo y control interno, 401 – auditoría en un ambiente de sistemas de información computarizados.

El ISA 401- emitido por la IFAC (2003), establece la auditoría en un ambiente de sistemas de información computarizados, considerando los siguientes aspectos:

a. El auditor debe considerar cómo un ambiente CIS[8] afecta la auditoría.
b. El auditor debe tener un conocimiento suficiente del CIS para planear, dirigir, supervisar y revisar el trabajo desempeñado.
c. El auditor debe considerar y de acuerdo con el ISA 400, la valoración del riesgo y control interno, éste debe obtener un entendimiento suficiente de los sistemas de contabilidad y control interno para planear la auditoría y desarrollar un enfoque de auditoría que sea efectivo.

La ley Sarbanex – Oxley[9] (2002) en su sección 2. (2), emite del término "Auditoría" el siguiente significado "un examen de los estados financieros de cualquier emisor, realizado por una firma independiente de contaduría pública, de acuerdo con las reglas de la Junta o de la comisión con el propósito de expresar una opinión sobre tales estados.

La AICPA (2001), emitió el SAS 94 "The Efecct of information Technology on the Auditor´s consideration of Internal Control in a Financial Statement Audit" (Efecto de la tecnología de la información sobre la consideración que el auditor hace del control interno en una auditoría de estados financieros). Éste provee orientaciones a los auditores sobre el efecto de las tecnologías de la información en el control interno, y en el entendimiento que el auditor tiene del control interno y en la valoración del riesgo de control. De los aspectos más importantes se señala:

[8] CIS: Computer Information Systems, término técnico que traduce: Sistemas de Información computarizado.

[9] La Sarbanes-oxley Act de 2002 es una de las principales respuestas, desde la perspectiva del Congreso de los Estados Unidos, a la crisis derivada de Enron, WorldCom, Andersen y empresas similares. La ley tiene un ámbito de aplicación muy preciso que es el mercado de valores, no obstante se presente por considerar algunos aspectos importantes relacionados con la auditoría.

a. Los procedimientos usados para ingresar los totales de las transacciones en el Libro mayor.
b. Los procedimientos para iniciar, registrar y procesar las entradas de los datos en el sistema de información contable.
c. Provee orientación para ayudar a los auditores a determinar si requieren habilidades especializadas para considerar el efecto que el procesamiento computarizado tiene sobre la auditoría.
d. Describe como la tecnología de la información puede afectar el control interno, la materia evidencial, y el entendimiento del auditor sobre el control interno y la valoración del riesgo de control.
e. Actualiza la terminología y las referencias a los sistemas y controles de Tecnologías de la Información.

Para Ratcliffe y Munter (2002), El sistemas procesamiento de datos modernos trae nuevos desafíos, colmado de riesgos al proceso tradicional de auditoría. Mientras que era una vez posible conducir una revisión de cuentas de declaración financiera, evaluando y supervisando los controles sobre la transacción a base de papel (documentos) y sistemas contables, los negocios cada vez más han dado vuelta a la transacción electrónica y sistemas contables. De ahí la importancia de SAS 94, el cual permite un direccionamiento en el sentido de establecer pruebas suficientes, competentes en un ambiente de tratamiento electrónico.

La auditoría debe lograr la interrelación entre lo más significativo y el riesgo en el proceso de auditoría interna[10]. En el ambiente informático se debe determinar la asociación entre la planeación de la auditoría, la evaluación del sistema de control interno y la estructura de control interno PED, con el fin de poder identificar los componentes del riesgo de auditoría:

[10] La NIA 25 - esta norma se refiere a la interrelación entre la significatividad y el riesgo en el proceso de auditoría. Identifica tres componentes distintos del riesgo de auditoría: riesgo inherente, riesgo de control y riesgo de detección. Tomando conciencia de la relación entre significatividad y riesgo, el auditor puede modificar sus procedimientos para mantener el riesgo de auditoría en un nivel aceptable

riesgo inherente, de control y de auditoría para planear la auditoría del ambiente PED, determinar el enfoque, alcance, objetivo y ejecución de las pruebas que han de realizarse.

La auditoría interna como eje orientado de la evaluación y el control en las organizaciones desempeñan un papel de gran importancia en el proceso de auditoría del sistema de información. El auditor tiene grandes responsabilidades, la de emitir una opinión objetiva que encamine a la optimización de los recursos y el cumplimiento de los objetivos organizacionales. No sólo, eso, lograr además la protección de usuarios y empresas frente a las amenazas creadas por usuarios malintencionados; hace poco la preocupación era por los virus, los gusanos y los troyanos; ahora se suman nuevas y sofisticadas amenazas que causan un perjuicio al usuario y a la empresa que exige nuevas soluciones. Según Ernst & Young, el fraude bancario y el robo de información confidencial (phishing) es una de las técnicas que más preocupa a las organizaciones y en especial a los responsables de TI – Tecnologías de la Información, en Crespo (2006:p.24).

En esa misma orientación, Whittington y Pany (2000), consideran para las aplicaciones en desarrollo, que el auditor interno participe en el diseño, para asegurar que el sistema proporcione un rastro de auditoría apropiado e incluya los controles adecuados. Una vez que el nuevo sistema entre en funcionamiento, la auditoría debe realizar pruebas para determinar si los controles recomendados funcionan de acuerdo con lo planificado, si el personal de programación tiene funciones separadas del personal que opera, si se mantiene la documentación adecuada y si las operaciones de control funcionan en forma efectiva.

Aunque el departamento o área de sistemas de información es responsable por el mantenimiento diario de los controles y del procesamiento de los datos en el computador, la auditoría interna debe evaluar la eficiencia global y la efectividad de las operaciones de los sistemas informáticos y los controles relacionados en toda la empresa. Por tanto debe "evaluarse en la auditoría si los modelos de seguridad están en consonancia con los criterios de la empresa, así como con las nuevas arquitecturas y plataformas tecnológicas, y las posibilidades y riesgos de los medios de comunicación" - Del Peso y Ramos (2002). Los

auditores han de ser competentes e independientes, esto último sería más probable si la auditoría fuese externa.

Las áreas que puede cubrir la auditoría interna y de carácter general dentro del contexto de seguridad en el ambiente PED, podrían ser:

- **Controles de Dirección Tecnológica**: fundamentados en el diseño de políticas, planes, objetivos de control, funciones, presupuestos para el desarrollo tecnológico.

- **Controles de orden Legal**: fundamentados en regulaciones o aspectos de orden jurídicos aplicables a cada entidad, podría considerarse el cumplimiento de contratos, etc.
- **Controles de Seguridad Física:** fundamentados en protecciones a inundaciones, incendios, explosiones, corte de energía eléctrica, vandalismo, huelgas, conatos de incendio y terremoto.
- **Controles de acceso**: fundamentado en controles físicos y lógicos.
- **Controles de protección de datos**: determinado por los datos y la información, la designación de responsables usuarios y propietarios, y los riesgos a que estén sometidos.
- **Controles de aplicaciones en producción**: fundamentado en la continuidad de las operaciones, controles de entrada de datos, procesamiento y salida.
- **Controles de aplicaciones en desarrollo**: fundamentados en lograr un entorno seguro, asegurando la incorporación de controles en los productos desarrollados.

Efectuada la evaluación a cada uno de los controles, los factores que deben considerarse para recomendar un determinado sistema de procesamiento de datos, está dado en el volumen de operaciones y de datos a procesar, la complejidad de las operaciones, la necesidad de una respuesta rápida, la volatilidad de la información y la relación costo beneficio.