IMPACTO DE LA LEY SARBANES-OXLEY A A LA SEGURIDAD DE LOS SISTEMAS DE TI

SANTIAGO CAMPUZANO VALLEJO
JUAN FERNANDO JARAMILLO

UNIVERSIDAD EAFIT
ESCUELA DE INGENIERÍA
2008

IMPACTO DE LA LEY SARBANES-OXLEY A LA SEGURIDAD DE LOS SISTEMAS DE TI

SANTIAGO CAMPUZANO VALLEJO
JUAN FERNANDO JARAMILLO

Trabajo de grado presentado como requisito parcial para optar al título de Ingenieros de Sistemas

Asesor: Diego Andrés Zuluaga

MEDELLÍN
UNIVERSIDAD EAFIT
INGENIERÍA DE SISTEMAS
2008

Nota de aceptación:

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Medellín, octubre de 2008

AGRADECIMIENTOS

A nuestras familias por darnos su apoyo durante las jornadas de investigación y dedicación a éste proyecto.

Al Ingeniero Diego Zuluaga, por sacar espacios de su apretada agenda y compromisos familiares, para brindarnos su valiosa asesoría y guía en todo el proyecto.

A Cementos Argos, en especial al Ingeniero Alejandro Galvez, Gerente de Tecnología, quien nos brindo su experiencia, para tener un punto de referencia de la implementación de la ley SOX en Colombia.

CONTENIDO

TABLAS

ILUSTRACIONES

GLOSARIO

COSO: Committee of Sponsoring Organizations of the Treadway Comisión, iniciativa privada, creada en el año de 1985 con el fin de combatir el fraude.

SOX: Diminutivo para Sarbanes-Oxley, ley promulgada por el congreso de los Estados Unidos, nombrada en honor a los senadores Paul Sarbanes y Michael G. Oxley, y cuyo objetivo es combatir el fraude financiero.

SEC: Securities and Exchange Comission, es una agencia independiente del gobierno de los Estados Unidos, cuya misión es regular los mercados bursátiles.

PCAOB: The Public Company Accounting Oversight Board, ente creado con la Ley SOX, es quien establece los estándares y vigila las firmas que auditan a las compañías que cotizan en bolsa.

IT / TI: Information Technology / Tecnología de la Información, término con el que se hace referencia en general a todas las tecnologías informáticas con las que cuentas las compañías.

CSO: Chief Security Officer, un ejecutivo responsable por la seguridad de la información y de los recursos tecnológicos de la compañía.

CIO: Chief Information Officer, es el ejecutivo responsable de toda el área de tecnología y/o informática.

CFO: Chief Financial Officer, gerente o director financiero de la compañía.

CEO: Chief Executive Office, gerente general o presidente de la compañía.

DATA STEWARD: Es la persona encargada de mantener los estándares que rigen para el manejo y almacenamiento de la información.

ERP: Enterprise Resource Planning, conjunto de sistemas de información que integran todas o casi todas las partes de una compañía (compras, ventas, etc.).

SOA: Service Oriented Architecture, una arquitectura que propone el ofrecimiento o la publicación de servicios de forma estandarizada.

WORM: Write One, Read Many, es un medio de almacenamiento usado para guardar información que no puede ser modificada, pero si leída muchas veces.

BACKUP: Realizar copia de seguridad de un sistema o información.

NYSE: New York Stock Exchange, el mercado de valores más grande de USA.

IPO: Initial Public Offering, Se trata de la primera venta de acciones de una compañía al público.

SDLC: System Development Life Cycle, Metodología de Ciclo de vida en el desarrollo y puesta en marcha de aplicaciones y plataformas de tecnología.

RESUMEN

Los graves escándalos financieros descubiertos a principios de este siglo, protagonizados algunas compañías norteamericanas, especialmente Enron, WorldCom y Tyco International, provocaron que el gobierno y el congreso de los Estados Unidos promulgaran una ley, conocida como la Ley Sarbanes-Oxley. Ésta está dividida en 11 capítulos que describen mandatos específicos sobre temas tales como responsabilidad corporativa, fraude financiero, mejoras en los reportes financieros, el comité de supervisión de contadores, independencia de los auditores, entre otros.

El impacto de ésta ley sobre todos los aspectos de una compañía ha sido enorme, desde el área de contabilidad, pasando por auditoría, finanzas, área de TI, etc. En mayor o menor medida, la ley impacta todas las áreas de la organización, pero es de especial atención para este trabajo, detallar el impacto que la ley tiene sobre el área de TI, su seguridad y cada uno de los aspectos detallados de los sistemas de información corporativos y de la plataforma tecnológica que los soporta.

Las compañías colombianas no son la excepción a éste impacto, ya que algunas de ésas han decidido entrar a cotizar a las bolsas de USA, o piensan hacerlo en un corto o mediano plazo.

INTRODUCCIÓN

Con éste trabajo se pretende resaltar la importancia y el impacto directo que tiene la promulgación de la Ley Sarbanes-Oxley sobre las TI. Muchas compañías no saben realmente que es lo que deben hacer al interior de sus áreas de TI para cumlir a cabalidad con todas las regulaciones de la Ley.

Gran parte del trabajo se enfoca en mostrar el impacto de la Ley sobre los diversos aspectos de un área de TI, en especial la seguridad, los sistemas de almcacenamiento y los sistemas ERP/Financieros.

El siguiente paso es elaborar un modelo basado en COBIT, que básicamente pretende mostrar el nivel de madurez de los distintos controles implementados en TI, para con esto saber que tan bien está la empresa respecto a la Ley SOX.

Finalmente se pretende aplicar este modelo a una empresa Colombiana, la cual servirá de punto de referencia para evaluar el estado de las grandes empresas colombianas respecto de la Ley Sarbanes-Oxley.

OBJETIVOS

Objetivo General

Identificar el impacto de la Ley Sarbanes-Oxley en la seguridad de los Sistemas y la Tecnología de Información para las empresas Colombianas.

Objetivos Específicos

- Analizar el impacto que genera dentro de los Sistemas y Tecnologías de Información (SI/TI) la aparición del acto Sarbanes-Oxley (SOX), que obliga a la transparencia y veracidad de los reportes financieros de las corporaciones.
- Presentar la importancia que tiene el que un sistema de información financiero pueda entregar información de forma oportuna, confiable y consistente. Entender como los sistemas de TI están envueltos en el soporte de las actividades financieras cotidianas de las empresas.
- Delimitar una serie de parámetros que permitan definir como la TI pueden ser confiable a la luz de esta ley, como las políticas de buen gobierno, las técnicas de auditoría y transparencia de los reportes financieros hacen un sistema de TI compatible con ésta.
- Comprender los impactos organizacionales y el rol que debe tomar el CIO (Chief Information Officer) y el CSO (Chief Security Officer) dentro del PCAOB (Public Company Accounting Oversight Board), como unas figuras creadas dentro del marco del acto SOX.

- Identificar los impactos en el manejo de los datos, la seguridad del sistema y las prácticas de archivado de reportes de los negocios, asegurando el cumplimiento de las políticas de SOX.
- Identificar el impacto que puede tener la ley SOX para las empresas colombianas.
- Analizar y presentar mejores prácticas, y referencias a marcos de trabajo y metodologías existentes aplicables a la seguridad de los SI/TI en las empresas colombianas.

1. CONTEXTO DE LA LEY SARBANES-OXLEY

1.1 EL ESCÁNDALO ENRON

Para poder entender las razones que desembocaron en la creación de la ley SOX, se debe entender en que consistió el fraude de ENRON Corporation, una empresa que en menos de 15 años pasó a convertirse en el séptimo grupo empresarial de los Estados Unidos a mediados del 2001, según la revista Forbes.

1.1.1 Historia de ENRON. ENRON surge en Julio de 1985, tras la fusión de Houston Natural Gas e Internorth, una compañía de gas natural de Omaha, Nebraska. En 1989, ENRON comienza a comercializar gas natural como una mercancía gracias a la desregulación de este producto, favorecida por la administración de George Bush. Para noviembre de 1999, ENRON lanza su sistema de transacciones globales en Internet, "ENRON Online", un sistema que permitía ver a sus clientes los precios del mercado en tiempo real, y hacer sus transacciones en línea. Los dos años en los que estuvo en funcionamiento esta plataforma, llegó a realizar transacciones diarias por un valor de 2.500 millones de dólares. En el lapso de 15 años, ENRON pasó a contar con más de 21.000 empleados en 40 países, y había superado los 100 billones de dólares en facturación en sus libros de finales de 2000. Su complicada estructura corporativa hizo imposible auditarla mediante los métodos convencionales, facilitándole la alteración y modificación de los resultados financieros. También tenían una gran influencia política, la administración Bush, padre e hijo, consultaban frecuentemente a Kenneth Lay, presidente ejecutivo, como asesor en asuntos

energéticos. Esto le permitió capturar millones de inversionistas captando fondos de pensiones en todo Estados Unidos.

1.1.2 El Colapso. Los factores de la debacle de ENRON se pueden encajar en una seguidilla de eventos que lo llevaron el 2 de diciembre de 2001, a presentarse en un tribunal de Nueva York, pidiendo acogerse a las leyes que regulan la quiebra de las empresas en los Estados Unidos. A continuación se muestra la secuencia de eventos:[1]

- Diciembre 2000. Kenneth Lay renuncia como presidente ejecutivo pero mantiene la presidencia del directorio a favor de Jeffrey Skilling.
- 28 Diciembre 2000. Las acciones alcanzan la cotización record de $84.87 – convirtiendo a ENRON en la séptima empresa más valiosa de Estados Unidos.
- 14 Agosto 2001. Jeffrey Skilling renuncia después de seis meses; Lay retoma las responsabilidades ejecutivas máximas de la compañía.
- 15 Agosto 2001. El empleado de ENRON, Sherron Watkins envía una carta a Kenneth Lay previniéndole de irregularidades contables que podrían poner en peligro a la compañía.
- 20 Agosto 2001. Lay convierte en acciones opciones por valor de $519,000.
- 21 Agosto 2001. Lay convierte en acciones más opciones por valor de $1.48m.
- Octubre 2001. La firma Arthur Andersen comienza a destruir documentos relacionados a las auditorías realizadas a ENRON. La destrucción continúa hasta Noviembre cuando la firma recibe una cédula para comparecer ante la Comisión de Seguridades y de Comercio.
- 15 Octubre 2001. Lay llama al Secretario de Comercio Don Evans, pero los funcionarios de la secretaría dicen que el llamado era referente a un problema que ENRON tenía con un proyecto energético en La India.

[1] Tomado de http://www.aunmas.com/ataque/globalidad_08.htm

- 16 Octubre 2001. ENRON reporta pérdidas por $638 millones de dólares entre Julio y Septiembre y anuncia una reducción de 1200 millones de dólares en su stock accionario. La reducción correspondía a asociaciones arregladas por el Vicepresidente Financiero Andrew Fastow.
- 22 Octubre 2001. La Comisión de Seguridades y Comercio abre una consulta sobre un posible conflicto de intereses en relación a las asociaciones realizadas por Fastow.
- 23 Octubre 2001. En una conferencia, Lay trata de dar confianza a los inversores y defiende el trabajo de Fastow.
- 24 Octubre 2001. ENRON echa a Fastow.
- 28 Octubre 2001. Kenneth Lay llama al Secretario del Tesoro Paul O'Neill para informarle de los problemas financieros que enfrenta la compañía. Una Segunda conversación de similar tenor se realiza el 8 de Noviembre. O'Neill dice que declinó ayudar a la firma, en la medida que no pudo detectar posibles repercusiones desfavorables en los mercados financieros debido a los problemas de ENRON.
- 29 Octubre 2001. Lay llama nuevamente al Secretario de Comercio Don Evans, para pedirle haga algo conducente a influenciar al Servicio para Inversores Moody para que no lo degrade demasiado en el ranking de créditos. Evans no interviene, diciendo que no sería apropiado influenciar la decisión de una agencia privada de inteligencia crediticia.
- 31 Octubre 2001 La requisitoria de la Comisión de Seguridad y Comercio se transforma en una investigación formal.
- 8 Noviembre 2001. ENRON revisa sus balances de los pasados cinco años. En lugar de los masivos beneficios previamente proclamados, la firma dice perder actualmente 586 millones de dólares.
- 9 Noviembre 2001. La firma competidora Dynergy, informa que estaría dispuesta a hacerse cargo del mucho mayor ENRON por 8000 millones de dólares en acciones.

- 19 Noviembre 2001. ENRON dice que las pérdidas de su tercer cuatrimestre son superiores a lo que se había informado y previene que necesitará financiar una deuda de 690 millones hacia fines de ese mes.
- 20 Noviembre 2001. El precio de las acciones de ENRON llega a su punto más bajo en 10 años mientras los inversores se preocupan acerca de si la empresa podrá superar sus problemas financieros.
- 21 Noviembre 2001. ENRON asegura una extensión de su deuda de 690 millones.
- 26 Noviembre 2001. Las acciones de ENRON están por el piso a $4.01.
- 28 Noviembre 2001. Dynergy retira su oferta cuando el rating crediticio de ENRON es degradado al nivel de bonos de descarte. Las acciones de ENRON descienden bajo $1 – el stock de acciones experimenta el más pesado descenso en un día en la historia para empresas listadas en el NYSE y en Nasdaq.
- 2 Diciembre 2001. ENRON pide la protección de bancarrota prevista en el Capítulo 11 y reclama legalmente a Dynergy por incumplimiento de contrato.
- ENRON prohíbe a sus empleados vender las acciones asignadas y ligas a sus planes de retiro.
- 9 Enero 2002. El Departamento de Justicia de Estados Unidos comienza la investigación criminal de ENRON.
- 10 Enero 2002. La Casa Blanca confirma que Kenneth Lay hacía lobby para apoyar a su empresa poco antes de que colapsara. Arthur Andersen reconoce que sus empleados destruyeron algunos documentos de ENRON.
- El Procurador General John Ashcroft, quién recibió de la empresa fondos para su campaña como Senador, se excluye de la investigación, al igual que el equipo de unos 100 investigadores federales de Houston, donde ENRON tiene su cuartel general.
- 12 Enero 2002. El Departamento de Justicia nombra a Joshua Hochberg, titular de la división de fraudes, como fiscal actuante para dirigir la investigación criminal dentro de ENRON.

- 15 Enero 2002. Arthur Andersen echa al ejecutivo David Duncan que estuvo a cargo de auditar a ENRON y coloca en su lugar a otros tres empleados.
- 16 Enero. Las acciones de ENRON son dadas de baja en la Bolsa de Nueva York.
- 23 Enero. Renuncia Kenneth Lay.
- 24 Enero. Comienza la audiencia del caso ENRON en el Congreso de Estados Unidos
- 25 Enero. Clifford Baxter, el anterior Vice Presidente del directorio de ENRON y Jefe Estratégico se suicida. Dejó abruptamente la firma en Mayo del 2001, después de haber chocado con Jeff Skilling por las prácticas contables de la firma.

ENRON, en menos de un año había pasado de ser la mayor compañía energética del mundo, a una compañía en ruina, todos sus reportes financieros habían sido manipulados con la complicidad de la firma Arthur Andersen; una de las cinco grandes compañías de auditoría a nivel mundial, esta firma auditora admitió haber destruido numerosos documentos de ENRON.

La quiebra dejo en la ruina a sus miles de empleados, cuyas acciones pasaron de $90 dólares a $0,42 dólares, además del fondo de pensiones estimado en más de $700 millones de dólares, quienes no podían vender sus acciones porque la legislación sobre pensiones se lo impedía, mientras que los principales ejecutivos de ENRON si liquidaron sus inversiones en la empresa, incluso antes de que reventara la crisis, adquiriendo más del $1.000 millones de dólares.

El colapso fue causado tras las prácticas irregulares de ENRON en cuestión a sus reportes financieros, debido a tener muchas sociedades incorporadas a la firma, justificó la separación de sus reportes financieros en base a la distinta naturaleza de las sociedades que lo conformaban, ocultando pasivos por más de $30.000 millones de dólares.

Según un comunicado oficial de la empresa, del 8 de noviembre de 2002, se redefinieron sus balances consolidados de la siguiente forma:

"La decisión de ENRON de que Chewco, empresa filial, debe ser consolidada desde noviembre de 1997, se basa en la información de que esta empresa filial no cumple con los criterios contables para ser considerada una SPE. Como resultado de este incumplimiento, otra sociedad denominada JEDI, en la cual Chewco tenía una participación limitada, también tenía que ser consolidada en los estados financieros de ENRON. En razón de estas consolidaciones, los reportes de pasivos de ENRON se vieron afectados, al alza, con los pasivos de ambas sociedades.

La decisión de ENRON de que la subsidiaria LJM1 debe ser consolidada en 1999 y 2000 se basa en la consideración de que esta subsidiaria no califica como no consolidable, en virtud de inadecuada capitalización, por lo que las inversiones que ENRON hizo a través de esta subsidiaria en Rhythms NetConnections, deben consolidarse en los balances de dichos años."[2]

El impacto del fraude ENRON quedo plasmado en una deuda estimada de 150 mil millones de dólares; a nivel individual, los 20.000 empleados de ENRON que perdieron sus empleos y sus ahorros de retiro, vieron como sus acciones pasaron a valer $0 dólares en un año, tal como lo muestra la gráfica del NYSE.

[2] http://www.fairfax.ca/Assets/Downloads/021108ceo.pdf

Ilustración 1. Valor de las Acciones de ENRON entre 1998 y 2004

El impacto de la caída de ENRON está aún por esclarecerse; se han descubierto contribuciones hechas por la empresa a numerosos políticos del mundo, en países en los cuales ENRON tenía intereses, también la firma Arthur Andersen ha sufrido numerosas investigaciones sobre obstrucción de la justicia en relación con el caso ENRON, lo que afecto a numerosas empresas a las que la firma presta sus servicios, como la empresa Worldcomm; de la que nos ocuparemos más adelante, quienes también alteraban sus resultados financieros.

1.2 ARTHUR ANDERSEN LLP

La firma Arthur Andersen LLP fue creada hacia finales de 1913 por Arthur Edward Andersen, en compañía de su amigo Clarence Delany, firma que inicialmente se llamó "Andersen, Delany & Company"; tiempo después su amigo dejo la compañía, que después fuera conocida como "Andersen & Company".

La firma tuvo una gran expansión en los años 20, dada el crecimiento de las compañías energéticas en EE.UU., "Andersen & Company" tomó estas como sus principales

clientes de servicios contables. Incluso en la crisis de 1930, la firma consiguió que los bancos les facilitaran el crédito a las empresas clientes, para que estas siguieran operando, lo que aumentó la reputación de la auditora a lo largo y ancho del país.

1.2.1 Implicación en el escándalo contable. El 15 de junio de 2002, Andersen fue declarada culpable de obstrucción de la justicia, referente a la destrucción de documentos de su auditoría a ENRON. Nancy Temple (Asesora Legal de Andersen), y David Duncan (Socio Conductor para la Contabilidad de ENRON), fueron citados a juicio por ser los autores intelectuales del escándalo. Debido a que estas firman fundamentan su funcionamiento en la credibilidad y confiabilidad de sus clientes, este escándalo termino por acabar las operaciones de la empresa el 31 de agosto de 2002, cuando la firma acepto entregar su licencia y su derecho a la práctica contable ante la Comisión de Seguridad e Intercambio de los Estados Unidos, lo que acabaría definitivamente con sus operaciones, y su posterior desmembramiento.

Irónicamente, el escándalo fue desencadenado por una de las empresas que Arthur Andersen LLP ayudo a sobrevivir la crisis de 1930. Quien fuera considerada una de las 5 grandes firmas de auditoría del mundo, terminaría siendo absorbida por sus principales competidoras, KPMG Consulting; ahora BearingPoint, en los EE.UU. Otras de sus filiales siguieron el mismo camino como Deloitte en España, quien absorbió todo el funcionamiento de la firma en ese país.

Tres años después de dictada la sentencia, el Tribunal Supremo de los EE.UU., ha revocado la sentencia condenatoria, según el tribunal, debido a que el jurado no dispuso de pruebas suficientes para emitir el veredicto, este fallo sale demasiado tarde, ya que la firma se disolvió para satisfacer a la opinión pública.[3]

El caso ENRON fue el desencadenante de la creación de la Ley Sarbanes-Oxley, cuyo objetivo es establecer medidas de control más estrictos y eficientes, para evitar que

[3] http://en.wikipedia.org/wiki/Arthur_Andersen_LLP_v._United_States

empresas públicas realicen fraudes como lo sucedido en ENRON.

2. INTRODUCCIÓN AL IMPACTO DE LA LEY SOX EN LAS TI

Es indiscutible que desde el mismo momento en que la Ley Sarbanes-Oxley fue promulgada por el Congreso de los Estados Unidos de América, y ratificada por el Presidente George W. Bush, se vaticinó casi de forma inmediata el gran impacto que ésta Ley iba a tener en los sistemas de información de las compañías que cotizan en las bolsas de valores de Estados Unidos.

El objetivo básico del acto SOX es proteger a los inversionistas mejorando la precisión y confiabilidad de los reportes financieros. SOX impone penas y castigos a los oficiales de compañías que fallen al garantizar la precisión de dichos reportes y va más allá penalizando a cualquiera que obstruya investigaciones de fraudes destruyendo o alterando documentos.

Dado que mucha de la información financiera de las empresas reside en sus bases de datos, sistemas de información y servidores, la responsabilidad de dichos controles internos recae directamente en los profesionales de TI.

2.1. SECCIONES DE SOX QUE TIENEN MAS IMPACTO EN TI

Primero, se dará una breve traducción casi literal de las secciones de la Ley Sarbanes-Oxley que tienen principal impacto en los sistemas de TI, para tener un primer acercamiento y un concepto preliminar de dichas secciones.[4]

[4] Tomadas del documento SOX Act, emitido por el Congreso de los Estados Unidos.

2.1.1. Sección 103. De ésta sección podemos tomar el siguiente parágrafo que nos ayuda a entender el porqué de su impacto en las TI: *"El comité debe exigir a las firmas de contadores públicos, Preparar y mantener por un periodo no inferior a 7 años, informes de auditoría y cualquier otra información o documento relacionado con el informe de auditoría, con el detalle suficiente para dar soporte a las conclusiones alcanzadas en dicho reporte".*

2.1.2. Sección 302. Considerada como la sección de más impacto en toda la Ley SOX, especialmente impactando los sistemas TI: "*El CEO (Chief Executive Officer y el CFO (Chief Financial Officer) deben certificar la veracidad de los reportes financieros (balances) periódicos y anuales, garantizando que no contienen información falsa y que dicho reporte refleja de la manera más fiel posible el estado financiero de la compañía; además, deben ser responsables por establecer controles internos sobre los flujos de información financiera al interior de la compañía, informar de manera oportuna las debilidades de dichos controles en los reportes."*

2.1.3. Sección 404. Está directamente relacionada con la sección 302, aunque hace más énfasis en los controles internos: "*Se responsabiliza a los CEO y a los CFO por la creación y el mantenimiento de una estructura de controles internos y de procedimientos para la elaboración de los reportes financieros. Además realizar una evaluación de la efectividad de los controles internos y los procedimientos de reporte. La firma de contabilidad que prepara el reporte de auditoría, debe además atestiguar la evaluación hecha por el CEO o CFO."*

2.1.4. Sección 409. Está relacionada directamente con la rapidez con la que las empresas publican información relevante a los inversionistas y a las entidades reguladoras: *"Las empresas deberían revelar cambios importantes en su condición financiera, de una forma rápida y constante. Esto se debe hacer en inglés plano y sencillo, se debe incluir información cualitativa y de tendencias, así como gráficos representativos. De ésta forma se pretende proteger a los inversionistas y el interés público".*

2.1.5. Sección 802 y 1102. Relacionada directamente con la destrucción, alteración o falsificación de documentos o registros durante una investigación federal o una bancarrota. *"Cualquiera que destruya, altere, modifique, oculte o falsifique cualquier documento, registro o archivo, con la intención de impedir, desviar o influenciar una investigación federal, puede incurrir en penas de hasta 20 años".* "*Cualquier contador que lleve una auditoría de la compañía, debe conservar toda la documentación de la auditoría y cualquier documento relacionado que soporte dicha auditoría (correos, memorandos, hojas de cálculo, etc.) por un período de 5 años, después que la auditoría haya sido terminada.*

2.1.6. Sección 806. Relacionada con la protección a los empleados de la compañía que quieran actuar de informantes en situaciones financieras irregulares o posible fraude: "*Ninguna compañía cobijada bajo las leyes de la SEC, o cualquier ejecutivo, empleado, contratista, subcontratista o agente de dicha compañía, podrá despedir, suspender, amenazar, descender o infligir cualquier otro tipo de discriminación sobre un empleado que, actuando dentro del marco de la ley, haya provisto información o haya asistido una investigación de una conducta que el empleado considere irregular respecto a cometer fraude financiero…."*

2.2 IMPACTO DE SOX EN LAS TI

Ahora que conocemos un poco acerca de estas secciones de la Ley SOX, y aunque a primera vista no hagan relación alguna con los sistemas de TI, daremos una breve introducción acerca de cómo cada una de ellas afecta de forma directa los distintos sistemas de software y hardware al interior de la compañía.

2.2.1 Secciones 103 y 802. Estas dos secciones están estrechamente relacionadas, en el sentido en que impactan directamente los sistemas y políticas de almacenamiento y gestión de la información de las compañías.

Realizando un análisis somero de ésta ley, podemos decir que las empresas tienen que lograr cumplir los siguientes puntos:

- Se debe considerar como información, registro ó documento, cualquier tipo de medio de información que sea relevante, incluyendo: correos electrónicos, documentos de papel, archivos electrónicos, conversaciones telefónicas, conversaciones de mensajería instantánea, etc.
- Tener claramente establecidos procedimientos y políticas para la administración de la información, registros y documentos.
- La compañía debe contar con un robusto sistema de almacenamiento, que permita gestionar de manera eficiente y segura, todo tipo de registro electrónico, relacionado con auditorías, y en general cualquier documento que se considere relevante. Este sistema debe garantizar:
  - Acoplamiento con las políticas y procedimientos de manejo de información definidos por la compañía.
  - El registro o documento debe permanecer como mínimo 7 años, por lo cual se debe contar con un sistema de respaldo.
  - La plena integridad y autenticidad de los registros almacenados.
  - Disponibilidad continua de toda la información, para cualquier sistema / persona autorizado.
  - Se debe llevar un registro de acceso, las modificaciones e intentos de eliminación de los registros. Con esto es posible determinar **quién** hizo **que** modificaciones sobre un registro,
  - Completa integración con el Directorio de Usuarios corporativo, de manera que los roles y permisos sobre la información sean definidos de una forma estructurada y jerárquica.

- Más importante que tener robustos sistemas de almacenamiento, es que el personal de la compañía tenga claro cuáles son las políticas de administración de información, y que de forma ética las siga al pie de la letra. Siempre ha sido conocido que los humanos son el primer punto de falla de cualquier sistema de información.

2.2.2 Sección 302. Como se vio anteriormente, ésta sección requiere que los ejecutivos de la compañía, especialmente el CEO y el CFO, aseguren que la información contenida en los balances es completamente acertada, vaya problema. Los balances financieros son elaborados centralizando información, en muchas ocasiones, de millones de documentos, facturas, archivos, registros, etc., almacenados en diversos sistemas de información en algunas ocasiones, en lugares geográficos diversos.

Los registros financieros por lo general siguen un camino a través de varios sistemas o procesos que por lo general incluyen humanos, sufren modificaciones, alteraciones, etc.; por todo esto, dichos registros fácilmente pueden contener errores (intencionales o accidentales), que finalmente se verán reflejados en el balance de la compañía. Por ello, la compañía debe contar con sistemas de información con un nivel de seguridad e integración muy altos.

El flujo de información a través de los diversos sistemas de información corporativos, debe ser transparente, es decir, debe fluir sin ningún impedimento. La información debe estar representada de tal forma que tenga el mismo significado en cualquier parte, no debe perder integridad ni ser alterada arbitrariamente; por ello, se recomienda el uso de formatos de estándares abiertos, como XML, para codificar la información, y de estándares como SOAP, para el intercambio de información entre sistemas.

Sería ideal tener un alto nivel de integración entre los diversos sistemas, ya sea porque se dispone de un mismo proveedor, o porque se dispone de mecanismos

avanzados de integración y orquestación de servicios (SOA, BPEL, ESB). Lo importante de tener integración, es lograr un nivel mínimo de intervención humana en pasos intermedios, evitar el uso de hoja de cálculo, etc., con lo que se garantiza una reducción considerable en las probabilidades de que la información sea alterada de forma intencional o accidental. Los procesos en los que intervienen personas, deben ser cuidadosamente supervisados, para validar que los cambios que se han efectuado, evidentemente sean legítimos.

El punto de entrada de la información a los sistemas de información de la compañía, los denominados "capture points", deben tener estrictos controles de verificación de integridad de la información que se está ingresando, ya que generalmente cuando la información ingresa dentro del perímetro de la compañía, lo hace por medios electrónicos (EDI, Web Services, etc.) y en segunda instancia es ingresada por humanos.

El acceso a la información, ya sea por humanos, o por sistemas, debe estar basado en un estricto sistema de seguridad, ojala, integrado con el directorio de usuarios de la compañía. De esta forma se puede llevar un completo control de quién o que accedió la información, y que modificaciones le hizo.

De esta forma, es posible elevar el nivel de veracidad de toda la información financiera que es recopilada para realizar los balances periódicos de la compañía, brindando confianza a los inversionistas, accionistas y a los ejecutivos de alto rango de la compañía.

2.2.3 Sección 409. Los sistemas de información corporativos (Especialmente los ERP y sistemas de Inteligencia de Negocios) deben contar con sistemas que sean capaces de detectar e informar de una manera inmediata, cambios importantes en las condiciones financieras de la empresa, de manera que los accionistas y los entes reguladores conozcan estos eventos con la mayor prontitud posible. De ésta manera se busca proteger los intereses de los inversionistas en la compañía.

2.2.4 Sección 806. La compañía debe contar con un mecanismo para permitir que los *informantes* de la compañía puedan comunicar de forma anónima, a los entes reguladores como la SEC, situaciones irregulares en casos de sospecha de fraude financiero. Se debe garantizar el completo anonimato de quien realiza el informe, así como la completa confidencialidad y reserva de la información que está siendo suministrada.

2.2.5 Sección 404. El impacto que esta sección tiene en los sistemas de información es enorme. Aunque explícitamente no habla de generar controles internos en los Sistemas de Información, es claro que éstos tienen que estar en el centro de ésta norma, dado que los controles internos se realizan en pro de buscar el cumplimiento de las demás secciones de la Ley SOX.

Pero después de todo, ¿Qué son controles internos? Podríamos definirlos brevemente como un conjunto de procesos de control liderados por los altos ejecutivos de la compañía, que buscan alcanzar objetivos claros en las siguientes categorías:[5]

- Efectividad y eficiencia en las operaciones de la compañía
- Confiabilidad en los reportes financieros
- Cumplimiento de las normativas y regulaciones establecidas.

Pero seamos más específicos, la SEC (Securities and Exchange Commission), acuñó el término *Controles Internos sobre Reportes Financieros*, que es una versión más específica de lo que son controles internos en el ambiente SOX:

"Es un proceso diseñado o que está bajo la supervisión del presidente de la compañía y de los ejecutivos financieros, o empleados con cargos similares, y efectuado por la junta directiva, las gerencias y otro personal, para proporcionar una aseguramiento

[5] Definición dada por la COSO

razonable de la confiabilidad de los reportes financieros y de la preparación de los estados financieros para propósitos externos a la compañía y en concordancia con los Principios de Contabilidad Generalmente Aceptados, e incluyen aquellas políticas y procedimientos que:

- *Pretenden el mantenimiento de registros que en un detalle razonable reflejen de forma precisa y correcta las transacciones y entregas de los activos del emisor.*
- *Proveen un aseguramiento razonable de que las transacciones son almacenadas el tiempo que sea necesario para permitir la preparación de estados financieros en concordancia con los Principios de Contabilidad Generalmente Aceptados, y que los recibos y gastos del emisor están siendo hechos con la autorización de los gerentes y directores de la compañía.*
- *Proveen un aseguramiento razonable respecto a la prevención o detección a tiempo de adquisición, uso o disposición no autorizadas de los bienes o activos de la compañía."* [6]

Podríamos decir que, logrando cumplir a cabalidad todos los requerimientos de ésta sección en especial, se lograría cumplir gran parte de los requerimientos de las demás secciones que impactan TI. Anteriormente mencionamos de forma dispersa los impactos de SOX en los sistemas de TI, ahora mencionemos las áreas de TI y los temas que sin importantes:

- Seguridad y Control Centralizado de Usuarios
- Sistemas ERP, CRM y SCM e integración de los mismos
- Sistemas de Almacenamiento y Resguardo de Información
- Redes de Comunicación
- Sistemas de Administración de Documentos
- Portal Corporativo Centralizado
- Sistemas de Inteligencia de Negocios y Análisis de Reportes

[6] Definición dada por la SEC, http://www.sec.gov/rules/final/33-8238.htm

- Sistema de Comunicación para Informantes

Ahora que sabemos que son los controles internos, y sabemos que pretenden lograr dentro de la compañía, podríamos preguntarnos: ¿Qué controles internos puedo aplicar a mis sistemas de información para cumplir con la Ley Sarbanes-Oxley? y ¿Cómo los puedo aplicar?. Bueno, la respuesta puede estar en el uso de uno de éstos dos *frameworks*: COSO Internal Control Framework y el otro llamado COBIT.

La siguiente tabla muestra un resumen general de la Ley Sarbanes-Oxley:

Tabla 1 - Sumario de la Ley Sarbanes-Oxley[7]

Sección	**Título**	**Condición/Responsabilidad**	**Impacto potencial en las funciones del CIO/TI**
I	Public Company Accounting Oversight Board (PCAOB)	Esta sección detalla la formación del PCAOB. Destaca los roles y obligaciones del grupo.	Se adiciona un CIO externo al Comité Auditor para la vigilancia de las TI
II	Independencia del Auditor	Regulaciones que determinan el rol y las obligaciones de los auditores externos. Detalla quien puede ser un auditor, períodos de retención de los materiales auditables, restricciones.	Grupo de Vigilancia de TI preferiblemente no deben ser seleccionados por el CIO o los administradores internos sino por miembros externos del grupo.
III	Responsabilidad corporativa	Esta sección detalla la responsabilidad corporativa para el reporte financiero, incluyendo los roles y castigos para los Oficiales y directores.	Se incrementa el enfoque al presupuesto de TI y el valor agregado.

[7] IT Governance and Sarbanes-Oxley: The latest sales pitch or real challenges for the IT function?; Michelle L. Kaarst-Brown, Shirley Kelly. School of Information Studies, Syracuse University, NY USA

302	Responsabilidad Corporativa para reportes financieros	El CEO y el CFO de la compañía deben preparar una declaración que está acompañando al reporte de auditoría que certifica sus declaraciones financieras y el acceso a las mismas.	El sistema financiero de reporte debe ser completo y auditable con un total acceso de donde se recoge la información. Se necesita un soporte de la documentación detallando procesos y procedimientos de donde y cuando se retiene la información.
IV	Mejoras al acceso financiero	Esta sección detalla cuando y que es incluido en los reportes financieros. También detalla como los auditores y oficiales de la compañía deben conducirse.	Puede requerir documentación financiera adicional, modificaciones de datos, o integración de sistemas. Puede requerir cambios a nuevo software, pero más aún, las necesidades del software existente deben ser revisadas y documentadas.
401	Acceso a reportes periódicos	Cada reporte anual y cuatrimestral debería incluir un reporte transacciones equilibradas y sus relaciones con entidades no-consolidadas que pueden tener un efecto futuro en las circunstancias financieras de la compañía.	Se necesita de un sistema financiero que pueda proporcionar la información requerida, en una manera oportuna y consistente. Monitoreo e

			integración de los detalles de los proveedores. Menos palabrería y más detalles en los informes del SEC.
404	Aseguramiento Administrativo de los controles internos	Los reportes anuales deben incluir reportes de control internos que certifiquen la responsabilidad de la creación y el mantenimiento de los reportes financieros. También deberán contener un aseguramiento de la efectividad de estos controles y procesos internos.	Los procesos apoyados por TI necesitan estar documentados y auditados para el cumplimiento en una base regular. Se incrementa el rol de la TI de monitorear y controlar los sistemas de información. Se expande la seguridad de la TI a un nivel de riesgos de manejo empresarial.
409	Acceso del emisor en tiempo real	Los cambios materiales que afectan los reportes financieros deben ser reportados en una base rápida y efectiva.	Los reportes se requieren en días (48 horas), en lugar de semanas, después de ciertos eventos materiales. Los sistemas financieros necesitan habilidades para recoger y asimilar la información necesaria casi en tiempo real.
V	Análisis de	Las compañías de auditoría y	La TI adquiere

	Conflictos de Interés	las asociaciones de seguridad registradas deben adoptar un conjunto de reglas de conflicto de interés que recomienda una imparcialidad en los reportes y auditorías.	un rol mayor al involucrarse de manera más cercana a las actividades de inversión. Los sistemas podrían incluir chequeos de cumplimiento.
VIII	Fraude criminal y corporativo contable	Castigos, estatutos de limitaciones, períodos de retención de papeles de auditoría, consecuencias por la obstrucción de la justicia y la protección a los soplones.	Realmente no hay ningún requisito legal para el CIO, sin embargo, un impacto definitivo en las políticas de retención y destrucción de transacciones y datos de comunicaciones. En el futuro, se espera que las corporaciones requieran una certificación del CIO de que los sistemas de información son seguros, trazables, y siguen los parámetros de retención.
802	Castigos criminales por alteración de documentos	Las compañías deben asegurar que sus registros son auténticos, consistentes, e incontrovertibles. Deben tener unas políticas establecidas y reforzadas para asegurar una apropiada retención y seguridad de los registros.	Impactos en el manejo de los datos, la seguridad de los sistemas y las prácticas de recuperación de los negocios. EL CIO debe entender estos

			requerimientos, asegurándose que se obedecen las políticas, y garantizando su cumplimiento. Se adquiere el rol del CAO (Chief Accuracy Officer), como un guardián de la exactitud de los datos.
IX	Ampliación de las penas a los criminales de cuello blanco	Castigos por intentos y conspiraciones a cometer fraude. Enmienda las responsabilidades corporativas para sentencia a las ofensas de cuello blanco.	La TI debe tener los sistemas adecuados para registrar y trazar algún cambio a la información recogida originalmente. Todas las modificaciones deben ser trazables e identificar a la persona que hizo algún cambio.

2.3 UNA APROXIMACIÓN A COSO

Committee of Sponsoring Organizations of the Treadway Commission, es una iniciativa del sector privado en Estados Unidos (principalmente sociedades de contadores), cuyo principal objetivo es determinar los factores que causan reportes financieros fraudulentos, y realizar recomendaciones para reducir dichos factores.

Es así, como COSO define lo que se conoce como el *Framework de Controles Internos COSO*, el cual incluye una serie de definiciones y lineamientos para la implementación

de Controles Internos en la compañía. Dicho framework esta constituido por 5 componentes principales, que por ahora solo mencionaremos:

1. Control del Ambiente
2. Gestión de Riesgos
3. Actividades de Control
4. Comunicación e información
5. Monitoreo

2.4 UN VISTAZO A COBIT

Control Objectives for Information and related Technology, COBIT, es un conjunto de buenas políticas de gestión de TI enfocada a administradores, auditores y usuarios de TI en pro de mejorar y maximizar los beneficios obtenidos del uso de TI y desarrollar un buen gobierno de TI.

COBIT contiene aproximadamente 34 objetivos generales, 318 objetivos específicos, los cuales están agrupados en 4 dominios principales, a saber:

1. Planeamiento y Organización
2. Adquisición e Implementación
3. Entrega y Soporte
4. Monitoreo y Evaluación

Este marco de trabajo es comúnmente complementado con el estándar de seguridad ISO 17799, el cual es aceptado internacionalmente.

Es indudable el importante papel que empieza a jugar el CIO (Chief Information Officer) en el cumplimiento de las exigencias de la Ley Sarbanes-Oxley, en especial las secciones 404 y 409.

Ahora que hemos presentado la historia de la Ley Sarbanes-Oxley y hemos dado un vistazo a su impacto en los sistemas de información, podemos empezar a develar las verdaderas implicaciones de SOX en TI y a presentar metodologías que puedan ayudarnos a cumplir con un único objetivo: Lograr que los Sistemas de Información de la compañía sean "*Sarbanes-Oxley Compliant*[8]" y que éstos a su vez ayuden al cumplimiento de toda la compañía.

[8] Término que hace referencia al que una empresa ó área esté cumpliendo las regulaciones de la ley SOX

3. IMPLICACIONES DE LA LEY SOX EN LA SEGURIDAD DE LA INFORMACIÓN

Como se mostró en el capítulo 2, el impacto del acto SOX en las TI es muy relevante, ahora bien, ¿Cuál es la implicación de la seguridad de la información en todo este panorama?

Cuando el acto SOX dio origen al PCAOB, éste creó una serie de estándares de auditoría, uno de los cuales titula "Una auditoría de control interno sobre los reportes financieros en conjunto con una auditoría de las declaraciones financieras". Este documento reconoce que no solo el alto mando deberá certificar los controles sobre el sistema, sino que también deberá controlar la manera en que la información financiera es accedida, almacenada, recolectada, procesada y transmitida a través del sistema.

El estándar abierto COBIT, publicado por el Instituto para el Gobierno de TI (IT Governance) y la Asociación de Auditoría y Control de Sistemas de Información, proporciona una serie de controles que deben ser tenidos en cuenta en el momento de certificar SOX en lo que concierne a las TI. Una de las previsiones en las que SOX es enfático, es en la apertura de los reportes financieros a los inversionistas y es en este punto donde la seguridad de la información se hace más relevante. Una buena política de seguridad de una compañía le garantiza al inversionista que se tiene en cuenta la necesidad de tener una información confidencial, confiable e íntegra, que proporciona los sistemas de información.

Otro aspecto importante es que SOX enfatiza en la exactitud de esos reportes, lo que hace relevante la seguridad de la información en la mejora de la confiabilidad y la integridad de esos reportes.

3.1 LOS DATOS: LA PARTE IMPORTANTE PARA SOX

Básicamente podemos decir que la relación directa entre SOX y la Seguridad de la Información, está implícita en la forma como se manejan los datos dentro de los sistemas de información de las compañías. Esa es la razón por la cual, es importante entender los atributos básicos de los datos, la forma de clasificación de los datos y los elementos que permiten establecer su privacidad y protección.

3.1.1 Clasificación de los datos. La clasificación de los datos es el primer tópico a ser tocado a la hora de implementar una estrategia o un acuerdo entre la alta gerencia de las organizaciones y el personal de TI antes de establecer los controles que permitan establecer un conjunto apropiado de controles sobre el acceso y la autenticación.

El propósito básico de clasificar los datos es el indicar el nivel requerido de CIA (Confidencialidad, Integridad y Disponibilidad –Availability-), para cada activo de información. Y asegurar que los datos sean protegidos de una forma costo-efectiva.

Una forma de clasificarlos es añadiéndoles capas de clasificación de confidencial, a secreto, a ultra-secreto y a altamente secreto, y así permitir establecer controles más cercanos a los datos, estableciendo su importancia, usuarios autorizados a manejarlos y acciones permitidas sobre los mismos.
Al proteger estos elementos de los datos y documentos que deben ser protegidos, es el factor clave en el cual la seguridad de la información adquiere una mayor relevancia.

Existen varios esquemas de clasificación como el esquema militar (Ultra secreto, Secreto, Confidencial, Sensitivo sin clasificar, sin clasificar), y de negocios

comerciales (Confidencial, Sensitivo, Privado y Público)[9]. Dennis C. Brewer, en su libro "Security Controls for Sarbanes-Oxley"[10], propone el siguiente esquema:

- Dominio público (Abierto)
- Protegidos
- Restringidos

3.1.2 Datos de Dominio Público o Abiertos. Un ejemplo básico de datos abierto puede ser un número telefónico en un directorio de teléfonos, datos de anuarios escolares, reportes de calificaciones, etc. Es relativamente poco lo que se puede hacer con esta información. Las compañías necesitan confiar en la precisión de estos datos, así pues, impedir el acceso a los mismos no ayuda a nada. Aquí de nuevo se hace énfasis en la necesidad de una integridad y disponibilidad de los datos. Sin embargo, escribir datos en esta categoría sí requiere de controles de acceso.

3.1.3 Datos de Dominio Protegido. La información protegida es simplemente aquella que usted no desea que todo el mundo sepa de ella. Un mínimo de controles de acceso para ésta información podría ser simplemente un usuario y una contraseña. Los negocios y organizaciones tienen información que merece ser protegida de los competidores. Acá es donde los controles de seguridad se enfocan en la necesidad de ser más formalizados. Éste tipo de datos es también compartido con entidades externas, así pues el problema en seguridad tiene que extenderse más allá de los bordes en los cuales la información es contenida.

3.1.4 Datos de Dominio Restringido. Las datos restringidos son aquellos los cuales no son rutinariamente compartidos, y su almacenamiento, lectura, escritura y ejecución están altamente controlados con mecanismos que incluyen pistas de cadena de custodia. Los elementos de información restringida son aquellos cuya apertura

[9] Curso de Certificación CISSP
[10] Dennis C. Brewer, Security Controls for Sarbanes-Oxley Section 404 IT Compliance

inapropiada puede causar daño, dificultades extremas o pérdidas financieras o que sean consideradas como una invasión de la privacidad.

Estas medidas de seguridad pueden y deben ser uniformemente diseñadas y aplicadas a cada nivel de clasificación en todos los sistemas empresariales, la regulación y clasificación de los datos habilita el diseño y la implementación de sistemas bien estandarizados.

3.2 ELEMENTOS ESENCIALES DE LA PROTECCIÓN Y PRIVACIDAD DE LOS DATOS

Brewer propone un conjunto de ambientes que permiten proteger los datos y su privacidad desde un nivel muy simple.

3.2.1 Protección contra la revelación de datos. Primeramente se debe proteger los datos importantes o la información de ser revelada de alguna manera, luego, otorgar los derechos de accederla solo a través de los controles apropiados.

3.2.2 Controlando lo que es revelado. Es importante tener en cuenta que cuando va a revelar información, se debe controlar que es lo que se va a revelar. Un conjunto de políticas de revelado permite que se faciliten intercambios y comercio, mientras que se controla de cerca la información que representa un sentido de importancia comercial para la organización.

El filtrado de datos sobre cuales detalles son revelados y cuáles no, es logrado a través de una profunda clasificación de los datos interactuando con los mecanismos de control de acceso de las TI. La relación de discriminación entre los datos y el garantizado de que los derechos de acceso cumple con los requisitos establecidos para los datos protegidos o restringidos deberán controlar y reportar con exactitud qué información se libera y a quien.

3.2.3 Controles sobre a quién se le exponen los datos. Las compañías no deben suministrar por ejemplo datos de un cliente a otro cliente. Es decir, debe haber cierta seguridad de que la información de una cuenta es compartida solamente con quienes tienen derecho a acceder dicha cuenta.

Los controles de acceso deben estar en la capacidad de hacer una discriminación centrada en la confiabilidad de la identidad de la persona que está tratando de obtener acceso, y una vez identificado, permitirle el acceso solo a conjuntos específicos de la información.

3.2.4 Controles sobre los datos una vez revelados. Esta es tal vez la tarea más desafiante. Una vez la información está disponible, el cómo es usada es la tarea más difícil de controlar, imposible en algunos casos. El diseño de los mecanismos de control de acceso puede utilizar ciertas características que permitan regular como se usa la información en algunos ambientes de tecnología. Muchas veces el único control posible sobre la información que ha sido revelada es mediante acuerdos legales y cláusulas de confidencialidad.

3.2.5 Controlando las condiciones de revelado. El establecimiento de controles sobre el revelado de los datos se trata de mantener a raya el espionaje industrial y los competidores, permitiendo el acceso apropiado a los usuarios finales, bajo las circunstancias establecidas.

Los controles sobre TI deben filtrarlos accesos no autorizados de manera inmediata y tener la capacidad adicional de diferenciar los permisos de los usuarios sobre otros aspectos de control.

3.2.6 Controlar CUANDO se revelan los datos. Se deben establecer mecanismos de control de acceso que permitan definir los momentos de uso de dichos datos. Es decir, si se debe generar un reporte financiero, el sistema debería tener conocimiento

de cuándo y a quien debe presentar dicho reporte, lo que permite garantizar de una manera más simple la confidencialidad e integridad de los datos contenidos en ese reporte. Los intentos de acceso en momentos no autorizados deben ser registrados, bloqueados y reportados por el sistema. El control de acceso de una manera creativa sobre el tiempo, el día y la fecha es una opción valiosa que puede ser considerada en los diseños de seguridad de cualquier modelo de acceso.

3.2.7 Controles sobre compartir, almacenar o mover datos. Los sistemas de información deben estar integrados con controles de acceso y puntos de flujo de los datos con características que permita a los dueños de los datos controlar donde se comparten los datos y donde pueden ser movidos. Diseños que no tienen este tipo de controles son simplemente considerados diseños fallidos desde la perspectiva de la seguridad de la información.

3.2.8 Controles sobre el porqué los datos son revelados. Es necesario concientizar a los usuarios en la necesidad de revelar su identidad con el objetivo de ser validados dentro de los sistemas de información. Controles tales como huellas digitales, escaneos biométricos, claves criptográficas, etc. permiten tener un control de acceso más preciso y facilitan la segregación de obligaciones mediante las cuales el sistema de información identifica al usuario que entra al sistema y que información deberá facilitarle.

3.2.9 Controles sobre la compensación por el revelado. A la luz de la seguridad de la información, el control de acceso a la información personal o la propiedad intelectual de la organización, deber ser considerado desde el punto de vista del valor de la información o el valor que dicha información adquiere cuando está totalmente disponible.

3.3 EL ROL DEL CSO

"Los directivos del área de TI han sido invitados muy tarde al baile". Ésta debería ser la expresión correcta para resaltar el hecho de que desde el principio la implementación de SOX fuese vista como un proyecto del área de finanzas y contabilidad. Muchos CSO pensaron inicialmente que SOX no tenía nada que ver con el área de seguridad de la información, que simplemente sería "una regulación más" que podría ser cumplida fácilmente.

Es importante recalcar que dados los controles de seguridad que se establecen en el área de TI, las funciones de la persona o grupo de personas encargadas de verificar que la información generada sea confiable, integra y esté disponible en el momento en que se requiera, crean la necesidad dentro de las empresas de crear el rol de CSO, e incluso hacerlo más extensivo definiendo el CISO (Chief Information Security Officer), como un soporte mediante el cual el CEO y el CFO se pueden apoyar, para garantizar la transparencia de los reportes financieros.

3.4 REQUISITOS DE LA RETENCIÓN DE DATOS

Los datos electrónicos son un factor crítico, copias de respaldo regulares, adicional a una estrategia de recuperación pueden cubrir las pérdidas de todo un sistema de información, causado por un desastre natural o hecho por el hombre.

Una segunda necesidad es satisfacer la necesidad de alimentar el creciente número de software de integración de negocios, sobre el cual se hacen decisiones tácticas y estratégicas.

Una tercera razón es cumplir con los requisitos regulatorios como SOX. En la legislación estadounidense, estas regulaciones incluyen:

- Registros de negocios: 7 años a permanente.
- Contratos: 7 años a permanente.
- Registros de nómina: 3 a 7 años.

Para cumplir con los estándares de auditoría concernientes a la retención de documentación auditable (SOX802), se requiere que esos registros sean retenidos por siete años luego que el auditor concluya su revisión. En el artículo "Data retention regulations: Keeping IT legal"[11] de Elizabeth Clark, se proporciona un sumario de los requisitos de retención de datos impuesto por la SEC. En dicho artículo, Clark explica que el requisito de la SEC es que dichos registros sean almacenados en un medio no-reescribible, no-borrable.

"In the past, this basically meant WORM technologies such as optical media, or so-called WORM tape approaches such as StorageTek's VolSafe. But last year, the SEC announced it would accept WORM-like magnetic-disk storage systems. Some of these products are based on inexpensive Advanced Technology Attachment (ATA) disks that can be used for on-line or near-line storage (more on this later). Under SEC 17a-3 and 17a-4, the records must also be time-stamped, and copies must be stored in separate locations. In essence, the authenticity, accuracy, and accessibility of these records must be ensured."

Clark describe los tres niveles de retención de los datos, los cuales, las organizaciones deben considerar en sus protocolos de retención de datos:
Los datos que son frecuentemente accedidos o que necesitan ser producidos rápidamente deben ser almacenados en línea.

Los datos que no son frecuentemente usados, o que no se requiere producir con rapidez, puede ser almacenado en medios near-line (cuasi en línea), como sistemas ópticos o librerías de cintas.

[11] Data Retention Regulations: Keeping It Legal. Network Magazine, April 2004. Elizabeth Clark.

Finalmente, los datos que no son accedidos regularmente, pueden ser almacenados off-line en cintas de archivo.

4. IMPACTO EN LOS SISTEMAS FINANCIEROS

Éste capítulo estará dedicado principalmente a analizar una parte de la sección 302 de la Ley SOX, aquella que habla de la importancia de tener reportes financieros lo más transparentes y veraces posibles, esto con el fin de proteger los intereses de los inversionistas y accionistas de las empresas. Además se analiza la relación de la sección 404 (controles internos) con los sistemas financieros. Durante el avance del capítulo se darán algunos lineamientos tecnológicos que ayudarán a alcanzar el cumplimiento de las secciones 302 y 404 de la Ley Sarbanes-Oxley.

4.1 SISTEMAS FINANCIEROS / ERP

Se ha visto a lo largo de este proyecto que la Ley Sarbanes-Oxley impacta en gran medida, de forma directa e indirecta, diversos aspectos tecnológicos de una organización. Los sistemas financieros en general, son los más afectados de forma directa por la Ley, ya que sobre ellos recae toda la responsabilidad de mantener la información financiera y contable en una forma íntegra y segura, pero disponible para cuando ésta sea requerida.

Se podría definir un sistema financiero como aquel que de alguna manera directa interactúa con la información financiera o contable de la compañía. Los sistemas financieros serían entonces abarcados por un conjunto de sistemas de información corporativos denominado ERP (Enterprise Resource Planning).

Por lo general, las medianas y grandes compañías disponen de un gran sistema ERP que puede manejar gran parte de los procesos e información de la compañía. Un buen

sistema ERP debería estar en capacidad de manejar ventas, entregas, pagos, producción, facturas, compras, administración de inventarios, calidad de administración, administración de recursos humanos y contabilidad. Algunos de los sistemas ERP más poderosos (Denominados comúnmente Business Suite[12]) están en capacidad de manejar toda la cadena de negocio completa, desde la parte de atrás de proveedores y compras (SCM y SRM) pasando por todos los procesos internos anteriormente mencionados (ERP, PLM) hasta llegar al proceso de ventas y gestión de clientes (CRM).

4.2 RESPONSABILIDAD DEL CFO Y EL CEO

Con las nuevas regulaciones de la Ley SOX, se le exige al CFO y al CEO, certificar con su firma la veracidad de toda la información contenida en los balances financieros en cada periodo fiscal de la compañía. Esto implica una gran responsabilidad para ambas personas, si tenemos en cuenta que los balances financieros se elaboran recopilando y procesando grandes cantidades de información provenientes de diversos sistemas de información presentes en las compañías. Además la sección 302 y 404 hacen un gran hincapié en el establecimiento de una estructura o mecanismo de control interno, y que regularmente realizan una revisión de la efectividad de dichos controles internos y de los procedimientos establecidos para elaborar reportes financieros.

4.3 CONTROLES INTERNOS

Los controles internos pueden significar cosas diferentes para diferentes personas. Afortunadamente la SEC ha dejado muy en claro la definición de control interno, dada por la COSO, organización recomendada por la SEC como la encargada de dar las directrices y entornos de trabajo en lo que a control interno se requiere.

[12] Término acuñado principalmente por Oracle y SAP

"Control interno es un proceso efectuado por la junta directiva, ejecutivos y otro personal, diseñado para proveer una garantía razonable de alcanzar unos objetivos específicos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de los reportes financieros
- Cumplimiento con las leyes y regulaciones "

Más relacionado con el tema de los sistemas financieros, está el término "Controles internos sobre la información financiera", término acuñado en el año 2003 por la SEC, y que es una variante del término "Control Interno" de COSO

Controles internos sobre la información financiera.

"Un proceso diseñado por, o bajo el control del CEO del emisor[13] y los ejecutivos y funcionarios financieros principales, o personas que ejerzan funciones similares, y ejecutado la junta directiva del emisor, gerentes y demás personal, para proporcionar una seguridad razonable con respecto a la fiabilidad de la información financiera y la preparación de los estados financieros para propósitos externos de conformidad con los principios contables generalmente aceptados (GAAP) e incluye aquellas políticas y los procedimientos que:

- Se refieren al mantenimiento de registros que con detalle razonable y bastante precisión reflejan las transacciones y disposiciones de los activos del emisor;
- Ofrecen garantías razonables de que las transacciones se registran como sea necesario para permitir la preparación de estados financieros de conformidad con los principios contables generalmente aceptados, y que los ingresos y los gastos del emisor se están realizando sólo en conformidad con las autorizaciones de gerentes y directivos del emisor, y

[13] El término emisor hace referencia a la compañía que está en la bolsa y emite las acciones

- Ofrecer garantías razonables en cuanto a la prevención o detección oportuna de la adquisición no autorizada, uso o enajenación de los activos del emisor que podría tener un efecto material sobre los estados financieros."

4.4 PROCESO DE CONTROL INTERNO

El proceso de control interno está enfocado en los esfuerzos corporativos por alcanzar los objetivos operativos y asistir en el tener información financiera confiable a la luz de regulaciones establecidas por la ley. Básicamente un buen sistema de control es el que lleva a la organización en su día a día, está ahí como guía para garantizar que las cosas se hagan como se deben hacer, pero esto no es garantía del éxito del negocio. Desafortunadamente el alcanzar los objetivos del Control Interno está en la mano de seres humanos, que cometen errores y que consciente o inconscientemente pueden alterar la información financiera de la empresa.

El proceso de control interno está compuesto principalmente de 5 partes interrelacionadas, las cuales surgen a partir de la manera como se componen los negocios. Estos componentes proveen un entorno apropiado para apreciar y analizar los controles internos implementados en la organización:

1. Ambiente de Control. El ambiente de control es la base o fundación de todos los otros componentes del control interno. Debe estar incrustado dentro de la cultura de la organización, de forma que toda la organización vea el control interno como algo que tiene que ver con el mejoramiento de la compañía.

2. Evaluación y manejo de riesgos. Toda compañía está sujeta a todo tipo de riesgos de carácter interno y externo que pueden llegar a afectar los objetivos de la empresa. El proceso de evaluación de riesgos implica una fase de identificar los riesgos, definir un plan para eliminarlos, y los que no se puedan eliminar, como

mitigarlos. Los riesgos casi siempre son muy variables y dependientes de factores externos, económicos, políticos, etc., la compañía debe estar en capacidad de hacer seguimiento de dichos factores para evaluar como cambian los riesgos.

3. Actividades de Control. Son los procedimientos y políticas que los gerentes elaboran para asegurarse de que los objetivos de la compañía sean cumplidos, para asegurarse de que los riesgos no están afectando el flujo del negocio. Las actividades de control están presentes a lo ancho y largo de la organización, en todas las actividades, procesos y funciones. Las actividades de control incluyen aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del rendimiento, seguridad de los activos y separación de tareas.

4. Información y comunicación. Este componente hace un llamado a las compañías para que establezcan mecanismos que generen información acerca del estado de sus controles internos, y que comunique esa información de forma rápida y efectiva a quien la necesite, es decir, al gerente, directivo o empleado encargado de realizar el seguimiento de ese control interno. COSO requiere que se haga un adecuado monitoreo de los controles internos. Toda la información relevante a los controles internos debe fluir libremente por los sistemas de información de forma que los empleados puedan saber que tipo de controles internos esperan los administradores y gerentes, y que tipo de ambiente de control se desea propiciar. En ocasiones es necesario también un flujo de información hacia fuera, por lo que se requiere una regulación adicional.

5. Monitoreo. Si la empresa ha tomado la decisión de implementar controles internos, bueno, entonces es necesario implementar mecanismos que permitan monitorear su eficiencia y rendimiento, y que permitan tomar medidas correctivas en caso de detectar fallas, en caso de que la falla sea grave, el reporte se debe escalar hasta donde sea necesario, incluso hasta la junta directiva. El monitoreo debe ocurrir en el curso o ejecución de las operaciones, pero periódicamente se deben programar monitoreos y evaluaciones por parte de supervisores. El alcance y frecuencia de la

evaluación de los controles internos dependerá exclusivamente en la evaluación de riesgos y de los procedimientos de monitoreo en curso.

El siguiente cubo muestra la relación entre los objetivos del control interno (en la cara superior), los componentes del proceso de control y los diferentes componentes de la organización.

Ilustración 2. El Cubo COSO

Entonces, ya que se tiene claro lo que es un control interno, y específicamente controles internos sobre la información financiera vamos a profundizar sobre algunos de los riesgos presentes en los sistemas financieros y los controles internos que deben ser implementados para tratar de mitigarlos.

4.5 RIESGOS MÁS COMUNES IDENTIFICADOS EN LOS SISTEMAS FINANCIEROS

4.5.1 Sistemas financieros y de planeamiento dispersos/dispares. Muchas de las grandes y medianas compañías del medio, poseen diversos sistemas financieros y de planeamiento para correr su negocio. Entre éstos podrían estar sistemas ERP, CRM de logística y por supuesto, sistemas financieros.

Hoy en día es muy común leer noticias sobre fusiones o adquisiciones de compañías en todo el globo. Esto obviamente también genera que hayan sistemas dispares de información, con sus consecuencias para el cumplimento de las regulaciones legales. Otro de los motivos para tener esta situación, es el caso de grandes multinacionales que poseen muchos tipos de negocios, cada cual, con sus propios sistemas de información.

El gran problema surge cuando se trata de consolidar o cruzar grandes cantidades de información provenientes de cada uno de esos sistemas, para, por ejemplo realizar informes financieros, o estados de cuenta, o para continuar una transacción o ejecutar una operación de un sistema a otro.

El flujo de información entre estos sistemas casi siempre se complica debido a que podrían estar separados geográficamente, estar corriendo sobre diversas plataformas, usar diversos protocolos de comunicación, lo que implica un gran reto tecnológico y corporativo, el poner a "hablar" esos sistemas, por lo cual, en muchas de las empresas actuales, la comunicación entre esos sistemas es muy precaria, casi manual.

Entonces, es necesario implementar mecanismo de integración de sistemas que permita que el flujo de mensajes e información sea transparente, con lo cual se estaría cumpliendo uno de los requerimientos de la Ley Sarbanes-Oxley.

Una de las aproximaciones que más aceptación está teniendo en este momento para dar solución al problema de integración de sistemas es SOA (Service Oriented Architecture), un concepto que está ganando adeptos.

SOA es una arquitectura de software que está basada alrededor del concepto de procesos de negocio, desarrollados como aplicaciones que pueden ser vistas como servicios ínter operativos, es decir, que se pueden llamar entre ellos mismos y pueden llamar y ser llamados por sistemas externos. La idea con SOA es quitar las restricciones que imponen los sistemas operativos, los lenguajes de programación y los protocolos de comunicación. Una de las grandes ventajas que tiene SOA, es que sus implementaciones son realizadas en base a estándares abiertos de comunicación y representación de datos, como XML, HTTP, SOAP, WSDL, entre otros.

Entonces la idea con SOA, es implementar para cada uno de los sistemas "legacy" o sistemas propietarios, un conjunto de adaptadores que puedan exponer las funciones de negocio prestadas por el sistema, como servicios que puedan ser consumidos. La idea es que todos esos servicios expuestos en todos los sistemas, puedan hablar el mismo lenguaje, de modo que puedan ser invocados desde cualquier sistema, como consecuencia haya un flujo libre de información.

El mecanismo que se implementa para que los mensajes entre los diversos sistemas fluyan, se denomina ESB (Enterprise Service Bus). En la gráfica que se presenta a continuación se esboza una implementación de SOA y de ESB, en la cual se incluyen servidores Mainframe, Bases de Datos, Servidores de Correo, Servidores eComerce, Servidores de MQ, entre otros. En ella se puede apreciar el rol que juega ESB como integrador de sistemas.

De todas formas existen otros mecanismos y arquitecturas que permiten realizar la integración de sistemas de información.

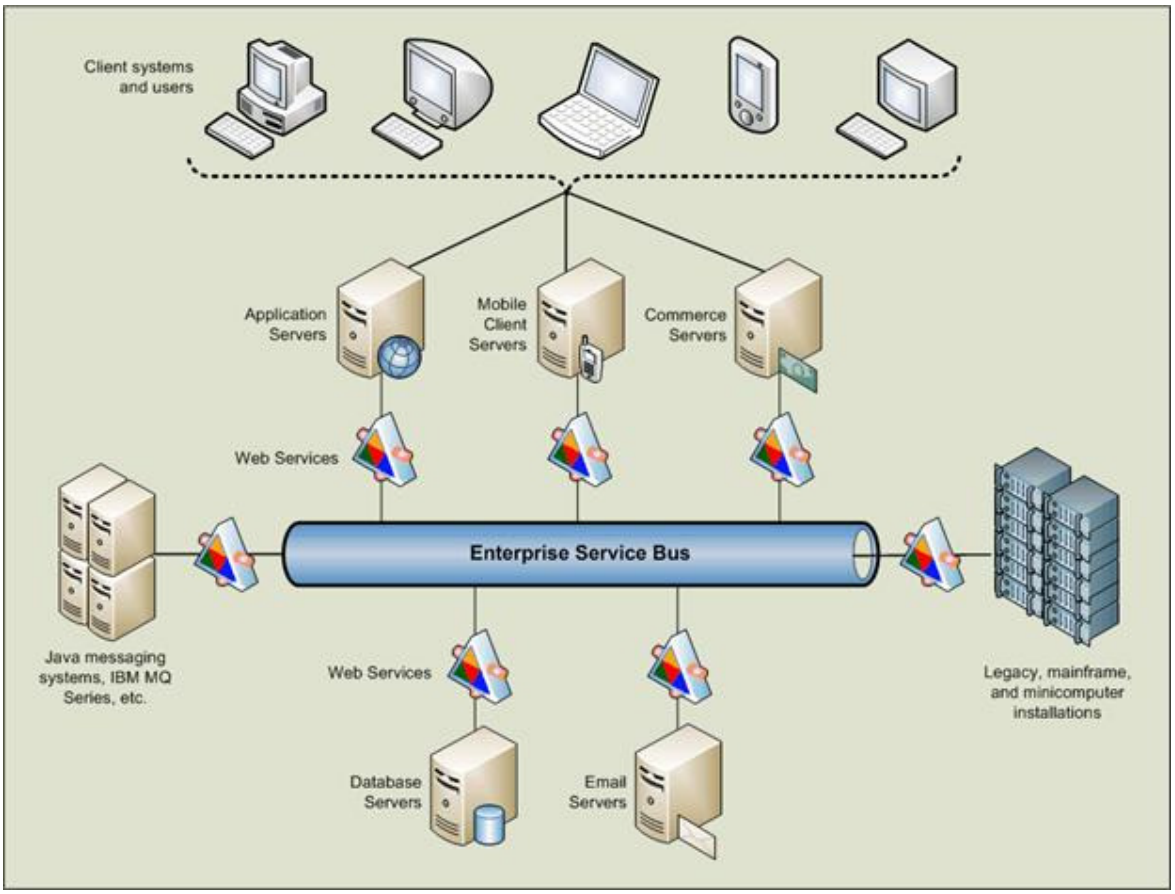

Ilustración 3. Integración de Sistemas Heterogéneos mediante ESB

4.5.2 Separación de actividades y aprobaciones. Algunas actividades y/o procedimientos críticos que impliquen el acceso a información financiera o movimientos de dinero, son realizados o ejecutados por una sola persona. Esto aumenta enormemente la probabilidad de cometer fraude o de obrar erróneamente.

Este riesgo puede ser mitigado fácilmente aplicando dos controles:

- Las tareas o procedimientos que impliquen varios pasos deben ser divididas entre 2 o más personas. Por ejemplo, si se va a realizar el pago de la nómina y ésta implica 5 pasos, lo ideal sería asignar cada paso a una persona diferente, para que así cometer un fraude o una equivocación involuntaria sea algo complicado.

- Realizar transacciones que impliquen dinero, deben ser autorizadas por una persona superior o por lo menos diferente. La transacción además debe quedar documentada.

En las reglas del negocio del sistema, se debe establecer que actividades o transacciones requieren la aprobación o supervisión de un tercero para ser ejecutadas. Una aprobación del supervisor, ya sea manual o electrónica, implica que él o ella han verificado que la actividad o transacción están en conformidad con las políticas y procedimientos de la compañía.

Éste control se puede establecer a nivel tecnológico, dado que la gran mayoría de sistemas ERP y financieros permiten la integración con el concepto de Workflow, el cual incluye separación de tareas y procesos de aprobación.

4.5.3 Control inadecuado de usuarios y privilegios de acceso. Para muchas empresas es un verdadero dolor de cabeza el manejo de cuentas de usuario y sus privilegios de acceso a la información. El riesgo real aparece cuando la empresa no cuenta con un mecanismo adecuado de gestión de identidad, que le permita tener verdadero control sobre los usuarios existentes, que estos usuarios realmente estén asociados a empleados actuales de la compañía o a terceros autorizados, y que dichos usuarios tengan estrictamente los permisos requeridos y niveles de acceso a la información financiera o aplicativos que maneje la compañía. Otro riesgo real surge cuando la compañía no cuenta con un repositorio central de usuarios, y por el contrario tiene dispersos, una serie de servidores de directorios y/o bases de datos de usuarios, cada uno de los cuales, para un sistema de información diferente.

Para muchos expertos, este es uno de los temas más álgidos y más sonados en la regulación exigida por Sarbanes-Oxley, incluso muchos se atreverían a decir que los controles internos hacen referencia directa a la gestión de usuarios y privilegios de

acceso. Según una encuesta realizada por una firma de auditoría muy respetada[14], el 70% de las deficiencias encontradas sobre la sección 404 de la ley SOX, están relacionadas con el manejo inadecuado de las políticas de gestión de identidad y acceso. O como diría un ejecutivo de Novell: "No es una sorpresa que muchos CIO's estén tomando la Seguridad y la Gestión de Identidad como una forma efectiva de manejar el proceso de implementar algunos de los requerimientos de SOX". Por esta razón, se le debe dar importancia a éste tema, y explicar porque, con Indentity Management podremos avanzar mucho en el tema de cumplimiento de la sección 404 de SOX.

Identity Management es un sistema integrado de tecnologías y políticas corporativas que pretenden brindar un mecanismo de acceso a los sistemas de información de la compañía.

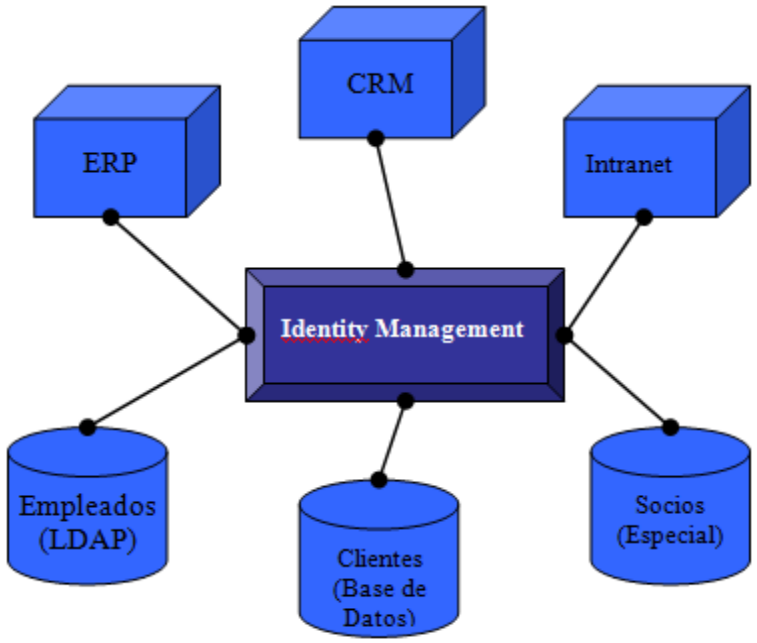

Ilustración 4. Un ejemplo de cómo usar Identity Management

[14] Fuente: Ernst & Young Engagement Analysis, Junio de 2004

En la gráfica anterior se pueden apreciar, en la parte inferior las fuentes o repositorios de usuarios de la compañía (empleados, clientes y socios) y en la parte superior algunos de los sistemas más importantes con los que cuenta la compañía. Identity Management entra a jugar un papel importante como repositorio unificado de usuarios y gestor de políticas de acceso a los diversos sistemas de información y aplicaciones de la compañía.

Para que una implementación de Identity Management pueda contribuir al cumplimiento de las regulaciones exigidas por la Ley Sarbanes-Oxley, ésta debe tener mas o menos estas características:

- Single Sign-On. Proveer, en la medida de lo posible, un mecanismo de Single Sign-On, es decir, la posibilidad de que el usuario se conecte una sola vez con su usuario y password, y éstas credenciales sean replicadas de forma automática a todos los aplicativos y recursos que el usuario necesite.

- Integración. Algunas organizaciones poseen docenas e incluso centenares de aplicaciones, sistemas de información y demás recursos, cada uno de los cuales puede poseer su propio repositorio de usuarios, esto implica la necesidad de tener una solución de Identity Management que se pueda integrar a todos esos sistemas.

- Aprovisionamiento. El sistema debe estar en capacidad de aprovisionar a los nuevos usuarios con las cuentas y privilegios apropiados para acceder a los recursos corporativos. Además, cuando sea el tiempo indicado para eliminar el usuario (por ejemplo, el empleado abandona la compañía, o el proveedor sale del proyecto), es necesario eliminar la(s) cuenta(s) asociada(s) al usuario y sus privilegios de acceso.

- Administración del Acceso. Dado que en el proceso de aprovisionamiento, al usuario le fueron concedidos una serie de privilegios de acceso sobre los sistemas o la información financiera, es necesario tener una plataforma que regule y controle las políticas de acceso. Éstas políticas deben incluir accesos a las aplicaciones, los sistemas de información, así como a las bases de datos más protegidas. Éstas políticas deben regir a través de todos los sistemas, plataformas y aplicaciones de toda la compañía.

- Monitoreo y auditoría. Como se había dicho anteriormente, mas importante que implementar y aplicar los controles internos, es saber si éstos están realmente funcionando. Se debe estar en capacidad de determinar de forma rápida los usuarios creados en el sistema, que privilegios tienen, que han hecho esos usuarios, si han tratado de hacer algo a lo que no tienen acceso, etc.

4.5.4 Uso de hojas de cálculo como herramienta financiera. El uso de hojas de cálculo se ha convertido en una importante herramienta financiera y en soporte a procesos operacionales, especialmente en las pequeñas y medianas compañías, aunque en las grandes compañías siga siendo la herramienta preferida para hacer reportes financieros y para realizar toma de decisiones.

Una encuesta del año 2003 hecha por el grupo Hackett encontró que el 48% de las compañías en Estados Unidos usaban hojas de cálculo para elaborar presupuestos y planeación de recursos. Considerando la importancia de la información que se almacena en esas hojas de cálculo, es alarmante encontrar que un estudio elaborado por Rajalingham, Chadwick and Knight, determinó que el 90% de las hojas de cálculo estudiadas contienen errores, lo que es inaceptable, ya que el CFO y el CEO deben certificar la veracidad de la información contenida en los reportes financieros.

Los riesgos potenciales y problemas que pueden surgir con el uso de las hojas de cálculo son variados, para poder evaluar el riesgo se debe tener en cuenta lo siguiente:

- Complejidad de la hoja de cálculo y de las fórmulas usadas
- Propósito y uso de la hoja
- Número de usuarios de la hoja y permisos de éstos sobre la misma
- Potenciales errores en la entrada de los datos
- Errores en la lógica de las fórmulas utilizadas
- Tamaño de la hoja de cálculo
- Grado de entendimiento de los usuarios de el funcionamiento de la hoja
- Usos de las salidas entregadas por la hoja
- Frecuencia y tamaño de cambios efectuados sobre la hoja
- Desarrollo y fase de prueba sobre la hoja antes de ser usada

Son muchos los errores graves que se pueden cometer por el uso inapropiado de las hojas de cálculo, para tomar uno como ejemplo, un artículo de PricewaterhouseCoopers[15], donde mencionan:

"Un error de hoja de cálculo en una importante institución financiera condujo a un error significativo de mil millones de dólares en los estados financieros. El error se debió a un proceso defectuoso de control de cambio -un cambio no autorizado a una fórmula en la hoja de cálculo- y otras deficiencias de control, incluida la falta de documentación técnica y para el usuario, la insuficiencia de pruebas y la insuficiencia de copias de seguridad y procedimientos de recuperación".

Luego, para remediar o mitigar éstos riesgos presentes sobre el manejo de las hojas de cálculo, no es necesario erradicar el uso de las hojas de cálculo, simplemente es

[15] *http://www.*pwc*.com/images/gx/eng/fs/insu/*rt5.pdf

implementar una política estricta de su creación y uso, y para ello se pueden implementar una serie requerimientos:

- Control de cambios y manejo de versiones. Se debe tener un mecanismo eficiente para realizar un seguimiento de los cambios en la hoja de cálculo, además como un proceso de aprobación de los mismos, cuando la hoja sea de misión crítica. Además, debe existir la capacidad de llevar un control de las versiones basado en los cambios hechos a la hoja.
- Control de acceso y separación de tareas. Se debe tener un control estricto a nivel de los permisos del archivo, para determinar quien o quienes pueden escribir, leer o eliminar la hoja.
- Inventario. Se debe realizar un proceso completo de inventariado de todas las hojas de cálculo, y de cada una de ellas levantar información básica como su nombre, breve descripción de la hoja y su uso, departamento y grupo de individuos que elaboraron la hoja, grupo de usuarios que hace uso de la hoja, etc.
- Aplicar un proceso de desarrollo de software. Se debe, en la medida de lo posible aplicar algún estándar de desarrollo de software a las hojas de cálculo de misión crítica o muy complejas. Es decir, toma de requerimientos, diseño, construcción, pruebas y mantenimiento, como si se tratara de un aplicativo normal.
- Respaldo y Recuperación. Como toda la información importante de la compañía, las hojas de cálculo deben estar incluidas en el proceso de respaldo corporativo de la información. Se debe tratar que las hojas de cálculo estén almacenadas en servidores de archivos o equivalentes, y no en las estaciones de trabajo de los usuarios.
- Integración. Integración con los sistemas de información financieros y contables para reducir la posibilidad de errores en la entrada / salida de datos.
- Migración, cuando sea posible, de las hojas de cálculo más críticas para el negocio a verdaderos módulos del sistema financiero o contable.

4.5.5 Ingreso de información financiera de forma manual. Éste riesgo está muy asociado con 2 riesgos anteriormente mencionados: La falta de integración de sistemas, y el uso inadecuado de hojas de cálculo. Es muy importante reducir al mínimo posible la intervención de humanos en la captura, ingreso y modificación directa de información financiera en los sistemas de información de la compañía. Ya anteriormente se brindo un claro ejemplo donde el mal uso de una hoja de cálculo produjo un error multimillonario en un balance financiero, y ni hablar de los ya muy mencionados "errores" multimillonarios cometidos en Enron y WorldComm. Los humanos somos susceptibles a cometer errores, ya sea de forma involuntaria, o con intención de cometer algún tipo de fraude.

Por esto, es muy importante contar con mecanismos de verificación de la información "ingresada" por empleados o terceros a los sistemas de información de la empresa.

4.5.6 Intervención y manipulación directa sobre la información financiera. En muchas compañías es muy común, que los usuarios del área de finanzas y contabilidad, por diversas razones, tengan "acceso directo" a las bases de datos que soportan los sistemas financieros y ERPs. Por ejemplo, cuando hay una inconsistencia en la información presentada por algún módulo del ERP, el usuario simplemente se conecta a la BD mediante una herramienta de escritorio, realiza la consulta que requiere, y luego tranquilamente realiza la actualización o borrado de la información que desea. Todo esto, en la mayoría de los casos se realiza sin ningún control, sin ninguna auditoría. No se percatan del riesgo que esto implica para la integridad de la información financiera. Muchas empresas se confían, en que ellos tienen políticas de seguridad para que solamente los usuarios autorizados puedan entrar a esas BD, pero, ¿Quién les garantiza que ese usuario no va a desestabilizar la información financiera?, ¿Cómo tienen ellos certeza de que fue realmente lo que hizo el usuario en la BD?.

Por todo esto, es necesario indicar los requerimientos que se deben implementar para evitar o mitigar el riesgo de corromper las Bases de Datos corporativas.

1. Aplicar controles a nivel de base de datos para supervisar y gestionar todos los accesos, actualizaciones, inserciones y supresiones realizadas a los datos financieros desde las aplicaciones de financieras y de contabilidad, así como los hechos desde otras herramientas de escritorio.
2. Restringir el acceso directo a las bases de datos a usuarios con un nivel de conocimiento avanzado del sistema ERP/Financiero, y requerir de procesos de aprobación-supervisión, para cuando se requieran realizar cambios directos sobre la información financiera.

5. IMPACTO EN EL MANEJO DE LA INFORMACIÓN Y LOS SISTEMAS DE ALMACENAMIENTO

Si bien una gran parte de la cobertura y la discusión respecto a la ley SOX se ha centrado en su impacto inmediato en las prácticas de contabilidad, información financiera y gobierno corporativo, el impacto de la ley no solo se limita a éstas áreas. De hecho, la ley alcanza el corazón de la compañía impactando directamente la forma en que las empresas deben mantener, controlar, gestionar el uso de un elemento vital de la organización-es decir, sus activos de información. Al igual que la gestión de la información y registros, el cumplimiento SOX es un proceso que requiere una aproximación tipo "top-to-bottom" y una vigilancia constante por parte de los responsables de velar por el cumplimiento.

La idea central de SOX es un intento por mejorar la contabilidad y la transparencia de las empresas que cotizan en la bolsa. La contabilidad y la transparencia dependerán de registros comerciales[16] confiables y precisos de la empresa. En esencia, los registros comerciales, deben servir como la base de la contabilidad y los sistemas de información financieros. Las cifras de utilidades, por ejemplo, no "salen del aire" – por el contrario, se derivan de los registros de las transacciones comerciales - facturas, órdenes de compra, contratos, información de pagos, y así sucesivamente. Obviamente, si estos registros son inexactos, también lo será la información en el sistema contable. Como tal, el cumplimiento de la ley SOX descansa en una base de prácticas de gestión de la información y registros, que garanticen la fiabilidad y exactitud de los registros comerciales.

[16] El término registro comercial hace referencia a la información registrada en documentos como facturas, ordenes de compra, etc.

Es fundamental entonces, que las empresas comprendan cómo la ley SOX impacta las políticas de gestión de la información y los registros, y como éstas se deben adaptar y mejorar para que cumplan con las regulaciones de la Ley SOX.

3.5 DEFINICIÓN DE INFORMACIÓN

Antes de comenzar a explicar el impacto que tiene Sarbanes-Oxley en el manejo de la información y los sistemas de almacenamiento, se comenzará por definir el término *información*. A pesar de que puede parecer un término trivial hay que diferenciar varias definiciones que a menudo tienden a confundirse: datos, e información

Un dato, podría definirse como una mera pieza de información o conjunto de ésta, que está representada de alguna forma distintiva o especial y que en sí no tiene algún significado propiamente. Podríamos decir por ejemplo, que el entero 980293 almacenado en dos bytes en un medio magnético, es un dato que por sí mismo no dice nada.

La información, por el contrario es el resultado de dar valor o significado a los datos, realizando algún tipo de interpretación, tabulación, ordenamiento ó procesamiento, de forma que se pueda obtener más de lo que inicialmente se tenía. La información tiene significado y valor en un contexto dado, por ejemplo dentro un sistema de información financiero, el mismo entero 980293, que por sí mismo es un dato, podría pasar a ser $980.293, el valor total de una factura por pagar.

Teniendo en cuenta lo anterior, debería estar claro que la información no es solamente aquella que está almacenada de forma electrónica. Se debe considerar como información, cualquier documento, registro, carta, memorando, mensaje de voz, factura impresa, y en general cualquier registro que contenga información pertinente al negocio.

3.6 IMPORTANCIA DE LA INFORMACIÓN EN UNA EMPRESA

Desde la aparición de los primeros computadores para uso empresarial en los años 60, la información digital ha pasado a tomar un papel importante en todos los procesos de las compañías.

La información y los datos han pasado de ser meros bytes y registros almacenados en discos duros, a convertirse en un verdadero activo que incluso muchas empresas registran en sus balances financieros. Incluso hoy en día se puede decir que existen grandes compañías que basan su negocio en poseer, procesar y dar valor agregado a enormes cantidades de información, como es el caso de Google y Yahoo!; sus fundadores se dieron cuenta del enorme valor que tiene el disponer de la información realmente importante, en cualquier momento.

El término informática, es acuñado precisamente como resultado del vocablo francés *information automatique*, o automatismo de la información; es decir, el procesamiento automático de la información, mediante el uso de sistemas computacionales y complejos procesos. Palabras más, palabras menos, toda la tecnología que conocemos hoy ha evolucionado gracias a la información.

Como se verá más adelante, el valor o importancia de la información cambia continuamente a medida que pasa el tiempo, llegando a un punto donde debe ser desechada para no causar costos innecesarios en la empresa.

3.7 APARECE EL ROL DE CDO

Grandes cantidades de información son almacenadas cada día en muchas de las grandes compañías del mundo, como dato curioso, WalMart tiene almacenados más de 460 TB de información, casi el doble de la información disponible en Internet. Pero, ¿Qué hacer con tanta información almacenada?, ¿Cómo aprovechar al máximo toda esa información?, ¿Cómo aprovechar al máximo los recursos de almacenamiento que posee la compañía?

A raíz de la importancia de la información y el manejo de los datos en las empresas, comienza a definirse de forma clara un Rol que hoy en día no es muy popular: El Chief Data Officer (Ejecutivo Administrador de la Información), pero que en grandes compañías como Yahoo! y CitiGroup ya tienen un importantísimo puesto asegurado entre los altos ejecutivos. Sin embargo, los Administradores de Datos han existido desde el mismo inicio de la computación, solo que siempre se ha considerado como algo que se debe hacer, pero hasta ahora no se le había dado el reconocimiento y la importancia que merecen.

El Rol del CDO se hace entonces necesario en una compañía, incluso si ésta no es muy grande. Podríamos decir que la principal función del CDO es la investigación, desarrollo y aplicación de políticas, procedimientos, arquitecturas, y prácticas mediante las cuales se pueda administrar de forma eficiente y adecuada toda la información que posee la compañía. Esto no necesariamente implica que el CDO posea conocimientos técnicos específicos como por ejemplo de administración de bases de datos, o manejo de data warehousing; es más un cargo estratégico que táctico. Sin embargo podríamos mencionar unas tecnologías y metodologías mediante las cuales el CDO puede aprovechar al máximo la información de la compañía: la Minería de Datos y la Inteligencia de Negocios.

Entre los principales desafíos que podría enfrentar el CDO se encuentran:[17]

[17] Tomado de http://www.tdan.com/view-articles/4581

- El Rol del CDO debe ser el de una persona tanto con habilidades tecnológicas, de administración y de negociación, y que le sean delegadas responsabilidades de toma de decisión.
- Otro reto importante es de alinear la estrategia del negocio con las políticas de administración de la información
- El manejo de grandes volúmenes de información, su procesamiento en tiempos cortos, su almacenamiento a largo plazo.
- Garantizar que la información que proviene de fuentes externas a la compañía (como los proveedores) no contiene errores (casi imposible), pero esto se puede lograr estableciendo acuerdos comunes.
- Responsabilidad en conocer todo el viaje que hace la información al interior de la compañía, y comprender su valor dentro de ella.
- La privacidad y la seguridad de la información, aunque no son responsabilidades propiamente del CDO, éste debe conocer que políticas y que controles está implementando el CSO.

Podría decirse entonces que el CDO se convierte en el administrador del activo más preciado y a la vez menos utilizado y comprendido de las empresas: la información. El CDO es quien debe velar porque las políticas de almacenamiento y gestión de la información estén presentes y sean implementadas de forma que se pueda garantizar la integridad y disponibilidad de la información. Él (ella) es quien puede dar un gran valor agregado a toda esa información que se encuentra almacenada en grandes bases de datos, él (ella) es quien debe velar por la integridad y confidencialidad de esos registros. En manos del CDO ésta la clave del éxito en el proceso de acomodar la compañía a las regulaciones legales a las que se afronta la empresa, entre ellas, SOX.

Toda empresa, sin importar su tamaño, o su línea de negocio, debería entonces contar con una figura visible, quien debería estar a cargo de la información de la compañía. Obviamente dependiendo del tamaño de la compañía, éste rol podría llamarse CDO,

en las grandes corporaciones, o simplemente "Data Steward", en las pequeñas y medianas empresas.

Poniendo toda esta información en contexto y relación con el impacto de la Ley Sarbanes-Oxley, se puede decir entonces que el CDO o Data Steward debe ser quien garantice la integridad de la información financiera, mediante la implementación de políticas y tecnologías.

3.8 RETENCIÓN DE LA INFORMACIÓN DE AUDITORÍA

Como se lee literalmente en la sección 103, Parte (a)(2)(A)(i), de la Ley Sarbanes-Oxley, *"...se debe preparar y mantener por un periodo no menor a 7 años, documentos del trabajo de auditoría, y cualquier otro documento relacionado, con el suficiente nivel de detalle para soportar las conclusiones alcanzadas en el informe de auditoría..."*.[18]

Pero antes de empezar a hablar del impacto sobre los sistemas y políticas de almacenamiento, definamos cuáles son esos documentos que se deben proteger y resguardar para el cumplimiento de la Ley, y qué debe ser considerado como documento. La SEC, define un lineamiento denominado *"Retention of Records Relevant to Audits and Reviews"*.[19]

Para que un documento sea seleccionado como candidato para ser retenido por los 7 años, debe cumplir básicamente 2 criterios:

- El documento debe ser creado, enviado o recibido en relación directa con la auditoría o revisión.
- Contiene conclusiones, opiniones, análisis o información financiera relacionada con la auditoría o revisión.

[18] Tomado del Acto SOX
[19] Tomado de http://www.sec.gov/rules/final/33-8180.htm

Estas dos afirmaciones implican un enorme trabajo tanto para las compañías como para las firmas de auditoría, algunos analistas incluso piensan que es casi imposible determinar que documentos están relacionados con los informes de auditoría presentados.

La ley SOX ha introducido además nuevas categorías de registros que deben ser retenidos y almacenados adecuadamente:

- **Registros de Sitios Web**. La sección 403 de la Ley SOX (y la regulación de la SEC relacionada) requiere que las compañías que tengan un portal corporativo, que pongan dentro de un tiempo especificado, un comunicado referente a ciertos cambios mayores en la propiedad de las acciones. [20] Por lo tanto, las compañías deberán estar en capacidad de retener y manejar adecuadamente la documentación relacionada con estos comunicados, incluyendo el comunicado en sí, su fecha de publicación, cuánto tiempo estuvo publicado, en que parte del portal web estuvo disponible, etc.
- **Reportes de Control Interno.** Los reportes de control interno requeridos por la Sección 404 y las certificaciones ejecutivas requeridas por la sección 302, son por sí mismos, registros y documentos que deben ser adecuadamente retenidos y administrados.[21] El procedimiento usado para generar esos reportes también produce en sí mismo una serie de información que las empresas deberían almacenar como registros y documentos, en pro de soportar las conclusiones contenidas en los reportes y certificaciones presentadas.
- **Quejas.** La sección 301 requiere al comité de auditoría de una compañía establecer "procedimientos para la recepción, retención y manejo de las quejas" recibidas de empleados respecto a posibles malos manejos contables o de auditoría. A los empleados se les debe respetar el derecho al anonimato, pero la ley es clara, los registros de esas quejas deben quedar almacenados.

[20] SEC Release 33-8230, Mayo 7 de 2003 - http://www.sec.gov/rules/final/33-8230.htm
[21] SEC Release 33-8328, Junio 5 de 2003 - http://www.sec.gov/rules/final/33-8238.htm

Adicionalmente se deben almacenar registros que muestren que el sistema ha sido implementado, y demostrar que el sistema si ha funcionado.

Teniendo bien claro cuáles son los documentos que se deben almacenar por esos 7 años, es ahora muy importante contar con una serie de políticas y tecnologías que permitan almacenarlos por dicho periodo. A continuación se presenta un concepto relativamente nuevo denominado ILM (Informaron Lifecycle Management), el cual, haciendo uso de una serie de tecnologías existentes, nos puede ser de gran ayuda para lograr los objetivos de cumplimiento de la ley SOX.

3.9 INFORMATION LIFECYCLE MANAGEMENT

Information Lifecycle Management (ILM), es una serie de políticas, procesos, practicas y herramientas tecnológicas usadas para balancear el cambiante valor de la información corporativa con la infraestructura de tecnología más apropiada y con costos razonables, desde el mismo momento en que la información es concebida (el momento en que la información es creada, cuando ingresa al sistema) hasta su fase final de destrucción o archivado permanente. La información es alineada con los requisitos del negocio a través de políticas de manejo y niveles de servicio asociados con las aplicaciones y la información. Básicamente ILM se basa en tomar decisiones sobre la información corporativa:

- Donde debe estar almacenada la información.
- Por cuánto tiempo debe estar almacenada en ese medio seleccionado.
- Cuando es preciso desechar o destruir la información.

El ciclo de vida de la información se compone principalmente de tres etapas, a saber:

1. Creación o adquisición: Hay dos formas mediante las cuales la información puede ser generada en una empresa: puede ser ingresada manualmente por usuarios, o puede ser adquirida externamente, como por ejemplo un correo electrónico, un documento en formato EDI, etc. En ésta etapa el valor de la información es muy alto, y su disponibilidad debe ser inmediata.
2. Publicación: Una vez que los documentos o registros han sido generados, pueden ser accedidos o modificados de forma constante. En este punto, el valor del documento puede ser también muy alto, aunque no sea tan primordial la disponibilidad inmediata.
3. Retención y Destrucción: Es importante definir por cuánto tiempo se debe almacenar un documento o registro, y definir, de acuerdo a las regulaciones legales, decidir cuándo debe ser destruido.

La siguiente gráfica (Tomada del articulo de HP "Information Lifecycle Management technical overview"[22]) muestra una relación muy interesante entre la cantidad de información y la probabilidad de que ésta sea usada a lo largo del tiempo.

[22] http://whitepapers.zdnet.com/abstract.aspx?docid=86993

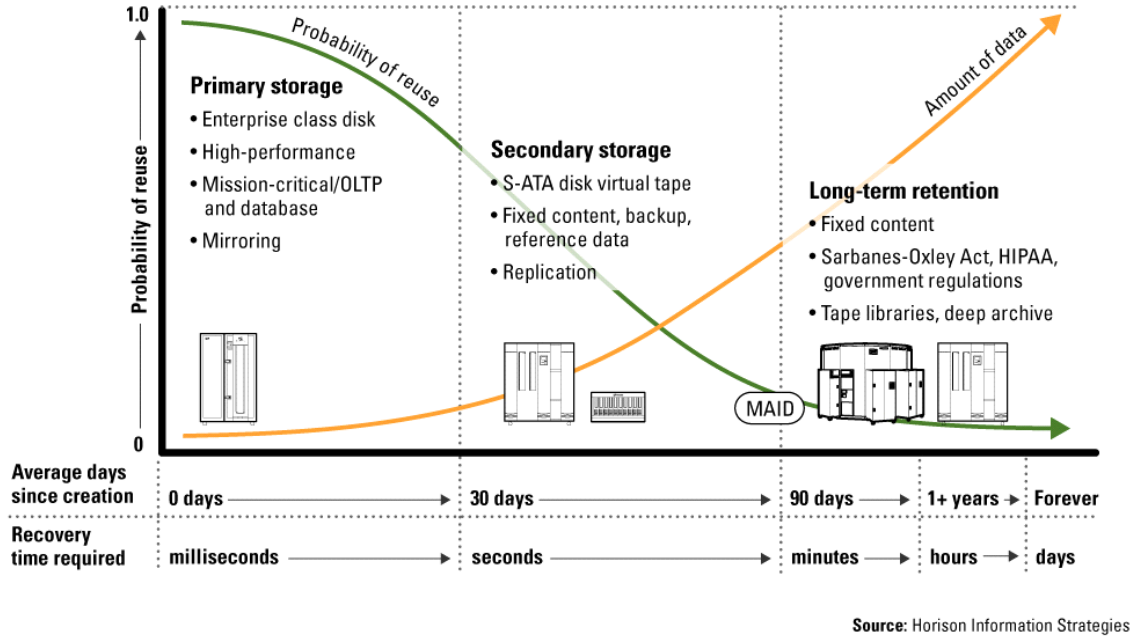

Ilustración 5. Ciclo de vida de la información

A medida que corre el tiempo, el uso de la información financiera se hace menos frecuente, por lo que ésta se hace menos valiosa. Esto es lo que se conoce como el ciclo de la vida de la información, que en el caso de aplicar la ley Sarbanes-Oxley, éste ciclo debería tener una duración de 7 años como mínimo, esto para garantizar que la información financiera y de auditoría esté disponible cuando pueda ser requerida por las autoridades gubernamentales (SEC, PCAOB, etc.).

Se aprecia un detalle importante en la gráfica: la información, a través del tiempo, es movida por los diferentes tipos de almacenamiento con los que cuente la compañía, empezando con los más rápidos y costosos, y terminando por los más económicos pero más lentos. Con esto, se reducen drásticamente los costos de almacenamiento, mientras garantizamos el cumplimiento de las regulaciones de la ley SOX.

Es acá donde la regulación de la ley SOX toma importancia. Habíamos hablado anteriormente que se debían tener mecanismos para seleccionar cuáles serían los documentos que se protegerían en modo *Archive*, para su almacenamiento a largo plazo. A continuación la decisión que se debe tomar es que tipo de almacenamiento usar. Obviamente que para tomar ésta decisión se deben tener en cuenta varios factores:

- Económico: Debemos pensar que tan importante es la información que queremos almacenar, éste será un criterio para determinar que tanto dinero invertir en los sistemas de almacenamiento: tendremos almacenamiento masivo y económico o poco almacenamiento costoso.
- Capacidad de Almacenamiento: Obviamente que si requerimos grandes capacidades de almacenamiento, lo mejor es adquirir almacenamiento de bajo costo como Librerías de Cintas.
- Disponibilidad Inmediata: Es necesario determinar que tan importante es para el negocio, disponer de esa información de forma "inmediata".

ILM puede ayudar a cumplir con las regulaciones de retención de información, a la vez que puede ayudar a reducir los costos

3.10 JERARQUÍA DE ALMACENAMIENTO

La explicación detallada que se hace de éste tema, es por su directa relación con ILM, y de su correcto entendimiento, depende que la implementación de ILM sea lo más beneficiosa posible en términos de costos y de cumplimiento. La jerarquía de almacenamiento es la forma en que se organizan los diversos dispositivos de almacenamiento que comúnmente son usados en sistemas informáticos. Ésta es comúnmente la organización que se hace:

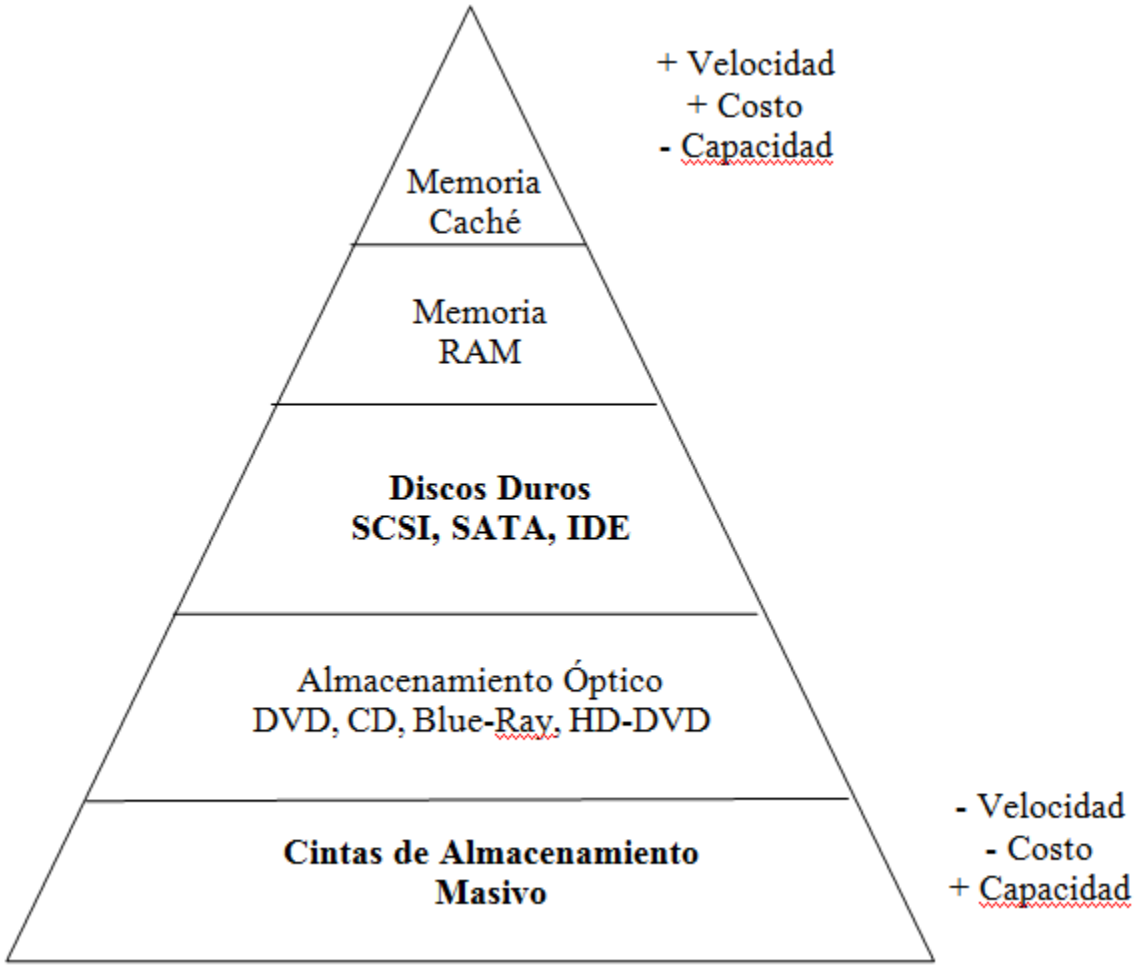

Ilustración 6. Jerarquía de almacenamiento

De ésta jerarquía podemos destacar los siguientes detalles:

- Cuando se desea tener una velocidad mayor de acceso, los costos aumentan y la capacidad de almacenamiento disminuyen.
- Cuando se desea tener gran capacidad de almacenamiento, es necesario sacrificar casi siempre la velocidad, a no ser que se quieran asumir costos exagerados.

A continuación se detallan los medios de almacenamiento más usados en las compañías de hoy en día, con sus respectivos costos (los costos corresponden a Mayo de 2008).

Tipo	Costo	Latencia	Velocidad de Transferencia
Discos SCSI	US$3,2 / GB	≈ 3 ms	Hasta 4 Gbps
Discos SATA	US$0,3 / GB	≈ 10 ms	Hasta 3 Gbps
Discos IDE	US$0,25 / GB	≈ 15 ms	Hasta 1 Gbps
Cintas	US$0.075 / GB	≈ 55 seg	Hasta 31 Mbps

3.11 COPIAS DE SEGURIDAD Y RECUPERACIÓN DE DESASTRES

Hasta ahora se han visto diversas metodologías para mantener la información por el tiempo correcto, en el medio de almacenamiento de correcto, para garantizar el cumplimiento de las regulaciones gubernamentales y minimizarle costos a la compañía. Pero ahora, ¿Cómo garantizar que esa información va a permanecer "intacta" por el tiempo necesario? Para ello vamos a hablar de algunas de las metodologías y herramientas de *Backup y Disaster Recovery* existentes.

Toda política de backup está principalmente enfocada en proteger la información ante cualquier probable incidente que la pueda alterar o destruir, entre éstos incidentes podemos nombrar:

- Virus ó troyano que afecte la máquina donde reside la información
- Factores ambientales perjudiciales
- Desastres naturales
- Daños físicos en los medios de almacenamiento
- Borrado / alterado de la información de forma accidental o intencional.

- Penetración en los sistemas de la compañía tendientes a destruir / alterar la información. (no cabe en la anterior)

A continuación se esboza una de las arquitecturas o configuraciones de backup más sencillas, pero a la vez más usadas, unos clientes, un servidor de backup, y unos repositorios de almacenamiento (librerías de cintas, SANs, etc.).

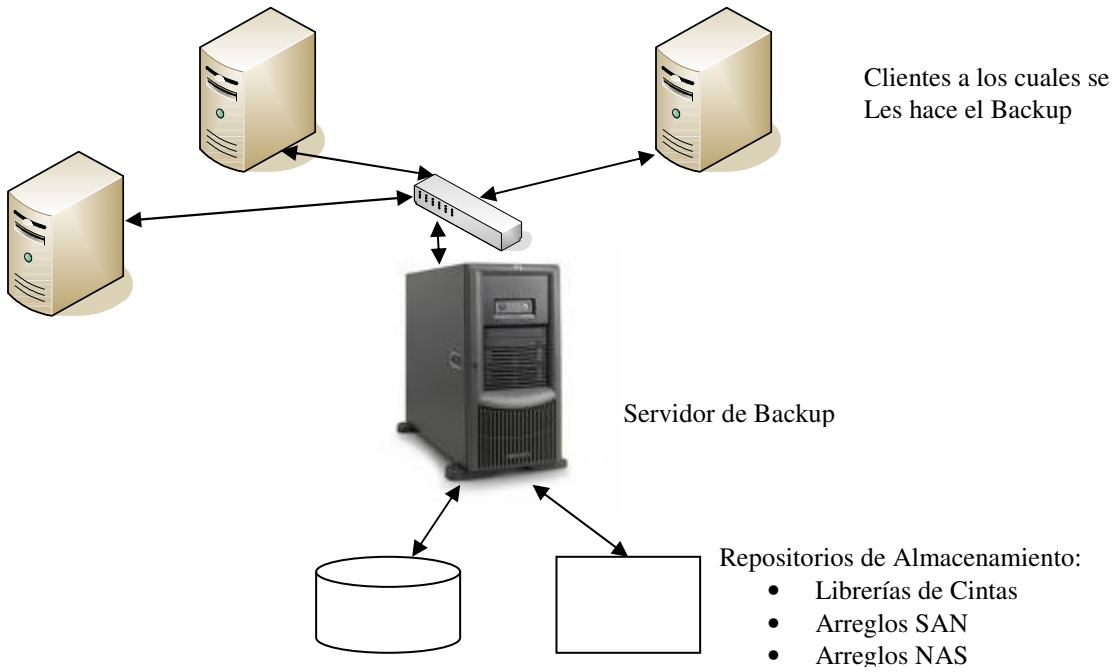

Ilustración 7: Una arquitectura simple para un sistema de Backup

El sistema de backup debe estar acompañado obviamente de unas buenas políticas y procedimientos que garanticen el nivel mínimo de riesgo de que haya pérdida de información, y que además se estén invirtiendo adecuadamente los recursos de backup en la información que realmente es necesaria. Por ejemplo, si se cuenta con una política para realizar un backup diario de la carpeta personal de cada usuario, y hay usuarios que están almacenando música y videos en dicha carpeta, ahí se estarían malogrando dichos recursos.

Ahora, un punto importante de los sistemas de Backup, tiene que ver con el punto anteriormente tratado (Information Lifecycle Management), es decir, ¿Por cuánto tiempo dejar almacenado el backup? , y lo más importante, ¿En que tipo de medio?. Porque para los sistemas de backup también existe lo que algunos proveedores de tecnología de backup (IBM, CA, etc.) conocen como Storage Pool Hierearchy[23], que hace que la información se vaya desplazando por distintos medios de almacenamiento, de acuerdo a políticas establecidas que van alineadas con las necesidades del negocio. Algunos de estos criterios para desplazar la información son:

- Antigüedad de la información en uno de los niveles de la jerarquía.
- Tipo de información siendo almacenada.
- La información ha perdido o ha disminuido su valor.
- Regulaciones legales o corporativas especiales.

Una buena política de backup debería ser elaborada teniendo en cuenta los siguientes ítems. Cada ítem se debe desarrollar de forma concienzuda teniendo en cuenta las necesidades reales del negocio y los riesgos que corre la información.

- Esbozo. Listado de servidores e información que va a ser respaldada. Este listado debe tener detalles técnicos del servidor, su rol en la compañía, y un listado de toda la información que se va a respaldar.
- Propósito. Aunque parezca un poco ridículo tener definido el propósito del backup, lo mejor para curarse en salud, es que se defina de forma clara cuál es el alcance y el propósito de tener implementada una política de respaldo en la compañía.
- Definiciones. Tenga en cuenta que este documento será leído por ejecutivos de la compañía y por otros empleados que muy posiblemente no tengan el mismo conocimiento técnico que usted tiene. Simples términos como *backup,*

[23] Término acuñado por el software IBM® Tivoli Storage Manager

archive, incremental, , que parecen sencillos, podrían terminar confundiendo a quien está analizando la política.

- Frecuencia. Defina claramente un "calendario de backup", donde se indique de forma precisa cuando se realizan los backups incrementales, cuando los backup full, o si cada día de la semana va a respaldar un grupo de servidores distinto, etc.
- Rotación de medios. Es importante tener claridad del procedimiento que se va a utilizar para rotar las cintas magnéticas: cuando salen de la empresa, cuánto tiempo permanecen por fuera, al cuanto tiempo son reemplazadas por una nueva, etc.
- Pruebas de restauración. Para que un sistema de backup sea efectivo, debe estar acompañado por pruebas periódicas que garanticen que los respaldos se están haciendo adecuadamente. Asegúrese de llevar una bitácora de las pruebas que realiza.
- Información. Se debe hacer hincapié en tener claro que es lo que exactamente se va a respaldar en los servidores y/o estaciones de trabajo. ¿Se va a respaldar solamente la información?, ¿Se van a realizar imágenes completas de los servidores?. ¿Se desean mantener todos los privilegios y atributos de la información?.
- Archivado de la información. Este punto en especial se menciona casi de forma directa en las secciones 103 y 802, las cuales mencionan que toda la documentación e información relacionada con las auditorías debe ser almacenada por 7 años. El archivado es un método de respaldo a largo plazo que garantiza que la información prevalezca durante largos periodos de tiempo, principalmente usando cintas y discos ópticos.
- Restauración de archivos. Describa como se va a realizar el proceso de respaldo de la información. ¿El usuario debe llenar un formulario?, ¿Existen mecanismos para que el usuario lo haga por su propia cuenta?
- Encriptación. Dependiendo de la sensibilidad de la información que está siendo respaldada, especialmente para los backups que están siendo almacenados off-site, se debería contar con un mecanismo de encriptación

para asegurar que el contenido de los backups no va a caer en manos equivocadas.

Ahora que se tienen unas nociones de lo que es una política de backup, deberíamos saber que ésta debe ir acompañada de una buena política de Recuperación de Desastres.

Aunque son eventos muy poco probables, los terremotos, los incendios, las inundaciones, las tormentas, y en general cualquier desastre natural o incidente (como un robo, un incendio, apagón de energía), deben ser tomados muy en serios como posibles causantes de la destrucción parcial o total de los sistemas de cómputo, y por ende de toda la información de la compañía.

Un Plan de Recuperación de Desastres, es una guía detallada que indica los procedimientos adecuados que se deben seguir para que, desde el punto de vista tecnológico, el negocio tenga continuidad con la mayor prontitud posible, ya sea en el mismo lugar del desastre, o preferiblemente en una sede alterna.

Un buen plan de Recuperación de Desastres se debería elaborar siguiendo los siguientes pasos:

1. Evaluar todos los posibles riesgos que puedan afectar la funcionalidad normal de los sistemas de cómputo. Entre éstos se pueden enumerar desastres naturales, cortes de energía, ataques terroristas, asaltos, errores humanos, incendios, etc. Asignarle a cada uno de éstos riesgos una probabilidad de ocurrencia asociada y un impacto en la continuidad del negocio.
2. Tratar de minimizar tanto como sea posible o incluso eliminar, aquellos riesgos que se pueden considerar “evitables”, como por ejemplo: los cortes de energía se pueden evitar adquiriendo sistemas UPS, la pérdida de información se puede evitar tendiendo backups off-site.

3. Para aquellos riesgos que no se pueden evitar (como por ejemplo un terremoto o un daño en los discos del servidor principal del ERP), se deben elaborar planes de contingencia en los que se conjugan tecnologías y metodologías.

Con la información que se ha presentado hasta el momento, es decir, las diversas metodologías y tecnologías disponibles para el salvaguardo de la información, hemos entendido como impacta el manejo y almacenamiento de los datos la Ley Sarbanes-Oxley. Más allá de tener todas estas políticas de respaldo y archivado de la información solamente para cumplir los requerimientos de archivado de los registros de auditoría, debemos pensar que con su correcta implementación estaremos además logrando otro de los propósitos importantes de la Ley SOX: lograr que la información financiera de la compañía, base de los reportes financieros, permanezca disponible e inalterada en todo momento.

6. COSO Y COBIT COMO MARCOS PARA LA APLICACION SOX

6.1 COSO

COSO (Committee of Sponsoring Organizations of the Treadway Commission) es una iniciativa del sector privado en los Estados Unidos, fundada en el año de 1985 con el propósito de brindar una serie de recomendaciones a las compañías, en pro de disminuir el fraude en los reportes y estados financieros. A pesar de que COSO es una iniciativa del sector privado, ha ganado mucho apoyo y reconocimiento por parte del sector oficial, especialmente de la SEC (Securities and Exchange Comission), ente encargado de regular y vigilar los mercados bursátiles en los Estados Unidos de América.

En el año de 1992, COSO publicó el documento "Internal Control, Integrated Framework", con el objetivo de brindar un marco de trabajo con el cual las compañías podrían implementar, evaluar o mejorar sus sistemas y metodologías de control interno. Éste documento tenía recomendaciones para que las compañías adoptaran un marco dentro del cual todas las transacciones son propiamente autorizadas y verificadas, hay controles contra el uso inapropiado de los sistemas, y todas las transacciones son registradas y almacenadas de forma apropiada.

La misma SEC asegura en un comunicado de prensa emitido en su sitio web:
"La comisión ha avalado por mucho tiempo el equipo de trabajo de COSO, dado que estos trabajan para proveer una completa guía para el Marco de Trabajo Integrado de Control Interno de COSO para direccionar las necesidades de las pequeñas y medianas empresas. La comisión espera que esta futura guía ayudara a las compañías de todos

los tamaños a un mejor entendimiento y aplicación del marco de trabajo, así como la relación de este último sobre el control interno de los reportes financieros. En tanto que la SEC desarrolla una guía para los administradores acerca de cómo evaluar sus controles internos sobre los reportes financieros, consideraremos el valor que pueda tener la guía adicional que COSO provea sea útil para las pequeñas compañías en completar sus evaluaciones de la Sección 404". [24]

Con este comunicado de prensa emitido por la SEC, vemos evidenciado el respaldo que la comisión brinda al marco de trabajo elaborado por COSO y a su esfuerzo por brindar una guía para que las compañías hagan lo mejor en cumplir los lineamientos de la Ley SOX en sus secciones 302 y 404.

En el entorno actual, los procesos de elaboración de reportes financieros son guiados por sistemas de TI. Dichos sistemas, bien sea un ERP o cualquier otro, están profundamente relacionados con la iniciación, autorización, almacenamiento, procesamiento y reporte de las transacciones financieras. Como tal, éstos están intrínsecamente relacionados al proceso de reportes financieros en general y por ello necesitan ser evaluados, con otros procesos importantes, con el fin de dar cumplimiento a la Ley SOX.

Se ha escrito mucho acerca de la importancia de la Ley Sarbanes-Oxley y los controles internos en general, sin embargo, existe poco sobre el importante papel que la tecnología de la información desempeña en este ámbito. Por ejemplo, la Ley Sarbanes-Oxley exige que las organizaciones seleccionen y apliquen un adecuado modelo de control interno. COSO se ha convertido en el más comúnmente utilizado marco por parte de las empresas que busquen cumplir la ley Sarbanes-Oxley, sin embargo, COSO no proporciona una gran cantidad de orientación para ayudar a las compañías en el diseño y la aplicación de controles de TI.

Por ello es que las organizaciones necesitan orientación para hacer frente a los

[24] Tomado de el comunicado de prensa de la SEC, http://www.sec.gov/news/press/2006/2006-75.htm

componentes de TI, dado que éstos se relacionan directamente con el proceso de cumplimiento en la presentación de reportes financieros.

Para los esfuerzos de cumplimiento con la Ley Sarbanes-Oxley, es importante demostrar como los controles de TI soportan al marco COSO. Una organización debería tener competencia en los controles de TI en todos los 5 componentes que COSO identifica como esencia para el control interno, estos son:

- Ambiente de Control
- Evaluación de Riesgos
- Actividades de Control
- Información y comunicación
- Monitoreo

A continuación se hará una breve descripción de cada uno de los componentes y unas consideraciones de TI relacionadas con el componente de COSO

6.1.1 Ambiente de Control. El ambiente de control crea las bases para un control interno efectivo, afecta la cultura organizacional y representa el esqueleto de la estructura organizacional. Cualquier cosa que afecte el ambiente de control, afecta toda la organización.

De todas formas, las Tecnologías de la Información casi siempre tienen características que podrían requerir énfasis adicional en la alineación con el negocio, roles y responsabilidades, políticas y procedimientos, y competencia técnica. La siguiente lista describe algunas consideraciones relacionadas con el ambiente de control y TI.

- TI es comúnmente considerado comúnmente como una unidad organizacional separada del negocio y por ende un ambiente de control separado.

- TI es algo complejo, no por sus componentes técnicos pero si por la forma en que esos componentes se relacionan e integran en el sistema de control interno de la organización.
- TI puede introducir riesgos adicionales o aumentados que requieren de una serie se actividades de control para mitigarlos satisfactoriamente,
- TI requiere habilidades y conocimientos especializados que no podrían estar disponibles,
- TI podría requerir el relegar en ciertos terceros los controles, donde algunos procesos significativos de TI sean mercerizados.
- La responsabilidad de los controles de TI no podría ser muy clara, especialmente los controles de aplicaciones.

6.1.2 Evaluación de Controles. La evaluación de riesgos es un proceso que involucra a la administración en la identificación y el análisis de los riesgos relevantes en pro de alcanzar objetivos predeterminados, lo que forma la base para determinar las actividades de control. Hay cierta tendencia a que los riesgos de control interno sean más dominantes en el área de TI que en otras áreas de la organización.

La evaluación de riesgos puede ocurrir a nivel de entidad (para toda la organización) o a nivel de actividad (para un proceso específico o unidad de negocio).

A nivel de entidad, se puede esperar lo siguiente;

- Un subcomité de planeación de TI, perteneciente al comité de direccionamiento de Sarbanes-Oxley de la compañía. Entre sus responsabilidades están las siguiente;
    - Vigilancia del desarrollo del plan estratégico de control interno de TI, su efectiva y rápida implementación/ejecución y su integración con el plan general de cumplimiento de la ley Sarbanes-Oxley.
    - Evaluación de los riesgos de TI, por ejemplo, administración de TI, seguridad de la información, desarrollo y cambio de las aplicaciones.

A nivel de actividades, se puede esperar lo siguiente:

- Las evaluaciones formales de riesgos son hechas a través de la metodología de desarrollo de sistemas.
- La evaluación de riesgos esta incrustada en la operación de la infraestructura y en el proceso de cambio.
- La evaluación de riesgos está incrustada en el proceso de cambios de las aplicaciones.

6.1.3 Actividades de Control. Las actividades de control son las políticas, procedimientos y prácticas que son implementadas de manera que los objetivos de negocio sean alcanzados y las estrategias de mitigación de riesgo sean llevadas a cabo.

Sin contar con sistemas de información confiables y actividades de control de TI confiables, las compañías públicas no estarían en capacidad de generar reportes financieros confiables, COSO reconoce esta relación e identifica 2 grandes grupos de actividades de control de los sistemas de información: controles generales y controles de aplicación.

Los controles generales, que están diseñados para que la información generada por los sistemas de información de la compañía, sea confiable, incluyen los siguientes controles:

- Controles de operación del centro de cómputo, tales como programación y ejecución de tareas, acciones de operador, y procedimientos de respaldo y recuperación.
- Controles de software de sistema, que se aplican sobre la adquisición, implementación y mantenimiento de software de sistema, bases de datos, software de telecomunicaciones, aplicativos de seguridad y utilidades.

- Controles de seguridad de acceso, los cuales previenen el uso no autorizado o inapropiado del sistema, incluyendo el nivel de sistema operativo, bases de datos y aplicación.
- Controles sobre el mantenimiento y desarrollo de las aplicaciones, dichos controles que se implementan en la metodología de desarrollo, incluyendo el diseño y la implementación de las aplicaciones.

Los controles de aplicaciones están embebidos dentro de las aplicaciones con el fin de prevenir o detectar transacciones no autorizadas. Cuando se configuran de forma apropiada, o son usados en combinación con otros controles manuales, los controles de aplicación soportan la completitud, precisión, autorización y existencia de las transacciones siendo procesadas.

Los controles generales son necesarios para soportar el funcionamiento de los controles a nivel de aplicación, y ambos son necesarios para soportar un procesamiento íntegro de la información y la integridad de la información resultante usada para generar reportes. A medida que los controles de aplicaciones automatizados están reemplazando cada vez más los controles manuales, los controles generales cada vez toman más importancia.

6.1.4 Información y comunicación. COSO establece que la información es requerida en todos los niveles de la organización para dar marcha al negocio y alcanzar los objetivos de control de la entidad[25]. De todas formas, la identificación, gestión y comunicación de la información relevante representa un reto continuo para el departamento de TI. La decisión de cuál es la información requerida para alcanzar los objetivos de control, y la comunicación de ésta información de una forma y en un tiempo, que permita a las personas llevar a cabo sus actividades, en apoyo a los otro cuatro componentes de COSO.

[25] En este caso la palabra entidad se refiere a la empresa o compañía como un todo.

El departamento de TI procesa en su gran mayoría información financiera. De todas formas su alcance es casi siempre mucho más amplio. El departamento de TI puede también asistir en la implementación de mecanismos para identificar y comunicar eventos significativos, como sistemas de correo electrónico o sistemas para apoyar la toma decisiones.

COSO también resalta que la calidad de la información consiste en determinar si la información es:

- Apropiada: ¿Es la información correcta?
- Oportuna: ¿Está disponible cuando se le requiere? ¿Es reportada a tiempo?
- Actualizada: ¿Es la última información disponible?
- Precisa: ¿La información es correcta?
- Accesible: ¿La información puede ser accedida en el momento que sea necesario por quienes estén autorizados?

A nivel de la entidad, se puede esperar lo siguiente:

- Desarrollo y comunicación de políticas corporativas.
- Desarrollo y comunicación de los requisitos de información, incluyendo plazos, reconciliaciones, y el formato y contenido de los reportes de administración mensuales, cuatrimestrales y anuales.
- Consolidación y comunicación de la información financiera.

A nivel de actividades, se puede esperar:

- Desarrollo y comunicación de estándares para alcanzar los objetivos de las políticas corporativas.
- Identificación y comunicación oportuna de la información en pro de alcanzar los objetivos de negocio.
- Identificación y comunicación oportuna de las violaciones de seguridad.

6.1.5 Monitoreo. El monitoreo[26], que cubre la supervisión del control interno por la administración, mediante evaluaciones continuas hechas en periodos determinados de tiempo, se está volviendo altamente importante para la administración de TI. Existen dos clases de actividades de monitoreo: monitoreo continuo y evaluaciones separadas.

Cada vez más, la efectividad y el desempeño de TI están siendo continuamente monitoreados usando mediciones de rendimiento que indican si un control interno está operando de forma efectiva, como fue diseñado. Considere los siguientes ejemplos:

- Detección y gestión de fallos. Establecer métricas y analizar las tendencias de los resultados actuales contra esas métricas puede proveer una base para comprender las razones subyacentes en las fallas del procesamiento. Corrigiendo esas causas, se puede mejorar el desempeño, precisión y disponibilidad del sistema.
- Monitoreo de la seguridad. Se debe contar con una infraestructura de seguridad efectiva de forma que se reduzca el riesgo de un acceso no autorizado. Mejorando la seguridad, se puede reducir el riesgo de procesar una transacción no autorizada y por ende generar reportes no autorizados, y debería repercutir en la disponibilidad de los sistemas, si algunos componentes son comprometidos.

A nivel de la entidad, se puede esperar lo siguiente:

- Monitoreo continuo y centralizado de las operaciones de cómputo.
- Monitoreo centralizado de la seguridad.
- Revisiones de auditoría internas en TI

[26] Aunque la palabra monitoreo no es castiza, la traducción de la palabra m*onitoring*, vigilancia, no suena bien en el contexto de tecnología y auditoría.

A nivel de actividades, puede esperarse lo siguiente:

- Identificación y gestión de fallos.
- Monitoreo local de la seguridad y de las operaciones de cómputo.
- Supervisión de personal de TI.

6.2 COBIT (Control Objectives for Information and Related Technology)

COBIT es un conjunto de buenas prácticas o marco de trabajo aplicable en el campo de las tecnologías de la información (TI). COBIT fue creado en el año de 1992, por ISACA (Information Systems Audit and Control Association) y el ITGI (IT Governance Institute), pero fue lanzado en el año de 1996. Su objetivo es el de ser una guía autoritativa, aceptada internacionalmente, como un conjunto de objetivos de control para el uso del día a día en el ámbito de las TI. Está pensado para ser usado por gerentes y auditores, pero el usuario final se ve muy beneficiado, ya que mediante su uso, puede realmente entender sus sistemas de TI, y definir estándares de seguridad y control para dichos sistemas.

Como se ha visto a lo largo de éste trabajo, la ley Sarbanes-Oxley impactará de una manera muy significativa los sistemas de TI en la empresa. A pesar de que en la sección 404 de ésta ley no se haga mención alguna de TI, ni de que controles de TI deben ser establecidos, es claro que las compañías deben implementar un mecanismo de control para los sistemas de TI.

Existen varios estándares que nos pueden ayudar a definir y documentar los controles internos, entre ellos ITIL[27] (IT Infraestructura Library), Six Sigma y COBIT –estándar de facto para adoptar SOX en el área de TI-.

[27] ITIL es un marco de trabajo para las tecnologías de la información, publicado por la Oficina de Comercio en el Reino Unido

COBIT, a pesar de que fue liberado en el año de 1996, se vino a dar de manera definitiva a partir de la emisión de la Ley Sarbanes-Oxley, ya que los auditores y personal de TI lo han seleccionado como su marco de trabajo preferido, dado que el estándar es independiente de la plataforma donde se esté implementando.

COBIT proporciona una aproximación metodológica a las funciones de TI para la implementación y el soporte de SOX. Sin embargo, la plataforma de desarrollo propuesta debe ser personalizada por las empresas diseñándolo a su propio tamaño y complejidad.

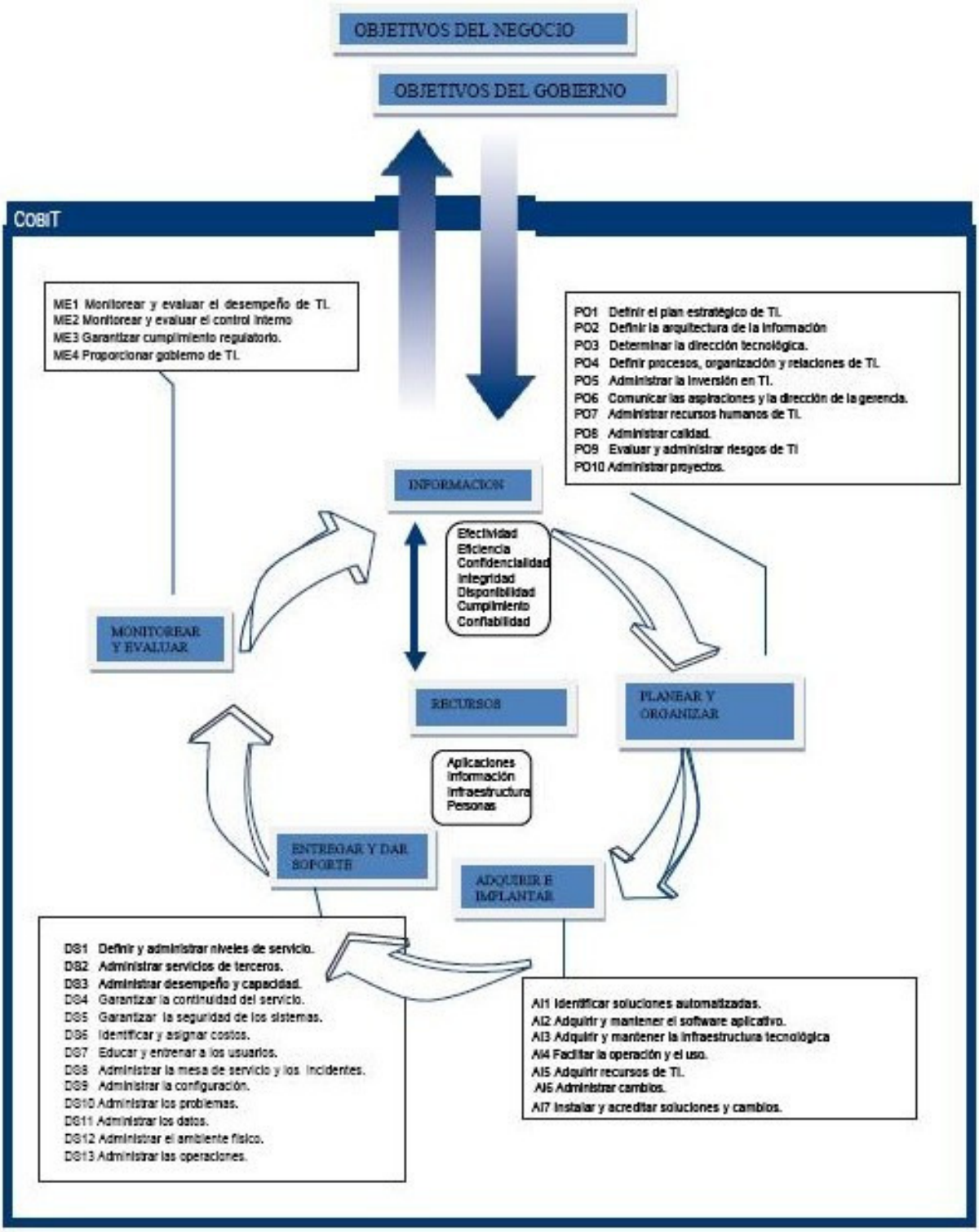

Ilustración 8. Marco de trabajo general de COBIT, tomado de ISACA

6.2.1 Componentes. COBIT está conformado por seis componentes:

1. Resumen Ejecutivo: Explica los principios y conceptos clave.
2. Plataforma: Fundamentación para aproximarse a los componentes de COBIT. Organiza el modelo del proceso en cuatro dominios:
    a. Planeación y organización.
    b. Adquisición e implementación.
    c. Entrega y soporte.
    d. Monitoreo y evaluación.
3. Objetivos de Control: Fundamentación para aproximarse a los elementos de COBIT. Organiza el proceso del modelo en los cuatro dominios.
4. Prácticas de Control: Identifica las mejores prácticas y describe los requisitos para los controles específicos.
5. Directrices Administrativas: Enlaza los negocios y los objetivos de TI y proporciona las herramientas para mejorar el desempeño de las TI.
6. Directrices de Auditoría: Proporciona orientación en como evaluar los controles, evaluar el cumplimiento, y documentar el riesgo con estas características:
    - Definición de controles internos para los reportes financieros.
    - Pruebas y evaluación de estos controles internos.
    - Soporte a las auditorías externas de control.
    - Documentación de los esfuerzos de cumplimiento.
    - Reporte de alguna deficiencia significativa o debilidad material.

COBIT es básicamente una aproximación al desafío de asegurarse que TI el record sistemático necesario para tener fuertes controles internos. COBIT es el más común y ampliamente aceptado conjunto de lineamientos de control de TI, sin embargo no es el único estándar, por ejemplo, la Organización Internacional de Estándares, que proporciona el bien conocido método para acreditar procesos de negocios: ISO 9001, también tiene el que es conocido como el Código de Prácticas para la Administración de la Seguridad de la Información (ISO/IEC 17799). Sin embargo, y sin estar COBIT validado por el PCAOB o cualquier otro cuerpo gubernamental, COBIT es el ganador de los estándares de COSO en lo que a TI se refiere.

COBIT es un estándar para el gobierno de TI, el cual está definido por ITGI e ISACA como la estructura que enlaza los procesos de TI, recursos de TI, e información de TI competente a las estrategias y objetivos de la compañía. El gobierno de TI integra e institucionaliza las mejores prácticas para planeación y organización. En síntesis, COBIT es una herramienta de gobierno de TI, la cual es consistente con COSO.

La ley SOX requiere que una compañía defina una plataforma de control y específicamente recomienda COSO como la plataforma para los controles generales de contabilidad. COBIT es la plataforma de control no oficial para los sistemas de TI que soportan los controles de COSO.

La premisa de COBIT es que el área de TI es la base fundamental de los controles que permiten una información financiera confiable. En esencia, COBIT define cinco áreas principales en las cuales TI tiene un papel fundamental, los cuales son:

6.2.2 Administración de la información y clasificación de datos. "Uno no puede manejar lo que no puede medir". Computadores, software, y toda el área de TI en general son herramientas de medida que se pueden usar para mantener el rastro de las transacciones en nuestros negocios. Contabilidad, ERP, y otro software, y los sistemas que los utilizan contienen datos vitales a cerca de las finanzas de la compañía. Para proporcionar la seguridad de que un sistema de TI tiene sus controles

internos reforzados, los administradores del sistema tienen que estar en capacidad de demostrar que esté maneja y clasifica los datos de acuerdo con estos controles específicos.

6.2.3 Administración de usuarios. Para tener una semblanza de control en TI que soporte del sistema de reporte financiero, se necesita saber quién está usando los sistemas en específicos, en qué momento, y para qué propósito. Y, se está seguro que los usuarios de los sistemas están autorizados para hacerlo, que puedan estar autenticados como los verdaderos usuarios que pretenden ser. También es de vital importancia que el sistema mantenga un registro de las acciones de cada usuario para una revisión posterior en un auditoría, si es que es necesario. Los sistemas de administración de usuarios, también conocidos como administradores de identidad hubo aplicaciones de administración de acceso, tiene la capacidad de asignar roles a usuarios individuales y como usuario, sus derechos de acceso y privilegios funcionales están dictados por el rol el cual se le fue asignado en el sistema de manejo de usuarios.

6.2.4 Reportes en tiempo real. Es bien conocido que los procesos de software, especialmente aquellos que ocurren entre más de un sistema en un ambiente distribuido son propensos a pausas, tiempos de espera baches en la transferencia de datos, y retardos causados por memoria. Sin embargo, en términos del control interno, un sistema bien configurado usualmente será capas de entregar información en una franja de tiempo adecuado para los reportes financieros.

6.2.5 Fallas en las transacciones y niveles de tolerancia. Los sistemas de TI que utilizan los controles de COSO deberían estar en la capacidad de monitorear transacciones y alertar a los administradores del sistema si ocurre una situación que requiere de investigación. Como muchos otros aspectos de los controles de TI, los mismos administrar del sistema tienen que estar controlando su propia plataforma, o

existe la posibilidad potencial de que se ignore la alerta, o sea ignorada o escondida de los auditores.

6.2.6 Validación e integridad del procesamiento de los datos. Sin una apropiada plataforma de control, el proceso de desarrollo, y el régimen de pruebas, es probable que para un sistema de contabilidad o una ERP, se han configuradas con errores o construidas con intentos fraudulentos en la funcionalidad programa.

6.3 DOMINIOS DE COBIT

La mejor manera de entender COBIT es empezando por los cuatro dominios primarios para el gobierno de TI, los cuales son: planeación y organización (PO), adquisición e implementación (AI), entrega y soporte (DS), monitoreo y evaluación (ME). Cada uno de estos dominios comprende varios procesos, cada proceso tiene un número el cual está precedido del dominio al cual corresponde. Por ejemplo si hablamos de AI6, nos estamos refiriendo a la administración de cambios, la cual pertenece al dominio de adquisición e implementación.

A su vez cada proceso, está compuesto de un variado conjunto de declaraciones de control, factores críticos de éxito, indicadores claves de desempeño, indicadores claves de meta, y modelos de madurez.

COBIT es en sí una plataforma de lineamientos sugeridos, no es necesariamente una lista de chequeo de actividades. Y es por esta razón, que cada compañía aplica COBIT a sus operaciones de TI seleccionando los procesos más relevantes y los indicadores claves de desempeño y medidas de control para cada uno de sus procesos.

ISACA tiene definido un resumen del cual tiene identificado los quince procesos más comunes de COBIT, los cuales se pueden observar en la siguiente tabla.

Tabla 2. Controles más comúnmente usados en COBIT (Encuesta de ISACA y ITGI)

OBJETIVOS DE CONTROL DE COBIT	DESCRIPCIÓN
PO1	Definir un plan estratégico de TI
PO3	Determinar la dirección de tecnología
PO5	Manejar las inversiones en TI
PO9	Evaluar los riesgos
PO10	Administración de proyectos
AI1	Identificación de soluciones
AI2	Adquisición y mantenimiento de aplicaciones de software
AI5	Instalación y acreditación de sistemas
AI6	Manejo de cambios
DS1	Definición de niveles de servicio
DS4	Aseguramiento del servicio continuo
DS5	Aseguramiento de la seguridad el sistema
DS10	Administración de problemas e incidentes
DS11	Manejo de datos
ME1	Monitoreo de los procesos

6.4 Relación de COBIT con Sarbanes-Oxley

El cumplimiento de SOX significativamente afecta la organización de TI de muchas de las compañías públicas. Sin embargo existe un enorme problema, y es que no existe una mención específica de TI en SOX404, y aún más importante, no se especifica cuáles son los controles que deben ser establecidos en la organización de TI para cumplir con la legislación de SOX.

Siendo así la situación, los administradores de TI se podrían preguntar cómo cumplir algo que no saben a ciencia cierta que es. Sin embargo existen varios estándares como se definen anteriormente, los cuales permiten garantizar ese cumplimiento.

Los quehaceres del cumplimiento de COBIT ayuda a la organización de TI a evaluar qué tan efectivos son los sistemas en lo que respecta a los controles internos. En adición a esto, COBIT proporciona un patrón definido de mejoramiento del nivel de la organización de TI adhiriéndose a sus controles. Ya que COBIT es un subconjunto de lineamientos de control interno del área de TI de COSO, siendo COSO la plataforma de control interno recomendada por la SEC para hacer cumplimiento de SOX, estamos en la capacidad afirmar que COBIT puede ser el estándar que mejor se aproxima a las necesidades de aseguramiento de la información y de control interno de las compañías que buscan dar cumplimiento a la ley SOX, dentro del área de TI. Y de hecho podemos encontrar dentro de cada uno de los objetivos de control de COBIT, que hay una serie de controles los cuales se encuentran relacionados con los objetivos de control de Sarbanes-Oxley.

Es crítico que el cumplimiento de SOX se ha visto como un proceso en curso en lugar de un evento de un solo momento. En los casos en que se requiera revisar, desarrollar, e implementar nuevos procedimientos y controles, sería vital que el éxito continuo de esos procedimientos y controles sea sostenible. En conclusión, es posible para una organización de TI, usar COBIT para lograr el cumplimiento de SOX. Sin embargo es importante recalcar que se debe personalizar y escalar los controles de COBIT para ajustarse de la mejor manera al ambiente organizacional de TI.

6.5 PLAN DE IMPLEMENTACIÓN DE COBIT

En esta sección se explorará el plan de implementación de COBIT[28] y sus nueve pasos que son generalmente requeridos para el cumplimiento de las TI a la luz de SOX. COBIT es un marco de trabajo que provee objetivos tanto a nivel de actividad como a nivel corporativo. Es posible realizar un mapeo directo de este marco con el marco de COSO y por eso muchos profesionales de TI confían en este marco para evaluar la efectividad de sus controles internos. A continuación mencionaremos las nueve fases necesarias y una breve explicación de cada una de ellas.

6.5.1 Fase 1: Planeación. Aunque parezca una de las fases más sencillas, realmente es una de las más complicadas. En esta fase, el entender como el proceso de reportes financieros trabaja es crítico; esto ayudara a entender e identificar los sistemas y componentes claves que necesitan ser evaluados. Cualquier sistema que cree, almacene o procese información financiera debe ser incluido en el alcance del proyecto. Por ejemplo: Sistemas de nomina, sistemas de facturación y sistemas de embarque.

Como un punto de inicio, realiza un inventario de los sistemas que contribuyen al proceso de reporte financiero, para ello tome por ejemplo una factura de venta y haga un proceso inverso para saber que sistemas alimentaron la información de dicha factura.

6.5.2 Fase 2: Evaluación de riesgos. Una vez identificado el conjunto de sistemas a ser evaluados, debemos realizar una evaluación de riesgo, para lo cual debe ser necesario identificar la probabilidad y el impacto de posibles eventos adversos. Para cada sistema debemos evaluar si la probabilidad de una falla es más que remota, y segundo, el impacto para la organización si un control falla. Estos son algunos ejemplos de controles que podrían impactar a la información financiera: impactar la

[28] Este plan fue tomado de el sitio www.watchit.com, Sarbanes-Oxley Compliance: Managing Technology Controls, Scott Green

integridad de la información, sobrepasar los privilegios de acceso a un sistema. Una vez se ha realizado la evaluación de riesgos, podemos priorizar los sistemas y las locaciones para la revisión. De esta forma se puede continuar a la fase de identificar cuentas y controles significativos.

6.5.3 Fase 3: Identificar Cuentas y Controles Significativos. Existen dos categorías de actividades de control para los sistemas de información reconocidas tanto por COSO como por COBIT:

- Existen controles que aplican a todos los sistemas de información y apoyan la operación continua y segura de toda la compañía.
- Los controles de aplicación, los cuales están diseñados para detectar y prevenir transacciones no autorizadas.

Los controles generales se relacionan principalmente al ambiente de control en general y a la evaluación de riesgos. Ellos establecen el tono para la efectividad de los otros controles. Aquellos que apoyan la calidad y la integridad de la información requerirán de evaluaciones, esto debido a que los auditores prestan especial atención a los controles generales dada su importancia en el sistema de control en general. Los auditores externos juzgaran esas medidas subjetivas tales como:

- Actitud de la alta gestión de TI.
- Integridad, valores éticos y competencia.
- Filosofía y estilo de administración.
- Delegación de autoridad y responsabilidad.
- Procedimientos y políticas de TI.
- La calidad y preparación de los empleados.

6.5.4 Fase 4: Documentar el Diseño de Control. El PCAOB fue establecido bajo la ley SOX para "Supervisar la auditoría de compañías que están sujetas a las leyes de la SEC"[29]. La mesa de auditoría ha indicado que la inadecuada documentación puede ser una deficiencia en los controles internos que podría elevar el nivel de debilidades materiales, incluso las compañías con más control no tienen sus estructuras de control documentadas.

Para muchos el preparar y evaluar la documentación será la actividad de cumplimiento más costosa en el proceso de implementar SOX. Muchas compañías han adquirido sistemas de documentación para cumplir esta tarea. La documentación puede presentarse de muchas formas, entre las cuales pueden estar:

- Manuales de políticas.
- Modelos de procesos.
- Diagramas de flujo.
- Descripción de roles.
- Documentos y formas.

La documentación existente debería ser actualizada, evaluada y discutida con los auditores externos, para que se puedan detectar deficiencias de forma temprana. En el ámbito de las transacciones, la documentación debe incluir como se inician las transacciones, como se almacenan, procesan, y reportan. Como mínimo esta documentación deberá contener:

- Una descripción de los procesos y subprocesos relacionados.
- Una descripción de los riesgos asociados, su probabilidad y el impacto posible.
- Una declaración de los objetivos de control diseñados para reducir el riesgo a un nivel aceptable.
- Una descripción de las actividades de control.

[29] Speech by SEC Chairman: Opening Statement on the PCAOB Budget at the Commission Open Meeting. http://www.sec.gov/news/speech/2006/spch120406cc.htm

- Una descripción de la aproximación seguida para probar la existencia y efectividad de las actividades de control.
- Conclusiones alcanzadas acerca de la efectividad de los controles, como resultado de las pruebas.

La documentación reflejará todos los procedimientos de procesamiento, así como el propietario del sistema o la información.

6.5.5 Fase 5: Evaluar el diseño de controles. En este punto de la implementación, los ejecutivos deben evaluar la capacidad del programa de control para reducir el riesgo de las operaciones de TI a niveles aceptables para la compañía. Es importante diferenciar entre los dos tipos de control que existen: Los preventivos y los de detección, los primeros son establecidos en la misma fuente del riesgo, mientras que los últimos solamente alertan cuando el problema surge.

Es importante resaltar que los controles automatizados son mucho más confiables que los controles manuales, y en este punto es donde las TI entran a jugar un papel bastante determinante en la implementación de SOX.

Se puede decir que se ha alcanzado un nivel de optimización en el proceso de control cuando hay controles automatizados en todos los procesos de la organización, y estos están debidamente documentados y son evaluados y monitoreados constantemente por personal altamente calificado de la compañía.

Para el caso de las compañías que no puedan disponer de controles automatizados, se debe diseñar un mecanismo de control que realice un seguimiento continuo de las transacciones.

6.5.6 Fase 6: Evaluando la efectividad operacional. Una vez que el diseño de los controles ha sido aprobado, la continua efectividad de los controles debe ser confirmada. Los recorridos o seguimientos a través de los flujos de los procesos

pueden ser una forma muy eficiente de determinar si los controles establecidos están realmente operando de la forma como fueron diseñados. Por ejemplo, realizar todo el seguimiento desde que un cliente hace un pedido hasta que este finalmente es despachado, pasando por el proceso de generar la factura y realizar el cobro respectivo.

Los auditores externos deberán probar los controles generales establecidos sobre TI, así que probar esos controles debe ser de la más alta prioridad. Los controles de las aplicaciones deben ser probados con menor frecuencia, pero aún así no se deben descuidar.

6.5.7 Fase 7: Determinando las Debilidades Materiales. Cuando el equipo de TI detecte una deficiencia en un control, se debe determinar si existe un control o controles que compensen esa deficiencia en pro de proteger la organización, si dichos controles existen se debe decidir si confiar en ellos o cortar el problema de raíz para implementar un control apropiado.

Si la deficiencia excluye la seguridad de que la información financiera es correcta, se debe tomar una acción correctiva con mucha prioridad.

6.5.8 Fase 8: Documentar los Resultados. Durante la fase de evaluación, los resultados de las pruebas deben ser documentados y finalmente consolidados en un reporte que será entregado a los consultores externos. De esta forma se puede demostrar la confiabilidad, calidad e integridad de los sistemas de información de la compañía.

6.5.9 Fase 9: Construyendo la sostenibilidad. La sostenibilidad puede ser alcanzada mediante la repetición continua de algunas de estas fases anteriormente mencionadas, especialmente las fases de pruebas y evaluaciones de la efectividad de los controles y de las operaciones en general.

7. MODELO DE MADUREZ DE LA LEY SARBANES-OXLEY RESPECTO A LAS TI

Todo proceso de implementación de la Ley Sarbanes-Oxley debe constar de una serie de etapas o pasos que deben ser ejecutados en pro de hacer que la compañía, especialmente las TI de la compañía, cumplan las regulaciones establecidas por la ley Sarbanes-Oxley.

La primera etapa en el proceso de implementar los requerimientos de la ley Sarbanes-Oxley en una compañía, es realizar un proceso de evaluación exhaustivo que permita determinar el estado de madurez de los controles implementados y de su efectividad.

La idea de esta evaluación es determinar el grado de madurez en el que se encuentran implementados los controles automáticos y manuales sobre las TI, o si es que éstos se encuentran implementados. En éste trabajo se desarrolla un modelo que le permite a la compañía, saber como se encuentra su área de TI respecto a lo que sería una compañía 100% "Sarbanes-Oxley Compliant". El hecho de que una compañía, y en general todas sus áreas, sea "Sarbanes-Oxley Compliant", depende en gran medida del nivel de madurez en el que se encuentren los controles de TI.

7.1 ESTADOS DE MADUREZ DE UN CONTROL

El estado de madurez o grado de madurez de un control, determina que tan bien está diseñado e implementado éste, y que tan bien cumple su fin.

A continuación se presenta un gráfico que explica de modo vago la relación entre la madurez de un control interno, y los beneficios que se alcanzan a medida que éste pasa por las 5 fases reales de madurez (la Fase 0 no se tiene en cuenta).

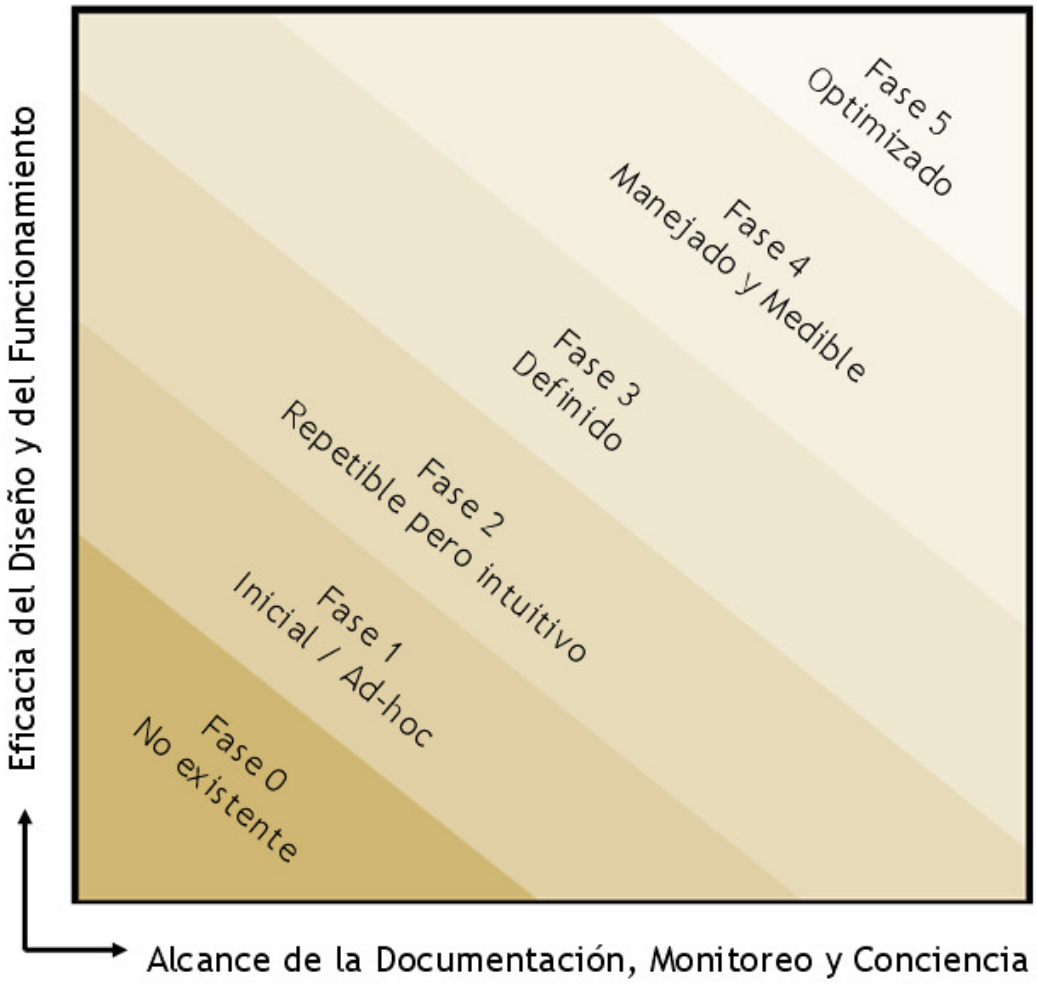

Ilustración 9. Fases de Madurez de un Control[30]

[30] Tomado del paper de ISACA "IT Controls for Sarbanes-Oxley"

Se puede decir que un control como tal empieza a existir desde la Fase 3, fase en la cual, la empresa ha reconocido como tal la necesidad de documentar formalmente la existencia del mismo, su finalidad, como funciona, quien es el encargado de monitorearlo, con qué frecuencia es vigilado, etc. En las Fases 1 y 2, es posible que el control se aplique de forma esporádica y manual, pero aún no está definido formalmente. Las fases 4 y 5 deben ser los estados o fases ideales para los controles. Se podría decir que un nivel de madurez avanzado es equivalente a la fase 4, mientras que un nivel óptimo de madurez, se podría equiparar con la fase 5. La gráfica es muy clara al evidenciar que a medida que aumenta el nivel de madurez de un control, aumentan la eficacia del control como tal, a la vez que se elabora más documentación y un mayor monitoreo.

En la siguiente tabla, se detalla cada una de las fases o estados de madurez por las que pasan los controles en una compañía. Además, en cada fase, se muestran las implicaciones para la ley SOX.

Tabla 3. Fases de los Controles [31]

	Fase 0 No existente	Fase 1 Inicial/Ad-hoc	Fase 2 Repetible pero intuitivo	Fase 3 Definido	Fase 0 Manejable y Medible	Fase 0 Optimizado
Características	En este nivel, hay una carencia total de cualquier proceso de control reconocible o la existencia de cualquiera de los procedimientos relacionados. La organización ni siquiera ha reconocido que hay una cuestión que debe abordarse, por lo tanto, no la comunicación sobre el tema se genera.	Hay una cierta evidencia que la organización reconoce que los controles y los procedimientos relacionados son importantes y necesitan ser tratados. Sin embargo, los controles y las políticas y los procedimientos relacionados no están en implementados y documentados. No existe un proceso para el manejo de eventos y revelaciones. Los empleados no son conscientes de su responsabilidad en las actividades de control. La eficacia del funcionamiento de las actividades del control no se evalúa de forma regular. Las deficiencias en el control no se identifican.	Los controles y las políticas y procedimientos existen, pero no siempre plenamente documentadas. Un proceso de manejo eventos y divulgaciones, pero no esta documentado. Los empleados pueden no ser conscientes de su responsabilidad con las actividades de control. La eficacia de funcionamiento de las actividades de control no está adecuadamente evaluada en una forma regular y el proceso no está documentado. Las deficiencias de control pueden ser identificadas, pero no se corrigen de manera oportuna.	Los controles y las políticas y procedimientos relacionados están implementados y debidamente documentados. Un proceso de manejo de eventos y divulgación está en implementado y debidamente documentado. Los empleados son conscientes de su responsabilidad con las actividades de control. La eficacia de funcionamiento de las actividades de control se evalúa en forma periódica (por ejemplo, trimestral), sin embargo, el proceso no está plenamente documentado. Las deficiencias de control son identificadas y solucionadas de manera oportuna.	Los controles y las políticas y procedimientos relacionados están implementados y debidamente documentados, y los empleados son conscientes de su responsabilidad con las actividades de control. Un proceso de manejo eventos y divulgaciones se encuentra implementado y está debidamente documentado y vigilado, pero no siempre es reevaluado a fin de reflejar cambios importantes en los procesos o la organización. La eficacia del funcionamiento de las actividades de control se evalúa en forma periódica (por ejemplo, semanal), y el proceso está adecuadamente documentado. El uso -principalmente táctico- de la tecnología, es para documentar los procesos, objetivos de control y actividades.	La Etapa 5 reúne todas las características de la etapa 4. Existe un programa de control y gestión de riesgos corporativo, de tal forma que los controles y procedimientos están bien documentados y son continuamente reevaluados con el fin de que reflejen los principales cambios en los procesos o la organización. Un proceso de auto-evaluación se utiliza para evaluar el diseño y la eficacia de los controles. La tecnología está siendo aprovechada al máximo para documentar los procesos, objetivos de control y actividades; determinar las debilidades, y evaluar la eficacia de los controles.

[31] Tomado del paper de ISACA "IT Controls for Sarbanes-Oxley"

Implicaciones para la Ley Sarbanes-Oxley	La organización está en total incapacidad para estar en cumplimiento incluso en el nivel mínimo.	Hay muy pocos controles, políticas, procedimientos y documentación para apoyar la toma de decisiones de la gerencia. El nivel de esfuerzo para documentar, probar y remediar los controles es muy alto.	A pesar de que los controles, políticas y procedimientos están implementados, existe insuficiente documentación para apoyar la certificación y afirmaciones de la gerencia. El nivel de esfuerzo para documentar, probar y poner remedio a los controles es muy alto.	Existe documentación suficiente para apoyar las afirmaciones y certificación de la gerencia. El nivel de esfuerzo para documentar, probar y poner remedio a los controles puede ser relevante, dependiendo de las circunstancias de la organización.	Existe documentación suficiente para apoyar las afirmaciones y la certificación de la gerencia. El nivel de esfuerzo para documentar, probar y poner remedio a los controles puede ser menos importante, en función de las circunstancias de la organización.	Permanecen las implicaciones de la etapa 4. Una gran mejora en la toma de decisiones, porque se dispone de información oportuna y de alta calidad. Los recursos internos se utilizan de manera eficaz y eficiente. La información es oportuna y fiable.

7.2 ELABORACIÓN DEL MODELO DE MADUREZ

Con todo el conocimiento recolectado a lo largo de la elaboración de éste trabajo, se logra elaborar un modelo que, como se explico al inicio del capítulo, logra determinar el estado de madurez que posee el área de TI de una compañía, respecto al cumplimiento de la ley Sarbanes-Oxley.

El modelo es elaborado basándonos en el documento "IT Control Objectives for Sarbanes-Oxley", obviamente realizando algunos ajustes y cambios, para adaptarlo a la percepción propia que se tiene de la relación entre la ley SOX y TI.

En el modelo, básicamente se agrupan o relacionan algunos controles de COBIT, en áreas o grupos de controles propiamente de Sarbanes-Oxley. Existen 14 áreas definidas, las cuales son evaluadas contra la realidad de la compañía, las áreas son:

1. Adquisición y Mantenimiento del Software de aplicaciones (AI2)
2. Adquisición y Mantenimiento de la Infraestructura de Tecnología (AI3)
3. Habilitación de Operaciones (PO6, PO8, AI6, DS13)
4. Instalar y Acreditar Soluciones y Cambios (AI7)
5. Administración de Cambios (AI6,AI7)
6. Definición y Administración de los niveles de Servicio (DS1)
7. Gestión de Servicios Tercereados(DS2)
8. Garantizar la Seguridad de los Sistemas(DS5)
9. Gestión de la configuración(DS9)
10. Gestión de Problemas e Incidentes (DS8, DS10)
11. Gestión de la Información (DS11)

12. Gestión de Operaciones (DS13)
13. Computación de Usuario Final

Cada una de esas áreas tiene definida una serie de preguntas, que indagan por controles específicos de TI, el encuestado, simplemente debe seleccionar en cuál de los siguientes estados de madurez se encuentra el control por el cual está siendo indagado:

- **0 - no existente** cuando
  No existe prevención sobre la importancia de ese aspecto.
- **1 - Inicial / Ad hoc** cuando
  La administración reconoce la necesidad ese aspecto.
- **2 - Repetible pero intuitiva** cuando
  Se cuenta con procesos similares que son seguidos de manera empírica.
- **3 - Definido** cuando
  Se reconoce la importancia del aspecto, este entendido y aceptado y. Existen procedimientos relacionados, herramientas y técnicas, no muy sofisticadas, y se han estandarizado y documentado como parte de actividades informales de entrenamiento. Se ha desarrollado un plan formal de entrenamiento, pero los modelos formalizados están basados aún en iniciativas individuales.
- **4 Manejado y Medible** cuando
  El desarrollo y refuerzo de este aspecto está completamente he soportado por métodos formales y técnicas. Se cuenta con herramientas a automatizadas pero aún no han sido integradas totalmente. Se han identificado métricas básicas y sistemas de medida. Un repositorio automatizado estar completamente implementado. Existen modelos complejos de datos que están siendo implementados para apalancar el contenido de la información en las bases de datos. Se cuenta con sistemas

de información ejecutivos y sistemas de soporte de secciones que están apalancando la información disponible.

- **5 - Optimizado** cuando
  Se cuenta con un refuerzo consistente en todos los niveles. Se cuenta con buenas prácticas empresariales en el desarrollo y mantenimiento de todos sus aspectos, incluyendo un continuo proceso de mejora. Se tienen estrategias de apalancamiento de la información a través de almacenes de datos y tecnología medida de datos definidos.

Éstos se le deben explicar al encuestado, por ejemplo, presentándole la Tabla 3.

Cada uno de los controles tiene una ponderación, es decir, un valor o importancia que se le da al control, dentro del proceso global de cumplimiento de la Ley SOX. La ponderación toma 3 valores: 10 para los controles de seguridad y en general para los controles más sensibles respecto a potenciales cambios en la información financiera; 8 para los controles relevantes y 6 para los controles medianamente relevantes en el proceso de cumplimiento de SOX. Cabe aclarar que en el proceso de ponderar los controles, puede haber percepciones subjetivas acerca de la importancia de cierto control. Esto debería ser adaptado de acuerdo al ambiente de TI de cada compañía.

Finalmente, con el valor de la ponderación del control, y la respuesta dada por el encuestado (el nivel de madurez), se calcula la Puntuación del control, que es equivalente a:

Puntuación = Valor de Cumplimiento * Ponderación

Donde: Valor de Cumplimiento = {0, 1, 2, 3, 4, 5}
y Ponderación = {6, 8, 10}

A continuación se anexa una “pantallazo" de la encuesta que es elaborada en la compañía que está siendo analizada. Cabe anotar que la encuesta y las tablas de resultados fueron elaboradas usando el software Microsoft Excel.

	CONTROL	CONTROL ILUSTRATIVO	OBJETIVOS DE CONTROL DETALLADOS	NIVEL DE CUMPLIMIENTO	PONDERACIÓN	VALOR DE CUMPLIMIENTO	PUNTUACIÓN
Adquisición y Mantenimiento del Software de aplicaciones (AI2)	Las aplicaciones están disponibles y alineadas con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la apropiada inclusión de los controles de aplicación y los requisitos de seguridad, y el desarrollo y configuración alineados con los estándares.	Cuentan con una metodología de SDLC.	PO8.3,AI2.3	**Inexistente**	10	**0**	0
		Dicha metodología incluye requerimientos de seguridad e integridad de la información	AI2.4	**Inexistente**	8	**0**	0
		Dicha metodología tiene documentado los procesos de adquisición y desarrollo de nuevos sistemas	PO6.3, AI6.2	**Inexistente**	6	**0**	0
		Se tiene dentro de la metodología un conjunto de procedimientos apropiados para ejecutar los cambios drásticos en los sistemas existentes	AI1, AI2.3	**Inexistente**	6	**0**	0
		Dentro de la metodología se tienen estructurados los procedimientos para incluir controles que soporten un completo, preciso y autorizado procesamiento de las transacciones	AI1, AI2.3	**Inexistente**	10	**0**	0
		La metodología cuenta con un proceso de planeamiento y adquisición que se alinea con la dirección estratégica	PO4.3, AI3.1	**Inexistente**	6	**0**	0
		Para el mantenimiento de un ambiente confiable, la administración de TI involucra a los usuarios en el diseño de las aplicaciones, selección de aplicativos comerciales y en las pruebas de los mismos	AI1,AI2.1,AI2.2,AI7.2	**Inexistente**	10	**0**	0
		Se hacen revisiones posteriores a la implementación, para verificar que los controles están operando de forma efectiva, y se reportan cambios significativos en caso de ser hallados	AI7.12	**Inexistente**	8	**0**	0
		La organización adquiere y/o desarrolla sistemas de software en concordancia con los procesos de planeamiento, desarrollo y adquisición.	AI2	**Inexistente**	10	**0**	0

Ilustración 10. Encuesta del modelo de Madurez de TI respecto a la ley SOX

7.3 CÁLCULO DE LOS RESULTADOS ENTREGADOS

El modelo de auditoría arroja una serie de gráficos y tablas que son interesantes para conocer el estado de madurez de los controles de TI respecto a SOX, desde varias perspectivas.

En la hoja "Resultados", del archivo de Excel que contiene el modelo de la empresa que está siendo auditada, se encuentran una serie de tablas que muestra de manera detallada, el nivel de cumplimiento en cada área, y el número de controles que están en cada nivel de cumplimiento.

7.3.1 Cálculo del puntaje total por área. Para calcular el puntaje total alcanzado en cada área, simplemente se suman todos los puntajes de los controles que componen el área, así:

Puntaje Total Área = $\sum_{i=0}^{n} puntaje\_control_i$

Donde n es el número de controles que componen el área

7.3.2 Cálculo del puntaje ideal o máximo. El puntaje ideal o máximo, es un límite que consideramos la empresa (el área de TI) debe alcanzar para estar en un nivel de cumplimiento óptimo o ideal respecto a la Ley SOX. Éste se calcula suponiendo que la empresa tiene todos los controles del área en un estado "Manejado y medible" (un valor de 4), estado en el cual ya la empresa cumple en un nivel muy aceptable las regulaciones de la Ley SOX.

El valor ideal podrá variar dependiendo de ajustes que se hagan en el modelo, esto por características particulares del ambiente de Ti de la empresa.

Puntaje ideal = $\sum_{i=0}^{n} ponderacion\_control_i * 4$

Donde n es el número de controles que componen el área

7.3.3 Porcentaje de cumplimiento. Habiendo obtenido el puntaje total del área, y el puntaje ideal del área, es posible realizar un simple cálculo matemático para obtener el Porcentaje de Cumplimiento, sobre la base del puntaje ideal para la compañía.

Porcentaje de Cumplimiento = $\left(1-\left(\frac{(PI-PT)}{PI}\right)\right)\times 100$

Donde PI es el Puntaje Ideal o máximo
PT es el Puntaje Máximo

Éste será un muy buen indicador para saber cuáles son las áreas que requieren trabajo adicional para alcanzar el cumplimiento, y cuáles áreas están más fortalecidas respecto a SOX.

A continuación se anexan un par de pantallazos, el primero muestra los resultados detallados por área, y el segundo es la hoja que muestra los resultados consolidados de toda el área de TI en general. Adicional, al final del capítulo, dos gráficos basados en la información consolidada en las 2 hojas de resultados.

	A	B	C	D	E	F	G
1	**MADUREZ DEL CONTROL**	**NUMERO DE CONTROLES**					
2	No existente	3		En esta hoja se encuentran los resultados de la encuesta que			
3	Inicial / Ad-hoc	13		usted acaba de llenar, especialmente el número de controles que			
4	Repetible pero intuitivo	17		se encuentran en cada estado de madurez. En la parte izquierda			
5	Definido	13		superior se muestra el consolidado total, en la parte inferior			
6	Manejado y medible	13		izquierda se muestran discriminados por categoría, y en la parte			
7	Optimizado	1		derecha inferior se calculan los porcentajes de cumplimiento.			
8							
9							
10							
11					**PUNTAJE TOTAL**	**PUNTAJE IDEAL**	**PORCENTAJE CUMPLIMIENTO**
12	**Adquisición y Mantenimiento del Software de aplicaciones (AI2)**	No existente	1		176	296	59%
13		Inicial / Ad-hoc	1				
14		Repetible pero intuitivo	2				
15		Definido	6				
16		Manejado y medible	2				
17		Optimizado	0				
18	**Adquisición y Mantenimiento de la Infraestructura de Tecnología (AI3)**	No existente	0		12	24	50%
19		Inicial / Ad-hoc	0				
20		Repetible pero intuitivo	0				
21		Definido	0				
22		Manejado y medible	0				
23		Optimizado	0				
24	**Habilitación de Operaciones (PO6, PO8, AI6, DS13)**	No existente	1		70	80	88%
25		Inicial / Ad-hoc	0				
26		Repetible pero intuitivo	0				
27		Definido	0				
28		Manejado y medible	0				
29		Optimizado	0				

Ilustración 11. Resultados detallados por área

	PUNTAJE TOTAL	PUNTAJE IDEAL	PORCENTAJE CUMPLIMIENTO	ESCALA DE CUMPLIMIENTO
Adquisición y Mantenimiento del Software de aplicaciones (AI2)	176	296	59%	INICIAL
Adquisición y Mantenimiento de la Infraestructura de Tecnología (AI3)	12	24	50%	INICIAL
Habilitación de Operaciones (PO6, PO8, AI6, DS13)	70	80	88%	OPTIMIZADO
Instalar y Acreditar Soluciones y Cambios (AI7)	92	144	64%	AVANZADO
Administración de Cambios (AI6,AI7)	134	152	88%	OPTIMIZADO
Definición y Administración de los niveles de Servicio (DS1)	30	48	63%	AVANZADO
Gestión de Servicios Tercerizados(DS2)	112	176	64%	AVANZADO
Garantizar la Segridad de los Sistemas(DS5)	276	472	58%	INICIAL
Gestión de la configuración(DS9)	58	168	35%	INICIAL
Gestion de Problemas e Incidentes (DS8, DS10)	56	104	54%	INICIAL
Gestión de la Información (DS11)	116	200	58%	INICIAL
Gestión de Operaciones (DS13)	70	104	67%	AVANZADO
Computación de Usuario Final	90	200	45%	INICIAL
PROMEDIO DE CUMPLIMIENTO DE TODAS LAS ÁREAS			61%	AVANZADO

Ilustración 12. Resultados consolidados de toda el área de TI

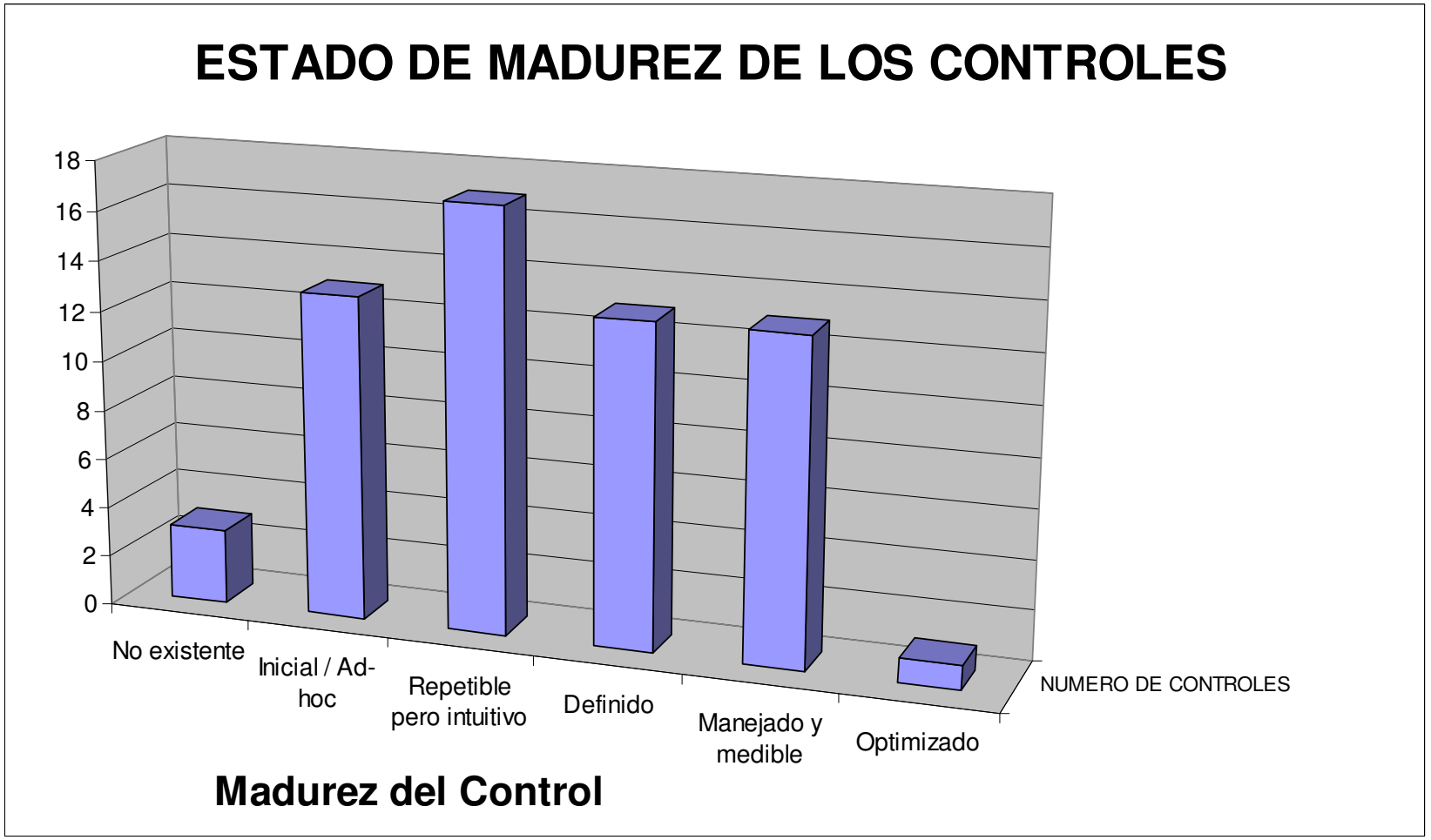

Ilustración 13. Número de controles en cada estado de madurez

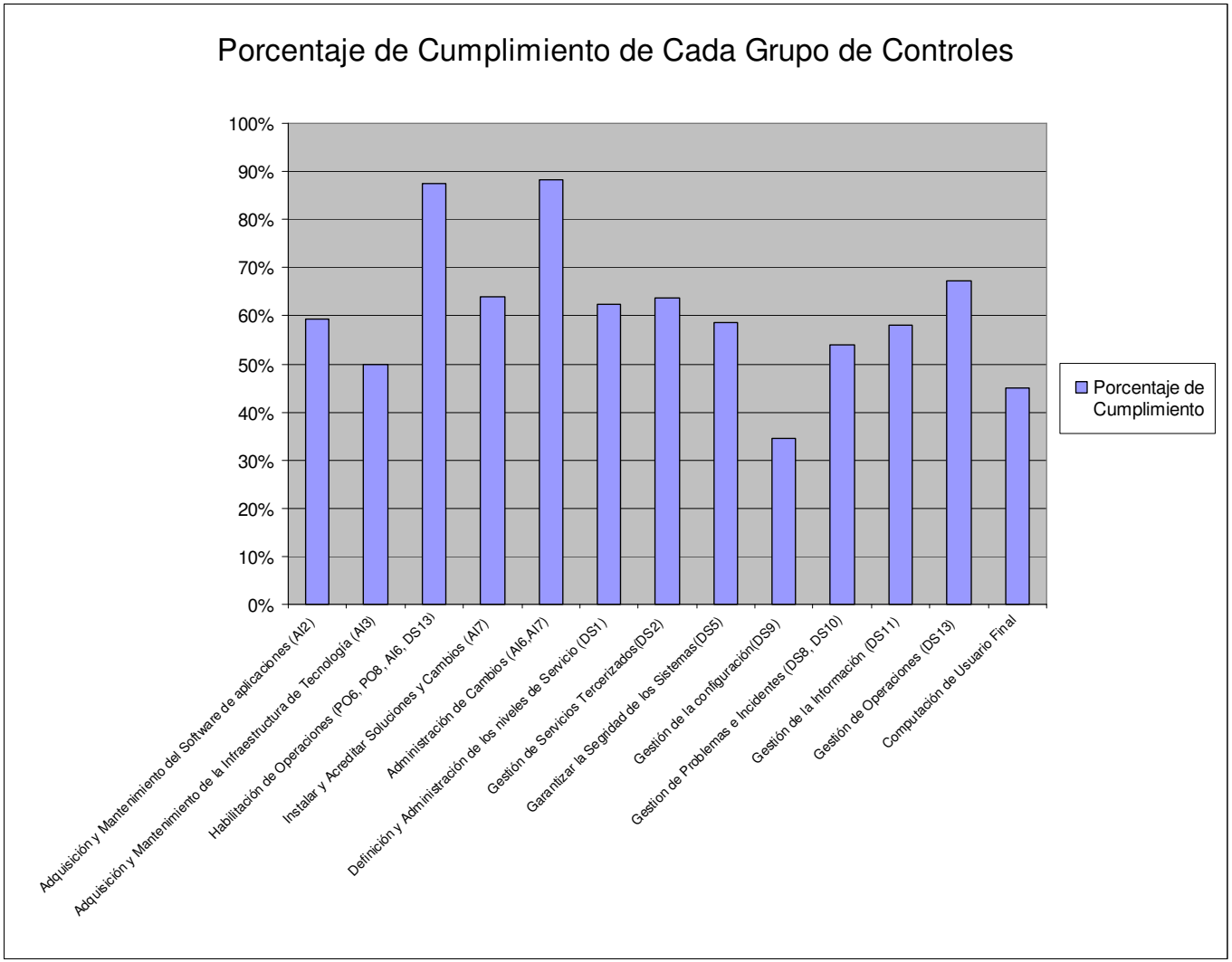

Ilustración 14. Porcentaje de cumplimiento de cada área de controles.

8. IMPACTO DE LA LEY SARBANES-OXLEY EN LAS EMPRESAS COLOMBIANAS

El buen momento por el que ha pasado la economía colombiana estos últimos años, ha llevado a varias empresas Colombianas a crecer considerablemente sus capitales propios, y a recurrir a socios extranjeros para cumplir sus planes de expansión por Latinoamérica y el mundo.

Algunas empresas colombianas han recurrido a la opción de cotizar cierto porcentaje de sus acciones en los mercados bursátiles extranjeros. Es el caso por ejemplo del banco Bancolombia y de la estatal ECOPETROL (la compañía más grande de Colombia), las cuales han tomado la decisión de entrar a cotizar acciones en la bolsa de valores de Nueva York (NYSE), con el fin de buscar capitales y recursos con los cuales puedan financiar sus proyectos de expansión. Como dato informativo, al momento de redactar éste párrafo, las acciones de Bancolombia (NYSE:CIB) se cotizaban a US$18,94 y las de ECOPETROL (NYSE:EC) a un precio de US$19,54[32].

Cuando una empresa extranjera desea entrar a cotizar en uno de las bolsas de Estados Unidos (NYSE, NASDAQ, Down Jones), debe acogerse al modelo conocido como ADR (American Depositary Receipt), que es un mecanismo implementado desde al año de 1927 en los Estados Unidos, con el fin de facilitar el proceso de compra y negociación de acciones en empresas extranjeras. Existen diferentes niveles de ADR[33], a los cuales la empresa extranjera se puede acoger para entrar al mercado bursátil de USA:

---

[32] Tomado de Google Finance, http://finance.google.com
[33] Tomado de http://www.corredores.com/Portal/eContent/library/documents/DocNewsNo216DocumentNo855.pdf

- **Nivel I**: Solo se negocian OTC (Over the Counter), y no transa en bolsa. Su ventaja principal es el bajo costo de emisión y mantenimiento.
- **Nivel II**: La compañía tiene el deber de realizar reportes financieros siguiendo los Principios Generalmente Aceptados de Contabilidad de Estados Unidos. Pueden ser listados en Bolsa, y no pueden llevarse a cabo IPOs[34] sobre este tipo.
- **Nivel III**: Siguen reglas muy estrictas similares a las compañías estadounidenses que cotizan en bolsa. Permiten a la compañía adelantar la emisión con ánimo de conseguir capital.

El Nivel III es por ejemplo en el que se encuentran ECOPETROL y Bancolombia, ya que éstas cotizan sus acciones en la NYSE y pueden obtener capital con recursos de ese país. En éste nivel se deben seguir todos los requerimientos de la SEC y de la PCAOB acerca de las regulaciones de la ley SOX.

Es claro que otras empresas que tengan en mente entrar a cotizar a las bolsas de valores de Estados Unidos, deberán empezar desde ya a implementar un estricto sistema de control interno que les permita ser "SOX Compliant" en el momento que estén listos para empezar a cotizar sus acciones en la NYSE.

La empresa con la que probamos el modelo de auditoría, explicado en el capítulo anterior, es Cementos Argos. Aunque actualmente no se encuentran cotizando en la bolsa de Nueva York, si lo piensan hacer en el corto o mediano plazo, todo depende de cómo siga el mercado financiero en Estados Unidos, el cual en octubre de 2008 está atravesando la crisis mas grave desde la depresión de los años 30.

[34] IPO: Initial Public Offering

8.1 EVALUACIÓN DEL MODELO EN CEMENTOS ARGOS

Cementos Argos ha venido trabajando desde hace varios años con compañías auditoras de presencia mundial como lo son Deloitte y KPMG, en el proceso de implementar la Ley Sarbanes-Oxley, no solo como cumplimiento a la Ley en sí (cuando empiecen a cotizar en NYSE) sino como una forma de mejorar continuamente los marcos de control interno y procesos de documentación.

Como parte de la presentación de tesis de proyecto de grado, en la cual se hace un análisis detallado del impacto que tiene la Ley Sarbanes-Oxley en las TI, se decidió realizar un modelo de auditoría en una de las empresas que está en proceso de hacer cumplimiento de la Ley en sus negociaciones con la bolsa de Nueva York. Se le solicitó al Ingeniero Alejandro Gálvez, Gerente de Tecnología de Cementos Argos S.A., nos diera un espacio en su agenda para realizar una serie de preguntas con el objetivo de determinar el estado de madurez de los aspectos evaluados en el modelo de auditoría que fue diseñado para tal fin.

Con base en los resultados obtenidos, se pudo determinar que Cementos Argos es una empresa que se encuentra en un nivel óptimo en su área de tecnología, lo que lo alinea con los estándares solicitados por COBIT para dar cumplimiento a la Ley. Aunque los hallazgos realizados en esta simulación de auditoría no están muy detallados en cuanto al estado de la tecnología, esta permite establecer una visión general de la estructura de tecnología de la empresa, mediante la cual podemos estar en capacidad de determinar su estado de madurez.

Cabe destacar que algunos aspectos de la evaluación fueron obviados ya que Cementos Argos no cuenta con áreas de desarrollo de Software, por lo cual

existen varios aspectos de la auditoría los cuales resultaron con una calificación de "Inexistente", lo cual puede generar errores en el modelo de auditoría, ya que pueden causar una pequeña desviación de la calificación definitiva del modelo de madurez.

En términos generales el modelo de simulación de auditoría, nos permitió establecer que Cementos Argos tiene los controles adecuados para una alineación estratégica con SOX; con base en el modelo de auditoría diseñado, y teniendo presente las limitaciones del mismo, a la luz de los objetivos de control recomendados por COBIT.

Debe recordarse la importancia de continuar con los esfuerzos de mantener un ambiente de seguridad en información que trabaje dimensiones técnicas y humanas apoyados en procedimientos estandarizados basados en normas internacionales como la ISO 27001 y 27002 y códigos de buenas prácticas como COBIT e ITIL que se aplique consistentemente en toda la infraestructura informática.

8.2 ANÁLISIS DE LA SITUACIÓN ACTUAL DE CEMENTOS ARGOS

En síntesis, y conforme con el modelo de auditoría planteado, Cementos Argos se encuentra en un estado de madurez óptimo para dar cumplimiento a la Ley SOX. La gestión de la infraestructura de tecnología, recursos humanos, información y aplicaciones las tienen en un estado muy avanzado, equiparable con la fase de "Manejado y medible", lo que les permite con toda tranquilidad, desde nuestra perspectiva, entrar a cotizar en la bolsa de NY sin mayores inconvenientes. El único aspecto en el que se le evidenciaron falencias fue en el de computación de usuario final, el cual según lo que nos explicó el Ingeniero Alejandro Gálvez, ninguna tarea que implique procesamiento de información financiera o relacionada, es ejecutada de forma directa en los sistemas del usuario final (por

ejemplo no se hace uso de hojas de cálculo para manipular información financiera). Por lo tanto el resultado del grupo de controles Computación de Usuario Final, no es relevante para el cumplimiento de la Ley SOX en Argos.

En el resto de los aspectos, la evaluación estuvo en promedio en un 88% del cumplimiento requerido según nuestro modelo.

8.3 ASPECTOS POSITIVOS

Es muy importante volver a recalcar, el modelo de auditoría realizado es un buen indicador, pero mira la empresa en aspectos generales, ya que no abarca a fondo todos los aspectos críticos de la infraestructura de TI, sin embargo, el conocimiento que tiene de su área el Gerente de Tecnología, nos permite modelar una visión global de la forma como está configurada el área de TI en términos de las aplicaciones, la infraestructura, el recurso humano y la información. Desde la evaluación se puede determinar que en términos generales, Cementos Argos se encuentra en un nivel más que aceptable para proceder a hacer negociaciones en la bolsa de NY.

El siguiente gráfico, permite ver de forma simple, los niveles de madurez en cada uno de los aspectos evaluados en la auditoría, en este modelo se puede evidenciar que Cementos Argos se encuentra gestionando su infraestructura de forma apropiada. Cada uno de los brazos del diagrama radial es uno de los aspectos evaluados en la auditoría, y en ellos podemos observar que la madurez del modelo es muy adecuada a excepción de la Computación de Usuario Final como se mencionó anteriormente.

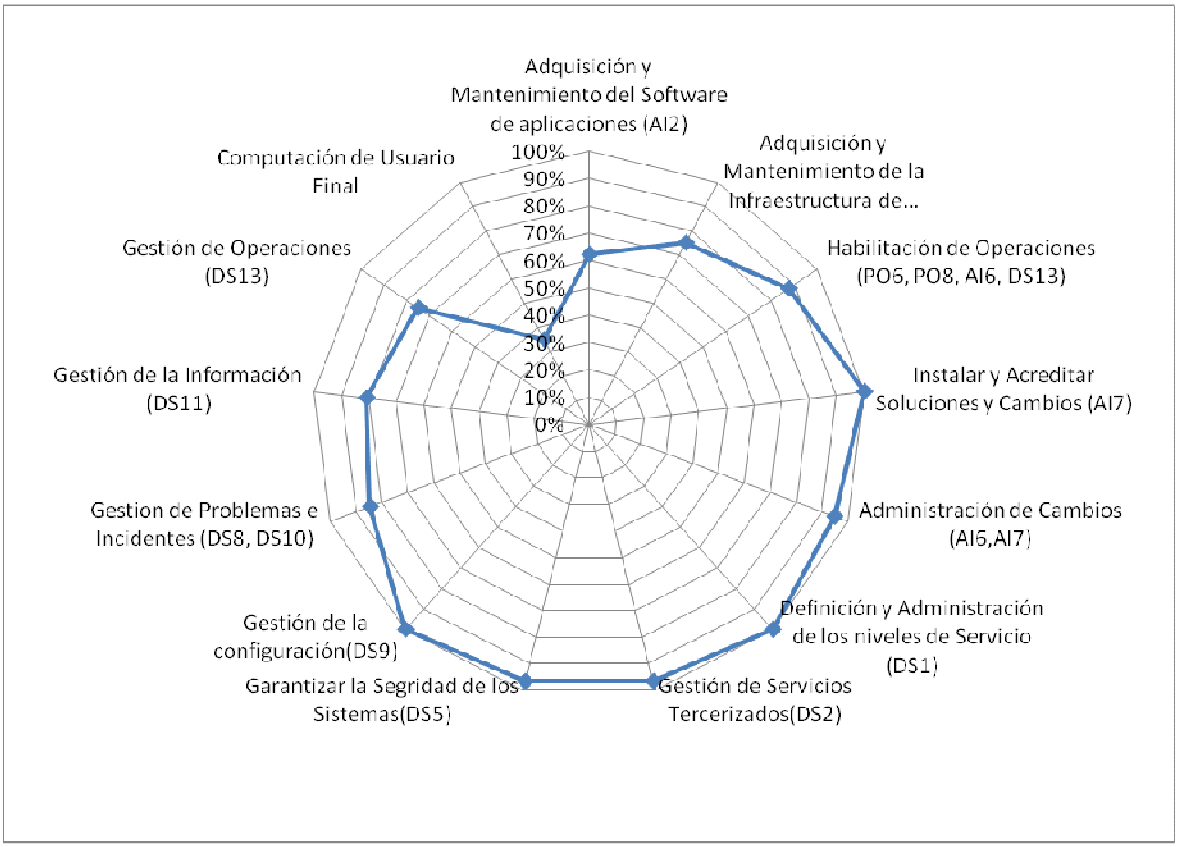

Ilustración 15. Porcentaje de cumplimiento de los aspectos evaluados

Entre los aspectos que mayor calificación obtuvieron se encuentran los siguientes:

- Instalar y Acreditar Soluciones y Cambios (AI7)
- Administración de Cambios (AI6,AI7)
- Definición y Administración de los niveles de Servicio (DS1)
- Gestión de Servicios Tercereados(DS2)
- Garantizar la Seguridad de los Sistemas(DS5)
- Gestión de la Configuración(DS9)

Los cuales fueron los que elevaron más la calificación de la evaluación, dado que en promedio lograron tener una calificación de 88%, lo que demuestra el alto

nivel de madurez en la gestión de tecnología con la que cuenta Cementos Argos y los niveles de control sobre la misma.

8.4 METODOLOGÍA PARA LA REALIZACIÓN DE LAS PRUEBAS

De acuerdo con la estructura de trabajo planteada y la información solicitada se procedió a seguir el siguiente orden metodológico para la realización del modelo de auditoría de Cementos Argos:

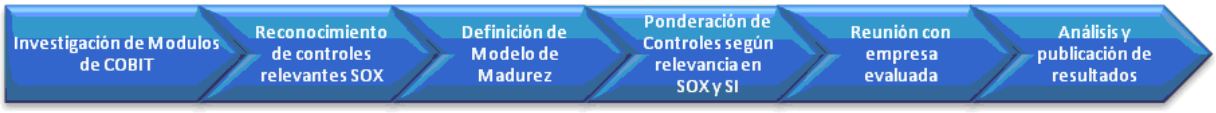

Ilustración 16 - Flujo de trabajo para el modelo de auditoría

Básicamente, los cuatro primeros pasos fueron ejecutados durante la elaboración del modelo de madurez, tratado específicamente en el capítulo anterior.

Los dos últimos pasos corresponden a la reunión con el Gerente de Tecnología de Cementos Argos S.A., durante la cual se hace el análisis; y la última fase, el análisis y publicación de resultados, que se presenta más adelante en éste capítulo.

Durante la reunión, se le explica al Gerente de Tecnología como se desarrolló el modelo, y como se realiza la evaluación de la compañía. A continuación se le empiezan a hacer cada una de las preguntas, a lo cual el Gerente, con el conocimiento que tiene del área de TI, responde en una escala de 0 a 5, previamente definida y explicada en el capítulo anterior.

8.5 SUPUESTOS, LIMITACIONES Y POSIBLES CAUSAS DE ERROR

Dado la naturaleza del modelo de auditoría planteado, era complicado llevar a fondo un análisis preciso de cada uno de los aspectos evaluados, así pues, y gracias a los buenos servicios prestados por el Ingeniero Alejandro Gálvez, se pudo realizar un modelo sencillo, que permitiera establecer de forma general un estado de madurez dentro del área de TI.

Por otro lado también es importante reconocer que dada las limitaciones del modelo, nos fue imposible obtener información más detallada de cada uno de los controles debido a que esto es información sensible dentro de la compañía Cementos Argos S.A.

8.6 RESULTADOS OBTENIDOS Y OPORTUNIDADES DE MEJORA

En términos generales Cementos Argos S.A. es una empresa que gestiona de forma OPTIMIZADA su área de TI. Los resultados obtenidos los cuales son presentados a continuación, ilustran la manera como la compañía maneja su área de tecnología en cada uno de los aspectos analizados de una forma clara y sencilla.

1. Adquisición y Mantenimiento del Software de aplicaciones (AI2)

DESCRIPCIÓN	Las aplicaciones están disponibles y alineadas con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la apropiada inclusión de los controles de aplicación y los requisitos de seguridad, y el desarrollo y configuración alineados con los estándares.
PUNTAJE TOTAL	184
PUNTAJE IDEAL	296

% DE CUMPLIMIENTO	62%
ESCALA DE CUMPLIMIENTO	AVANZADO

Observaciones:

Es importante recalcar varios aspectos de este aspecto evaluado, los tres primeros aspectos evaluados:

- Cuentan con una metodología de SDLC[35].
- Dicha metodología incluye requerimientos de seguridad e integridad de la información
- Dicha metodología tiene documentado los procesos de adquisición y desarrollo de nuevos sistemas

Dieron como resultado Inexistente, debido a que Cementos Argos no cuenta con un área de desarrollo de software como tal, y este resultado podría ser obviado lo que haría que la evaluación varíe de forma alta.

2. Adquisición y Mantenimiento de la Infraestructura de Tecnología (AI3)

DESCRIPCIÓN	Las organizaciones tienen procesos para la adquisición, implementación, y mejora de la infraestructura de tecnología. Esto requiere una aproximación planificada para adquirir, mantener, y proteger la infraestructura.
PUNTAJE TOTAL	18
PUNTAJE IDEAL	24
% DE CUMPLIMIENTO	75%
ESCALA DE CUMPLIMIENTO	AVANZADO

[35] SDLC: Software Development Life Cycle, metodología para el desarrollo y mantenimiento de software

Observaciones:

Este aspecto solo contiene un control, y aunque se indicó que se contaba con dicha metodología, el propio Gerente decidió "castigarlo" dado que no esta funcionando de la forma en que él desearía que funcionara.

3. Habilitación de Operaciones (PO6, PO8, AI6, DS13)

DESCRIPCIÓN	Estos controles proporcionan una garantía razonable de que las políticas y procedimientos que definen los procesos de mantenimiento y adquisición requeridos han sido desarrollados y son mantenidos, y de que ellos definen la documentación necesaria para apoyar el uso apropiado de las aplicaciones y las soluciones tecnológicas puestas en marcha.
PUNTAJE TOTAL	70
PUNTAJE IDEAL	80
% DE CUMPLIMIENTO	88%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

En este aspecto fue en donde se obtuvo una de las calificaciones más elevadas ya que Cementos Argos cuenta con una línea base mediante la cual pueden basarse en caso de requerir realizar una re-configuración de todo el sistema de TI, y dichos procesos se encuentran debidamente documentados.

4. Instalar y Acreditar Soluciones y Cambios (AI7)

DESCRIPCIÓN	Los nuevos sistemas tienen que ser operacional es una vez su desarrollo sea completado. Esto requiere realizar las pruebas asociadas en un ambiente dedicado a los datos de prueba apropiados, definición y desarrollo de las instrucciones de migración, y revisiones posteriores a la implementación.
PUNTAJE TOTAL	144

PUNTAJE IDEAL	144
% DE CUMPLIMIENTO	100%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

En este aspecto se obtuvo una calificación perfecta, este comprendía cuatro controles:

- Una estrategia de pruebas es desarrollada y seguida para todos los cambios significativos en las aplicaciones y en la infraestructura tecnológica, la cual persigue la unidad, el sistema, la integración y las pruebas del nivel de aceptación del usuario, de manera que operen de la forma prevista.

- Pruebas de carga y estrés son ejecutadas de acuerdo a un plan de pruebas y a unos estándares de pruebas definidos.

- Las interfaces con otros sistemas son probadas para confirmar que las transmisiones de información son completas, precisas, y válidas

- La conversión de la información es probada entre el origen y el destino, para confirmar que la información es completa, precisa y válida

Estos controles arrojaron excelentes resultados en Cementos Argos, a excepción del segundo, pero éste control no tenía una ponderación tan elevada dentro del modelo de auditoría, razón por la cual la calificación fue sumamente positiva.

5. Administración de Cambios (AI6,AI7)

DESCRIPCIÓN	Estos controles proveen una garantía razonable de que los cambios al sistema financiero son autorizados y probados de forma apropiada antes de ser implementados en producción.
PUNTAJE TOTAL	144

PUNTAJE IDEAL	152
% DE CUMPLIMIENTO	95%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

En este aspecto, todos los resultados fueron óptimos a excepción de:

- La administración de TI implementa sistemas de software que no ponen en riesgo la seguridad de la información y los programas almacenados en el sistema

En este control, el Ingeniero Gálvez declaro tener una metodología medible, pero que el esperaría un sistema mejor calificado para gestionar los riesgos de la seguridad de la información que se maneja en estos sistemas de almacenamiento.

6. Definición y Administración de los niveles de Servicio (DS1)

DESCRIPCIÓN	Existe una adecuada comunicación entre la administración de TI y los clientes de negocio en lo que se refiere a los servicios requeridos habilitando ser un documento de definición y acuerdo en los servicios de TI y niveles de servicio.
PUNTAJE TOTAL	48
PUNTAJE IDEAL	48
% DE CUMPLIMIENTO	100%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

Aunque los controles evaluados en este aspecto arrojaron resultados de manejable y medible, la ponderación de dichos controles era muy baja, y adicional a esto, el nivel de cumplimiento, basado en la calificación ideal, refleja que a pesar de no tener los controles en un nivel de madurez más elevado, la metodología implementada para éste aspecto es la adecuada.

7. Gestión de Servicios Tercereados(DS2)

DESCRIPCIÓN	Asegurar que los servicios tercereados (vendedores, proveedores y socios) cumplen con los requisitos solicitados por el negocio de los procesos de administración tercereados. Este proceso se cumple definiendo claramente en los roles, responsabilidades y expectativas de los acuerdos así como una revisión y monitoreo para lograr una efectividad y un cumplimiento.
PUNTAJE TOTAL	170
PUNTAJE IDEAL	176
% DE CUMPLIMIENTO	97%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

En términos generales, este aspecto evaluado tenía una muy baja ponderación dentro del modelo de auditoría; a excepción del de la revisión periódica de la seguridad, razón por la cual a pesar de que en promedio los controles realizados arrojaron como resultado que solo contaban con una metodología de Manejado y Medible, en general se obtuvo una buena calificación de todo el aspecto. Aunque es importante destacar que sería bueno que se mejoren las metodologías de las revisiones periódicas de seguridad con el objetivo de incrementar el nivel de madurez de las mismas.

8. Garantizar la Seguridad de los Sistemas(DS5)

DESCRIPCIÓN	La necesidad de mantener la integridad de la información y proteger activos de TI requiere de un proceso administrativo de seguridad. Este proceso

	incluye establecer y mantener roles de seguridad de TI y responsabilidades, políticas, estándares, y procedimientos. La administración de TI también incluye monitoreo del desempeño periódico y pruebas, así como acciones correctivas para debilidades hoy dientes de seguridad.
PUNTAJE TOTAL	456
PUNTAJE IDEAL	472
% DE CUMPLIMIENTO	97%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

Este aspecto fue también uno de los que más alta calificación obtuvo, en términos generales, el nivel de madurez acá fue de Manejado y Medible, a excepción del siguiente control:

"Donde sea apropiado, existen controles para que ninguna de las partes pueda denegar transacciones, y hay controles implementados para proveer el no repudio (certificación de quien envía y de quien recibe) del origen o del destino, prueba de envío y confirmación de la transacción".

Este aspecto, aunque no se le agrego mucha ponderación, es importante tener en cuenta que se implementen los controles adecuados para confirmar la veracidad y la autenticidad de la información que se envía y se recibe, para garantizar que esta proviene de las fuentes que dice proceder, pero en síntesis es un control que aunque Cementos Argos no lo tenga totalmente implementado, están conscientes de que lo tienen que implementar y se encuentran en proceso de hacerlo.

9. Gestión de la configuración(DS9)

DESCRIPCIÓN	Garantizar la integridad de las configuraciones de hardware y software requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la

	verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad, minimiza los problemas de producción y resuelve los problemas más rápido.
PUNTAJE TOTAL	168
PUNTAJE IDEAL	168
% DE CUMPLIMIENTO	100%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

En este aspecto la empresa obtuvo la más alta calificación, y aunque solo uno de los controles sugeridos dentro de éste aspecto tenía una ponderación alta, es importante recalcar que cualquier empresa que desee tener unas medidas de seguridad apropiadas, y que se encuentre en el proceso de iniciar el cumplimiento de la ley SOX, debe tener una apropiada metodología de configuración de los dispositivos de la infraestructura de TI, así como también sus aplicaciones.

10. Gestión de Problemas e Incidentes (DS8, DS10)

DESCRIPCIÓN	Los controles proporcionan aseguramiento razonable de que algún problema y/o incidente son propiamente atendidos para registrar, resolver o investigar su apropiada resolución.
PUNTAJE TOTAL	88
PUNTAJE IDEAL	104
% DE CUMPLIMIENTO	85%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

En este otro aspecto se tenían tres controles, de los cuales solo uno tenía la ponderación más alta, y vale la pena señalar que justo el fin de semana anterior a la realización de este modelo, la empresa realizó un simulacro para verificar su plan de contingencia o BCP, con resultados óptimos. Aunque el mismo

Gerente indicó el deseo de castigar estos controles con el objetivo de manejar una perspectiva autocrítica de lo que realizan y elevar los niveles de madurez deseados.

11. Gestión de la Información (DS11)

DESCRIPCIÓN	Existen políticas y procedimientos para la distribución y retención de datos y reportes generados
PUNTAJE TOTAL	162
PUNTAJE IDEAL	200
% DE CUMPLIMIENTO	81%
ESCALA DE CUMPLIMIENTO	OPTIMIZADO

Observaciones:

En términos generales, el nivel de madurez de este aspecto es de Definido, pero debido a que en promedio la ponderación de los controles de este aspecto solo alcanza el 8,333, es un aspecto que no tiene un impacto muy fuerte dentro de todo el marco de gobernabilidad de TI, lo que hace que la calificación sea muy buena. En este aspecto es importante recalcar que todas las calificaciones realizadas, aunque se encontraban en un nivel adecuado, el Gerente de Tecnología decidió reconocer sus debilidades en ciertos controles, y su intención de modificarlos para que funcionen a un nivel mejorado.

12. Gestión de Operaciones (DS13)

DESCRIPCIÓN	El procesamiento completo y preciso de los datos requiere un administración efectiva de los procedimientos de procesamiento de los datos y mantenimiento diligente del hardware. Este proceso incluye la definición de políticas operativas y procedimientos para una administración efectiva de las actividades de procesamiento programadas, protegiendo a salida sensitivas, monitor el desempeño de la infraestructura y asegurándose con mantenimientos preventivos del hardware
PUNTAJE TOTAL	78

PUNTAJE IDEAL	104
% DE CUMPLIMIENTO	75%
ESCALA DE CUMPLIMIENTO	AVANZADO

Observaciones:

Este aspecto tuvo una evaluación buena, aunque se podrían mejorar los controles para la retención de información, el registro cronológico de eventos, y la mesa de servicios no se encuentra debidamente configurada para lograr que estos controles se cumplan de manera apropiada. Este aspecto es de vital importancia para el cumplimiento de SOX, debido a que uno de los requerimientos fundamentales de la Ley y la SEC es que los reportes financieros se mantengan como mínimo 7 años dentro de la compañía para ser revisados cuando sea necesario. Aún así se determina que para este aspecto, la metodología de Cementos Argos es la apropiada pero podría mejorarse.

13. Computación de Usuario Final

DESCRIPCIÓN	Estos controles son presentados para direccionar las características de un ambiente típico de computación de usuario final, los procesos apropiados de COBIT aplican a este ambiente.
PUNTAJE TOTAL	70
PUNTAJE IDEAL	200
% DE CUMPLIMIENTO	35%
ESCALA DE CUMPLIMIENTO	INICIAL

Observaciones:

Este es tal vez el único aspecto en el que se observa un nivel de madurez incipiente dentro de Cementos Argos, pero debido a la conversación sostenida con el Ingeniero Alejandro Gálvez, parece ser que los controles que se plantean dentro de éste aspecto no son los que se aplican para la empresa, debido a la

misma razón que se indicó al inicio de la auditoría, Cementos Argos no cuenta con un Área de Desarrollo de Software.

9. CONCLUSIONES

- Se concluye que el impacto de la Ley Sarbanes-Oxley dentro del la infraestructura de TI y en general en todos los procesos de TI, ha sido muy importante dado que aunque la Ley no hace una mención directa al área de TI, es claro que su cumplimiento depende principalmente de unos sistemas de TI confiables y seguros.

- Como se expresa en el capítulo de impacto en la seguridad de la información la ley Sarbanes-Oxley reglamenta la forma en que se procesan los datos y los requisitos para establecer quién es el dueño de la información y a quién va dirigida. Requisitos fundamentales que garantizan la transparencia de los datos en los reportes financieros.

- Se determinó el impacto que tienen las diversas plataformas tecnológicas y tecnologías de información y como se puede mejorar considerablemente la confiabilidad en la información financiera mediante controles rigurosos en los sistemas financieros y su tecnología de soporte.

- Los requerimientos de retención de informes de auditoría y documentación relacionada, asi cómo los requerimientos de control establecidos por la SEC, han llevado a que muchas empresas tengan que implementar o mejorar las políticas de almacenamiento, respaldo de la información y realizar inversiones considerables en equipos y software, para garantizar

el cumplimiento, el mantenimiento de registros y que la información permanezca íntegra el tiempo requerido.

- Se evidenció como con COBIT se pudo desarrollar un modelo de auditoría, que permite determinar de forma general, cuáles son los controles y aspectos de TI que se están aplicando dentro de la organización, y fundamentado sobre esos controles, se pueda determinar el nivel de madurez de la empresa en el área de TI con el objetivo de dar cumplimiento a la Ley Sarbanes-Oxley.

- El rol del CIO ó CDO, a pesar de que existe formalmente en unas pocas empresas a nivel mundial, debe ser tenido en cuenta, ya que es esa persona en especial quien debe estar encargado de definir políticas y procedimientos encaminados a la protección y administración de la información de la compañía, en especial de la información financiera.

- Los papeles del CSO, CIO y CDO básicamente están encaminados a convertirse en los protagonistas en lo que respecta al manejo y flujo de la información dentro de la organización, razón por la cual sus funciones tienden a fusionarse hasta convertirse en un solo rol, que se encarga de gestionar las operaciones diarias en lo que a la información respecta.

- Siendo EE.UU. uno de los principales aliados comerciales de Colombia, la relevancia de la ley Sarbanes-Oxley para nuestro país es de primera línea, dado el efecto global de la economía, el cual ha causado que las empresas tengan que empezar a pensar en las regulaciones de los mercados extranjeros, y buscar mecanismos que les permitan adaptarse de una manera adecuada a dichas regulaciones.

- Como se pudo ver con empresas como Argos, Bancolombia y ECOPETROL, El proceso continuo de globalización hará que cada vez más, empresas colombianas incursionen en los mercados bursátiles de los Estados Unidos, por lo cual, se verán obligadas a hacer cambios significativos al área de TI, con el fin de adaptarla a las regulaciones establecidas por la Ley SOX.

- Las observaciones obtenidas gracias al modelo de auditoría desarrollado, permitieron establecer de manera general, la forma como se puede generar una serie de directrices que le permitan a las empresas, determinar que tan alto está el nivel de madurez de sus controles internos en el área de TI, y cuales áreas debe fortalecer con el objetivo de dar cumplimiento a la Ley Sarbanes-Oxley.

- La revisión realizada en Cementos Argos con base en el modelo COBIT, permitió establecer que el modelo desarrollado, aunque de forma general, facilita obtener una apreciación del estado de cumplimiento de los diferentes aspectos de TI, en relación a la Ley Sarbanes-Oxley.

- Se pudo evidenciar que es adecuado y recomendable para las empresas colombianas utilizar el marco de trabajo de COBIT, para el cumplimiento de la Ley Sarbanes-Oxley dado que es un subconjunto de objetivos de control del área de TI recomendadas por COSO, y a su vez COSO es recomendado por la SEC, la cual dictamina las regulaciones legales de ésta Ley.

10. BIBLIOGRAFÍA

BREWER, DENNIS C. Security Controls for Sarbanes-Oxley Section 404 IT Compliance. Indianapolis: Wiley Publishing, Inc. 2006.

BLOEM, JAAP. ET AL. Making IT Governance Work in a Sarbanes-Oxley World. Indianapolis: Wiley Publishing, Inc. 2006.

TAYLOR, HUGH. The Joy of Sarbanes-Oxley. Indianapolis: Wiley Publishing, Inc. 2006.

IT GOVERNANCE INSTITUTE. COBIT 4.0. IT Governance Institute publication. 2005.

TARANTINO, ANTHONY. Manager's Guide to Compliance. New Jersey: Wiley Publishing, Inc. 2006.

ANAND, SANJAY. Sarbanes-Oxley Guide for Finance and IT Professionals. New Jersey: Wiley Publishing, Inc. 2006.

LAHTI, CHRISTIAN. Sarbanes-Oxley Compliance using COBIT and Open Source Tools. New York: Syngress Publishing, Inc. 2005.

SARBANES, PAUL ET AL. Sarbanes-Oxley Act. Washington DC: US Congress Library. 2002.

IT GOVERNANCE INSTITUTE. IT Control Objectives for Sarbanes-Oxley. Rolling Meadows: IT Governance Institute Publication. 2006.

WELYTOK, JILL GILBERT. Sarbanes-Oxley for Dummies. Indianapolis: Wiley Publishing, Inc. 2006.

HEWLETT PACKARD. Information Lifecycle Management Technical Overview. 2006.

IBM. Addressing the key implications of Sarbanes-Oxley. 2004.

SPEARS, JANINE. A Preliminary Investigation of the Impact of the Sarbanes-Oxley Act on Information Security. Proceedings of the 39th Hawaii International Conference on System Sciences. 2006.

CHAMERO, JUAN. El Escándalo ENRON. [en línea]. < http://www.aunmas.com/ataque/globalidad_08.htm >. 16 de marzo de 2007.

RASCH, MARK. Sarbanes-Oxley for IT Security.[en línea]. < http://www.securityfocus.com/columnists/322 >.2 de mayo de 2005.

WILLIAMS, FIONA. Sarbanes-Oxley and You. [en línea]. < http://www.csoonline.com/article/218577/Sarbanes_Oxley_and_You >. 1 de octubre de 2003.

WIKIPEDIA. Sarbanes-Oxley Act. [en línea]. < http://en.wikipedia.org/wiki/Sarbanes-Oxley_Act >. 1 de Noviembre de 2006.

SECURITIES AND EXCHANGE COMISSION. Home Page. [en línea]. < http://www.sec.gov > . 24 de Diciembre de 2007.

DIBY MALAKAR. Chief Data Steward or Chief Data Officer: Another C-Level Acronym? [material en línea] <http://www.tdan.com/view-articles/4581>