UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN

CUMPLIMIENTO DE LA LEY SARBANES OXLEY BAJO LOS MARCOS DE REFERENCIA CoBIT Y COSO

DISEÑO DE UN PROYECTO PARA UNA ORGANIZACIÓN

QUE PARA OBTENER EL TÍTULO DE:
LICENCIADO EN INFORMÁTICA

PRESENTA:

JORGE ARMANDO MEDINA CASTRO

ASESOR:

M. EN I. GRACIELA BRIBIESCA CORREA

MÉXICO, D. F. 2006

Autorizo a la Dirección General de Bibliotecas de la UNAM a difundir en formato electrónico e impreso el contenido de mi trabajo recepcional.

NOMBRE: Verónica Castro Vargas Hernández

FECHA: 07/agosto/2015

FIRMA:

CUMPLIMIENTO DE LA LEY SARBANES OXLEY BAJO LOS MARCOS DE REFERENCIA CoBIT Y COSO

Agradecimientos

Gracias a Dios por permitirme alcanzar uno de los más grandes sueños que tiene un estudiante, concluir una carrera universitaria.

Gracias a mis padres (Filemon y Carmen) por darme la vida, cuidarme y darme la mejor herencia que pudieron brindarme, la educación…

Gracias a Azucena que siempre estuvo al pendiente de que concluyera mis tareas, mis materias y sobretodo, mi carrera… Su apoyo incondicional se ve reflejado en este libro…

Gracias a mis amigos y compañeros del Consejo de la Judicatura Federal (Noé, Kenia, Guillermo, Víctor, Sara, Lic. Izcoatl) por brindarme una oportunidad en el área de Auditoría Informática, ya que gran parte de éste libro lo debo a sus enseñanzas y conocimientos

Gracias Juan Antonio Segura, Alejandro Cervantes y Fernando Mata, sus consejos y enseñanzas han dejado una huella profunda en éste trabajo...

Gracias a la vida por permitirme llegar a feliz término mi licenciatura, es un pequeño paso en mi educación, pero un gran paso en mi formación...

Gracias a la Universidad Nacional Autónoma de México, semillero de grandes talentos que me abrió sus puertas y permitió concluir el primero de muchos sueños educativos...

Sobretodo, Gracias Fac. de Contaduría y Administración, fuiste, eres y serás mi casa...

INDICE

CAPÍTULO 1. Introducción al Proceso de Auditoría

1.1 Introducción

Los cambios trascendentes operados en la actualidad en el mundo moderno, se caracterizan fundamentalmente por un crecimiento acelerado en tecnología, especialmente cuando se trata de automatizar la información a fin de obtener en menor tiempo y mayor precisión la información requerida para la toma de decisiones de una empresa.

La acentuada dependencia que incorpora en alto volumen de información y los sistemas que la proveen; el aumento de la vulnerabilidad y el amplio espectro de amenazas, tales como las amenazas cibernéticas; la escala y los costos de las inversiones actuales y futuras en información y en sistemas de información; y el potencial que poseen las tecnologías para cambiar drásticamente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos, han impuesto nuevos retos a la práctica de la profesión de auditoría, en particular a la Auditoría Interna.

Las características generales en el entorno de cualquier entidad moderna, que incorpore a su gestión las Tecnologías de Información (TI), sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información, para maximizar a través de su soporte logístico el control interno, y consecuentemente sus resultados, demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior mediante la Auditoría y en especial en la Auditoría Informática.

Practicar Auditorías en una organización en la que el éxito de su gestión depende, como factor crítico, de la eficiente administración de la información y la Tecnología de Información, en la que los Sistemas de Gestión han alcanzado un desarrollo tan notable, demanda la introducción de una concepción muy diferente a la que primó para esta disciplina durante décadas. Tal concepción demanda, la participación inexcusable de la tecnología como herramienta, permitiéndole evolucionar al ritmo de los cambios tecnológicos incorporados a la estructura del registro y del control interno y muy especialmente, para evaluar mediante Auditorías a las Tecnologías de Información, los procedimientos de control específicos, dentro del ámbito de su soporte tecnológico, que a su vez, garantice una información objetiva sobre el grado de cumplimiento de las políticas y normativas establecidas por la organización para lograr sus objetivos.

A todo esto, la Auditoría Informática tiene como principal objetivo, evaluar el grado de efectividad de las Tecnologías de Información, dado que evalúa en toda su dimensión, en que medida se garantiza la información a la Organización, su grado de Eficacia, Eficiencia, Confiabilidad e Integridad para la toma de decisiones, convirtiéndola en el método más eficaz para tales propósitos.

Su ámbito de acción se centra, en revisar y evaluar: los procesos de planificación; inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras.

La generalizada informatización de los procesos y disciplinas que impactan directamente en la sociedad, en especial las relacionadas con la gestión económica, que hace apenas una década se procesaban manualmente, así como los propios cambios que introduce su tratamiento informatizado, introducen transformaciones sustanciales sobre el concepto tradicional del control interno, la estructura del registro y consecuentemente la práctica de las Auditorías.

La Auditoría Interna, en su desempeño, tiene también la responsabilidad de velar por el adecuado empleo y utilización de los recursos Informáticos y por el cumplimiento de la misión que a éstos le ha asignado la organización.

Tal conclusión conduce, a la inexcusable necesidad de practicar "Auditorías Informáticas", a partir de un conjunto de técnicas y procedimientos que evalúen los controles internos intrínsecos y específicos de los Sistemas de Información; en consecuencia, determina, que conceptualmente, no es dependiente ni evoluciona desde la Auditoría convencional: sus puntos de partida son esencialmente diferentes ya que no analiza la corrección o incorrección de cuentas contables, sino que constituye un instrumento de control superior para valorar la correcta administración de los recursos de Tecnología de Información como: Datos, Aplicaciones, Tecnología, Instalaciones, y Personal para valorar la efectividad de la información que requiere la organización. Su concepción se refiere a la integración de las técnicas informáticas y de auditoría para practicar un nuevo estilo de verificación, sobre un ambiente no convencional, con herramientas de punta y con procedimientos inexistentes y que puede definirse como: *"El conjunto de Procedimientos y Técnicas que evalúan, parcial o totalmente los Controles Internos de los Sistemas de Información; la protección de sus activos y recursos; verifica si su explotación se desarrolla con eficiencia, de acuerdo con las políticas y normativas establecidas por cada entidad y valora si se alcanza el grado de organización previsto para el marco donde participa y actúa".*

En correspondencia con la definición que antecede, así como por su finalidad, objetivos y utilidad que le atribuimos, la Auditoría Informática se clasifica en: Auditorías Informáticas de Seguridad, de Redes, de Sistemas o Aplicaciones, de Explotación de los Sistemas, de Planificación y Organización y de Gestión de la Tecnología para el logro de los propósitos de la organización. Consecuentemente, se han diseñado un conjunto de premisas, principios, y procedimientos para la práctica de estas auditorías.

1.2 Concepto de Auditoría

A finales del siglo XX, los Sistemas Informáticos se han constituido como las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los Sistemas de Información de la empresa.

La informática hoy, está subsumida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben estar, por lo tanto, sometidos a los controles generales de la misma. En consecuencia, las organizaciones informáticas forman parte de lo que se ha denominado gestión de la empresa. Cabe aclarar que la informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. A causa de esto, se ha tomado la frase *"Tiene Auditoría"* como sinónimo de que, en dicha entidad, antes de realizarse la auditoría, ya se habían detectado fallas.

El concepto de auditoría es mucho más que esto, la palabra auditoría proviene del latín *auditorius*, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír[1].

Si consultamos el Boletín C de Normas de auditoría[2] del Instituto Mexicano de Contadores Públicos nos dice: *"La auditoría no es una actividad meramente mecánica que implique la aplicación de ciertos procedimientos cuyos resultados, una vez llevado a cabo son de carácter indudable. La auditoría requiere del ejercicio de un juicio profesional, sólido y maduro, para juzgar los procedimientos que deben seguirse y estimar los resultados obtenidos."*

De todo esto sacamos como deducción que la auditoría es un examen crítico pero no mecánico, que no implica la preexistencia de fallas en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Otros autores la definen como: *"La revisión y evaluación de los controles, sistemas y procedimientos de la informática; de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que servirá para una adecuada toma de decisiones".*

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente y eficaz Sistema de Información.

[1] Auditoria Informática, José Antonio Echenique García, 2ª Edición pp.2
[2] Normas y procedimientos de Auditoría, Instituto Mexicano de Contadores Públicos.

Claro está que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, ya que una universidad, una dependencia gubernamental o un hospital son tan empresas, como una sociedad anónima o empresa pública. Todos utilizan la informática para gestionar sus "negocios" de forma rápida y eficiente con el fin de obtener beneficios económicos y reducción de costos.

Por eso, al igual que los demás órganos de la empresa (balances y cuentas de resultados, tarifas, sueldos, etc.), los Sistemas Informáticos están sometidos al control correspondiente, o al menos debería estarlo. La importancia de llevar un control de esta herramienta se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los centros de proceso de datos se convirtieron en blancos apetecibles no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso interviene la Auditoría Informática de Seguridad.
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus Sistemas Informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a aplicaciones independientes. En este caso interviene la Auditoría Informática de Datos.
- Un Sistema Informático mal diseñado puede convertirse en una herramienta peligrosa para la empresa: como las maquinas obedecen ciegamente a las órdenes recibidas y la modelización de la empresa está determinada por las computadoras que materializan los Sistemas de Información, la gestión y la organización de la empresa no puede depender de un software y hardware mal diseñados. Estos son solo algunos de los varios inconvenientes que puede presentar un Sistema Informático, por eso, la necesidad de la Auditoría de Sistemas.

La auditoría en informática se enfoca en evitar la interrupción de las operaciones del negocio y, al mismo tiempo, busca salvaguardar los activos relacionados de manera natural con el campo de acción de la informática.

Los auditores en informática dirigirán la participación directa y entusiasta del personal de informática y de los usuarios involucrados durante la auditoría. Cada proyecto de la auditoría se orienta al cumplimiento de normas, procedimientos y estándares, tanto de auditoría como de informática, comúnmente aceptados.

1.3 Concepto de Informática

El concepto de informática en los últimos años ha venido a revolucionar completamente la visión del personal informático, esto es consecuencia de los cambios tecnológicos y la importancia de los recursos informáticos para las organizaciones.

Una definición del concepto de informática dada en la conferencia del 5 al 9 de diciembre de 1983 en el Centro de Informática de la Facultad de Contaduría y Administración (CIFCA) de la Universidad Nacional Autónoma de México la conceptúa como: *"No existe una concepción acerca de qué es informática: etimológicamente la palabra informática deriva del francés* ***informatique.*** *Este neologismo proviene de la conjunción de* ***information*** *(información) y* ***automatique*** *(automática). Su creación fue estimulada por la intención de dar una alternativa menos tecnológica y menos mecanicista al concepto de* ***"proceso de datos"***[3]

1.3.1 Alcance de la Auditoría Informática

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática, misma que se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. Ejemplo: ¿Se someterán los registros grabados a un control de integridad exhaustivo? ¿Se comprobará que los controles de validación de errores son adecuados y suficientes? La indefinición de los alcances de la auditoría compromete el éxito de la misma.

- Control de integridad de registros:
  Hay aplicaciones que comparten registros, son registros comunes. Si una aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

- Control de validación de errores:
  Se corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente.

1.3.2 Características de la Auditoría Informática

La información de la empresa y para la empresa, siempre importante, se ha convertido en un Activo Real de la misma, como sus stocks o materias primas si las hay. Por ende, han de realizarse inversiones informáticas, materia de la que se ocupa la Auditoria de Inversión Informática.

[3] Boletín del Centro de Informática de la FCA, UNAM, núm. 99, Vol. 11, mayo de 1984

Del mismo modo, los Sistemas Informáticos han de protegerse de modo global y particular: a ello se debe la existencia de la *Auditoría de Seguridad Informática* en general, o a la *Auditoría de Seguridad* de alguna de sus áreas, como pudieran ser Desarrollo o Técnica de Sistemas. Cuando se producen cambios estructurales en la informática, se reorganiza de alguna forma su función: esto implica que se esta en el campo de la *Auditoría de Organización Informática.*

Estos tres tipos de auditorías engloban a las actividades auditoras que se realizan en una auditoría parcial, de otra manera: cuando se realiza una Auditoría del área de Desarrollo de Proyectos de la informática de una empresa, es porque en ese desarrollo existen, además de ineficiencias, debilidades de organización, o de inversiones, o de seguridad, o alguna mezcla de ellas.

1.3.3 Campos de la Auditoría en Informática[1]

El campo de acción de la auditoría en informática es:

- La evaluación administrativa del área de informática
- La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información. La evaluación de la eficiencia y eficacia con la que se trabaja
- La evaluación del proceso de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, base de datos, comunicaciones)
- Seguridad y confidencialidad de la información
- Aspectos generales de los sistemas y de la información
- La evaluación de controles generales aplicados a las normas de auditoría con una metodología como COSO o CoBIT

Para el correcto análisis e interpretación de los puntos antes señalados se necesita:

A. Evaluación administrativa del departamento de informática. Esto comprende la evaluación de:

    - Los objetivos del departamento, dirección o gerencia
    - Metas, planes, políticas y procedimientos de procesos electrónicos establecidos
    - Organización del área y su estructura orgánica
    - Funciones y niveles de seguridad y responsabilidad del área de procesos electrónicos
    - Integración de los recursos materiales
    - Dirección
    - Costos y controles presupuestales

[1] Auditoria Informática, José Antonio Echenique García, 2ª Edición pp 20.

- Controles administrativos del área de procesos electrónicos

B. Evaluación de los sistemas y procedimientos y de la eficiencia y eficacia que se tienen en el uso de la información. lo cual comprende:

- Evaluación del análisis de los sistemas y sus diferentes grupos
- Evaluación del diseño lógico del Sistema
- Evaluación del desarrollo físico del sistema
- Facilidades para la elaboración de los sistemas
- Control de proyectos
- Control de sistemas y programación
- Instructivos y documentación
- Formas de implantación
- Seguridad física y lógica de los sistemas
- Confidencialidad de los sistemas
- Controles de mantenimiento y forma de respaldo de los sistemas
- Utilización de los sistemas
- Prevención de factores que puedan causar contingencias: seguros y recuperación en caso de desastre
- Productividad
- Derechos de autor y secretos industriales

C. Evaluación del proceso de datos y de los equipos de cómputo que comprende:

- Controles de los datos fuente y manejo de cifras de control
- Control operación
- Control de salida
- Control de asignación de trabajo
- Control de medios de almacenamiento masivos
- Control de otros elementos de cómputo
- Control de medios de comunicación
- Orden en el centro de cómputo

D. Seguridad:

- Seguridad física y lógica
- Confidencialidad
- Respaldos
- Seguridad del personal
- Seguros
- Seguridad en la utilización de los equipos
- Plan de contingencias y procedimientos de respaldo para casos de desastre
- Restauración de equipo y de sistemas

La auditoría informática debe evaluar todo el funcionamiento de la organización, con un enfoque apegado a las normas de auditoría administrativa, auditoría interna, auditoría

contable/financiera y a su vez, proporcionar información confiable, oportuna, verídica y manejarse en forma segura y con la suficiente confidencialidad para la toma de decisiones.

Si es cierto que la auditoría informática lleva un enfoque administrativo/contable, también lo es que los sistemas de información en conjunto a las Tecnologías de Información están siendo día con día parte fundamental del desarrollo de las empresas, sean públicas y/o privadas, por lo que conlleva a que el área informática sea altamente evaluada y controlada para evitar desastres económico-financieros, al ver a toda entidad no solo como un empresa, sin importar su condición, sino como un ente que con o sin lucro, debe monitorear constantemente sus sistemas de información.

1.3.4 Desafíos de la Auditoría Interna

La función de auditoría interna y sus tradicionales esquemas de trabajo se han visto impactados por la evolución de los sistemas de Tecnología de Información y por la aplicación de nuevas estrategias administrativas motivadas por las necesidades de los negocios de expandir sus segmentos de mercado y por la diversificación y aseguramiento de la calidad en sus productos y servicios.

Estas realidades han propiciado que la demanda de los servicios de auditoría cobre fuerza en la actualidad; en este sentido los profesionales dedicados a la práctica de la auditoría interna, desde sus diversos ámbitos de actuación, buscan y desarrollan nuevos modelos de trabajo que satisfagan los requerimientos presentes de las organizaciones.

Sin embargo, así mismo se debe reflexionar que la implantación de estos nuevos modelos de evaluación puede revolucionar los servicios que actualmente la auditoría interna proporciona a la organización, con la perspectiva de ofrecer más con menos recursos.

Para que estos nuevos modelos funcionen se necesita un cambio radical en la cultura y esquemas de control en las organizaciones mismo que deberá estar soportado por la decisión de los más altos niveles directivos de la misma.

En este ámbito de transformación de la auditoría interna, los sistemas informáticos de la organización representan un reto y una solución cuando son utilizados como un medio de evaluación constante de controles. A través de las técnicas para la evaluación de operaciones procesadas a través de sistemas informáticos se podrá desarrollar un sistema automatizado de revisión, el cual permitirá a la auditoría cambiar de un enfoque de revisión periódica a un enfoque de revisión constante.

Mediante los desarrollos anteriores y sin descuidar el cumplimiento estricto de las normas internacionales emitidas para la práctica profesional de la auditoría interna y de las funciones prevista en su manual de organización, la auditoría interna espera enfrentar los retos presentes y los que le demande el inminente siglo XXI.

1.4 Objetivos Generales de la Auditoría Informática

Lo que podemos definir como Objetivos Generales que toda Auditoría Informática, o bien Auditoría de Sistemas de Información se engloban en una serie de consideraciones a tomar en forma general, buscando siempre una homogeneidad, veracidad y controles. A continuación haremos mención de los objetivos generales que toda Auditoría Informática debe perseguir:

- Proporcionar administración con razonable seguridad de que se lograrán los objetivos de control.[5]
- Identificar las debilidades del control, además de sustentar los resultados de riesgos
- Proponer recomendaciones sobre acciones correctivas y preventivas.
- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados, diseñados e implantados.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados.
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad de personal, datos, hardware, software e instalaciones.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de Tecnología de Información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los Sistemas de Información.

[5] Curso CoBIT. Expositor: Segura González, Juan Antonio CISA, CISM

CAPÍTULO 2. Marcos de Referencia COSO y CoBIT

2.1 Modelo COSO

La auditoría en informática, es el proceso de recolección y evaluación de evidencias para determinar cuándo son salvaguardados los activos de los sistemas de información, de qué manera se mantiene la integridad de los datos y cómo se logran los objetivos de la organización eficazmente y se usan los recursos consumidos eficientemente.[6]

En un ambiente de evolución permanente, determinado por las actuales tendencias mundiales, las cuales se centran en el plano económico soportadas por la evolución tecnológica, surge la necesidad de que la función de auditoría interna pretenda el mejoramiento de su gestión.

Los tópicos que se comentan a continuación se refieren a la práctica de nuevas técnicas para evaluar el control interno a través de las cuales la función de auditoría interna pretende mejorar la efectividad de su función y con ello ofrecer servicios más eficientes y con un valor agregado.

2.1.1 Concepto de Control Interno

Diferentes grupos de interés de Canadá, Estados Unidos, Reino Unido, Francia, Nueva Zelanda y otros países han realizado considerables esfuerzos para definir formalmente los objetivos y elementos del control interno y establecer los respectivos roles de todos los interesados incluyendo la junta directiva, los directivos, los jefes de mando medio, los supervisores y empleados.

Las definiciones emergentes convergen hacia los siguientes conceptos claves:

- El control interno es un proceso dirigido hacia el logro de objetivos
- La gente de todos los niveles de la organización comparte la responsabilidad de diseñar, implementar y mantener el control interno.
- El control interno solo provee garantía razonable de que los objetivos se están logrando.
- El control interno está sujeto a la intervención humana.
- Los controles pueden minimizar la ocurrencia de errores pero no pueden asegurar su total prevención.

De acuerdo con los conceptos anteriores, la Comisión Treadway[7] estableció la siguiente definición de control interno la cual ha sido adoptada ampliamente a nivel internacional.

---

[6] Auditoría en Informática Segunda Edición. Echenique García, José Antonio. Edit. McGraw-Hill Página 26

[7] Comité conformado por: American Institute of Certified Public Accountants, American Accounting Association, The Institute of Internal Auditors, Institute of Management Accountants y Financial Executives Institute.

"El control interno es un proceso llevado a cabo por la junta directiva de la entidad, los directivos y otro personal designado para proveer garantía razonable en cuanto al logro de objetivos en las tres siguientes categorías:

- Eficiencia y eficacia de las operaciones
- Confiabilidad de los estados financieros.
- Cumplimiento con las políticas y procedimientos internos y con las leyes y regulaciones aplicables".

2.1.2 Evaluación del Control Interno

En la evolución de la teoría del control interno se definió en principio a los controles como mecanismos o prácticas para prevenir o identificar actividades no autorizadas. más tarde se incluyó el concepto de lograr que las cosas se hagan: la corriente actual define al control como cualquier esfuerzo que se realice para aumentar las posibilidades de que se logren los objetivos de la organización.

En este proceso evolutivo se considera actualmente, y en muchas organizaciones, al Director de Finanzas. Contralor o al Director de Auditoría como los responsables principales del correcto diseño y adecuado funcionamiento de los controles internos.

A la auditoría externa también le corresponde evaluar el control interno contable de acuerdo a los parámetros establecidos en las Normas de Auditoría Generalmente Aceptados.

2.1.3 Objetivos de Control Interno

Como se mencionó con anterioridad, el logro de objetivos que persigue el modelo COSO se refiere a:

- Efectividad y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y ordenamientos.

Dichos objetivos deben ser definidos de modo que puedan identificar los criterios para medir el rendimiento y establecer factores críticos de éxito (que pueden ser a nivel de actividad o unidad operacional), coherentes y compatibles.

Cabe hacer mención que el primer objetivo (Eficacia y Eficiencia de las operaciones) se ubica justamente en el Objetivo de Actividades de Control (Control Activities) del Modelo COSO.

Mientras que los siguientes objetivos (Confiabilidad de la información financiera –que profundizaremos en el Capítulo 4 del presente trabajo – y Cumplimiento de las leyes y ordenamientos) se ubican dentro del Ambiente de Control (Control Environment)

2.1.4 Importancia del Control Interno

Para este modelo, el control interno es:

- El corazón de una organización
- La cultura, las normas sociales y ambientales que la gobiernan.
- Los procesos del negocio (Los mecanismos por medio de los cuales una organización proporciona bienes y/o servicios de valor agregado).
- La infraestructura, la tecnología de la información, las actividades, las políticas y los procedimientos.

2.2 Marco de Referencia COSO[8]

La actual definición del control interno emitida por The Committee of Sponsoring Organizations of the Treadway Commission de los Estados Unidos de Norteamérica, a través del documento denominado "Control Interno-Marco Integrado" mejor conocido como el Modelo de Control COSO, amplia el concepto de la siguiente manera:

"...un proceso... efectuado por la Junta Directiva de la entidad, por la Administración y por otro personal... diseñado para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos..."[9]

En este sentido se entiende que el control interno se encuentra sobre las personas y, en consecuencia, en cualquier parte de los sistemas, procesos, funciones o actividades y no en forma separada como teóricamente se pudiera interpretar de los enunciados del proceso administrativo, que declara que la administración organiza, planea, dirige y controla.

MODELO DE CONTROL INTERNO COSO

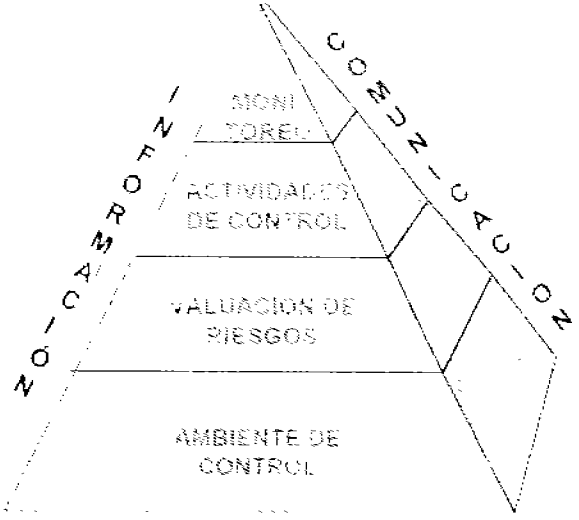

Figura 1. Estructura del Modelo COSO

Teniendo la infraestructura apropiada se debe pensar en los posibles problemas que se pueden presentar y que impedirán el logro de los objetivos fijados o en otras palabras qué riesgos debe enfrentar la empresa. Cuando son identificados dichos riesgos el siguiente paso consiste en minimizarlos utilizando controles. Sin embargo, es claro que para mantener un efectivo sistema de control de la organización, la información y los canales de

[8] Committee of Sponsoring Organizations of the Treadway Commission.
[9] V Reunión de Auditores Internos de Banca Central, Cruz, Jorge, 16 Páginas

comunicación son claves y las actividades de monitoreo permiten detectar las desviaciones que dificultarán la consecución de los objetivos.

Con esta breve ilustración (figura 1), a continuación se describen los cinco elementos: **Ambiente de control (Control Environment), Valoración de riesgos (Risk Assessment), Actividades de control (Control Activities), Información y comunicación (Information and Communication) y Monitoreo (Monitoring)**, tal como son presentados en el Control Interno-Marco Integrado publicado por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway, ampliamente conocida como **COSO**.

2.2.1 Estructura del Control Interno

La estructura del control interno, propuesta por el modelo COSO, identifica cinco componentes interrelacionados:

- Ambiente de Control (Control Environment)
- Evaluación de riesgos (Risk Assessment)
- Actividades de control (Control Activities)
- Información y comunicación (Information and Communication)
- Monitoreo (Monitoring)

2.2.1.1 Ambiente de Control

El ambiente de control (Control Environment) es el elemento que proporciona disciplina y estructura. El ambiente de control se determina en función de la integridad y competencia del personal de una organización: los valores éticos son un elemento esencial que afecta a otros componentes del control. Entre sus factores se incluye la filosofía de la administración, la atención y guía proporcionados por el consejo de administración, el estilo operativo, así como la manera en que la gerencia confiere autoridad y asigna responsabilidades, organiza y desarrolla a su personal.

Define el tono de una organización influenciando la conciencia de control de su gente. Es el cimiento para todos los otros elementos del control interno, suministrando disciplina y estructura. Los factores del Ambiente de Control incluyen la integridad, los valores éticos y la competencia de la gente de la entidad, la filosofía de la administración y el estilo operacional, la forma cómo la administración asigna autoridad y responsabilidad y organiza y desarrolla a su gente y la atención y dirección provista por la Junta Directiva.

Un adecuado Ambiente de Control se verifica por medio de 7 aspectos fundamentales:

1. Integridad y valores éticos
2. Compromiso de competencia profesional

3. Filosofía de dirección y el estilo de gestión
4. Estructura Organizacional
5. Asignación de autoridad y responsabilidad
6. Políticas y Prácticas de Recursos Humanos
7. Consejo de Administración / Comité de Auditoría

2.2.1.2 Evaluación de Riesgos

La evaluación de riesgos (Risk Assessment) se define como la identificación y análisis de los riesgos que se relacionan con el logro de los objetivos: la administración debe cuantificar su magnitud, proyectar su probabilidad y sus posibles consecuencias.

En la dinámica actual de los negocios, se debe prestar especial atención a:

- Los avances tecnológicos.
- Los cambios en los ambientes operativos.
- Las nuevas líneas de negocios.
- La reestructuración corporativa.
- La expansión o adquisiciones extranjeras.
- El personal de nuevo ingreso.
- El rápido crecimiento.

El enfoque no se determina en el uso de una metodología particular de evaluación de riesgos, sino en la realización de la evaluación de riesgos como una parte natural del proceso de planeación.

Se define como riesgo la probabilidad de que un suceso ocurra y provoque pérdidas.

Cada entidad enfrenta una variedad de riesgos de fuentes internas y externas que deben ser evaluadas. La evaluación de riesgos comprende su identificación y análisis, conformando una base para determinar como los riesgos deben ser manejados.

Es necesario entonces, que la organización posea mecanismos para identificar y manejar riesgos nuevos debido a las condiciones cambiantes de la economía, industria, condiciones reglamentarias y operacionales.

Un adecuado análisis de riesgos se verifica por medio de 4 aspectos:

1. Objetivos Organizacionales Globales
2. Objetivos asignados a cada Actividad
3. Identificación de Riesgos
4. Administración del Riesgo y Cambio

2.2.1.3 Actividades de Control

Las actividades de control (Control Activities) ocurren a lo largo de la organización, en todos los niveles y todas las funciones, incluyendo los procesos de aprobación, autorización, conciliaciones, etc. Las actividades de control se clasifican en:

- Controles preventivos.
- Controles detectivos.
- Controles correctivos.
- Controles manuales o de usuario.
- Controles de cómputo o de tecnología de información.
- Controles administrativos.

Las actividades de control deben ser apropiadas para minimizar los riesgos; el personal realiza cada día una gran variedad de actividades específicas para asegurarse que la organización se adhiera a los planes de acción y al seguimiento de la consecución de objetivos.

Entre los puntos más importantes que deben cubrir las Actividades de Control se encuentran:

- Referencias a las políticas y procedimientos que ayudan a asegurar que los objetivos de la organización se lleven a cabo.
- Ayudar a asegurar que se tomen acciones necesarias para atacar riesgos y lograr los objetivos de la entidad.
- Ocurrencia a través de toda la organización, a todos los niveles y en todas las funciones.
- Incluir una gran y variada gama de actividades como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones de comportamiento operacional, seguridad de activos y segregación de tareas, entre otras.

Las actividades de control se pueden dividir en cuatro categorías, basadas en la naturaleza de los objetivos de la entidad con las cuales se relaciona: **operación, información financiera, cumplimiento y salvaguarda de activos**. Si bien algunos de los controles se relacionan con un área a menudo se sobreponen, dependiendo de las circunstancias una actividad particular de control puede ayudar a satisfacer los objetivos en mas de una de las cuatro categorías de objetivos, así, los controles de operación también pueden ayudar a asegurar información financiera confiable, los controles de información financiera pueden servir para efectuar cumplimiento y así todo lo demás.

COSO reconoce las siguientes actividades de control:

1. Análisis efectuados por la dirección
2. Administración directa de funciones por actividades
3. Proceso de información
4. Controles físicos contra los registros

5. Indicadores de rendimiento
6. Segregación de funciones
7. Políticas y procedimientos

2.2.1.4 Información y Comunicaciones

En este elemento del sistema de control interno (Information and Communication) se diferencian la información de la comunicación, en que la primera son los datos necesarios para cumplir con las funciones y la comunicación es la manera como la información fluye.

La información pertinente debe ser identificada, capturada y comunicada de cierta forma y dentro de un marco de tiempo que permita a la gente cumplir con sus responsabilidades. Los sistemas de información producen reportes que contienen información relacionada con aspectos operacionales, financieros y de cumplimiento que hacen posible el manejo y control de la organización.

Este elemento del modelo no sólo está relacionado con la información generada internamente, sino también con la información de eventos externos.

Una comunicación eficaz debe ocurrir en un sentido amplio, circulando hacia abajo, hacia arriba y a través de toda la organización. Todo el personal debe recibir un mensaje claro de la alta dirección que controla las responsabilidades y el personal debe tener medios para comunicar información significativa hacia arriba. Además, todos los individuos deben entender su propio rol en el sistema de control interno, así como la manera en que sus actividades individuales se relacionan o afectan el trabajo de los demás. Adicionalmente, se necesita tener una comunicación eficaz con los interesados externos, tales como clientes, proveedores, reguladores y accionistas.

Se debe generar información relevante y comunicarla oportunamente, de tal manera que permita a las personas entenderla y cumplir con sus responsabilidades.

Una evaluación adecuada de mecanismos de información, se forma de:

1. La información interna y externa que provee a la Dirección los reportes necesarios para el establecimiento de objetivos organizacionales
2. La información proporcionada a las personas adecuadas con suficiente detalle y oportunidad para cumplir con sus responsabilidades
3. Los Sistemas de Información están basados en un "Plan Estratégico" (vinculados a la estrategia global de la organización)
4. Apoyo de la dirección al desarrollo de los sistemas de información necesarios (aporte de los recursos adecuados, tanto humanos como financieros)

Por el contrario, una evaluación adecuada de mecanismos de comunicación se enfoca a:

1. La comunicación al personal, es eficaz en la descripción de sus funciones y responsabilidades con respecto al control Interno.
2. El establecimiento de canales de comunicación para la denuncia de posibles actos indebidos.
3. La alta dirección es receptiva a sugerencias de los empleados.
4. La comunicación a través de toda la empresa es efectiva.
5. Seguimiento oportuno y adecuado de la dirección de la información obtenida de clientes, proveedores, organismos de control y otros terceros.

2.2.1.5 Monitoreo

Los sistemas de control interno necesitan ser monitoreados constantemente para asegurarse que el proceso se encuentra operando como se planeó y comprobar que son efectivos ante los cambios de las situaciones que les dieron origen. El alcance y la frecuencia del monitoreo dependen de los riesgos que se pretenden cubrir. El monitoreo es un proceso que evalúa la calidad del comportamiento de los sistemas a través del tiempo.

Las actividades de monitoreo constante pueden ser implantadas en los propios procesos del negocio o a través de evaluaciones separadas de la operación, es decir, mediante auditoría interna o externa.

- Los controles internos se deben implementar en los procesos del negocio, sin inhibir el desarrollo del proceso operativo.
- Los controles que hacen que la ejecución sea lenta, son evitados, lo cual puede ser más dañino que no tener controles, debido al falso sentido de seguridad.
- Los controles son efectivos cuando en los procedimientos no se les recuerda constantemente de su existencia.

Los sistemas de control interno cambian con el tiempo. La manera como se aplican los controles tiene que evolucionar. Debido a que los procedimientos pueden tornarse menos efectivos, o quizás no se desempeñen ampliamente.

Ello puede ocurrir a causa de la llegada de personal nuevo, la variación de la efectividad del entrenamiento y la supervisión, la reducción de tiempo y recursos u otras presiones adicionales. Además, las circunstancias para las cuales se diseñó el sistema de control interno pueden cambiar, originando que se llegue a ser menos capaz de anticiparse a los riesgos originados por las nuevas condiciones. Por consiguiente, la administración necesita determinar si el sistema de control interno continúa siendo relevante y capaz de manejar los nuevos riesgos.

El monitoreo asegura que el control interno continúa operando efectivamente. Este proceso implica la valoración, por parte del personal apropiado, del diseño y de la operación de los controles en una adecuada base de tiempo y realizando las acciones necesarias. Se aplica

para todas las actividades en una organización, lo mismo que algunas veces para contratistas externos. Por ejemplo, el outsourcing del procesamiento.

El monitoreo puede hacerse de tres maneras: **mediante actividades sobre la marcha o mediante evaluaciones separadas o a través de una combinación de las dos.** Los sistemas de control interno usualmente se estructurarán para monitorearse a sí mismos sobre una base de monitoreo sobre la marcha en algún grado. A mayor grado de efectividad del monitoreo sobre la marcha, se necesitan menos evaluaciones separadas. La frecuencia de las evaluaciones separadas necesarias para que la administración tenga una seguridad razonable respecto de la efectividad del sistema de control interno es asunto del juicio de la administración. Para tomar tal determinación deben hacerse las siguientes consideraciones: la naturaleza y el grado de cambios que ocurren y sus riesgos asociados, la competencia y la experiencia de la gente en la implementación de los controles, lo mismo que los resultados del monitoreo sobre la marcha. Usualmente, alguna combinación de monitoreo sobre la marcha y evaluaciones separadas asegurará que el sistema de control interno mantenga su efectividad en el tiempo.

Debe reconocerse que los procedimientos de monitoreo sobre la marcha se construyen en las actividades normales, repetitivas, de una entidad. Puesto que se desempeñan con una base de tiempo real, reaccionan dinámicamente a las condiciones cambiantes y están integrados en la entidad, son más efectivos que los procedimientos desempeñados en evaluaciones separadas. Dado que las evaluaciones separadas se realizan luego de los hechos, los problemas a menudo serán identificados más rápidamente por las rutinas de monitoreo sobre la marcha. Algunas empresas con sólidas actividades de monitoreo sobre la marcha conducirán al menos a una evaluación separada de sus sistema de control, o de parte del mismo cada uno o dos años. Una entidad que percibe una necesidad de evaluaciones separadas frecuentes deberá centrarse en mejorar sus actividades de monitoreo sobre la marcha y por consiguiente enfatizar en construir controles inmersos en las actividades en vez de añadirlos.

2.2.1.5.1 Monitoreo sobre la marcha

Son múltiples las actividades que sirven para monitorear la efectividad del control interno en el curso ordinario de las operaciones. Incluyen actos regulares de administración y supervisión, comparaciones, conciliaciones, aprobaciones, arqueos y otras acciones rutinarias.

Los siguientes son ejemplos de actividades de monitoreo sobre la marcha:

- En el desarrollo de las actividades regulares de administración, la gestión operativa obtiene evidencia de que el sistema de control interno continúa funcionando cuando los reportes de operación están integrados o se concilian con el sistema de información financiera y se usan para administrar operaciones en una base de monitoreo sobre la marcha, las inexactitudes o excepciones significativas a los resultados anticipados es probable que sean detectadas fácilmente. La efectividad

del sistema de control interno es aumentada mediante la información oportuna y completa y mediante la solución de esas excepciones.

- Las comunicaciones recibidas de partes externas corroboran la información generada internamente o señalan problemas. Las entidades financieras corroboran implícitamente los datos de saldos al no elevar quejas o reclamos. Mediante el diálogo u otros medios, los reclamos de los clientes respecto a los saldos pueden indicar deficiencias sistémicas en el procesamiento de la información De la misma manera, los reguladores también pueden comunicarse con la entidad respecto del cumplimiento u otros asuntos que se reflejan en el funcionamiento del sistema de control interno.

- La estructura organizacional apropiada y las actividades de supervisión proporcionan una visión amplia de las funciones de control y de la identificación de deficiencias. Por ejemplo, la revisión de las tareas entre diferentes individuos sirve par prevenir el fraude de empleados puesto que inhibe la habilidad de un individuo para encubrir sus actividades sospechosas.

- Los datos registrados mediante los sistemas de información se comparan con las existencias físicas. Los inventarios de productos terminados, por ejemplo, se pueden examinar periódicamente.

Puede verse que cada una de esas actividades de monitoreo sobre la marcha orienta aspectos importantes de cada uno de los componentes del control interno.

2.2.1.5.2 Evaluaciones separadas:

Mientras que los procedimientos de monitoreo sobre la marcha usualmente proporcionan retroalimentación importante sobre la efectividad de otros elementos de control, puede ser útil tomar de tiempo en tiempo una mirada centrada directamente en la efectividad del sistema. Ello también proporciona una oportunidad para considerar la continua efectividad de los procedimientos de monitoreo sobre la marcha.

Las evaluaciones del control interno varían en alcance y frecuencia, dependiendo del significado de los riesgos que están siendo controlados y de la importancia de los controles en la reducción de aquellos. Los controles que se orientan a riesgos de prioridad alta y a aquellos más críticos para reducir un riesgo dado, tenderán a ser evaluados más frecuentemente. La evaluación de un sistema de control interno completo – que será necesitada con menos frecuencia que la valoración de controles específicos – puede motivarse por diversas razones: estrategia principal o cambio administrativo, adquisiciones y disposiciones, o cambios significativos en las operaciones o en los métodos de procesamiento de información financiera. Cuando se toma una decisión para evaluar el sistema de control interno completo de una entidad, la atención se debe dirigir a cada uno de los elementos del control interno con respecto a todas las actividades significativas.

El alcance de la evaluación también dependerá de las categorías de objetivos – gestión, información financiera, cumplimiento y salvaguarda de activos – a los cuales está orientado.

A menudo, las evaluaciones toman la forma de auto-valoraciones, en las que las personas responsables por una unidad o función particular determinan la efectividad de los controles para sus actividades.

Los auditores internos normalmente realizan evaluaciones del control interno como parte de sus obligaciones regulares, o por petición especial de la alta dirección. De la misma manera, la administración puede usar el trabajo de los auditores externos para considerar la efectividad del control interno. Puede emplearse una combinación de esos esfuerzos para conducir cualquiera de los procedimientos de evaluación que la administración considere necesarios.

Cada elemento afecta a todos los demás y el funcionamiento e interrelación de todos ellos originan un sistema integrado que reacciona dinámicamente ante las condiciones cambiantes. Así, por ejemplo, si se desmejora el ambiente de control, los riesgos a afrontar cambiarán y por ende los controles, las funciones de supervisión y el tipo de información y comunicación necesaria.

2.3 Modelo CoBIT[10]

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de la información y de la Tecnología de Información (TI) Relacionada. En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) esta criticidad emerge de:

- La creciente dependencia en información y en los sistemas que proporcionan dicha información
- La creciente vulnerabilidad y un amplio espectro de amenazas, tales como las "ciber amenazas" y la guerra de información
- La escala y el costo de las inversiones actuales y futuras en información y en Tecnología de Información; y
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos

Para muchas organizaciones, la información y la tecnología que la soporta, representan los activos más valiosos de la empresa. Es más, en nuestro competitivo y rápidamente cambiante ambiente actual, la Gerencia ha incrementado sus expectativas relacionadas con la entrega de servicios de TI. Por lo tanto, la administración requiere niveles de servicio que presenten incrementos en calidad, en funcionalidad y en facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega; al tiempo que demanda que esto se realice a un costo más bajo.

Muchas organizaciones reconocen los beneficios potenciales que la tecnología puede proporcionar. Las organizaciones exitosas, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nuevas tecnologías.

La dependencia en la información electrónica y en los sistemas de TI es esencial para soportar los procesos críticos del negocio. Adicionalmente, el ambiente regulatorio demanda control estricto sobre la información. Esto a su vez conduce a un incremento de los desastres en los sistemas de información y al incremento del fraude electrónico. La administración de los riesgos relacionados con TI está siendo entendida como un aspecto clave en el gobierno o dirección empresarial.

Dentro del Gobierno Empresarial, el Gobierno / Gobernabilidad de TI[11] se está volviendo más y más importante y está definido como una estructura de relaciones y procesos para dirigir y controlar a la empresa con el fin que ésta pueda cumplir sus metas dando valor agregado mientras balancea sus riesgos versus el retorno sobre TI y sus procesos. El

[10] CoBIT Objetivos de Control. Tercera Edición, Comité Directivo de CoBIT & IT Governance Institute Página 5

[11] Gobierno de TI (IT Governance) Governance es un término que representa el sistema de control o administración que establece la alta gerencia para asegurar el logro de los objetivos de una Organización.

Gobierno de TI es parte integral del éxito de la Gerencia de la empresa al asegurar mejoras medibles, eficientes y efectivas de los procesos relacionados de la empresa.

El Gobierno de TI provee las estructuras que unen los procesos de TI, los recursos de TI y la información con las estrategias y los objetivos de la empresa. Además, el Gobierno de TI integra e institucionaliza buenas prácticas de Planeación y Organización, Adquisición e Implementación, Entrega de servicios y Soporte y Monitorea el desempeño de Tecnologías de Información para asegurar que la información de la empresa y las tecnologías relacionadas soportan sus objetivos del negocio. El Gobierno de TI conduce a la empresa a tomar total ventaja de su información logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva

Las organizaciones deben cumplir con requerimientos de calidad, fiduciarios y de seguridad, tanto para su información, como para sus activos. La administración deberá además optimizar el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus objetivos, la administración debe entender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

La administración debe asegurar que los sistemas de control interno o el marco referencial están funcionando y soportan los procesos del negocio y debe tener claridad sobre la forma como cada actividad individual de control satisface los requerimientos de información e impacta los recursos de TI. El impacto sobre los recursos de TI son resaltados en el Marco de Referencia de CoBIT junto con los requerimientos del negocio que deben ser alcanzados: eficiencia, efectividad, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración. La administración, mediante este gobierno corporativo, debe asegurar que todos los individuos involucrados en la administración, uso, diseño, desarrollo, mantenimiento u operación de sistemas de información actúen con la debida diligencia.

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI.

La orientación al negocio es el tema principal del marco de referencia CoBIT. Está diseñado no solo para ser utilizado por usuarios y auditores, sino que, lo más importante, esta diseñado para ser utilizado por los propietarios de los procesos de negocio como una guía clara y entendible. A medida que ascendemos, las prácticas de negocio requieren de una mayor delegación y empoderamiento de los dueños de los procesos para que estos tengan total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En particular, esto incluye el proporcionar controles adecuados.

CoBIT proporciona, al propietario de procesos de negocio, herramientas que facilitan el cumplimiento de esta responsabilidad. El Marco de Referencia comienza con una premisa simple y práctica: *Con el fin de proporcionar la información que la empresa necesita para*

alcanzar sus objetivos, los recursos de TI deben ser administrados por un conjunto de procesos de TI agrupados en forma natural[12]

El Marco de Referencia continúa con un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios: Planeación y Organización, Adquisición e Implementación, Entrega de servicios y Soporte y Monitoreo. Esta estructura cubre todos los aspectos de información y de tecnología que la soporta. Administrando adecuadamente estos 34 Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información.

El Marco de Referencia de CoBIT provee además una guía o lista de verificación para el Gobierno de TI. El Gobierno de TI proporciona las estructuras que encadenan los procesos de TI, los recursos de TI y la información con los objetivos y las estrategias de la empresa. El Gobierno de TI integra de una forma óptima el desempeño de la Planeación y Organización, la Adquisición e Implementación, la Entrega de servicios y Soporte y el Monitoreo. El Gobierno de TI facilita que la empresa obtenga total ventaja de su información y así mismo maximiza sus beneficios, capitalizando sus oportunidades y obteniendo ventaja competitiva

Adicionalmente, correspondiendo a cada uno de los 34 objetivos de control de alto nivel, existe una Guía o directriz de Auditoría o de aseguramiento que permite la revisión de los procesos de TI contra los 318 objetivos detallados de control recomendados por COBIT para proporcionar a la Gerencia la certeza de su cumplimiento y/o sugerencias para su mejoramiento.

2.3.1 Concepto de CoBIT

CoBIT, lanzado en 1996, como herramienta de gobierno de TI, ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, CoBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

CoBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Su misión es investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores

[12] CoBIT Objetivos de Control, Tercera Edición, Comité Directivo de CoBIT & IT Governance Institute Página 6

2.3.2 Historia y Antecedentes de CoBIT

La primera edición de CoBIT (Objetivos de control para Tecnologías de Información y Tecnologías Relacionadas), fue liberada por la Information Systems Audit and Control Foundation (ISACF) en 1996. La segunda edición que refleja un incremento en el número de documentos fuente, una revisión en el alto nivel y objetivos de control detallados y la adición del Conjunto de herramientas de Implementación fue publicada en 1998. La tercera edición (empleada para el desarrollo del presente proyecto) marca el ingreso de un nuevo editor para CoBIT: El Instituto de Gobernabilidad[13] de TI (IT Governance Institute).

El Instituto de Gobierno de TI fue formado por la Information Systems Audit and Control Association (ISACA) y su fundación asociada en 1998 para avanzar en el entendimiento y la adopción de principios de gobierno de TI. Con la adición de las Directrices Gerenciales en la tercera edición de CoBIT y su expansión y mayor cubrimiento sobre el Gobierno de TI, el Instituto de Gobierno de TI adquirió un rol de liderazgo en el desarrollo de la publicación.

CoBIT se basó originalmente en los Objetivos de Control de la ISACF[14] y ha sido mejorado con los actuales estándares internacionales a nivel técnico, profesional, regulatorio y específicos de la industria. Los objetivos de control resultantes han sido desarrollados para su aplicación en sistemas de información de toda la empresa.

El término "generalmente aplicable y aceptado" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés).

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades del negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización.

Sin excluir ningún otro estándar aceptado en el campo del control de sistemas de información que pudiera emitirse durante la investigación, las fuentes han sido identificadas inicialmente como:

- Estándares Técnicos de ISO, EDIFACT, etc.
- Códigos de Conducta emitidos por el Council of Europe, OECD, ISACA, etc.;
- Criterios de Calificación para sistemas y procesos de TI: ITSEC, ISO9000, SPICE, TickIT, Common Criteria, etc.;

[13] Gobierno (Governance): Sistema que establece la alta gerencia para asegurar el logro de los objetivos de una Organización.
[14] ISACF, Fundación de Auditores de Sistemas de Información y Control, fundada en 1996

- Estándares Profesionales para control interno y auditoría: reporte COSO, IFAC, IIA, ISACA, GAO, PCIE, CICA, AICPA, etc.;
- Prácticas y requerimientos de la Industria de foros industriales (ESF, 14) y plataformas patrocinadas por el gobierno (IBAG, NIST, DTI); y
- Nuevos requerimientos específicos de la industria de la banca, Comercio Electrónico y manufactura de TI.

Por lo que respecta a éste punto, CoBIT, en su tercera edición, evolucionará a través de los años y será el fundamento de investigaciones futuras. Por lo tanto, se generará una gama de productos de CoBIT y al ocurrir esto, las tareas y actividades que sirven como estructura para organizar los Objetivos de Control de TI, serán refinadas posteriormente. También será revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria. Por el momento, ISACA y el IT Governance Institute contemplan los siguientes productos de la familia CoBIT[15].

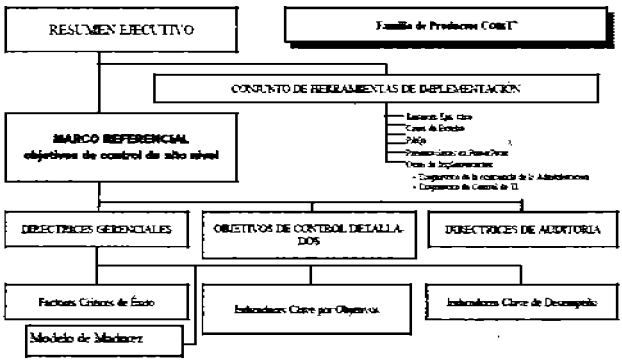

Figura 2 Productos de la Familia CoBIT

[15] CoBIT Objetivos de Control, Tercera Edición, Comité Directivo de CoBIT & IT Governance Institute Página 21

2.4 Marco de Referencia CoBIT

En los últimos años, ha sido cada vez más evidente la necesidad de un Marco Referencial para la seguridad y el control de Tecnología de Información (TI). Las organizaciones exitosas requieren una apreciación y un entendimiento básico de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles adecuados.

La administración debe decidir cual es la inversión razonable en seguridad y en control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos, no los eliminan. Adicionalmente, el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre.

Finalmente, la administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Juzgar cual puede ser el nivel tolerable, particularmente cuando se tiene en cuenta contra el costo, puede ser una decisión difícil para la administración. Por esta razón, la Administración necesita un marco de referencia de las prácticas generalmente aceptadas de control y seguridad de TI para compararlos contra el ambiente de TI existente y planeado.

Existe una creciente necesidad entre los usuarios de los servicios de TI, de estar protegidos a través de la acreditación y la auditoría de servicios de Tecnología de Información proporcionados internamente o por terceras partes, que aseguren la existencia de controles y seguridades adecuadas. Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación, tales como ITSEC, TCSEC, evaluaciones ISO9000, nuevas evaluaciones de control interno COSO, etc. Como resultado, los usuarios necesitan que se establezca una base general como un primer paso.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar su opinión acerca de los controles internos frente a la Gerencia. Sin contar con un marco referencial, ésta se convierte en una tarea demasiado complicada. Incluso, la administración consulta cada vez más a los auditores para que la asesoren en forma proactiva en lo referente a asuntos de seguridad y control de TI.

En pocas palabras, CoBIT se define como un modelo referencia que permite a la audiencia (administradores, usuarios, auditores) reducir los espacios existentes entre los riegos de negocio, las necesidades de control y los aspectos tecnológicos inherentes con el fin de lograr una adecuada gobernabilidad de los recursos de tecnología de información (COSO & CoBIT).

En efecto CoBIT apoya la gobernabilidad de los recursos de TI mediante la compresión y la administración de los riesgos asociados a las Tecnologías de Información a través de un

Marco Referencial de dominios, procesos y tareas estructuradas (actividades) en forma simple y lógica.

2.4.1 Ambiente de Negocios: Competencia, Cambio y Costos

Las organizaciones se reestructuran con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en TI para mejorar su posición competitiva. La reingeniería en los negocios, las reestructuraciones o rightsizing, el outsourcing, el empoderamiento, las organizaciones horizontales y el procesamiento distribuido son cambios que impactan la manera en la que operan tanto los negocios como las entidades gubernamentales. Estos cambios han tenido y continuarán teniendo, profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo. La especial atención prestada a la obtención de ventajas competitivas y a la eficiencia en costos implica una dependencia creciente en la tecnología como el componente más importante en la estrategia de la mayoría de las organizaciones. La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en las computadoras y en las redes, tanto para las basadas en hardware como las basadas en software.

Dentro del marco referencial de cambios acelerados, si los administradores, los especialistas en sistemas de información y los auditores desean en realidad ser capaces de cumplir con sus tareas en forma efectiva, deberán aumentar y mejorar sus habilidades tan rápidamente como lo demandan la tecnología y el ambiente. Debemos comprender la tecnología de controles involucrada y su naturaleza cambiante si deseamos emitir y ejercer juicios razonables y prudentes al evaluar las prácticas de control que se encuentran en los negocios típicos o en las organizaciones gubernamentales.

2.4.2 Gobierno de la Empresa y Gobierno de TI

Para lograr el éxito en esta economía de información, el Gobierno de la empresa (o Gobierno Corporativo) y el Gobierno de TI no pueden ser considerados en forma separada y en distintas disciplinas. El gobierno efectivo de la empresa enfoca el conocimiento y la experiencia en forma individual y grupal, donde puede ser más productivo, monitoreado y medido el desempeño así como provisto el aseguramiento para aspectos críticos. TI, por mucho tiempo considerada aislada dentro del logro de los objetivos de la empresa debe ahora ser considerada como una parte integral de la estrategia.

El Gobierno de TI provee la estructura que une los procesos y recursos de TI y las estrategias y objetivos de la empresa. El Gobierno de TI integra e institucionaliza de una manera óptima la planeación y organización, la adquisición e implementación, la entrega de servicios y soporte y el monitoreo del desempeño de TI. El Gobierno de TI es integral para el éxito del Gobierno Corporativo, asegurando una eficiente y efectiva medición para

mejorar los procesos de la empresa. El Gobierno de TI le permite a la empresa tomar ventaja total de su información, al maximizar sus beneficios, capitalizar sus oportunidades y ganar ventaja competitiva.

Observando en el contexto a la empresa y los procesos del Gobierno de TI con mayor detalle, el gobierno de la empresa, el sistema por el cual las entidades son dirigidas y controladas, direcciona y analiza el Gobierno de TI. Al mismo tiempo, TI debería proveer insumos críticos y constituirse en un componente importante de los planes estratégicos. De hecho TI puede influenciar las oportunidades estratégicas de la empresa.

GOBIERNO CORPORATIVO vs. GOBIERNO DE TI

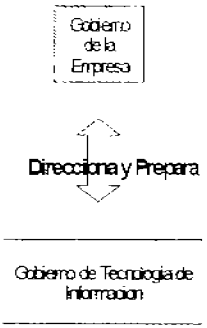

Figura 3 Gobierno Corporativo y Gobierno de TI

Las actividades de la empresa requieren información de las actividades de TI con el fin de satisfacer los objetivos del negocio. Organizaciones exitosas aseguran la interdependencia entre su plan estratégico y sus actividades de Tecnología de Información. TI debe estar alineado y debe permitir a la empresa tomar ventaja total de su información para maximizar sus beneficios, capitalizar oportunidades y ganar ventaja competitiva.

Las empresas son gobernadas por buenas prácticas generalmente aceptadas para asegurar que la empresa cumpla sus metas asegurando que lo anterior esté garantizado por ciertos controles. Desde estos objetivos fluye la dirección de la organización, la cual dicta ciertas actividades a la empresa usando sus propios recursos. Los resultados de las actividades de la empresa son medidos y reportados proporcionando insumos para el mantenimiento y revisión constante de los controles, comenzando el ciclo de nuevo.

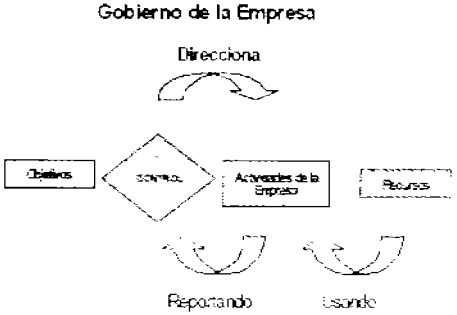

Figura 4 Resultados de las actividades del Gobierno de la Empresa

En contraparte, podemos encontrar 5 elementos claves dentro del Gobierno de TI[16], mismos que mencionamos a continuación para su mejor comprensión:

1. Asegurar que el Consejo de Administración/accionistas suministren un marco de trabajo para las TI's
2. Enfocarse sobre los resultados Financieros
3. Dirigir los cuatro activos (Infraestructura, Clientes y Terceros interesados (stakeholders), Personal Interno y Procesos, Creación de valor) en tres dimensiones: Cumplimiento, Desempeño y Responsabilidad (Rendición de cuentas) para establecer los estadios actual y futuro de la organización
4. Organización basada en el involucramiento de los interesados adecuados
5. Alinear todas las iniciativas y recursos de TI mediante el establecimiento de Niveles de Servicio que requieren ser administrados.

Figura 5 Activos a ser Dirigidos dentro del Gobierno de TI

[16] Sarbanes Oxley Retos y Realidades de la Ley. Ponencia: Importancia del Gobierno Corporativo y Gobierno de TI. Expositor: Carlos Zamora. ISACA. Cd. México

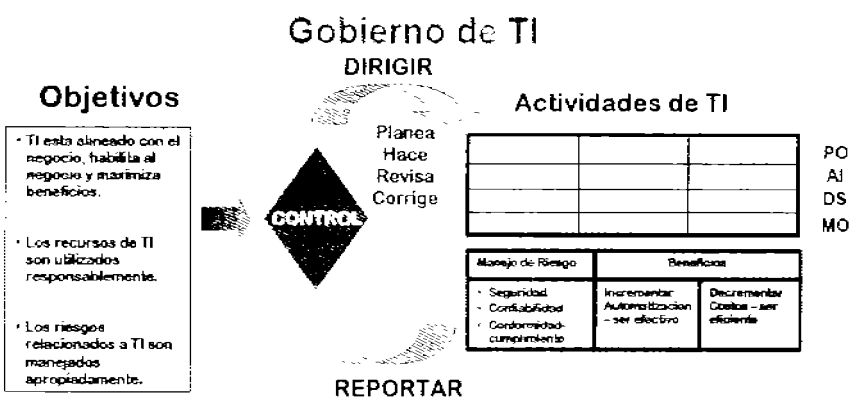

Figura 6 Gobierno de TI

Por lo tanto, el objetivo principal del proyecto CoBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. La meta del proyecto es desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa.

2.4.3 Los Principios del Marco de Referencia

Existen dos clases distintas de modelos de control actualmente disponibles, aquéllos de la clase del "modelo de control de negocios" y los "modelos más enfocados a TI". CoBIT intenta cubrir la brecha que existe entre los dos. Debido a esto, CoBIT se posiciona como una herramienta más completa para la administración y para operar a un nivel superior a los estándares de tecnología para la administración de sistemas de información. Por lo tanto, CoBIT es el modelo para el gobierno de TI

El concepto fundamental de CoBIT se refiere a que el enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

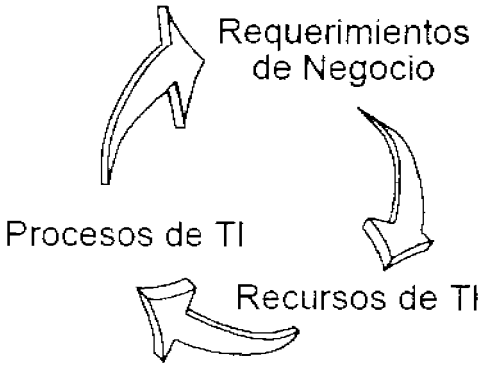

Figura 7 Principios del Marco de Referencia

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que CoBIT hace referencia como requerimientos de negocio para la información. Al establecer la lista de requerimientos, CoBIT combina los principios contenidos en los modelos referenciales existentes y conocidos:

2.4.3.1 Requerimientos de Calidad

La calidad ha sido considerada principalmente por su aspecto "negativo" (ausencia de fallas, confiabilidad, etc.), lo cual también se encuentra contenido en gran medida en los criterios de integridad. Los aspectos positivos, pero menos tangibles, de la calidad (estilo, atractivo, "ver y sentir", desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades.

El aspecto utilizable de la calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega o distribución del servicio de la calidad se traslapa con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el costo también es considerado, siendo cubierto por la eficiencia.

En resumen, los requerimientos de calidad son:

- Calidad
- Costo
- Entrega o Distribución

2.4.3.2 Requerimientos fiduciarios (COSO)

Para los requerimientos fiduciarios, se utilizaron las definiciones de COSO para la efectividad y eficiencia de las operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, confiabilidad de información fue ampliada para incluir toda la información, no sólo información financiera.

Los requerimientos fiduciarios, en resumen son:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de la información
- Cumplimiento de las leyes y regulaciones

2.4.3.3 Requerimientos de Seguridad

Con respecto a los aspectos de seguridad, CoBIT identificó la confidencialidad, integridad y disponibilidad como los elementos clave, se encontró que estos mismos tres elementos son utilizados a nivel mundial para describir los requerimientos de seguridad.

Se resumen en tres requerimientos, éstos son:

- Confidencialidad
- Integridad
- Disponibilidad

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad, se extrajeron siete categorías distintas, que a continuación se muestran como definiciones de CoBIT:

- Efectividad: La información debe ser relevante y pertinente para los procesos de negocio, así como generada y emitida de una forma consistente, correcta, fácil de usar y en tiempo requerido.
- Eficiencia: Se refiere a la provisión de información a través del uso óptimo de recursos.
- Confidencialidad: Se refiere a la protección de información sensible derivada de acuerdos no autorizados.
- Integridad: Se relaciona con la exactitud y suficiencia de la información, así como su relevancia y conformidad con los valores, expectativas del negocio.
- Disponibilidad: La información debe estar disponible cuando es requerida por los procesos de negocio y también se refiere a la salvaguarda de recursos.
- Cumplimiento: Trata con el cumplimiento con aquellas leyes, regulaciones y acuerdos contractuales a los cuales los negocios están sujetos.
- Confiabilidad de la Información: Asegura veracidad de la información generada y apropiada para su uso en la operación financiera y para las entidades regulatorias.

Los recursos de TI identificados en CoBIT pueden definirse como se muestran a continuación:

- Datos: Los objetos de datos en su más amplio sentido, externos e internos, estructurados y no estructurados, gráficas, sonidos, etc.
- Sistemas de Aplicaciones: Entendimiento de la suma de procedimientos manuales y programados
- Tecnología: Cubre el hardware, sistemas operativos, sistemas manejadores de base de datos, redes, multimedia, etc.
- Instalaciones: Recursos para mantener y soportar a los sistemas de información.
- Gente: Habilidades del staff, conocimiento y productividad para planear, organizar, adquirir, liberar, soportar y monitorear los sistemas de información y servicios.

Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación:

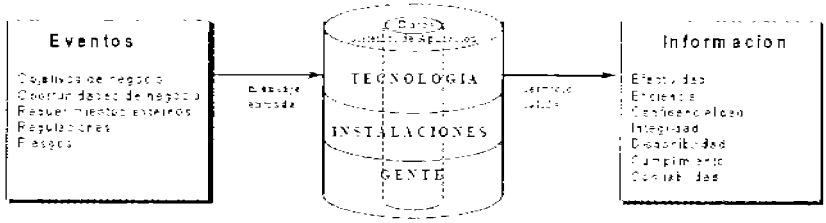

Figura 8 Principios del Marco de Referencia

El dinero o capital no se tuvo en cuenta como un recurso para la clasificación de objetivos de control para TI debido a que puede considerarse como la inversión en cualquiera de los recursos mencionados anteriormente. Es importante hacer notar también que el *Marco Referencial* no menciona, en forma específica para todos los casos, la documentación de todos los aspectos "materiales" importantes relacionados con un proceso de TI particular. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión.

Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorearse medidas de control adecuadas para estos recursos.

Es aquí donde se requiere un sano marco referencial de Objetivos de Control para Tecnología de Información. El diagrama mostrado a continuación ilustra este concepto.

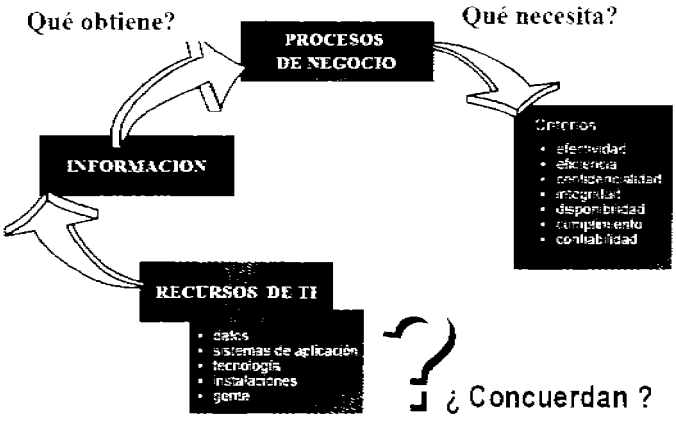

Figura 9 Marco Referencial de Objetivos de Control

2.4.4 Objetivos de Control

El Marco de Referencia de CoBIT consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos. Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas.

Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas. En el nivel más alto, los procesos son agrupados de manera natural en dominios. Esto se puede ejemplificar en la siguiente figura:

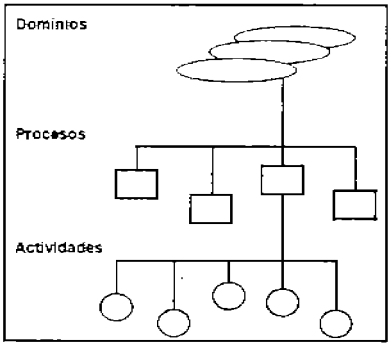

Figura 10 Componentes de CoBIT

Su agrupamiento natural es denominado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI.

Por lo tanto, el Marco de Referencia conceptual puede ser enfocado desde tres puntos estratégicos: Criterios de información, Recursos de TI y Procesos de TI. Estos tres puntos estratégicos son descritos en el Cubo CoBIT que se muestra a continuación:

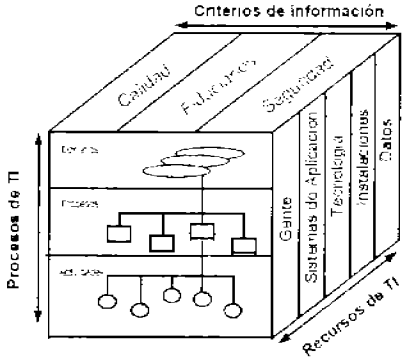

Figura 11 Cubo CoBIT

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización. Por lo tanto, cuatro grandes dominios son identificados: Planeación y Organización (Planning & Organization, PO), Adquisición e Implementación (Acquisition & Implementation, AI); Entrega y Soporte (Delivery & Support, DS) y Monitoreo (Monitoring, M).[17]

2.4.4.1 Planeación y Organización (PO)

Este dominio cubre las estrategias y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberá establecerse una organización y una infraestructura tecnológica apropiadas.

Este dominio consta de 11 objetivos de alto nivel, mismos que se mencionan a continuación:

1. Definir un plan estratégico de TI

[17] CoBIT consta de 4 grandes dominios, con 34 Objetivos de Alto Nivel: 11 PO, 6 AI, 13 DS y 4 M reconocidos por las siglas de cada dominio en ingles

2. Definir la arquitectura de información
3. Determinar la dirección tecnológica
4. Definir la organización y relaciones de TI
5. Manejo de la inversión en TI
6. Comunicación de la Directrices Gerenciales
7. Administración del Recurso Humano
8. Asegurar el cumplir requerimientos externos
9. Evaluación de Riesgos
10. Administración de Proyectos
11. Administración de Calidad

2.4.4.2 Adquisición e Implementación (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes, para asegurar que el ciclo de vida es continuo para esos sistemas

Para este dominio, se toman en consideración los siguientes objetivos de alto nivel:

1. Identificación de soluciones
2. Adquisición y mantenimiento de software aplicativo
3. Adquisición y mantenimiento de arquitectura TI
4. Desarrollo y mantenimiento de Procedimientos de TI
5. Instalación y Acreditación de sistemas
6. Administración de Cambios

2.4.4.3 Entrega y Soporte (DS)

En este dominio se hace referencia a la entrega o distribución de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la continuidad de las operaciones así como aspectos sobre entrenamiento.

Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos el cual es ejecutado por los sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

Los objetivos de alto nivel que comprende este dominio son:

1. Definición del nivel de servicio
2. Administración del servicio de terceros

3. Administración de la capacidad y el desempeño
4. Asegurar el servicio continuo
5. Garantizar la seguridad del sistema
6. Identificación y asignación de costos
7. Capacitación de usuarios
8. Soporte a los clientes de TI
9. Administración de la configuración
10. Administración de problemas e incidentes
11. Administración de datos
12. Administración de Instalaciones
13. Administración de Operaciones

2.4.4.4 Monitoreo (M)

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control. Este dominio también advierte a la administración sobre la necesidad de asegurar procesos de control independientes, los cuales son provistos por auditorías internas y externas u obtenidas de fuentes alternativas.

Por último, éste dominio abarca los siguientes:

1. Monitoreo de los procesos
2. Evaluar lo adecuado del control Interno
3. Obtener aseguramiento independiente
4. Proveer una auditoría independiente

Es importante tener en cuenta que estos procesos de TI pueden ser aplicados en diferentes niveles de la organización. Por ejemplo, algunos de los procesos serán aplicados al nivel de la empresa, otros al nivel de la función de TI, otros al nivel del propietario de los procesos del negocio, etc.

Debe notarse además, que el criterio de efectividad en los procesos que planean o distribuyen soluciones para los requerimientos del negocio cubrirá algunas veces los criterios de disponibilidad, integridad y confidencialidad— en la práctica, éstos se han convertido en requerimientos del negocio. Por ejemplo, el proceso de "identificar soluciones" tiene que ser efectivo en proveer requerimientos de Disponibilidad, Integridad y Confidencialidad.

Es claro que todas las medidas de control no necesariamente satisfarán los diferentes requerimientos del negocio para la información en el mismo grado[18].

[18] Estas medidas de control (criterios y requerimientos de TI) serán analizados a detalle en la Sección 2.4.5 Principios de los Objetivos de Control

- Primario: Es el grado en el cual se definen objetivos de control que impactan directamente los criterios de información considerados.
- Secundario: Es el grado en el cual se definen objetivos de control que solo satisfacen una extensión pequeña o satisfacen indirectamente al criterio de información considerado.
- En blanco: Podría ser aplicable, sin embargo los requerimientos son satisfechos de una forma mas apropiada por otro criterio en este proceso y/o en otro proceso.

En forma similar, todas las medidas de control no necesariamente impactarán a los diferentes recursos de TI en el mismo grado. Por consiguiente, el marco de referencia de CoBIT indica específicamente la aplicabilidad de los recursos de TI que son específicamente administrados por el proceso bajo consideración (no solamente los que toman parte en el proceso)

Esta clasificación se realiza con el marco de referencia de CoBIT, basado sobre un riguroso proceso de recolección de ideas proporcionadas por investigadores, expertos y revisores, usando estrictas definiciones previamente indicadas.

En resumen, con el fin de proveer la información que la organización necesita para lograr sus objetivos, el Gobierno de TI debe ser entrenado por la organización para asegurar que los recursos de TI serán administrados por una colección de procesos de TI agrupados naturalmente. El siguiente diagrama ilustra este concepto.

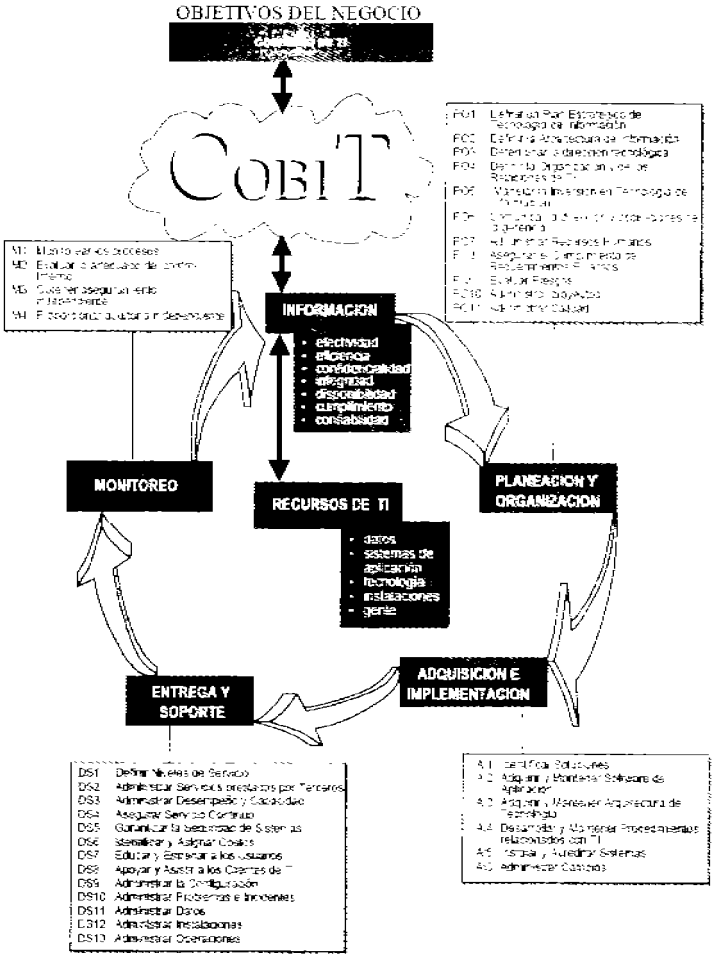

Figura 12 Procesos de TI de CoBiT

2.4.5 Principios de los Objetivos de Control[19]

CoBIT, tal como aparece en esta última versión de los objetivos de control refleja los compromisos de ISACA[20] para engrandecer y mantener el cuerpo común del conocimiento requerido para soportar la profesión de auditoria y control de los sistemas de información

El marco de referencia de CoBIT ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de TI particular, cuyo logro es posible a través del establecimiento de controles, para el cual deben considerarse controles potenciales aplicables.

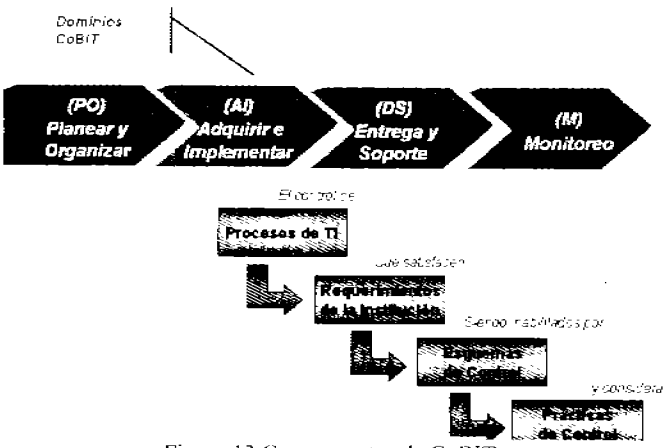

Figura 13 Componentes de CoBIT

Los objetivos de control de TI han sido organizados por proceso/actividad y también se han proporcionados ayudas de navegación no solamente para facilitar la entrada a partir de cualquier punto de vista estratégico como se explicó anteriormente, sino también para facilitar enfoques combinados o globales, tales como instalación/implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de TI por un proceso.

También deberá tomarse en cuenta que los objetivos de control de CoBIT han sido definidos de una manera genérica, por ejemplo, sin depender de la plataforma técnica, aceptando el hecho de que algunos ambientes de tecnología especiales pueden requerir una cobertura separada para objetivos de control.

Mientras que el marco de referencia de CoBIT enfoca **controles a alto nivel** para cada proceso, los *Objetivos de Control* se enfocan sobre objetivos de control detallados y

[19] CoBIT Objetivos de Control, Tercera Edición, Comité Directivo de CoBIT & IT Governance Institute Página 23
[20] ISACA: Information Systems audit And Control Association

específicos asociados a cada proceso de TI. Por cada uno de los 34 procesos de TI del marco referencial, hay desde 3 hasta 30 objetivos de control detallados, para un total de 318.

Los *Objetivos de Control* se alinean para cubrir todo el marco referencial con objetivos de control detallados con base en 41 fuentes primarias que comprenden estándares y regulaciones internacionales de TI. Contiene sentencias de los resultados deseados o propósitos a ser alcanzados mediante la implementación de procedimientos de control específicos en una actividad de TI, de esta manera provee políticas claras y buenas prácticas para los controles de TI a través de la industria, alrededor del mundo.

Los *Objetivos de Control* están dirigidos a la administración y al staff de TI, a las funciones de control y auditoría, y lo más importante, a los propietarios de los procesos del negocio. Los objetivos de control proporcionan un trabajo, que es un documento de escritorio para esos individuos. Se identifican definiciones precisas y claras para un mínimo conjunto de controles con el fin de asegurar la efectividad, eficiencia y economía de la utilización de los recursos. Objetivos de control detallados son identificados para cada proceso, como los controles mínimos necesarios. Esos controles serán analizados por los profesionales de control para verificar su suficiencia.

Los *Objetivos de Control* permiten el traslado de los conceptos presentados en el *Marco de Referencia* hacia controles específicos aplicables a cada proceso de TI.

La siguiente tabla proporciona una indicación, por proceso y dominio de TI, de cuáles criterios de información son impactados por los objetivos de alto nivel, así como una indicación de cuáles recursos de TI son aplicables.

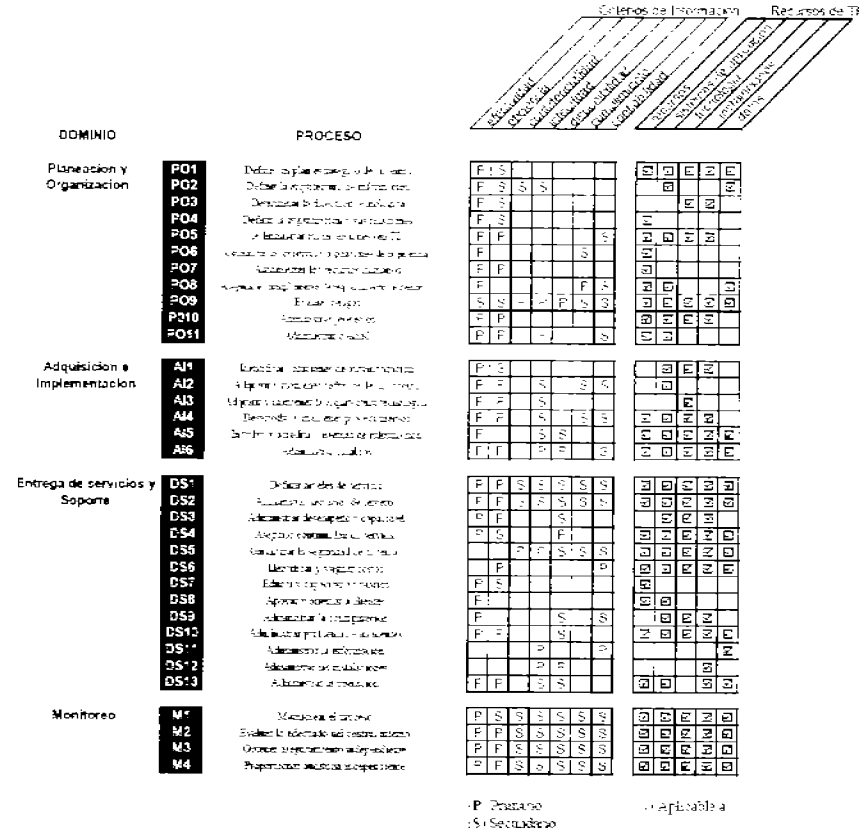

Figura 14 Indicador de Dominios, Procesos de TI, Criterios y Recursos de TI

CAPÍTULO 3. Seguridad de los Sistemas de Información

3.1 Introducción a la Seguridad de la Información

La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

La seguridad de la información se define aquí como la preservación de las siguientes características[21]:

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.
b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarcan políticas, prácticas, procedimientos, estructuras organizacionales y funciones del software.

Se deben establecer estos controles para garantizar que se logren los objetivos específicos de seguridad de la organización.

Figura 15 Componentes de SI[22]

[21] Esquema 1de Norma IRAM-ISO "IEC" 17799, Instituto Argentino de Normalización, Pag. 9
[22] SI: Seguridad de la Información

3.1.1 Por qué es necesaria la Seguridad de la Información

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus redes y sistemas de información, se enfrentan en forma creciente con amenazas relativas a la seguridad, de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como ataques mediante virus informáticos, "hacking" y denegación de servicio se han vuelto más comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a seguridad. La interconexión de las redes públicas y privadas y el uso compartido de los recursos de información incrementa la dificultad de lograr el control de los accesos. La tendencia hacia el procesamiento distribuido ha debilitado la eficacia del control técnico centralizado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados. La identificación de los controles que deben implementarse requiere una cuidadosa planificación y atención a todos los detalles. La administración de la seguridad de la información, exige, como mínimo, la participación de todos los empleados de la organización. También puede requerir la participación de proveedores, clientes y accionistas. Asimismo, puede requerirse el asesoramiento experto de organizaciones externas. Los controles de seguridad de la información resultan considerablemente más económicos y eficaces si se incorporan en la etapa de especificación de requerimientos y diseño.

3.1.2 Punto de partida para la Seguridad de la Información

Algunos controles pueden considerarse como principios rectores que proporcionan un buen punto de partida para la implementación de la seguridad de la información. Están basados en requisitos legales fundamentales, o bien se consideran como práctica recomendada de uso frecuente concerniente a la seguridad de la información.

Los controles que se consideran esenciales para una organización, desde el punto de vista legal comprenden:

a) Protección de datos y confidencialidad de la información personal
b) Protección de registros y documentos de la organización
c) Derechos de propiedad intelectual

Los controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información comprenden:

a) Documentación de la política de seguridad de la información
b) Asignación de responsabilidades en materia de seguridad de la información
c) Instrucción y entrenamiento en materia de seguridad de la información
d) Comunicación de incidentes relativos a la seguridad
e) Administración de la continuidad de la empresa

Estos controles son aplicables a la mayoría de las organizaciones y en la mayoría de los ambientes.

Se debe observar que aunque todos los controles mencionados son importantes[23], la relevancia de cada uno de ellos debe ser determinada teniendo en cuenta los riesgos específicos que afronta la organización. Por ello, si bien el enfoque delineado precedentemente se considera un buen punto de partida, éste no pretende reemplazar la selección de controles que se realiza sobre la base de una evaluación de riesgos.

3.1.2.1 Protección de datos y confidencialidad de la información personal

Diversos países han introducido leyes que establecen controles sobre el procesamiento y transmisión de datos personales. Dichos controles pueden imponer responsabilidades a aquellas personas que recopilan, procesan y divulgan información personal, y pueden limitar la capacidad de transferir dichos datos a otros países.

El cumplimiento de la legislación sobre protección de datos requiere una estructura y un control de gestión adecuados. Frecuentemente, esto se logra de la mejor manera mediante la designación de un responsable a cargo de la protección de datos que oriente a los gerentes, usuarios y prestadores de servicios acerca de sus responsabilidades individuales y de los procedimientos específicos que deben seguirse. Debe ser responsabilidad del propietario de los datos, informar al responsable de la protección de los mismos, acerca de las propuestas para mantener la información personal, en un archivo estructurado, y para garantizar el conocimiento de los principios de protección de datos, definidos en la legislación pertinente.

3.1.2.2 Protección de registros y documentos de la organización

Los registros importantes de la organización deben protegerse contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del negocio.

[23] Esquema 1de Norma IRAM-ISO "IEC" 17799, Instituto Argentino de Normalización. Pag. 11

El plazo y el contenido de los datos para la retención de información pueden ser establecidos por leyes o normas nacionales.

Los registros deben ser clasificados en diferentes tipos, por ejemplo, los registros contables, registros de base de datos, logs[24] de transacciones, de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento. Las claves criptográficas asociadas con archivos cifrados o firmas digitales deben mantenerse en forma segura y estar disponibles para su uso por parte de personas autorizadas cuando resulte necesario.

Si se seleccionan medios de almacenamiento electrónicos, deben incluirse procedimientos para garantizar la capacidad de acceso a los datos durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas pro futuros cambios tecnológicos.

A fin de cumplir con estas obligaciones, se deben tomar las siguientes medidas dentro de la organización.

a) Se debe emitir lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información;
b) Se debe preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Se debe mantener un inventario de fuentes de información clave.
d) Se debe implementar adecuados controles para proteger los registros y la información esenciales contra pérdida, destrucción y falsificación.

3.1.2.3 Derechos de propiedad intelectual

Se deben implementar procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del cual puedan existir derechos de propiedad intelectual, como derechos de diseño o marcas registradas. La infracción de derechos de autor (derecho de propiedad intelectual) puede tener como resultado acciones legales que podrían derivar en demandas penales.

Los requisitos legales, normativos y contractuales pueden poner restricciones a la copia de material que constituya propiedad de una empresa. En particular, pueden requerir que sólo pueda utilizarse material desarrollado por la organización, o material autorizado o suministrado a la misma por la empresa que lo ha desarrollado.

Los productos de software también constituyen parte de la propiedad de una empresa, regidos bajo un acuerdo de licencia que limita el uso de los productos a máquinas específicas y puede limitar la copia a la creación de copias de resguardo solamente. Se deben considerar los siguientes controles:

[24] Entiéndase "logs" como bitácoras o registros históricos

a) Publicación de una política de cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software:
b) Emisión de estándares para los procedimientos de adquisición de productos de software:
c) Mantenimiento de la concientización respecto de las políticas de adquisición y derecho de propiedad intelectual de software, y notificación de la determinación de tomar acciones disciplinarias contra el personal que incurra en el incumplimiento de las mismas:
d) Mantenimiento adecuado de registros de activos:
e) Mantenimiento de pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
f) Implementación de controles para garantizar que no se exceda el número máximo permitido de usuarios;
g) Comprobaciones para verificar que sólo se instalan productos con licencia y software autorizado;
h) Emisión de una política para el mantenimiento de condiciones adecuadas con respecto a las licencias;
i) Emisión de una política con respecto a la eliminación o transferencia de software a terceros:
j) Utilización de herramientas de auditoría adecuadas:
k) Cumplimiento de términos y condiciones con respecto a la obtención de software e información en redes públicas.

3.1.2.4 Documentación de la política de seguridad de la información

Los responsables del nivel gerencial deben aprobar y publicar un documento que contenga la política de seguridad y comunicarlo a todos los empleados, según corresponda. Éste debe poner de manifiesto su compromiso y establecer el enfoque de la organización con respecto a la gestión de la seguridad de la información. Como mínimo, deben incluirse las siguientes pautas:

a) Definición de la seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo que permite la distribución de la información
b) Una declaración del propósito de los responsables del nivel gerencial, apoyando los objetivos y principios de la seguridad de la información
c) Una breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad, que son especialmente importantes para la organización, por ejemplo:

    1) Cumplimiento de requisitos legales y contractuales
    2) Requisitos de instrucción en materia de seguridad
    3) Prevención y detección de virus y demás software malicioso
    4) Administración de la continuidad comercial

5) Consecuencias de las violaciones a la política de seguridad

d) Una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluyendo la comunicación de los incidentes relativos a la seguridad
e) Referencias a documentos que puedan respaldar la política

Esta política debe ser comunicada a todos los usuarios de la organización de manera pertinente, accesible y comprensible.

3.1.2.5 Asignación de responsabilidades en materia de seguridad informática

Deben definirse claramente las responsabilidades para la protección de cada uno de los recursos y por la implementación de procesos específicos de seguridad.

La política de seguridad de la información debe suministrar una orientación general acerca de la asignación de funciones de seguridad y responsabilidades dentro la organización. Esto debe complementarse, cuando corresponda, con una guía más detallada para sitios, sistemas o servicios específicos. Deben definirse claramente las responsabilidades locales para cada uno de los procesos de seguridad y recursos físicos y de información, como la planificación de la continuidad de los negocios.

Es esencial que se establezcan claramente las áreas sobre las cuales es responsable cada gerente; en particular se debe cumplir lo siguiente.

a) Deben identificarse y definirse claramente los diversos recursos y procesos de seguridad relacionados con cada uno de los sistemas.
b) Se debe designar al gerente responsable de cada recurso o proceso de seguridad y se deben documentar los detalles de esta responsabilidad.
c) Los niveles de autorización deben ser claramente definidos y documentados.

3.1.2.6 Instrucción y entrenamiento en materia de seguridad de la información

Todos los empleados de la organización y, cuando sea pertinente, los usuarios externos, deben recibir una adecuada capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización. Esto comprende los requerimientos de seguridad, las responsabilidades legales y controles del negocio, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información, antes de que se les otorgue acceso a la información o a los servicios.

3.1.2.7 Comunicación de incidentes relativos a la seguridad

Los incidentes relativos a la seguridad deben comunicarse a través de canales gerenciales apropiados tan pronto como sea posible

Se debe establecer un procedimiento formal de comunicación, junto con un procedimiento de respuesta a incidentes, que establezca la acción que ha de emprenderse al recibir un informe sobre incidentes. Todos los empleados y contratistas deben estar al corriente del procedimiento de comunicación de incidentes de seguridad y deben informar de los mismos tan pronto como sea posible.

Deberán implementarse adecuados procesos de "feedback" para garantizar que las personas que comunican los incidentes sean notificadas de los resultados una vez tratados y resueltos los mismos. Estos incidentes pueden ser utilizados durante la capacitación a fin de crear conciencia de seguridad en el usuario.

3.1.2.8 Administración de la continuidad de la empresa

Se debe implementar un proceso controlado para el desarrollo y mantenimiento de la continuidad de los negocios en toda la organización. Este debe contemplar los siguientes aspectos clave de la administración de la continuidad:

a) Comprensión de los riesgos que enfrenta la organización en términos de probabilidad de ocurrencia e impacto, incluyendo la identificación y priorización de los procesos críticos de los negocios
b) Comprensión del impacto que una interrupción puede tener en los negocios y definición de los objetivos comerciales de las herramientas de procesamiento de información
c) Considerar la contratación de seguros que podrían formar parte del proceso de continuidad del negocio
d) Elaboración y documentación de una estrategia de continuidad de los negocios consecuente con los objetivos y prioridades de los negocios acordados
e) Elaboración y documentación de planes de continuidad del negocio de conformidad con la estrategia de continuidad acordada
f) Pruebas y actualización periódicas de los planes y procesos implementados
g) Garantizar que la administración de la continuidad de los negocios esté incorporada a los procesos y estructura de la organización. La responsabilidad por la coordinación del proceso de administración de la continuidad debe ser asignada a un nivel jerárquico adecuado dentro de la organización.

3.2 Estándar ISO 17799

Las siglas ISO son la denominación que recibe la Organización Internacional de Normalización (International Organization For Standardization), la cual agrupa a aproximadamente 100 países y 180 comités técnicos que se encargan de establecer los mecanismos a seguir para facilitar el intercambio universal de bienes y servicios, así como promover la cooperación en actividades intelectuales, científicas, tecnológicas y económicas.

La Norma ISO 17999 es un conjunto de controles que incluyen las "mejores prácticas" en seguridad de la información, ya que es un estándar genérico reconocido a nivel internacional y cuya principal intención es servir como un punto de referencia único para identificar los controles necesarios en la mayoría de las situaciones en los que los sistemas de información se ven involucrados en la industria y el comercio.

Esta norma nace como consecuencia de la demanda a nivel internacional de una norma de calidad que regule la seguridad de la información. La tarea del ISO comenzó con la adaptación del BS 7799[25], una norma de calidad de gestión de seguridad de la información nacida inicialmente en 1995. Es una guía para empresas y organizaciones, ya que establece lo que la empresa debería hacer para contar con una gestión eficaz de la seguridad de la información. Por esto no es posible obtener una certificación en base a esta primera parte.

Como complemento, el contenido del BS 7799 lo constituyen 127 controles (agrupados en 10 asociaciones) que la empresa ha de implantar para contar con una gestión de la seguridad de la información que sea válida. En ellos se dispone lo que la organización "tiene que hacer" y, en caso de cumplimiento con lo dispuesto por los citados controles, es posible obtener la certificación.

Es importante resaltar que la intención del estándar ISO17799, es servir como punto de referencia único para identificar los controles necesarios, en la mayor parte de las situaciones en que los sistemas de información se ven involucrados en la industria y el comercio. También funciona para facilitar la comunicación y las transacciones en un entorno confiable; además, es un estándar genérico de seguridad reconocido internacionalmente.

Al respecto, el estándar ISO 17799 es una norma de amplio alcance que abarca aspectos técnicos como sistemas, redes, e infraestructura tecnológica, además de factores que pudieran afectar la seguridad de la información, como políticas y procedimientos, personal, seguridad física y ambiental, entre otros aspectos[26].

[25] BS7799: Estándar Británico de Seguridad de la Información del cual ISO tomó su referencia para la creación del estándar ISO17799

[26] Enrique Daltabuit Godas. Investigador Titular de la Dirección General de Sistemas de Cómputo Académico de la UNAM (DGSCA) al periódico EL UNIVERSAL. Fecha: Lunes 24 de Mayo de 2004

3.2.1 Secciones del ISO 17799

Las secciones que integran el estándar ISO17799 se agrupan en 10 grandes grupos, 36 objetivos de control y 127 controles, mismos que conforman lo que se denomina un ISMS (Information Security Management System) o Sistema de Gestión de Seguridad de la Información. En los puntos siguientes, mencionaremos en forma genérica los 10 grupos que abarca el estándar ISO17799, así como los 36 Objetivos que cubren en conjunto, van desde 1 hasta 8 Objetivos de control por cada "proceso de seguridad"

3.2.1.1 Administración de la continuidad del negocio

El objetivo es contrarrestar las interrupciones de las actividades críticas del negocio, así como evitar fallas mayores o desastres. Debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables.

Al utilizar los controles de seguridad contra desastres naturales, interrupciones operacionales y fallas potenciales de seguridad ayuda a fomentar la continuidad de funciones del negocio.

Los objetivos de control que se persiguen son los siguientes:

1. Aspectos de Administración de continuidad de negocio

3.2.1.2 Sistemas de control de acceso

Administrar los niveles de acceso de todos los empleados ayuda a controlar la seguridad de la información en una organización. Controlar niveles de acceso a la red puede llegar a ser un factor crítico de éxito cuando se protegen los sistemas de documentación o información en la red.

Para lograrlo, se deben tener en cuenta las siguientes políticas de difusión y autorización de la información:

1. Requerimientos de negocio para control de acceso
2. Administración de acceso de usuarios
3. Responsabilidades de Usuarios
4. Control de acceso a redes
5. Control de acceso a sistemas operativos
6. Controles de aplicación
7. Monitoreo de acceso y uso de sistemas
8. Cómputo móvil y trabajo a distancia

3.2.1.3 Desarrollo y mantenimiento de sistemas

El objetivo que se persigue es asegurar que la seguridad es incorporada a los sistemas de información. El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información.

La administración de la seguridad es imperativa en el desarrollo, mantenimiento y operación exitosa de un sistema de información[27].

Los objetivos de control a cubrir son los siguientes:

1. Requerimientos de seguridad de sistemas
2. Seguridad en sistemas de aplicación
3. Controles criptográficos
4. Seguridad de archivos de sistemas
5. Seguridad en procesos de desarrollo y soporte

3.2.1.4 Seguridad física y ambiental

Asegurar las áreas físicas y los ambientes de trabajo dentro de la organización contribuye significativamente a la administración de la seguridad de la información. Cualquier persona que se relaciona con su establecimiento físico, así sean los empleados, proveedores o clientes, tienen un papel enorme en determinar la protección de seguridad organizacional.

Para el cumplimiento del objetivo de control de alto nivel, se requiere cubrir:

1. Áreas Seguras
2. Seguridad de Equipos
3. Controles Generales

3.2.1.5 Cumplimiento

Todos los involucrados deben evitar infringir cualquier norma civil o penal, ley, reglamento, obligación contractual o cualquier requerimiento de seguridad; asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad; maximizar la efectividad y minimizar las interferencias en el sistema.

[27] ¿Qué es la Norma ISO17799? Y razones para que usted la quiera. BSI Management System, 2001. Pág. 6

El uso de asesores legales se está volviendo más importante para asegurar la observancia de una organización con las obligaciones contractuales, la ley y requisitos de seguridad.

Es importante cumplir con lo siguiente:

1. Cumplimiento con requerimientos legales
2. Revisiones de políticas de seguridad y cumplimiento técnico
3. Consideraciones de Auditoría de Sistemas

3.2.1.6 Seguridad del personal

La evaluación y asignación de las responsabilidades de seguridad de los empleados permite una administración de recursos humanos más efectiva. Las responsabilidades de la seguridad deben ser determinadas durante el reclutamiento de todo el personal y durante toda la propiedad del empleado en la organización.

Se deben de tomar los siguientes preceptos:

1. Seguridad en la descripción de puestos y en el reclutamiento
2. Capacitación de usuarios
3. Respuesta a incidentes de seguridad y malos funcionamientos

3.2.1.7 Seguridad de la organización

Este control de seguridad delimita cómo la alta administración puede dirigir la implementación de seguridad de la información dentro de una organización. Proporciona un foro para revisar y aprobar las políticas de seguridad y asignar los roles de seguridad.

Para su cumplimiento, debe de tomarse en cuenta los siguientes objetivos de control:

1. Infraestructura de Seguridad de Información
2. Seguridad de acceso de terceros
3. Tercerización (Outsourcing)

3.2.1.8 Administración de las operaciones y equipo de cómputo

Evita al máximo el riesgo de fallas en el sistema, incluido el hardware y software. Es transmitir claramente las instrucciones de seguridad a los empleados ayuda a administrar las operaciones diarias de los recursos de procesamiento de información.

Los objetivos de control a alcanzar son:

1. Responsabilidades de procedimientos operacionales
2. Planeación y aceptación de Sistemas
3. Protección contra software malicioso
4. Mantenimiento
5. Administración de Redes
6. Seguridad y manejo de medios
7. Intercambio de información y software

3.2.1.9 Clasificación y control de activos

Deberá mantenerse la protección adecuada de los activos corporativos y garantizar que los activos informáticos reciban un nivel adecuado de protección.

Éste control se basa en administrar los activos físicos e intelectuales que son importantes para mantener las protecciones apropiadas. Determina la responsabilidad de quién es dueño de qué activo de la organización.

Su cumplimiento requiere:

1. Responsabilidad de los activos
2. Clasificación de información.

3.2.1.10 Políticas de seguridad

La política documentada ayuda a proyectar las metas de seguridad de la información de una organización. Debe estar claramente redactada y comprensible para sus lectores. La política ayuda a la administración con el manejo de la seguridad de la información a través de la organización.

1. Política de Seguridad de Información

En términos generales, cada uno de estos puntos representa un sinnúmero de procedimientos, componentes tecnológicos, verificaciones de seguimiento, etcétera; lo más importante, es reconocer que no importa el tamaño y tipo de organización, la seguridad de su infraestructura, sus sistemas e información bien merecen prácticas de seguridad que minimicen los riesgos de un incidente que destruya uno de los activos más valiosos de nuestra organización: el conocimiento detrás de la información.

3.2.2 BS7799 e ISO 17799

La correcta interpretación de las normas puede ayudarle a implementar las políticas adecuadas y obtener la certificación sin dolores de cabeza. Cada vez hay un mayor interés en las empresas por certificarse ante los estándares de seguridad de la información como el ISO 17799 y el BS 7799.

Es importante destacar que estos dos estándares, en particular, tienen relación entre sí, ya que el ISO 17799 nace a partir del BS 7799-1.

Es evidente que las empresas buscan, por medio de esta certificación, una mejoría efectiva en la seguridad de la información, pero realmente hoy en día muchas de ellas lo hacen por obtener una diferenciación en el mercado.

El ISO 17799:2000 tiene la intención de ser un documento de referencia y no debería ser usada en verificaciones y certificaciones. Actualmente el ISO 17799 está siendo revisado y se están realizando cambios a su estructura.

El BS 7799-2:2002 es una metodología estructurada y reconocida internacionalmente para evaluar, implementar y administrar la seguridad de la información; en este caso sí es evaluable y certificable. En ambos estándares, se definen un grupo de controles generales que engloban las mejores prácticas en la seguridad.

El mito se genera cuando las empresas piensan que norma BS 7799-2 es una norma técnica. Esto no es cierto, ya que no define o explica los controles exactos que se deben de implementar, sino genéricamente indica qué tipo de controles se deben de implementar.

Pero existen otros mitos y recomendaciones, por ejemplo, para poder certificarse, se debe de definir un alcance para un ISMS[28] (Information Security Management System). Este alcance puede ser toda la empresa, algún área específica o un servicio. Esto permite certificarse igual que al ISO 9000, donde sólo se eligen algunas áreas críticas para la empresa.

Cuando se definen los controles en la etapa de planeación; estos controles deben ser basados según el análisis de riesgo que se realizó al ISMS.

No hay que buscar implementar todos los controles que vienen en el estándar; solo aquellos que únicamente hacen sentido para su ISMS. Muchas empresas, tratan de implementar los 127 controles y esto puede ser muy desgastante y tedioso.

El BS 7799 establece un modelo que se debe de cumplir, el cual es conocido como el PDCA "Plan, Do, Check, Act" (Planear, Hacer, Revisar, Actuar), el cual define en pocas palabras el estándar completo.

[28] ISMS (Information Security Management System) o Sistema de Gestión de Seguridad de la Información

3.3 Informática Forense

El Análisis Forense surge como consecuencia de la necesidad de investigar los incidentes de Seguridad Informática que se producen en las entidades. Persigue la identificación del autor y del motivo del ataque. Igualmente, trata de hallar la manera de evitar ataques similares en el futuro y obtener pruebas periciales.

Permite descubrir el origen del atacante, identificar detalladamente las acciones realizadas, determinar las herramientas y métodos utilizados, y lo más importante: descubrir las vulnerabilidades que lo han hecho posible con objeto de poder fortificar el sistema ante futuros incidentes. De este modo, no sólo protege a la empresa contra estos incidentes, sino que puede verificar el alcance de los mismos y tomar las medidas oportunas.

Inicialmente la auditoría forense[29] se definió como una auditoría especializada en descubrir, divulgar y atestar sobre fraudes y delitos en el desarrollo de las funciones públicas considerándose un verdadero apoyo a la tradicional auditoría gubernamental, en especial ante delitos tales como: enriquecimiento ilícito, peculado, cohecho, soborno, desfalco, malversación de fondos, prevaricato, conflicto de intereses, etc.

Sin embargo, la auditoría forense no solo está limitada a los hechos de corrupción administrativa, también el profesional forense es llamado a participar en actividades relacionadas con investigaciones sobre:

- Crímenes fiscales
- Crimen corporativo y fraude.
- Lavado de dinero y terrorismo
- Discrepancias entre socios o accionistas.
- Siniestros asegurados.
- Disputas conyugales, divorcios y
- Pérdidas económicas en los negocios, entre otros

Sobre este tema, la actitud de los auditores ha generado un gran giro, especialmente al comprender cómo su labor facilita el apoyo a las investigaciones judiciales que mediante evidencias contables aclaran diferentes disputas legales.

La informática forense tiene 3 objetivos, a saber:

1. La compensación de los daños causados por los criminales o intrusos.
2. La persecución y procesamiento judicial de los criminales.
3. La creación y aplicación de medidas para prevenir casos similares.

Estos objetivos son logrados de varias formas, entre ellas, la principal es la recolección de evidencia.

[29] Auditoría forense es el uso de técnicas de investigación, integradas con la contabilidad y con habilidades de negocio, para brindar información y opiniones, como evidencia en la corte.

Adicional a los objetivos perseguidos por la informática forense o Análisis Forense, se basa en:

1. Experticias, Auditoria e Inspecciones en Computadoras y Páginas Web.
2. Ubicación de origen de correos anónimos y archivos anexos.
3. Determinación de propietarios de Dominios .com .net .org y otros.
4. Pruebas de violación de derechos de autor.
5. Control preventivo y restricción de uso de computadores e Internet.
6. Protección de información y derechos de autor.
7. Recuperación de datos y archivos borrados intencionalmente o por virus.
8. Recuperación y descifrado de las claves.

La experiencia nos dice, que para complementar los conocimientos del auditor habitual y formarlo como auditor forense, se deben incluir aspectos de investigación legal y formación jurídica, con énfasis en la recolección de pruebas y evidencias, ya que sus habilidades en el manejo de evaluación de control interno y procedimientos de auditoría, lo destacan como un profesional de alta idoneidad.

El objetivo de un análisis forense informático es realizar un proceso de búsqueda detallada y minuciosa para reconstruir a través de todos los medios, bitácoras de acontecimientos que tuvieron lugar desde el mismo instante cuando el sistema estuvo en su estado íntegro hasta el momento de detección de un estado comprometedor.

Es decir, el análisis forense opera diversas herramientas informáticas para determinar el estado de un sistema luego de que sus medidas de seguridad han sido sobrepasadas y vulneradas, con la finalidad de encontrar evidencias que permitan definir, con toda certeza, los mecanismos que los intrusos utilizaron para acceder a ella, así como de desarrollar las mejoras y/o técnicas que deben seguirse para evitar futuras incursiones ajenas en el sistema.

Las herramientas que utilizan los peritos forenses en materia de cómputo para dar con los intrusos, y saber a ciencia cierta qué hicieron en el sistema, se han desarrollado al paso del tiempo, para que nos ayuden en cuestiones de velocidad y faciliten identificar lo que realmente le pasó al sistema y qué es lo que le puede suceder, en su contraparte igualmente se han desarrollado herramientas bastantes sofisticadas en contra de los análisis forenses.

El campo de la seguridad informática es inmensamente heterogéneo e interesante. Analizar un entorno atacado y comprometido es un desafiante ejercicio de aplicación de ingeniería inversa, para el cual es necesario tener gran conocimiento del funcionamiento de los sistemas involucrados, las técnicas de ataque y los rastros que dejan las mismas.

Basado en la premisa de que un análisis forense busca la interrelación entre una escena del crimen, un sospechoso y una victima, la evidencia física es parte fundamental de la investigación para llegar hasta el origen mismo que precede siempre de un sistema de información o bien de componentes tecnológicos cuyo papel principal siempre estará en juego, esto es a lo que se llama comúnmente como Principio de Intercambio. La siguiente figura muestra dicha interrelación, así como sus componentes:

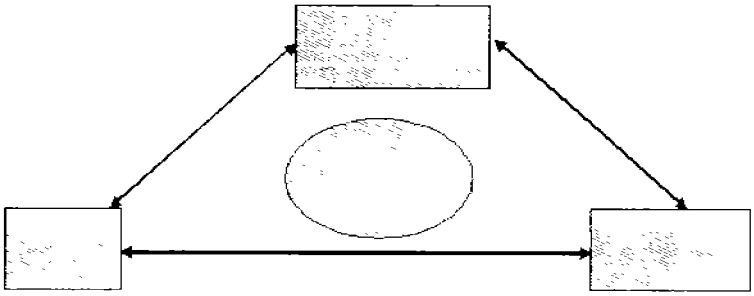

Figura 16 Principio de Intercambio

3.3.1 Evidencia Digital

La evidencia digital es única, cuando se compara con otras formas de "evidencia documental". A diferencia de la documentación en papel, la evidencia digital es frágil y una copia de un documento almacenado en un archivo es idéntica al original. Otro aspecto único de la evidencia digitsl es el potencial de realizar copias no autorizadas de archivos, sin dejar rastro de que se realizó una copia. Esta situación crea problemas concernientes a la investigación del robo de secretos comerciales, como listas de clientes, material de investigación, archivos de diseño asistidos por computador, fórmulas y software propietario.

Debe tenerse en cuenta que los datos digitales adquiridos de copias no se deben alterar de los originales del disco, porque esto invalidaría la evidencia; por esto los investigadores deben revisar con frecuencia que sus copias sean exactas a las del disco del sospechoso, para esto se utilizan varias tecnologías.

La IOCE (International Organization On Computer Evidence) define los siguientes cinco puntos como los principios para el manejo y recolección de evidencia digital:

1. Sobre recolectar evidencia digital, las acciones tomadas no deben cambiar por ningún motivo esta evidencia.
2. Cuando es necesario que una persona tenga acceso a evidencia digital original, esa persona debe ser un profesional forense.
3. Toda la actividad referente a la recolección, el acceso, almacenamiento o a la transferencia de la evidencia digital, debe ser documentada completamente, preservada y disponible para la revisión.
4. Un individuo es responsable de todas las acciones tomadas con respecto a la evidencia digital mientras que ésta esté en su posesión.
5. Cualquier agencia que sea responsable de recolectar, tener acceso, almacenar o transferir evidencia digital es responsable de cumplir con estos principios.

Además definen que los principios desarrollados para la recuperación estandarizada de evidencia digital se deben gobernar por los siguientes atributos:

1. Consistencia con todos los sistemas legales.
2. Permitir el uso de un leguaje común.
3. Durabilidad.
4. Capacidad de cruzar límites internacionales.
5. Capacidad de ofrecer confianza en la integridad de la evidencia.
6. Aplicabilidad a toda la evidencia forense.

3.3.2 Los 4 pasos del proceso forense

Como todo regla, norma o fundamento, existen ciertos lineamientos que deben cubrirse para lograr las "mejores prácticas", sobretodo en materia informática, por lo vertiginoso que es la tecnología y los sistemas de información, cada vez más complejos, con mecanismos más vulnerables y que requieren un monitoreo continuo, efectivo y que mitigue los riesgos a fin de que el riesgo residual[30] sea mínimo

- Identificar la evidencia.
  - Identificar la información que se encuentra disponible
  - Determinar la mejor manera de recolectarla

- Preservar la evidencia.
  - Con la menor cantidad de cambios
  - El forense debe poder demostrar su responsabilidad en cualquier cambio que tenga la evidencia
  - Demostrar que lo que se tiene como evidencia es exactamente igual a lo que originalmente se recolectó

- Analizar la evidencia
  - Extraer, procesar e interpretar
  - La extracción puede obtener solo imágenes binarias, que no son comprendidas por los humanos
  - La evidencia se procesa para poder obtener información que entiendan los investigadores
  - Para interpretar la evidencia se requiere conocimiento profundo para entender cómo embonan las piezas
  - El análisis efectuado por el forense debe de poder ser repetido

- Presentar la Evidencia

[30] Se denomina así al Riesgo Tratado como un intento adicional para mitigarlo, luego de habérsele aplicado controles.

- Abogados, fiscales, jurado, etc.
- La aceptación dependerá de factores como:
  - La forma de presentarla
  - El perfil y credibilidad del expositor
  - La credibilidad de los procesos usados para preservar y analizar la evidencia.

CAPÍTULO 4. Ley Sarbanes Oxley (Implementación de CoBIT para el cumplimiento de la Ley SOX)

4.1 Introducción

Las Tecnologías de Información se han convertido en el corazón de las operaciones de cualquier empresa, desde sistemas transaccionales hasta aplicaciones enfocadas a la alta gerencia. En este contexto, ha habido cambios fundamentales en la forma de realizar auditoría, incluso apegándose a lineamientos internacionales para el cumplimiento de los objetivos de negocio. Por ello, se creó la Ley Sarbanes Oxley[31], cuyo objetivo es crear un marco de transparencia para las actividades de las empresas especialmente multinacionales que cotizan en la Bolsa de Valores de Nueva York con la finalidad de brindarles un mayor grado de certidumbre a inversionistas. Esta ley estadounidense ocasiona un impacto directo en toda empresa pública de los Estados Unidos y sus subsidiarias en todo el mundo – incluyendo a México – así como empresas extranjeras que coticen en cualquier Bolsa de Valores en los Estados Unidos.

En los últimos años, en Estados Unidos ha habido grandes escándalos financieros en donde grandes empresas falsean su información financiera para publicar resultados positivos en sus estados financieros, cuando la realidad es que están teniendo enormes pérdidas de dinero. Las acciones de las empresas tienen un valor mayor al que en verdad tienen y cuando esto se descubre, el precio de las acciones baja de manera estrepitosa hasta llegar a la quiebra de la empresa.

Casos como lo sucedido con el gigante energético Enron, Worldcom, Tyco, entre otras, sacan a la luz publica los casos de corrupción practicados por estas multinacionales, sin medir el daño causado tanto a ahorradores que veían en sus estados financieros una empresa sólida con magníficas rentabilidades como una buena opción para invertir, sin mencionar la cantidad de trabajadores que serían despedidos y el daño tan grande hecho a la credibilidad de la información financiera, poniendo en crisis la realización de negocios ya que se generan en un ambiente caracterizado por las dudas, por una incertidumbre creciente surgida de las manipulaciones de la información con base en la cual los inversionistas tomaran sus decisiones.

Esta crisis tiene un origen o lo tenía desde un principio y con el tiempo se convirtió en una gran depresión, la flexibilidad de las normas que cada país adopta de acuerdo a su entorno, no crea un ambiente confiable para otro país que quiera venir a invertir, las auditorías realizadas por contadores que en su afán de independizarse de una normativa profesional trabajan a su amaño o al de sus intereses, entonces se deberán adoptar ejemplares sanciones contra firmas contables de prestigio mundial y por que no establecer tribunales éticos para sancionar un ejercicio profesional de dudosa moralidad.

Debido a los casos presentados en Estados Unidos y en Europa se produjo un consenso sobre la necesidad de una acción legislativa fuerte y rápida, dando lugar al fortalecimiento de normas que controlan y endurecen el control interno y que ya muchos países lo están también haciendo, como la ley emitida por el Congreso de los Estados Unidos, conocida como la ley Sarbanes Oxley, para proteger a los inversionistas, con la cual crearon un

[31] Ley Sarbanes Oxley (SOX), se define así a los lineamientos

nuevo organismo supervisor de la contabilidad, una reforma a la contabilidad corporativa, la protección del inversionista y se aumentaron las penas criminales y civiles por las violaciones al mercado de valores.

Como una de muchas reacciones al fenómeno Enron, el 30 de julio de 2002, el gobierno norteamericano aprobó la ley Sarbanes Oxley en la que se establecen nuevas normas sobre contabilidad corporativa, así como penalidades por malos manejos u omisiones de información. Esta ley está conformada por 11 apartados que abarcan desde responsabilidades adicionales a las ya existentes para los comités de auditoría, hasta penas de cárcel por fraude. La ley todavía tiene pendientes regulaciones específicas para su aplicación y, aunque ésta tiene un fundamento local, también aplica fuera del país de origen, afectando a las empresas registradas ante la Security Exchange Commission (SEC[32]) y sujetas al Formato 20 F.

4.1.1 La Ley Sarbanes Oxley

La ley Sarbanes Oxley (SOX) se creó en el año 2002, para las empresas que a partir del 15 de noviembre de 2005 generen más de 75 millones de dólares al año y además, coticen en las Bolsas de Valores de los Estados Unidos, con el fin de incrementar la confianza pública en reportes financieros y para fortalecer los mercados de capitales.

La ley SOX contempla una revisión mucho más rigurosa de los datos financieros que una empresa declara en sus estados financieros y que utiliza para sus controles internos. Las subsidiarias mexicanas de empresas estadounidenses son responsables de poner al día sus propios métodos y prácticas contables con el fin de dar una valoración del estado financiero de la empresa en México. Información errónea por parte de ellas podría afectar también los estados financieros de la oficina matriz. Las multas por proveer información falsa o incorrecta son muy severas, éstas pueden llegar al extremo de encarcelar a los ejecutivos de la empresa, o que ésta sea retirada de la Bolsa de Valores en donde cotiza.

Aunque la ley SOX afecta directamente a empresas estadounidenses y sólo a un grupo pequeño de firmas mexicanas que cotizan en la NYSE[33], muchos analistas creen que es punta de lanza para el establecimiento de un código de ética dirigido para las compañías en México en general.

Como referencia, en México, durante el año 2004, se exportaron cerca de 16,200 millones de dólares y en gran porcentaje a empresas transnacionales ubicadas en el país[34]. En este aspecto, es cuando la ley SOX afecta a las empresas mexicanas. Esto las obliga a tener un verdadero control de sus procesos internos para poder asegurar que van a poder cumplir con los acuerdos aceptados. Es importe decir que el hacer las cosas más rápido y con una mejor

[32] SEC (Securities and Exchange Commision): Comisión de Bolsa y Valores
[33] NYSE: Bolsa de Valores de Nueva York
[34] INEGI, Cuadro Resumen de Exportaciones, 2004

eficiencia e inteligencia dará a las empresas mexicanas un buen posicionamiento y una ventaja competitiva contra sus posibles competidores[35].

4.1.1.1 Fundadores de la Ley SOX

Los fundadores de la ley Sarbanes Oxley. Paul S. Sarbanes (Senador Demócrata) y Michael G. Oxley (Congresista Republicano); preocupados por el fenómeno tan continuo de empresas multinacionales en quiebra por errores en sus estados financieros, de manera dolosa por el Director General (CEO). Director de Finanzas (CFO) o bien los accionistas estuvieran enterados de manera fehaciente del comportamiento del valor de sus acciones, propusieron al Congreso de los Estados Unidos el poder establecer ciertas normas o reglas con las cuales impidieran que las empresas, en forma dolosa alteraran sus estados financieros con el fin de aumentar el valor de sus acciones, por ello, inspiraron una ley que regulara estas actividades con el fin de evitar pérdidas financieras.

4.1.1.1.1 Paul S. Sarbanes[36]

Paul Sypos Sarbanes, Senador Demócrata por el estado de Maryland, nació en Salisbury, Maryland el 3 de febrero de 1933. Hijo de inmigrantes griegos que vinieron de Laconia, Grecia. Después de graduarse de Wicomico High School, Salisbury, recibió una beca académica y atlética para la Universidad de Princeton. Después de graduarse en 1960 de la Escuela de Leyes de Harvard, fungió como secretario del tribunal para el Juez Federal Morris A. Soper antes de ingresar a la práctica privada en dos bufetes legales en Baltimore.

Figura 17 Senador Paul S Sarbanes

Los principios de justicia y oportunidad que inculcaron sus padres desde una edad temprana, lo llevaron a una vida de servicio público. En 1966, Sarbanes se postuló para la Cámara de Delegados de Maryland en la Ciudad de Baltimore y ganó la elección. El 2 de

[35] Revista Expansión No. 861, Artículo: Riesgo Operativo, una ventaja competitiva, Pricewaterhouse Coopers, Marzo 19, 2003

[36] Biografía obtenida en el portal electrónico del Senador Paul S Sarbanes. http://sarbanes.senate.gov

noviembre de 1976, fue electo al Senado de los Estados Unidos y reelecto en los periodos de 1982, 1988, 1994 y 2000.

Su contribución a la ley que lleva su nombre se debe principalmente como respuesta al fracaso financiero de Enron Corp. en 2001, momento en que esta compañía era la séptima corporación más grande en los Estados Unidos, Sarbanes, en su capacidad como Presidente del Comité de Banca, Vivienda y Asuntos Urbanos del Senado, llevó a cabo una serie de audiencias que tuvieron como resultado la aprobación de una ley bipartidista para reformar la industria de la contabilidad y restaurar la confianza de los inversionistas que se había erosionado con el colapso de Enron.

Inmediatamente después de la aprobación de la ley por parte del Comité de la Banca del Senado en junio del 2002, las dificultados contables de WorldCom sacudieron aún más a los mercados financieros y crearon una gran ola de apoyo para la legislación de Sarbanes.

4.1.1.1.2 Michael G. Oxley[37]

Michael G Oxley nació el 11 de febrero de 1944. Obtuvo el grado de leyes en la Estatal de Ohio en 1969. Es congresista por el Octavo Distrito de Ohio.

Figura 18 Representante Michal Oxley

Abogado de profesión, obtuvo la lic. en filosofía y letras en la Universidad de Miami en 1966 y el grado de leyes en la Universidad de Ohio. Fue aceptado como Practicante en la Suprema Corte de Estados Unidos. Tiene experiencia de 8 años en el Octavo Distrito junto al Representante Jackson Betts, el gobernador John Browm y el abogado general William Saxbe.

Michael Oxley sirve en su decimosegundo periodo en la cámara de representantes y es presidente del Comité de la Cámara de Servicios Financieros. Liderea a 37 republicanos, 32 demócratas y 1 independiente en el comité, que vigila Wall Street, bancos e industrias de seguros. Además de la rama financiera, Oxley tiene gran desenvolvimiento en comercios, telecomunicaciones y energía. Creyente de los mercados competitivos, utiliza su

[37] Biografía obtenida en el portal electrónico del Congresista Michael G Oxley. http: www.oxley.house.gov

especialización comercial y financiera para defender políticas que promueven economías personales, trabajos y crecimiento económico.

Oxley es coautor de la ley Sarbanes Oxley, que estableció nuevas protecciones al inversionista y juega con las más altas normas del gobierno corporativo, como respuesta de los escándalos comerciales. Firmando la ley el 30 de julio del 2002, el presidente George W. Bush llamó a Oxley "*un verdadero abogado de la integridad corporativa*". El comité de Oxley fue el primero en poner atención en los fraudes financieros de Enron, WorldCom y otras compañías.

4.1.1.2 Apartados específicos de la ley SOX

Básicamente la razón de ser de ley Sarbanes Oxley, es incrementar la confianza pública de los reportes financieros y fortalecer los mercados. Pero no solo es una revisión contable y financiera, sino que en estos tiempos, en donde la tecnología de información juega un papel primordial para la generación de la información financiera, se considera altamente importante que también la tecnología sea analizada conforme a una serie de estándares.

Al ser el área de TI el corazón de cualquier organización, el CIO es el responsable de ofrecer las diferentes herramientas y estrategias para poder hacer cumplir la ley SOX. Toda la información financiera de la organización está almacenada y operada por Tecnología de Información.

Dentro de las secciones de la ley, existen tres que involucran directamente al departamento de Tecnología de Información, estas son la 302, 404 y 409. Para efectos prácticos, analizaremos las dos primeras secciones.

4.1.1.2.1 Sección 302

La sección 302 de la ley SOX habla sobre la obligación de generar reportes financieros donde muestren el resultado de la empresa (estados financieros) y que además, el reporte debe estar avalado en cuanto a su integridad por el CEO[38] y el CFO[39].

A continuación, se hace mención de la ley SOX referente a la sección 302:

Sección 302. "Responsabilidad de la compañía por los Informes Financieros"[40]

A. Reglamentos Requeridos. La comisión, por reglamento, requerirá de cada compañía que presente informes periódicos bajo la sección 13(a) o 15(d) del Acta de Intercambio de Valores de 1934 que el principal funcionario o funcionaros ejecutivos y el principal o principales funcionarios financieros, o personas que

[38] CEO (Chief Executive Officer): Director General de la compañía
[39] CFO (Chief Financial Officer): Director de Finanzas de la compañía
[40] Acta del 2002 Sarbanes Oxley, Cámara de Representantes, EEUU, Junio 24, 2002

efectúen funciones similares en cada informe anual o trimestral presentado o suministrado bajo cualquier sección de tal Acta certifique que:

1. El funcionario firmante ha revisado el informe:
2. Basado en el conocimiento del funcionario, el informe no contiene ninguna declaración falsa de un hecho material ú omite declarar un hecho material necesario a fin de hacer que a la luz de las circunstancias bajo las cuales fueron hechos tales informes no son fraudulentos;
3. Basado en el conocimiento del funcionario, los estados financieros , y otra información incluida en el informe presentan razonablemente en todo aspecto significativo la situación financiera y los resultados de las operaciones del emisor por los periodos presentados en el informe;
4. Los funcionarios firmantes:
    A. Son responsables por establecer y mantener controles internos:
    B. Han diseñado controles internos para asegurar que información importante referente al emisor y a sus subsidiarias consolidadas se ha puesto en conocimiento de tales funcionarios, particularmente durante el periodo en el cual están siendo preparados informes periódicos;
    C. Han evaluado la efectividad de los controles internos del emisor a una fecha dentro de los 90 días antes del informe; y
    D. Han presentado en el informe sus conclusiones sobre la efectividad de los controles internos basados en su evaluación a esa fecha.
5. Los funcionarios firmantes han revelado a los auditores del emisor y al Comité de Auditoría de la Junta de Directores (o personas que desempeñan función equivalente):
    A. Todas las deficiencias significante en el diseño u operación de los controles internos que podrían afectar adversamente la habilidad del emisor para registrar, procesar, resumir y reportar datos financieros y han identificado las debilidades materiales en los controles internos; y
    B. Cualquier fraude, significativo o no, que involucre a la gerencia u otros empleados que desempeñan un rol importante en los controles internos del emisor; y
6. Los funcionarios firmantes han indicado en el informe si hubieron o no cambios significantes en los controles internos o en otros factores que podrían afectar significativamente los controles internos después de la fecha de su evaluación, incluyendo cualquier acción correctiva respecto a deficiencias significantes y debilidades materiales.

B. No tienen efecto las reincorporaciones extranjeras. Nada en la sección 302 será interpretado o aplicado para permitir reducir la obligación legal de declaración requerida bajo esta sección 302, para un emisor que se ha reincorporado o se ha comprometido en cualquier otra transacción que resulte en la transferencia de domicilio u oficinas de la compañía dentro o fuera de los Estados Unidos.

C. Fecha límite. Los reglamentos requeridos por la sub-sección (A) serán efectivos a no más tardar 30 días después de la fecha de entrada en vigencia de esta Acta.

4.1.1.2.2 Sección 404

La cláusula 404 de la ley SOX menciona que deben existir procedimientos y políticas que aseguren la integridad de la información así como la disponibilidad de ella.

Se hace mención de la ley referente a la sección 404:

Sección 404. "Evaluación de la Gerencia de los Controles Internos"[41]

A. Regulaciones Requeridas. La comisión prescribirá regulaciones requiriendo que cada informe anual requerido por la sección 13(a) o 15(d) del Acta de Intercambio de Valores de 1934 contenga un informe de control interno, el cual:
    1. Determinará la responsabilidad de la gerencia por establecer y mantener una estructura adecuada de control interno y los procedimientos para información financiera; y
    2. Contendrá una evaluación, al final del año fiscal más reciente del emisor, de la estructura de control interno y los procedimientos del emisor para información financiera.
B. Evaluación e informe del Control Interno. Con respecto a la evaluación del control interno requerido por la sub-sección (A), cada firma de contabilidad pública registrada que prepara o emite el informe de auditoría para el emisor testificará, e informará sobre la evaluación hecha por la gerencia del emisor. Una testificación bajo esta sub-sección será hecha de acuerdo con las normas para compromisos de testificación emitidas o adoptadas por la Junta. La testificación no estará sujeta a un compromiso separado.

4.1.1.3 Repercusiones de la ley SOX

Las modificaciones más significativas que introdujo la ley SOX a las perdurables leyes norteamericanas de 1934 pueden resumirse así:

1. Regulación de la actividad contable y de auditoría.

    La ley SOX creó el Public Company Accounting Oversight Borrad (PCAOB), un órgano colegiado, de derecho privado, organizado en forma de corporación sin ánimo de lucro integrado por cinco miembros, de los cuales solo dos podrán tener la calidad de contadores públicos y cuyas acciones serán objeto de revisión por parte de la SEC (Securities and Exchange Commission). Este órgano colegiado lleva el registro de todas las firmas de auditoría, establece o adopta principios de auditoría, control de calidad, ética e independencia en la preparación de dictámenes.

    El Gobierno de cada país deberá establecer un sistema nacional de acreditación de calidad de las firmas de auditoría; la Superintendencia de Sociedades definirá las

[41] Acta del 2002 Sarbanes Oxley. Cámara de Representantes. EEUU. Junio 24, 2002

normas técnicas o las especificaciones que se consideren como indispensables para evaluar el sistema de control de calidad del ejercicio de la profesión de contaduría a través de personas jurídicas, y para calificar la calidad de los servicios de auditoría de estados financieros. Esta Superintendencia, en consecuencia, administrará y supervisará la acreditación de los auditores y llevará el sistema de matrícula de los contadores.

2. Mayor independencia de las firmas de auditoría.

   Las compañías que prestan los servicios de auditoría deben guardar plena independencia con los auditados. Desde que entró en vigor la ley SOX y sus normas complementarias, no podrán, custodiar los libros contables de la compañía, prestar servicios de actuaría, diseñar sistemas de información financiera, administrar recursos humanos de las auditadas, prestar servicios de outsourcing para auditoría interna, ser consejera de finanzas de la auditada, prestar servicios legales o brindar experticios de ningún tipo, salvo los tributarios. La ley SOX enumeró taxativamente los servicios que no podrán realizar las firmas de auditoría; los demás servicios, como podría ser el de asesoría tributaria, deberá ser aprobado previamente por el Comité de Auditoría e informado luego a la SEC.

3. Previsiones sobre el gobierno corporativo:

   La ley SOX enderezó un llamado a la SEC, para que en poco tiempo (270 días), dictara el reglamento y reformulara el funcionamiento de los Comités de Auditoría. La regulación de dichos Comités se edificó sobre las siguientes bases:

   a) Cada miembro del Comité debe ser independiente, esto significa que no podrá recibir ningún tipo de compensación por parte de la auditada, distinta de la que recibe por ser director o por ser miembro del Comité;
   b) Al menos uno de los miembros debería, aunque no es obligatorio, ser experto en finanzas;
   c) El Comité de Auditoría será responsable del cumplimiento de las funciones del auditor independiente; y,
   d) El Comité deberá establecer procedimientos para recibir quejas o informes de los trabajadores sobre las expresiones contables o de auditoría que parezcan cuestionables.

   La ley SOX, faculta a los Comités de Auditoría para cambiar de auditor cuando no satisfaga las exigencias u objetivos propuestos o incumpla sus directivas. El auditor independiente deberá reportarle al Comité de Auditoría las prácticas contables, y los tratamientos alternativos que se le den a los GAAP (General Accepted Acounting Principles) y puedan suscitar alguna discusión.

4. Prohibición de conferir o modificar favorablemente créditos a los CEO's y directores:

   Según la ley SOX, sólo en casos excepcionales las compañías podrán otorgar créditos a sus ejecutivos, o modificar para bien las situaciones en que se adquirieron préstamos antiguos. Claro está, esta disposición no tendrá efectos retroactivos y prohíbe solo los nuevos créditos y las nuevas modificaciones. Aunque no sea explícito, la redacción de la ley SOX indica que esta prohibición cobija incluso los

créditos que se confieren como parte de arreglos compensatorios, como sucede con los que se le otorgan a quien se traslada a otra ciudad. Claramente, la prohibición se dirige a castigar el otorgamiento de créditos a directores o CEO's para adquirir acciones en orden a evadir ingresos gravados tributariamente. Ya en varios foros extranjeros, especialmente europeos, se han enderezado propuestas tendientes a que esta prohibición sólo opere frente a los emisores norteamericanos.

5. Obligación de certificar por parte de los CEO's y los CFO's.

   Un punto que preocupa a los Directores Generales y los Directores de Finanzas de todo el mundo consiste en la obligación de certificar personalmente los reportes anuales y trimestrales que rinden las emisoras a la SEC (Sección 302a). Este reporte, similar al que rinden los auditores independientes, y distinto en cuanto no tiene como marco los GAAP, consta en una proforma que debe ser firmada por los CEO's y CFO's que respaldan la información contable y financiera que se publica, y en ella debe afirmarse, por lo menos, que: el ejecutivo ha revisado el reporte; que según su conocimiento el reporte es exacto y da cuenta, razonablemente, de la situación financiera y de los resultados de la operación de la compañía; que el ejecutivo es responsable de establecer los sistemas de control interno de la compañía, cuyos efectos ha evaluado y revelado; que el suscriptor ha revelado al auditor independiente y al Comité de Auditoría las deficiencias materiales relacionadas con el control interno o cualquier fraude. En el formato que se completa también hay una fórmula sacramental que advierte que una inconsistencia injustificada en los reportes puede configurar un delito al margen de ley penal norteamericana.

4.2 Administración de Riesgos de TI

En el mundo cambiante de la tecnología de información, las compañías deben enfrentar el reto constante de lograr un equilibrio entre las metas comerciales y los riesgos de negocio que supone el uso de la tecnología. La Administración de Riesgos de Información (Information Risk Management - IRM) constituye una disciplina que brinda asesoría a compañías en la administración de riesgos relacionados con el uso de tecnología de información.

La administración de riesgos de TI brinda a los equipos de auditoría y compañías un mayor entendimiento de las implicaciones y el impacto de la Tecnología de Información en los aspectos principales del negocio. Su objetivo consiste en identificar y administrar los riesgos inherentes a los sistemas tecnológicos, y ofrecer a las compañías información con el fin de ayudarles a alcanzar los objetivos financieros y estratégicos del negocio. Asimismo, ayuda a la administración a comprender los procesos implantados por la compañía y mejorarlos sin disminuir la eficacia de los controles[42].

4.2.1 Enfoque de Administración de Riesgos ERM

El enfoque del Marco Integrado de Administración de Riesgos Corporativos (Enterprise Risk Management – Integrated Framework), define a la Administración de Riesgos Corporativos como un proceso efectuado por el Director General, la Gerencia y otros miembros del personal, aplicado en el establecimiento de la estrategia y a lo largo de la organización, diseñado para identificar eventos potenciales que pueden afectarla y administrar riesgos de acuerdo a su apetito de riesgo, de modo de proveer seguridad razonable en cuanto al logro de los objetivos de la organización.[43]

Es importante señalar que un ERM es un proceso, efectuado por el Comité Ejecutivo de una Entidad, la Gerencia y demás personal, aplicado en un estratégico conjunto y a través de toda la empresa, designado para identificar potenciales eventos que puedan afectar a la entidad, y gerenciar los riesgos de acuerdo al apetito sobre dichos riesgos, para proveer razonable aseguramiento acerca del cumplimiento de los objetivos corporativos.

El marco ERM de COSO, por ejemplo, provee:

- La definición de administración de riesgos corporativos.
- Los principios críticos y componentes de un proceso de administración de riesgos corporativos efectivo.
- Pautas para las organizaciones sobre como mejorar su administración de riesgos
- Criterios para determinar si la administración de riesgos es efectiva, y si no lo es que se necesita para que lo sea.

[42] KPMG, Costa Rica
[43] Enterprise Risk Management Integrated Framework, PricewaterhouseCoopers Uruguay, 2004

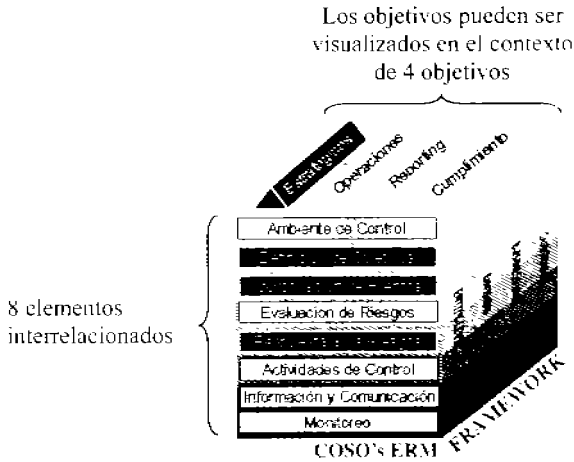

Figura 19 Informe COSO ERM Framework

Los componentes del Informe COSO ERM Framework son:

- Ambiente de Control:
  Es la base fundamental para los otros componentes del ERM, dando disciplina y estructura. Incide en:
  - La concientización del personal respecto del riesgo y el control
  - El modo en que las estrategias y objetivos son establecidos, las actividades de negocio son estructuradas y los riesgos son identificados, evaluados y gerenciados.

- Definición de Objetivos:
  Condición previa para la identificación de eventos, evaluación de riesgos y respuesta al riesgo. Consiste en metas de alto nivel que se alinean con y sustentan la misión/visión y reflejan las elecciones estratégicas de la gerencia sobre cómo la organización buscará crear valor para sus grupos de interés

- Identificación de Eventos:
  Se deben identificar eventos potenciales que afectan la implementación de la estrategia o el logro de los objetivos, con impacto positivo, negativo o ambos

- Evaluación de Riesgos:
  Permite a la entidad considerar el grado en el cual eventos potenciales podrían impactar en el logro de los objetivos. La evaluación de riesgos puede realizarse desde dos perspectivas: probabilidad de ocurrencia e impacto.
  - Considera que la evaluación se debe realizar tanto para riesgos inherentes como residuales

- La metodología de evaluación de riesgos comprende una combinación de técnicas cualitativas y cuantitativas

- Respuestas a los Riesgos:
  Una vez evaluado el riesgo, la gerencia identifica y evalúa posibles respuestas al riesgo en relación al apetito de riesgo de la entidad

- Actividades de Control:
  Integración con Respuesta al Riesgo.
  - Son las políticas y procedimientos necesarios para asegurar que las respuestas al riesgo se llevan a cabo de manera adecuada y oportuna
  - La selección o revisión de las actividades de control comprende la consideración de su relevancia y adecuación a la respuesta al riesgo y al objetivo relacionado
  - Se realizan a lo largo de toda la organización, a todos los niveles y en todas las funciones

- Información y Comunicación:
  La información es necesaria en todos los niveles de la organización para identificar, evaluar y dar una respuesta al riesgo.
  - Se debe identificar, capturar y comunicar la información pertinente en tiempo y forma que permita a los miembros de la organización cumplir con sus responsabilidades.
  - La información relevante es obtenida de fuentes internas y externas
  - La comunicación se debe realizar en sentido amplio, y fluir por la organización en todos los sentidos (ascendente, descendente, paralelo).
  - Asimismo, debe existir una comunicación adecuada con partes externas a la organización como ser: clientes, proveedores, reguladores y accionistas.

- Monitoreo:
  Implica monitorear que el proceso de administración de riesgos mantiene su efectividad a lo largo del tiempo y que todos los componentes del marco ERM funcionen adecuadamente a través de:
  - Actividades de monitoreo continuo, que se llevan a cabo durante el curso normal de las operaciones
  - Evaluaciones puntuales, realizadas por personal que no es el responsable directo de la ejecución de las actividades. Su alcance y frecuencia de realización depende de los resultados de la evaluación de riesgos y de la efectividad de las actividades de monitoreo continuo
  - Una combinación de ambas formas

4.2.2 Proceso de Administración de Riesgos

El primer paso en el proceso de administración de riesgos es la identificación y clasificación de los recursos de información o de los activos que necesitan protección porque son vulnerables a las amenazas. El propósito de clasificar los recursos de TI puede ser o bien priorizar investigaciones posteriores e identificar la protección apropiada, o bien permitir la aplicación de un modelo estándar de protección. Los activos típicos asociados con información y TI son:[44]

- Información y datos
- Hardware
- Software
- Servicios
- Documentos
- Personal

El siguiente paso es estudiar las amenazas y vulnerabilidades asociadas con el recurso de información y la probabilidad de que ocurran. En este contexto, amenazas son cualquier circunstancia o evento con el potencial de dañar un recurso de TI tales como destrucción, revelación, modificación de datos y/o negación de servicio. Las clases más comunes de amenazas son:

- Errores
- Daño intencional
- Fraude
- Robo
- Falla del equipamiento (software)

Las amenazas ocurren por causa de las vulnerabilidades asociadas al uso de recursos de TI. Las vulnerabilidades son características de los recursos de información que pueden ser explotadas por una amenaza para causar daños.

Una vez que se han establecido los elementos de riesgo, éstos se combinan para formar una visión general del riesgo. Un método común de combinar los elementos es calcular la vulnerabilidad de impacto de "x" para cada amenaza y dar así una medida de riesgo general. El riesgo es proporcional al valor de la pérdida o daño y a la frecuencia estimada de la amenaza.

Una vez que se han identificado los riesgos, se pueden evaluar los controles existentes o bien, diseñar los nuevos controles para reducir las debilidades hasta un nivel aceptable de riesgo. La fortaleza de un control puede ser medible en términos de su fortaleza inherente o de diseño y probabilidad de su efectividad.

[44] Manual de Preparación al Examen CISA 2005, ISACA, 2005 pp.520

4.2.3 Tipos de Riesgo

Los riesgos son una medida de incertidumbre. En el proceso comercial, la incertidumbre trata de lograr objetivos organizacionales. Puede consistir en consecuencias positivas o negativas, aunque la mayoría de los riesgos positivos se llaman oportunidades y los riesgos negativos se llaman riesgos.

Generalmente el riesgo puede ser transferido, rechazado, reducido o aceptado. En el momento de implementar los controles, una organización puede considerar los costos y beneficios de implementarlo. Si el costo de los controles excede los beneficios, una organización puede elegir aceptar el riesgo en lugar de incurrir en costos adicionales que en asegurar su sistema. Los riesgos se pueden clasificar de la siguiente forma:
Riesgo Absoluto e Inherente:

- Corresponde a la evaluación propia e intrínseca de cada riesgo.
- Es el riesgo que existe con anterioridad a la existencia de cualquier acción.
- No depende de ningún control para mitigarlo, ni de tratamiento llevado a cabo para disminuir su probabilidad de ocurrencia ni su impacto.

Riesgo Controlado:

- Surge de la aplicación de los controles existentes, o bien de la definición de nuevos controles para mitigar el riesgo inherente.
- Disminuirá la probabilidad, la consecuencia o ambas, una vez puestos los controles en acción.

Riesgo Residual:

- Se denomina así al Riesgo Tratado como un intento adicional para mitigarlo, luego de habérsele aplicado controles.
- Corresponde al tratamiento que se ha dado al riesgo, a fin de ubicarse en una escala con menor probabilidad y/o impacto.
- La decisión de asumir o tratar el riesgo residual deberá estar debidamente documentada.

La siguiente figura muestra una matriz de riesgos, la cual se crea a través de un análisis de probabilidades vs. consecuencias:

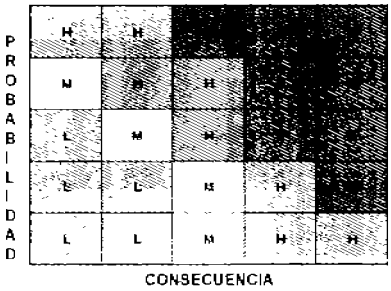

Figura 20 Store de Riesgo

Las secciones marcadas con la letra "E", significan los riesgos inherentes o que no depende de ningún control para mitigarlo. La sección marcada con la letra "H", muestra el riesgo controlado, es decir, aquellos riesgos que se controlan con mecanismos ya implementados. La sección marcada con la letra "M", representa el riesgo residual o bien, aquel riesgo que fue mitigado, sin embargo, puede dejar secuelas.

La nomenclatura general es la siguiente:

- Riesgo Extremo (EXTREME RISK). Requiere acción inmediata.
- Riesgo Alto (HIGH RISK). Necesita atención de la alta gerencia.
- Riesgo Moderado (MODERATE RISK). Debe especificarse responsabilidad gerencial.
- Riesgo Bajo (LOW RISK). Administrar mediante procedimientos de rutina.

4.3 Cumplimiento de la ley SOX bajo los Marcos de Referencia CoBIT y COSO

La ley SOX demuestra la resolución firme del congreso de los Estados Unidos a mejorar la responsabilidad corporativa. Fue creada para restaurar la confianza del inversionista en los mercados públicos que se vieron dañados debido a los escándalos financieros de Enron y WorldCom. Aunque la ley apoya las regulaciones actuales, han vuelto a escribir las reglas de responsabilidad, resolución y reporteo. La premisa es: un buen gobierno corporativo y prácticas comerciales éticas no son opcionales.

La ley SOX ha cambiado fundamentalmente el ambiente de negocios y regulaciones. Apunta a reforzar el gobierno corporativo a través de medidas que fortalezcan revisiones internas y balances y, finalmente, fortalecer la responsabilidad corporativa. Sin embargo, es importante enfatizar que en la sección 404 no requiere mayor administración y los dueños del proceso de negocio meramente establecen y mantienen una adecuada estructura de control interno, pero también evalúan su efectividad en forma anual.

Para algunas organizaciones que han iniciado el proceso de reingeniería, tienen que poner en claro rápidamente el papel que juega la tecnología de información en el control interno. Sistemas, datos y componentes de infraestructura son esenciales en el proceso del reporte financiero.

4.3.1 Normas Generales

El 9 de marzo de 2004, la PCAOB (Public Company Accounting Oversight Borrad) aprobó la Norma de Auditoria No. 2, titulada "Audit. Of Internal Control Over Financial Reporting Performed in Conjuntion with an audit. Of Financial Statements". Esta Norma de Auditoria establece los requisitos para realizar una auditoría de control interno sobre reportes financieros y proporciona algunas directrices importantes en el alcance requerido por los auditores.

La norma PCAOB incluye requisitos específicos a los auditores para entender el flujo de transacciones, incluyendo como se inician, autorizan, graban, procesan y monitorean. Los flujos de transacciones normalmente involucran sistemas de aplicaciones que automatizan procesos y apoyan altos volúmenes y proceso de transacciones complejas.

La ley Sarbanes Oxley solicita a las organizaciones seleccionar e implementar un marco de referencia de controles internos adecuado. El Marco Integrado de Control Interno COSO, ha venido a facilitar esta tarea. Generalmente la SEC registra y encuentra detalles adicionales que pueden implementarse. De manera similar, el PCAOB indica la importancia de los controles de TI, pero no hace mención a detalle. Como resultado, el marco de referencia CoBIT, publicó a través del IT Governance Institute, el uso de sus documentos como base para ver más a detalle los controles de TI.

Mientras el marco de referencia de CoBIT proporciona controles de directrices operacionales y objetivos de control, solo aquellos relacionados directamente con el reporte financiero se usaron para desarrollar CoBIT. Considerando que se dio otro sentido a las guías de control de TI, se incluyó el estándar ISO17799 y la Biblioteca de Infraestructura de Tecnología de Información (ITIL[45]).

Es así como se le da sentido que la ley SOX exige un marco de referencia o estándar internacional: debido a ésta situación, el marco de referencia de COSO permite cubrir las secciones 302 y 404 de la ley, sin embargo, carecen de ciertos lineamientos para obtener las mejores prácticas.

Por ello, CoBIT es el marco de referencia empleado para el cumplimiento de la ley SOX, ya que al ser un Framework que contempla lo mejor de cada estándar internacional, su campo de acción es muy amplio.

A continuación, para poder obtener las mejores prácticas en el cumplimiento de la ley SOX, se muestra la siguiente figura que contempla el marco COSO, CoBIT y las secciones de la ley SOX.

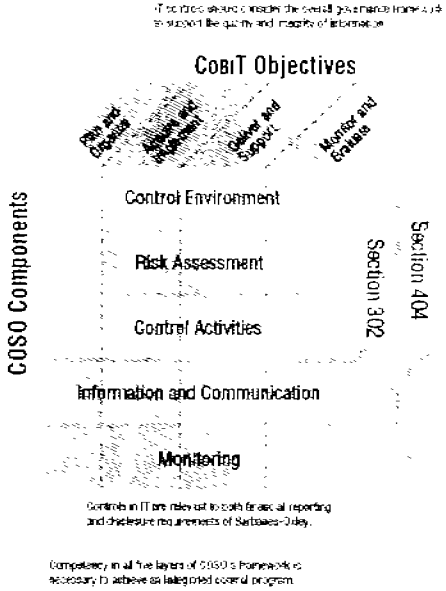

Figura 21 Componentes de control interno

[45] ITIL: Estándar internacional encaminado a los Servicios de TI

4.3.2 Controles de TI. Desafío Único

La ley SOX responsabiliza a los ejecutivos de la organización la evaluación y monitoreo de la efectividad del control interno sobre el reporte financiero. Para la mayoría de las organizaciones, el papel de la tecnología de información es crucial para lograr los objetivos del negocio. Si a través de un sistema ERP (SAP, PeopleSoft, JD Edwards) unificado o una colección de software operacional y administración financiera de aplicaciones, con la tecnología de información se implementa un sistema eficaz de control interno para generar los reportes financieros.

Esta situación crea un único desafío, muchos profesionales de TI son responsables de la calidad e integridad de la información generada por los sistemas de información, basados en que no se encuentran en las complejidades del control interno. Esto sugiere que un riesgo no administrado por TI, sino que no puede formalizarse o estructurarse por requerimientos de la administración de la organización o sus auditores, no pueda ser mitigado.

Las organizaciones necesitan personal de TI en sus equipos de trabajo para el cumplimiento de la ley SOX para asegurarse que los controles generales de TI y los controles aplicativos existan y apoyan los objetivos del negocio. Algunas de las áreas de responsabilidad de TI incluyen:

- Mantenimiento de los planes de control interno de las organizaciones y el procedimiento del reporte financiero
- Mapeo de los sistemas de TI que apoyan el control interno y el procedimiento del reporte financiero informando la situación financiera de la organización
- Identificación de riesgos relacionados con sistemas de TI
- Diseño e implementación de controles diseñados para mitigar los riesgos identificados y monitorear los controles efectivos
- Documentar y probar los controles de TI
- Demostrar que la actualización y cambios en los controles de TI corresponden con los cambios en el control interno o en los procedimientos del reporte financiero
- Monitorear que los controles de TI son efectivos con la operación eficaz del negocio
- Participación de TI en el proyecto de administración de la ley SOX

Mientras algunas industrias, como las de servicios financieros, están familiarizadas con regulaciones estrictas y requerimientos complejos de los mercados financieros, otras no. Al conocer la exigencia de la ley SOX, la mayoría de las organizaciones requerirán cambios culturales. Probablemente las mejoras a los sistemas de información y procesos no requieran tantos cambios, pero es notable que el diseño, documentación, retención de evidencia del control y evaluación de controles de TI si se vean afectados. Porque el costo del incumplimiento puede devastar a la organización, por ello es crucial adoptar medidas y tomar el desafío inmediatamente.

4.3.3 Ejecución de la ley SOX

Debe entenderse que la aplicación de la ley SOX a una organización – basada en características de negocio – puede ayudar en el desarrollo de programas de controles internos. Muchos factores juegan un papel importante, y las grandes corporaciones enfrentarán los desafíos de la ley al igual que las pequeñas. Sin embargo, la magnitud de la fortaleza de los controles internos está dándole sentido a sus actividades.

La ejecución de la ley SOX, ilustrada en la figura 22, muestra la dirección que los profesionales de TI deben conocer para enfrentar los desafíos de la ley SOX. Debe integrarse con los objetivos del negocio llevados al proceso global de la organización. Desde que los controles generales de TI requieren una base de conocimiento, la responsabilidad de los proveedores de servicios de TI se define e implementa para obtener lo que se denomina "mejores prácticas".

Sin embargo, incluso los reportes financieros, firmados por la organización (CEO y/o CFO), no muestran la firma del personal de TI. Esto aplica por lo regular cuando una organización tiene outsourcing. Para los controles aplicativos de TI, el negocio, debe definir los controles requeridos, especialmente para los sistemas financieros que son a menudo complejos por naturaleza, desde la perspectiva de la organización.

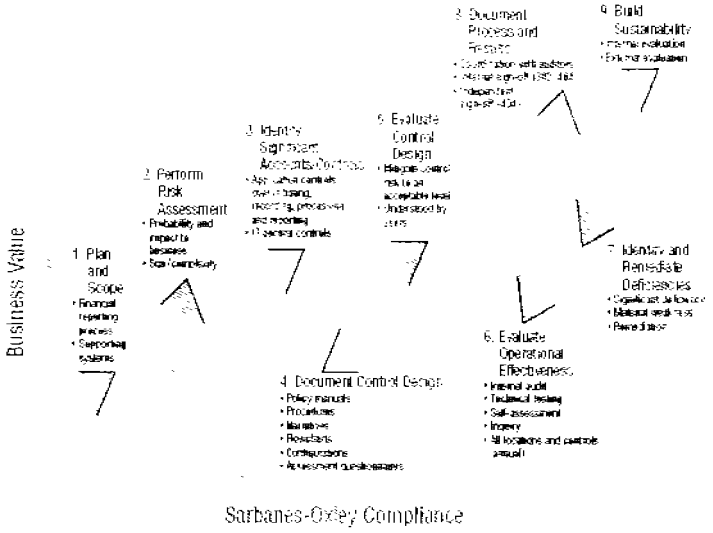

Figura 22 Ruta de ejecución de la ley SOX

4.3.4 Objetivos de Control de TI para la ley SOX

Esta fase es de gran importancia para TI al preparar el cumplimiento a la ley SOX, el enfoque vuelve a los objetivos de control específicos de la organización que son punta de partida para el programa de control de TI.

La figura 23 y 24 muestran los procesos de TI para CoBIT y su relación con el marco de referencia COSO. Se evidencia que los procesos TI de CoBIT están relacionados con los componentes de COSO. Esto es debido a la naturaleza de los controles generales de TI y a sus atributos básicos de relación que demuestran porque los controles de TI son la base de otros controles y en especial de aquellos del programa de control interno. CoBIT es una referencia para el marco de referencia de para la administración de riesgo y controles de TI, comprendido por 4 dominios (PO, AI, DS y M), 34 procesos y 318 objetivos de control. CoBIT incluye controles que dan directrices operacionales y objetivos de alto nivel, pero solo aquellos que se relacionan con el cumplimiento de la ley SOX se muestran en las figuras siguientes:

			COSO Component				
Company Level	Activity Level	CobiT Area	Control Environment	Risk Assessment	Control Activities	Information and Communication	Monitoring
		Plan and Organize (IT Environment)					
●		IT strategic planning	●	●		●	●
●		Information architecture			●	●	
		Determine technological direction					
●		IT organization and relationships	●			●	
		Manage the IT investment					
●		Communication of management aims and direction	●			●	●
●		Management of human resources	●			●	
●		Compliance with external requirements				●	●
●		Assessment of risks		●			
		Manage projects					
●		Management of quality	●		●	●	●
		Acquire and Implement (Program Development and Program Change)					
		Identify automated solutions					
	●	Acquire or develop application software			●		
	●	Acquire technology infrastructure			●		
	●	Develop and maintain policies and procedures			●	●	
	●	Install and test application software and technology infrastructure			●		
	●	Manage changes			●		●

Figura 23 Componentes COSO / CoBIT

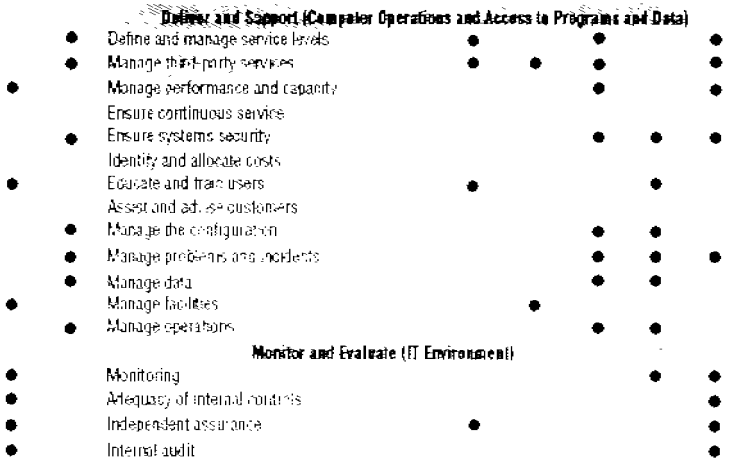

Figura 24 Componentes COSO / CoBIT

4.3.5 Llenado de Matriz de Riesgo y Controles

Ya explicamos con anterioridad, que la sección 404 de la ley SOX menciona que deben existir procedimientos y políticas que aseguren la integridad de la información así como la disponibilidad de ella. Para ello, una forma de evaluar esta sección, es utilizando matrices de riesgo y controles, definidas como una herramienta para dar orden a los controles que sean probados por su clasificación de riesgo.

Cabe señalar que las matrices de riesgo y controles pueden ser aplicadas para:

- Aplicaciones (ERP's como SAP, PeopleSoft, Desarrollos Internos, etc.)
- Bases de Datos (Oracle, Informix, Sybase, etc.)
- Sistemas Operativos (Unix, Solaris, HP-UX, etc.)

La naturaleza de las matrices no limita su uso exclusivamente a un sistema de información, sino que son una guía eficaz de presentar a los niveles directivos, el análisis resumido de los controles que se tienen hasta el momento dentro de la organización.

La ley SOX estipula que los controles de TI deben evaluarse en base al estado en que se tomen, es decir, que la "fotografía" tomada de la organización en un tiempo determinado, y corresponderá a los controles implementados hasta ese momento; las fallas de control detectadas, se enviarán a un plan de remediación, mismo que la organización se encargará de darle seguimiento y ejecución, acordes a las recomendaciones otorgadas por el grupo de auditores contratados.

A continuación, desglosaremos un pequeño formato de llenado de una matriz de riesgo y controles, aplicables a la evaluación de la sección 404 de la ley SOX:

Encabezado: Dividido en dos secciones:

- Evaluación del Diseño de los Controles[46]:
  Se refiere a las características que aplican a los riesgos y controles examinados dentro de un organismo, subsidiaria o dirección corporativa. En esta parte tenemos que analizar las características actuales del control dentro del procedimiento.

- Plan de Remediación:
  Ante debilidades de control se deben proponer acciones necesarias para fortalecer los controles o bien crearlos (si estuviesen ausentes), con el fin de mitigar un riesgo.

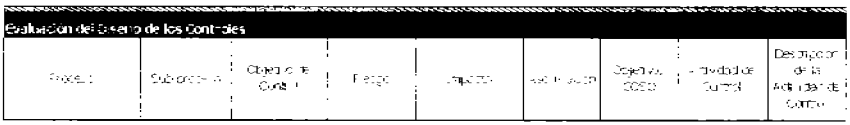

Figura 25 Evaluación del Diseño de los Controles

- Proceso:
  Es el macroproceso a evaluar, éste encierra uno o varios objetivos de control

- Sub proceso:
  En esta parte se explica el subproceso, mismo que debe ser acorde al macroproceso anteriormente descrito.

- Objetivo de Control:
  Aquí se explica claramente cuál es el objetivo que se desea alcanzar al implementar el control.

- Riesgo:
  Describe el riesgo en el que se incurriría, en el caso de NO alcanzar el objetivo de control.

- Impacto:
  Es una cuantificación del posible impacto en los Estados Financieros en caso de NO alcanzar el objetivo de control (es una combinación de la consecuencia financiera que produciría y la probabilidad de ocurrencia), se clasifica en: Alto, Medio y Bajo.

- Aseveración de los Estados Financieros:
  Se refiere a las afirmaciones que se intentan probar mediante el objetivo de control, y que se hallan amenazadas por un riesgo. Se clasifican en: Integridad,

[46] Inclusive, ésta parte es llamada AS IS

Existencia, Exposición, Derechos y Obligaciones, Valuación, Autorización, Oportunidad, Salvaguarda de Activos.

- Objetivos COSO:
  Son los Objetivos del Control Interno según el enfoque COSO:
  - Eficacia y eficiencia en las operaciones (E).
  - Confiabilidad de la información financiera (F).
  - Cumplimiento de las leyes y normas aplicables (C)

- Actividades de Control:
  Corresponde al nombre de la actividad de control.

- Descripción de la Actividad de Control:
  En esta parte, se describe en forma sintética las principales características que se espera cumpla dicha actividad de control (como se desconoce con exactitud el funcionamiento en cada proceso, se pueden incorporar ejemplos que sirvan de guía).

Hasta aquí hemos descrito la forma de llenar una matriz de riesgo y controles, esta sección se denomina también "AS IS", ya que describe el control tal y como debería llevarse, todo esto basado en las buenas prácticas de los marcos de Referencia de COSO y/o CoBIT.

La siguiente sección, describe la forma de llenar la matriz a través de entrevista directa con los usuarios, esta parte se denomina el "TO BE" o bien la forma en que se lleva el control por parte de la organización; a continuación, profundizaremos sobre las columnas que contiene.

Evaluación del Diseño de los Controles								
Descripción del Funcionamiento de Control	Referencia Documental	Evidencia		Automatizado				
		SI / NO	Descripción	SI / NO	Plataforma	Aplicación	Parametrizable	Ubicación Física

Figura 26 Evaluación del Diseño de los Controles

- Descripción del funcionamiento del control:
  Se refiere a la forma en la que se realiza el control en la organización. Es muy aceptable transcribir el control de acuerdo al narrativo del procedimiento (si el mismo está bien redactado).

- Referencia documental:
  Se colocará el código con el cual se identifica este control dentro del diagrama de flujo del proceso, o bien una referencia al procedimiento narrativo donde se describe el control.

- Evidencia: Existen 2 campos a completar:
  a) Si existe o no evidencia de que se realice el control

b) En caso afirmativo, describir las evidencias que se conservan como respaldo del control. Se espera además que se guarden papeles de trabajo dicha evidencia.

- Automatizado: Existen 5 campos a completar:
  a) Si son o no realizados por un sistema de información (sin intervención humana y en base a parámetros preestablecidos)
  b) La plataforma sobre la cual opera el control (Ejemplo: Oracle)
  c) La aplicación sobre la cual opera el control (Ejemplo: SAP R3)
  d) Si son o no parametrizables. Los controles automáticos siempre son controles parametrizables.
  e) La localización física de los controles. Comúnmente corresponde a la localización física del equipo servidor.

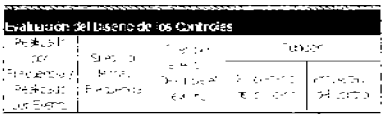

Figura 27 Evaluación del Diseño de los Controles

- Realizado por:
  Se refiere a la periodicidad con la que se realiza el control. Se debe aclarar si se realiza en un momento determinado por intervalos establecidos (por Frecuencia) o bien si se realiza dependiendo de la ocurrencia de un determinado hecho (por Evento).

- Si es por Frecuencia:
  Indicar la frecuencia con la que se realiza: Anual, Semestral, Trimestral, Mensual, Diario, Varias veces al día.

- Si es por Evento:
  Describir el / los eventos, de los cuales depende la realización del control.

A partir de aquí indicaremos las características del control.

- Función:
  En esta casilla debemos especificar, el puesto y nombre del dueño del proceso y del dueño del control.
  - Propietario del proceso:
    Se refiere a la persona responsable por el proceso.
  - Propietario del control:
    Se refiere a la persona responsable del cumplimiento del control. Por lo general es la persona que ejecuta el control.

Figura 28 Evaluación del Diseño de los Controles

- Relevancia del Control:
  Colocar en esta casilla solamente una letra: "C" si es "Control Clave", (si el control –en el supuesto de funcionar de manera eficaz – es útil para mantener bajo control un riesgo significativo).

- Tipo de Control:
  Se colocará en esta casilla el tipo de control, puede ser Detectivo (D), Preventivo (P) o Correctivo (C). Se debe distinguir si el control se realiza para detectar errores, omisiones o irregularidades, o bien se realiza con para prevenir la ocurrencia de dichos problemas.

- Naturaleza del Control:
  Indicar en esta casilla si la naturaleza del control es de: Autorización / Comparación / Conciliación / Acceso restringido / Otro (colocar).

- Calificación del Control:
  Dependiendo del análisis del AS IS vs. TO BE, el control se evaluará en su diseño de la siguiente manera: (C): CUMPLE / (CP): CUMPLE PARCIALMENTE / (NC): NO CUMPLE / (NA): NO APLICA.

- Será Probado?:
  Haciendo una evaluación del impacto del control, en estados financieros, se determinará en conjunto con el Comité Operativo de la organización si se harán pruebas de efectividad de los controles.

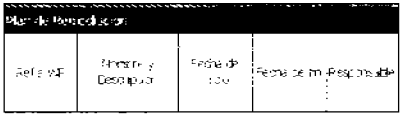

Figura 29 Evaluación del Diseño de los Controles

- Ref a WP:
  En esta casilla se colocará los papeles de trabajo que hacen referencia a la actividad de control, mismos que se obtuvieron en el proceso de evaluación de los objetivos de control.

- Nombre y Descripción:
  En esta casilla se indicará el nombre del plan (se debería dar una denominación). La Descripción debe ser en forma clara, como la corrección propuesta y la manera en que se llevará a cabo la rectificación de la debilidad detectada.

- Fecha de Inicio:
  Fecha estimada del momento en que se comenzará a realizar la(s) medida(s) necesarias para rectificar la falla de control.

- Fecha de Fin:
  Fecha estimada en la cual el dueño del proceso se compromete a concluir e implementar el plan de remediación para mitigar las fallas detectadas en los objetivos de control.

- Responsable:
  En esta casilla, la organización deberá anotar el nombre de la persona responsable del cumplimiento (dueño del proceso) de la actividad del control.

CAPÍTULO 5. Certificación CISA, CISM y CISSP

5.1 Antecedentes

La ISACA (Information Systems Audit And Control Association) es una asociación formada en 1967 cuando un grupo de personas con trabajos y actividades similares – controles de auditoría en sistemas computarizados que se estaban haciendo cada vez más críticos para las operaciones – se sentaron a discutir la necesidad de tener una fuente central de información y guía en el campo. En 1969 se formalizó el grupo, incorporándose bajo en nombre de EDP Auditors Association (Asociación de Auditores de Procesamiento Electrónico de Datos). En 1976, la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimiento y el valor del campo de gobernación y control de Tecnología de Información (TI).

Hoy, los miembros de ISACA – más de 47,000 en todo el mundo, y más de 400 en México – se caracterizan por su diversidad. Los miembros viven y trabajan en más de 140 países y cubren una variedad de puestos profesionales relacionados con TI (sólo para nombrar algunos ejemplos, Auditor de SI, Consultor, Educador, Profesional de Seguridad de SI, Regulador, Director Ejecutivo de Información y Auditor Interno). Algunos son nuevos en el campo, otros están en niveles medios de supervisión y algunos otros están en los rangos más elevados. Trabajan en casi todas las categorías de industrias, incluyendo finanzas y banca, contaduría pública, gobierno y sector público. Esta diversidad permite a los miembros que aprendan unos de otros, e intercambien puntos de vista con divergencias significativas en una variedad de tópicos profesionales. Ha sido considerada durante largo tiempo como uno de los puntos fuertes de ISACA.

Otro de los puntos fuertes de ISACA es su red de capítulos. ISACA tiene capítulos en más de 60 países en todo el mundo, y dichos capítulos brindan a los miembros educación, recursos compartidos, promoción, contactos profesionales y una amplia gama de beneficios adicionales a nivel local.

En los treinta años desde su creación, ISACA se ha convertido en una organización global que establece pautas para los profesionales de Gobernabilidad, Control, Seguridad y Auditoría de Información. Sus normas de Auditoría y Control de Sistemas de Información son respetadas por profesionales de todo el mundo, sus investigaciones resaltan temas profesionales que desafían a sus constituyentes.

ISACA publica un periódico técnico líder en el campo de control de la información, el Periódico de Control de Sistemas de Información (Information Systems Control Journal). Organiza una serie de conferencias internacionales que se concentran en tópicos técnicos y administrativos pertinentes a las profesiones de Gobierno de TI y Aseguramiento, Control, Seguridad de Sistemas de Información. Juntos, ISACA y el Instituto de Gobernabilidad de TI (IT Governance Institute) asociado lideran la comunidad de control de TI y sirven a sus practicantes brindando los elementos que necesitan los profesionales de TI en un entorno mundial en cambio permanente.

5.1.1 Tipos de Certificación

ISACA ofrece dos tipos de certificaciones para los especialistas de Tecnología de Información, mismas que son reconocidas a nivel mundial. Su certificación CISA (Certified Information Systems Auditor) o Auditor Certificado de Sistemas de Información es reconocida en forma global y ha sido obtenida por más de 40,000 profesionales. Su nueva certificación CISM (Certified Information Security Manager) o Gerente Certificado de Seguridad de Información se concentra exclusivamente en el sector de Gerencia de Seguridad de la Información (en México se esta implementado la Certificación CISM a partir del año 2006).

5.1.2 Certificación CISA

ISACA (Asociación de Auditoría y Control de Sistemas de Información), ofrece entre sus alternativas a los profesionales de TI, la Certificación de Auditor de Sistemas de Información (CISA), administrada por el Comité de Certificación de la Asociación y tiene la responsabilidad de velar por el programa de Certificación CISA y su administración

Establecida en 1978, el programa de certificación CISA de la prestigiosa organización ISACA se ha convertido en el programa de certificación internacional de referencia para evaluar y acreditar la competencia de profesionales del sector de la Auditoría de Sistemas y Seguridad de la Información.

La certificación CISA goza de gran reputación tanto a nivel nacional como internacional. Es una certificación de referencia para las empresas auditoras y consultoras, e incluso en numerosos concursos públicos de administración.

Esta certificación va dirigida específicamente a:

1 Profesionales del sector de las Tecnologías de Información interesados o con responsabilidad en Control Interno, Seguridad y Auditoría de Sistemas de Información
2 Gerentes y especialistas de alto nivel con responsabilidad en áreas de seguridad en todo tipo de empresas y organizaciones
3 Responsables o Gerentes de Sistemas de Información
4 Responsables de Organización y Calidad de empresas y administraciones públicas
5 Consultores y Asesores en TI de empresas y administraciones públicas
6 Especialistas en protección de datos que necesiten avalar su trabajo con un certificado internacional
7 Auditores contables y financieros, que deseen adquirir una especialización en Control Interno y Auditoría de Sistemas de Información
8 Profesionales del derecho implicados en áreas de nuevas Tecnologías, Control Interno, Seguridad y Auditoría de Sistemas de Información

5.1.2.1 Requerimientos para la Certificación

La designación CISA es un reconocimiento a los individuos interesados en la Auditoría, Control y Seguridad de los Sistemas de Información que cumplen con lo siguiente:

1 Aprobar exitosamente el examen CISA (75 puntos al menos en cada módulo)
2 Experiencia en Auditoría, Control y Seguridad de Sistemas de Información
3 Código de Ética Profesional
4 Programa de Educación continua

5.1.2.1.1 Aprobar Exitosamente el Examen CISA[47]

La examinación está abierta a todos los individuos que tienen interés en el campo de la Auditoría, Control y Seguridad de Sistemas de Información. En base a las numerosas tareas ejecutadas por los profesionales de la Auditoría, Control y Seguridad de Sistemas de Información, ISACA relacionó y clasificó los temas en siete dominios que contienen el trabajo profesional de la Auditoría, Control y Seguridad de Sistemas de Información.

Estos dominios fueron clasificados según su grado de importancia para fines de examinación.

1	Dominio 1	El proceso de auditoría de los Sistemas de Información
2	Dominio 2	Gobernabilidad de Tecnologías de Información
3	Dominio 3	Ciclo de Vida de Sistemas e Infraestructura
4	Dominio 4	Entrega y Soporte de Servicios de TI
5	Dominio 5	Protección de los Activos de Información
6	Dominio 6	Recuperación de Desastres y Continuidad del Negocio

5.1.2.1.2 Experiencia como Auditor de Sistemas de Información

El aspirante debe tener un mínimo de cinco años de experiencia en Auditoría de Sistemas de Información, Control o Seguridad requerido para la certificación. Existen algunos ítems que pueden sustituir años de experiencia, como a continuación se menciona:

1 Un máximo de 1 año de experiencia en Sistemas de Información o 1 año en Auditoría Financiera u Operativa puede sustituir 1 año de experiencia en Auditoría, Seguridad o Control en Sistemas de Información.
2 Asimismo, 60 a 120 horas de Universidad (equivalente a estudios de Postgrado) pueden sustituir 1 o 2 años, respectivamente de experiencia en Auditoría, Seguridad y Control en Sistemas de Información, y

[47] Examen CISA 2006: A partir del 2006, el formato del examen cambia a 6 módulos. Fuente: ISACA Internacional

3 2 años como Académico en la universidad en temas relacionados (Ciencias de la Computación, Auditoría de Sistemas de Información, etc.) pueden sustituir 1 año de experiencia en Auditoria, Seguridad y Control en Sistemas de Información.

La experiencia debe ser obtenida dentro de los 10 años precedentes a la fecha de aplicación de la certificación o dentro de los cinco años desde la fecha pasada la certificación.

5.1.2.1.3 Código de Ética Profesional

La Asociación de Auditoría y Control de Sistemas de Información, aplica un Código de Ética Profesional para guiar a los profesionales, miembros de la Asociación en su conducta como personas y profesionales. De esta forma, los auditores certificados CISA deben:

1 Sustentar el establecimiento y cumplimiento apropiado de los estándares, procedimientos y controles de los Sistemas de Información
2 Dar cumplimiento a los estándares de Auditoría en Tecnologías de Información adoptados por la Asociación de Auditoría y Control de Sistemas de Información (ISACA)
3 Servir en beneficio de sus empleados, accionistas, clientes y el público en general, en forma diligente, leal y honesta, y no pertenecer bajo conocimiento, a ninguna sociedad ilegal o de actividades impropias
4 Mantener la confidencialidad de la información obtenida durante el transcurso de sus deberes. Esta información no deberá ser utilizada en beneficio personal ni entregada a grupos inapropiados
5 Realizar sus tareas en forma independiente y objetiva. Deberán evitar actividades que amenacen o que pretendan amenazar su independencia
6 Mantener la competencia en campos interrelacionados con la Auditoría en Tecnología de Información mediante la participación en actividades de desarrollo profesional
7 Actuar con precaución en la obtención de documentación suficiente de hechos en los cuales se base para sus conclusiones y recomendaciones
8 Informar a las partes apropiadas sobre los resultados del trabajo de auditoría realizados
9 Promover la educación de la gerencia, clientes y público en general para reforzar el entendimiento sobre la Auditoría en Tecnologías de Información
10 Mantener altos estándares de conducta y carácter tanto en las actividades personales como profesionales

5.1.2.1.4 Política de Educación Continua

Los objetivos del Programa de Educación Continua son:

1 Mantener la competencia individual como requisito para actualizar los conocimientos y destrezas en las áreas de la Auditoría de Sistemas de Información,

Administración, Contabilidad y Áreas de Negocios relacionadas a industrias específicas

2 Proveer un medio para diferenciarse entre los Auditores Certificados CISA y quienes aún no alcanzan los requisitos para continuar con su certificación
3 Proveer un mecanismo para Monitorear el mantenimiento de Profesionales en Auditoría de Sistemas de Información, Control y Seguridad
4 Ayudar a la Administración Ejecutiva a desarrollar Auditorías de Seguridad y Control de Sistemas de Información, proporcionando sensatez y criterio para la selección de personal, y
5 Mantener una cuota anual y un mínimo de 20 horas de Educación Continua son requeridos anualmente. Además de un mínimo de 120 horas de educación durante un periodo de 3 años.

5.1.3 Certificación CISM

Otra de las certificaciones ofrecidas por ISACA (Asociación de Auditoría y Control de Sistemas de Información) es la Certificación de Gestión de Sistemas de Información (CISM): programa desarrollado específicamente para los experto en la Administración de Seguridad de la Información y Administradores responsables de la Seguridad de la Información. La certificación CISM va dirigida a administradores, diseñadores, gerentes y/o encargados de la Seguridad de la Información en las empresas.

La certificación CISM promueve prácticas internacionales y provee aseguramiento a la Gerencia Ejecutiva de la experiencia y conocimiento requeridos para proporcionar eficiencia en la Seguridad y servicios que consultan. Los individuos certificados se convierten en parte de una red de élite, obteniendo una credencial premier. El trabajo de los especialistas CISM también define una descripción de las funciones globales para que el encargado de la Seguridad de la Información mida al personal existente y compare con nuevos principios.

Aunque la certificación CISM es reconocida mundialmente, no es obligatoria en este momento, un creciente número de organizaciones requiere empleados que se certifiquen. Para ayudar a asegurar el éxito en el mercado global, es vital seleccionar el programa de certificación basado en Prácticas de Administración de Seguridad de la Información universalmente aceptadas.

5.1.3.1 Requerimientos para la Certificación

La certificación CISM es un reconocimiento a todos los profesionales interesados en la Seguridad de la información, para obtener dicha certificación, los candidatos requieren:

1. Aprobar exitosamente el examen CISM
2. Código de Ética Profesional

3. Programa de Educación continua
4. Experiencia en Seguridad de la Información

5.1.3.1.1 Aprobar Exitosamente el Examen CISM

El candidato que desea ser Gerente Certificado en Seguridad de la Información (CISM) requiere un puntaje alto en el examen, o bien, sin tener la experiencia profesional requerida, ésta será valida por cinco años. Si el aspirante no cumple con los requisitos de la certificación dentro de los cinco años posteriores a la fecha de examen, su certificación será removida.

5.1.3.1.2 Código de Ética Profesional

La Asociación de Auditoría y Control de Sistemas de Información, aplica un Código de Ética Profesional para guiar a los profesionales, miembros de la Asociación en su conducta como personas y profesionales. De esta forma, los auditores certificados CISA deben:

1. Sustentar el establecimiento y cumplimiento apropiado de los estándares, procedimientos y controles de los Sistemas de Información
2. Dar cumplimiento a los estándares de Auditoría en Tecnologías de Información adoptados por la Asociación de Auditoría y Control de Sistemas de Información (ISACA)
3. Servir en beneficio de sus empleados, accionistas, clientes y el público en general, en forma diligente, leal y honesta, y no pertenecer bajo conocimiento, a ninguna sociedad ilegal o de actividades impropias
4. Mantener la confidencialidad de la información obtenida durante el transcurso de sus deberes. Esta información no deberá ser utilizada en beneficio personal ni entregada a grupos inapropiados
5. Realizar sus tareas en forma independiente y objetiva. Deberán evitar actividades que amenacen o que pretendan amenazar su independencia
6. Mantener la competencia en campos interrelacionados con la Auditoría en Tecnología de Información mediante la participación en actividades de desarrollo profesional
7. Actuar con precaución en la obtención de documentación suficiente de hechos en los cuales se base para sus conclusiones y recomendaciones
8. Informar a las partes apropiadas sobre los resultados del trabajo de auditoría realizados
9. Promover la educación de la gerencia, clientes y público en general para reforzar el entendimiento sobre la Auditoría en Tecnologías de Información
10. Mantener altos estándares de conducta y carácter tanto en las actividades personales como profesionales

5.1.3.1.3 Política de Educación Continua

Los objetivos del Programa de Educación Continua son:

1. Mantener la competencia individual como requisito para actualizar los conocimientos y destrezas en las áreas de la Auditoría de Sistemas de Información, Administración, Contabilidad y Áreas de Negocios relacionadas a industrias específicas
2. Proveer un medio para diferenciarse entre los Auditores Certificados CISM y quienes aún no alcanzan los requisitos para continuar con su certificación
3. Proveer un mecanismo para Monitorear el mantenimiento de las competencias de los Auditores de Sistemas de Información, Control y Seguridad
4. Ayudar a la Administración Ejecutiva a desarrollar Auditorías de Seguridad y Control de Sistemas de Información, proporcionando sensatez y criterio para la selección de personal, y
5. Mantener una cuota anual y un mínimo de 20 horas de Educación Continua requeridas anualmente. Además de un mínimo de 120 horas de educación durante un periodo de 3 años.

5.1.3.1.4 Experiencia en Seguridad de la Información

El aspirante debe tener un mínimo de cinco años de experiencia en Seguridad de la Información, con un mínimo de 3 años como Gerente de Seguridad de la Información en 3 o más prácticas laborales. Existen algunos ítems que pueden sustituir años de experiencia, como a continuación se menciona:

Dos años:

- Auditor Certificado en Sistemas de Información (CISA) es un buen comienzo
- Profesional Certificado en Seguridad de Sistemas de Información (CISSP) es un buen comienzo
- Postgrado en campos relacionados de Seguridad de la Información (Administrador de negocios, Sistemas de Información, Aseguramiento de la Información)

Un año:

- Un año de experiencia como Gerente o Administrador de Sistemas de Información
- Tener bases de otras certificaciones (SANS, Certificación de Aseguramiento Global de Información (GIAC), Ingeniero de Sistemas Microsoft Certificado (MCSE), Seguridad CompTIA, etc.)

La experiencia sustituida no exime el requisito de tres años de experiencia profesional como Gerente de Seguridad de la Información.

5.2 ISC², Seguridad Informática

El ISC² (International Information Systems Security Certification Consortium Inc)[48] es una organización no lucrativa, incorporada a la Comisión de Massachussets, con sede en Palm Harbor, Florida. Con sede en Viena (Virginia, Estados Unidos) y con delegaciones en Londres y Hong Kong. Es la principal organización mundial dedicada a difundir a los profesionales y expertos en seguridad de la información el estándar de certificación profesional del CBK[49] de ISC², un compendio de los métodos óptimos de seguridad de la información.

Desde su constitución en 1989, esta organización sin fines de lucro ha proporcionado formación y certificaciones con el objeto de promover estándares de seguridad unificados. ISC² expide la certificación CISSP (Certified Information Systems Security Professional), que requiere años de experiencia en el terreno profesional y el respaldo de un profesional familiarizado con la formación profesional del candidato.

5.2.1 Certificación CISSP

La certificación CISSP, es la primera acreditada por ANSI del estándar ISO 17024:2003 en el área de Seguridad de Información. La certificación provee a los Profesionales de Seguridad de Información no solo una medida objetiva de capacidad, sino un reconocimiento global. La Certificación CISSP demuestra la capacidad del individuo en los 10 capítulos o dominios que componen el CBK (Common Body of Knowledge). Estos diez capítulos, son:

1. Prácticas en la Gestión de la Seguridad
2. Sistema de Control de Acceso y Metodología
3. Seguridad de Operaciones
4. Seguridad en Redes, Telecomunicaciones e Internet
5. Criptografía
6. Arquitectura de Seguridad y Modelos
7. Seguridad en el Desarrollo de Sistemas y Aplicaciones
8. Plan de Continuidad del Negocio (BCP) y Plan de Recuperación de Desastres (DRP).
9. Seguridad Física
10. Leyes, Investigaciones y Ética

La certificación CISSP se considera la máxima acreditación en Seguridad Informática y la otorga el consorcio ISC² a aquellos profesionales de seguridad que superan con éxito un

[48] ISC2: Organización no lucrativa especializada en Seguridad de Sistemas con sede en Palm Harbor, Florida
[49] CBK: Common Body of Knowledge

completo examen, poseen 4 años de experiencia en el campo de la seguridad, se adhieren al código ético de ISC^2 y son avalados por un CISSP o profesional equivalente.

5.2.1.1 Requerimientos para la Certificación

Para obtener la certificación CISSP de la ISC^2 los profesionales de seguridad de la información requiere:

1. Aprobar el examen con un puntaje de 700/1000 puntos o superior
2. Contar con al menos cuatro años de experiencia en alguno de los 10 dominios de la CBK CISSP, o tres años de experiencia y contar con un título universitario.
3. Enviar el formulario de consentimiento adecuadamente completado, firmado por un CISSP o superior.
4. Dar respuesta adecuada a la auditoría que se efectúe, en caso de ser seleccionado aleatoriamente para la misma.
5. Suscribirse al Código de Ética de la ISC^2.

Conclusiones Generales

Las empresas mexicanas deben asegurar sus procesos ayudados por tecnologías de información como lo son ERP's. SCM y CRM, estas 3 áreas complementan la cadena de valor de los productos y especialmente el SCM ayuda a controlar los procesos que se tienen de manera externa y que de alguna manera no se tiene un control total de ellos.

Por otro lado, el cumplimiento de la ley SOX obliga a las empresas a asegurar sus procesos y certificarlos en diferentes normas internacionales como lo son el ISO 9000 y 14000.

Aunado a que el corazón de los procesos de las organizaciones son las Tecnologías de Información, es indispensable pensar ya en la norma ISO 17799. La norma ISO 17799 (derivada de la BS7799-1) menciona a 3 grandes áreas que son el aseguramiento de la información mediante la confidencialidad, integridad y disponibilidad de la información, que en palabras de la ley SOX, y la administración de la cadena de proveedores es la que debe de asegurar que la información financiera de las organizaciones no sea alterada de manera dolosa o no intencional, que además se puede acceder a ella en el momento que se requiera y que además sea confidencial y de acceso controlado.

Pareciera que la ley Sarbanes Oxley no tiene nada que ver con el área de las Tecnologías de Información y mucho menos con la cadena de proveedores y su administración, pero en este análisis realizado para este diseño de proyecto, podemos ver como de manera directa las empresas proveedoras de productos tiene incluso una relación directa con una de las secciones de la ley.

El asegurar el cumplimiento de la ley SOX es un mecanismo complejo que requiere tiempo, inversión y sobre todo certeza de que los objetivos de control interno deben mitigarse hasta lograr obtener la certificación. Actualmente la información es poder y en la ley Sarbanes Oxley en relación con la administración de la cadena de proveedores toma un verdadero sentido ya que la buena administración de la cadena puede evitar que una empresa pierda dinero y sobre todo pueda dar al cliente lo pactado en cuanto a tiempo de entrega y servicio

APÉNDICE

Terminología Básica

Administración / Gerencia:
Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información frecuentemente impredecible.

Administración de Riesgos (Risk Management):
Proceso de identificar, analizar, controlar, evaluar y otorgar seguimiento a los distintos elementos que conforman el riesgo.

Análisis de Riesgos (Risk Analysis):
El potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a los mismos. El impacto o severidad relativa del riesgo es proporcional al valor para el negocio, de las pérdidas o daños y a la frecuencia estimada de la amenaza

Amenazas:
Cualquier circunstancia o evento con el potencial de dañar un recurso de TI tal como destrucción, revelación, modificación de datos y/o negación de servicio.

Auditor:
Encargado de realizar un estudio de análisis y riesgos. Véase Auditoría

Auditoría (Audit):
Proceso sistemático por el cual una persona competente e independiente obtiene y evalúa objetivamente evidencia relativa a aseveraciones sobre una entidad o evento económico, con el propósito de formarse una opinión y reportar el grado en que la aseveración está acorde con un conjunto de estándares identificados.

Auditoría Basada en Controles (Controls Based Auditing):
Auditorías que usan el Sistema de Control Interno como su Objetivo de la Auditoría. *Vea para contraste Auditoría Basada en Riesgos.*

Auditoría Basada en Riesgos (Risk Based Auditing):
Auditorías que enfocan en el riesgo y Administración de Riesgos como el Objetivo de la Auditoría. Para contraste *vea Auditoría Basada en Controles.*

Auditoría forense:
Es el uso de técnicas de investigación, integradas con la contabilidad y con habilidades de negocio, para brindar información y opiniones, como evidencia en la corte.

Auditoría de Sistemas de Información:
Proceso de recolección y evaluación de evidencia para determinar si los sistemas de información y los recursos relacionados: Salvaguardan adecuadamente los activos, Mantienen la integridad de los datos y del sistema, Proveen información relevante y confiable, Alcanzan efectivamente los objetivos organizacionales, Consumen los recursos eficientemente, y Cuentan con controles internos que provean una seguridad razonable de que los objetivos operacionales y de control serán satisfechos y de que los eventos no deseados serán prevenidos o detectados y corregidos de manera oportuna.

BS7799:
Es una norma que presenta los requisitos para un Sistema de Gestión de Seguridad de la Información (*Véase ISMS*). Ayudará a identificar, administrar y minimizar la gama de amenazas a las cuales está expuesta regularmente la información.

CBK:
Common Body of Knowledge, definida como la Base Común de Conocimientos requerida por la ISC^2 para obtener la Certificación CISSP. *Véase* ISC^2

CISA:
Certified Information.Systems Auditor. Es la certificación ofrecida por ISACA para aquellos profesionales enfocados en un área de tecnología de información interesados o con responsabilidad en control interno, seguridad y auditoría de sistemas de información.

Los candidatos a la Certificación CISA deben contar con experiencia profesional mínima de cinco años en Auditoría, Control y Seguridad de Sistemas de Información antes de presentarse al examen CISA y cada año deben tomar cursos de educación continua. *Véase ISACA*.

CISM:
Certified Information Security Manager. También bajo el auspicio de ISACA, la certificación CISM se centra exclusivamente en la administración de seguridad de la información.

Los candidatos a la certificación CISM deben tener al menos cinco años de experiencia en seguridad de la información y un mínimo de tres años de experiencia en gestión de seguridad de la información. Es requisito fundamental para los que obtengan la certificación CISM completar un mínimo de 20 horas de Educación Profesional Continua por año.

CISSP:
Certificación otorgada por la ISC^2, la cual se considera la máxima acreditación en seguridad informática otorgada a aquellos profesionales de seguridad que superan con éxito un completo examen, poseen 4 años de experiencia en el campo de la seguridad, se adhieren al Código Ético de la ISC^2 y son avalados por un CISSP o profesional equivalente.

CoBIT:
Marco de Referencia denominado Objetivos de Control para Tecnologías de Información y Tecnologías relacionadas, basado en la premisa de un Gobierno Corporativo y Gobierno de TI. CoBIT es un modelo estructurado, lógico de mejores prácticas de Tecnología de Información, definidas por un consenso de expertos en todo el mundo en aspectos técnicos, seguridad, riesgos, calidad y control

Cómputo Forense:
Véase Auditoría forense

Confidencialidad:
Principio de la información que garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

Control:
Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos

Control Interno (Internal Control):
Todos los medios, tangibles e intangibles, que se emplean o se usan para asegurar que los objetivos establecidos se alcanzan.

COSO:
Un sistema de controles internos o Estructura de Controles definido por el Comité de Organizaciones Patrocinadores de la Comisión Treadway (USA).

Disponibilidad:
Principio de la información que garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera.

Eficacia:
Capacidad de alcanzar las metas y/o resultados propuestos.

Eficiencia:
Capacidad de producir el máximo de resultados con el mínimo de recursos, energía y tiempo. Se refiere básicamente a los objetivos empresariales.

ERM:
Enterprise Risk Management (Administración de Riesgos Corporativos). Definido como proceso, efectuado por el Comité Ejecutivo de una Entidad, la Gerencia y demás personal, aplicado en un conjunto estratégico y a través de toda la Empresa, designado para identificar potenciales eventos que puedan afectar a la Entidad, y gerenciar los riesgos de acuerdo al apetito sobre dichos riesgos, para proveer razonable aseguramiento acerca del cumplimiento de los objetivos corporativos.

Evaluación de Riesgos (Risk Assessment / Evaluation):
La identificación de riesgos, la medida de riesgos, y el proceso de clasificar los riesgos en orden de prioridad. *Vea Medición de Riesgos.*

Evidencia:
Es un requerimiento que las conclusiones del auditor deben basarse en prueba suficiente y competente.

Gobierno de TI:
Una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el retorno sobre TI y sus procesos.

Gobierno Corporativo:
Es un patrón de comportamiento sistemático del consejo de accionistas, administradores y personal de una organización, que se encuentran concentrados en el logro de resultados financieros sustentables. Este comportamiento debe estar dirigido hacia el logro de los cuatro principales activos de la organización: Infraestructura, Clientes y Terceros Interesados (Stakeholders[50]), Personal Interno, Procesos y la creación de VALOR.

Informática forense:
Es la aplicación legal de métodos, protocolos y técnicas para obtener, analizar y preservar

[50] Stakeholders: Cualquier grupo o individuo que puede afectar a, o puede ser afectado por el logro de los objetivos de una organización.

evidencia digital relevante a una situación en investigación.

Integridad:
Principio de la información que salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

ISACA:
ISACA (Information Systems Audit And Control Association) es la asociación fundada en 1967, encargada a nivel mundial de ofrecer las Certificaciones CISA y CISM.

ISC^2:
International Information Systems Security Certification Consortium. Organización sin fines de lucro dedicada a difundir a profesionales y expertos en seguridad de la información el estándar de certificación profesional de los 10 capítulos o dominios que abarca el CBK. *Véase CBK.*

ISMS:
Acrónimo de Information Security Management System (Sistema de Gestión de Seguridad de la Información), basado en la administración de controles individuales de seguridad, los cuales, cuando se integran como un todo, ayudan a administrar eficazmente los aspectos de seguridad de un negocio completo.

ISO 17799
Conjunto de controles que incluyen las "mejores prácticas" en seguridad informática, ya que es un estándar genérico reconocido a nivel internacional y cuya principal intención es servir como un punto de referencia único para identificar los controles necesarios en la mayoría de las situaciones en los que los sistemas de información se ven involucrados en la industria y el comercio.

Matriz de Riesgos (Risk Matrix):
Una combinación de Medición de Riesgos y Priorización de Riesgos que consiste en el uso de riesgos en el eje horizontal y componentes de sistema o pasos de auditoría en el eje izquierdo. Ambos ejes se ponen en grupos en la esquina izquierda (Alto), creando una matriz con cuadrantes de grupos Alto, Medio y Bajo de componentes y riesgos.

Matriz de Riesgos y Controles (Risk and Control Matrix):
Una herramienta usada para dar orden a los Controles que sean probados por su Clasificación de Riesgo. Vea el método alternativo, Matriz de Riesgos.

Medición de Riesgos (Risk Measurement):
La evaluación de la gravedad de riesgos.

Seguridad de la Información:
Vea Seguridad Informática

Seguridad Informática:
Se define como la preservación de la información de una amplia gama de amenazas a fin de garantizar la continuidad, minimizar el daño y maximizar el retorno sobre las inversiones y las oportunidades, conteniendo los principios de Confidencialidad, Integridad y Disponibilidad.

Objetivo de Control:
Una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

Outsourcing:
Técnica innovadora de administración, que consiste en la transferencia a terceros de ciertos procesos complementarios que no forman parte del giro principal del negocio, permitiendo la concentración de los esfuerzos a las actividades esenciales a fin de obtener competitividad y resultados tangibles.

Planificación Estratégica (Strategic Planning):
Planes a largo plazo basados en los objetivos totales de la empresa. Los planes estratégicos típicamente son para varios años y pueden extenderse hasta 5 o 10 años usando Escenarios u otros métodos de planificación que identifican conjeturas, Riesgos, y factores de Ambiente.

Riesgo (Risk):
Una medida de Incertidumbre. En el proceso comercial, la incertidumbre trata de lograr objetivos organizacionales. Puede consistir en Consecuencias positivas o negativas, aunque la mayoría de los riesgos positivos se llaman Oportunidades y los riesgos negativos se llaman riesgos.

Sistema (System):
Dos o más elementos interrelacionados de cualquier clase que tienen un propósito común.

Stakeholders: Cualquier grupo o individuo que puede afectar a, o puede ser afectado por el logro de los objetivos de una organización.

Tecnología de Información:
Se define como aquellas herramientas y métodos empleados para recabar, retener, manipular o distribuir información. La tecnología de la información se encuentra generalmente asociada con las computadoras y las tecnologías afines aplicadas a la toma de decisiones

Usuarios:
Para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información proporcionados internamente o por terceras partes.

Bibliografía

Acta Sarbanes Oxley del 2002
170 Congreso de los Estados Unidos, 2002
Aporte realizado por Raúl Vásquez Erquicio, Lima Perú (Traducción al Español)
133 pp.

Auditoría en Informática, Segunda Edición
Echenique García, José Antonio
Mc Graw-Hill, 2001
300 pp

Auditoría en Informática: Un enfoque metodológico y práctico
Hernández Hernández, Enrique
CECSA, 1996
315 pp

CoBIT, Objetivos de Control
Comité Directivo de CoBIT & IT Governance Institute
3ª Edición
185 pp

CoBIT, Directrices de Auditoría
Comité Directivo de CoBIT & IT Governance Institute
3ª Edición
229 pp

CoBIT, Guías de Implementación
Comité Directivo de CoBIT & IT Governance Institute
3ª Edición
88 pp

Esquema 1de Norma IRAM-ISO "IEC" 17799
Instituto Argentino de Normalización

IT Control Objetives For Sarbanes Oxley
IT Governance Institute, 2004
86 pp

Mejores Prácticas en la Auditoría Interna
V Reunión de Auditores Internos de Banca Central, 2000
16 pp

Metodología del Trabajo de Auditoría
Banco de la República de Colombia, 1991
85 pp

Normas y procedimientos de auditoría
Instituto Mexicano de Contadores Públicos

¿Qué es la Norma ISO17799? Y razones para que usted la quiera
BSI Management System, 2001
11 pp

Sarbanes Oxley Act 2002
One Hundred Seventh Congress of the United States of America, 2002
66 pp

Conferencias, Cursos y Otros:

Conferencia:
Ley Sarbanes Oxley. Retos y Realidades de la Ley
Organizador: ISACA. Capítulo Cd. México
Agosto, 2005
Importancia del Gobierno Corporativo y Gobierno de TI
Carlos Zamora. ISACA. Cd. México

Lo que necesitan saber los profesionales involucrados sobre la ley
Andrés Lerch. Mancera. Ernest & Young

Enfoque de cumplimiento de la ley. basado en un análisis de riesgos
Rhys DJones. DMR

Adoptando los modelos de control interno de COSO y CoBIT
Juan Antonio Segura. BDO Hernández Marrón y CIA
Jorge Valencia del Toro. BDO Hernández Marrón y CIA.

Cursos:
Curso CoBIT
Organizador: BDO, Hernández Marrón y Cía.
Juan Antonio Segura González, CISA, CISM

Otros:
EL UNIVERSAL
Todo va hacia un estándar de seguridad
NORMA ISO17799,
Enrique Daltabuit Godas, DGSCA, UNAM
Lunes 24 de Mayo de 2004

REVISTA EXPANSIÓN
Riesgo Operativo. una ventaja competitiva.
Pricewaterhouse Coopers
Miércoles 19 de Marzo de 2003