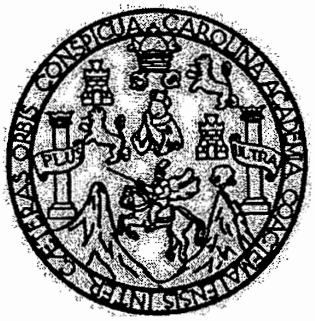
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

FUNDAMENTOS TEÓRICOS Y ANÁLISIS DE LOS ESTÁNDARES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

WILLIAM RODOLFO CADENILLAS CIFUENTES
ASESORADO POR EL ING. JORGE ESTUARDO ESPINOZA RAMÍREZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JULIO DE 2012

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Juan Carlos Molina Jiménez
VOCAL V	Br. Mario Maldonado Muralles
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

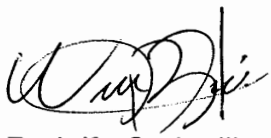
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. Ludwing Federico Altán Sac
EXAMINADOR	Ing. César Augusto Fernández Cáceres
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

FUNDAMENTOS TEÓRICOS Y ANÁLISIS DE LOS ESTÁNDARES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha 1 de julio de 2011.



William Rodolfo Cadenillas Cifuentes

Guatemala, 17 de Abril de 2012

Ingeniero
Carlos Azurdia.
Coordinador de Privados y Revisión de de Trabajos de Graduación
Carrera de Ingeniería en Ciencias y Sistemas
Facultad de Ingeniería
Universidad de San Carlos de Guatemala

Estimado Ingeniero:

Por este medio hago de su conocimiento que he revisado el trabajo de investigación titulado FUNDAMENTOS TEORICOS Y ANALISIS DE LOS ESTANDARES DE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN que el estudiante WILLIAM RODOLFO CADENILLAS CIFUENTES, quien se identifica con el número de carné 1998-19257, esta desarrollando y que hasta la fecha 17 de Abril de 2012 ha completado el trabajo de graduación que corresponden con el protocolo para el desarrollo de esta investigación. Manifiesto por este medio mi aprobación por el esfuerzo, dedicación y resultados obtenidos por el estudiante hasta este punto de desarrollo del trabajo de investigación.

Sin más por el momento y agradeciendo la oportunidad de colaboración a la educación e investigación universitaria que me da, me despido.

Atentamente:

Jorge Estuardo Espinoza Ramírez
INGENIERO EN CIENCIAS Y SISTEMAS
COLEGIADO No. 11192

Jorge Estuardo Espinoza Ramírez
Ingeniero en Ciencias y Sistemas

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 2 de Mayo de 2012

Ingeniero
Marlon Antonio Pérez Turk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **WILLIAM RODOLFO CADENILLAS CIFUENTES** carné **1998-19257**, titulado: **"FUNDAMENTOS TEÓRICOS Y ANÁLISIS DE LOS ESTÁNDARES DE LA AUDITORIA DE SISTEMAS DE INFORMACIÓN"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación titulado ***"FUNDAMENTOS TEÓRICOS Y ANÁLISIS DE LOS ESTÁNDARES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN"*** *presentado por el estudiante WILLIAM RODOLFO CADENILLAS CIFUENTES, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

Ing. Marlon Antonio Pérez Turk
Director, Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 09 de julio 2012

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.318.2012

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **FUNDAMENTOS TEÓRICOS Y ANÁLISIS DE LOS ESTÁNDARES DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN**, presentado por el estudiante universitario: **William Rodolfo Cadenillas Cifuentes,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, julio de 2012

/cc

ACTO QUE DEDICO A:

Dios Jesucristo	Por darme la salvación eterna, darle gloria cada día y ser mi fortaleza en cada momento.
Guatemala	Por ser mí amada patria.
La Universidad de San Carlos de Guatemala	Por ser mi casa de estudio y desarrollo académico.
A toda mi familia y en especial a	Mi amada esposa Shirley Marroquín, mi amado hijo William Alejandro, por el amor, apoyo y confianza para seguir adelante. Mis padres Carlos Rodolfo Cadenillas Salas y Miria Yolanda Cifuentes de León de Cadenillas, por el sacrificio, el ejemplo, la motivación y el apoyo incondicional en todo momento. Mis hermanos Jessica y Giovanni, por el amor fraternal y valioso apoyo en todos estos años. Mis abuelos Marta, Oswaldo, Carlos y María. Mis suegros Juan Carlos Marroquín Salazar y Enma Verónica Vásquez Ortega de Marroquín. Mis sobrinos Melany, Bella, Carlos, Sara, Gian Carlo y Marian. Mis cuñados Rafael López, Rafael López Chen, Linda, Juan Carlos, Christian, Jhonatan, Josué, tíos y primos.

Mis amigos

Por todos los esfuerzos llevados a cabo y a sus familias por abrirnos las puertas de sus hogares y su hospitalidad, por ser ejemplo y apoyo para culminar la carrera y el apoyo incondicional.

AGRADECIMIENTOS A:

Dios Jesucristo	Por permitir que se haga su voluntad en mi vida y culminar esta meta.
Mi amada esposa Shirley Marroquín	Por apoyarme, amarme y animarme para alcanzar esta de muchas metas.
Mi amado hijo William Alejandro	Por ser una fuente de amor en su tierna edad y por enseñarme a ver con nuevos ojos la vida misma.
Mis padres	Carlos Rodolfo Cadenillas Salas y Miria Yolanda Cifuentes de León de Cadenillas. Lo que soy, lo que he logrado y lo que seguiré cosechando es fruto de su amor, esfuerzo, sacrificio y oraciones.
Mis hermanos	Son mi fuente de inspiración, ejemplo y apoyo incondicional.
Mis abuelos	Esta meta alcanzada es parte de su legado.
Mis suegros	Juan Carlos Marroquín Salazar y Enma Verónica Vásquez Ortega de Marroquín por su ejemplo y apoyo.

Mis cuñados	Muchas gracias por apoyarme.
Mis sobrinos	Por inspirar alegría y gozo en todo momento.
Mis tíos y primos	Porque en algún momento de esta larga carrera me apoyaron y dieron palabras de aliento para seguir.
Mis amigos	Por el apoyo incondicional y ser parte de muchos momentos de mi vida.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

AICPA	Siglas de Instituto Americano de Contadores Públicos Certificados, institución involucrada en el desarrollo de SYSTRUST.
Back-up	Copia de seguridad. Acción de copiar documentos, archivos o ficheros de tal forma que puedan recuperarse en caso de fallo en el sistema.
Base de datos	Es un conjunto de información estructurada en registros y almacenada en un soporte electrónico legible desde un ordenador.
Batch	Lote de órdenes de procesamiento de información que se ejecutarán una tras otra.
Check-list	Lista de acciones que se deben tomar en respuesta a un evento en particular.
CICA	Son las siglas *de* Canadian Institute of Chartered Accountants, institución involucrada en desarrollar SYSTRUST.

COBIT	Siglas en inglés de Objetivos de Control para la Información y Tecnologías Relacionadas, que es un estándar de auditoría de sistemas de información.
Control interno (CI)	Proceso a través del cual se desarrolla un conjunto de actividades de verificación, comparación y validación de cifras, procedimientos, políticas, programas y resultados con el fin de garantizar que la entidad pueda alcanzar las metas y objetivos previstos.
COSO	Siglas en inglés del comité de organizaciones patrocinadoras de la comisión de seguimiento para evaluar los controles internos.
CPU	Siglas en inglés de Unidad Central de Proceso, que es la unidad donde se ejecutan las instrucciones de los programas y se controla el funcionamiento de los distintos componentes del ordenador.
CRMR	Siglas en inglés de la metodología de evaluación de la gestión de recursos informáticos.
Efectividad	Concepto que involucra la eficiencia y la eficacia, consistente en alcanzar los resultados programados a través de un uso óptimo de los recursos involucrados.

Eficiencia	Se refiere al uso óptimo de recursos en programas, subprogramas y proyectos.
Encriptación	Proceso de codificar la información de manera que sólo sea accesible a quien posea un código de descodificación.
Firma digital	Código digital que se puede adjuntar a un mensaje transmitido por medios electrónicos y que identifica de manera exclusiva al remitente.
Hardware	Componentes físicos de un ordenador o de una red, en contraposición con los programas o elementos lógicos que los hacen funcionar.
Informática	Es la ciencia de la información automatizada, todo aquello que tiene relación con el procesamiento de datos, utilizando la computadora o los equipos de proceso automatizado de información.
ISACF	Siglas en inglés de Fundación de Auditoría y Control de Sistemas de Información, institución involucrada en desarrollar COBIT.
MARGERIT	Son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Modularidad	Es la propiedad de un sistema que ha sido descompuesto en un conjunto de módulos coherentes e independientes.
On-line	En línea. Condición de estar conectado a una red.
Ordenador	Dispositivo electrónico compuesto básicamente de un procesador, una memoria y los dispositivos de entrada/salida (E/S).
Password	Clave de acceso o contraseña necesario para acceder a un determinado recurso.
Plan de contingencia	Un proyecto de acciones neutralizadoras para enfrentarse a cierto tipo de posible peligro o para resistir cierta clase de ataque previsto.
SAC	Siglas de Auditoría y Control de Sistemas, es un estándar para los auditores internos en el área de auditoría de sistemas de información y tecnología.
Seguridad física	Mecanismos de control que evitan el uso no autorizado de recursos *hardware*.
Seguridad lógica	Mecanismos de control que evitan el uso no autorizado de recursos *software*.

Sistema Operativo	Conjunto de *software* que controla los distintos recursos del ordenador.
Sistemas de información	Es el conjunto de funciones y procedimientos encaminados a la captación, desarrollo, recuperación, almacenamiento, etcétera, de información en el seno de una organización.
Software	Es la parte lógica del ordenador, esto es, el conjunto de programas que puede ejecutar el *hardware* para la realización de las tareas de computación a las que se destina.
SYSTRUST	Es un estándar desarrollado por AICPA y CICA para asesorar en temas de auditoría informática.
TI	Siglas de Tecnología de Información. Nombre del conjunto para todo el *hardware* y el *software* del campo de los ordenadores y las comunicaciones.
Tiempo real	Rápida transmisión y proceso de datos orientados a eventos y transacciones a medida que se producen, en contraposición a almacenarse y retransmitirse o procesarse por lotes.
Trazabilidad	Característica que permite rastrear la fuente de información de forma eficiente.

Tunning	Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto.

RESUMEN

La auditoría de sistemas de información se basa en la revisión y evaluación de los controles, sistemas, procedimientos de informática, su utilización, eficiencia y seguridad, de una manera ordenada, estructural, sistemática y objetiva, como parte integral del logro de los objetivos en una organización.

En este trabajo se describe una clasificación general de los controles necesarios para la evaluación de las tecnologías de información, los controles físicos y lógicos, controles automáticos y administrativos. Además, contiene la descripción de las metodologías utilizadas para el desarrollo de una auditoría informática, abordando todas las etapas y recursos necesarios para llevar a cabo una revisión y evaluación de todos los procesos y componentes de TI.

El trabajo contiene los estándares de auditoría de sistemas de información utilizados en la industria como fuente para definir, valorizar, reportar y mejorar el control interno y ser utilizados como marco de referencia dentro de una organización.

Se muestra un análisis entre los estándares más utilizados en la industria, y las diferencias entre las audiencias, los objetivos organizacionales, los componentes y otros elementos que conforman dichos estándares, sobre la infraestructura sobre la cual fueron desarrollados para el diseño y evaluación de los sistemas de control interno.

OBJETIVOS

General

Estudiar y analizar los fundamentos y estándares de la auditoría de sistemas de información, las diferencias entre los tipos de estándares y la manera en que una organización comercial puede adoptar una auditoría de su sistema de información.

Específicos

1. Describir los fundamentos de la auditoría de sistemas de información.

2. Estudiar los diferentes controles y metodologías para la recopilación y evaluación de los sistemas de información.

3. Estudiar los diferentes tipos de estándares sobre la protección de la información.

4. Evaluar y analizar estándares para el desarrollo de una auditoría de sistemas de información.

5. Estudiar las buenas prácticas de auditoría de sistemas aplicadas en Guatemala.

INTRODUCCIÓN

El presente trabajo fue elaborado sobre los fundamentos y estándares de la auditoría de sistemas de información, la cual se basa en la revisión y evaluación de los controles, sistemas, procedimientos de informática, su utilización, eficiencia y seguridad, de una manera ordenada, estructural, sistemática y objetiva, como parte integral del logro de los objetivos en una organización.

El tema se desarrolla en cuatro capítulos, el primer capítulo incluye la descripción de los fundamentos de la auditoría informática, sus características, y la clasificación sobre cuatro áreas generales de auditorías de TI, auditoría informática de usuario, de actividades internas, de dirección y de seguridad; y describe las divisiones sobre las cuatro áreas generales, auditoría informática de explotación, de sistemas, de telecomunicaciones y de desarrollo de proyectos.

El segundo capítulo trata de los controles y metodologías de la auditoría informática, describiendo una clasificación general de los controles para evaluar las tecnologías de información. Entre otros controles se mencionan los físicos y lógicos, controles automáticos y administrativos. Se destacan las metodologías utilizadas para la auditoría de sistemas y se describe una metodología común para llevar a cabo una auditoría junto con todos los componentes necesarios para evaluar la TI de una organización.

El capítulo tres aborda los estándares de auditoría de sistemas utilizados en la industria, describiendo sus componentes y la manera en que están estructurados y bajo que infraestructura fueron desarrollados. Entre algunos estándares que se explican están: COBIT, COSO y SAC.

El cuarto capítulo es un análisis de los estándares COBIT, COSO y SAC, mostrando un cuadro comparativo de los atributos de dichos estándares y explica las diferencias y similitudes entre cada uno de sus atributos, componentes, la manera en que reportan los problemas de control interno y sus herramientas, entre otros.

El último capítulo es un estudio de las buenas prácticas de auditoría de sistemas que se están aplicando en Guatemala, el cual muestra la importancia del valor agregado al implementar las mejores prácticas en el tema y como el sector financiero guatemalteco ha sido uno de los pioneros en el establecimiento de normas acerca del control interno y administración del riesgo tecnológico.

1. FUNDAMENTOS DE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

1.1. Conceptos de auditoría de sistemas de información

La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones, con actividades dirigidas a verificar y juzgar información, representan algunos de los conceptos generales de una auditoría informática.

De forma general, el examen y evaluación de los procesos del área de procesamiento automático de datos y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas, son parte de los elementos de una auditoría de sistemas, junto con el proceso de recolección y evaluación de evidencia para determinar si un sistema automatizado es eficiente, confiable y salvaguarda la información de la empresa.

1.1.1. Auditoría financiera y operativa

La auditoría financiera efectúa un examen sistemático de los estados financieros, los registros y las operaciones contables, para determinar la disciplina de los principios de contabilidad generalmente aceptados, de las políticas de la administración y de la planificación.

La auditoría operativa es una evaluación sistemática de las actividades de una organización en relación con sus objetivos específicos, con el fin de evaluar el comportamiento, señalar oportunidades de mejora y generar recomendaciones para un mejor logro de los objetivos.

1.1.2. Auditoría informática

Se encarga de la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una organización para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información. La auditoría de sistemas es una rama especializada de la auditoría que promueve y aplica conceptos de auditoría en el área de sistemas de información.

También tiene a cargo la verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad, encaminando todas las actividades a verificar y juzgar la información. Además, conlleva la realización de exámenes y evaluación de los procesos en el área de procesamiento de información y la forma en que los recursos son utilizados y aplicados, para obtener el grado de eficiencia y efectividad de los sistemas de información.

Dentro del proceso de la auditoría de sistemas se encuentra la recolección y evaluación de toda la evidencia para determinar si un sistema:

- Realiza *back-ups* de activos, contra daños, destrucción, uso no autorizado o robo.

- Mantiene la integridad de los datos, para obtener la información precisa, completa, oportuna y confiable.

- Alcanza las metas de la organización, como contribución de la función de la tecnología de información.

- Consume recursos eficientemente, utiliza los recursos adecuadamente en el procesamiento de la información.

El examen o revisión que se realiza es de carácter objetivo, con crítica, sistémico y selectivo de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con el sistema de información, con el objetivo de obtener un resultado imparcial sobre la eficiencia de los recursos informáticos, validez de la información y efectividad de los controles establecidos.

1.1.3. Auditoría interna y auditoría externa

La auditoría interna es la que se realiza con recursos que pertenecen a la organización que se está auditando. Este tipo de auditoría puede ser disuelta en cualquier momento por decisión de los altos directivos de la organización. Por otro lado, la auditoría externa es realizada por personas ajenas a la organización auditada. Se presupone una mayor objetividad que en la auditoría interna, debido al mayor distanciamiento entre auditores y auditados.

La auditoría informática interna cuenta con algunas ventajas adicionales muy importantes respecto de la auditoría externa, las cuales no son tan visibles como en las auditorías convencionales.

La auditoría interna tiene la ventaja de que puede actuar periódicamente realizando revisiones globales, como parte de su plan anual y de su actividad normal. Los auditados conocen estos planes y se adecuan a las auditorías, especialmente cuando las consecuencias de las recomendaciones benefician su trabajo.

Una de las desventajas de la auditoría informática interna se encuentra en la disposición del departamento de informática de una organización, el cual es el encargado de la orientación e información sobre los detalles técnicos y costos sobre el sistema al realizar la auditoría, teniendo la organización la obligación de controlar sus sistemas sobre los procedimientos y estándares de la organización.

1.1.4. Alcance de la auditoría informática

El alcance define con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, se complementa con los objetivos de esta. El alcance se expresa claramente dentro de un informe final, de modo que quede perfectamente determinado no solamente hasta qué puntos se ha llegado, sino qué áreas han sido omitidas. Por ejemplo, se pueden o no someter a una auditoría los registros sobre un exhaustivo control de integridad. Se puede o no auditar los controles de validación de errores, etcétera.

1.1.5. Características de la auditoría informática

Existen tres características de la auditoría informática que engloba todas las actividades de una auditoría parcial: auditoría de inversión informática, auditoría de seguridad informática y auditoría de organización informática.

La auditoría de inversión informática se encarga de realizar un chequeo sobre las actividades de inversión que se realizan en el departamento de informática de una organización, de modo que se puedan detectar anomalías o cualquier otro tipo de situación anormal sobre las inversiones que una organización hace para la mejora y desarrollo de su departamento de informática.

La auditoría de seguridad informática se encarga de proteger de manera global o particular los sistemas automatizados en cualquiera de sus áreas, ya sea de desarrollo o el área técnica del sistema.

Y por último la auditoría de organización informática se encarga de tener un control sobre los cambios estructurales o funcionales que se producen en el departamento de informática de una organización.

1.1.6. Síntomas de necesidad de una auditoría informática

Las necesidades de una auditoría de sistemas es parte del control de la función informática, como el análisis de la eficiencia de los Sistemas Informáticos, para verificar el cumplimiento de las normas y políticas en este ámbito y mejorar ciertas características como la eficiencia, eficacia, rentabilidad y seguridad.

1.1.6.1. Desorganización

Esto ocurre cuando los objetivos del departamento de informática de una organización y los objetivos de la propia organización no coinciden. Los estándares de productividad se desvían de los promedios conseguidos regularmente.

1.1.6.2. Mala imagen e insatisfacción de los usuarios

Se produce cuando no se atienden las peticiones de cambios de los usuarios. Por ejemplo, los cambios de *software* en los terminales de usuario, variación de los archivos que deben ponerse diariamente a su disposición, etcétera. Otro ejemplo es el caso de que no se reparan los daños de *hardware* ni se resuelven incidencias en plazos razonables.

El usuario percibe que está abandonado y desatendido permanentemente. Además, no se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.

1.1.6.3. Debilidades económico-financieras

Se produce un incremento desmesurado de costes o bien la organización no está absolutamente convencida de la justificación de una inversión informática. Por ejemplo, suelen darse desviaciones presupuestarias significativas sobre los costes y plazos de nuevos proyectos.

1.1.6.4. Inseguridad

Existe una evaluación de nivel de riesgos el área de seguridad lógica, física y confidencial, pues los datos son propiedad inicialmente de la organización que genera esa información y por ende son confidenciales.

La continuidad del servicio, es un concepto aún más importante que la seguridad. Establece las estrategias de continuidad entre fallos mediante planes de contingencia totales y locales.

1.1.6.5. Planes de contingencia

Estos planes son especificaciones de que acciones tomar dada una situación o situaciones en particular. Por ejemplo, se sufre un corte total de energía, ¿Cómo se sigue operando la información en otro lugar? Lo que generalmente se pide es que se hagan *back-ups* de la información diariamente y que aparte, sea doble. Entonces los planes de contingencia mantienen un nivel de riesgo mínimo con el fin de poder seguir procesando la información y evitar daños o pérdidas de la misma.

1.1.6.6. Otros síntomas de necesidad de auditoría

- La información es un recurso clave para planear el futuro, controlar el presente y evaluar el pasado.
- Las operaciones dependen cada vez más de la sistematización.
- Los riesgos tienden a aumentar, debido a la pérdida de información, pérdida de activos, pérdida de servicios o ventas.
- La sistematización representa un costo significativo en cuanto a *hardware*, *software* y personal.
- Los problemas se identifican sólo al final.

1.2. Tipos y clases de auditorías

Existen cuatro áreas generales de la auditoría informática, la auditoría informática de usuario, la auditoría informática de actividades internas, la auditoría informática de dirección y la auditoría de seguridad. La auditoría orientada en el usuario, destaca las actividades proyectadas al usuario, en contraparte con la auditoría orientada a las actividades internas que se enfoca en la informática cotidiana y real.

La auditoría de dirección tiene el objetivo de revisar las interrelaciones entre la dirección y los usuarios y la capacidad de interpretar las necesidades o requerimientos. Por último la auditoría de seguridad tiene a cargo la revisión lógica, física y confidencialidad de la información que se procesa.

Dentro de las áreas generales, se establecen las siguientes divisiones de la auditoría informática: de explotación, de sistemas, de comunicaciones y de desarrollo de proyectos. Estas son las áreas específicas de la auditoría informática más importantes. Cada área específica puede ser auditada desde los siguientes criterios generales:

- Desde su propio funcionamiento interno
- Desde el apoyo que recibe de la dirección
- Desde la perspectiva de los usuarios
- Desde el punto de vista de la seguridad que ofrece la informática en general o la rama auditada.

1.2.1. Auditoría informática de explotación

Consiste en auditar las secciones que la componen y sus interrelaciones. Se ocupa de producir resultados informáticos de todo tipo: listados impresos, archivos soportados magnéticamente para otros usos informáticos, órdenes automatizadas para lanzar o modificar procesos industriales, etcétera. La explotación informática se puede considerar como una fábrica con ciertas características que la distinguen de las reales.

Para realizar la explotación informática se dispone de una materia prima, los datos, que son necesarios transformar y que se someten previamente a controles de integridad y calidad.

La transformación se realiza por medio del proceso informático, el cual está gobernado por programas. Obtenido el producto final, los resultados son sometidos a varios controles de calidad y, finalmente, son distribuidos al cliente y al usuario. La explotación informática se divide en tres grandes áreas: planificación, producción y soporte técnico, en la que cada cual tiene varios grupos.

1.2.1.1. Control de entrada de datos

Se analiza la captura de la información, el cumplimiento de plazos y calendarios de tratamientos y entrega de datos; la correcta transmisión de datos entre entornos diferentes. Se verifica que los controles de integridad y calidad de datos se realizan de acuerdo con las normas establecidas.

1.2.1.2. Planificación y recepción de aplicaciones

Se auditan las normas de entrega de aplicaciones por parte de desarrollo, verificando su cumplimiento y su calidad de participante. Se realizan muestreos selectivos de la documentación de las aplicaciones explotadas. Se examina la anticipación de contactos con desarrollo para la planificación a medio y largo plazo.

1.2.1.3. Centro de control y seguimiento de trabajos

Se analiza cómo se prepara, se lanza y se sigue la producción diaria. Básicamente, la explotación informática ejecuta procesos por cadenas o lotes sucesivos o en tiempo real. Mientras que las aplicaciones de telecomunicaciones están permanentemente activas y la función de explotación se limita a vigilar y recuperar incidencias, el trabajo en lotes absorbe una buena parte de los efectivos de explotación.

1.2.1.3.1. *Batch* y tiempo real

Las aplicaciones que son *batch* son aplicaciones que cargan mucha información durante el día y durante la noche se corre un proceso enorme que lo que hace es relacionar toda la información, realizar cálculos y obtener como salida, por ejemplo, reportes. O sea, recolecta información durante el día, pero todavía no procesa nada.

Las aplicaciones que son tiempo real u *on-line*, son las que, luego de haber ingresado la información correspondiente, inmediatamente procesan y devuelven un resultado. Son sistemas que tienen que responder en tiempo real.

1.2.1.4. Operación en la sala de ordenadores

Se analizan las relaciones personales y la coherencia de cargos y salarios, así como la equidad en la asignación de turnos de trabajo. Se verifica la existencia de un responsable de sala en cada turno de trabajo. Se analiza el grado de automatización de comandos, se verificará la existencia y grado de uso de los manuales de operación.

Se analiza no sólo la existencia de planes de capacitación, sino el cumplimiento de los mismos y el tiempo transcurrido para cada operador desde el último curso recibido. Se estudian los montajes diarios y por horas de cintas o cartuchos, así como los tiempos transcurridos entre la petición de montaje por parte del sistema hasta el montaje real. Se verifican las líneas de papel impresas diarias y por horas, así como la manipulación de papel que comportan.

1.2.1.5. Centro de control de red y centro de diagnosis

Sus funciones se refieren exclusivamente al ámbito de las comunicaciones, estando muy relacionado con la organización de *software* de comunicaciones de técnicas de sistemas. Se analiza la fluidez de esa relación y el grado de coordinación entre ambos. Se verifica la existencia de un punto concéntrico único, desde el cual sean perceptibles todas las líneas asociadas al sistema.

El centro de diagnosis es el ente en donde se atienden las llamadas de los usuarios-clientes que han sufrido averías o incidencias, tanto de *software* como de *hardware*. El centro de diagnosis está especialmente indicado para informáticos grandes y con usuarios dispersos en un amplio territorio.

El centro de diagnosis es auditado desde la perspectiva de la sensibilidad del usuario sobre el servicio que se le dispone. No basta con comprobar la eficiencia técnica del centro, es necesario analizarlo simultáneamente en el ámbito de usuario.

1.2.2. Auditoría informática de desarrollo de proyectos o aplicaciones

La función de desarrollo es una evolución del llamado análisis y programación de sistemas y aplicaciones. A su vez, engloba muchas áreas. Muy directamente, una aplicación recorre las siguientes fases:

- Prerrequisitos del usuario y del entorno
- Análisis
- Diseño
- Desarrollo
- Pruebas
- Implantación

Estas fases se someten a un exigente control interno. Finalmente, la auditoría tiene a cargo el deber de comprobar la seguridad de los programas en el sentido de garantizar que los ejecutados por la máquina sean exactamente los previstos y no otros.

Una auditoría de aplicaciones pasa por la observación y el análisis de cuatro consideraciones:

- Revisión de las metodologías utilizadas: se analizan de modo que se asegure la modularidad de las posibles futuras ampliaciones de la aplicación y el fácil mantenimiento de las mismas.

- Control interno de las aplicaciones: se revisan las mismas fases que presuntamente han debido seguir el área correspondiente de desarrollo.

- Estudio de viabilidad de la aplicación: es muy importante para aplicaciones largas, complejas y caras.

- Definición lógica de la aplicación: se analiza que se han observado los principios lógicos del proceso, en función de la metodología elegida y la finalidad que persigue el proyecto.

- Desarrollo técnico de la aplicación: se verifica que es ordenado y correcto. Las herramientas técnicas utilizadas en los diversos programas deben ser compatibles.

- Diseño de programas: deben poseer la máxima sencillez, modularidad y economía de recursos.

- Métodos de pruebas: se realizan de acuerdo con las normas de la instalación. Se utilizan juegos de ensayo de datos, sin que sea válido el uso de datos reales.

- Documentación: debe cumplir la normativa establecida en la instalación, tanto la de desarrollo como la de entrega de aplicaciones a explotación.

- Equipo de programación: deben fijarse las tareas de análisis puro, de programación y las intermedias. En aplicaciones complejas se producirían variaciones en la composición del grupo.

- Satisfacción de usuarios: una aplicación técnicamente eficiente y bien desarrollada, debe considerarse fracasada si no sirve a los intereses del usuario que la solicitó. La aprobación del usuario proporciona grandes ventajas posteriores, ya que evita reprogramaciones y disminuirá el mantenimiento de la aplicación.

- Control de procesos y ejecuciones de programas críticos: el auditor no debe descartar la posibilidad de que se esté ejecutando un módulo que no corresponde con el programa fuente que desarrolló, codificó y probó el área de desarrollo de aplicaciones.

Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Los programas fuente que hayan sido dados por buen desarrollo, son entregados a explotación.

1.2.3. Auditoría informática de sistemas

Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Las comunicaciones, líneas y redes de las instalaciones informáticas, se auditan por separado, aunque formen parte del entorno general de sistemas.

1.2.3.1. Sistemas Operativos

Engloba los subsistemas de telecomunicaciones, entrada/salida, etcétera. Se verifica en primer lugar que los sistemas están actualizados con las últimas versiones del fabricante, indagando las causas de las omisiones si las hubiera.

El análisis de las versiones de los Sistemas Operativos permite descubrir las posibles incompatibilidades entre otros productos de *software* básico adquiridos por la instalación y determinadas versiones.

1.2.3.2. *Software* básico

Es fundamental para el auditor conocer los productos de *software* básico que han sido facturados aparte de la propia computadora. Esto, por razones económicas y por razones de comprobación de que la computadora podría funcionar sin el producto adquirido por el cliente.

En cuanto al *software* desarrollado por el personal informático, el auditor debe verificar que este no dañe ni condicione al sistema. Igualmente, debe considerar el esfuerzo realizado en términos de costes, por si hubiera alternativas más económicas.

1.2.3.3. *Tunning*

Es el conjunto de técnicas de observación y de medidas encaminadas a la evaluación del comportamiento de los subsistemas y del sistema en su conjunto.

Las acciones de *tunning* se diferencian de los controles habituales que realiza el personal de técnica de sistemas. El *tunning* posee una naturaleza más revisora, estableciéndose previamente planes y programas de actuación según los síntomas observados. Se pueden realizar:

- Cuando existe sospecha de deterioro del comportamiento parcial o general del sistema.

- De modo sistemático y periódico. En este caso sus acciones son repetitivas y están planificados y organizados de antemano.

El auditor debe conocer el número de *tunning* realizados en el último año, así como sus resultados. Debe analizar los modelos de carga utilizados y los niveles e índices de confianza de las observaciones.

1.2.3.4. Optimización de los sistemas y subsistemas

Técnica de sistemas debe realizar acciones permanentes de optimización como consecuencia de la realización de *tunnings* preprogramados o específicos.

El auditor verifica que las acciones de optimización son efectivas y no comprometen la operatividad de los sistemas ni el plan crítico de producción diaria de explotación. Se realiza un análisis del desempeño del sistema o subsistemas para luego optimizarla y mejorar el rendimiento del sistema.

1.2.3.5. Administración de bases de datos

El auditor de base de datos debe asegurarse que explotación conoce suficientemente las bases de datos que son accedidas por los procedimientos que ella ejecuta. Debe analizar los sistemas de *back-ups* existentes, que competen igualmente a explotación. Debe revisar finalmente la integridad y consistencia de los datos, así como la ausencia de redundancias entre ellos.

1.2.4. Auditoría informática de comunicaciones y redes

Para el informático y para el auditor informático, el esqueleto conceptual que constituyen las redes de nodos, líneas, concentradores, multiplexores, redes locales, etcétera, no son sino el soporte físico y lógico del tiempo real.

El auditor analiza las situaciones y hechos alejados entre sí y está condicionado a la participación de la empresa de telefonía que presta el soporte. La auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en comunicaciones y en redes locales.

El auditor de comunicaciones debe inquirir sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Debe proveerse de la topología de la red de comunicaciones, actualizada, la inexistencia de datos sobre cuántas líneas existen, cómo son y dónde están instaladas, supondría que se bordea la inoperatividad informática.

1.2.5. Auditoría de la seguridad informática

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del *hardware* y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etcétera.

La seguridad lógica se refiere a la seguridad de uso del *software*, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

Un método eficaz para proteger sistemas de computación es el *software* de control de acceso. Estos paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial.

La seguridad informática se puede dividir como área general y como área específica (seguridad de explotación, seguridad de las aplicaciones, etcétera). Así, se puede efectuar auditorías de la seguridad global de una instalación informática y auditorías de la seguridad de un área informática determinada. El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades

- Seguridad física y contra catástrofes (incendio, terremotos, etcétera)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba

La auditoría informática de seguridad global, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que está sometida. Se crean matrices de riesgo, en donde se consideran los factores de las amenazas a las que está sometida una instalación y su impacto. Las matrices de riesgo se representan en cuadros de doble entrada amenaza-impacto, en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

1.3. Objetivos de la auditoría informática

El objetivo principal de la auditoría de sistemas es identificar si las tecnologías de información son utilizadas para salvaguardar la información de la empresa, además, comprueba si mantiene la integridad de los datos, alcanza las metas organizaciones y consume recursos eficientemente.

1.3.1. La operatividad

La operatividad es una función consistente en que la organización y las máquinas funcionen. No es aceptable detener la maquinaria informática para descubrir sus fallos y comenzar de nuevo. La auditoría debe iniciar su actividad cuando los sistemas están operando. Tal objetivo debe conseguirse tanto a nivel global como parcial.

La operatividad de los sistemas es la principal preocupación del auditor informático. Para conseguirla hay que acudir a la realización de controles técnicos generales de operatividad y controles técnicos específicos de operatividad, previos a cualquier actividad del auditor.

1.3.1.1. Controles técnicos generales

Son los que se realizan para verificar la compatibilidad de funcionamiento simultáneo del Sistema Operativo y el *software* base con todos los subsistemas existentes, así como la compatibilidad del *hardware* y del *software* instalado.

Estos controles verifican las instalaciones que cuentan con *hardware* variado, debido a que el exceso de entornos de trabajo muy diferentes obliga a la contratación de diversos productos de *software* básico, con el riesgo de abonar más de una vez el mismo producto o desaprovechar parte del *software* garantizado. Además, estos controles analizan los productos de *software* base desarrollados por el personal de sistemas, sobre todo cuando los diversos equipos están ubicados geográficamente distantes.

1.3.1.2. Controles técnicos específicos

Estos controles son necesarios para lograr la operatividad de los sistemas. Un ejemplo de lo que verifica estos controles es el chequeo de los parámetros de asignación automática de espacio en disco que dificulten o impidan su utilización posterior.

También verifican los períodos de retención de archivos comunes a varias aplicaciones, donde la pérdida de información ocurre con facilidad, quedando sin operación la explotación de alguna de las aplicaciones.

1.3.2. Revisión de controles de gestión informática

Una vez conseguida la operatividad de los sistemas, el segundo objetivo de la auditoría es la verificación del cumplimiento de las normas teóricamente existentes en el departamento de informática y su coherencia con las del resto de la organización. Para esto se debe revisar sucesivamente y en el orden siguiente:

- Las normas generales de la instalación informática. Se realiza una revisión inicial sin estudiar a fondo las contradicciones que pueden existir, pero se registran las áreas que no tengan normas establecidas y sobre todo se verifica que la normativa general informática no está en contradicción con alguna norma general de otra área de la organización.

- Los procedimientos generales informáticos. Se verifica que existan los procedimientos, al menos en los sectores más importantes. Por ejemplo, la recepción definitiva de las máquinas debería estar firmada por los responsables de explotación. Tampoco el alta de una nueva aplicación podría producirse si no existieran los procedimientos de *back-up* y recuperación correspondientes.

- Los procedimientos específicos informáticos. Se revisa si existe en las áreas fundamentales. Así, explotación no debería explotar una aplicación sin haber exigido a desarrollo la respectiva documentación. Del mismo modo, debe comprobarse que los procedimientos específicos no se opongan a los procedimientos generales. A su vez, se verifica que no existe contradicción con la norma y los procedimientos generales de la propia organización.

1.3.3. Objetivos generales de la auditoría informática

- 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

1.3.4. Objetivos específicos de la auditoría informática

- Participación en el desarrollo de nuevos sistemas
- Evaluación de controles
- Cumplimiento de la metodología
- Evaluación de la seguridad en el área informática
- Evaluación de suficiencia en los planes de contingencia
- Respaldos, prever qué va a pasar si se presentan fallas
- Opinión de la utilización de los recursos informáticos

- Resguardo y protección de activos
- Control de modificación a las aplicaciones existentes
- Fraudes
- Control a las modificaciones de los programas
- Participación en la negociación de contratos con los proveedores
- Revisión de la utilización del Sistema Operativo y los programas
- Programas utilitarios
- Control sobre la utilización de los Sistemas Operativos
- Auditoría de la base de datos
- Estructura sobre la cual se desarrollan las aplicaciones
- Auditoría de la red de telecomunicaciones
- Desarrollo de *software* de auditoría

El desarrollo de un *software* capaz de estar ejerciendo un control continuo sobre las operaciones de área de procesamiento automático de datos, es el objetivo final de una auditoría de sistemas de información.

1.4. Similitudes y diferencias con la auditoría tradicional

Entre las similitudes y diferencias con la auditoría tradicional se encuentra las siguientes para llevar a cabo una auditoría informática:

- No se requieren nuevas normas de auditoría, son las mismas

- Los elementos básicos de un buen sistema de control contable interno siguen siendo los mismos; por ejemplo, la adecuada segregación de funciones.

- Los propósitos principales del estudio y la evaluación del control contable interno son la obtención de evidencia para respaldar una opinión y determinar la base, oportunidad y extensión de las pruebas futuras de auditoría.

- Se establecen algunos nuevos procedimientos de auditoría

- Hay diferencias en las técnicas destinadas a mantener un adecuado control interno contable.

- Hay alguna diferencia en la manera de estudiar y evaluar el control interno contable. Una diferencia significativa es que en algunos procesos se usan programas.

- El énfasis en la evaluación de los sistemas manuales está en la evaluación de transacciones, mientras que el énfasis en los sistemas informáticos, está en la evaluación del control interno.

1.5. Aspectos del entorno informático que afecta el enfoque de la auditoría de sistemas

- Complejidad de los sistemas
- Uso de lenguajes
- Metodologías, como parte de las personas y su experiencia
- Centralización
- Departamento de sistemas que coordina y centraliza todas las operaciones.
- Relaciones de los usuarios altamente dependientes del área de sistemas
- Controles del computador
- Confiabilidad electrónica
- Debilidades de las máquinas y tecnología
- Transmisión y registro de la información en medios magnéticos, óptico y otros.
- Almacenamiento en medios que deben acceder a través del computador mismo.
- Centros externos de procesamiento de datos

1.6. Herramientas y técnicas para la auditoría informática

Para llevar a cabo una auditoría de sistemas para evaluar la eficiencia de los recursos informáticos y salvaguardar la información se encuentran las siguientes herramientas: cuestionarios, entrevistas, *check-list*, trazas y *software* de interrogación.

1.6.1. Cuestionarios

El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de una opinión global objetiva, siempre fundamentada en hechos demostrables, llamados también evidencias, producto de la recolección de información y documentación de todo tipo y emisión de informes finales donde se analizan las situaciones de debilidad o fortaleza en los diferentes entornos.

Para la realización de esto se solicita el cumplimiento de cuestionarios preimpresos que se envían a las personas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar.

Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación y muy cuidados en su fondo y su forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que el análisis determine a su vez la información que debe elaborar el propio auditor. El cruzamiento de ambos tipos de información es una de las bases fundamentales de la auditoría.

1.6.2. Entrevistas

El auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:

- Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

- Mediante entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

- Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

Por medio de la entrevista se recoge más información y mejor ajustada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. La entrevista entre auditor y auditado se basa fundamentalmente en el concepto de interrogatorio; es lo que hace un auditor, interroga y se interroga a sí mismo.

El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, con el fin de que la conversación sea correcta y lo menos tensa posible, el auditado conteste sencillamente y con esmero a una serie de preguntas variadas y también sencillas.

1.6.3. *Check-list*

El conjunto de preguntas elaboradas en función de los escenarios auditados recibe el nombre de *check-list*. Son útiles para extraer la información que se necesita y de forma coherente, permitiendo una correcta descripción de los puntos débiles y fuertes del área que se audita, de modo que las preguntas bien estudiadas se formulan de manera muy flexible.

Según la claridad de las preguntas y el modo del auditor, el auditado debe responder desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que este formula.

Por ello, aún siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía es más importante el modo y el orden de su formulación. El auditor debe aplicar los *check-list* de modo que el auditado responda clara y escuetamente. Se debe interrumpir lo menos posible a este y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta.

Algunas de las preguntas de las *check-list* utilizadas para cada sector, deben ser repetidas, con apariencia distinta y el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas o en fechas diferentes.

De este modo, se pueden descubrir con mayor facilidad los puntos contradictorios; el auditor debe analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. Los *check-list* responden fundamentalmente a dos tipos de filosofía de calificación o evaluación: rango y binarias.

1.6.3.1. *Check-list* de rango

Contiene preguntas que el auditor sitúa dentro de un rango específico, por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo. Se figuran posibles respuestas de los auditados.

Las preguntas deben sucederse sin que parezcan ajustadas ni clasificadas previamente. Basta con que el auditor lleve un pequeño listado. El cumplimiento del *check-list* no debe realizarse en presencia del auditado.

Las *check-list* de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones y permiten una mayor precisión en la evaluación.

1.6.3.2. *Check-list* binaria

Está constituida por preguntas con respuesta única y excluyente: si o no. Aritméticamente, equivalen a uno o cero, respectivamente. Las *check-list* binarias siguen una elaboración inicial mucho más ardua y compleja. Deben ser de gran precisión, como corresponde a la suma precisión de la respuesta.

1.6.4. Trazas o huellas

El auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas y no otras. Para ello, se debe apoyar en productos *software* que rastrean los caminos que siguen los datos a través del programa.

Esta trazabilidad se utiliza para comprobar la ejecución de las validaciones de datos previstas. No deben modificar en absoluto el sistema. Si la herramienta auditora produce incrementos apreciables de carga, se establecen de antemano las fechas y horas más adecuadas para su empleo.

Por lo que se refiere al análisis del sistema, se emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las librerías más importantes del mismo. Estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante.

1.6.5. *Software* de interrogación

Existen paquetes de *software* para auditoría, capaces de generar programas para auditores. Estos paquetes han ido evolucionando hacia la obtención de muestreos estadísticos que permiten la obtención de consecuencias e hipótesis de la situación real de una instalación. Los productos de *software* actuales se orientan principalmente hacia lenguajes que permiten la interrogación de archivos y bases de datos, siendo utilizados por los auditores externos.

2. CONTROLES Y METODOLOGÍAS

2.1. Controles

Son un conjunto de instrucciones sistemáticas, cuyo fin es vigilar las funciones y actitudes que permiten verificar si todo se realiza conforme a los programas establecidos, órdenes impartidas y principios admitidos dentro de una organización. Los controles también se definen como un proceso de medir el progreso hacia un desempeño planeado y de aplicar medidas correctivas para asegurar que el desempeño esté alineado con los objetivos de la organización.

2.1.1. Clasificación general de los controles

De acuerdo con el momento de llevar a cabo el control dentro de una auditoría de sistemas, los controles se clasifican en: preventivos, detectivos, correctivos y de retroalimentación.

2.1.1.1. Controles preventivos

Son aquellos controles que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de posibilidad de que ocurran los defectos. Estos controles se aplican antes de que se desempeñe una actividad. Su objetivo es prevenir los problemas que genera una desviación de los parámetros del desempeño.

Este control tiene lugar antes de principiar las operaciones e incluye la creación de políticas, procedimientos y reglas diseñadas para asegurar que las actividades planeadas serán ejecutadas consistentemente.

2.1.1.2. Controles detectivos

Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. En cierta forma sirven para evaluar la eficiencia de los controles preventivos. Por ejemplo, archivos y procesos que sirvan como pistas de auditoría o procedimientos de validación.

2.1.1.3. Controles correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

2.1.1.4. Controles de retroalimentación

Este tipo de control se enfoca sobre el uso de la información de los resultados anteriores, para corregir posibles desviaciones futuras del estándar aceptable.

2.1.2. Controles físicos y lógicos

Los controles particulares físicos y lógicos que se ejercen en la auditoría informática se especifican a continuación:

- Autenticidad: permiten verificar la identidad, contraseñas y firmas digitales.

- Exactitud: aseguran la coherencia de los datos, validación de campos y validación de excesos.

- Totalidad: evitan la omisión de registros así como garantizan la conclusión de un proceso de envió, conteo de registros y cifras de control.

- Redundancia: evitan la duplicidad de datos, cancelación de lotes y verificación de secuencias.

- Privacidad: aseguran la protección de los datos, compactación y encriptación.

- Existencia: aseguran la disponibilidad de los datos, bitácora de estados y mantenimiento de activos.

- Protección de activos: destrucción o corrupción de información o del *hardware*.

- Efectividad: aseguran el logro de los objetivos, encuestas de satisfacción y medición de niveles de servicio.

- Eficiencia: aseguran el uso óptimo de los recursos, programas monitores y análisis costo-beneficio.

2.1.3. Controles automáticos

Para controles de mayor eficiencia, dentro de los sistemas informáticos es posible integrar eventos para alimentar bases de datos de control para identificar si los procedimientos están de acuerdo con las políticas o normas establecidas.

2.1.3.1. Cambio de claves de acceso

Este control verifica que los cambios de las claves de acceso a los programas se realicen periódicamente y con la magnitud de evitar el uso de claves repetidas durante un intervalo de tiempo, es decir, que al momento de realizar el cambio de clave, esta clave nueva no sea igual a ninguna de las cinco claves anteriores que el usuario ha utilizado.

2.1.3.2. Combinación de alfanuméricos en claves de acceso

Este control pretende la verificación de que las claves de acceso no estén compuestas únicamente por datos alfabéticos o sólo numéricos, donde la clave sea muy fácil de interceptar por medio de búsquedas aleatorias de claves o por ingeniería social.

2.1.3.3. Verificación de datos de entrada

Se verifica la compatibilidad de los datos, pero no la exactitud o de los mismos, por ejemplo, se realiza la validación del tipo de datos que contienen los campos o la revisión de que el valor se halle dentro de algún rango.

2.1.3.4. Conteo de registros

Verifica la totalización de los registros, de manera que se crean campos de memoria para ir acumulando cada registro que se ingresa y verificar el total con los registros ya existentes.

2.1.3.5. Totales de control

Se realiza mediante la creación de totales de línea, columnas, cantidad de formularios, cifras de control, etcétera y automáticamente se verifica con un campo en el cual se van acumulando los registros, separando sólo aquellos formularios o registros con diferencias.

2.1.3.6. Verificación de límites

Consiste en la verificación automática de tablas, códigos, límites mínimos y máximos o bajo determinadas condiciones dadas previamente.

2.1.3.7. Verificación de secuencias

Consiste en verificar la secuencia numérica o alfabética de los procesos de los registros, ascendente o descendente, esta verificación se realiza mediante rutinas independientes del programa en sí.

2.1.3.8. Digito autoverificador

Consiste en incluir un dígito adicional a una codificación, el mismo que es resultado de la aplicación de un algoritmo o fórmula, conocido como módulos, que detecta la corrección o no del código. Por ejemplo, del décimo dígito de la cédula de identidad, calculado con el módulo 10.

2.1.3.9 Utilización de *software* de seguridad en los ordenadores

El *software* de seguridad restringe el acceso al ordenador, de tal modo que sólo el personal autorizado pueda utilizarlo. Este *software* permite la separación de funciones y la confidencialidad de la información mediante controles para que los usuarios puedan acceder sólo a los programas y datos para los que están autorizados.

2.1.4. Controles administrativos en el procesamiento de datos

Tanto en el desarrollo de *software*, su mantenimiento y su uso, se integran actividades de control a nivel administrativo que identifican los roles y recursos necesarios para auditar y ser auditados.

2.1.4.1. Controles de preinstalación

Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes, asegurando que el *hardware* y *software* se adquieran. Las acciones de este control son las siguientes:

- Elaboración de un informe técnico en el que se justifique la adquisición del equipo, *software* y servicios de computación, incluyendo un estudio costo-beneficio.

- Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación.

- Elaborar un plan de instalación de equipo y *software* (fechas, actividades, responsables) el mismo que debe contar con la aprobación de los proveedores del equipo.

- Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales. Este proceso debe enmarcarse en normas y disposiciones legales.

- Efectuar las acciones necesarias para una mayor participación de proveedores.

- Asegurar respaldo de mantenimiento y asistencia técnica.

2.1.4.2. Controles de organización y planificación

Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades, en labores tales como:

- Diseñar un sistema

- Elaborar los programas

- Operar el sistema

- Control de calidad

Evita que una misma persona tenga el control de toda una operación. Estos controles verifican la utilización óptima de recursos mediante la preparación de planes que serán evaluados continuamente. Las acciones de este control son las siguientes:

- La unidad informática debe estar al más alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.

- Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.

- Deben existir mecanismos necesarios con el fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.

- Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.

- El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.

- Las actividades del centro de cómputo deben obedecer a planificaciones a corto, mediano y largo plazo sujetos a evaluación y ajustes periódicos como un plan maestro de informática.

- Debe existir una participación efectiva de directivos, usuarios y personal del centro de cómputo en la planificación y evaluación del cumplimiento del plan.

- Las instrucciones deben impartirse por escrito

2.1.4.3. Controles de desarrollo y producción

Este control se enmarca en la justificación que los sistemas han sido la mejor opción para la organización, bajo una relación costo-beneficio que proporcionen oportuna y efectiva información, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados. Las acciones a seguir para el control del sistema de desarrollo y producción son los siguientes:

- Los usuarios deben participar en el diseño e implantación de los sistemas pues aportan conocimiento y experiencia de su área y esta actividad facilita el proceso de cambio.

- El personal de auditoría interna debe formar parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de control.

- El desarrollo, diseño y mantenimiento de sistemas obedece a planes específicos, metodologías estándares, procedimientos y en general a normatividad escrita y aprobada.

- Cada fase concluida debe ser aprobada documentadamente por los usuarios mediante actas u otros mecanismos con el fin de evitar reclamos posteriores.

- Los programas antes de pasar al sistema en producción deben ser probados con datos que agoten todas las excepciones posibles.

- Todos los sistemas deben estar debidamente documentados y actualizados. La documentación debe contener: informe de factibilidad, diagrama de bloque, diagrama de lógica del programa y objetivos del programa.

- Listado original del programa y versiones que incluyan los cambios efectuados con antecedentes de pedido y aprobación de modificaciones.

- Implantar procedimientos de solicitud, aprobación y ejecución de cambios a programas y formatos de los sistemas en desarrollo.

- El sistema concluido será entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos.

2.1.4.4. Controles de procesamiento

Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información, lo que conlleva al establecimiento de una serie de seguridades para:

- Asegurar que todos los datos sean procesados

- Garantizar la exactitud de los datos procesados

- Garantizar que se grabe un registro para uso de la gerencia y con fines de auditoría.

- Asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.

Las acciones que se encuentran en el control de procesamiento son las siguientes:

- Validación de datos de entrada previo procesamiento debe ser realizada en forma automática: clave, dígito autoverificador, totales de lotes, etcétera.

- Preparación de datos de entrada debe ser responsabilidad de usuarios y consecuentemente su corrección.

- Recepción de datos de entrada y distribución de información de salida debe obedecer a un horario elaborado en coordinación con el usuario, realizando un debido control de calidad.

- Adoptar acciones necesarias para correcciones de errores

- Analizar conveniencia costo-beneficio de estandarización de formularios, fuente para agilizar la captura de datos y minimizar errores. Los procesos interactivos deben garantizar una adecuada interrelación entre usuario y sistema.

- Planificar el mantenimiento del *hardware* y *software*, tomando todas las seguridades para garantizar la integridad de la información y el buen servicio a usuarios.

2.1.4.5. Control de operación

Abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento, la administración del ordenador de las cintas de *back-up* y la operación de terminales y equipos de comunicación por parte de los usuarios de sistemas *on-line*. Este control de operación tiene como fin:

- Prevenir o detectar errores accidentales que puedan ocurrir en el centro de cómputo durante un proceso.

- Evitar o detectar el manejo de datos con fines fraudulentos por parte de funcionarios del centro de cómputo.

- Garantizar la integridad de los recursos informáticos

- Asegurar la utilización adecuada de equipos acorde a planes y objetivos

Las acciones para el control de operación son las siguientes:

- El acceso al centro de cómputo debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado.

- Implantar contraseñas para garantizar la operación de consola y equipo central a personal autorizado.

- Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y cómo responder ante esos eventos.

- Mantener una bitácora de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.

- Los operadores del equipo central deben estar entrenados para recuperar o restaurar información en caso de destrucción de archivos.

- Los *back-up*s no deben ser menores de dos y deben guardarse en lugares seguros y adecuados, preferentemente en bóvedas de bancos.

- Se deben implantar calendarios de operación con el fin de establecer prioridades de proceso.

- Todas las actividades del centro de cómputo deben regularse mediante manuales, instructivos, normas, reglamentos, etcétera.

- El proveedor de *hardware* y *software* deberá proporcionar lo siguiente: manual de operación de equipos, de lenguaje de programación, de utilitarios disponibles, de Sistemas Operativos.

- Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras.

- Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como: reguladores de voltaje, supresores pico, UPS y generadores de energía.

- Contratar pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos imprevistos o mala operación.

2.1.5. Controles de uso del ordenador

Estos controles se ejecutan sobre el uso adecuado de los ordenadores y la confidencialidad e integridad de la información, debido a la vulnerabilidad de los equipos y el fácil acceso que pueda existir sobre ellos. Las acciones que se encuentran dentro de este control son los siguientes:

- Adquisición de equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo.

- Vencida la garantía de mantenimiento del proveedor se debe contratar mantenimiento preventivo y correctivo.

- Establecer procedimientos para obtención de *back-up*s de paquetes y de archivos de datos.

- Revisión periódica y sorpresiva del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la organización.

- Mantener programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos.

- Estandarización del Sistema Operativo, *software* utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y mantener actualizadas las versiones y la capacitación sobre modificaciones incluidas.

2.2. Metodologías de la auditoría de sistemas

Para llevar a cabo una auditoría informática existen diferentes metodologías que permiten establecer los controles necesarios y determinar las oportunidades de mejora en los procesos.

2.2.1. Metodología estándar de una auditoría de sistemas

Existe una metodología estándar que se puede llevar a cabo al momento de auditar sistemas, con el fin de establecer los pasos desde la preparación de la auditoría hasta emitir los informes finales.

2.2.1.1. Definición del alcance y objetivos

El alcance de la auditoría expresa los límites de la misma, dejando un acuerdo muy preciso entre auditores y clientes sobre las funciones, las materias y las organizaciones a auditar.

Tanto los alcances como las excepciones deben figurar al comienzo del informe final. Las personas que realizan la auditoría deben conocer con la mayor exactitud posible los objetivos de sus tareas. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas. Una vez definidos los objetivos específicos, se añadirán a los objetivos generales y comunes de toda auditoría informática.

2.2.1.2. Estudio inicial del entorno auditable

Para realizar dicho estudio se examinan las funciones y actividades generales de la informática. Para su realización el auditor debe conocer la organización, el entorno operacional y las aplicaciones de bases de datos y archivos.

2.2.1.3. Organización

La organización provee el conocimiento de quién ordena, quién diseña y quién ejecuta. Para realizar esto el auditor debe tomar en cuenta los siguientes aspectos:

- Organigrama: el organigrama expresa la estructura oficial de la organización a auditar. Si se descubriera que existe un organigrama real diferente al oficial, se pone de manifiesto tal circunstancia.

- Departamentos: se entiende como departamento a los órganos que siguen inmediatamente a la dirección. El equipo auditor debe describir brevemente las funciones de cada uno de ellos.

- Relaciones jerárquicas y funcionales entre órganos de la organización: el equipo auditor verifica si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama o por el contrario detectará, por ejemplo, si algún empleado tiene dos jefes. Las de jerarquía implican la correspondiente subordinación. Las funcionales por el contrario, indican relaciones no estrictamente de subordinados.

- Flujos de información: además de las corrientes verticales entre departamentos, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extradepartamentales. Los canales alternativos de información también se verifican, sin los cuales las funciones no podrían ejercerse con eficacia.

- Número de puestos de trabajo: el equipo auditor comprueba que los nombres de los puestos de trabajo de la organización corresponden a las funciones reales distintas. Si no es así, esta situación pone de manifiesto deficiencias estructurales, entonces los auditores dan a conocer tal circunstancia y expresan el número de puestos de trabajo verdaderamente diferentes.

- Número de personas por puesto de trabajo: es un parámetro que los auditores informáticos consideran. La incompatibilidad del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

2.2.1.4. Entorno operacional

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse. Este conocimiento previo se logra determinando los siguientes extremos:

- Situación geográfica de los sistemas: se determina la ubicación geográfica de los distintos centros de proceso de datos en la organización. A continuación, se verifica la existencia de responsables en cada uno de ellos, así como el uso de los mismos estándares de trabajo.

- Arquitectura y configuración de *hardware* y *software*: cuando existen varios equipos, es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible bien comunicado. La configuración de los sistemas está muy ligada a las políticas de seguridad lógica de la organización. Los auditores, en su estudio inicial, deben tener en su poder la distribución e interconexión de los equipos.

- Inventario de *hardware* y *software*: el auditor recaba información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación. En cuanto a *hardware* figuran CPU, unidades de controles locales y remotos, periféricos de todo tipo, etcétera.

El inventario de *software* debe contener todos los productos lógicos del sistema, desde el *software* básico hasta los programas de utilidad adquiridos o desarrollados internamente.

- Telecomunicaciones: en el estudio inicial los auditores deben disponer del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones. Igualmente, deben poseer información de las redes locales de la organización.

2.2.1.5. Aplicaciones de bases de datos y archivos

El estudio inicial que realizan los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la organización auditada. Para la información siguiente es necesario conocer lo siguiente:

- Volumen, antigüedad y complejidad de las aplicaciones.

- Metodología del diseño: se clasifica globalmente la existencia total o parcial de metodología en el desarrollo de las aplicaciones. Si se han utilizado varias metodologías a lo largo del tiempo se pone de manifiesto.

- Documentación: la existencia de una adecuada documentación de las aplicaciones proporciona beneficios tangibles e inmediatos muy importantes. La documentación de programas disminuye gravemente el mantenimiento de los mismos.

- Cantidad y complejidad de bases de datos y archivos: el auditor recaba información de tamaño y características de las bases de datos, clasificándolas en relación y jerarquías. Se halla un promedio de número de accesos a ellas por hora o días. Esta operación se repetirá con los archivos, así como la frecuencia de actualizaciones de los mismos. Estos datos proporcionan una visión aceptable de las características de la carga informática.

2.2.1.6. Determinación de recursos de la auditoría informática

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

2.2.1.6.1. Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente. Las herramientas *software* propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente. Los recursos materiales del auditor son de dos tipos:

- Recursos materiales *software*: programas propios de la auditoría, habitualmente se añaden a las ejecuciones de los procesos del cliente para verificarlos.

- Recursos materiales *hardware*: los recursos *hardware* que el auditor necesita deben ser proporcionados por el cliente. Los procesos de control deben efectuarse necesariamente en las computadoras del auditado. Para lo cual habrá de convenir, tiempo de máquina, espacio de disco, impresoras ocupadas, etcétera.

2.2.1.6.2. Recursos humanos

La cantidad de recursos depende del volumen auditable. Las características y perfiles del personal seleccionado dependen de la materia auditable. En la tabla I se muestran los perfiles de los profesionales requeridos para llevar a cabo una auditoría de sistemas de información.

Tabla I. **Perfiles profesionales de los auditores informáticos**

Profesión	**Actividades y conocimientos deseables**
Informático generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en explotación y en desarrollo de proyectos. Conocedor de sistemas.
Experto en desarrollo de proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de desarrollo más importantes.
Técnico de sistemas	Experto en Sistemas Operativos y *software* básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de explotación.
Experto en bases de datos y administración de las mismas	Con experiencia en el mantenimiento de bases de datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación.
Experto en *software* de comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en subsistemas de teleproceso.

Continuación de la tabla I.

Experto en explotación y gestión de centros de procesamientos de datos	Responsable de algún centro de cálculo. Amplia experiencia en automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de costes	Economista con conocimiento de informática. Gestión de costes.

Fuente: <www.funredes.org>. [Consulta: en agosto de 2011].

2.2.1.7. Elaboración del plan de trabajo

Una vez asignados los recursos, el responsable de la auditoría y sus colaboradores establecen un plan de trabajo. Se procede a la programación del mismo y el plan se elabora teniendo en cuenta los siguientes criterios:

- Si la revisión debe realizarse por áreas generales o áreas específicas. En el primer caso, la elaboración es más compleja y costosa.

- Si la auditoría es global, de toda la informática o parcial. El volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal. Dentro del plan se tienen contemplados los siguientes aspectos:

- En el plan no se consideran calendarios debido al manejo de recursos genéricos y no específicos.

- En el plan se establecen los recursos y esfuerzos globales que van a ser necesarios.

- En el plan se establecen las prioridades de materias auditables, siempre de acuerdo con las prioridades del cliente.

- El plan establece disponibilidad futura de los recursos durante la revisión.

- El plan estructura las tareas a realizar por cada integrante del grupo.

- En el plan se expresan todas las ayudas que el auditor ha de recibir del auditado.

Una vez elaborado el plan, se procede a la programación de actividades. Esta ha de ser lo suficientemente flexible como para permitir modificaciones a lo largo del proyecto.

2.2.1.8. Actividades de la auditoría informática

La auditoría informática global se realiza por áreas generales o por áreas específicas. Si se examina por grandes temas, resulta evidente la mayor calidad y el empleo de más tiempo total y mayores recursos.

Cuando la auditoría se realiza por áreas específicas, se abarcan de una vez todas las peculiaridades que afectan a la misma, de forma que el resultado se obtiene más rápidamente y con menor calidad. Dentro de las actividades y herramientas utilizadas se encuentran las siguientes:

- Actividades
- Análisis de la información recabada del auditado
- Análisis de la información propia
- Cruzamiento de las informaciones anteriores
- Entrevistas
- Simulación
- Muestreos
- Herramientas
- Cuestionario general inicial
- Cuestionario *check-list*
- Estándares
- Monitores

- Simuladores
- Paquetes de auditoría
- Matrices de riesgo

2.2.1.9. Informe final

La función de la auditoría se materializa exclusivamente por escrito. Por lo tanto la elaboración final es la muestra de su calidad. Resulta evidente la necesidad de redactar borradores e informes parciales previos al informe final, los que son elementos de contraste entre opinión entre auditor y auditado y que pueden descubrir fallos de apreciación en el auditor.

2.2.1.9.1. Estructura del informe final

El informe comienza con la fecha de inicio de la auditoría y la fecha de redacción del mismo. Se incluyen los nombres del equipo auditor y los nombres de todas las personas entrevistadas, con indicación de la jefatura, responsabilidad y puesto de trabajo que ejecute. La estructura es la siguiente:

- Definición de objetivos y alcance de la auditoría
- Enumeración de temas considerados
- Cuerpo expositivo: para cada tema, se sigue el siguiente orden:

- Situación actual: cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expone la situación prevista y la situación real.

- Tendencias: se trata de hallar parámetros que permitan establecer tendencias futuras.

- Puntos débiles y amenazas

- Recomendaciones y planes de acción: constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.

- Redacción posterior de la carta de introducción o presentación

2.2.1.9.2. Modelo conceptual de la exposición del informe final

El informe debe incluir solamente hechos importantes. La publicación de hechos poco relevantes o accesorios desvía la atención del lector. Además, debe consolidar los hechos que se describen en el mismo. El término de hechos consolidados adquiere un especial significado de verificación objetiva y de estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios.

- El hecho debe poder ser sometido a cambios

- Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.

- No deben existir alternativas viables que superen al cambio propuesto

- La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

La aparición de un hecho en un informe de auditoría implica necesariamente la existencia de una debilidad que ha de ser corregida. A continuación se muestra el flujo del hecho o debilidad.

- Hecho encontrado: debe ser relevante para el auditor y para el cliente. Ha de ser exacto y además convincente. No deben existir hechos repetidos.

- Consecuencias del hecho: las consecuencias deben redactarse de modo que sean directamente deducibles del hecho.

- Repercusión del hecho: se redactan las influencias directas que el hecho pueda tener sobre otros aspectos informáticos u otros ámbitos de la organización.

- Conclusión del hecho: no deben redactarse conclusiones más que en los casos en que la exposición haya sido muy extensa o compleja.

- Recomendación del auditor informático: debe entenderse por sí sola, por simple lectura. Debe ser concreta y exacta en el tiempo, para que pueda ser verificada su implementación. Y la recomendación se redacta de forma que vaya dirigida expresamente a la persona o personas que puedan implementarla.

2.2.1.10. Carta de introducción o presentación del informe final

La carta de introducción tiene especial importancia porque en ella ha de resumirse la auditoría realizada. Se destina exclusivamente al responsable máximo de la organización o a la persona concreta que encargó o contrató la auditoría. Así como pueden existir tantas copias del informe final como solicite el cliente, la auditoría no debe hacer copias de la citada carta de introducción. La carta de introducción posee los siguientes atributos:

- Tiene como máximo 4 folios
- Incluye la fecha, naturaleza, objetivos y alcance
- Cuantifica la importancia de las áreas analizadas
- Proporciona una conclusión general, concretando las áreas de gran debilidad.
- Presenta las debilidades en orden de importancia y gravedad

2.2.2. CRMR

CRMR (por sus siglas en inglés, Computer Resource Management Review), destaca la posibilidad de realizar una evaluación de eficiencia de utilización de los recursos por medio de la administración. Una revisión de esta naturaleza no tiene el grado de profundidad de una auditoría informática global, pero proporciona soluciones más rápidas a problemas concretos y notorios.

2.2.2.1. Supuestos de aplicación

La metodología CRMR es aplicable más a deficiencias organizativas y gerenciales que a problemas de tipo técnico, pero no cubre cualquier área de un centro de procesos de datos. El método CRMR puede aplicarse cuando se producen algunas de las situaciones de las siguientes:

- Se detecta una mala respuesta a las peticiones y necesidades de los usuarios.
- Los resultados del centro de procesos de datos no están a disposición de los usuarios en el momento oportuno.
- Se genera con alguna frecuencia información errónea por fallos de datos o proceso.
- Existen sobrecargas frecuentes de capacidad de proceso
- Existen costes excesivos de proceso en el centro de proceso de datos

2.2.2.2. Áreas de aplicación

Las áreas en que el método CRMR puede ser aplicado corresponden a las condiciones de aplicación señaladas en el punto anterior:

- Gestión de datos
- Control de operaciones

- Control y utilización de recursos materiales y humanos
- Interfaces y relaciones con usuarios
- Planificación
- Organización y administración

2.2.2.3. Objetivos

CRMR tiene como objetivo fundamental evaluar el grado de bondad o ineficiencia de los procedimientos y métodos de gestión que se observan en un centro de proceso de datos. Las recomendaciones que se emitan como resultado de la aplicación del CRMR, tendrán como finalidad algunas de las siguientes:

- Identificar y fijar responsabilidades
- Mejorar la flexibilidad de realización de actividades
- Aumentar la productividad
- Disminuir costes
- Mejorar los métodos y procedimientos de dirección

2.2.2.4. Alcance

Se fijan los límites que abarca el CRMR, antes de comenzar el trabajo. Se establecen tres clases:

- Reducido: el resultado consiste en señalar las áreas de actuación con gran potencial e inmediata obtención de beneficios.

- Medio: en este caso, el CRMR ya establece conclusiones y recomendaciones, tal y como se hace en la auditoría informática ordinaria.

- Amplio: el CRMR incluye planes de acción, aportando técnicas de implementación de las recomendaciones, a la par que desarrolla las conclusiones.

2.2.2.5. Información necesaria para la evaluación del CRMR

Se determinan en este punto los requisitos necesarios para que esta asociación de auditoría y consultoría pueda llevarse a cabo con éxito. A continuación se describen los tres aspectos más importantes de información para llevar a cabo el CRMR.

- Integración del auditor en el centro de procesos de datos: el trabajo de campo del CRMR se realiza completamente integrado en la estructura del centro de proceso de datos del cliente y con los recursos de él. Se evalúan las actividades desde el punto de vista gerencial.

- Programa de trabajo clasificado por tareas: se debe cumplir un detallado programa de trabajo por tareas. Todo trabajo debe ser descompuesto en tareas. Cada una de ellas se somete a la siguiente sistemática:

  - Identificación de la tarea

  - Descripción de la tarea

  - Descripción de la función de dirección cuando la tarea se realiza incorrectamente.

  - Descripción de ventajas, sugerencias y beneficios que puede originar un cambio o modificación de tarea.

  - Test para la evaluación de la práctica directiva en relación con la tarea.

  - Posibilidades de agrupación de tareas

  - Ajustes en función de las características de un departamento concreto.

  - Registro de resultados, conclusiones y recomendaciones

- Información necesaria del cliente: el cliente es el que facilita la información que el auditor diferencia con su trabajo de campo. A continuación se muestra una *check-list* completa de los datos necesarios para llevar a cabo el CRMR:

- Datos de mantenimiento preventivo de *hardware*
- Informes de anomalías de los sistemas
- Procedimientos estándar de actualización
- Procedimientos de emergencia
- Monitorización de los sistemas
- Informes del rendimiento de los sistemas
- Mantenimiento de las librerías de programas
- Gestión de espacio en disco
- Documentación de entrega de aplicaciones a explotación
- Utilización de CPU, canales y discos
- Datos de paginación de los sistemas
- Volumen total y libre de almacenamiento
- Ocupación media de disco
- Manuales de procedimientos de explotación

3. ESTÁNDARES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

3.1. COBIT

COBIT significa Objetivos de Control para la Información y Tecnologías Relacionadas y es un estándar aplicable para las buenas prácticas de seguridad y control en tecnología de información. Se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF). El desarrollo de COBIT es la publicación de los siguientes aspectos:

- Resumen ejecutivo: consiste en una síntesis ejecutiva que proporciona el entendimiento y conciencia sobre los conceptos clave y principios de COBIT y el marco referencial proporciona un entendimiento más detallado de los conceptos clave y principios de COBIT e identifica los cuatro dominios de COBIT y los correspondientes 34 procesos de TI.

- Marco referencial: describe los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información y los recursos de TI.

- Objetivos de control: contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control, detallados y específicos a través de los 34 procesos de TI.

- Guías de auditoría: contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar soporte a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar recomendaciones de mejora.

- Conjunto de herramientas de implementación: incluye la síntesis ejecutiva, proporcionando conciencia y entendimiento de COBIT. También incluye una guía de implementación con dos útiles herramientas. La primera es el diagnóstico de la conciencia de la gerencia (Management Awareness Diagnostic) y la segunda es el diagnóstico de control de TI (IT Control Diagnostic) que proporcionan soporte en el análisis del ambiente de control en TI de una organización.

3.1.1. Audiencia

Dentro de la metodología COBIT se encuentran los siguientes actores como parte de la audiencia a quien se dirige la auditoría:

- Administración: es utilizado para dar soporte y lograr un balance entre los riesgos y las inversiones en control en un ambiente de TI frecuentemente impredecible.

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

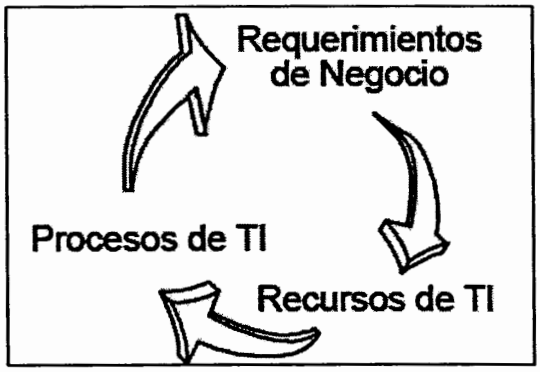
- Auditores de sistemas de información: es utilizado para dar soporte a las opiniones mostradas a la administración sobre los controles internos.

Además de responder a las necesidades de la audiencia inmediata de la alta gerencia, a los auditores y a los profesionales dedicados al control y seguridad, COBIT puede ser utilizado dentro de las organizaciones por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso y por todos aquellos responsables de TI en la organización.

3.1.2. El marco referencial

El concepto fundamental del marco referencial 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 tomando en cuenta a la información como el resultado de la aplicación combinada de recursos relacionados con la IT que deben ser administrados por procesos de TI. La figura 1 muestra los principios del marco referencial, que se componen de los requerimientos de información del negocio, los recursos de TI y procesos de TI.

Figura 1. **Principios del marco referencial**



Fuente: <www.isaca.org>. [Consulta: en agosto de 2011].

3.1.2.1. Requerimientos de información del negocio

Dichos requerimientos son informaciones que se necesitan 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 de los modelos referenciales existentes y conocidos tales como:

- Requerimientos de calidad: entre estos se encuentran la calidad, el costo y entrega. La calidad es considerada principalmente por no fallas, confiable, etcétera, donde también se encuentran los criterios de integridad. La premisa se refiere a que la primera prioridad está dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto útil de la calidad está cubierto por los criterios de efectividad.

- Requerimientos fiduciarios: en estos requerimientos se encuentra la efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento le leyes. Y a continuación se describe cada uno de estos conceptos de acuerdo con COBIT.

  - Efectividad: se refiere a que la información debe ser relevante y apropiada para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

  - Eficiencia: se refiere a que se debe proveer información mediante el empleo óptimo de los recursos. Esta es la forma más productiva y económica.

- Confiabilidad: se refiere a que se debe proveer la información apropiada para que la administración tome las decisiones adecuadas para manejar la empresa y cumplir con sus responsabilidades.

- Cumplimiento de las leyes: son compromisos pactados con los cuales está comprometida la organización.

- Requerimientos de seguridad: con respecto a los aspectos de seguridad, existen tres componentes que son la confidencialidad, integridad y disponibilidad como los elementos clave. Y a continuación se describe cada uno de estos conceptos de acuerdo con COBIT:

  - Confidencialidad: es la protección de la información contra divulgación no autorizada.

  - Integridad: se refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la organización.

  - Disponibilidad: se refiere a la accesibilidad a la información cuando sea requerida por los procesos del negocio y el *back-up* de los recursos y capacidades asociadas a la misma.

Las medidas de control no se satisfacen necesariamente en los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación dentro del marco referencial que a continuación se describe:

- Primario: es el grado de impacto directo del objetivo de control definido sobre el requerimiento de información de interés.

- Secundario: es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

- Blanco: los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y por otro proceso.

3.1.2.1.1. Recursos de TI

COBIT establece los datos, aplicaciones, tecnología, instalaciones y personas como los recursos en TI necesarios para alcanzar los objetivos de negocio. El dinero o capital no es considerado como un recurso para la clasificación de objetivos de control para TI debido a que la inversión puede realizarse en cualquiera de los recursos mencionados anteriormente y puede causar confusión con los requerimientos de auditoría financiera. A continuación se describen los recursos de TI:

- Datos: son todos los objetos de información. Se considera información interna y externa, estructurada o no, gráficas, sonidos, etcétera.

- Aplicaciones: son los sistemas de información, que integran procedimientos manuales y sistematizados.

- Tecnología: es el *hardware* y *software* básico, Sistemas Operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etcétera.

- Instalaciones: son los recursos necesarios para alojar y dar soporte a los sistemas de información.

- Personas: es utilizado por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de información.

3.1.2.1.2. Procesos de TI

El marco referencial 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 tres niveles de actividades de TI al considerar la administración de sus recursos, como lo muestra la figura 2.

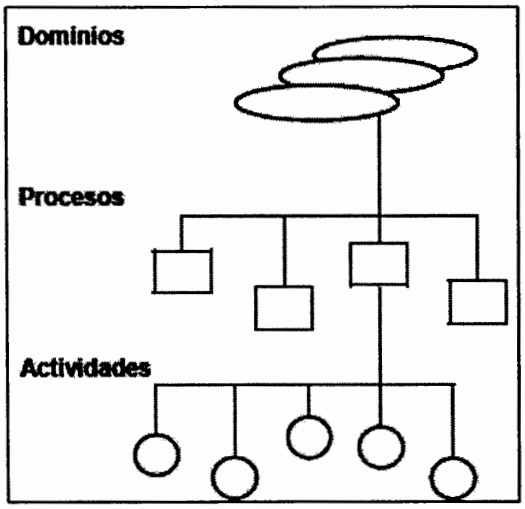
Comenzando por la base, se encuentran las actividades y las tareas necesarias para encontrar un resultado que se pueda medir. Las actividades cuentan con un concepto de ciclo de vida, pero se consideran más discretas.

Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios. La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Por lo que, los procesos se definen en un nivel superior como una serie de actividades o tareas conjuntas con cortes o límites de control. Al nivel más alto, los procesos son agrupados en dominios. Ese agrupamiento se refiere a dominios de responsabilidad en una estructura organizacional y está en línea con el ciclo administrativo aplicable a los procesos de TI.

Las actividades son acciones requeridas para lograr un resultado que se puede medir. La figura 2 muestra como están conformados los procesos de alto nivel y del nivel inferior.

Figura 2. **Agrupación de procesos de TI**



Fuente: <www.isaca.org>. [Consulta: en agosto de 2011].

3.1.2.2. Dominios

Es el agrupamiento lógico de procesos, se entiende como dominios de responsabilidad dentro de una estructura y se ajusta en el ciclo de vida aplicable a los procesos de TI. Entonces, existen cuatro grandes dominios: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo. Las definiciones para los dominios mencionados son las siguientes:

- Planeación y organización: este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la IT puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, mantiene la consecución de la visión estratégica, que necesita ser planeada, comunicada y administrada desde diferentes perspectivas.

- Adquisición e implementación: 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.

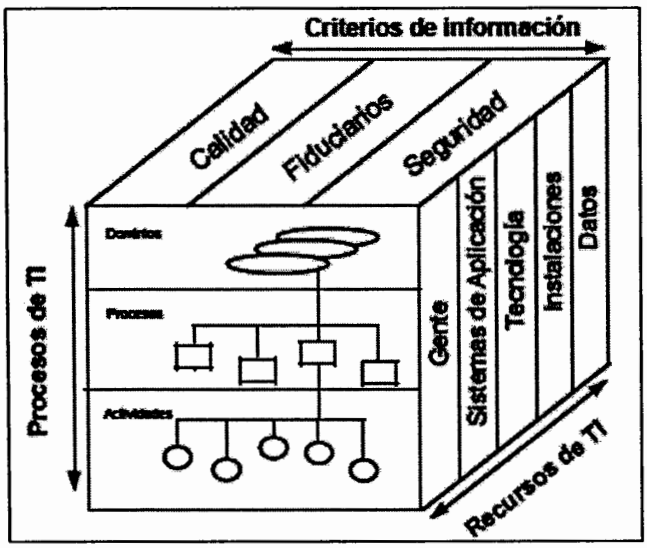
- Entrega y soporte: en este dominio hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, se establecen los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- Monitoreo: todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

3.1.2.3. Cubo de interrelaciones

En la figura 3 se muestra el llamado cubo de interrelaciones definido por COBIT. Se utiliza para facilitar el empleo eficiente de los objetivos de control como soporte a los diferentes puntos de vista. Además, se representan los objetivos de control de alto nivel y las tres dimensiones del marco referencial: procesos, recursos y criterios.

Figura 3. **Cubo de interrelaciones**



Fuente: <www.isaca.org>. [Consulta: en agosto de 2011].

La parte superior del cubo representa la vista de la dirección, es decir, que proporciona la clave para el criterio de la información mediante el conjunto de requerimientos de la información: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad, identificando así cuál criterio y en qué grado (primario o secundario) es aplicable a cada objetivo de control de TI de alto nivel.

La cara derecha del cubo identifica los recursos de TI que son administrados en forma específica por el proceso que se considera en ese momento y no aquellos que simplemente toman parte en el proceso. Por ejemplo, el proceso llamado administración de información se concentra particularmente en la integridad y confiabilidad de los recursos de datos, mientras que disponibilidad y confidencialidad son proporcionadas por los procesos que administran los recursos que utilizan los datos, como por ejemplo, aplicaciones y tecnología.

3.1.3. Objetivos de control

Un objetivo de control es la declaración del resultado deseado o propuesto que se ha de alcanzar mediante la aplicación de procedimientos de control en cualquier actividad de TI. Se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI. La tabla II proporciona una indicación por proceso y dominio de TI, de cuales criterios de información (primarios y secundarios) tienen impacto en los objetivos de alto nivel así como una indicación de cuales recursos de TI son aplicables.

La P significa que son criterios de información primarios y la S significa que son criterios de información secundarios y el cheque indica que ese recurso de TI es aplicable para el proceso de TI.

Tabla II. **Resumen de los objetivos de control**

Dominio	Proceso	Criterios de información							Recursos de TI				
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Recursos humanos	Información	Tecnología	Instalaciones	Datos
Planeación y organización													
PO1	Definir un plan estratégico de TI	P	S						✓	✓	✓	✓	✓
PO2	Definir la arquitectura de información	P	S	S	S					✓			✓
PO3	Determinar la dirección tecnológica	P	S								✓	✓	
PO4	Definir la org. y relaciones de TI	P	S						✓				
PO5	Manejar la inversión en TI	P	P					S	✓	✓	✓	✓	
PO6	Comunicar las directrices gerenciales	P					S		✓				
PO7	Administrar recursos humanos	P	P						✓				
PO8	Asegurar el cumplir req. externos	P					P	S	✓	✓			✓
PO9	Evaluar riesgos	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
PO10	Administrar proyectos	P	P						✓	✓	✓	✓	
PO11	Administrar calidad	P	P		P			S	✓	✓			
Adquisición e implementación													
AI1	Identificar soluciones	P	S							✓	✓	✓	
AI2	Adquis. y mantener *software* de aplic.	P	P		S		S	S		✓			
AI3	Adquirir y mantener arquitectura de TI	P	P		S						✓		
AI4	Desarr. y mantener proc. relac. con TI	P	P		S		S	S	✓	✓	✓	✓	
AI5	Instalar y acreditar sistemas	P			S	S			✓	✓	✓	✓	✓
AI6	Administrar cambios	P	P		P	P		S	✓	✓	✓	✓	✓
Servicios y soporte													
DS1	Definir niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS2	Administrar servicios de terceros	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS3	Administrar desempeño y capacidad	P	P			S				✓	✓	✓	

Continuación de la tabla II.

DS4	Asegurar servicio continuo	P	S			P			✓	✓	✓	✓	✓
DS5	Garantizar la seguridad de sistemas			P	P	S	S	S	✓	✓	✓	✓	✓
DS6	Identificar y asignar costos		P					P	✓	✓	✓	✓	✓
DS7	Capacitar usuarios	P	S						✓				
DS8	Asistir a los clientes de TI	P							✓	✓			
DS9	Administrar la configuración	P				S		S		✓	✓	✓	
DS10	Administrar problemas e incidentes	P	P			S			✓	✓	✓	✓	✓
DS11	Administrar datos				P			P					✓
DS12	Administrar instalaciones				P	P						✓	
DS13	Administrar operaciones	P	P		S	S			✓	✓	✓	✓	✓
Monitoreo													
M1	Monitorear los procesos	P	S	S	S	S	S	S	✓	✓	✓	✓	✓
M2	Evaluar lo adecuado del control Interno	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
M4	Proveer auditoría independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

Fuente: <www.isaca.org>. [Consulta: en agosto de 2011].

3.2. COSO

El informe COSO es un manual de control interno publicado por Committee of Sponsoring Organization of the Treadway Commission donde se integran las metodologías y conceptos en todos los niveles de las áreas administrativas y operativas de una organización bajo una estructura de control interno.

El control interno definido por COSO, es un proceso integrado a los procesos empresariales efectuado por los altos directivos de la organización, la administración y el resto del personal de una unidad organizativa, diseñado con el propósito de proporcionar una garantía para el logro de objetivos siguientes:

- Eficacia y eficiencia de las operaciones

- Confiabilidad de la información financiera

- Cumplimiento de las leyes, reglamentos y políticas

La eficacia se refiere a la capacidad de alcanzar las metas propuestas, mientras que la eficiencia se refiere a la capacidad de producir el máximo de resultados con el mínimo de recursos, refiriéndose básicamente a los objetivos empresariales: rendimiento, rentabilidad y *back-ups* de los recursos.

La confiabilidad de la información financiera se refiere a la elaboración y publicación de estados financieros confiables, incluyendo la información de uso interno. El control interno es un proceso, es decir, un medio para alcanzar un fin y no un fin en sí mismo, que es llevado a cabo por las personas que actúan en todos los niveles sin que se trate solamente de manuales de organización y procedimientos, proporcionando un nivel de seguridad en su ejecución.

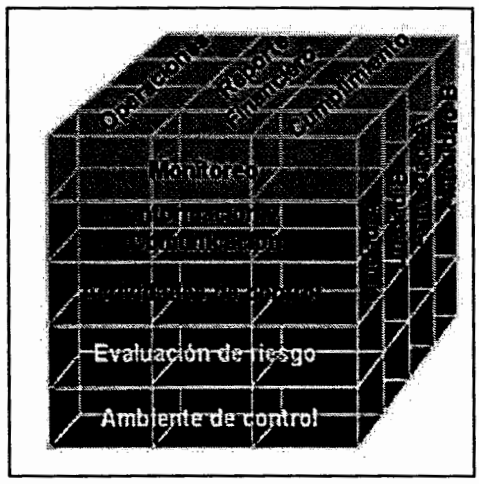
Al hablarse del control interno como un proceso, se hace referencia a una cadena de acciones extendida a todas las actividades, propios a la gestión e integrados a los demás procesos básicos de la misma: planificación, ejecución y supervisión. Tales acciones se hallan incorporadas a la infraestructura de la unidad organizativa, para influir en el cumplimiento de sus objetivos y apoyar sus iniciativas de calidad.

3.2.1. Componentes

El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión

Figura 4. **Componentes de COSO**



Fuente: <www.coso.org>. [Consulta: en agosto de 2011].

En la figura 4 se muestran los componentes de COSO donde el ambiente de control es la base para influir en la conciencia de control de su personal. Es el fundamento de los demás componentes del control interno y provee disciplina y estructura. La evaluación del riesgo es la identificación y el análisis de los riesgos relevantes que corre la organización para el logro de sus objetivos, formando la base para determinar cómo se deben administrar los riesgos.

Los sistemas de información y comunicación soportan la base para identificar, capturar e intercambiar información en una forma y período de tiempo que permita al personal cumplir con sus responsabilidades. Las actividades de control son las políticas y los procedimientos que deben seguirse para tener certeza que las instrucciones de la gerencia se llevan a cabo. Monitoreo es un proceso para verificar la calidad de desempeño del control interno a través del tiempo.

3.2.1.1. Ambiente de control

El ambiente de control refleja la actitud general, el grado de conciencia y las acciones de la junta directiva, la gerencia, los dueños y otros involucrados a la importancia del control y el énfasis en el control sobre las políticas, procedimientos, métodos y estructura organizacional de la organización. El ambiente de control incluye la actitud de la gerencia hacia el desarrollo de estimaciones contables y en la filosofía para reportar información financiera, es el contexto en que operan el sistema contable y los controles internos.

El entorno del control es la atmósfera dentro de la cual existen los controles contables de una organización y se preparan los estados financieros. Los principales factores del ambiente de control son:

- La filosofía y estilo de la dirección y la gerencia

- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.

- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.

- Las formas de asignación de responsabilidades y de administración y desarrollo del personal.

- El grado de documentación de políticas y decisiones; y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.

El sistema de control interno se sustenta en los valores éticos, que definen la conducta de quienes lo operan. Estos valores éticos pertenecen a una dimensión moral y, por lo tanto, van más allá del mero cumplimiento de las leyes, decretos, reglamentos y otras disposiciones normativas.

El comportamiento y la integridad moral encuentran su base y desarrollo en la cultura de la organización, donde esta determina, en gran medida, cómo se hacen las cosas, qué normas y reglas se observan.

La alta dirección de la organización especifica el nivel de competencia requerido para las distintas tareas y traducirlo en requerimientos de conocimientos y habilidades. Los métodos de contratación de personal aseguran que el candidato posea el nivel de preparación y experiencia que se ajuste a los requisitos especificados. Una vez incorporado, el personal debe recibir la orientación, capacitación y adiestramiento necesarios en forma práctica y metódica.

La estructura organizativa, formalizada en un organigrama, constituye el marco formal de autoridad y responsabilidad en el cual las actividades que se desarrollan en cumplimiento de los objetivos del organismo, son planeadas, efectuadas y controladas. La organización completa su organigrama, con un manual de organización, en el cual se debe asignar la responsabilidad, las acciones y los cargos, a la par de establecer las diferentes relaciones jerárquicas y funcionales para cada uno de estos.

La misión, los objetivos y las políticas de cada organismo están relacionados, debiendo estar explicitados en documentos oficiales. Dichos documentos son difundidos a la comunidad y a todos los niveles organizacionales.

Los procedimientos de contratación, inducción, capacitación y adiestramiento, calificación, promoción y disciplina, se corresponden con los propósitos enunciados en la política de la organización.

3.2.1.2. Evaluación de riesgos

Para comprender el proceso de evaluación de riesgo a nivel de empresa, el equipo a cargo del proyecto debe considerar factores tales como:

- Si se han establecido y comunicado los objetivos a nivel de empresa, incluyendo la manera como están soportados por planes estratégicos y complementados a nivel de proceso o de aplicación.

- Si se ha establecido un proceso de evaluación de riesgos que incluya una estimación de la importancia de los riesgos, evaluación de las probabilidades de que ocurran y determinación de las acciones necesarias.

- Si se han establecido mecanismos para anticipar, identificar y reaccionar a situaciones que puedan tener un efecto dramáticamente extenso en la empresa.

- Si existen mecanismos para anticipar, identificar y reaccionar a eventos rutinarios o a actividades que afecten el logro de los objetivos de la entidad o a nivel de proceso o aplicación.

- Si el departamento de contabilidad ha establecido procesos para identificar cambios significativos en los principios de contabilidad generalmente aceptados promulgados por las autoridades pertinentes.

- Si los canales de comunicación están facultados para notificar al departamento de contabilidad los cambios en las prácticas de negocios de la empresa que pueden afectar el método o el proceso de registrar transacciones.

- Si el departamento de contabilidad tiene procesos para identificar cambios importantes en el entorno operativo, incluyendo cambios regulativos.

Se identifican los riesgos relevantes que enfrenta un organismo en la persecución de sus objetivos, ya sean de origen interno como externo. Su desarrollo comprende la realización de un mapeo del riesgo, que incluya la especificación de los dominios o puntos claves del organismo, la identificación de los objetivos generales y particulares y las amenazas y riesgos que se pueden tener que afrontar. Una vez identificados, el análisis de los riesgos incluye:

- Una estimación de su importancia y trascendencia

- Una evaluación de la probabilidad y frecuencia

- Una valoración de la pérdida que podría resultar

- Una definición del modo en que habrán de manejarse

También son necesarios los mecanismos para detectar y encarar el tratamiento de los riesgos asociados con el cambio. Aunque el proceso de evaluación es similar al de los otros riesgos, la gestión de los cambios se efectúa independientemente, dada su gran importancia y las posibilidades de que los mismos pasen inadvertidos para quienes están inmersos en las rutinas de los procesos. Existen circunstancias que pueden merecer una atención especial en función del impacto potencial que plantean:

- Cambios en el entorno
- Redefinición de la política institucional
- Reorganizaciones o reestructuraciones internas
- Ingreso de empleados nuevos o rotación de los existentes
- Nuevos sistemas, procedimientos y tecnologías
- Aceleración del crecimiento
- Nuevos productos, actividades o funciones

3.2.1.3. Actividades de control

Están constituidas por los procedimientos específicos establecidos como una garantía para el cumplimiento de los objetivos, orientados principalmente hacia la prevención y neutralización de los riesgos.

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos según lo expresado en el punto anterior: conociendo los riesgos, se disponen los controles destinados a evitarlos o minimizarlos, los cuales pueden agruparse en tres categorías, según el objetivo de la entidad con el que estén relacionados:

- Las operaciones
- La confiabilidad de la información financiera
- El cumplimiento de leyes y reglamentos

A su vez en cada categoría existen diversos tipos de control:

- Preventivo / correctivos
- Manuales / automatizados o informáticos
- Gerenciales o directivos

Las actividades de control se dividen en las siguientes categorías:

- Análisis efectuados por la dirección
- Seguimiento y revisión por parte de los responsables de las diversas funciones o actividades.

- Comprobación de las transacciones en cuanto a su exactitud, totalidad y autorización pertinente: aprobaciones, revisiones, cotejos, recálculos, análisis de consistencia y prenumeraciones.

- Controles físicos patrimoniales: arqueos, conciliaciones, recuentos

- Dispositivos de seguridad para restringir el acceso a los activos y registros.

- Segregación de funciones

- Aplicación de indicadores de rendimiento

Las tareas y responsabilidades esenciales relativas al tratamiento, autorización, registro y revisión de las transacciones y hechos, son asignadas a personas diferentes. El propósito de esta norma es procurar un equilibrio conveniente de autoridad y responsabilidad dentro de la estructura organizacional. Cada área o subárea del organismo opera coordinadamente, manteniendo interrelaciones con las restantes áreas o subáreas.

La estructura de control interno y todas las transacciones y hechos significativos, son claramente documentados y la documentación debe estar disponible para su verificación. Todo organismo debe contar con la documentación referente a su sistema de control interno y a los aspectos pertinentes de las transacciones y hechos significativos.

El acceso a los recursos, activos, registros y comprobantes, debe estar protegido por mecanismos de seguridad y limitado a las personas autorizadas, quienes están obligadas a rendir cuenta de su custodia y utilización.

Todo activo de valor debe ser asignado a un responsable de su custodia y contar con adecuadas protecciones, a través de seguros, almacenaje, sistemas de alarma, pases para acceso, etcétera.

El sistema de información es controlado con el objetivo de garantizar su correcto funcionamiento y asegurar el control del proceso de diversos tipos de transacciones. Un sistema de información abarca información cuantitativa, tal como los informes de desempeño que utilizan indicadores y cualitativa, tal como la atinente a opiniones y comentarios.

Los recursos de la tecnología de informar son controlados con el objetivo de garantizar el cumplimiento de los requisitos del sistema de información que la organización necesita para el logro de su misión. La información que necesitan las actividades del organismo, es provista mediante el uso de recursos de tecnología de información. Estos abarcan datos, sistemas de aplicación, tecnología asociada, instalaciones y personal.

3.2.1.4. Información y comunicación

Información y comunicación es el proceso de capturar e intercambiar información que se necesita para ejecutar, administrar y controlar las operaciones de la organización. Información y comunicación abarcan la captura y la emisión de información al personal adecuado para que este pueda cumplir con sus responsabilidades, incluyendo una comprensión de las funciones y responsabilidades individuales que pertenecen al control interno sobre reportes de información financiera. La información y comunicación atiende a los siguientes mecanismos:

- La información interna y externa provee a la Dirección los reportes necesarios para el establecimiento de objetivos organizacionales.

- Es proporcionada información a las personas adecuadas con suficiente detalle y oportunidad para cumplir con sus responsabilidades.

- Los sistemas de información están basados en un plan estratégico

- Apoyo de la dirección al desarrollo de los sistemas de información necesarios.

- La comunicación al personal, es eficaz en la descripción de sus funciones y responsabilidades con respecto al control interno.

- El establecimiento de canales de comunicación para la denuncia de posibles actos indebidos.

- La alta dirección es receptiva a sugerencias de los empleados

- La comunicación a través de toda la empresa es efectiva

- Seguimiento oportuno y adecuado de la dirección de la información obtenida de clientes, proveedores, organismos de control y otros terceros.

El sistema de información se diseña atendiendo a la estrategia y al programa de operaciones de la organización, sirviendo para tomar decisiones a todos los niveles; evaluar el desempeño de la organización, de sus programas, proyectos, sectores, procesos, actividades, operaciones, etcétera y rendir cuenta de la gestión.

La calificación de sistema de información se aplica, tanto al que cubre la información financiera de una organización como al destinado a registrar otros procesos y operaciones internos.

El sistema de información es revisado para la verificación del diseño y para la detección de deficiencias en su funcionamiento y productos. Cuando el organismo cambia de estrategia, misión, política, objetivos, programa de trabajo, etcétera, se contempla el impacto en el sistema de información.

El interés y el compromiso de la autoridad superior del organismo con los sistemas de información, se manifiesta mediante una asignación de recursos suficientes para su funcionamiento eficaz.

Es fundamental que la autoridad superior de un organismo tenga total comprensión del importante rol que desempeñan los sistemas de información para el correcto desenvolvimiento de sus deberes y responsabilidades y en tal sentido debe mostrar una actitud comprometida hacia los mismos.

Los canales de comunicación presentan un grado de apertura y eficacia adecuado a las necesidades de información internas y externas. El sistema se estructura en canales de transmisión de datos e información. En gran medida el mantenimiento del sistema radica en vigilar la apertura y buen estado de estos canales, que conectan diferentes emisores y receptores de variada importancia.

3.2.1.5. Supervisión

La supervisión es un proceso de evaluación para determinar la calidad del control interno a través del tiempo, considerando si los controles están operando para lo que fueron diseñados y asegurando que son modificados apropiadamente por condiciones cambiantes. Esto implica evaluar el diseño y la operación de los controles con regularidad, tomando las acciones correctivas necesarias.

Este proceso se logra mediante actividades sobre la marcha y evaluaciones separadas o combinaciones de ambas. Para comprender el proceso de monitoreo a nivel de empresa, el equipo a cargo del proyecto debe tener presente factores tales como:

- Si se llevan a cabo evaluaciones periódicas del control interno

- Grado en que el personal, en el desarrollo de sus funciones regulares, obtiene evidencia de que el sistema de control interno continúa funcionando.

- Grado en que las comunicaciones de partes externas corroboran la información generada internamente o indican problemas.

- Si la gerencia sigue las recomendaciones que le hacen los auditores internos y los auditores independientes.

- Enfoque de la gerencia para corregir oportunamente las condiciones de información conocidas.

- Enfoque de la gerencia para manejar los reportes y recomendaciones provenientes de autoridades reguladoras.

- Existencia de una función de la auditoría interna que la gerencia usa para ayudarse en el monitoreo, la cual incluye factores tales como la independencia y reportes directamente a la junta directiva o al comité de auditoría.

- Idoneidad en la asignación de personal, entrenamiento y existencia de destrezas especializadas de acuerdo con el entorno.

- Cumplimiento con las normas profesionales aplicables

- Alcance de actividades, un balance entre auditorías financieras y operacionales, cobertura y rotación de operaciones descentralizadas.

- Idoneidad de la planeación, evaluación de riesgos y documentación del trabajo ejecutado y las conclusiones alcanzadas.

- Inexistencia de responsabilidades operativas

El equipo a cargo del proyecto es el que evalúa si el sistema de control interno está sujeto a automonitoreo y si incluye mecanismos apropiados para asegurar que cualquier deficiencia observada sea corregida. En el caso de que los métodos de automonitoreo y corrección de deficiencias sean evaluados como inadecuados, el equipo propone recomendaciones específicas para mejorar el sistema.

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales. Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real, generan respuestas dinámicas a las circunstancias sobrevivientes. En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

- Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que estos conllevan, la competencia y experiencia de quienes aplican los controles y los resultados de la supervisión continuada.

- Son ejecutados por los propios responsables de las áreas de gestión (autoevaluación), la auditoría interna y los auditores externos.

- La tarea del evaluador es averiguar el funcionamiento real del sistema, que los controles existan y estén formalizados, que se apliquen cotidianamente como una rutina incorporada a los hábitos y que resulten aptos para los fines perseguidos.

- Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.

- El nivel de documentación de los controles varía según la dimensión y complejidad de la entidad.

La naturaleza y el nivel de la documentación requieren mayor rigor cuando se necesite demostrar la fortaleza del sistema ante terceros. Se confecciona un plan de acción que contemple:

- El alcance de la evaluación
- Las actividades de supervisión continuadas existentes
- La tarea de los auditores internos y externos
- Áreas o asuntos de mayor riesgo
- Programa de evaluaciones
- Evaluadores, metodología y herramientas de control
- Presentación de conclusiones y documentación de soporte
- Seguimiento para que se adopten las correcciones pertinentes

Las deficiencias o debilidades del sistema de control interno detectadas a través de los diferentes procedimientos de supervisión son comunicadas a efectos de que se adopten las medidas de ajuste correspondientes. Según el impacto de las deficiencias, los destinatarios de la información pueden ser tanto las personas responsables de la función o actividad implicada como las autoridades superiores.

3.3. SAC

El informe SAC se basa en una estructura de control interno, describiendo sus componentes y provee las clasificaciones de los controles, definiendo los objetivos de control y riesgos y el rol del auditor interno para llevar a cabo una auditoría informática. El informe es una guía sobre el uso, administración y protección de los recursos de tecnología informática y discute los efectos de la computación de usuario final, las telecomunicaciones y las tecnologías emergentes.

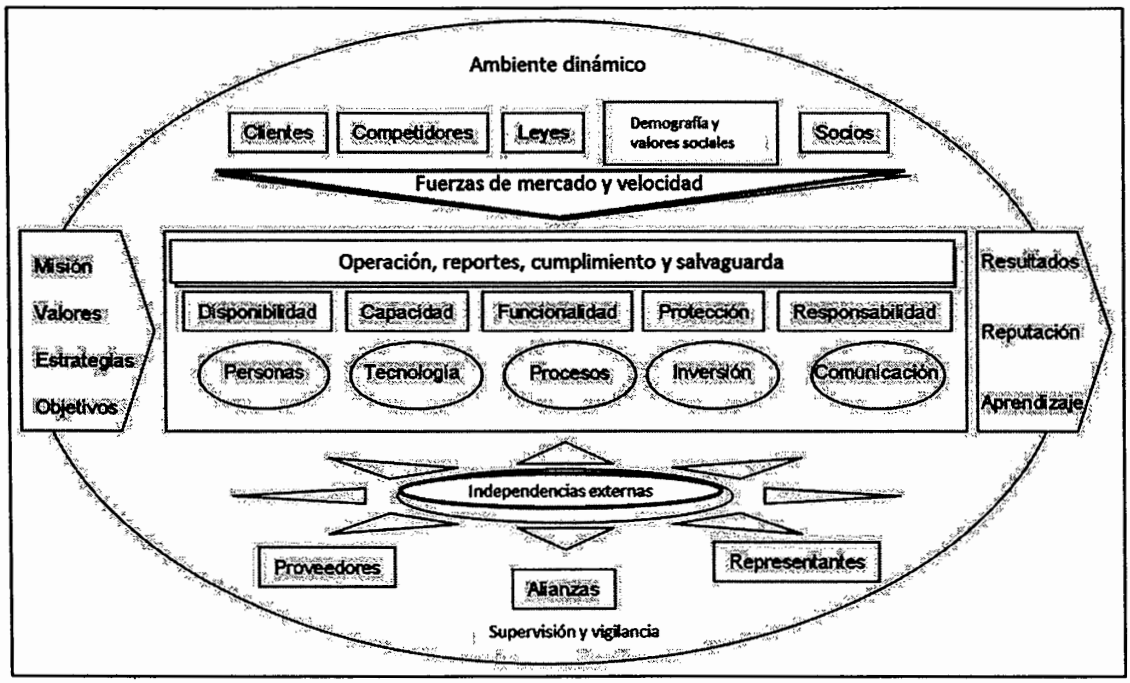
El informe SAC es una fuente de información la cual se centra en el entendimiento, monitoreo, evaluación y la minimización de los riesgos en IT, examinando los riesgos en todos los componentes del sistema de negocio, incluyendo clientes, competidores, proveedores y socios. El informe SAC define a un sistema de control interno como un conjunto de procesos, funciones, actividades, subsistemas y gente que son agrupados o conscientemente segregados para asegurar el logro efectivo de los objetivos y metas.

El informe enfatiza el rol e impacto de los sistemas computarizados de información sobre el sistema de control interno. El mismo acentúa la necesidad de evaluar los riesgos, pesar los costos y beneficios y construir controles en los sistemas en lugar de agregarlos luego de la implementación.

Este modelo está desarrollado para facilitar la evaluación y discusión acerca de la respuesta a las estrategias sobre la administración de riesgos, centrándose en la disponibilidad, capacidad, funcionalidad, protección, responsabilidad de la IT de una organización, las redes y su infraestructura.

Tal y como el modelo COSO contiene un lenguaje común de control para la administración y los auditores, el modelo SAC tiene una facilidad de discusión sobre los objetivos, riesgos y su minimización para el entorno de la organización. Se enfoca en la administración de riesgos como resultado de los cambios frecuentes en la tecnología y los modelos de negocios.

Figura 5. **Modelo SAC**



Fuente: <www.theiia.org>. [Consulta: en agosto de 2011].

En la figura 5 se muestra el modelo SAC, en donde se enmarcan varios componentes de IT de modelos de negocios, los cuales se toman en cuenta en el reporte SAC para su control interno, donde en una organización se persigue la misión establecida por medio de estrategias y objetivos que son consistentes con la misión. La flecha de lado izquierdo indica tal proceso.

La organización pretende alcanzar estos resultados mientras que preserva su reputación y aprende como mejorar su desempeño en el futuro. Estos resultados se demuestran con la flecha derecha del modelo. El amplio contexto de control de efectividad y eficiencia de las operaciones, reportes administrativos y financieros, cumplimiento de leyes y el resguardo de los activos de una organización están representados en el centro superior de la figura 5 y están representados como operaciones, reportes, cumplimiento y *back-ups*.

En la flecha derecha de los atributos de control de disponibilidad, capacidad, funcionalidad, protección y responsabilidad representan las actividades pertinentes de un modelo de negocios, que pueden ser llamados objetivos de aseguramiento del negocio. Estos objetivos de aseguramiento del negocio están creados con el propósito de proveer la infraestructura para el modelo SAC. Los objetivos mencionados se resumen de la siguiente manera:

- Disponibilidad: es la habilidad de recibir, aceptar, procesar y dar soporte a las transacciones en todo momento como se requiera.

- Capacidad: se refiere a una entrega de punto a punto, completa y confiable de las transacciones en todo momento.

- Funcionalidad: se refiere a que el sistema la infraestructura necesaria, sensibilidad y fácil uso para el usuario de acuerdo con sus necesidades y expectativas.

- Protección: se refiere a los controles lógicos y físicos de la seguridad que administran el acceso a los servidores, las aplicaciones y la información.

- Responsabilidad: se refiere a que el procesamiento de las transacciones son exactas, completas y no repudiables.

El modelo pretende alcanzar la disponibilidad, capacidad, funcionalidad, protección y responsabilidad por medio de una infraestructura, recursos y una comisión organizacional, que están conformados por personas, tecnología, procesos, inversiones y comunicación como se muestra en los óvalos en la tercera fila en el centro del modelo.

La complejidad del ambiente en el modelo está representado por las fuerzas externas, en la figura 5 se muestra como las flechas multidireccionales, donde el impacto del crecimiento de la interacción, interconectividad y compartimiento del sistema con las fuerzas externas (clientes, competidores, proveedores, comunidad) y la velocidad de cambio, compuesto por las interdependencias externas (proveedores, alianzas, representantes), muestra como las diferentes fuerzas afectan el ambiente del negocio.

El ambiente en el modelo SAC se muestra como el gran ovalo de la figura 5. El ambiente dinámico es también llamado el ambiente del control o riesgos. El modelo SAC muestra que los elementos primarios para el mantenimiento de un ambiente estable y controlado son la supervisión y la vigilancia.

El sistema de control interno consiste en tres componentes: el ambiente de control, los sistemas manuales y automatizados y los procedimientos de control. El ambiente de control incluye la estructura de la organización, la estructura de control, las políticas y procedimientos y las influencias externas.

Los sistemas automatizados consisten en sistemas y *software* de aplicación. SAC discute los riesgos de control asociados con los sistemas de usuario final y sistemas departamentales pero no describe ni define los sistemas manuales. Los procedimientos de control consisten en controles generales, de aplicaciones y compensatorios.

SAC provee cinco esquemas de clasificación para los controles internos en los sistemas informáticos: preventivos, detectivos y correctivos, discrecionales y no discrecionales, voluntarios y obligatorios, manuales y automatizados y controles de aplicaciones y generales.

Estos esquemas se enfocan en cuánto se aplica el control, si el control puede ser evitado, quién impone la necesidad del control, cómo se implementa el control y dónde se implementa el control en el *software*.

Entre los riesgos que toma en cuenta SAC, incluyen fraudes, errores, interrupción del negocio y el uso ineficiente e inefectivo de los recursos. Los objetivos de control reducen estos riesgos y aseguran la integridad de la información, la seguridad y el cumplimiento. La integridad de la información es resguardada por los controles de calidad entrada, procesamiento, salidas y *software*.

Las medidas de seguridad incluyen los controles de seguridad de los datos, física y de programas. Los controles de cumplimiento aseguran conformidad con las leyes y regulaciones, los estándares contables y de auditoría y las políticas y procedimientos internos.

Las responsabilidades de los auditores internos incluyen asegurar la adecuación del sistema de control interno, la confiabilidad de los datos y el uso eficiente de los recursos de la organización. A los auditores internos también les concierne la prevención y detección de fraudes y la coordinación de actividades con los auditores externos.

Para los auditores internos es necesaria la integración de las habilidades de auditoría y sistemas de información y una comprensión del impacto de la tecnología informática sobre el proceso de auditoría. Estos profesionales realizan ahora auditorías financieras, operativas y de los sistemas de información.

3.4. Otros estándares de auditoría de sistemas

Dentro de la industria se encuentran otros estándares para la auditoría de sistemas como AICPA SYSTRUST y MARGERIT, los cuales contemplan una serie de parámetros y procedimientos para llevar a cabo la evaluación y diagnóstico de los sistemas de información.

3.4.1. AICPA - SYSTRUST

SYSTRUST es un documento desarrollado por AICPA (American Institute of Certified Public Accountantsy) y CICA (Canadian Institute of Chartered Accountants), para el asesoramiento y desarrollo de una auditoría informática. SYSTRUST es un conjunto de servicios y alertas de seguridad, basados en una infraestructura común, compuesta de capas de principios y criterios para el control de los riesgos y oportunidades de IT.

Los principios son un conjunto amplio de objetivos y los criterios son *benchmarks* utilizados para medir y presentar los intereses subjetivos y contra qué se deben evaluar esos intereses. SYSTRUST Principles and Criteria for Systems Reliability, utiliza los principios de disponibilidad, seguridad, integridad y mantenimiento para evaluar si un sistema de información es fiable. Los principios y criterios están organizados dentro de las siguientes áreas:

- Políticas: la organización tiene definidas y documentadas las políticas relevantes para un principio en particular.

- Comunicaciones: la organización tiene comunicadas las políticas a los usuarios con la autorización debida.

- Procedimientos: la organización utiliza procedimientos para alcanzar los objetivos en concordancia con las políticas definidas.

- Supervisión: la organización supervisa el sistema y toma las acciones necesarias para mantener concordancia con las políticas definidas.

3.4.1.1. Disponibilidad

Se refiere a la accesibilidad del sistema, productos y servicios como los establecidos en cualquier contrato, niveles de servicio u otros acuerdos, tomando en cuenta que este principio no establece por sí mismo los niveles de desempeño requeridos, sino que estos son establecidos por las entidades involucradas en el desarrollo y utilización del sistema. En la tabla III se muestra el principio de disponibilidad y los criterios asociados a la misma.

Tabla III. **Criterios del principio de disponibilidad**

Disponibilidad: el sistema está disponible para la operación y uso en cualquier momento de acuerdo con los niveles de servicio.	
Criterio	
A1 La entidad tiene definidos y comunicados los objetivos de desempeño, políticas y estándares para la disponibilidad del sistema	
A1.1	Los requerimientos de disponibilidad del sistema para usuarios autorizados y objetivos de disponibilidad del sistema, políticas y estándares están identificados y documentados.
A1.2	Los objetivos de disponibilidad del sistema, políticas y estándares documentados han sido comunicados a los usuarios autorizados.
A1.3	Los objetivos de disponibilidad del sistema, políticas y estándares documentados son consistentes con los requerimientos de disponibilidad especificados en el contrato legal y cualquier otro servicio de acuerdo legal y de aplicaciones a las leyes y regulaciones.
A1.4	La responsabilidad de la disponibilidad del sistema está asignada.
A1.5	Los objetivos de disponibilidad del sistema, políticas y estándares documentados son comunicados a la entidad responsable de implementar dichos objetivos, políticas y estándares documentados.
A2 La entidad utiliza procedimientos, personas, *software*, información e infraestructura para alcanzar los objetivos de disponibilidad en concordancia con las políticas y estándares establecidos.	
A2.1	La adquisición, implementación, configuración y administración de los componentes del sistema relacionados a la disponibilidad del sistema son consistentes con los objetivos, políticas y estándares documentados de la disponibilidad del sistema.

Continuación de la tabla III.

A2.2	Existen procedimientos para proteger el sistema contra riesgos potenciales que puedan interferir con la operación del sistema y deteriorar la disponibilidad del sistema.
A2.3	Existe retroalimentación continua sobre los errores de procesamiento menores, destrucción de registros e interrupciones importantes que pudieron deteriorar la disponibilidad del sistema.
A2.4	Existen procedimientos para asegurar que el personal responsable del diseño, desarrollo, implementación y operación de la disponibilidad del sistema están calificados y llena todos los requisitos para satisfacer la responsabilidad de la disponibilidad del sistema
A3 La entidad supervisa el sistema y toma las acciones necesarias para alcanzar lo conforme a los objetivos, políticas y estándares de la disponibilidad del sistema.	
A3.1	El desempeño de la disponibilidad del sistema es revisado periódicamente y comparado con los requerimientos documentados de disponibilidad del sistema de usuarios autorizados, contratos legales y otros acuerdos de niveles de servicio.
A3.2	Existe un proceso para identificar daños potenciales a la capacidad de disponibilidad del sistema, de acuerdo con los objetivos, políticas y estándares documentos y tomar las acciones necesarias.
A3.3	Se supervisan los cambios ambientales y tecnológicos y su impacto en la disponibilidad del sistema se determina periódicamente en una base de tiempo.

Fuente: <www.aicpa.org>. [Consulta: en agosto de 2011].

3.4.1.2. Seguridad

Se refiere a la protección de los componentes del sistema de accesos no autorizados, tanto lógicos como físicos. Este principio contiene criterios para la limitación del acceso a los componentes del sistema, con el propósito de prevenir abusos potenciales de los componentes, hurto de recursos, uso incorrecto del *software*, alteración o destrucción de la información. La tabla IV muestra los criterios del principio de seguridad.

Tabla IV. **Criterios del principio de seguridad**

Seguridad: el sistema está protegido contra accesos no autorizados físicos y lógicos.	
Criterios	
S1 La entidad tiene definidos y comunicados los objetivos de desempeño, políticas y estándares de la seguridad del sistema.	
S1.1	Los requerimientos de la seguridad del sistema para usuarios autorizados y los objetivos de seguridad, políticas y estándares, están identificados y documentados.
S1.2	Los objetivos, políticas y estándares de la seguridad documentados están bien comunicados hacia las personas autorizadas.
S1.3	Los objetivos, políticas y estándares de la seguridad documentados son consistentes con los requerimientos de seguridad del sistema definidos en el contrato legal y otros acuerdos de niveles de servicio y leyes aplicables y regulatorias.
S1.4	La responsabilidad de la seguridad del sistema está asignada.
S1.5	Los objetivos, políticas y estándares de la seguridad documentados son comunicados al personal responsable de su implementación.

Continuación de la tabla IV.

S2 La entidad utiliza procedimientos, personas, *software*, información e infraestructura para alcanzar los objetivos de seguridad del sistema en concordancia con las políticas y estándares establecidos.	
S2.1	La adquisición, implementación, configuración y administración de los componentes del sistema relacionados a la seguridad del sistema son consistentes con los objetivos, políticas y estándares de la seguridad documentados.
S2.2	Hay procedimientos para identificar y autenticar a todos los usuarios autorizados para tener acceso al sistema.
S2.3	Hay procedimientos para conceder privilegios de acceso al sistema a usuarios en concordancia con las políticas y estándares para conceder dichos privilegios.
S2.4	Hay procedimientos para restringir el acceso a las salidas de procesamiento de información a usuarios autorizados.
S2.5	Hay procedimientos para restringir el acceso a información almacenada *off-line* como medios de *back-ups* a usuarios autorizados.
S2.6	Hay procedimientos para proteger el acceso a puntos externos contra el acceso lógico no autorizado.
S2.7	Hay procedimientos para proteger el sistema contra infecciones de virus, códigos maliciosos y *software* no autorizado.
S2.8	Amenazas de sabotaje, terrorismo, vandalismo y otros ataques físicos se han considerado al localizar el sistema.
S2.9	Hay procedimientos para repudiar funciones incompatibles dentro del sistema con autorizaciones de la seguridad.
S2.10	Hay procedimientos para proteger el sistema contra accesos físicos no autorizados.

Continuación de la tabla IV.

S2.11	Hay procedimientos para asegurar que el personal responsable del diseño, desarrollo, implementación y operación de la seguridad del sistema están calificados y llena todos los requisitos para satisfacer la responsabilidad de la seguridad del sistema.
S3 La entidad supervisa el sistema y toma las acciones necesarias para alcanzar lo conforme a los objetivos, políticas y estándares de la seguridad del sistema.	
S3.1	El desempeño de la seguridad del sistema es revisado periódicamente y comparado con los requerimientos documentados de seguridad del sistema de usuarios autorizados, contratos legales y otros acuerdos de niveles de servicio
S3.2	Existe un proceso para identificar daños potenciales a la capacidad de seguridad del sistema de acuerdo con los objetivos, políticas y estándares documentos y tomar las acciones necesarias.
S3.3	Se supervisan los cambios ambientales y tecnológicos y su impacto en la seguridad del sistema se determina periódicamente en una base de tiempo.

Fuente: <www.aicpa.org>. [Consulta: en agosto de 2011].

3.4.1.3. Integridad

Se refiere al procesamiento completo, exacto, puntual y autorizado del sistema. La completitud indica que todas las transacciones y servicios son procesados o desempeñados sin excepciones. La exactitud incluye el aseguramiento de que la información que se procesa seguirá siendo exacta a través del proceso de la transacción.

La puntualidad se refiere a la entrega oportuna de la información y la autorización incluye el aseguramiento de que las transacciones se ejecutan de acuerdo con los privilegios definidos por las políticas que gobiernan el proceso del sistema. En la tabla V se muestran los criterios del principio de integridad.

Tabla V. **Criterios del principio de integridad**

Integridad: el procesamiento del sistema es completo, exacto, puntual y autorizado.	
Criterio	
I1 La entidad tiene definidos y comunicados los objetivos de desempeño, políticas y estándares de la integridad de procesamiento del sistema.	
I1.1	Los requerimientos de la integridad del procesamiento del sistema para usuarios autorizados y los objetivos de la integridad del sistema, políticas y estándares, están identificados y documentados.
I1.2	Los objetivos, políticas y estándares documentados de la integridad del sistema están bien comunicados hacia las personas autorizadas.
I1.3	Los objetivos, políticas y estándares documentados de la integridad del sistema son consistentes con los requerimientos de integridad del sistema definidos en el contrato legal y otros acuerdos de niveles de servicio y leyes aplicables y regulatorias.
I1.4	La responsabilidad de la integridad del sistema está asignada.
I1.5	Los objetivos, políticas y estándares documentados de la integridad del sistema son comunicados al personal responsable de su implementación.
I2 La entidad utiliza procedimientos, personas, *software*, información e infraestructura para alcanzar los objetivos de integridad del sistema en concordancia con las políticas y estándares establecidos.	

Continuación de la tabla V.

I2.1	La adquisición, implementación, configuración y administración de los componentes del sistema relacionados a la integridad del sistema son consistentes con los objetivos, políticas y estándares documentados de la integridad del procesamiento del sistema.
I2.2	Los procedimientos de integridad del procesamiento de información relacionados a las entradas de información son consistentes con los requerimientos documentados de la integridad del sistema.
I2.3	Hay procedimientos para asegurar que el procesamiento del sistema sea completo, exacto, puntual y autorizado.
I2.4	Los procedimientos de integridad del procesamiento de información relacionados a las salidas de información son consistentes con los requerimientos documentados de la integridad del sistema.
I2.5	Hay procedimientos para asegurar que el personal responsable del diseño, desarrollo, implementación y operación de la integridad del sistema están calificados y llena todos los requisitos para satisfacer la responsabilidad.
I2.6	Hay procedimientos de trazabilidad de la información, tanto desde la fuente hacia el final del procesamiento como del final del procesamiento hacia la fuente de información.
I3 La entidad supervisa el sistema y toma las acciones necesarias para alcanzar lo conforme a los objetivos, políticas y estándares.	
I3.1	El desempeño de la integridad del sistema es revisado periódicamente y comparado con los requerimientos documentados de integridad del sistema de usuarios autorizados, contratos legales y otros acuerdos de niveles de servicio.

Fuente: <www.aicpa.org>. [Consulta: en agosto de 2011].

3.4.1.4. Mantenimiento

Se refiere a que las actualizaciones en el sistema no afectan la disponibilidad, seguridad e integridad del sistema. En la tabla VI se muestran los criterios del principio de mantenimiento para un sistema informático, con el fin de auditar esa área del sistema y verificar que los mantenimientos al sistema no afectan los demás principios definidos en el SYSTRUST.

Tabla VI. **Criterios del principio de mantenimiento**

Mantenimiento: el sistema puede ser actualizado cuando se requiera, de tal manera que el sistema continué proveyendo disponibilidad, seguridad e integridad.	
Criterios	
M1 La entidad tiene definidos y comunicados los objetivos de desempeño, políticas y estándares para el mantenimiento del sistema.	
M1.1	Los objetivos, las políticas y los estándares documentados de la capacidad de mantenimiento del sistema toman en cuenta todas las áreas afectadas por los cambios de sistema.
M1.2	Los objetivos de mantenimiento del sistema, políticas y estándares son comunicados a todos los usuarios autorizados.
M1.3	Los objetivos, políticas y estándares documentados del mantenimiento del sistema son consistentes con los requerimientos de mantenimiento del sistema definidos en el contrato legal y otros acuerdos de niveles de servicio y leyes aplicables y regulatorias.
M1.4	La responsabilidad para el mantenimiento del sistema está asignada.
M1.5	Los objetivos, políticas y estándares documentados de mantenimiento del sistema son comunicados al personal responsable de su implementación.

Continuación de la tabla VI.

M2	La entidad utiliza procedimientos, personas, *software*, información e infraestructura para alcanzar los objetivos del mantenimiento del sistema en concordancia con las políticas y estándares establecidos.
M2.1	Los recursos disponibles para el mantenimiento del sistema son consistentes con los requerimientos documentados de usuarios autorizados y objetivos, políticas y estándares documentados.
M2.2	Procedimientos para administrar, planificar y documentar todos los cambios previstos para el sistema se aplican a las modificaciones de los componentes del sistema para mantener la disponibilidad, seguridad e integridad del sistema consistente con los objetivos, políticas y estándares documentados.
M2.3	Hay procedimientos para asegurar que sólo los cambios autorizados, probados y documentados son realizados en el sistema y en la información.
M2.4	Hay procedimientos para comunicar los cambios del sistema planificados y terminados a la gerencia de sistemas de información y a los usuarios autorizados.
M2.5	Hay procedimientos a tomar en cuenta y para controlar cambios de emergencia.

Fuente: <www.aicpa.org>. [Consulta: en agosto de 2011].

3.4.2. MARGERIT

Es un estándar de análisis y gestión de riesgos de los sistemas de información en materia de seguridad de sistemas de información, este estándar presenta un objetivo definido en el estudio de los riesgos que afectan los sistemas de información y el entorno de ellos haciendo unas recomendaciones de las medidas apropiadas que deberían adoptarse para conocer, prevenir, evaluar y controlar los riesgos investigados.

MARGERIT desarrolla el concepto de control de riesgos en las guías de procedimientos, técnicas, desarrollo de aplicaciones, personal y cumplimiento de normas legales. MARGERIT persigue los siguientes objetivos:

- Directos: concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de impedirlos a tiempo, ofrecer un método sistemático para analizar tales riesgos y ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

- Indirectos: preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MARGERIT está enfocado en la administración de los riesgos y expone de una manera conceptual en qué consiste el análisis de riesgos y su gestión. Se definen dos grandes áreas: análisis de riesgos y gestión de riesgos. El análisis de riesgos permite determinar qué tiene la organización y estimar lo que podría pasar. Está compuesto por los siguientes elementos:

- Activos: son los elementos del sistema de información o componentes del mismo, que aportan valor a la organización.

- Amenazas: son situaciones que les pueden pasar a los activos causando un perjuicio a la organización.

- *Back-ups*: son elementos de defensa utilizados para minimizar el daño que causen las amenazas.

Con estos elementos se puede estimar el impacto refiriéndose a lo que podría pasar y el riesgo refiriéndose a lo que probablemente pase. El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

La otra gran área de MARGERIT es la gestión de riesgos, que tiene como propósito la gestión de la seguridad de un sistema de información siendo esta la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

3.4.2.1. Análisis de riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo los siguientes pasos:

- Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué costo supondría su degradación.

- Determinar a qué amenazas están expuestos aquellos activos

- Determinar qué *back-ups* hay dispuestos y cuán eficaces son frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

A continuación se presentan los pasos anteriores, tratándose los pasos primero, segundo, cuarto y quinto, obviando el paso tercero, de forma que las estimaciones de impacto y riesgo sean potenciales, en caso de que no hubiera *back-up*. Una vez obtenido este escenario teórico, se incorporan los *back-ups* del paso tercero, derivando estimaciones realistas de impacto y riesgo.

3.4.2.1.1. Activos

Se denominan activos a los recursos del sistema de información o relacionados con este, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información que maneja el sistema, es decir, los datos. Y alrededor de estos datos se pueden identificar otros activos relevantes:

- Los servicios que se pueden prestar gracias a aquellos datos y los servicios que se necesitan para poder gestionar dichos datos.

- Las aplicaciones informáticas (*software*) que permiten manejar los datos.

- Los equipos informáticos (*hardware*) y que permiten hospedar datos, aplicaciones y servicios.

- Los soportes de información que son dispositivos de almacenamiento de datos.

- Las redes de comunicaciones que permiten intercambiar datos.

- Las instalaciones que acogen equipos informáticos y de comunicaciones.

- Las personas que explotan u operan todos los elementos anteriormente citados.

Aunque en cada caso se adapta a la organización que se analiza, con frecuencia se puede estructurar el conjunto de activos en capas, donde las capas superiores dependen de las inferiores:

- Capa 1: son activos que se precisan para garantizar las siguientes capas:
  - Equipamiento y suministros: energía, climatización y comunicaciones.
  - Personal: de dirección, de operación, de desarrollo, etcétera.
  - Otros: edificios, mobiliario, etcétera.
- Capa 2: el sistema de información propiamente dicho
  - Equipos informáticos *hardware*

- Aplicaciones *software*
- Comunicaciones
- Soportes de información: discos, cintas, etcétera

- Capa 3: la información
  - Datos
  - Metadatos: estructuras, índices, claves de cifra, etcétera

- Capa 4: las funciones de la organización, que justifican la existencia del sistema de información y le dan finalidad.
  - Objetivos y misión
  - Bienes y servicios producidos

- Capa 5: otros activos
  - Credibilidad o buena imagen

3.4.2.1.2. Amenazas

El siguiente paso consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son cosas que ocurren. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a los activos y causar un daño.

Existen accidentes naturales (terremotos, inundaciones, etcétera) y desastres industriales (contaminación, fallos eléctricos, etcétera) ante los cuales el sistema de información es víctima pasiva, pero no por ser pasivo puede ser indefenso. Hay amenazas causadas por las personas, bien errores, bien ataques intencionados.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cantidad. Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

- Degradación: cuán perjudicado resultaría el activo

- Frecuencia: cada cuánto se materializa la amenaza

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera. La degradación se suele caracterizar como una fracción del valor del activo. Cuando las amenazas no son intencionales, probablemente basta conocer la fracción físicamente perjudicada dé un activo para calcular la pérdida proporcional de valor que se pierde. Pero, cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar muchísimo daño de forma selectiva.

La frecuencia pone en perspectiva la degradación, pues una amenaza puede ser de terribles consecuencias pero de muy improbable realización, mientras que otra amenaza puede ser de muy bajas consecuencias, pero tan frecuente como para acabar acumulando un daño considerable.

La frecuencia se modela como una tasa anual de ocurrencia, siendo valores típicos los siguientes:

- 100 muy frecuente a diario
- 10 frecuente mensualmente
- 1 normal una vez al año
- 1/10 poco frecuente cada varios años

3.4.2.1.3. Determinación del impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la ejecución de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema. La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen concretarse en los medios.

3.4.2.1.4. Determinación del riesgo

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

3.4.2.1.5. *Back-ups*

Se definen los *back-ups* como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se ejecutan simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), otras son de seguridad física y, por último, está la política de personal.

Los *back-ups* se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden instar. El *back-up* ideal es 100% eficaz, lo que implica que:

- Es teóricamente idónea
- Esta perfectamente desplegada, configurada y mantenida
- Se emplea siempre
- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados
- Existen controles que avisan de posibles fallos

3.4.2.2. Gestión de riesgos

El análisis de riesgos determina impactos y riesgos. Los impactos recogen daños absolutos, independientemente de que sea más o menos probable que se dé la circunstancia. En cambio el riesgo pondera la probabilidad de que ocurra. El impacto refleja el daño posible, mientras que el riesgo refleja el daño probable.

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial, sin *back-up* alguno y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias. Si el valor residual es igual al valor potencial, los *back-ups* existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer.

Si el valor residual es despreciable, se da por concluido. Esto no quiere decir descuidar la guardia, pero si afrontar el día con cierta confianza. Mientras el valor residual sea más que despreciable, hay una cierta exposición. Es importante entender que un valor residual es sólo un número. Para su correcta interpretación debe venir acompañado de la relación de lo que se debería hacer y no se ha hecho.

La dirección de la organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Cualquier nivel de impacto o riesgo es aceptable si lo conoce y acepta formalmente la alta dirección.

4. ANÁLISIS DE LOS ESTÁNDARES DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

4.1. Estándares

Existen tres estándares que gobiernan la manera de definir la auditoría y los métodos para llevarla a cabo. Estos estándares emitidos son el resultado de los esfuerzos continuos para definir, evaluar, reportar y mejorar el control interno. Estos son:

- COBIT
- SAC
- COSO

COBIT es una estructura que provee una herramienta para los propietarios de los procesos del negocio para llevar a cabo eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos. SAC ofrece asistencia a los auditores internos sobre el control y auditoría de los sistemas y tecnología informática. COSO brinda recomendaciones a la dirección sobre cómo evaluar, reportar y mejorar los sistemas de control.

Como diferentes entidades han desarrollado dichos estándares para encarar las necesidades específicas de sus propias audiencias, pueden existir algunas diferencias. Sin embargo, cada estándar se enfoca en el control interno y cada audiencia.

Una comparación de los estándares revela que cada uno de ellos se construyó sobre la base de las contribuciones de los estándares previos. COBIT incorpora como parte de sus fuentes tanto a COSO como a SAC. Toma su definición de control de COSO y su definición de Objetivos de Control de TI de SAC, COSO utiliza los conceptos de control interno de SAC. En la tabla VII se muestra un cuadro comparativo entre los atributos de estos tres estándares.

Tabla VII. **Comparación de los atributos de control interno**

Atributo	**COBIT**	**SAC**	**COSO**
Audiencia primaria	Dirección, usuarios, auditores de SI.	Auditores Internos	Dirección
CI visto como	Conjunto de procesos incluyendo políticas, procedimientos y prácticas estructuras organizacionales.	Conjunto de procesos, subsistemas y gente.	Procesos
Objetivos organizacionales del CI	Operaciones efectivas y eficientes. Confidencialidad, integridad y disponibilidad de información. Informes financieros confiables. Cumplimiento de las leyes y regulaciones.	Operaciones efectivas y eficientes. Informes financieros confiables. Cumplimiento de las leyes y regulaciones.	Operaciones efectivas y eficientes. Informes financieros confiables. Cumplimiento de las leyes y regulaciones.

Continuación de la tabla VII.

Componentes o dominios	Dominios. Planeamiento y organización. Adquisición e implementación. Entrega y soporte. Monitoreo.	Componentes. Ambiente de control. Manual y automatizado. Procedimientos de control de sistemas.	Componentes. Supervisión. Ambiente de control. Administración de riesgos. Actividades de control. Información y comunicación.
Foco	Tecnología informática	Tecnología informática	Toda la entidad
Efectividad del CI evaluado	Por un período de tiempo	Por un período de tiempo.	En un momento dado
Responsabilidad por el sistema de CI	Dirección	Dirección	Dirección
Tamaño	187 páginas en cuatro documentos.	1 193 páginas en 12 módulos.	353 páginas en cuatro volúmenes.

Fuente: elaboración propia.

La Information Systems Audit and Control Foundation (ISACF) desarrolló los Objetivos de Control para la Información y Tecnología relacionada COBIT para servir como una estructura generalmente aplicable y prácticas de seguridad y control de sistemas de información para el control de la tecnología de la información. Esta estructura COBIT le permite a la gerencia comparar la seguridad y prácticas de control de los ambientes de TI, permite a los usuarios de los servicios de TI asegurarse que existe una adecuada seguridad y control; y permite a los auditores sustanciar sus opiniones sobre el control interno y aconsejar sobre materias de seguridad y control de TI.

La motivación primaria para brindar esta estructura fue posibilitar el desarrollo de una política clara y buenas prácticas para el control de TI a través de toda la industria en todo el mundo.

La fase del proyecto COBIT provee un resumen ejecutivo, un marco para el control de TI, una lista de objetivos de control y un conjunto de guías de auditoría. Los objetivos de control y las guías de auditoría están referenciados a la estructura.

COBIT adaptó su definición de control a partir de COSO refiriéndose a que las políticas, procedimientos, prácticas y estructuras organizacionales están diseñadas para proveer aseguramiento razonable de que se lograrán los objetivos del negocio y que serán prevenidos, detectados y que se corregirán los eventos no deseables.

COBIT adapta su definición de un objetivo de control de TI del SAC refiriéndose a una declaración del resultado deseado o propósito a lograr implementando procedimientos de control en una actividad particular de TI.

COBIT enfatiza el rol e impacto del control de TI en lo relacionado con los procesos del negocio, describiendo los objetivos de control de TI independientes de plataformas y aplicaciones.

COBIT clasifica los recursos de TI como datos, sistemas de aplicación, tecnología, instalaciones y personal. Los datos son definidos en su sentido más amplio e incluyen no sólo números, textos y fechas, sino también objetos tales como gráficos y sonido. Los sistemas de aplicación son comprendidos como la suma de procedimientos manuales y programados.

La tecnología se refiere al *hardware*, Sistemas Operativos, equipos de redes y otros. Instalaciones son los recursos utilizados para albergar y soportar los sistemas de información. Gente comprende las capacidades y habilidades individuales para planear, organizar, adquirir, entregar, apoyar y monitorear los servicios y sistemas de información.

Para satisfacer los objetivos del negocio, la información necesita conformarse a ciertos criterios a los cuales COBIT se refiere como requerimientos del negocio respecto de la información. COBIT combina los principios en tres amplias categorías: calidad, responsabilidad fiduciaria y seguridad.

De estos amplios requerimientos, el informe extrae siete categorías de criterios para evaluar que tan bien están satisfaciendo los recursos de TI los requerimientos de información del negocio. Estos criterios son efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

COBIT clasifica los procesos de TI en cuatro dominios. Estos cuatro dominios son planeamiento y organización, adquisición e implementación, entrega, soporte y monitoreo. El agrupamiento de procesos en dominios es llamado también como dominios de responsabilidad en las estructuras organizacionales y sigue el ciclo gerencial o ciclo de vida aplicable a los procesos de TI en cualquier ambiente de TI.

COBIT presenta una estructura de control para los propietarios de los procesos del negocio. Cada vez más, la dirección está totalmente facultada con responsabilidad y autoridad completa por los procesos del negocio. COBIT incluye definiciones tanto de control interno como de los objetivos de control de TI, cuatro dominios de procesos y 32 declaraciones de control de alto nivel para esos procesos, 302 objetivos de control referenciados a esos 32 procesos y guías de auditoría vinculadas a los objetivos de control.

La estructura COBIT provee declaraciones de control de alto nivel para los procesos particulares de TI. La estructura identifica la necesidad del negocio satisfecha por la declaración de control, identifica los recursos de TI administrados por los procesos, establece los controles habilitados y lista los principales objetivos de control aplicables.

Ahora, el informe COSO define el control interno, describe sus componentes y provee criterios contra los cuales pueden evaluarse los sistemas de control. El informe ofrece una guía para la elaboración de informes públicos sobre control interno y provee materiales que la gerencia, los auditores y otros pueden utilizar para evaluar un sistema de control interno.

Dos objetivos principales del informe son establecer una definición común de control interno que sirve a muchas partes diferentes y provee un estándar contra el cual las organizaciones pueden evaluar sus sistemas de control y determinar como mejorarlos.

El informe COSO define control interno como un proceso, efectuado por la dirección, la gerencia y otro personal de la entidad, diseñado para proveer un aseguramiento razonable en relación al logro de los objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones

- Confiabilidad de los reportes financieros

- Cumplimiento con las leyes y regulaciones aplicables

Aunque el informe define el control interno como un proceso, recomienda evaluar la efectividad del control interno a un momento dado. El sistema de control interno consiste en cinco componentes interrelacionados: ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y supervisión. El ambiente de control provee la base para los otros componentes.

Este estándar abarca factores tales como filosofía y estilo operativo de la gerencia, políticas y prácticas de recursos humanos, la integridad y valores éticos de los empleados, la estructura organizacional y la atención y dirección del directorio. El informe COSO brinda una guía para evaluar cada uno de estos factores.

Por ejemplo, la filosofía gerencial y el estilo operativo pueden ser evaluados examinando la naturaleza de los riesgos del negocio que acepta la gerencia, la frecuencia de su interacción con los subordinados y su actitud hacia los informes financieros.

La evaluación de riesgo que maneja COSO, consiste en la identificación del riesgo y el análisis del riesgo. La identificación del riesgo incluye examinar factores externos tales como los desarrollos tecnológicos, la competencia y los cambios económicos y factores internos tales como calidad del personal, la naturaleza de las actividades de la entidad y las características de procesamiento del sistema de información. El análisis de riesgo involucra estimar la significación del riesgo, evaluar la probabilidad de que ocurra y considerar cómo administrarlo.

Las actividades de control manejadas por COSO, consisten en las políticas y procedimientos que aseguran que los empleados lleven a cabo las directivas de la gerencia. Las actividades de control incluyen revisiones del sistema de control, los controles físicos, la segregación de tareas y los controles de los sistemas de información.

Los controles sobre los sistemas de información incluyen los controles generales y los controles de las aplicaciones. Controles generales son aquellos que cubren el acceso, el desarrollo de *software* y sistemas. Controles de las aplicaciones son aquellos que previenen que ingresen errores en el sistema o detectan y corrigen errores presentes en el sistema. La entidad obtiene información pertinente y la comunica a través de la organización. El sistema de información identifica, captura y reporta información financiera y operativa que es útil para controlar las actividades de la organización.

Dentro de la organización, el personal debe comprender sus roles en el sistema de control interno, tomar seriamente sus responsabilidades por el control interno y, si es necesario, reportar problemas a los altos niveles de gerencia.

La gerencia monitorea el sistema de control revisando la salida generada por las actividades regulares de control y realizando evaluaciones especiales. Las actividades regulares de control incluyen comparar los activos físicos con los datos registrados, seminarios de entrenamiento y exámenes realizados por auditores internos y externos.

Las evaluaciones especiales pueden ser de distinto alcance y frecuencia. Las deficiencias encontradas durante las actividades regulares de control son normalmente reportadas al supervisor a cargo; las deficiencias detectadas durante evaluaciones especiales son normalmente comunicadas a los niveles altos de la organización.

El informe COSO encara las limitaciones de un sistema de control interno y los roles y responsabilidades de las partes que afectan a un sistema. Las limitaciones incluyen el juicio humano defectuoso, falta de comprensión de las instrucciones, errores, atropellos de la gerencia, complicidad y consideraciones de costo *versus* beneficio.

El informe COSO define deficiencias como condiciones dentro de un sistema de control interno que requiere de atención. Las deficiencias deben ser reportadas a la persona responsable por la actividad y a la gerencia que está como mínimo un nivel por encima del individuo responsable. Un sistema de control interno es juzgado efectivo si están presentes y funcionando efectivamente los cinco componentes respecto de las operaciones, los reportes financieros y el cumplimiento.

COBIT, SAC y COSO definen el control interno, describen sus componentes y proveen herramientas de evaluación. SAC y COSO también sugieren formas de reportar los problemas de control interno. Adicionalmente COBIT provee una estructura amplia facilitando el análisis y comunicación de las observaciones de control interno.

4.1.1. Definiciones

Aunque las tres definiciones de control contienen esencialmente los mismos conceptos, el énfasis es algo diferente. COBIT ve el control interno como un proceso que incluye políticas, procedimientos, prácticas y estructuras organizacionales que soportan procesos y objetivos de negocio. SAC enfatiza que el control interno es un sistema, por ejemplo, que el control interno es un conjunto de funciones, subsistemas y gente y sus interrelaciones. COSO resalta el control interno como un proceso, por ejemplo, el control interno debería ser una parte integrante de las actividades del negocio en curso.

El personal es parte del sistema de control interno. COBIT clasifica al personal, definida como habilidad, concientización y productividad del personal para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información, como uno de los recursos primarios administrados por distintos procesos de tecnología informática.

SAC define explícitamente a la gente como una parte integral del sistema de control interno. COSO denota que la gente involucrada con el control interno son miembros de la dirección, la gerencia u otro personal de la entidad. Los documentos acuerdan que la gerencia es la parte responsable por establecer, mantener y monitorear el sistema de control interno.

Los tres documentos acentúan el concepto de aseguramiento razonable en lo que se relaciona con el control interno. El control interno no garantiza que la entidad logrará sus objetivos ni que permanecerá en el negocio. Por lo contrario, el control interno está diseñado para proveer a la dirección con un aseguramiento razonable respecto del logro de los objetivos.

Los estándares también reconocen que hay limitaciones inherentes al control interno y que, por consideraciones de costo/beneficio, no serán implementados todos los controles posibles. Las limitaciones inherentes pueden causar que los controles internos sean menos efectivos que lo planeado.

Al presentar las definiciones de control interno, los estándares asumen que la entidad ha establecido objetivos para sus operaciones. COBIT establece la premisa de que estos objetivos son soportados por procesos de negocio. Estos procesos, a la vez, son soportados por la información provista mediante el uso de recursos de tecnología informática.

Los requerimientos del negocio para esa información sólo son satisfechos mediante medidas adecuadas de control. SAC establece que el logro de los objetivos del negocio debería ser realizado efectivamente y acentúa que los objetivos deberían ser traducidos en metas mensurables.

COSO categoriza los objetivos como operacionales, reportes financieros y cumplimiento. Mientras que SAC y COSO se interesan con objetivos en las tres categorías.

4.1.2. Componentes

SAC describe tres componentes del sistema de control interno. El informe COSO considera cinco componentes. COBIT incorpora los cinco componentes considerados en el informe COSO y los canaliza dentro del entorno del control interno de tecnología informática. El diseño de COBIT salta la brecha entre los modelos de control de negocios tales como COSO y los modelos de control de sistemas de información más altamente técnicos, disponibles en todo el mundo.

4.1.2.1. Ambiente de control

COBIT, SAC y COSO todos incluyen el ambiente de control como un componente y discuten esencialmente los mismos conceptos. Los factores que impactan el ambiente de control incluyen la integridad y valores éticos de la gerencia, la competencia del personal, la filosofía gerencial y el estilo operativo, cómo se asignan la autoridad y responsabilidades y la guía que provee el directorio.

COBIT enlaza las incompatibilidades del ambiente de control en todos los objetivos de control aplicables. Categoriza los procesos dentro de planeamiento y organización, adquisición e implementación, entrega y soporte; y monitoreo. También habla del ambiente de control donde es apropiado. SAC divide el ambiente de control en unas pocas categorías, está más orientado a los sistemas de información e incluye ideas como parte del ambiente de control que los otros dos estándares discuten como parte de otros componentes.

En la mayoría de las áreas, los conceptos de control interno se desarrollaron de SAC a COSO a COBIT. COSO utiliza una mayor cantidad de categorías de conceptos ambientales y en consecuencia define bien al ambiente de control.

4.1.2.2. Información y comunicación

COBIT, SAC y COSO difieren en sus focos y profundidad de tratamiento de los sistemas de información y comunicación. El foco exclusivo de COBIT es el establecimiento de una estructura de referencia para seguridad y control en tecnología informática.

Define un vínculo claro entre los controles de los sistemas de información y los objetivos del negocio. Además, provee objetivos de control validados globalmente para cada proceso de tecnología informática lo cual brinda una guía de control para todas las partes interesadas. COBIT también provee un vehículo para facilitar las comunicaciones entre la gerencia, los usuarios y los auditores en relación a los controles de los sistemas de información.

SAC se enfoca en los sistemas de información automatizados. El documento examina las relaciones entre control interno y *software* de sistemas, sistemas de aplicación y los sistemas departamentales de usuarios finales. El *software* de sistemas provee el Sistema Operativo, telecomunicaciones, administración de datos y otras funciones de utilidad requeridas por los sistemas de aplicación.

Los sistemas de aplicación incluyen los sistemas de negocios, financieros y operativos de la entidad, por ejemplo, recursos humanos, cuentas por cobrar y programación de la producción, respectivamente. Los sistemas departamentales y de usuarios finales sirven a las necesidades de grupos específicos de usuarios. Muchos de los volúmenes del informe SAC proveen guías del control interno necesario en cada una de estas áreas.

COSO discute tanto información como comunicación. En su discusión sobre información, COSO revisa la necesidad de capturar la información pertinente interna y externa, el potencial de sistemas estratégicos e integrados, y la necesidad de calidad en los datos. La discusión sobre comunicación se focaliza en trasmitir asuntos de control interno y recoger información competitiva, económica y legislativa.

4.1.2.3. Actividades de control

COBIT y SAC examinan procedimientos de control relativos al sistema automatizado de información de una entidad, en cambio COSO discute los procedimientos y actividades de control utilizados en toda la entidad. COBIT clasifica los controles en 32 procesos agrupados naturalmente en cuatro dominios aplicables a cualquier ambiente de procesamiento de información. SAC utiliza cinco esquemas de clasificación diferentes para los procedimientos de control del sistema de información.

COSO utiliza sólo un esquema de clasificación para los procedimientos de control del sistema de información. La discusión de COSO sobre las actividades de control enfatiza en quién realiza las actividades y en lo operativo más que en los objetivos de informes financieros. COSO también enfatiza la integración las actividades de control con la evaluación de riesgos.

4.1.2.4. Evaluación de riesgos

COSO identifica la evaluación de riesgos como un componente importante del control interno. COBIT identifica un proceso dentro del ambiente de tecnología informática como evaluando riesgos. Este proceso en particular cae dentro del dominio de planeamiento y organización y tiene seis objetivos específicos de control asociados al mismo.

Aunque la evaluación de riesgos no es un componente explícito del sistema de control interno de SAC, el estándar contiene amplias discusiones sobre riesgo. COBIT considera en profundidad varios componentes de evaluación de riesgos en un ambiente de tecnología informática.

Esto incluye evaluación de riesgos del negocio, el enfoque de evaluación de riesgos, identificación de riesgos, medición de los riesgos, plan de acción sobre riesgos y aceptación de riesgos. Trata directamente con tipos de riesgos de tecnología informática tales como riesgos de tecnología, seguridad, continuidad y regulatorios. Adicionalmente, considera el riesgo tanto desde la perspectiva global como los específicos de sistemas.

Los conceptos de riesgo presentados en SAC y COSO son similares. Además del riesgo de fallar en satisfacer los objetivos de informes financieros, SAC y COSO tratan los riesgos de fallar en el cumplimiento y especialmente, en los objetivos operativos. COSO discute la identificación de los riesgos internos y externos para toda la entidad y para las actividades individuales. COSO considera también el análisis del riesgo por la gerencia estimando la significación del riesgo, evaluando su probabilidad de ocurrencia y considerando como administrarlo.

SAC examina los riesgos para el sistema automatizado de información y provee un análisis detallado de los riesgos del sistema de información y explora cómo podría mitigarse cada uno de estos riesgos. SAC y COSO enfatizan en consideraciones de costo/beneficio, la necesidad de interrelacionar los objetivos de la entidad y los controles, la naturaleza de la identificación y evaluación de riesgos y la habilidad gerencial para ajustar el sistema de control interno de la entidad.

4.1.2.5. Monitoreo

En contraste con COBIT y COSO, SAC no incluye explícitamente el monitoreo como un componente del sistema de control interno. Estos estándares asignan a la gerencia la responsabilidad de asegurar que los controles continúen operando apropiadamente. COBIT considera la responsabilidad gerencial de monitorear todos los procesos de tecnología informática y la necesidad de obtener un aseguramiento independiente sobre los controles. Clasifica monitoreo como un dominio en línea con el ciclo gerencial.

SAC reconoce las responsabilidades de los auditores internos para seleccionar áreas de tecnología informática en las cuales una revisión independiente puede producir mayores beneficios y para verificar controles para obtener evidencia del cumplimiento y eficacia vigentes. Como los controles internos deberían evolucionar y evolucionan con el tiempo, COSO reconoce la necesidad de que la gerencia monitoree todo el sistema de control interno de las actividades en marcha incorporadas en el sistema de control en sí mismo y mediante evaluaciones especiales dirigidas a áreas o actividades específicas.

Aunque SAC y COSO comparten la misma perspectiva interna, COSO discute el monitoreo de actividades en términos amplios y SAC discute actividades específicas de monitoreo que deberían ser realizadas por o dentro de los sistemas automatizados de información de la entidad. COBIT en forma parecida, pero de manera más profunda, define los requerimientos y responsabilidades específicas de monitoreo dentro de la función de tecnología informática.

4.1.3. Reportar problemas de control interno

COBIT brinda la definición de controles y objetivos de control para procesos específicos de tecnología informática. En forma similar a COSO, los informes de COBIT sobre problemas de control interno se asume que están disponibles para el propietario del proceso de negocio responsable desde distintas fuentes. Estas pueden ir desde la autoevaluación del control hasta revisiones de auditorías externas, todas realizadas utilizando la estructura COBIT.

SAC asigna a los auditores internos la responsabilidad de evaluar si hay vigentes controles apropiados y si estos controles están funcionando como fueron diseñados. Los auditores internos envían los resultados de sus auditorías financieras, operativas y de los sistemas de información a la gerencia y al comité de auditoría. Ellos deberían articular los costos y beneficios de los cambios propuestos para remediar las deficiencias en el sistema de control interno.

COSO discute cómo recolecta y reparte la gerencia la información sobre las deficiencias de control interno. La gerencia puede tomar conocimiento de las deficiencias a través de los reportes generados por el sistema de control interno en sí mismo, las evaluaciones realizadas por la gerencia o los auditores internos o comunicaciones de terceras partes tales como clientes, reguladores, o auditores externos. La gerencia quiere información relacionada con cualquier deficiencia que podría afectar la habilidad de la entidad para lograr sus objetivos operativos, de información financiera o de cumplimiento.

COSO recomienda que el personal de la entidad reporte las deficiencias a los supervisores inmediatos y a la gerencia ubicada como mínimo un nivel por encima de la persona directamente responsable. Deberían existir canales de comunicación separados para reportar información sensible.

4.1.4. Período de tiempo *versus* un momento dado

COBIT es una estructura modelo. Soporta evaluaciones a un momento dado o durante períodos de tiempo, dependiendo de la preferencia del revisor. Aunque SAC no establece explícitamente si la efectividad interna debería evaluarse a un momento dado o durante un período de tiempo, parece favorecer más las evaluaciones por períodos de tiempo.

Por ejemplo, SAC habla de asegurar la confiabilidad de los datos financieros y operativos, describe el uso de módulos de auditoría incorporados para monitorear y analizar transacciones en forma continuada y recomienda emplear controles de cambios para asegurar la estabilidad de las aplicaciones y el *software* de los sistemas.

Aunque COSO acentúa al control interno como un proceso, el informe establece que la efectividad del control interno es un estado o condición del proceso a un momento dado. Si las deficiencias de control interno han sido corregidas a la fecha de emitir un informe, COSO aprueba los informes gerenciales dirigidos a terceros que describen que el control interno es efectivo.

4.1.5. Herramientas

COBIT provee explícitamente una guía para los 32 procesos que define. Esta guía toma la forma de más de 302 objetivos de control. Luego provee ayudas de navegación que todos los usuarios, dependiendo de su perspectiva particular, implementan para organizar y categorizar los objetivos de control de acuerdo con las vistas de control de los procesos de TI, los criterios de información o los recursos de TI.

SAC provee una guía detallada sobre los controles necesarios en el desarrollo, implementación y operación de sistemas automatizados de información a través de la mayoría de sus 12 módulos. Muchos módulos contienen secciones particulares sobre los riesgos y controles asociados a los tópicos discutidos en ese módulo.

El informe COSO brinda al lector herramientas que se pueden utilizar para evaluar el sistema de control interno. Un volumen entero está dedicado a las formas sugeridas para utilizar en el examen de los controles y a muestras de formularios completados.

5. BUENAS PRÁCTICAS DE AUDITORÍA DE SISTEMAS APLICADAS EN GUATEMALA

5.1. Importancia del uso de buenas prácticas

Las buenas o mejores prácticas corresponden a un conjunto de técnicas, métodos, procesos o actividades, que son consideradas como las más eficaces e innovadoras para resolver problemas o promover el desarrollo en diferentes campos. Se les reconoce como exitosas en el tiempo y entorno de aplicación y se espera que lo continúen siendo en ambientes similares.

Provienen de fuentes distintas, no son producto de un único origen y es responsabilidad utilizarlas de forma consistente. Pueden aplicar a cada empresa en particular y también son importantes cuando se implementan en empresas relacionadas entre sí. Pueden agruparse en función de los vínculos u obligaciones que adquiere la empresa, de la siguiente manera:

- Las que se relacionan con los clientes internos y externos
- Las que se asocian con su propio desarrollo
- Las que se gestionan en grupos de empresas, la forma de redes o sistemas.

Las mejores prácticas de auditoría proporcionan a las empresas métodos utilizados para estandarizar procesos y administrar de una mejor manera y asegurar que el uso de los recursos informáticos cumplen con las políticas y normas para el resguardo de la información y funcionamiento de la empresa.

5.1.1. Esquema de auditoría

El esquema busca identificar las necesidades de la organización que deben ser definidas respecto de la auditoría de sistemas, así como las debilidades propias, con el fin de determinar el objetivo a seguir, incorporando conceptos de calidad total aplicada a la auditoría sobre la base de la mejora continua, con el concepto de medición y evaluación de resultados.

Al integrar un proceso de comunicación, se busca establecer un vínculo interno que se apegue a informar lo actuado, lo planeado y las mejoras obtenidas, apoyado en la tecnología, se utilizan recursos informáticos al proceso de auditorías con el fin de contribuir a la eficacia, eficiencia y oportunidad en los resultados de las revisiones.

Bajo la inclusión de interrelaciones, se mantienen estrechas vinculaciones profesionales con otras gerencias de auditoría con el fin de intercambiar estrategias, criterios y resultados, promoviendo ser agentes de cambio, proporcionando las bases para posicionar a la auditoría como el iniciador del rumbo a seguir en la organización con el fin de implementar autoevaluaciones del control, junto con un cambio funcional proyectando a los auditores como facilitadores de la autoevaluación del control.

5.1.2. Aseguramiento de la información

El aseguramiento de la información es la base sobre la que se elabora la toma de decisiones de una organización. Sin dicho aseguramiento, las empresas no tendrían certidumbre de que la información sobre la que sustentan sus decisiones es confiable, segura y está disponible cuando se le necesita.

Hace referencia a la utilización de información y de diferentes actividades operativas, con el fin de proteger la información, los sistemas de información y las redes de forma que se preserve la disponibilidad, integridad, confidencialidad, autenticación y el no repudio, ante el riesgo de impacto de amenazas locales o remotas a través de comunicaciones e Internet.

Una tarea de aseguramiento puede darse a cualquier nivel, por lo se consideran las más importantes como el aseguramiento de los datos, los procesos, el comportamiento según las normas o mejores prácticas y el sistema de gestión.

5.1.3. Aseguramiento de la calidad de la información

La administración del aseguramiento de la calidad verifica que los sistemas de información logren las metas de calidad y que el desarrollo, implementación, operación y mantenimiento de los sistemas informáticos, cumplan con un conjunto de normas de calidad.

Cada vez los requerimientos de información son más exigentes en términos de la calidad del *software* que se emplean para realizar las tareas, por ello actualmente el aseguramiento de la calidad ha tomado mayor importancia en muchas organizaciones.

Las organizaciones se están comprometiendo en proyectos de sistemas de información que tienen requerimientos de calidad más estrictos y se preocupan cada vez más sobre sus responsabilidades legales al producir y vender *software* defectuoso.

Debido a esto, mejorar la calidad del *software* es parte de una tendencia universal entre las organizaciones proveedoras para mejorar la calidad de los productos y los servicios que ofrecen, agregando valor a los controles de producción, implementación, operación y mantenimiento de los recursos informáticos.

5.1.4. Prácticas de auditoría informática

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos. Los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Hace referencia a un proceso llevado a cabo por profesionales especialmente capacitados para el efecto y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos y cumple con las leyes y regulaciones establecidas.

Permiten detectar de forma sistemática el uso de los recursos y los flujos de información dentro de una organización y determinar qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costes, valor y barreras, que obstaculizan flujos de información eficientes.

El análisis de la eficiencia de los sistemas informáticos, la verificación del cumplimiento las normas y la revisión de la eficaz gestión de los recursos informáticos, son algunos de los objetivos de la auditoría informática, que contribuyen a la mejora de características en la empresa como el desempeño, fiabilidad, eficacia, rentabilidad, seguridad y privacidad.

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO e ITIL, generalmente desarrollados en el gobierno corporativo, administración del ciclo de vida de los sistemas, servicios de entrega y soporte, protección y seguridad, planes de continuidad y recuperación de desastres. Actualmente, la certificación de ISACA para ser CISA Certified Information Systems Auditor es una de las más reconocidas y avaladas por los estándares internacionales.

5.1.5. Generación de valor

Uno de los principales objetivos que constituyen las buenas prácticas de la auditoría informática es el análisis y control de la eficiencia de los sistemas informáticos, verificando el cumplimiento de la normativa general de la empresa en este ámbito y la revisión de la eficaz gestión de los recursos materiales y humanos informáticos.

Para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido, comprendiendo que las empresas utilizan la informática para gestionar sus modelos de negocio de forma rápida y eficiente con el fin de obtener beneficios económicos y de costes.

Por eso, al igual que las demás unidades de negocio de las empresas, 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.

En el contexto en el que se desarrollan las auditorías de sistemas, se establece la importancia de la generación de valor en todo el proceso que se lleva a cabo, sin comprometer la integridad de la auditoría. Agregar valor hace referencia a dar más por encima de los resultados esperados.

Algunas organizaciones han utilizado las mejores prácticas de auditoría de sistemas para desarrollar sistemas de gestión de la calidad de la información que están integrados en su manera de hacer negocios y son útiles en ayudarlos a lograr sus objetivos estratégicos de negocio, agregando valor a la organización.

Por el contrario otras organizaciones simplemente han creado una serie de procedimientos y registros burocráticos que no reflejan la realidad de la manera como la organización trabaja realmente y simplemente agregan costo, sin ser útiles. En otras palabras, estos no agregan valor.

Un enfoque de auditoría que no agrega valor podría responder a la siguiente pregunta: ¿Qué procedimientos se tendrían que escribir para obtener llevar a cabo una auditoría de sistemas? Por el contrario, un enfoque que agrega valor tiene la respuesta a la siguiente pregunta: ¿Cómo se podría usar el proceso de auditoría de sistemas para que apoye a la mejora continua del modelo de negocio de las empresas?

El enfoque de agregar valor debiera ser una función del nivel de madurez de la cultura de calidad de la organización y de qué tanto el proceso de auditoría de sistemas excede los requisitos de las mejores prácticas aplicadas. La cultura de calidad incluye el grado de conciencia, compromiso y actitud colectiva así como el desempeño de la organización con respecto a la calidad.

5.2. Gestión de TI

La gestión de TI es una disciplina basada en procesos, enfocada en alinear los servicios de TI proporcionados con las necesidades de las empresas, poniendo énfasis en los beneficios que puede percibir el cliente final.

5.2.1. Gobierno de TI

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, integra e institucionaliza buenas o mejores prácticas de planificación y organización, adquisición e implementación, entrega de servicios y soporte, y monitoriza el rendimiento de TI para asegurar que la información de la empresa y las tecnologías relacionadas soportan sus objetivos del negocio.

Conduce a la empresa a tomar total ventaja de su información logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva, siendo una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar sus objetivos y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos.

Cuando TI se gestiona como un negocio dentro del negocio, el concepto de gobierno es también aplicable a la gestión de TI. En muchas organizaciones, TI es fundamental para mantener y hacer que crezca el negocio.

Como consecuencia, la gerencia necesita entender la importancia estratégica de TI y debería tener en su agenda el gobierno de TI. El principal objetivo del gobierno de TI es entender las cuestiones y la importancia estratégica de TI para permitir a la organización que mantenga sus operaciones e implemente las estrategias necesarias para sus proyectos y actividades futuras.

El núcleo de TI consta de dos responsabilidades principales, la entrega de valor al negocio y mitigar los riesgos relacionados con TI. La gerencia de la organización necesita ampliar sus responsabilidades de gobierno a TI y proveer estructuras y procesos que aseguren que las Tecnologías de Información son capaces de soportar los objetivos y estrategias de la organización.

5.2.1.1. Gobierno de la organización y gobierno de TI

El gobierno efectivo de la empresa enfoca el conocimiento y la experiencia en forma individual y grupal, donde puede ser más productivo, monitorizado y medido el rendimiento 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.

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 TI. 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.

Para asegurar que la Gerencia alcance los objetivos de negocio, esta debe dirigir y administrar las actividades de TI para alcanzar un balance efectivo entre la gestión de riesgos y los beneficios encontrados. Para cumplir esto, la Gerencia necesita identificar las actividades más importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando lo bien que se están desarrollando los procesos de TI.

Una necesidad básica para toda organización es entender la situación de sus propios sistemas de TI y decidir qué seguridad y control se les debe suministrar. Obtener una visión objetiva del propio nivel de una organización no es fácil para saber qué se debe medir y de qué manera hacerlo.

Además de la necesidad de medir dónde se encuentra una organización, está la importancia de la constante mejora en las áreas de seguridad y control de TI y la necesidad de un conjunto de herramientas de administración para monitorizar esta mejora.

5.2.1.2. COBIT y gobierno de TI

Las organizaciones deben cumplir con requerimientos de calidad, fiduciarios y de seguridad, tanto para su información, como para sus activos. La gerencia deberá además optimizar el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos.

Los Objetivos de Control para la Información y las Tecnologías Relacionadas (COBIT), ayudan a satisfacer las múltiples necesidades de la administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. Provee buenas prácticas y presenta actividades en una estructura manejable y lógica.

La gerencia debe asegurar que los sistemas de control interno o el marco referencial están funcionando y soportan los procesos del negocio y debe ser consciente de cómo 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 gerencia. La gerencia, 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.

5.2.2. Servicios TI

La información es probablemente la fuente principal de negocio y ese negocio a su vez genera enormes cantidades de información, siendo su correcta gestión de importancia estratégica. Los objetivos de una buena gestión de servicios TI incluye proporcionar una adecuada gestión de la calidad, aumentar la eficiencia, alinear los procesos de negocio y la infraestructura TI, reducir los riesgos asociados a los servicios TI y generar negocio.

ITIL nace como un código de buenas prácticas dirigidas a alcanzar esas metas mediante un enfoque sistemático del servicio TI centrado en los procesos y procedimientos y el establecimiento de estrategias para la gestión operativa de la infraestructura TI.

5.2.2.1. ITIL

ITIL como metodología propone el establecimiento de estándares que ayuden en el control, operación y administración de los recursos, ya sean propios o de los clientes. Plantea hacer una revisión y reestructuración de los procesos existentes en caso de que estos lo necesite, por ejemplo, si el nivel de eficiencia es bajo o que haya una forma más eficiente de hacer las cosas, lo que lleva a una mejora constante.

Para cada actividad que se realice se debe hacer la documentación pertinente, ya que esta puede ser de gran utilidad para otros miembros del área, además de que quedan asentados todos los movimientos realizados, permitiendo que toda la gente esté al tanto de los cambios y no se tome a nadie por sorpresa.

La prestación de servicios muchas veces no sería posible sin la gestión de infraestructura, así mismo, las perspectivas del negocio no se darían sin la prestación de servicio y los servicios no serían posibles sin un soporte al servicio.

El punto de interacción que se da entre estos segmentos del negocio es la búsqueda de soluciones, donde lo que se busca es que las perspectivas del negocio estén soportadas con base en la prestación de servicios; la prestación de servicios requiere que se le dé un soporte al servicio para que esté siempre disponible, la disponibilidad se logra mediante una gestión de la infraestructura.

ITIL postula que el servicio de soporte, la administración y la operación se realiza a través de cinco procesos, manejo de incidentes, manejo de problemas, manejo de configuraciones, manejo de cambios y manejo de entregas.

5.2.2.1.1. Manejo de incidentes

Su objetivo primordial es reestablecer el servicio lo más rápido posible para evitar que el cliente se vea afectado, esto se hace con la finalidad de que se minimicen los efectos de la operación. El proveedor del servicio debe encargarse de que el cliente no perciba todas aquellas pequeñas o grandes fallas que llegue a presentar el sistema.

Para este proceso se tiene un diagrama que en cada una de sus fases maneja cuatro pasos básicos que son: propiedad, monitoreo, manejo de secuencias y comunicación.

5.2.2.1.2. Manejo de problemas

El objetivo de este proceso es prevenir y reducir al máximo los incidentes, y esto lleva a una reducción en el nivel de incidencia. Por otro lado ayuda a proporcionar soluciones rápidas y efectivas para asegurar el uso estructurado de recursos.

En este proceso lo que se busca es que se pueda tener pleno control del problema, esto se logra dándole un seguimiento y un monitoreo al problema. El esquema de este proceso es muy particular, ya que se maneja en dos fases: la primera está relacionada con lo que es el control del problema y la segunda es con el control del error.

5.2.2.1.3. Manejo de configuraciones

Su objetivo es proveer con información real y actualizada de lo que se tiene configurado e instalado en cada sistema del cliente. Este proceso es de los más complejos, ya que se mueve bajo cuatro vértices que son: administración de cambios, administración de liberaciones, administración de configuraciones y la administración de procesos diversos.

El nivel de complejidad de este modelo es alto, ya que influyen muchas variables y muchas de ellas son dinámicas, entonces al cambiar una o varias de ellas se afecta el sistema en general, lo que hace que sea muy difícil de manipular. Aunque es lo más parecido a la realidad, porque el entorno es dinámico y las decisiones de unos afectan a otros.

5.2.2.1.4. Control de cambios

El objetivo de este proceso es reducir los riesgos tanto técnicos, económicos y de tiempo al momento de la realización de los cambios.

Al tener un registro y clasificación del cambio que se tiene que hacer, se pasa a la fase de monitoreo y planeación, si el rendimiento es satisfactorio se da la aprobación del cambio y en caso de que el rendimiento sea malo se pasa a la fase de reingeniería hasta que el proceso funcione adecuadamente.

Ya que se aprueban los cambio, se construyen prototipos o modelos en los que se van a hacer las pruebas, se hacen las pruebas pertinentes para ver las capacidades del sistema, ya que el proceso está probado se da la autorización e implementación; ya implementado se ve que no se hayan tenido desviaciones y se ajusta a las necesidades actuales que también se le considera como revisión postimplementación.

5.2.2.1.5. Manejo de entregas

Su objetivo es planear y controlar exitosamente la instalación de *software* y *hardware* bajo tres ambientes: ambiente de desarrollo, ambiente de pruebas controladas y ambiente real. Este proceso tiene un diagrama que marca la transición que se da de acuerdo con los ambientes por los que se va dando la evolución del proyecto.

En lo que respecta al ambiente de desarrollo se tiene que hacer la liberación de las políticas, la liberación de la planeación, el diseño lógico de la infraestructura que se va a implementar y la adquisición de *software* y *hardware* están entre los ambientes de desarrollo y de pruebas controladas; ya que se requiere que ambos hagan pruebas sobre ellos.

En el ambiente de pruebas controladas se hace la construcción y liberación de las configuraciones, se hacen las pruebas para establecer los acuerdos de aceptación; se da la aceptación total de versiones y de modelos, se arranca la planeación y finalmente las pruebas y comunicaciones; y en lo que es el ambiente real se da la distribución e instalación.

En la etapa del ambiente real es la que se ve de forma más concreta, ya que muchas veces se tiene idea de todo lo que pasa hasta antes de la instalación.

En el proceso de entrega del servicio es el punto en el que el usuario hace uso del servicio y no sabe que detrás del servicio que está recibiendo hay un sin fin de actividades y de decisiones que se tuvieron que tomar para llegar a este punto.

5.2.3. Planes de continuidad y recuperación de desastres

Teniendo en cuenta la explosión de datos que están experimentando las empresas y la ciega confianza que ponen en sus sistemas de TI a la hora de generar ingresos, cualquier tipo de interrupción implica repercusiones graves, tanto materiales como intangibles.

Los sistemas de tecnología de la información que gestionan el abastecimiento de información empresarial aportan un valor extraordinario pero implican también una vulnerabilidad: si se produce una interrupción en el acceso a los datos cruciales, la empresa sufrirá las consecuencias.

Un fallo en los sistemas de TI puede acarrear, como mínimo, elevados costes por la pérdida de ingresos, la reducción de la productividad y problemas jurídicos. Y, en un caso extremo, una interrupción duradera del servicio puede poner en peligro la propia existencia de la empresa.

Las situaciones que podrían paralizar la estructura informática de una empresa pueden ser muy variadas, ya sea como consecuencia de un fallo en la red de alimentación, un atentado terrorista, una inundación o cualquier otra catástrofe natural, las empresas de todo el mundo cuentan con ejemplos muy recientes que confirman la importancia de una planificación ante desastres. Se debe tener presente la probabilidad de un fallo total de los sistemas de TI en un futuro.

La anticipación de estos sucesos y la planificación de los procesos necesarios para contrarrestar su impacto es hoy en día un requisito imprescindible para el éxito de una empresa.

La preparación de una estrategia de cara a lo inesperado es de lo que se ocupa la planificación de la continuidad de los negocios (Business Continuity Planning por sus siglas en inglés BCP). Una de las subáreas de BCP comprende las medidas preventivas adoptadas por un grupo de TI para garantizar el acceso permanente a los recursos de información, lo que se denomina planificación de recuperación de desastres (Disaster Recovery Planning por sus siglas en inglés DRP).

En todo caso, tanto para los analistas de aplicaciones como para el personal comercial involucrado en el proceso, es esencial entender el lenguaje utilizado para describir el DRP.

Las propuestas para la protección de los sistemas críticos para el negocio están a menudo salpicadas de expresiones enrevesadas y extravagantes, por lo que la valoración de un concepto concreto de DRP resultará bastante difícil sin unas nociones generales del lenguaje utilizado.

5.2.3.1. BCP

El procedimiento completo que emplea una empresa para garantizar que los procesos empresariales esenciales estén en condiciones de seguir funcionando en caso de surgir un desastre se denomina planificación de la continuidad de los negocios (BCP).

Se encarga de definir todas las instalaciones (oficinas, bodegas y establecimientos de venta al por menor) que deben utilizarse cuando dejan de estar accesibles los emplazamientos comerciales normales, directrices para los departamentos que especifican cómo mantener las operaciones bajo circunstancias anormales y muchos otros aspectos.

5.2.3.2. DRP

La planificación de la recuperación de desastres (DRP) constituye un subconjunto de BCP y se centra exclusivamente en la recuperación de los sistemas de TI.

Cada aplicación empresarial debe ser catalogada, sus exigencias en materia de recuperación, evaluadas y documentadas y la importancia que la aplicación tiene para la empresa debe ser cuantificada de modo que el personal de TI pueda sentar prioridades en el proceso de recuperación.

5.2.3.3. Análisis del impacto empresarial

Un análisis del impacto empresarial (Business Impact Analysis, BIA) cuantifica las consecuencias de una interrupción del servicio en cada uno de los sistemas empresariales. El BIA determina el efecto que tendrá la pérdida de un sistema de TI específico en la empresa. Por ejemplo, un fallo que interrumpa el sistema de acreedores comerciales puede repercutir gravemente en el flujo de efectivo, la fidelidad de la clientela y el nivel de solvencia crediticia de la empresa.

En el marco del BIA es necesario llevar a cabo un análisis de riesgos para determinar las posibilidades de que se produzca una interrupción de las aplicaciones empresariales. La probabilidad de un suceso se equipará con el alcance de las repercusiones que podría causar dicho suceso. Los resultados obtenidos del BIA permiten al departamento de TI definir las estrategias oportunas para interceptar el riesgo en caso de presentarse una incidencia.

5.2.3.4. Tolerancia a desastres

Conscientes de la importancia de DRP, los diseñadores de aplicaciones están empezando a integrar funciones para la preparación ante desastres en sus sistemas empresariales.

La tolerancia a desastres es un término utilizado para la designación de un sistema con una determinada capacidad para resistir un fallo grave. Existen varias tecnologías que facilitan la tolerancia a desastres, como redundancia de *hardware*, duplicación de datos, granja de servidores y centros de datos remotos.

5.2.3.5. Alta disponibilidad

Los sistemas de mayor tolerancia a desastres se distinguen como sistemas de alta disponibilidad (HA). Estas configuraciones están diseñadas de forma que se eliminan el tiempo de interrupción de las aplicaciones mediante *hardware* redundante y componentes de red, así como con *software* especial para aplicaciones y Sistemas Operativos. Los sistemas HA son capaces de circunvalar los fallos en la infraestructura informática directamente y sin alterar el acceso de los usuarios a los datos.

La estabilidad de un sistema HA se mide, con frecuencia, a través de terminología adoptada del sector de las telecomunicaciones. Una configuración que ofrece una disponibilidad del 99,999%, denominada también *five-nines*, por ejemplo, no sobrepasará los cinco minutos de interrupción al año.

5.2.3.6. RPO y RTO

El BIA arroja dos parámetros básicos que definen la capacidad de un sistema empresarial para tolerar la pérdida de datos e interrupciones. El Recovery Point Objective (RPO) expresa la cantidad de datos que una aplicación puede llegar a perder antes de que ello suponga repercusiones negativas para la empresa.

El Recovery Time Objective (RTO) indica cuánto tiempo puede emplear el personal de TI para volver a poner la aplicación en línea después de ocurrir un desastre. La unidad de medición, tanto en el RPO como en el RTO, es el tiempo, con valores que abarcan desde segundos hasta días o semanas.

Cuanto más se aproximen los valores RPO y RTO de una aplicación a cero, mayor será la dependencia de la organización del proceso en particular y, por consiguiente, mayor prioridad tendrá a la hora de recuperar los sistemas en caso de desastre.

5.2.3.7. Estrategias de recuperación de desastres

Las estrategias aplicadas para la protección de datos contra la pérdida como consecuencia de un desastre deben reflejar las prioridades de la empresa. Gastar un millón de dólares en asegurar una recuperación rápida de un servidor de archivos o de impresión puede ser excesivo, pero la inversión de esta misma cantidad de dinero para salvaguardar una aplicación crítica que genera ingresos puede justificarse.

El RPO y el RTO proporcionan a los administradores de TI la información necesaria para identificar la estrategia idónea para una aplicación en concreto. Estos dos parámetros del DRP pueden resultar también útiles a la hora de verificar el resultado de una estrategia elegida en el marco de un ensayo de DR.

Las redes de alta velocidad hacen hoy posible la conservación de copias de los datos de producción en emplazamientos remotos, sin que para ello deba recurrirse a la recuperación basada en cinta y sus impredecibles consecuencias.

La disponibilidad generalizada y los costes relativamente bajos de las redes de ancho de banda extenso han permitido que la duplicación de datos suplante a las cintas magnéticas tradicionales, convirtiéndose en la clave de una recuperación de desastres eficaz.

5.3. Administración del riesgo tecnológico

La gestión del riesgo tecnológico se ocupa del control y la seguridad de la infraestructura tecnológica en general, incluyendo servicios abarcan la seguridad de la información, servicios de supervisión de la seguridad, servicios de planificación de la continuidad de los negocios y comercio electrónico.

5.3.1. Asociaciones de auditoría informática en Guatemala

En Guatemala existen diversas asociaciones acerca de la auditoría de sistemas, por ejemplo, el capítulo ISACA Guatemala y la IIA, que se encargan de promover las mejores prácticas de la auditoría informática.

5.3.1.1. ISACA

El Capítulo ISACA Guatemala está constituido por un equipo de profesionales enfocados en el desarrollo de las TI en Guatemala. Su objetivo principal es el de promover la educación, ayudando a expandir el conocimiento y habilidades de sus integrantes en los campos relacionados con la auditoría, seguridad, control y gestión de sistemas de información.

Para lograr estos objetivos entre otras estrategias se tiene la de comunicar a las gerencias, auditores, universidades y profesionales de sistemas de información acerca de la importancia de establecer sistemas eficientes de control, auditoría y seguridad tecnológica así como llevar a cabo actividades que coadyuven a compartir conocimientos y crear comunidad entre sus miembros.

La Asociación de Auditoría y Control de Sistemas de Información (ISACA), es una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.

Los miembros de ISACA se caracterizan por su diversidad ya que están presentes en más de 100 países y cubren una variedad de puestos profesionales relacionados con TI, como son los Auditores de SI, Consultores, Educadores, Profesionales de Seguridad de SI, Reguladores, Directores Ejecutivos de Información y Auditores Internos, por mencionar sólo algunos.

En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información.

ISACA organiza una serie de conferencias internacionales que se concentran en tópicos técnicos y administrativos pertinentes a las profesiones de gobernación de TI y aseguración, control, seguridad de SI. Juntos, ISACA y su *IT Governance Institute*, asociado lideran la comunidad de control de tecnología de la información y sirven a sus practicantes brindando los elementos que necesitan los profesionales de TI en un entorno mundial en cambio permanente.

Las empresas públicas y privadas están valorando cada día más la creciente importancia que representa mantener sistemas informáticos seguros, confiables y confidenciales, que eviten o prevengan la ocurrencia de errores u operaciones ilegales a partir de debilidades en los sistemas de control.

5.3.1.1.1. Certified Information Security Auditor

ISACA provee una Certificación en Auditor en Sistemas de Información (CISA), por medio de un examen anual que realiza el Instituto a los candidatos, el cual cubre el conocimiento de actividades requeridas para la función de Auditoría en TI, para lo cual presenta un Manual de Información Técnica para la preparación de los candidatos.

La certificación de CISA (Certified Information Systems Auditor) es otorgada por la ISACA y es considerada en la actualidad como un reconocimiento de que se cuenta con los conocimientos teóricos y prácticos necesarios para desempeñarse como Auditor de Sistemas siguiendo los estándares y directrices definidos para una mejor preparación.

La designación de CISA, se considera hoy en día, una ventaja competitiva y resulta de beneficio no sólo para las organizaciones que deben cumplir con requerimientos de certificación profesional de sus colaboradores, sino para las personas que buscan un desarrollo profesional y la obtención de certificaciones que ofrecen oportunidades a nivel internacional.

5.3.1.1.2. Certified Information Security Manager

También ISACA provee la Certificación para la Administración de la Seguridad de la Información del cual intenta garantizar que existan administradores de seguridad de TI que tengan los conocimientos necesarios para reducir el riesgo y proteger a la organización.

La certificación CISM está diseñada para dar la certeza de que los individuos certificados tengan los conocimientos para ofrecer una eficaz administración y consultoría de seguridad.

Está orientada a profesionales que administran la seguridad de la información en una organización y tienen el conocimiento y la experiencia para montar, implementar y dirigir una estructura de seguridad para administrar el riesgo con eficacia y tienen la responsabilidad de entender la relación entre las necesidades comerciales y la seguridad de TI.

Para obtener esta certificación, los profesionales deben aprobar el examen, adherirse a un código ético y presentar pruebas verificadas de que tienen una experiencia laboral de cinco años en seguridad de la información.

Los principales objetivos de esta certificación incluye desarrollar modelos de riesgos que midan mejor los riesgos de seguridad y los potenciales impactos sobre el negocio, aumentar la calidad de la gestión ejecutiva de las nuevas amenazas y las ya existentes, a través de la convergencia entre la organización y las medidas de seguridad, impulsar la unificación del enlace entre la seguridad de las organizaciones y los organismos gubernamentales y legislativos, informándoles de las mejores prácticas en seguridad, continuar definiendo la cualificación, certificación y formación de los Directores de Seguridad y otros puestos.

5.3.1.2. Institute of Internal Auditors

El Institute of Internal Auditors (IIA) es una organización profesional con sede en Estados Unidos, que anualmente organiza su Conferencia Internacional, la que habitualmente congrega a más de un millar de auditores de todos los continentes. El IIA es reconocido mundialmente como una autoridad, pues es el principal educador y el líder en la certificación, la investigación y la guía tecnológica en la profesión de la auditoría interna.

El desarrollo de los Estándares de la Práctica Profesional de Auditoría Interna, así como las Certificaciones de Auditor Interno (CIA), de Autoevaluación de Control (CCSA) y de Auditor Interno Gubernamental (CGAP) y su participación en el diseño del Enfoque COSO son sólo algunos de los hitos que han transformado al IIA en la entidad internacional señera en la profesión.

Establecen el IIA como el recurso de conocimiento primario sobre las mejores prácticas y publicaciones (cuestiones) que afectan la profesión interna de auditoría. Encuentran las necesidades de desarrollo de profesional que se desarrollan de médicos internos de auditoría.

Con el apoyo del Instituto Global, tiene a disposición de los asociados un portal del Instituto para el Desarrollo de Auditores Internos-IDEAS Guatemala. La visión es propiciar un mejor intercambio de comunicación apoyados en los recursos y facilidades que hoy día proporciona la tecnología.

A través de IIA Guatemala los asociados pueden consultar artículos de interés que permiten estar al día con los cambios que la profesión de la auditoría informática interna está experimentando a nivel mundial, manteniendo comunicación constante con los capítulos del IIA en otros países de Latinoamérica y España, los cuales preparan documentos de alto nivel técnico.

5.3.1.2.1. Certified Internal Auditor

El IIA cuenta con su propia Certificación de Auditores Internos CIA, la cual se da tanto a proveedores de estos servicios. Contar con profesionales certificados en auditoría interna, para la organización significa contar con un valioso recurso para la dirección y el consejo de administración, que ayuda a garantizar el avance en la dirección correcta para el logro de sus metas y objetivos.

La certificación como auditor interno la otorga el Institute of Internal Auditors que es una asociación internacional de profesionales especialistas en auditoría interna, administración de riesgos, gobierno corporativo, control interno, auditoría a tecnología de información, educación y seguridad.

La Certificación CIA (Certified Internal Auditor) tiene un reconocimiento mundial que demuestra la capacidad profesional, el dominio de los estándares y de las normas internacionales de la práctica de auditoría interna, el manejo de los principios y controles de la tecnología de información y las estrategias emergentes para mejorar a la organización y a su gobierno corporativo.

Para obtener la certificación CIA además de los requisitos educacionales y de experiencia sino el apego al Código de Ética y el desarrollo profesional continuo. Los rigurosos requerimientos de este programa, aseguran que los auditores internos que logran la certificación, están armados con herramientas invaluables que pueden ser aplicadas globalmente en cualquier organización o industria.

5.3.2. Sector financiero guatemalteco

El riesgo tecnológico es una parte importante del riesgo operacional, esto se da en la medida que los procesos de negocio de las empresas dependan de las Tecnologías de la Información (TI), situación que hoy es muy común.

Diversos entes reguladores de distintos países de Latinoamérica han adoptado la Supervisión Basada en Riesgo (SBR), la cual toma el riesgo operacional como base de la autosupervisión.

Todas estas normativas, recomendaciones y modelos de autorregulación hacen referencia a que el riesgo tecnológico es pilar fundamental del riesgo operacional, pero de alguna manera no está definido cuál es el nivel de madurez que debería existir en el control interno de TI.

Si bien muchas compañías han logrado un nivel de madurez de sus áreas de TI, es común encontrarse con gerentes que han manifestado su descontento con relación a la TI, luego de haber realizado grandes inversiones de dinero.

Por su parte, cada vez más el gobierno corporativo de las organizaciones, se está dando cuenta de la importancia que tiene el área de tecnología de información vista tradicionalmente como ejecutora de proyectos específicos de automatización y como consumidora de recursos.

De alguna manera las organizaciones tienen claro dónde deberían estar, qué estándares adoptar, qué certificaciones obtener, entre otros. Pero el paso previo que se debe realizar siempre, es conocer su estado actual. Resulta casi imposible definir el objetivo a alcanzar, así como trabajar en cómo y cuándo alcanzarlo, si no se conoce el estado inicial.

En este punto es donde se recomienda adoptar como marco referencial a COBIT, ya que es el complemento tecnológico para COSO, que es el marco de control recomendado por los organismos de supervisión.

La principal utilidad de COBIT en esta etapa, es que permite comparar los elementos de control interno TI con las mejores prácticas. Una vez realizada esta comparación con COBIT, se tiene el punto de partida, enfocándose en trabajar con base en los riesgos propios del negocio, regulaciones específicas y los más importantes, las definiciones como Gobierno Corporativo de cuál es el grado de madurez que se requiere para el área de TI y cuál es el nivel de control interno que la compañía define.

5.3.2.1. Reglamento para la administración del riesgo tecnológico

El riesgo tecnológico es uno de los componentes principales del riesgo operacional y hace referencia a la contingencia de que la interrupción, alteración o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución.

Las Tecnologías de Información (TI) juegan un rol importante en el desarrollo de las actividades de las organizaciones bancarias, por lo que el riesgo tecnológico debe gestionar debido a la alineación de la TI para que soporten el logro de los objetivos del negocio siendo esta una tarea fundamental, asegurar el valor de la TI y el incremento en el número de requerimientos normativos y de control.

La Superintendencia de Bancos de Guatemala, a través de la resolución JM-102-2011 de la Junta Monetaria, tiene en consideración el proyecto de Reglamento para la Administración del Riesgo Tecnológico en el cual establece que para el desarrollo normal de sus actividades, las entidades del sistema financiero supervisado dependen en alto grado del uso de tecnología de la información por lo que se hace necesario gestionar adecuadamente el riesgo tecnológico para asegurar la integridad, disponibilidad, confidencialidad de la información, así como la continuidad de la prestación de sus servicios.

En el artículo 55 de la Ley de Bancos y Grupos Financieros establece que los bancos y las empresas que integran grupos financieros deberán contar con procesos integrales que incluyan, entre otros, la administración del riesgo operacional, del cual forma parte el riesgo tecnológico, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos.

De conformidad con buenas prácticas a nivel internacional es conveniente que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades *off shore*, así como las empresas especializadas en servicios financieros que forman parte de grupos financieros, cuenten con lineamientos mínimos que deben observar con el fin de llevar a cabo una adecuada administración del riesgo tecnológico, con el objetivo de mitigar el riesgo de pérdidas financieras ocasionadas por la materialización de dicho riesgo.

Este reglamento tiene por objeto establecer los lineamientos mínimos que los bancos, las sociedades financieras, las entidades fuera de plaza o entidades *off shore* y las empresas especializadas en servicios financieros que forman parte de un grupo financiero, deberán cumplir para administrar el riesgo tecnológico, estructurado de la siguiente manera:

- Disposiciones generales

- Organización para la administración del riesgo tecnológico

- Políticas y procedimientos orientados a la administración del riesgo tecnológico, en concordancia con el nivel de tolerancia al riesgo de la institución.

- Responsabilidades del Consejo de Administración, entre estas la de velar porque se implemente y mantenga una adecuada administración del riesgo tecnológico.

- Comité de Gestión de Riesgos a cargo de la dirección de la administración del riesgo tecnológico, entre otros riesgos.

- Unidad de Administración de Riesgos para realizar las actividades operativas respecto a la administración de riesgos tecnológicos.

- Plan estratégico de TI alineado con la estrategia de negocios, para administrar la TI, considerando la gestión del riesgo tecnológico.

- Organización de TI capaz de soportar las necesidades del negocio

- Manual de administración del riesgo tecnológico con las políticas y procedimientos por escrito y con la debida aprobación del Consejo de Administración.

- Infraestructura tecnológica, sistemas de información, bases de datos y servicios de TI.

- Esquema de la información del negocio

- Inventario de infraestructura de TI, sistemas de información y bases de datos.

- Administración de las bases de datos

- Monitoreo de TI
- Adquisición y mantenimiento de TI
- Gestión de servicios de TI
- Ciclo de vida de los sistemas de información
- Seguridad de la tecnología de información
- Confidencialidad, integridad y disponibilidad de los datos
- Monitoreo de la seguridad
- Roles y responsabilidades
- Clasificación de la información
- Seguridad física
- Seguridad lógica
- Copias de respaldo
- Continuidad de operaciones de TI
- Plan de continuidad del negocio
- Plan de continuidad de operaciones de TI

- Análisis de Impacto al Negocio (BIA)
- Plan de Recuperación ante Desastres (DRP)
- Revisión, pruebas y actualización de los planes
- Personal crítico de TI
- Centro de cómputo alterno
- Seguridad en el intercambio de información
- Protección de datos
- Control de la infraestructura
- Registro y bitácoras de transacciones
- Disposiciones transitorias y finales

CONCLUSIONES

1. La auditoría informática comprende la intervención y evaluación de la organización en cuanto a su gestión sobre las tecnologías de información, el control para el desarrollo de sistemas de documentación, operaciones, el sistema de entrada, proceso y salida de información, estudios de seguridad física conjuntamente con el análisis de los riesgos o amenazas a que está expuesta la información computarizada y los equipos, tanto por elementos externos como internos, que en forma voluntaria o accidental pudieran variar la economía, eficiencia y efectividad de la producción de informática.

2. Los controles y metodologías que provee la auditoría informática es parte de los procesos de negocio y está integrado en ellos, permitiendo su funcionamiento adecuado y supervisando su comportamiento y aplicabilidad en cada momento siendo una herramienta útil para la gestión, pero no un sustituto de ésta.

3. Los estándares de la auditoría informática contienen una colección de objetivos de control relacionados a los requerimientos de información del negocio, ofreciendo una guía detallada sobre los efectos de distintos aspectos de TI, para ayudar a las organizaciones a realizar operaciones eficaces y eficientes.

4. El estándar COBIT está focalizado exclusivamente en los controles sobre la tecnología informática en soporte de los objetivos del negocio, en cuanto que SAC se enfatiza en tecnología informática y COSO provee una visión amplia a nivel de toda la organización.

5. En Guatemala, la mayoría de las organizaciones dependen de procesos de negocio soportados por recursos informáticos que en su mayoría aún no cuentan con buenas prácticas de auditoría para salvaguardar el activo intangible de las organizaciones, siendo el mayor enfoque en la seguridad y no el gobierno de TI.

RECOMENDACIONES

1. El proceso de promover la auditoría informática debe estar conformada por un buen planeamiento, mantenimiento de la ejecución y estar preparados para cualquier cambio que pueda traer con el pasar del tiempo.

2. Se debe evaluar la capacidad de los controles y metodologías aplicadas de auditoría de sistemas de información para reducir el riesgo a un nivel aceptable y que apoyen la calidad y la integridad de la información.

3. Toda organización que posea sistemas de información medianamente complejos, deben someterse a un control interno de evaluación de eficacia y eficiencia, con personal altamente capacitado en cualesquiera de los tres estándares COBIT, COSO y SAC, de acuerdo al giro del negocio, precisando de gran conocimiento de informática, seriedad, capacidad, minuciosidad y responsabilidad en cuanto a la ejecución de dicho control interno.

4. Para la utilización de cualquiera de los estándares de la auditoría informática se debe tomar en cuenta que dicho estándar cubra todos los objetivos organizacionales y que sus componentes abarquen en su mayoría los requerimientos de evaluación y control interno en una organización.

5. Para gestionar el riesgo tecnológico y los requisitos de cumplimiento de forma sistemática y exhaustiva en las empresas guatemaltecas, la auditoría en sistemas debe basarse en las mejores prácticas de la industria para dar garantía y seguridad de la tecnología, logrando al mismo tiempo satisfacer sus requisitos de negocio.

BIBLIOGRAFÍA

1. AICPA. *Understanding internal control and internal control services* [en línea]. <http://www.journalofaccountancy.com/Issues/2009/Sep/White+Paper+Understanding+Internal+Control+and+Internal+Control+Services.htm>. [Consulta: octubre de 2011].

2. _____; CICA. *Suitable trust services criteria and illustrations for security, availability, processing integrity, online privacy, and confidentiality* [en línea]. <http://www.webtrust.org/>. [Consulta: agosto de 2011].

3. BERNAL MONTAÑÉS, Rafael; COLTELL SIMÓN, Óscar. *Auditoría de los sistemas de información*. 2a ed. España: Universidad Politécnica de Valencia, 1996. 683 p. ISBN: 8477213933.

4. COSO. *Embracing enterprise risk management: practical approaches for getting started* [en línea]. <http://www.coso.org/guidance.htm>. [Consulta: octubre de 2011].

5. ERNST; YOUNG LLP. *Evaluación del control interno* [en línea]. <http://www.pericia.cl/Doc/control_interno.pdf>. [Consulta: agosto de 2011].

6. GLOBALTEK Security. *Análisis y evaluación de riesgos metodología MARGERIT* [en línea]. <http://www.acis.org.co/fileadmin/Conferencias/ConfArmandoCarvajMayo8.pdf>. [Consulta: agosto de 2011].

7. IIA. *Certificaciones* [en línea]. <http://www.imai.org.mx/index.php?option=com_content&view=article&id=61&Itemid=56>. [Consulta: octubre de 2011].

8. ISACA. *IS Standards, guidelines and procedures for auditing and control professionals* [en línea]. <http://www.whitehouse.gov/files/documents/cyber/ISACA 20- 20IS 20Standards, 20Guidelines, 20and 20Procedures 20for 20Auditing 20and 20Control 20Professionals.pdf>. [Consulta: agosto de 2011].

9. ISACA Guatemala Chapter. *COBIT 5* [en línea]. <http://www.isaca-guatemala.org/content/cobit5>. [Consulta: enero de 2012].

10. ISACA Journal. *The source for IT governance professionals* [en línea]. <http://www.isaca.org/Journal/Pages/default.aspx>. [Consulta: agosto de 2011].

11. PIATTINI, Mario; DEL PESO, Emilio. *Auditoría informática: un enfoque práctico*. 2a ed. España: Alfaomega, 2001. 660 p. ISBN: 9701507312.

12. SIB. *Reglamento para la administración del riesgo tecnológico* [en línea]. <http://www.sib.gob.gt/web/sib/leyesyreglamentos/reglamentos>. [Consulta: enero de 2012].