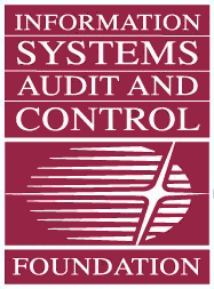
COBIT™

GOVERNANCE,
CONTROL *and* AUDIT
for INFORMATION *and*
RELATED TECHNOLOGY



Planificación y Gestión de Sistemas de Información

TRABAJO DE TEORÍA

(Dirección: Francisco Ruiz González)

Roberto Sobrinos Sánchez
Escuela Superior de Informática de Ciudad Real
Universidad de Castilla – La Mancha
19 de Mayo de 1999

1. Índice

2. Introducción

Hoy en día, uno de los aspectos más importantes (y críticos a la vez) para el éxito y la supervivencia de cualquier organización, es la gestión efectiva de la información así como de las tecnologías relacionadas con ella (tecnologías de la información → TI). En esta sociedad 'informatizada', donde la información viaja a través del ciberespacio sin ninguna restricción de tiempo, distancia y velocidad; esta importancia y criticacalidad surge de los siguientes aspectos:

- aumento de la dependencia de la información, así como de los sistemas que proporcionan dicha información;
- aumento de la vulnerabilidad, así como un amplio espectro de amenazas (como las amenazas del ciberespacio y la lucha por la información);
- escala y coste de las inversiones actuales y futuras en información y tecnologías de la información;
- potencial de las tecnologías para realizar cambios importantes en las organizaciones y en las prácticas de negocio, creando nuevas oportunidades y reduciendo costes.

Para muchas organizaciones, la información y las tecnologías que las soportan representan su medio o recurso más valioso (de hecho, muchas organizaciones reconocen los beneficios potenciales que la tecnología puede aportar). Además, en los cada vez más cambiantes y competitivos entornos de negocio que existen en la actualidad, la gestión ha aumentado las espectativas con respecto a las funciones de liberización de las tecnologías de la información. Verdaderamente, la información y los sistemas de información están adentrándose a lo largo y ancho de las organizaciones (desde la plataforma del usuario hasta las redes de area local y ancha, los sistemas cliente/servidor y los grandes mainframes o supercomputadores). Así, la gestión requiere de un aumento de la calidad, funcionalidad y facilidad de uso; disminuyendo a la vez los periodos de entrega; y mejorando continuamente los niveles de servicio (con la exigencia de que esto se lleve a cabo con costes más bajos).

Las organizaciones deben cumplir con los requerimientos de calidad, de informes fiduciarios y de seguridad, tanto para su información, como para sus activos. La administración deberá obtener un balance adecuado en el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus expectativas, la administración deberá establecer un sistema adecuado de control interno. Por lo tanto, este sistema o marco referencial deberá existir para proporcionar soporte a los procesos de negocio y debe ser preciso en la forma en la que cada actividad individual de control satisface los requerimientos de información y puede impactar a los recursos de TI. Este impacto en los recursos de TI es enfatizado en el Marco Referencial de COBIT conjuntamente a los requerimientos de información del negocio que deben ser alcanzados: efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. El control, que incluye políticas, estructuras, prácticas y procedimientos organizacionales, es responsabilidad de la administración.

De esta forma, la gestión de la información necesita tener una apreciación y un entendimiento básico de los riesgos y restricciones de las tecnologías de la información, en orden de proporcionar directrices efectivas así como los controles adecuados, es decir, la realización de un proceso de revisión y verificación de la información y de las tecnologías que las soportan. Todo este procedimiento es lo que se conoce como Auditoría que, al estar aplicada sobre el uso y manejo de la información y de sus tecnologías, será una Auditoría Informática. *The COBIT Framework* es un conjunto de objetivos de control que ayudan (dando unas pautas de actuación) en la realización de una Auditoría Informática.

Antes de ver de qué trata y qué elementos contiene este *COBIT Framework,* veremos en profundidad que es exactamente una Auditoría (Informática en nuestro caso) y cuales son sus elementos y pasos de actuación.

3. Auditoría

3.1. AUDITORÍA. CONCEPTO

Conceptualmente la auditoría, en general, es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas.

Podemos descomponer este concepto en los elementos fundamentales que a continuación se especifican:

- Contenido: una opinión.
- Condición: profesional.
- Justificación: sustentada en determinados procedimientos. [1]
- Objeto: una determinada información obtenida en un cierto soporte.
- Finalidad: determinar si presenta adecuadamente la realidad o ésta responde a las expectativas que le son atribuidas, es decir, su fiabilidad.

En todo caso es una función que se realiza a posteriori, en relación con actividades ya realizadas, sobre las que hay que emitir una opinión.

3.2. CLASES DE AUDITORIA

Los dos últimos elementos (objeto y finalidad) distinguen de qué clase o tipo de auditoría se trata. El objeto sometido a estudio, sea cual sea su soporte, por una parte, y la finalidad con que se realiza el estudio, definen el tipo de auditoría de que se trata. Las más importantes (a título ilustrativo) son las siguientes:

- Financiera: el objeto de esta es revisar las cuentas anuales, y su finalidad es presentar la realidad de dichas cuentas.

- Informática: es la auditoría que nosotros estudiaremos con más detenimiento. Su objeto es la revisión de sistemas de aplicación, recursos informáticos, planes de contingencia, etc. La finalidad es comprobar la operatividad (que esta sea eficiente), según las normas establecidas.

- Gestión: su objeto es la dirección, y su finalidad es comprobar la eficacia, eficiencia y economicidad.

- Cumplimiento: el objeto es comprobar las normas establecidas. La finalidad es ver que las operaciones se adecuan a estas normas.

[1] **Procedimientos**: La opinión profesional, elemento esencial de la auditoría, se fundamenta y justifica por medio de unos procedimientos específicos tendentes a proporcionar una seguridad razonable de lo que se afirma. Como es natural, cada una de las clases o tipos de auditoría posee sus propios procedimientos para alcanzar el fin previsto, aún cuando puedan en muchos casos coincidir. El alcance de la auditoría, concepto de vital importancia, nos viene dado por los procedimientos. La amplitud y profundidad de los procedimientos que se apliquen nos definen su alcance.

3.3. FUNCIONES DE CONTROL INTERNO Y AUDITORÍA INFORMÁTICA

3.3.1. Control Interno Informático

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales. La misión del control interno informático es asegurarse de que las medidas que se obtienen de los mecanismos implantados por cada responsable sean correctas y válidas.

El Control Interno Informático suele ser un órgano staff[2] de la Dirección del Departamento de Informática y está dotado de las personas y medios materiales proporcionados a los cometidos que se le encomienden. Como principales objetivos del Control Interno Informático, podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el conocimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio informático, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

3.3.2. Auditoría Informática

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos. De este modo la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría, los cuales son:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos sino también los de eficacia y eficiencia.

El auditor evalúa y comprueba en determinados momentos del tiempo los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso del software. En muchos casos, ya no es posible verificar manualmente los procedimientos informatizados que resumen, calculan y clasifican datos, por lo que se deben emplear software de auditoría y otras técnicas asistidas por ordenador.

[2] **Staff**: los puestos staff de una organización, son órganos de apoyo que surgen para diferenciar las actividades de la línea (toma de decisiones), y tienen dos funciones: asesoramiento, sugerencia y orientación para la planificación de objetivos, políticas y procedimientos; y la realización de actividades de servicios para la línea como el establecimiento de sistemas de contratación del personal de línea.

El auditor es responsable de revisar e informar a la Dirección de la Organización sobre el diseño y el funcionamiento de los controles implantados y sobre la fiabilidad de la información suministrada.

Se pueden establecer tres grupos de funciones a realizar por un auditor informático:

- Participar en las revisiones durante y después del diseño, realización, implantación y explotación de aplicaciones informáticas, así como en las fases análogas de realización de cambios importantes.
- Revisar y juzgar los controles implantados en los sistemas informáticos para verificar su adecuación a las órdenes e instrucciones de la Dirección, requisitos legales, protección de confidencialidad y cobertura ante errores y fraudes.
- Revisar y juzgar el nivel de eficiencia, utilidad, fiabilidad y seguridad de los equipos e información.

La Auditoría Informática y el Control Interno Informático son campos análogos. De hecho, muchos de los actuales responsables de control interno informático recibieron formación en seguridad informática tras su paso por la formación en auditoría. Numerosos auditores se pasan al campo de control interno debido a la similitud de los objetivos profesionales de control y auditoría. Pese a que ambas figuras tienen objetivos comunes, existen diferencias que conviene matizar. Veamos una tabla ilustrativa que muestra las similitudes y diferencias entre ambas disciplinas:

	CONTROL INTERNO INFORMÁTICO	***AUDITOR INFORMÁTICO***
SIMILITUDES	✓ Personal interno. ✓ Conocimientos especializados en Tecnología de la Información. ✓ Verificación del cumplimiento de controles internos, normativa y procedimientos establecidos por la Dirección de Informática y la Dirección General para los sistemas de información.	
DIFERENCIAS	✓ Análisis de los controles en el día a día. ✓ Informa a la Dirección del Departamento de Informática. ✓ Sólo personal interno. ✓ El alcance de sus funciones es únicamente sobre el Departamento de Informática.	✓ Análisis de un momento informático determinado. ✓ Informa a la Dirección General de la Organización. ✓ Personal interno y/o externo. ✓ Tiene cobertura sobre todos los componentes de los sistemas de información de la Organización.

Tabla 1. Diferencias y similitudes del Control interno y la Auditoría Informática

3.4. SISTEMAS DE CONTROL INTERNO INFORMÁTICO

3.4.1. Definición y tipos de controles internos

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para conseguir sus objetivos.

Los controles cuando se diseñen, desarrollen e implanten han de ser al menos completos, simples, fiables, revisables, adecuados y rentables. Respecto a esto último será preciso analizar el coste-riesgo de su implantación.

Los controles internos que se utilizan en el entorno informático continúan evolucionando hoy en día a medida que los sistemas informáticos se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se emplean tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Para asegurar la integridad, disponibilidad y eficacia de los sistemas, se requieren complejos mecanismos de control, la mayoría de los cuales son automáticos. Resulta interesante observar, sin embargo, que hasta en los sistemas cliente/servidor avanzados, aunque algunos controles son completamente automáticos, otros son completamente manuales, y muchos dependen de una combinación de elementos de software y de procedimientos.

Históricamente, los objetivos de los controles informáticos se han clasificado en las siguientes categorías:

- Controles preventivos: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.

- Controles detectivos: cuando fallan los preventivos, para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de acceso no autorizados, el registro de la actividad diaria para detectar errores u omisiones, etc.

- Controles correctivos: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad.

3.4.2. Implantación de un sistema de controles internos informáticos

Los controles pueden implantarse a varios niveles diferentes. La evaluación de los controles de la Tecnología de la Información exige analizar diversos elementos independientes. Por ello es importante llegar a conocer bien la configuración del sistema, con el objeto de identificar los elementos, productos y herramientas que existen para saber dónde pueden implantarse los controles, así como identificar posibles riesgos. Para llegar a conocer la configuración del sistema es necesario documentar los detalles de la red, así como los distintos niveles de control y elementos relacionados:

- Entorno de red: esquema de la red, descripción de la configuración hardware de comunicaciones, descripción del software que se utiliza como acceso a las telecomunicaciones, control de red, situación general de los ordenadores de entornos de base que soportan aplicaciones críticas y consideraciones relativas a la seguridad de la red.

- Configuración del ordenador base: configuración del soporte físico, entorno del sistema operativo, software con particiones, entornos (pruebas y real), bibliotecas de programas y conjunto de datos.

- Entorno de aplicaciones: procesos de transacciones, sistemas de gestión de bases de datos y entornos de procesos distribuidos.

- Productos y herramientas: software para desarrollo de programas, software de gestión de bibliotecas y para operaciones automáticas.

- Seguridad del ordenador base: identificar y verificar usuarios, control de acceso, registro e información, integridad del sistema, controles de supervisión, etc.

Para la implantación de un sistema de controles internos informáticos habrá que definir las siguientes características:

- Gestión de sistemas de información: políticas, pautas y normas técnicas que sirvan de base para el diseño y la implantación de los sistemas de información y de los controles correspondientes.

- Administración de sistemas: controles sobre la actividad de los centros de datos y otras funciones de apoyo al sistema, incluyendo la administración de las redes.

- Seguridad: incluye las tres clases de controles fundamentales implantados en el software del sistema, como son la integridad del sistema, la confidencialidad (control de acceso) y la disponibilidad.

- Gestión del cambio: separación de las pruebas y la producción a nivel de software y controles de procedimientos, para la migración de programas software aprobados y probados.

Figura 1. Control Interno y Auditoría

La implantación de una política y cultura sobre la seguridad, requiere que sea realizada por fases y esté respaldada por la Dirección. Cada función juega un papel importante en las distintas etapas que son, básicamente, las siguientes:

- Dirección de Negocio o Dirección de Sistemas de Información (S.I.): han de definir la política y/o directrices para los sistemas de información en base a las exigencias del negocio, que podrán ser internas o externas.

- Dirección de Informática: ha de definir las normas de funcionamiento del entorno informático y de cada una de las funciones de informática mediante la creación y publicación de procedimientos, estándares, metodología y normas, aplicables a todas las áreas de informática, así como a los usuarios que establezcan el marco de funcionamiento.

- Control Interno Informático: ha de definir los diferentes controles periódicos a realizar en cada una de las funciones informáticas, de acuerdo al nivel de riesgo de cada una de ellas, y ser diseñados conforme a los objetivos de negocio y dentro del marco legal aplicable. Estos se plasmarán en los oportunos procedimientos de control interno y podrán ser preventivos o de detección. Realizará periódicamente la revisión de los controles establecidos de Control Interno Informático, informando de las desviaciones a la Dirección de Informática y sugiriendo cuantos cambios crea convenientes en los controles. Deberá, además, transmitir constantemente a toda la Organización de Informática la cultura y políticas del riesgo informático.

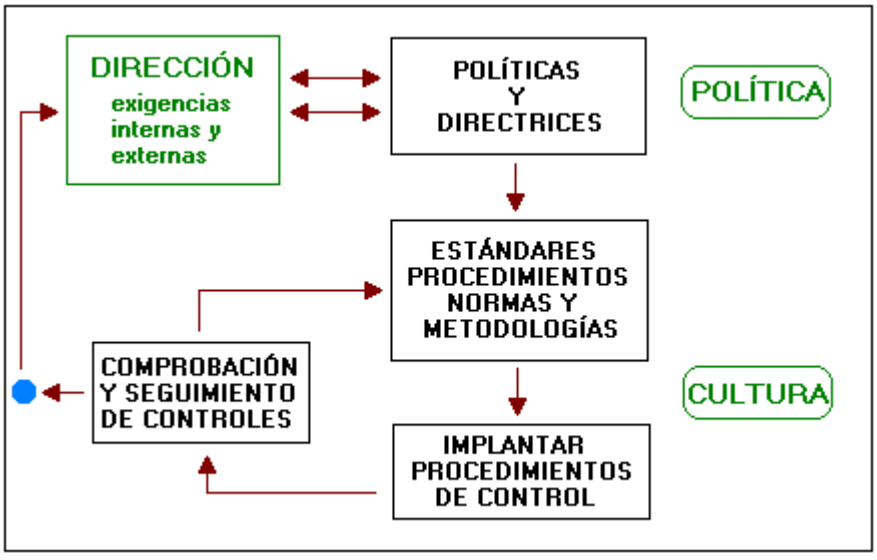


Figura 2. Control Interno Informático

- Auditor interno/externo informático: ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de la normativa interna y externa, de acuerdo al nivel de riesgo y conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará también a la Alta Dirección, de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

La creación de un sistema de control informático es una responsabilidad de la Gerencia y un punto destacable de la política en el entorno informático.

A continuación, se indican algunos controles internos para los sistemas de información, agrupados por secciones funcionales, y que serían los que el Control Interno Informático y la Auditoría Informática deberían verificar para determinar su cumplimiento y validez:

- Controles generales organizativos: engloba una serie de elementos, tales como:

  - ✓ *Políticas.*
  - ✓ *Planificación (plan estratégico de información, plan informático, plan general de seguridad y plan de emergencia ante desastres).*
  - ✓ *Estándares.*
  - ✓ *Procedimientos.*
  - ✓ *Organizar el departamento de informática.*
  - ✓ *Descripción de las funciones y responsabilidades dentro del departamento.*
  - ✓ *Políticas de personal.*
  - ✓ *Asegurar que la dirección revisa todos los informes de control y resuelve las excepciones que ocurran.*
  - ✓ *Asegurar que existe una política de clasificación de la información.*
  - ✓ *Designar oficialmente la figura del Control Interno Informático y de la Auditoría Informática.*

- Controles de desarrollo, adquisición y mantenimiento de sistemas de información: se utilizan para que se puedan alcanzar la eficacia del sistema, economía y eficiencia, integridad de los datos, protección de los recursos y cumplimiento con las leyes y regulaciones. Se compone de:

  - ✓ *Metodología del ciclo de vida del desarrollo de sistemas.*
  - ✓ *Explotación y mantenimiento.*

- Controles de explotación de sistemas de información: consta de:

  - ✓ *Planificación y gestión de recursos.*
  - ✓ *Controles para usar de manera efectiva los recursos en ordenadores.*
  - ✓ *Procedimientos de selección del software del sistema, de instalación, de mantenimiento, de seguridad y de control de cambios.*
  - ✓ *Seguridad física y lógica.*

- Controles en aplicaciones: cada aplicación debe llevar controles incorporados para garantizar la entrada, actualización, y mantenimiento de los datos:

  - ✓ *Control de entrada de datos.*
  - ✓ *Controles de tratamiento de datos.*
  - ✓ *Controles de salida de datos.*

- Controles específicos de ciertas tecnologías:

  - ✓ *Controles en Sistemas de Gestión de Bases de Datos.*
  - ✓ *Controles en informática distribuida y redes.*
  - ✓ *Controles sobre ordenadores personales y redes de área local.*

3.5. METODOLOGÍAS DE CONTROL INTERNO, SEGURIDAD Y AUDITORÍA INFORMÁTICA

3.5.1. Conceptos fundamentales

En general, una metodología es un conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal, es decir, que cualquier proceso científico debe estar sujeto a una disciplina definida con anterioridad. En el campo de la informática, el cual ha sido siempre una materia compleja en todos sus aspectos, se hace necesaria la utilización de metodologías debido, precisamente, a esa dificultad. Estas metodologías, se aplican en la totalidad de ámbitos de esta materia, desde su diseño de ingeniería hasta el desarrollo del software, y como no, la auditoría de los sistemas de información.

La metodología es necesaria para que un equipo de profesionales alcance un resultado homogéneo tal como si lo hiciera uno sólo. Por ello, resulta habitual el uso de metodologías en las empresas auditoras/consultoras profesionales (desarrolladas por los más expertos) para conseguir resultados similares (homogéneos) en equipos de trabajo diferentes (heterogéneos).

El uso de métodos de auditoría es casi paralelo al nacimiento de la informática, en la que existen muchas disciplinas cuyo uso de las metodologías constituye una práctica habitual. Una de ellas es la seguridad de los sistemas de información, que si la definimos como la doctrina que trata de los riesgos informáticos o creados por la informática, entonces la auditoría es una de las figuras involucradas en este proceso de protección y preservación de la información y de sus medios de proceso. Por lo tanto, el nivel de seguridad informática en una entidad es un objetivo a evaluar y está directamente relacionado con la calidad y eficacia de un conjunto de acciones y medidas, destinadas a proteger y preservar la información de dicha entidad y sus medios de proceso.

Resumiendo, la informática crea unos riesgos informáticos de los que hay que proteger y preservar a la entidad con un entramado de contramedidas, y la calidad y la eficacia de las mismas es el objetivo a evaluar para poder identificar así sus puntos débiles y mejorarlos. Ésta, es una de las funciones de los auditores informáticos, por lo que debemos profundizar más en este entramado de contramedidas para ver qué papel tienen las metodologías y los auditores en el mismo. Para explicar este aspecto, diremos que cualquier contramedida nace de la composición de varios factores (expresados en la *Figura 3*). Todos los factores de la pirámide intervienen en la composición de una contramedida:

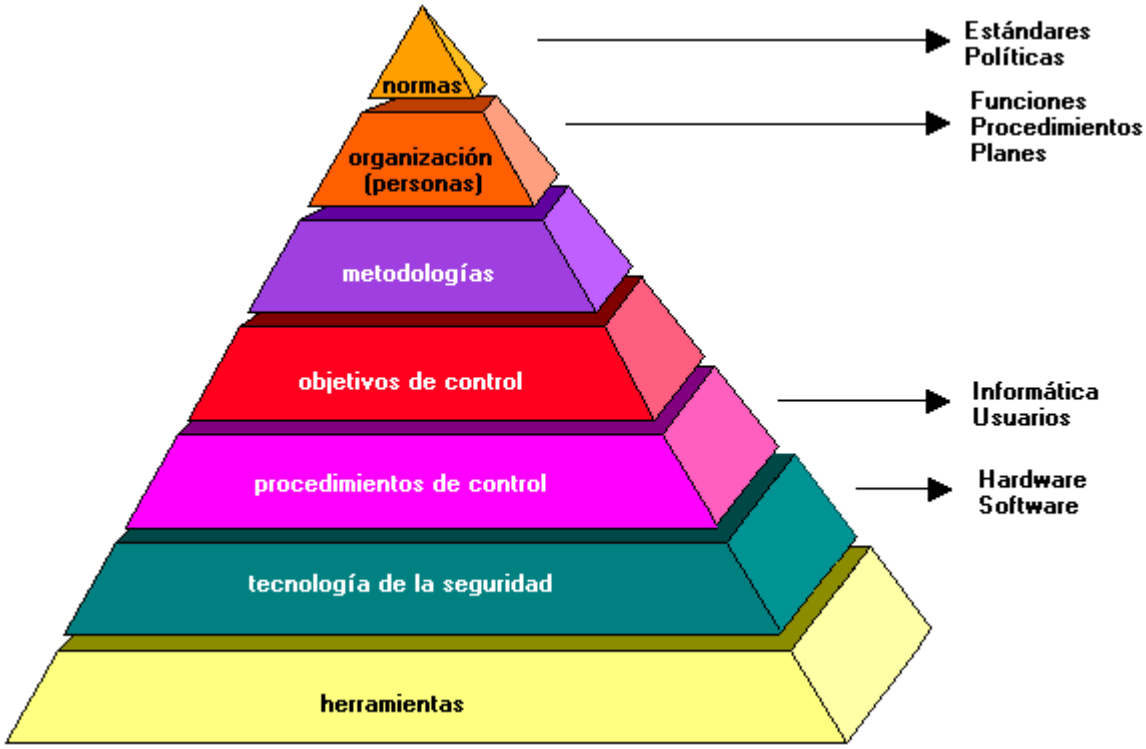


Figura 3. Factores de la Contramedida

Veamos más detalladamente cada uno de los elementos que conforman la contramedida:

- La Normativa: debe definir de forma clara y precisa todo lo que debe existir y ser cumplido, tanto desde el punto de vista conceptual, como práctico, desde lo general a lo particular. Debe inspirarse en estándares, políticas, marco jurídico, políticas y normas de empresa, experiencia y práctica profesional. Desarrollando la normativa, debe alcanzarse el resto del "gráfico valor" mostrado en la *Figura 3*. Se puede dar el caso en que una normativa y su carácter disciplinado sea el único control de un riesgo (aunque esto no sea frecuente).

- La Organización: la integran personas con funciones específicas y con actuaciones concretas, procedimientos definidos metodológicamente y aprobados por la dirección de la empresa. Éste es el aspecto más importante, dado que sin él, nada es posible. Se pueden establecer controles sin alguno de los demás aspectos, pero nunca sin personas, ya que son éstas las que realizarán los procedimientos y desarrollan los diversos planes (Plan de Seguridad, Plan de Contingencias, Auditorías, etc).

- Las Metodologías: son necesarias para desarrollar cualquier proyecto que nos propongamos de manera ordenada y eficaz.

- Los Objetivos de Control: son los objetivos a cumplir en el control de procesos. Este concepto es el más importante después de 'la organización', y solamente de un planteamiento correcto de los mismos, saldrán unos procedimientos eficaces y realistas.

- Los Procedimientos de Control: son los procedimientos operativos de las distintas áreas de la empresa, obtenidos con una metodología apropiada, para la consecución de uno o varios objetivos de control y, por lo tanto, deben estar documentados y aprobados por la Dirección. La tendencia habitual de los informáticos es la de dar más peso a la herramienta que al propio control o contramedida, pero no se debe olvidar que una herramienta nunca es solución sino una ayuda para conseguir un control mejor. Sin la existencia de estos procedimientos, las herramientas de control son solamente una 'anécdota'.

- La Tecnología de Seguridad: dentro de este nivel, están todos los elementos (hardware y software) que ayudan a controlar un riesgo informático. En este concepto están los cifradores, autentificadores, equipos denominados 'tolerantes al fallo', las herramientas de control, etc.

- Las Herramientas de Control: son elementos software que permiten definir uno o varios procedimientos de control para cumplir una normativa y un objetivo de control.

Todos estos factores están relacionados entre sí, así como la calidad de cada uno con la de los demás. Cuando se evalua el nivel de Seguridad de Sistemas en una institución, se están evaluando todos estos factores (mencionados antes), y se plantea un Plan de Seguridad nuevo que mejore dichos factores, aunque conforme vayamos realizando los distintos proyectos del plan, no irán mejorando todos por igual. Al finalizar el plan se habrá conseguido una situación nueva en la que el nivel de control sea superior al anterior.

Llamaremos **Plan de Seguridad** a una estrategia planificada de acciones y proyectos que lleven a un sistema de información y sus centros de proceso de una situación inicial determinada (y a mejorar) a una situación mejorada.

En la *Figura 4* se expone la tendencia actual en la organización de la seguridad de sistemas en la empresa. Por una parte un comité que estaría formado por el director de la estrategia y de las políticas; y por otra parte, el control interno y la auditoría informática. La función del control interno se ve involucrada en la realización de los procedimientos de control, y es una labor del día a día.
La función de la auditoría informática está centrada en la evaluación de los distintos aspectos que designe su **Plan Auditor**, con unas características de trabajo que son las visitas concretas al centro, con objetivos concretos y, tras terminar su trabajo, la presentación del informe de resultados.

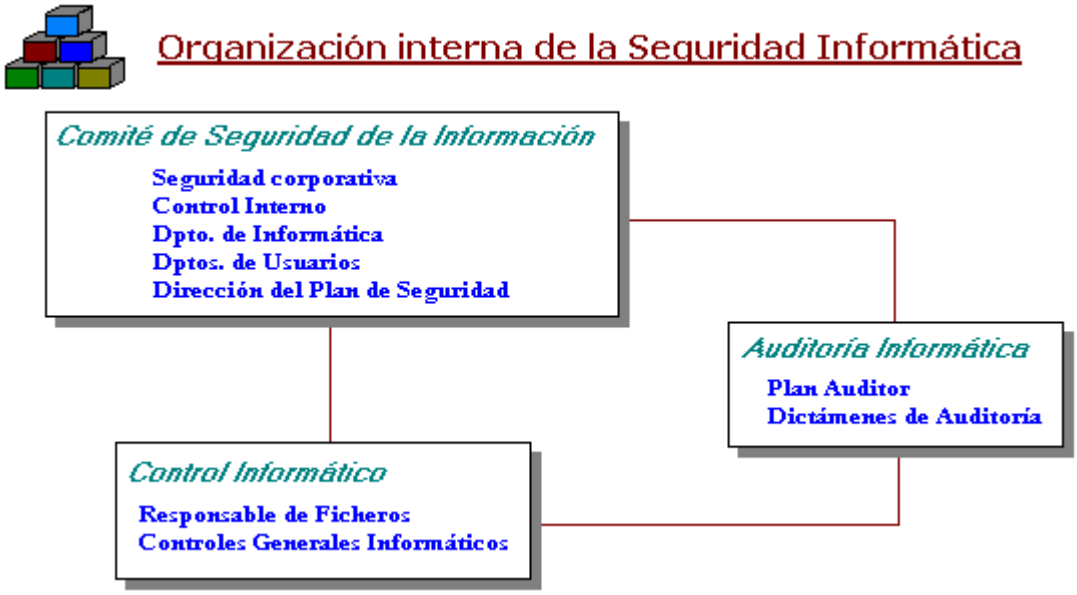


Figura 4. Organización interna de la Seguridad Informática

Queda pues por decir, que ambas funciones deben ser independientes de la informática, dado que por la disciplina laboral, la labor de las dos funciones quedaría mediatizada y comprometida. Esto es lo que se llama ”segregación de funciones” entre éstas y la informática.

3.5.2.Metodologías de evaluación de sistemas

En el mundo de la seguridad de sistemas, se utilizan todas las metodologías necesarias para realizar un plan de seguridad además de las de auditoría informática.

Las dos metodologías de evaluación de sistemas por antonomasia son las de Análisis de Riesgos y las de Auditoría Informática, con dos enfoques distintos. La auditoría informática sólo identifica el nivel de “exposición” por la falta de controles, mientras que el análisis de riesgos facilita la “evaluación” de los riesgos y recomienda acciones en base al coste-beneficio de las mismas.

Veamos una serie de definiciones para profundizar en estas metodologías:

- Amenaza: todo aquello que se ve como posible fuente de peligro o catástrofe (ya sea persona o cosa, tal como robo de datos, incendios, sabotaje, falta de procedimientos de emergencia, divulgación de datos, aplicaciones mal diseñadas, gastos incontrolados, etc).

- ♦ Vulnerabilidad: Situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático (como por ejemplo, la falta de control de acceso lógico, la falta de control de versiones, la inexistencia de un control de soportes magnéticos, etc).

- ♦ Riesgo: probabilidad de que una amenaza llegue acaecer por una vulnerabilidad (como, por ejemplo, los datos estadísticos de cada evento de una base de datos de incidentes).

- ♦ Exposición o impacto: es la evaluación del efecto del riesgo (por ejemplo, es frecuente evaluar el impacto en términos económicos, aunque no siempre lo es, como vidas humanas, imagen de la empresa, honor, defensa nacional, etc).

Todos los riesgos que se presentan podemos:

- Evitarlos (no construir un centro donde hay peligro constante de inundaciones).
- Transferirlos (uso de un centro de cálculo contratado).
- Reducirlos (sistema de detección y extinción de incendios).
- Asumirlos, que es lo que se hace si no se controla el riesgo en absoluto.

Para los tres primeros, se actúa si se establecen controles o contramedidas. Todas las metodologías existentes en seguridad de sistemas van encaminadas a establecer y mejorar un entramado de contramedidas que garanticen que la probabilidad de que las amenazas se materialicen en hechos (por falta de control) sea lo mas baja posible o, al menos, que quede reducida de una forma razonable en costo-beneficio.

Todas las metodologías existentes desarrolladas y utilizadas en la auditoría y el control informáticos, se pueden agrupar en dos grandes familias:

- Cuantitativas: basadas en un modelo matemático numérico que ayuda a la realización del trabajo.

- Cualitativas: basadas en el criterio y raciocinio humano capaz de definir un proceso de trabajo, para seleccionar en base a la experiencia acumulada.

Metodologías Cuantitativas

Estan diseñadas para producir una lista de riesgos que pueden compararse entre sí con facilidad por tener asignados unos valores numéricos. Estos valores en el caso de metodologías de análisis de riesgos o de planes de contingencias son datos de probabilidad de ocurrencia (riesgo) de un evento que se debe extraer de un registro de incidencias donde el número de ellas sea suficientemente grande. Esto no pasa en la práctica, y se aproxima ese valor de forma subjetiva restando, así, rigor científico al cálculo (pero dado que el cálculo se hace para ayudar a elegir el método entre varias contramedidas podríamos aceptarlo.

En general, podemos observar con claridad dos grandes inconvenientes que presentan estas metodologías. Por una parte, la debilidad de los datos de la probabilidad de ocurrencia por los pocos registros y la poca significación de los mismos a nivel mundial; y por otro, la imposibilidad o difilcutad de evaluar económicamente todos los impactos que pueden acaecer frente a la ventaja de poder usar un modelo matemático para el análisis.

Metodologías Cualitativas ó Subjetivas

Están basadas en métodos estadísticos y lógica difusa (humana, no matemática → FUZZY LOGIC). Precisan de la colaboración de un profesional experimentado, pero requieren menos recursos humanos/tiempo que las metodologías cuantitativas.

La tendencia de uso en la realidad, es la mezcla de ambas. En la *Tabla 2* se muestra el cuadro comparativo de ambas metodologías:

	Cuantitativa	Cualitativa ó Subjetiva
PROS	Enfoca pensamientos mediante el uso de números. Facilita la comparación de vulnera-bilidades muy distintas. Proporciona una cifra "justificante" para cada contramedida.	Enfoque lo amplio que se desee. Plan de trabajo flexible y reactivo. Se concentra en la identificación de eventos. Incluye factores intangibles.
CONTRAS	Estimación de probabilidad depende de estadísticas fiables inexistentes. Estimación de las pérdidas potenciales sólo si son valores cuantificables. Metodologías estándares. Difíciles de mantener o modificar. Dependencia de un profesional.	Depende fuertemente de la habilidad y calidad del personal involucrado. Puede excluir riesgos significantes desconocidos. Identificador de eventos reales más claros al no tener que aplicarles probabilidades complejas de calcular. Dependencia de un profesional.

Tabla 2. Comparación entre metodologías cuantitativas y cualitativas

Las metodologías usadas más comunmente son las siguientes:

Metodologías de Análisis de Riesgos

Están desarrolladas para la identificación de la falta de controles y el establecimiento de un plan de contramedidas. En base a unos cuestionarios, se identifican vulnerabilidades y riesgos, y se evalúa el impacto para más tarde identificar las contramedidas y el coste. La siguiente etapa es la más importante, pues mediante un juego de simulación (que llamaremos 'Que pasa sí?...') analizamos el efecto de las distintas contramedidas en la disminución de los riesgos analizados, eligiendo de esta manera un plan de contramedidas (plan de seguridad) que compondrá el informe final de la evaluación.

El esquema básico de una metodología de análisis de riesgos es, en esencia, el representado en la *Figura 5*.

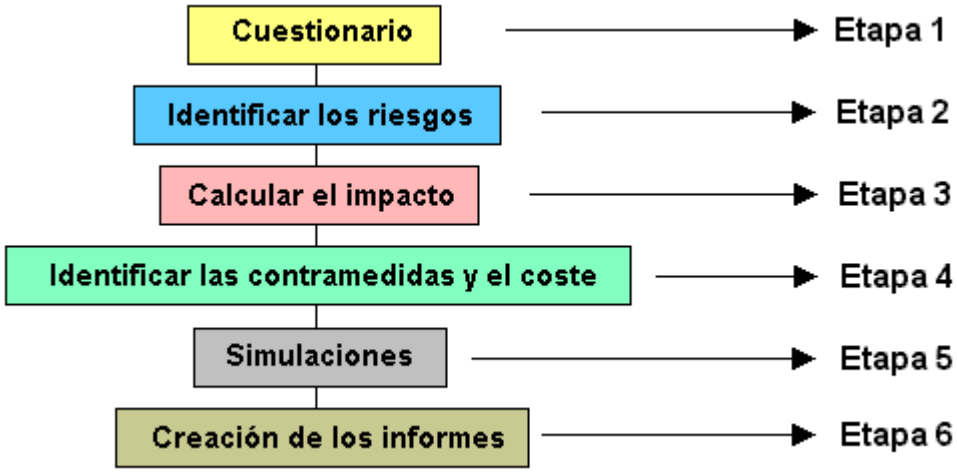


Figura 5. Esquema básico de una metodología de análisis de riesgos

Plan de Contingencias

El auditor debe conocer perfectamente los conceptos de un plan de contingencias para poder auditarlo. El plan de contingencias y de recuperación de negocio es lo mismo, pero no así el plan de restauración interno. También se manejan a veces los conceptos de plan de contigencias informático y plan de contingencias corporativo, cuyos conceptos son sólo de alcance. El corporativo cubre no sólo la informática, sino todos los departamentos de una entidad, y puede incluir también el informático como un departamento más. Frecuentemente, se realiza el informático.

El plan de contingencias es una estrategia planificada constituida por un conjunto de recursos de respaldo, una organización de emergencia y unos procedimientos de actuación, encaminada a conseguir una restauración progresiva y ágil de los servicios de negocio afectados por una paralización total o parcial de la capacidad operativa de la empresa. Esa estrategia, materializada en un manual, es el resultado de todo un proceso de análisis y definiciones que es lo que dá lugar a las metodologías.

Es muy importante tener en cuenta que el concepto a considerar es “la continuidad en el negocio”; es decir, estudiar todo lo que puede paralizar la actividad y producir pérdidas. Todo lo que no considere este criterio no será nunca un plan de contingencias. Veamos cuales son las fases de un plan:

- Análisis y Diseño: se estudia la problemática, las necesidades de recursos, las alternativas de respaldo, y se analiza el coste/beneficio de las mismas. Ésta es la fase más importante, pudiendo llegarse al final de la misma incluso a la conclusión de que no es viable o es muy costoso su seguimiento.

- Desarrollo del Plan: esta fase y la siguiente son similares en todas las metodologías. En ella se desarrolla la estrategia seleccionada, implantándose hasta el final todas las acciones previstas. Se definen las distintas organizaciones de emergencia y se desarrollan los procedimientos de actuación generando, así, la documentación del plan. Es en esta fase cuando se analiza la vuelta a la normalidad, dado que pasar de la situación normal a la alternativa debe concluirse con la reconstrucción de la situación inicial antes de la contingencia, y esto es lo que no todas las metodologías incluyen.

- Pruebas y Mantenimiento: en esta fase se definen las pruebas, sus características y sus ciclos, y se realiza la primera prueba como comprobación de todo el trabajo realizado, así como mentalizar al personal implicado.

- Herramientas: en este caso, como en todas las metodologías, la herramienta es una anécdota, y lo importante es tener y usar la metodología apropiada para desarrollar más tarde la herramienta que se necesite. Toda herramienta debería tener, al menos, los siguientes componentes: base de datos relacional, módulo de entrada de datos, módulo de consultas, procesador de textos, generador de informes, ayudas *on-line*, hoja de cálculo, gestor de proyectos y generador de gráficos.

3.5.3. Las metodologías de auditoría informática

Las únicas metodologías que podemos encontrar en la auditoría informática son dos familias distintas: las auditorías de Controles Generales como producto estándar de las auditorias profesionales, que son una homologación de las mismas a nivel internacional, y las Metodologías de los auditores internos.

El objetivo de las auditorías de controles generales es 'dar una opinión sobre la fiabilidad de los datos del ordenador para la auditoría financiera'. El resultado externo es un escueto informe como parte del informe de auditoría, donde se destacan las vulnerabilidades encontradas. Están basadas en pequeños cuestinarios estándares que dan como resultado informes muy generalistas.

Veamos brebemente cuales son las partes básicas de un plan auditor informático:

- Funciones. Ubicación de la figura en el organigrama de la empresa

- Procedimientos para las distintas tareas de las auditorías. Entre ellos están el procedimiento de apertura, el de entrega y discusión de debilidades, entrega de informe preliminar, cierre de auditoría, redacción de informe final, etc.

- Tipos de auditorías que realiza. Metodologías y cuestionarios de las mismas. Existen dos tipos de auditoría según su alcance: la Completa (*Full*) de un área y la Acción de Inspección Correctiva *(Corrective Action Review* o *CAR*) que es la comprobación de acciones correctivas de auditorías anteriores.

- Sistema de evaluación y los distintos aspectos que evalúa. Deben definirse varios aspectos a evaluar como el nivel de gestión económica, gestión de recursos humanos, cumplimiento de normas, etc, así como realizar una evaluación global de resumen para toda la auditoría. Esta evaluación final nos servirá para definir la fecha de repetición de la misma auditoría en el futuro, según el nivel de exposición que se le haya dado a este tipo de auditoría en cuestión.

- Nivel de exposición. Es un valor definido subjetivamente que permite definir la fecha de la repetición de la misma auditoría, en base a la evaluación final de la última auditoría realizada sobre ese tema.

- Lista de distribución de informes.

- Seguimiento de las acciones correctoras.

- Plan quinquenal. Todas las áreas a auditar deben corresponderse con cuestionarios metodológicos y deben repartirse en cuatro o cinco años de trabajo. Esta planificación, además de las repeticiones y añadido de las auditorías no programadas que se estimen oportunas, deberá componer anualmente el plan de trabajo (anual).

- Plan de trabajo anual. Deben estimarse tiempos de manera racional y componer un calendario que, una vez terminado, nos dé un resultado de horas de trabajo previstas y, por tanto, de los recursos que se necesitarán.

Las metodologías de auditoría informática son del tipo cualitativo/subjetivo (podemos decir que son las subjetivas por excelencia). Por tanto, están basadas en profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas, que exigen una gran profesionalidad y formación continuada. Solo así esta función se consolidará en las entidades, esto es, por el "respeto profesional" a los que ejercen la función.

3.5.4 Control Interno Informático. Sus métodos y procedimientos. Las herramientas de control.

Hoy en día, la tendencia generalizada es contemplar, al lado de la figura del auditor informático, la de control interno informático. Tal es el caso de la organización internacional **I.S.A.C.A.** (*Information Systems Audit and Control Association* → Asociación para la auditoría y control de los sistemas de información), creadora de la norma **COBIT** (tema de estudio de este informe) y que, con anterioridad, se llamó *The EDP Auditors Association INC.***,** incluyendo en la actualidad las funciones de control informático además de las de auditoría.

Pese a su similitud, podríamos decir que existen claras diferencias entre las funciones del control informático y las de la auditoría informática:

- El área informática monta los procesos informáticos seguros.
- El control interno monta los controles.
- La auditoría informática evalúa el grado de control.

Las funciones básicas del control interno informático son las siguientes:

- Administración de la seguridad lógica.
- Funciones de control dual con otros departamentos.
- Función normativa y del cumplimiento del marco jurídico.
- Responsable del desarrollo y actualización del Plan de Contingencias, Manuales de procedimientos, etc.
- Dictar normas de seguridad informática.
- Definir los procedimientos de control.
- Control del Entorno de Desarrollo.
- Controles de soportes magnéticos según la clasificación de la información.
- Controles de soportes físicos.
- Control de información comprometida o sensible.
- Control de calidad del software.
- Control de calidad del servicio informático.
- Control de costes.

- Responsable de los departamentos de recursos humanos y técnico.
- Control y manejo de claves de cifrado.
- Vigilancia del cumplimiento de las normas y controles.
- Control de cambios y versiones.
- Control de paso de aplicaciones a explotación.
- Control de medidas de seguridad física o corporativa en la informática.
- Responsable de datos personales.

Todas estas funciones son un poco ambiciosas para desarrollarlas desde el instante inicial de la implantación de esta figura, pero no debemos perder el objetivo de que el control informático es el componente de la "actuación segura" entre los usuarios, la informática y el control interno, todos ellos auditados por la auditoría informática.

Para obtener el entramado de contramedidas o controles compuesto por los factores que veíamos en la *Figura 3*, debemos ir abordando proyectos usando distintas metodologías, tal como se observa en la *Figura 6*, que irán conformando y mejorando el número de controles.

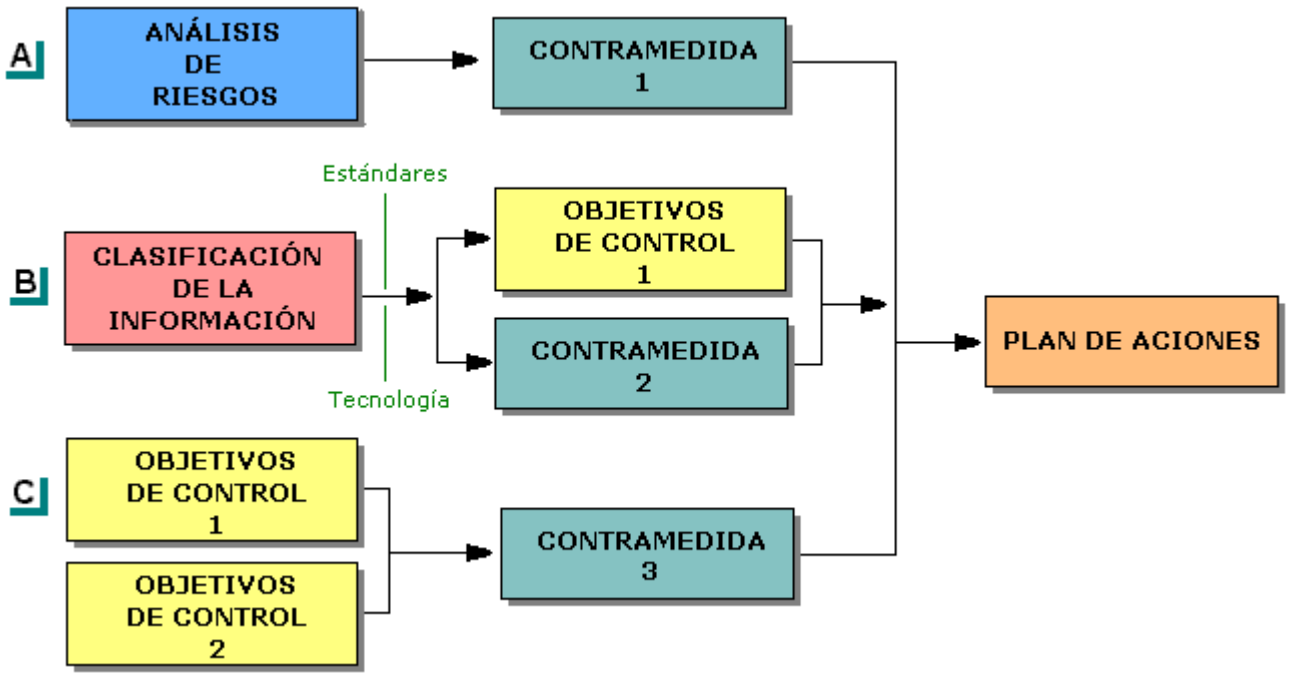


Figura 6. Obtención de los Controles

Las Herramientas de Control

En la última fase de la pirámide (*Figura 3*), nos encontramos las herramientas de control. En la tecnología de la seguridad informática que se ve envuelta en los controles, existe tecnología hardware (como los cifradores) y software. Las herramientas de control son elementos software que por sus características funcionales permiten vertebrar[3] un control de una manera más actual y más automatizada. Como se vió antes, el control se define en todo un proceso metodológico, y en un punto del mismo se analiza si existe una herramienta que automatice o mejore el control para más tarde definirlo con la herramienta incluida, y al final documentar los procedimientos de las distintas áreas involucradas para que estas los cumplan y sean auditados. Es decir, comprar una herramienta sin más y ver qué podemos hacer con ella es un error profesional grave que no conduce a nada, comparable a trabajar sin método e improvisando en cualquier disciplina informática.

Las herramientas de control (software) más comunes son:

- Seguridad lógica del sistema.
- Seguridad lógica complementaria al sistema (desarrollado a medida).
- Seguridad lógica para entornos distribuidos.
- Control de acceso físico. Control de presencia.
- Control de copias.
- Gestión de copias.
- Gestión de soportes magnéticos.
- Gestión y control de impresión y envío de listados por red.
- Control de proyectos.
- Control y gestión de incidencias.
- Control de cambios.

Todas estas herramientas están inmersas en controles nacidos de unos objetivos de control y que regularán la actuación de las distintas áreas involucradas.

3.6. ASPECTOS FINALES

Son muchas, pués, las metodologías que se pueden encontrar en el mundo de la auditoría informática y control interno. Como resumen, se podría decir que la metodología es el fruto del nivel profesional de cada uno y de su visión de cómo conseguir un mejor resultado en el nivel de control de cada entidad, aunque el nivel de control resultante debe ser similar.

Pero en realidad, todas ellas son herramientas de trabajo mejores o peores que ayudan a conseguir mejores resultados, ya que las únicas herramientas verdaderas de la auditoría y el control informático son la “actitud y aptitud”, junto con una postura vigilante y una formación continuada.

3.7. LECTURAS RECOMENDADAS

Piattini Velthuis, Mario G.; Del Peso Navarro, Emilio. 1998. RA-MA “*AUDITORÍA INFORMÁTICA. Un enfoque práctico*”. E-MAIL: rama@arrakis.es

[3] **Vertebrar**: dar consistencia y estructura internas; dar organización y cohesión.

4. The COBIT Framework

4.1. FUNCIÓN BÁSICA Y ORIENTACIÓN DEL COBIT.

El COBIT, es una herramienta de gobierno de las Tecnologías de la Información que ha cambiado de igual forma que lo ha hecho el trabajo de los profesionales de TI. La ISACF, organización creadora de esta norma COBIT (Information Systems Audit and Control Foundation) así como sus patrocinadores, han diseñado este producto principalmente como una fuente de instrucción para los profesionales dedicados a las actividades de control. La defnición que nos ofrece el sumario ejecutivo del COBIT (*Control OBjetives for Information and related Tecnology* → Gobierno, Control y Revisión de la Información y Tecnologías Relacionadas) es la siguiente:

La misión del COBIT: buscar, desarrollar, publicar y promover un autoritario y actualizado conjunto internacional de objetivos de control de tecnologías de la información, generalmente aceptadas, para el uso diario por parte de gestores de negocio y auditores.

Dicho de una forma menos formal, señalaremos que el COBIT ayuda a salvar las brechas existentes entre los riesgos de negocio, necesidades de control y aspectos técnicos. Además, proporciona "prácticas sanas" a través de un Marco Referencial (*Framework*) de dominios y procesos, y presenta actividades en una estructura manejable y lógica. Las “prácticas sanas” del COBIT representan el consenso de los expertos (ayudarán a los profesionales a optimizar la inversión en información, pero aún más importante, representan aquello sobre lo que serán juzgados si las cosas salen mal).

El tema principal que trata el COBIT es la orientación a negocios. Éste, está diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, esta diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. De forma creciente, las prácticas de negocio comprenden la completa autorización de los procesos propios de negocio, con lo que poseen una total responsabilidad para todos los aspectos de dichos procesos. La norma COBIT, proporciona una herramienta para los procesos propios de negocio que facilitan la descarga de esta responsabilidad. La norma parte con una simple y pragmática premisa:

> ***En orden de proporcionar la información que la organización necesita para llevar a cabo sus objetivos, los requisitos de las tecnologías de la información necesitan ser gestionados por un conjunto de procesos agrupados de forma natural.***

La norma continua con un conjunto de 34 objetivos de control de alto nivel para cada uno de los procesos de las tecnologías de la información, agrupados en cuatro dominios: planificación y organización, adquisición e implementación, soporte de entrega y monitorización. Esta estructura, abarca todos los aspectos de la información y de la tecnología que la mantiene. Mediante la dirección de estos 34 objetivos de control de alto nivel, los procesos propios de negocio pueden garantizar la existencia de un sistema de control adecuado para los entornos de las tecnologías de la información. En suma, cada uno de los 34 objetivos de control de alto nivel correspondiente, es una directiva de revisión o seguridad para permitir la inspección de los procesos de las tecnologías de la información en contraste con los 302 objetivos de control detallados en el COBIT para el suministro de una gestión de seguridad, así como de un aviso para la mejora. La norma COBIT contiene un conjunto de herramientas de implementación el cual aporta una serie de lecciones de aprendizaje, con las que las organizaciones podrán aplicar de forma rápida y satisfactoria esta norma a sus entornos de trabajo.

En definitiva, el COBIT es una herramienta que permite a los gerentes comunicarse y salvar la brecha existente entre los requerimientos de control, aspectos técnicos y riesgos de negocio. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI, a través de organizaciones a nivel mundial. El objetivo del COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo. Por lo tanto, COBIT esta orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con las tecnologías de la información y con las tecnologías relacionadas.

4.2. HISTORIA Y EVOLUCIÓN DEL COBIT.

El proyecto COBIT se emprendió por primera vez en el año 1995, con el fin de crear un mayor producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. La primera edición del COBIT, fué publicada en 1996 y fue vendida en 98 paises de todo el mundo. La segunda edición (tema de estudio en este informe) publicada en Abril de 1998, desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados (de forma detallada) objetivos de control de alto nivel, intensificando las lineas maestras de auditoría, introduciendo un conjunto de herramientas de implementación, así como un CD-ROM completamente organizado el cual contiene la totalidad de los contenidos de esta segunda edición.

Evolución del producto COBIT

El COBIT evolucionará a través de los años y será el fundamento de investigaciones futuras, por lo que se generará una familia de productos COBIT. Al ocurrir esto, las tareas y actividades que sirven como la estructura para organizar los Objetivos de Control de TI, serán refinadas posteriormente, siendo también revisado el balance entre los dominios y los procesos a la luz de los cambios en la industria.

Una temprana adición significativa visualizada para la familia de productos COBIT, es el desarrollo de las Guías de Gerencia que incluyen Factores Críticos de Exito, Indicadores Clave de Desempeño y Medidas Comparativas. Los Factores Críticos de Éxito, identificarán los aspectos o acciones más importantes para la administración y poder tomar, así, dichas aciones o considerar los aspectos para lograr control sobre sus procesos de TI. Los Indicadores Clave de Desempeño proporcionarán medidas de éxito que permitirán a la gerencia conocer si un proceso de TI esta alcanzando los requerimientos de negocio. La Medidas Comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: determinar el nivel actual de madurez de la empresa; determinar el nivel de madurez que se desea lograr, como una función de sus riesgos y objetivos; y proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición, proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de COBIT.

En definitiva, la organización ISACF (creadora, como ya se ha comentado, de la norma) espera que el COBIT sea adoptado por las comunidades de auditoría y negocio como un estándar generalmente aceptado para el control de las Tecnologías de la Información.

4.3. DESARROLLO Y COMPONENTES DEL COBIT.

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información. El COBIT es, pues, una herramienta innovadora para el gobierno de las Tecnologías de la Información.

El COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulativos y específicos para la industria, tanto los ya existentes como los que están surgiendo en la actualidad. Los Objetivos de Control resultantes han sido desarrollados para su aplicación en sistemas de información en toda la empresa. El término "generalmente aplicables y aceptados" es utilizado explícitamente en el mismo sentido que los Principios de Contabilidad Generalmente Aceptados (PCGA o GAAP por sus siglas en inglés). Para propósitos del proyecto, "buenas prácticas" significa consenso por parte de los expertos.

Este estándar es relativamente pequeño en tamaño, con el fin de ser práctico y responder, en la medida de lo posible, a las necesidades de negocio, manteniendo al mismo tiempo una independencia con respecto a las plataformas técnicas de TI adoptadas en una organización. El proporcionar indicadores de desempeño (normas, reglas, etc.), ha sido identificado como prioridad para las mejoras futuras que se realizarán al marco referencial.

El desarrollo de COBIT ha traído como resultado la publicación del Marco Referencial general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

Se determinó que las mejoras a los objetivos de control originales deberían consistir en:

- el desarrollo de un marco referencial para el control en tecnologías de la información como fundamento para los objetivos de control en TI, y como una guía para la investigación consistente en auditoría y control de las tecnologías de la información;
- una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho;
- y una revisión crítica de las diferentes actividades y tareas que conforman los dominios de control en tecnología de información y, cuando fuese posible, la especificación de indicadores de desempeño relevantes (normas, reglas, etc.), así como una revisión crítica y una actualización de las guías actuales para el desarrollo de auditorías de los sistemas de información.

Componentes del COBIT 2ª Edición

El desarrollo del COBIT (2ª Edición), ha resultado en la publicación de los siguientes componentes:

Un Resumen Ejecutivo (Executive Sumary), el cual consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios del COBIT;

un Marco Referencial (Framework), el cual proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios del COBIT, e identifica los cuatro dominios de COBIT describiendo en detalle, además, los 34 objetivos de control de alto nivel e identificando los requerimientos de negocio para la información y los recursos de las Tecnologías de la Información que son impactados en forma primaria por cada objetivo de control;

los Objetivos de Control (Control Objetives), los cuales 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 las Tecnologías de la Información;

las Guías de Auditoría (Audit Guidelines), las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia 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 a la gerencia certeza o unas recomendaciones para mejorar;

un Conjunto de Herramientas de Implementación (Implementation Tool Set), el cual proporciona las lecciones aprendidas por organizaciones que han aplicado COBIT rápida y exitosamente en sus ambientes de trabajo. Este conjunto de herramientas de implementación incluye la Síntesis Ejecutiva, proporcionando a la alta gerencia conciencia y entendimiento del COBIT. También incluye una guía de implementación con dos útiles herramientas: Diagnóstico de la Conciencia de la Gerencia y el Diagnóstico de Control de TI, para proporcionar asistencia en el análisis del ambiente de control en TI de una organización. También se incluyen varios casos de estudio que detallan como organizaciones en todo el mundo han implementado COBIT exitosamente. Adicionalmente, se incluyen respuestas a las 25 preguntas mas frecuentes acerca del COBIT, así como varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones;

Por último, se incluye un completo CD-ROM en el cual se puede encontrar toda la información detallada en los manuales descritos anteriormente.

4.4. EL MARCO REFERENCIAL DEL COBIT (COBIT FRAMEWORK).

La necesidad de control en tecnología de información

Como se comentó en la introducción de este informe, hoy en día uno de los aspectos más importantes para el éxito y la supervivencia de cualquier organización, es la gestión efectiva de la información así como de las tecnologías relacionadas con ella (TI). Por lo general, la administración debe decidir la inversión razonable en seguridad y control de estas tecnologías de la Información y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI frecuentemente impredecible. La administración, necesita un Marco Referencial de prácticas de seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente de TI, tanto el existente como el planeado.

Existe una creciente necesidad entre los usuarios en cuanto a la seguridad en los servicios de TI, a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados. Actualmente, sin embargo, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales. Esta confusión proviene de los diferentes métodos de evaluación (tal como la evaluación ISO9000), nuevas evaluaciones de control interno COSO[4], etc. Como resultado, los usuarios necesitan una base general para ser establecida como primer paso.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar frente a la Gerencia su opinión acerca de los controles internos. Sin contar con un marco referencial, ésta se convierte en una tarea demasiado complicada. Esto ha sido mostrado en varios estudios recientes acerca de la manera en la que los auditores evalúan situaciones complejas de seguridad y control en TI, estudios que fueron dados a conocer casi simultáneamente en diferentes partes del mundo. Incluso, la administración consulta cada vez más a los auditores para que le asesoren en forma proactiva en lo referente a asuntos de seguridad y control de TI.

El ambiente de negocios: competencia, cambio y costes

La competencia global es ya un hecho. Las organizaciones se reestructuran con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en tecnología de sistemas de información para mejorar su posición competitiva. La reingeniería en los negocios, las reestructuraciones, el outsourcing[5], las organizaciones horizontales y el procesamiento distribuido son cambios que impactan la manera en la que operan tanto los negocios como las entidades

[4] **COSO**: Committee of Sponsoring Organisations of the Treadway Commisssion Internal Control-Integrated Framework

[5] **Outsourcing**: Contratación global o parcial de servicios informáticos. Se trata de la subcontratación de todo o de parte del trabajo informático mediante un contrato con una empresa externa que se integra en la estrategia de la empresa y busca diseñar una solución a los problemas existentes

gubernamentales. Estos cambios han tenido y continuarán teniendo, profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo.

La especial atención prestada a la obtención de ventajas competitivas y a la economía, implica una dependencia creciente en la computación como el componente más importante en la estrategia de la mayoría de las organizaciones. La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en las computadoras y en las redes, tanto los basados en hardware como los basados en software. Además, las características estructurales fundamentales de estos controles están evolucionando al mismo paso que las tecnologías de computación y las redes.

Si los administradores, los especialistas en sistemas de información y los auditores desean en realidad ser capaces de cumplir con sus tareas en forma efectiva dentro de un marco contextual de cambios acelerados, deberán aumentar y mejorar sus habilidades tan rápidamente como lo demandan la tecnología y el ambiente.

Es preciso, pues, comprender la tecnología de controles involucrada y su naturaleza cambiante, si se desea emitir y ejercer juicios razonables y prudentes al evaluar las prácticas de control que se encuentran en los negocios típicos o en las organizaciones gubernamentales.

Respuesta a las necesidades

En vista de estos continuos cambios, el desarrollo de este Marco Referencial de objetivos de control para TI, conjuntamente con una investigación continua aplicada a controles de TI basada en este marco referencial, constituyen el fundamento para el progreso efectivo en el campo de los controles de sistemas de información.

Por otra parte, hemos sido testigos del desarrollo y publicación de modelos de control generales de negocios como *COSO* en los Estados Unidos, *Cadbury* en el Reino Unido, *CoCo* en Canadá y *King* en Sudáfrica. Por otro lado, existe un número importante de modelos de control más enfocados al nivel de tecnología de información. Algunos buenos ejemplos de esta última categoría son el *Código de Seguridad de Conducta* del DTI (Departamento de Comercio e Industria, Reino Unido) y el *Manual de Seguridad* del NIST (Instituto Nacional de Estándares y Tecnología, EEUU). Sin embargo, estos modelos de control con orientación específica, no proporcionan un modelo de control completo y utilizable sobre la tecnología de información como soporte para los procesos de negocio. El propósito de COBIT es el cubrir este vacío proporcionando una base que esté estrechamente ligada a los objetivos de negocio, al mismo tiempo que se enfoca a la tecnología de información.

Un enfoque hacia los requerimientos de negocio en cuanto a controles para tecnología de información y la aplicación de nuevos modelos de control y estándares internacionales relacionados, hicieron evolucionar los Objetivos de Control y pasar de una herramienta de auditoría al COBIT, que es una herramienta para la administración. COBIT es, por lo tanto, la herramienta innovadora para el gobierno de TI que ayuda a la gerencia a comprender y administrar los riesgos asociados con TI. Por lo tanto, la meta del proyecto es el desarrollar estos objetivos de control principalmente a partir de la perspectiva de los objetivos y necesidades de la empresa. Esto concuerda con la perspectiva *COSO*, que constituye el primer y mejor marco referencial para la administración en cuanto a controles internos. Posteriormente, los objetivos de control fueron desarrollados a partir de la perspectiva de los objetivos de auditoría (certificación de información financiera, certificación de medidas de control interno, eficiencia y efectividad, etc.)

Audiencia: administración, usuarios y auditores

COBIT esta diseñado para ser utilizado por tres audiencias distintas:

ADMINISTRACION:

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

USUARIOS:

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

AUDITORES DE SISTEMAS DE INFORMACION:

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 empresas por el propietario de procesos de negocio en su responsabilidad de control sobre los aspectos de información del proceso, y por todos aquéllos responsables de TI en la empresa.

Orientación a objetivos de negocio

Los Objetivos de Control muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoría. Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Se proporcionan, además, consideraciones y guías para definir e implementar el Objetivo de Control de TI.

La clasificación de los dominios a los que se aplican los objetivos de control de alto nivel (dominios y procesos); una indicación de los requerimientos de negocio para la información en ese dominio, así como los recursos de TI que reciben un impacto primario por parte del objetivo del control, forman conjuntamente el Marco Referencial COBIT. El marco referencial toma como base las actividades de investigación que han identificado 34 objetivos de alto nivel y 302 objetivos detallados de control. El Marco Referencial fue mostrado a la industria de TI y a los profesionales dedicados a la auditoría para abrir la posibilidad a revisiones, dudas y comentarios. Las ideas obtenidas fueron incorporadas en forma apropiada.

Definiciones

Para propósitos de este proyecto, se proporcionan una serie de definiciones. La definición de "Control" está adaptada del reporte *COSO*, y la definición para "Objetivo de Control de Tecnologías de la Información" ha sido adaptada del reporte *SAC*[6] .

[6] **SAC**: Systems Auditability and Control Report

Control se define como	Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.
Objetivo de control en TI se define como	Una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de TI particular.

4.5. LOS PRINCIPIOS DEL MARCO REFERENCIAL.

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

El concepto fundamental 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 considerando a la información como el resultado de la aplicación combinada de recursos relacionados con la Tecnología de Información que deben ser administrados por procesos de TI.

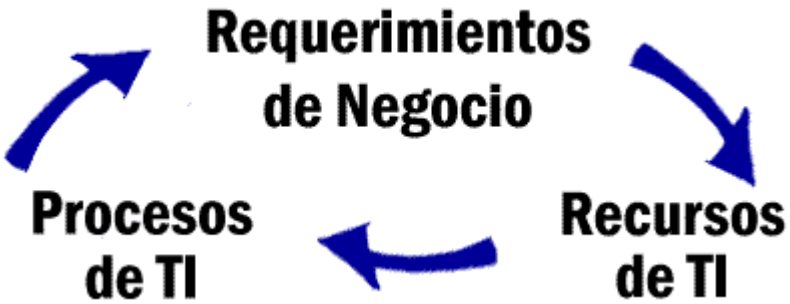


Figura 7

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

Requerimientos de calidad

Calidad
Coste
Entrega (de servicio)

Requerimientos Fiduciarios (COSO)

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

Requerimientos de Seguridad

Confidencialidad
Integridad
Disponibilidad

La Calidad ha sido considerada principalmente por su aspecto 'negativo' (sin fallos, confiable, etc.), lo cual también se encuentra contenido en gran medida en los criterios de Integridad. Los aspectos positivos pero menos tangibles de la calidad (estilo, atractivo, "ver y sentir", desempeño más allá de las expectativas, etc.) no fueron, por un tiempo, considerados desde un punto de vista de Objetivos de Control de TI. La premisa se refiere a que la primera prioridad deberá estar dirigida al manejo apropiado de los riesgos al compararlos contra las oportunidades. El aspecto utilizable de la Calidad está cubierto por los criterios de efectividad. Se consideró que el aspecto de entrega (de servicio) de la Calidad se traslapa[7] con el aspecto de disponibilidad correspondiente a los requerimientos de seguridad y también en alguna medida, con la efectividad y la eficiencia. Finalmente, el coste es también considerado que queda cubierto por la eficiencia.

[7] **traslapar**: cubrir total o parcialmente una cosa

Para los requerimientos fiduciarios[8], COBIT no intentó "reinventar le rueda". Se utilizaron las definiciones de *COSO* para la efectividad y eficiencia de operaciones, confiabilidad de información y cumplimiento con leyes y regulaciones. Sin embargo, la confiabilidad de información fue ampliada para incluir toda la información (no sólo información financiera).

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

Comenzando el análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad más amplios, se extrajeron siete categorías distintas, ciertamente superpuestas. A continuación se muestran las definiciones de trabajo de COBIT:

Efectividad

Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

Eficiencia

Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

Confidencialidad

Se refiere a la protección de información sensible contra divulgación no autorizada.

Integridad

Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

[8] **Fiduciario**: que depende del crédito o confianza

Disponibilidad

Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento

Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocio está sujeto, por ejemplo, criterios de negocio impuestos externamente.

Confiabilidad de la información

Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Los recursos de las tecnologías de la información identificados en COBIT pueden explicarse o definirse como se muestra a continuación:

Datos

Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

Aplicaciones

Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

Tecnología

La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Instalaciones

Recursos para alojar y dar soporte a los sistemas de Información.

Personal

Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorizar servicios y sistemas de información.

El dinero o capital no fue considerado como un recurso para la clasificación de objetivos de control para TI debido a que puede definirse como la inversión en cualquiera de los recursos mencionados anteriormente y podría causar confusión con los requerimientos de auditoría financiera.

El Marco referencial no menciona, en forma específica para todos los casos, la documentación de todos los aspectos "materiales" importantes relacionados con un proceso de TI particular. Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión.

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

Figura 8. Relación de los recursos de TI

La información que los procesos de negocio necesitan es proporcionada a través del empleo de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información son satisfechos, deben definirse, implementarse y monitorizarse medidas de control adecuadas para estos recursos. ¿Como pueden entonces las empresas estar satisfechas respecto a que la información obtenida presente las características que necesitan? Es aquí donde se requiere de un sano marco referencial de Objetivos de Control para TI. El diagrama mostrado a continuación ilustra este concepto.

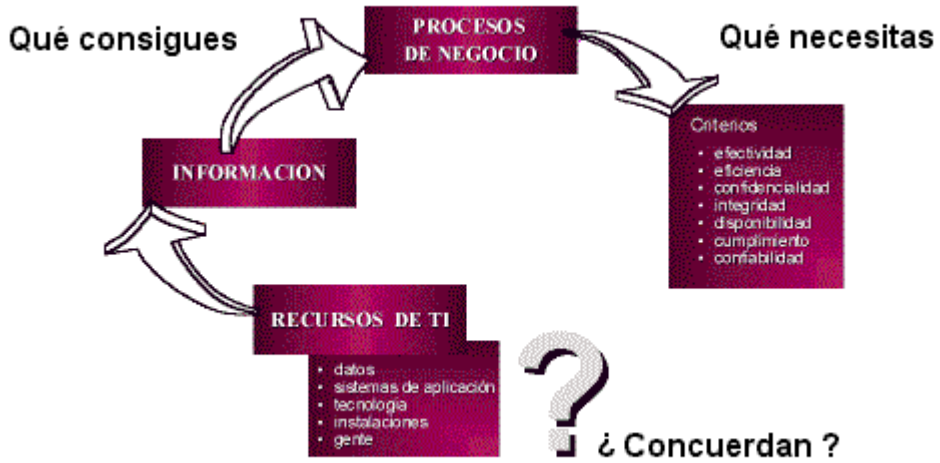


Figura 9. Obtención y análisis de la Información

El marco referencial consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos.

Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta típicamente con requerimientos de control diferentes a los de actividades 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 tecnologías de la información, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño. Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas con "cortes" naturales (de control). Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de tecnologías de la información.

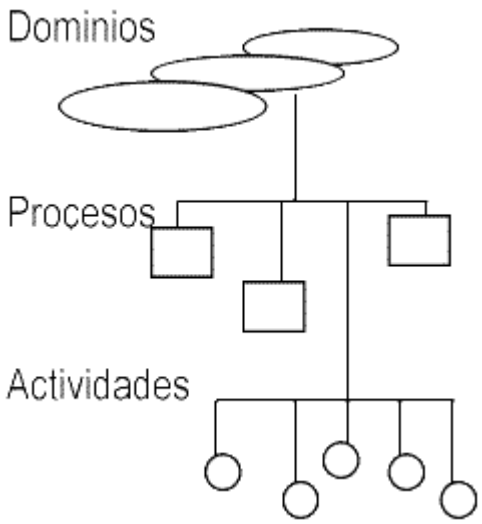


Figura 10. Niveles de Actividades de TI

Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: recursos de TI, requerimientos de negocio para la información y procesos de TI. Estos puntos de vista diferentes permiten al marco referencial ser accedido eficientemente. Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad, seguridad o fiduciario (traducido por el marco referencial en siete requerimientos de información específicos). Un Gerente de TI puede desear considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán desear enfocar el marco referencial desde un punto de vista de cobertura de control. Estos tres puntos estratégicos son descritos en el Cubo COBIT que se muestra a continuación:

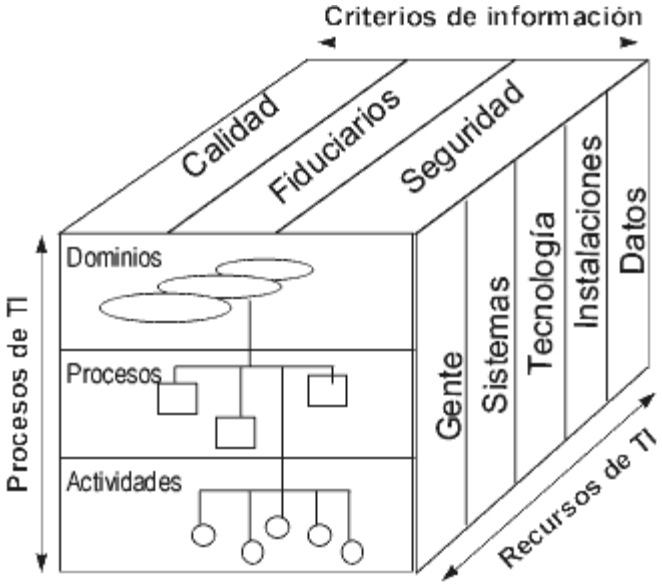


Figura 11. El Cubo COBIT

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización (y no la "jerga" del auditor). Por lo tanto, cuatro grandes dominios son identificados: planificación y organización, adquisición e implementación; entrega y soporte, y monitorización.

Las definiciones para los dominios mencionados son las siguientes:

Planificación y Organización

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

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 se 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, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación

Monitorización

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

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos. El siguiente diagrama ilustra este concepto:

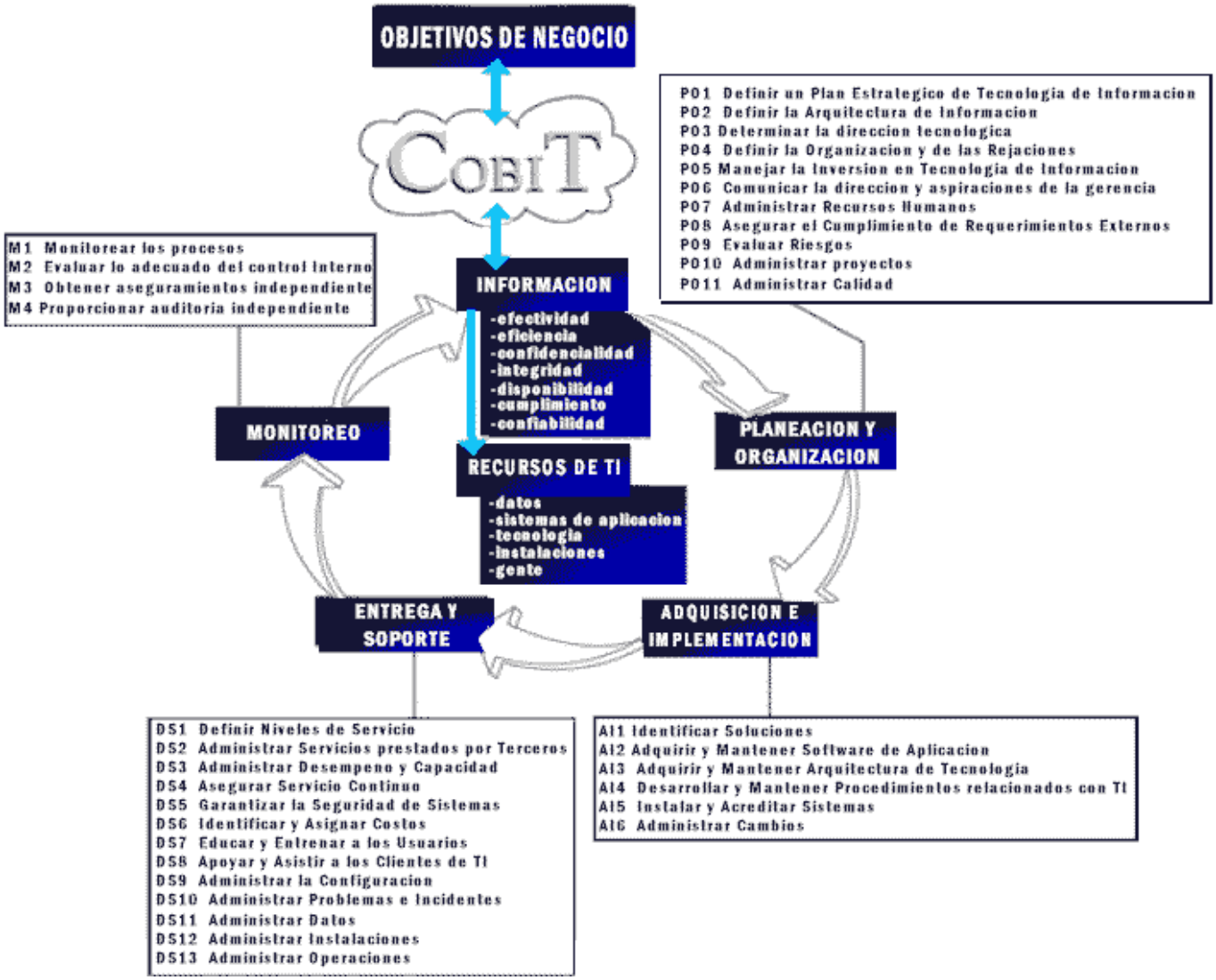


Figura 12. Procesos de TI del COBIT definidos dentro de los cuatro dominios.

Debe tomarse en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel corporativo, otros al nivel de la función de servicios de información, y otros al nivel del propietario de los procesos de negocio.

También debe ser tomado en cuenta que el criterio de efectividad de los procesos que planean o entregan soluciones a los requerimientos de negocio, cubrirán algunas veces los criterios de disponibilidad, integridad y confidencialidad (en la práctica, se han convertido en requerimientos del negocio). Por ejemplo, el proceso de "identificar soluciones automatizadas" deberá ser efectivo en el cumplimiento de requerimientos de disponibilidad, integridad y confidencialidad.

Resulta claro que las medidas de control no satisfarán necesariamente los diferentes requerimientos de información del negocio en la misma medida. Se lleva a cabo una clasificación dentro del marco referencial COBIT basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente. Esta clasificación es la siguiente:

- Primario: es el grado al cual el objetivo de control definido impacta directamente 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 (vacío): podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Similarmente, todas las medidas de control no necesariamente tendrán impacto en los diferentes recursos de TI a un mismo nivel. Por lo tanto, el Marco Referencial de COBIT indica específicamente la aplicabilidad de los recursos de TI que son administrados en forma específica por el proceso bajo consideración (no por aquellos que simplemente toman parte en el proceso). Esta clasificación es hecha dentro el Marco Referencial de COBIT basado en el mismo proceso riguroso de información proporcionada por los investigadores, expertos y revisores, utilizando las definiciones estrictas indicadas previamente.

4.6. OBJETIVOS DE CONTROL DEL MARCO REFERENCIAL (THE COBIT FRAMEWORK).

El marco refencial del COBIT ha sido limitado a una serie de objetivos de control de alto nivel, enfocados a las necesidades de negocio, dentro de un proceso de tecnologías de la información determinado.

Los objetivos de control de las tecnologías de la información han sido organizados por proceso/actividad. Su forma de uso ha sido proporcionada no sólo para facilitar la entrada desde un punto de vista ventajoso, sino también para facilitar aproximaciones globales (o combinadas), tales como la implementación/instalación de un proceso, responsabilidades globales de administración para un proceso, y el uso de los recursos de las TI por parte de un proceso.

Es preciso señalar que los objetivos de control de las TI han sido definidos de una forma general (no dependen de ninguna plataforma técnica), aunque se debe aceptar el hecho de que algunos entornos de tecnología especiales pueden necesitar espacios separados para los objetivos de control.

La forma en que el marco referencial del COBIT presenta los objetivos de control es la siguiente:

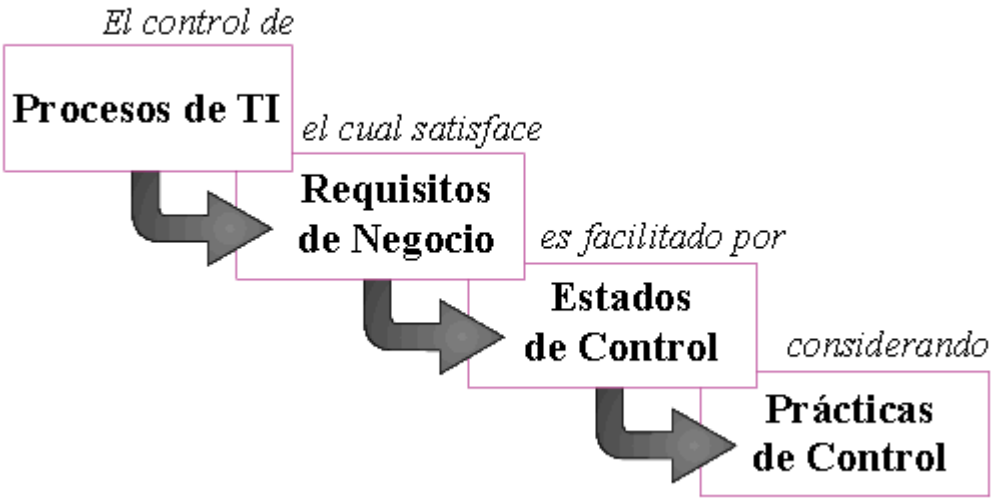


Figura 13. Organización del Marco Referencial.

El marco refencial se divide en cuatro partes correspondientes a los cuatro dominios existentes (planificación y organización, adquisición e implementación, entrega y soporte y monitorización). En cada parte, se reflejan los objetivos de control de alto nivel correspondientes a cada dominio (34 objetivos en total). Para cada uno de los objetivos de control, se sigue una organización como la mostrada en la *Figura 13*. Además, se muestran dos tablas: una que identifica los criterios que son aplicables a cada objetivo de control y en qué grado lo hacen (P→ primario, S→ secundario, "Blanco" → no se aplica ese criterio); y otra que identifica los recursos de TI que son gestionados específicamente por el proceso que se está considerando.

Veamos ya, los 34 objetivos de control de alto nivel de las tecnologías de la información reflejados en el Marco de Referencia COBIT (***COBIT FRAMEWORK***):

Objetivos de Control de Alto Nivel

Dominio de Planificación & Organización

PO1 Definir un plan Estratégico de Tecnología de la Información

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

Definir un plan estratégico de TI

que satisface el requisito de negocio

hallar un balance óptimo de oportunidades de tecnología de la información y los requisitos de negocio así como también asegurar su realización adicional

es facilitado por

un proceso planificador estratégico emprendido a intervalos regulares dando origen a planes a largo plazo; los planes a largo plazo deberían ser traducidos periódicamente en planes operacionales que coloquen metas claras y concretas a corto plazo

y toma en consideración

- definición de los objetivos de negocio y necesidades para las TI
- inventario de soluciones tecnológicas e infraestructura actual
- servicios de "tecnología de vigilancia"
- cambios organizativos
- estudio de viabilidad oportuno
- existencia de evaluaciones de sistemas

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

PO2 Definir la Arquitectura de la Información

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
S	confidencialidad

S	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

definir la arquitectura de la información

que satisface el requisito de negocio

una mejor organización de los sistemas de información

es facilitado por

creando y manteniendo un modelo de información de negocio y asegurando que los sistemas apropiados son definidos para optimizar el uso de esta información

y toma en consideración

- documentación
- diccionario de datos
- reglas sintácticas de datos
- propiedad de datos y clasificación crítica

	personas
X	aplicaciones
	tecnología
	facilidades
X	datos

PO3 Determinar la Dirección Tecnológica

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

determinar la dirección tecnológica

que satisface el requisito de negocio

tomar ventaja de la tecnología disponible y emergente

es facilitado por

creación y mantenimiento de un plan de infraestructura tecnológica

y toma en consideración

- adecuación y evolución de la capacidad de la infraestructura actual

- monitorización de los desarrollos tecnológicos
- contingencias
- planes de adquisición

	personas
	aplicaciones
X	tecnología
X	facilidades
	datos

PO4 Definir la Organización y las Relaciones de las TI

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

definir la organización y las relaciones de las TI

que satisface el requisito de negocio

entregar los servicios de las TI

es facilitado por

una organización apropiada en números y habilidades con roles y responsabilidades comunicadas y definidas

y toma en consideración

- comité de dirección
- consejo de nivel de responsabilidad
- propiedad, custodia
- supervisión
- segregación de obligaciones
- roles y responsabilidades
- descripciones del trabajo
- provisión de niveles
- clave personal

X	personas
	aplicaciones
	tecnología
	facilidades
	datos

PO5 Administrar la Inversión en TI

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
S	confiabilidad

Control sobre el proceso de TI de

administrar la inversión en TI

que satisface el requisito de negocio

garantizar la consolidación y controlar el gasto de los recursos financieros

es facilitado por

una inversión periódica y un presupuesto operacional establecido y aprobado por la empresa

y toma en consideración

- consolidación de alternativas
- control del gasto efectivo
- justificación de los costes
- justificación de los beneficios

X	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

PO6 Comunicar la Dirección y las Aspiraciones de la Gerencia

Objetivos de Control de Alto Nivel

P	efectividad
	eficiencia
	confidencialidad
	integridad
	disponibilidad
S	conformidad
	confiabilidad

Control sobre el proceso de TI de

comunicar la dirección y las aspiraciones de la gerencia

que satisface el requisito de negocio

garantizar el conocimiento del usuario y entendimiento de esos fines

es facilitado por

políticas establecidas y comunicadas a la comunidad de usuario; además, los estándares necesitan ser establecidos para traducir las opciones de estrategia en reglas de usuario que sean prácticas y útiles

y toma en consideración

- código de conducta/ética
- directrices de tecnología
- conformidad
- comisión de calidad
- políticas de seguridad
- políticas de control interno

X	personas
	aplicaciones
	tecnología
	facilidades
	datos

PO7 Administrar los Recursos Humanos

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

administrar los recursos humanos

que satisface el requisito de negocio

maximizar las contribuciones del personal a los procesos de TI

es facilitado por

técnicas firmes de gestión de personal

y toma en consideración

- refuerzo y promoción
- requisitos de calidad
- entrenamiento
- construcción del conocimiento
- cross training
- procedimientos libres
- evaluación de la ejecución objetiva y medible

X	personas
	aplicaciones

	tecnología
	facilidades
	datos

PO8 Asegurar el Cumplimiento de los Requisitos Externos

Objetivos de Control de Alto Nivel

P	efectividad
	eficiencia
	confidencialidad
	integridad
	disponibilidad
P	conformidad
S	confiabilidad

Control sobre el proceso de TI de

asegurar el cumplimiento de los requisitos externos

que satisface el requisito de negocio

encontrar obligaciones legales, contractuales y reguladas

es facilitado por

identificación y análisis de requisitos externos para su impacto en las TI, y toma de medidas apropiadas para llevar a cabo su cumplimiento.

y toma en consideración

- leyes, regulaciones y contratos
- monitorización legal y desarrollos regulados
- inspecciones regulares para cambios y mejoras
- búsqueda de consejos legales
- seguridad y ergonomía
- privacidad
- propiedad intelectual
- flujo de datos

X	personas
X	aplicaciones
	tecnología
	facilidades
X	datos

PO9 Evaluar los Riesgos

Objetivos de Control de Alto Nivel

S	efectividad
S	eficiencia
P	confidencialidad
P	integridad

P	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

evaluar los riesgos

que satisface el requisito de negocio

de asegurar la realización de los objetivos de TI y respondiendo a las amenazas para el suministro de los servicios de TI

es facilitado por

la organización se autocompromete en los riesgos de las TI identificando y analizando el impacto, y tomando medidas efectivas de costes para mitigar los riesgos

y toma en consideración

- diferentes tipos de riesgos de TI (tecnología, seguridad, continuidad, etc.)
- alcance: global o sistemas específicos
- evaluación de riesgos hasta la fecha
- metodología de análisis de riesgos
- medidas de riesgo cuantitativas y/o cualitativas
- plan de acción de riesgos

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

PO10 Administrar los Proyectos

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

administrar los proyectos

que satisface el requisito de negocio

establecer prioridades y salvar a tiempo, y dentro del presupuesto

es facilitado por

la organización identificando y dando prioridad a los proyectos en línea junto al plan operacional; además, la organización debería adoptar y aplicar técnicas de gestión de proyectos para cada uno

de los proyectos tomados.

y toma en consideración

- propiedad de proyectos
- complicación del usuario
- interrupción de tareas
- distribución de responsabilidades
- proyecto y fase de aprobación
- costes y presupuesto del personal
- planes de seguridad de la calidad y métodos

X	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

PO11 Administrar la Calidad

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
P	integridad
	disponibilidad
	conformidad
S	confiabilidad

Control sobre el proceso de TI de

administrar la calidad

que satisface el requisito de negocio

encontrar los requisitos individuales de las TI

es facilitado por

la planificación, implementación y mantenimiento de estándares de gestión de calidad y sistemas por la organización; además, la organización debería adoptar y aplicar una metodología que se suministrase para las distintas fases del desarrollo y pudiese prever fases claras y libres

y toma en consideración

- plan de estructura de la calidad
- responsabilidades de seguridad de la calidad
- metodología del ciclo de vida del desarrollo del sistemas
- programación y testeación de sistemas y documentación
- inspección de seguridad de la calidad e informes

X	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

Dominio de Adquisición & Implementación

AI1 Identificar Soluciones

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de
identificar soluciones

que satisface el requisito de negocio
de asegurar la mejor aproximación para satisfacer los requisitos del usuario

es facilitado por
un análisis claro de las oportunidades alternativas medidas contra los requisitos de usuario

y toma en consideración
- definición de la información de requisitos
- estudios factibles (costes, beneficios, alternativas, etc.)
- requisitos de usuario
- arquitectura de la información
- seguridad del coste-efectivo
- rastros de auditoría
- contratación externa
- aceptación de las facilidades y la tecnología

	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

AI2 Adquisición y Mantenimiento de Aplicaciones Software

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
S	integridad
	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

adquisición y mantenimiento de aplicaciones software

que satisface el requisito de negocio

suministrar funciones automáticas que soporten de forma efectiva los procesos de negocio

es facilitado por

la definición de estados específicos de los requisitos funcionales y operativos, y una implementación estructurada con dictámenes claros

y toma en consideración

- requisitos de usuario
- archivo, gasto, proceso y requisitos externos
- interfaz de la máquina-usuario
- embalajes habituales
- testeo funcional
- controles de aplicación y requisitos de seguridad
- documentación

	personas
X	aplicaciones
	tecnología
	facilidades
	datos

AI3 Adquisición y Mantenimiento de la Infraestructura de la Tecnología

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
S	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

adquisición y mantenimiento de la infraestructura de la tecnología

que satisface el requisito de negocio

suministrar las plataformas adecuadas para soportar las aplicaciones de negocios

es facilitado por

el asentamiento de la implantación de hardware y software, la provisión de mantenimiento del hardware preventivo, y la instalación, seguridad y control de los sistemas software

y toma en consideración

- asentamiento de la tecnología

- mantenimiento del hardware preventivo
- seguridad del sistema software, instalación, mantenimiento y cambio de controles

	personas
	aplicaciones
X	tecnología
	facilidades
	datos

AI4 Desarrollar y Mantener Procedimientos de TI

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
S	integridad
	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

desarrollar y mantener procedimientos de TI

que satisface el requisito de negocio

asegurar el uso apropiado de las aplicaciones y que las soluciones tecnológicas estén en su sitio

es facilitado por

una aproximación estructurada para el desarrollo de los usuarios y de los manuales de procedimiento de operaciones, requisitos de servicio y materiales de entrenamiento

y toma en consideración

- procedimientos de usuario y controles
- procedimientos operacionales y controles
- materiales de entrenamiento

X	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

AI5 Instalación y Acreditación de Sistemas

Objetivos de Control de Alto Nivel

P	efectividad
	eficiencia
	confidencialidad
S	integridad

S	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de
instalación y acreditación de sistemas

que satisface el requisito de negocio
verificar y confirmar que la solución es conveniente para los propósitos propuestos

es facilitado por
la realización de una migración de instalación bien formalizada, conversión y un plan aceptado

y toma en consideración
- entrenamiento
- datos carga/conversión
- testeos específicos
- acreditación
- inspecciones post-implementación

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

AI6 Gestión de Cambios

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
P	integridad
P	disponibilidad
	conformidad
S	confiabilidad

Control sobre el proceso de TI de
gestionar los cambios

que satisface el requisito de negocio
minimizar la posibilidad de ruptura, alteraciones no autorizadas, y errores

es facilitado por
un sistema de gestión que se suministre para el análisis, implementación y obtención de todos los cambios solicitados y realizados para las infraestructuras de TI existentes

y toma en consideración

- identificación de los cambios
- categorizar, priorizar y procedimientos de emergencia
- asentamiento de impactos
- cambio de autoridad
- gestión de venta
- distribución de software

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

Dominio de Entrega & Soporte

DS1 Definir Niveles de Servicio

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
S	confidencialidad
S	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

definir niveles de servicio

que satisface el requisito de negocio

establecer un entendimiento común del nivel de servicio requerido

es facilitado por

el establecimiento de un nivel de servicio conforme que formalice el criterio de realización en comparación con que la cantidad y calidad de servicio será medida

y toma en consideración

- acuerdos formales
- definición de responsabilidades
- tiempos de respuesta y volúmenes
- cobro
- garantías de integridad
- acuerdos no declarados

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

DS2 Gestionar los Servicios Prestados por Terceros

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
S	confidencialidad
S	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

gestionar los servicios prestados por terceros

que satisface el requisito de negocio

asegurar que las reglas y las responsabilidades de terceras partes están definidas de forma clara, adheridas y continuar satisfaciendo los requisitos

es facilitado por

medidas de control dirigidas en la inspección y monitorización de contratos existentes y procedimientos para su efectividad y conformidad con la política de la organización.

y toma en consideración

- acuerdos de servicio con terceras partes
- acuerdos no declarados
- requisitos legales y regulados
- monitorización del servicio entregado

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

DS3 Administrar el Cumplimiento y la Capacidad

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
	integridad
S	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

administrar el cumplimiento y la capacidad

que satisface el requisito de negocio

asegurar que la capacidad adecuada está disponible y que se está haciendo un uso óptimo y mejor para encontrar las necesidades de cumplimiento requeridas

es facilitado por

controles de gestión de capacidad y cumplimiento que coleccionen datos e informen en la gestión de trabajo, dimensionado de la aplicación, recursos y gestión demandada

y toma en consideración

- disponibilidad y cumplimiento de los requisitos
- monitorización e información
- herramientas de modelado
- gestión de la capacidad
- disponibilidad del recurso

	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

DS4 Asegurar el Servicio Continuo

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
	confidencialidad
	integridad
P	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

asegurar el servicio continuo

que satisface el requisito de negocio

hacer que los servicios de TI requeridos estén disponibles y asegurar un impacto de negocio mínimo en caso de una ruptura mayor

es facilitado por

posesión de un continuado y testeado plan de TI que esté en línea con la totalidad del plan continuo de negocio y con sus requisitos de negocio relacionados

y toma en consideración

- clasificación crítica
- plan documentado
- procedimientos alternativos
- copias de seguridad y recuperación
- análisis y entrenamiento regular y sistemático

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

DS5 Garantizar la Seguridad del Sistema

Objetivos de Control de Alto Nivel

	efectividad
	eficiencia
P	confidencialidad
P	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

garantizar la seguridad del sistema

que satisface el requisito de negocio

salvaguardar la información contra el uso no autorizado, descubrimiento o modificación, daño o pérdida

es facilitado por

controles de acceso lógico que aseguren que el acceso a los sistemas, datos y programas está restringido a los usuarios autorizados

y toma en consideración

- autorización
- autenticidad
- acceso
- uso de protección e identificación
- gestión de clave criptográfica
- incidencia de manejo, informar y completar
- camino custodiado
- detección y prevención de virus
- cortafuegos

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

DS6 Identificar y Atribuir Costes

Objetivos de Control de Alto Nivel

	efectividad
P	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
P	confiabilidad

Control sobre el proceso de TI de

identificar y atribuir costes

que satisface el requisito de negocio

asegurar un correcto conocimiento de los costes atribuidos a los servicios de TI

es facilitado por

un sistema de contabilidad de costes que asegure que dichos costes son registrados, calculados y localizados para el nivel de detalle requerido

y toma en consideración

- recursos identificables y medibles
- imposición de políticas y procedimientos
- imponer valores

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

DS7 Educar y Entrenar a los Usuarios

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

educar y entrenar a los usuarios

que satisface el requisito de negocio

asegurar que los usuarios son eficientes en el uso de la tecnología y que son conscientes de los riesgos y responsabilidades en las que están involucrados

es facilitado por
un entrenamiento comprensivo y un plan de desarrollo

y toma en consideración
- plan de estudios de entrenamiento
- campañas de conocimiento
- técnicas de conocimiento

X	personas
	aplicaciones
	tecnología
	facilidades
	datos

DS8 Asistencia y Consejo a los Clientes de TI

Objetivos de Control de Alto Nivel

P	efectividad
	eficiencia
	confidencialidad
	integridad
	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de
asistir y aconsejar a los clientes de TI

que satisface el requisito de negocio
asegurar que cualquier problema experimentado por el usuario será resuelto apropiadamente

es facilitado por
una fácil ayuda que suministre soporte de primer orden y consejo

y toma en consideración
- cuestiones del cliente y respuestas al problema
- monitorización de cuestiones y aclaraciones
- análisis de tendencias e información

X	personas
X	aplicaciones
	tecnología
	facilidades
	datos

DS9 Gestión de la Configuración

Objetivos de Control de Alto Nivel

P	efectividad
	eficiencia
	confidencialidad
	integridad
S	disponibilidad
	conformidad
S	confiabilidad

Control sobre el proceso de TI de

gestionar la configuración

que satisface el requisito de negocio

considerar todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proveer de un fundamento para una gestión de cambio firme

es facilitado por

controles que identifiquen y registren todos los medios de TI y su localización física, y un programa regular de verificación que confirme dicha existencia

y toma en consideración

- medios de registro
- gestión del cambio de configuración
- chequeo del software no autorizado
- controles de almacenamiento de software

	personas
X	aplicaciones
X	tecnología
X	facilidades
	datos

DS10 Gestión de Problemas e Incidentes

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
	integridad
S	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

gestionar los problemas e incidentes

que satisface el requisito de negocio

asegurar que los problemas e incidentes serán resueltos, e investigando la causa para prevenir una nueva aparición de estos

es facilitado por

una sistema de gestión de problemas que registre y avance todos los incidentes

y toma en consideración

- reglas suficientes de auditoría de problemas y soluciones
- resolución oportuna de problemas anunciados
- subida de procedimientos
- informes de incidentes

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

DS11 Gestión de Datos

Objetivos de Control de Alto Nivel

	efectividad
	eficiencia
	confidencialidad
P	integridad
	disponibilidad
	conformidad
P	confiabilidad

Control sobre el proceso de TI de

administrar los datos

que satisface el requisito de negocio

asegurar que los datos permanecen completos, correctos y válidos durante su introducción, actualización y almacenamiento

es facilitado por

una combinación efectiva de aplicación y controles generales sobre las operaciones de TI

y toma en consideración

- diseño del modelo
- controles de documentos fuente
- controles de entrada
- controles de proceso
- controles de salida
- identificación multimedia, mecanismo y gestión de biblioteca
- almacenamiento multimedia y gestión de copias de seguridad
- autenticidad e integridad

	personas
	aplicaciones
	tecnología
	facilidades
X	datos

DS12 Administrar las Instalaciones

Objetivos de Control de Alto Nivel

	efectividad
	eficiencia
	confidencialidad
P	integridad
P	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

administrar las instalaciones

que satisface el requisito de negocio

proveer de un medio físico apropiado que proteja el equipamiento de las TI y a las personas contra riesgos naturales y riesgos provocados por el hombre

es facilitado por

la instalación de controles físicos apropiados que son revisados regularmente para su propia función

y toma en consideración

- acceso a facilidades
- identificación de la situación
- seguridad física
- salud y seguridad del personal
- protección de amenazas del entorno

	personas
	aplicaciones
	tecnología
X	facilidades
	datos

DS13 Gestión de Operaciones

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
	confidencialidad
S	integridad

S	disponibilidad
	conformidad
	confiabilidad

Control sobre el proceso de TI de

gestionar las operaciones

que satisface el requisito de negocio

asegurar que las funciones importantes soportadas de las TI son realizadas regularmente y de una forma ordenada

es facilitado por

un planificador de actividades soportadas que es registrado y aclarado para el cumplimiento de todas las actividades

y toma en consideración

- manual de procedimiento de operaciones
- documentación del proceso puesto en marcha
- gestión de servicios de la red
- planificación del trabajo y el personal
- proceso cambiado
- registro del suceso del sistema

X	personas
X	aplicaciones
	tecnología
X	facilidades
X	datos

Dominio de Monitorización

M1 Monitorizar los Procesos

Objetivos de Control de Alto Nivel

P	efectividad
S	eficiencia
S	confidencialidad
S	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

monitorizar los procesos

que satisface el requisito de negocio

asegurar la realización de la ejecución de los objetivos establecidos para los procesos de las TI

es facilitado por

la definición de la administración del informe relevante de gestión e indicadores realizados, implementación de los sistemas soportados así como la aclaración del informe sobre los fundamentos regulares

y toma en consideración

- indicadores de realización de claves
- factores de sucesos crítico
- evaluaciones de la satisfacción del cliente
- informe de la gestión

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

M2 Evaluar lo Adecuado del Control Interno

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
S	confidencialidad
S	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

evaluar lo adecuado del control interno

que satisface el requisito de negocio

asegurar la realización de los objetivos de control internos establecidos para los procesos de las TI

es facilitado por

la comisión de la administración para monitorizar controles internos, fijando su efectividad, e informando de ellos con bases regulares

y toma en consideración

- monitorización de controles internos en proceso
- test de pruebas (benchmarks)
- informe de error y excepción
- autoevaluación
- informe de la administración

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

M3 Obtener Aseguramientos Independientes

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
S	confidencialidad
S	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de
obtener aseguramientos independientes

que satisface el requisito de negocio
incrementar la confianza y el cuidado entre la organización, los clientes, y los proveedores a terceros

es facilitado por
inspecciones de la seguridad independiente llevadas a cabo en intervalos regulares

y toma en consideración
- certificaciones/acreditaciones independientes
- evaluaciones de efectividad independientes
- seguridad independiente de conformidad con leyes y requisitos regulados
- seguridad independiente de conformidad con comisiones contractuales
- inspecciones a proveedores de servicios a terceros
- realización de inspecciones de seguridad por personal cualificado
- involucración de auditorías proactivas

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

M4 Suministrar una Auditoría Independiente

Objetivos de Control de Alto Nivel

P	efectividad
P	eficiencia
S	confidencialidad
S	integridad
S	disponibilidad
S	conformidad
S	confiabilidad

Control sobre el proceso de TI de

suministrar una auditoría independiente

que satisface el requisito de negocio

incrementar los niveles de confianza y beneficios desde el mejor consejo de práctica

es facilitado por

auditorías independientes llevadas a cabo en intervalos regulares

y toma en consideración

- independencia de las auditorías
- involucración de auditorías proactivas
- realización de auditorías por personal cualificado
- claridad de las decisiones y recomendaciones
- actividades continuas

X	personas
X	aplicaciones
X	tecnología
X	facilidades
X	datos

4.7. LECTURAS RECOMENDADAS

"Control Objetives for Information and Related Technology. 2º Edition". 1998. Information Systems Audit and Control Foundation. E-MAIL: research@isaca.org

"I.S.A.C.A. (Information Systems Audit and Control Association)", 1998. Información electrónica. Dirección: http://www.isaca.org

"COBIT 2º Edition Home" 1998. Información electrónica. Dirección: http://www.isaca.org/cobit.html

"COBIT 2º Edition Project Web Site" 1998. Información electrónica. Dirección: http://www.isaca.org/ct_proj.html

"COBIT 2º Edition Web Site (Downloads)" 1998. Información electrónica. Dirección: http://208.240.90.17/ct_dwnld.html

5. Vocabulario

A

activo, *3*: importe total de los valores, efectos, créditos y derechos que posee una persona o sociedad comercial.

C

contingencia, *4*: posibilidad de que una cosa suceda o no suceda. Riesgo.

confiabilidad*, 3*: fiabilidad, probabilidad de buen funcionamiento de una cosa.

confidencialidad*, 3*: calidad de confidencial. Que se hace o se dice en confidencia, que contiene una confidencia.

contramedida*, 11*: medida tomada para paliar o anular otra.

categorizar, 52: ordenar o clasificar por categorías.

D

disponibilidad*, 3*: propiedad de un sistema que representa la continuidad del servicio prestado.

E

efectividad*, 3*: calidad de efectivo.

eficiencia*, 3*: virtud y facultad para obtener un efecto determinado.

F

fiduciario*, 3*: que depende del crédito o confianza.

funcionalidad*, 3*: propiedad de lo que es funcional. Práctico, eficaz, utilitario.

I

integridad*, 3*: calidad de íntegro. De una perfecta probidad.

P

priorizar*, 52*: dar prioridad. Anterioridad de una cosa respecto a otra, en tiempo o en orden.

R

regulativo*, 24*: que regula. Ajustado y conforme a regla.

requerimiento, 3:requisito.Condición necesa- ria para hacer una cosa.

S

salvaguardar*, 5*: proteger. Registrar un conjunto de informaciones contenidas en la memoria del ordenador sobre un soporte magnético.

T

traslapar*, 30*: cubrir total o parcialmente una cosa.

V

vertebrar*, 21*: dar consistencia y estructura internas; dar organización y cohesión.

6. Bibliografía

Piattini Velthuis, Mario G.; Del Peso Navarro, Emilio. 1998. RA-MA. "*AUDITORÍA INFORMÁTICA. Un enfoque práctico*". E-MAIL: rama@arrakis.es

"COBIT. Control Objetives for Information and Related Technology. 2º Edition". 1998. Information Systems Audit and Control Foundation. E-MAIL: research@isaca.org

"I.S.A.C.A. (Information Systems Audit and Control Association)", 1998. Información electrónica. Dirección: http://www.isaca.org

"COBIT 2º Edition Home" 1998. Información electrónica. Dirección: http://www.isaca.org/cobit.html

"COBIT 2º Edition Project Web Site" 1998. Información electrónica. Dirección: http://www.isaca.org/ct_proj.html

"COBIT 2º Edition Web Site (Downloads)" 1998. Información electrónica. Dirección: http://208.240.90.17/ct_dwnld.html

"Canning College WEB Site", 1997. Dirección: http://www.canningcollege.wa.edu.au/reference.html

"Curtin University of Technology Library and Information Service WEB Site", 1998. Dirección: http://www.curtin.edu.au:80/curtin/library/findinfo/handouts/erefs.html