UNIVERSIDAD DE COSTA RICA
SEDE GUANACASTE

AUDITORÍA DE LA GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN

INFORMÁTICA EMPRESARIAL

Auditoría Informática
IF8200

PROFESOR

BAYRON ESPINOZA ORTIZ

GRUPO 1

II SEMESTRE, 2019

CONTENIDO

Introducción 1

1. Auditoria de la gestión de TI 2

Estructura Organizacional 2

Estructura de entrega de servicios de TI 3

Estructura de la Gestión de TI 4

Equipos de trabajo de las Tecnologías de la Información 4

Comité Ejecutivo 5

Comité Informático. 5

Comité de Dirección de TI 5

1.1 COBIT como marco de referencia para la Auditoría de TI 6

Marco de Referencia 6

Satisfacer las necesidades de las partes interesadas 7

Cubrir la empresa de extremo a extremo 9

Aplicar un marco de referencia único integrado 10

Hacer posible un enfoque holístico 11

Separar el gobierno de la gestión 12

Implementación 13

1.2 Iniciativas de la SUGEF 13

1.3 Iniciativas de Contraloría General de la República 14

1.4 Otras iniciativas 14

1.4.1 Sarbarnes Oxley 14

1.4.2 Basilea 2 ..... **¡Error! Marcador no definido.**

1.5 Auditando la gestión en TI 17

1.5.1 Puntos relevantes a evaluar. 18

Riesgos de la gestión de TI 18

Aspectos por evaluar en la gestión de TI 19

Referencias 21

INTRODUCCIÓN

La Auditoría Informática, como se ha mencionado antes, es un campo nuevo en los procesos de auditoría. Esto debido a la inclusión de las tecnologías de información en los procesos de las organizaciones para ser más competitivos en un mercado global cambiante.

Pero, al hablar de auditoría informática no solo nos referimos a los programas de computadora que se utilizan, o el código fuente. Más que analizar un código fuente que puede ser tedioso, se basa en otros aspectos que son, directa o indirectamente, relacionados a las tecnologías: la seguridad física, seguridad lógica, integridad de los datos, etc.

Uno de los aspectos que incluye la auditoría informática está gestión de las tecnologías de información y comunicación que se lleva a cabo en las empresas, una labor un poco menos técnica pero que concierne a temas importantes. La administración y gestión del recurso informático de manera efectiva y eficaz, así como los controles que la alta gerencia haya dispuesto para cumplir sus objetivos son temas que a la auditoría le importan.

En esta lección, nos centraremos en la Gestión de las Tecnologías de Información y Comunicación dentro de las organizaciones, qué puntos son importantes tomar en cuenta en una auditoría como esta, así como herramientas y buenas prácticas que nos ayudarán en la labor de verificación y análisis.

1. AUDITORIA DE LA GESTIÓN DE TI

En las organizaciones, es importante que el área, departamento o gerencia de TI esté organizado y esté alineado al negocio.

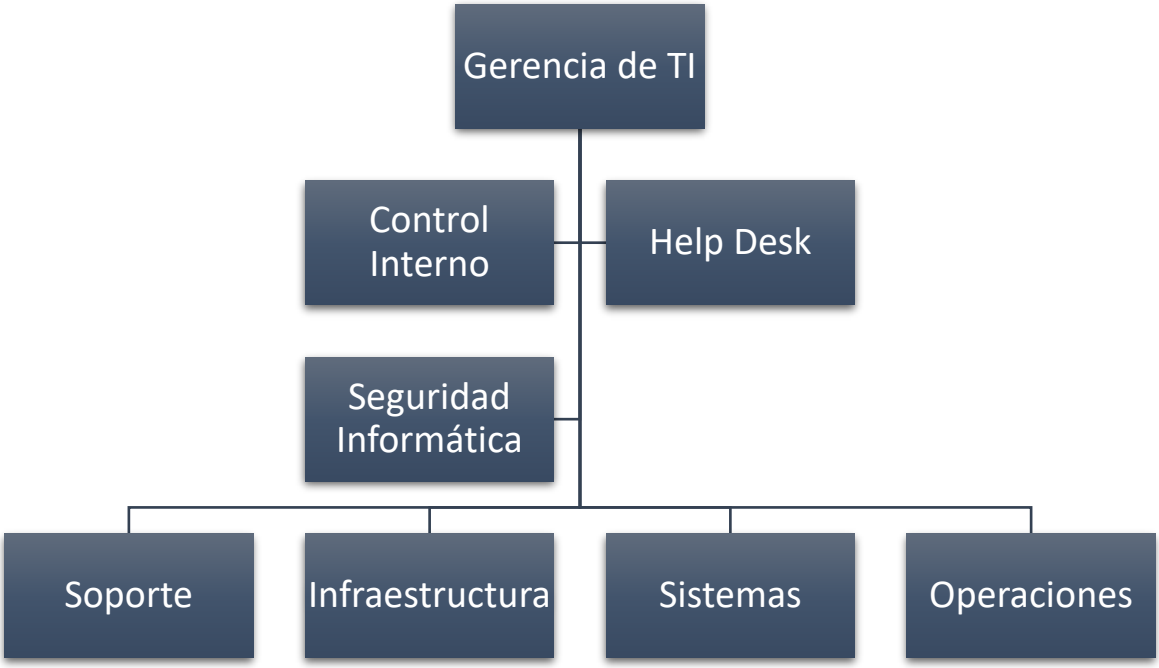
Se menciona **organizado** en todo el sentido: estructura, planificación, administración y gestión de los recursos informáticos y de personal.

Alineado al negocio porque el área de TI no es ajena a la organización y esta debe contribuir al cumplimiento de los objetivos organizacionales.

La Gestión de TI es el proceso de supervisión de todos los procesos que tienen relación con los recursos tecnológicos de información. Con ello, se asegura que los recursos sean utilizados eficiente y eficazmente para que proporcione valor a la organización. Las personas que trabajan en la gestión de las TI deben demostrar habilidades en áreas generales de la gestión: liderazgo, planificación estratégica y asignación de recursos.

Estructura Organizacional

Las TI deben, al menos, tener una estructura que cubra las necesidades de la organización.



Cabe mencionar que la anterior estructura no es obligatoria, sino una generalidad. Las secciones de Control Interno, Help Desk o Seguridad Informática son de staff, es decir, que ayudan o "colaboran directamente" con el gerente. Otras secciones es posible que estén unidas.

Teniendo esto en cuenta, TI presenta una estructura que puede soportar cualquier organización.

Estructura de entrega de servicios de TI

La Gestión en las Tecnologías de Información buscan disponer de una estructura adecuada de entrega de servicios de TI, de calidad y que cumplan con las necesidades manifestadas por el Negocio, misma que será llevada a

cabo como Proveedores de Servicios de TI a través de la combinación apropiada de Personas, Procesos y Tecnologías y Terceros.

Estructura de la Gestión de TI

Gestión	Desarrollo y mantenimiento de sistemas	Administración de Infraestructura	Servicio al cliente
Planificación	Nuevas funciones	Configuración	Solicitudes de servicio
Riesgos	Gestión de cambios	Operaciones	Incidentes/problemas
Control Interno		Desempeño y capacidad	Soporte
Calidad		Seguridad	Administración de proveedores
Desempeño			
Adquisiciones			

Equipos de trabajo de las Tecnologías de la Información

Para que el trabajo de la Gestión de las TI sea más eficiente, requiere de equipos interdisciplinarios en las organizaciones. De este modo, hay una mayor compresión del trabajo por parte de otras áreas y que colaboran en la priorización e influyen en la planificación de proyectos de TI.

Comité Ejecutivo

Lo preside el Gerente o Presidente (CEO) y los altos jerarcas. Ayuda a establecer y aprobar las estrategias corporativas, además que determina la estrategia de TI. El gerente o jefe de TI debe estar invitado en estas reuniones.

Comité Informático.

También llamado Comité de Estrategia de TI o Comité de TI. Este comité lo lidera el gerente o jefe de TI, además de los gerentes de altos rangos.

Acá conciernen temas para un buen Gobierno de TI, mediante:

- Principios básicos de gestión
- Políticas de inversión de TI
- Se priorizan las iniciativas y proyectos

Este comité informa mediante reportes al Comité Ejecutivo

Comité de Dirección de TI

En el Comité de Dirección de TI participan los responsables de las áreas de TI (encargados de áreas de la estructura) donde se realizan las tareas:

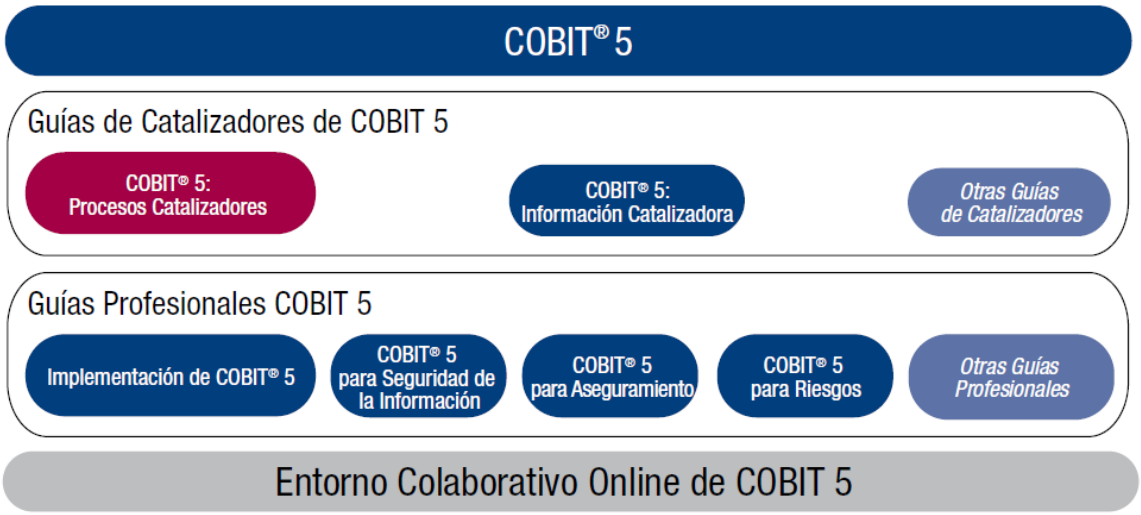
- Materialización de la estrategia de TI.
- Decisiones sobre la arquitectura de servicios.
- Manejo del portafolio de proyectos de TI.

1.1 COBIT como marco de referencia para la Auditoría de TI

El ***C****ontrol* ***Ob****jectives for* ***I****nformation and related* ***T****echnology* (Control de Objetivos para Tecnologías de Información y Relacionadas), conocido por sus siglas, COBIT, es un marco de referencia de mejores prácticas para el control y supervisión de las tecnologías de información. Es patrocinado por ISACA y el IT GI (IT Governance Institute) incluye una serie de herramientas, framework, objetivos de control y una serie guías que también pueden ser usados para la auditoría de tecnologías de información. Su más reciente versión es 5, llamada CobIT 5, que surge una serie de cambios respecto a sus antecesores.

Marco de Referencia

COBIT 5 provee un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos, para el gobierno y la gestión de las TI corporativas.



En síntesis: ayuda a las empresas a crear el valor óptimo desde TI, manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y uso de recursos.

Permite a las TI ser *gobernadas* y *gestionadas* de un modo holístico, abarcando al negocio completo de principio a fin y a las áreas funcionales de responsabilidad de TI, considerando los interesas relacionados con TI de las partes interesadas, internas y externas.

La siguiente figura, muestra los **principios** por los que se rige COBIT 5.

Satisfacer las necesidades de las partes interesadas

Las empresas existen para **crear valor** para sus partes interesadas, manteniendo el equilibrio entre la relación de beneficios y la optimización de los riesgos y el uso de recursos.

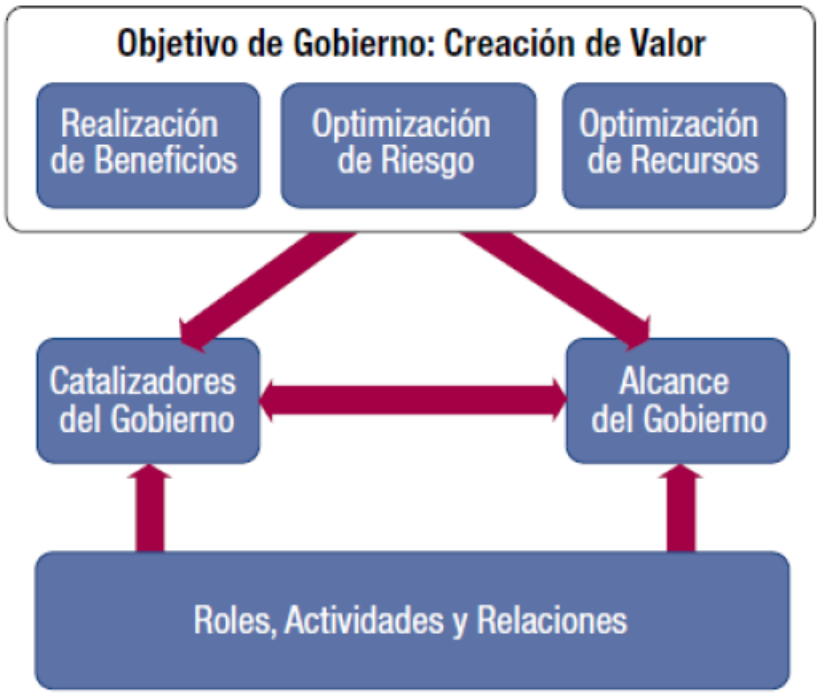
Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas.

Se realiza traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

Cubrir la empresa de extremo a extremo

COBIT 5 cubre todas las funciones y procesos dentro de la empresa y no solo se enfoca en "la función de TI", sino que trata la información y las tecnologías relacionadas como activos que deben ser tratado como cualquier otro activo en la empresa.

Considera que los catalizadores relacionados con TI para el Gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos, interno y externos, los que sean relevantes para el gobierno y la gestión de la información de la empresa y tecnologías de información relacionadas.

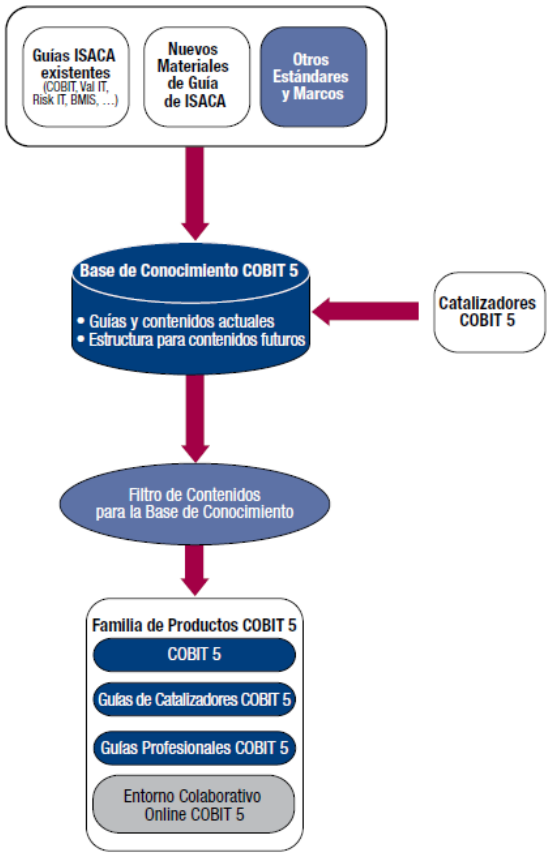


Aplicar un marco de referencia único integrado

Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI.

COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

Es completo en cuanto a la cobertura de la empresa, porque proporciona una base para integrar de manera efectiva otros marcos, estándares y buenas prácticas utilizadas, ejemplo: ISO/IEC 27000, ITIL, COSO, ISO 9001, etc.

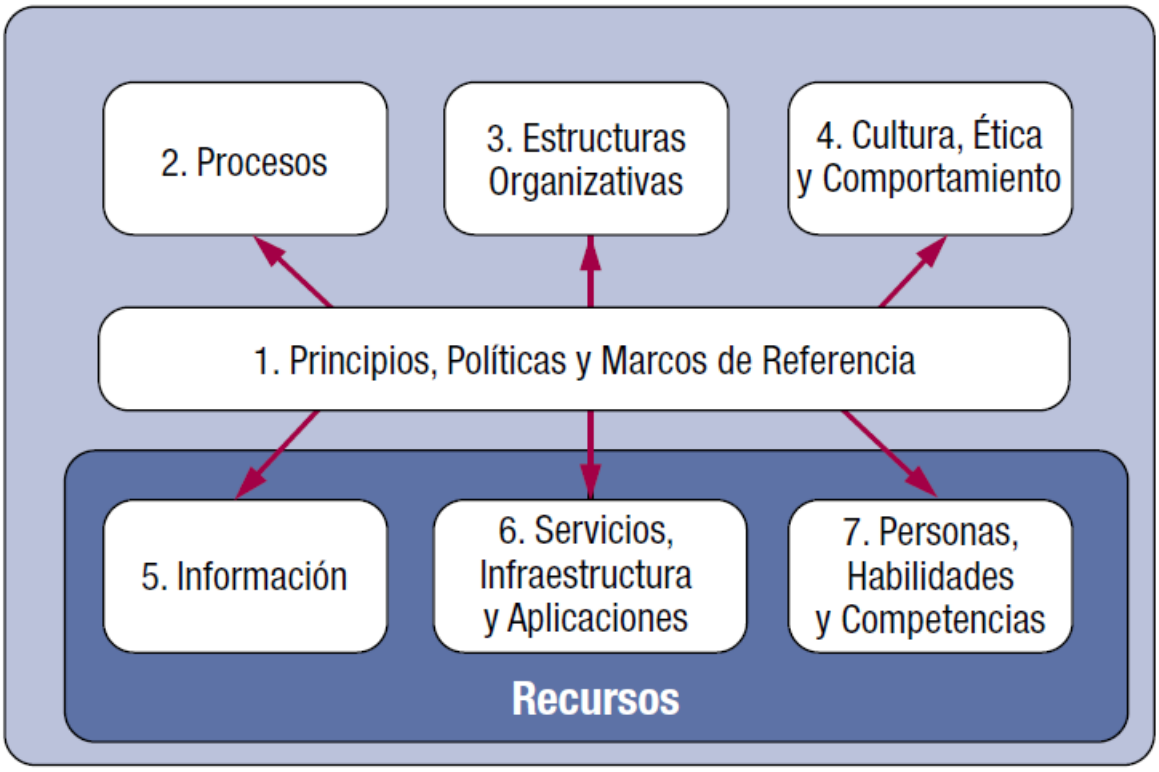


Hacer posible un enfoque holístico

Un gobierno y gestión de TI organizacional efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta componentes interactivos.

COBIT 5 define un conjunto de catalizadores (enablers) para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa.

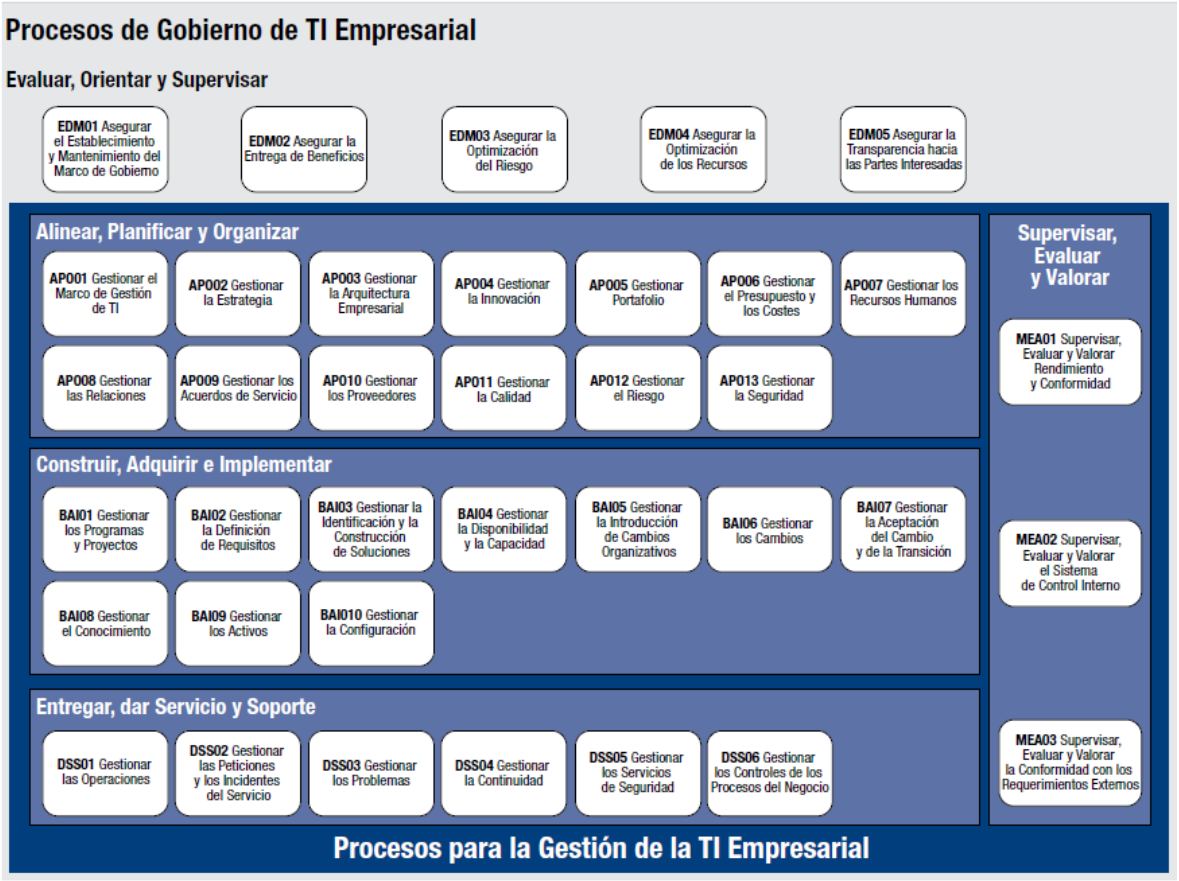
Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo COBIT 5 define 7 categorías de catalizadores/habilitadores.



Separar el gobierno de la gestión

El **gobierno** asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzas las metas corporativas equilibradas y acordadas, estableciendo la dirección a través de la priorización y la toma de decisiones y midiendo el rendimiento y cumplimiento respecto a la dirección y metas acordadas.

La **gestión** planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.



Implementación

ISACA proporciona amplias y prácticas guías de implementación en su publicación “COBIT5 implementación”, que está basada en un ciclo de vida de mejora continua para:

- Realizar un caso de negocio para la implementación y mejora del gobierno y gestión de TI.
- Reconocer los típicos puntos débiles y eventos desencadenantes.
- Crear el entorno apropiado para la implementación.
- Aprovechar COBIT para identificar carencias y guiar en el desarrollo de elementos facilitadores como políticas, procesos, principios, estructuras organizativas; y roles y responsabilidades.

1.2 Iniciativas de la SUGEF

Esta iniciativa corresponde al “Reglamento General de Gestión de la Tecnología de Información”, acuerdo de la Superintendencia de General de Entidades Financieras, acuerdo 14-17, publicado en el Alcance N° 80 del diario oficial La Gaceta N° 71 del 17 de abril de 2017.

El Artículo 1 “*establece los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense*.”

Así como la lista de tipos de entidades las cuales están obligadas a cumplirlo, que incluye SUGEF (Bancos y financieras), SUGEVAL (fondos de inversión y valores), SUGESE (aseguradoras) y SUPEN (sistemas de pensión). Todas las anteriores pertenecen al CONASSIF (Consejo Nacional de Supervisión del Sistema Financiero).

1.3 Iniciativas de Contraloría General de la República

La Contraloría General de la República, emitió en las ***"Normas técnicas para la gestión y el control de las Tecnologías de Información"***, documento **N-2-2007-CO-DFOE**, aprobados mediante Resolución del Despacho de la Contralora General de la República, Nro R-CO-26-2007 del 7 de junio, 2007 y que fue publicado en **La Gaceta Nro 119** del 21 de junio, 2007.

Esta normativa deroga el "Manual sobre normas técnicas de control interno a los sistemas de información computarizados", oficializado en febrero 1996.

1.4 Otras iniciativas

1.4.1 Sarbarnes Oxley

La iniciativa Sarbarnes Oxley se refiere a una ley de los Estados Unidos en respuesta a los sucesos de la corporación Enron y sus subsidiarias, Tyco

International, WorldCom y Peregrine System. Dichos escándalos dieron una mala imagen a los sistemas de contabilidad y de auditoría.

Esta establece nuevos estándares para los concejos de administración y dirección, así como los mecanismos contables a todas las empresas que cotizan en bolsa en los EE.UU. También introduce responsabilidades penales para los consejos de administración y establece una comisión reguladora de mercado de valores.

Puntos introducidos por la Ley Sarbanes-Oxley

- La creación del "Public Company Accounting Oversight Board" (Comisión encargada de supervisar las auditorías de las compañías que cotizan en bolsa).
- El requerimiento de que las compañías que cotizan en bolsa garanticen la veracidad de las evaluaciones de sus controles internos en el informe financiero, así como que los auditores independientes de estas compañías constaten esta transparencia y veracidad.
- Certificación de los informes financieros, por parte del comité ejecutivo y financiero de la empresa.
- Independencia de la empresa auditora.
- El requerimiento de que las compañías que cotizan en bolsa tengan un comité de auditores completamente independientes, que supervisen la relación entre la compañía y su auditoría. Este comité de auditores pertenece a la compañía, no obstante los miembros que

lo forman son completamente independientes a la misma. Esto implica que sobre los miembros, que forman el comité de auditores, recae la responsabilidad confirmar la independencia.

- Prohibición de préstamos personales a directores y ejecutivos.
- Trasparencia de la información de acciones y opciones, de la compañía en cuestión, que puedan tener los directivos, ejecutivos y empleados claves de la compañía y consorcios, en el caso de que posean más de un 10% de acciones de la compañía. Asimismo estos datos deben estar reflejados en los informes de las compañías.
- Endurecimiento de la responsabilidad civil así como las penas, ante el incumplimiento de la Ley. Se alargan las penas de prisión, así como las multas a los altos ejecutivos que incumplen y/o permiten el incumplimiento de las exigencias en lo referente al informe financiero.
- Protecciones a los empleados caso de fraude corporativo. La OSHA (Oficina de Empleo y Salud) se encargará en menos de 90 días, reinsertar al trabajador, se establece una indemnización por daños, la devolución del dinero defraudado, los gastos en pleitos legales y otros costes.

1.4.2 Basilea 2

Nuevo Acuerdo de Capital emitido por el Comité de Basilea que debe comenzar aplicarse a fines de 2006 y 2007 oficialmente y en prueba a partir de 2006 por los Bancos que indiquen los Bancos Centrales que adhieran al mismo.

Este comité tiene sede en la ciudad Suiza del mismo nombre y funciona en el edificio del Bank for International Settlements (BIS). El Comité de Basilea es también conocido como el «Banco Central de los Bancos Centrales» porque está integrado por representantes de los Bancos Centrales de más de 100 países miembros, entre ellos el Banco Central de Costa Rica. Debe aclararse que Basilea emite recomendaciones que orientan pero que no son obligagtorias para los Supervisores Bancarios (léase bancos centrales) de cada país.

Entre los objetivos que persigue Basilea II se destacan:

- Perfeccionar el acuerdo anterior;
- Promover la seguridad y la salud de los sistemas financieros;
- Fomentar la competencia en igualdad de condiciones;
- Definición de capitales mínimos regulados en base a criterios más sensibles al riesgo;
- Mejora en performance de los procesos bancarios: eficiencia;
- Mejorar la supervisión bancaria (a través de los Bancos Centrales);
- Transparencia en las informaciones.

1.5 Auditando la gestión en TI

De acuerdo a los puntos anteriores, es importante evaluar la gestión de las TI, con el fin de que las labores y esfuerzos, así como los proyectos y estructura de TI estén acordes a los objetivos de la organización.

1.5.1 Puntos relevantes a evaluar.

Antes de mostrar los puntos relevantes a evaluar, es importante destacar en primer lugar los riesgos asociados a la Gestión de las TI.

Riesgos de la gestión de TI

A continuación, una lista de riesgos de la gestión de TI

- La estructura no ha sido aceptada por el negocio y los procesos de TI no se relacionan con los requerimientos del negocio
- Estructura de los procesos de TI incompletos.
- Conflictos e interdependencias entre los procesos poco claros
- Traslapes entre actividades
- Organización de TI inflexible
- Brechas entre procesos
- Duplicación de procesos
- Falta de compromiso de la administración superior
- Los recursos de TI no soportan efectivamente al negocio
- TI no le da la suficiente importancia a la estrategia
- TI se mantiene como un área separada del negocio
- Ausencia de dirección del negocio
- Falta de comunicación de las iniciativas del negocio
- Soporte al negocio insuficiente
- Requerimientos no están claros
- Estrategias de adquisición inadecuadas
- Inflexibilidad de TI para cambios en las necesidades del Negocio
- No hay cumplimiento de las regulaciones
- Información comprometida
- El reclutamiento no funciona según lo requerido
- Uso de sistemas fraudulentos

- Falta de respuesta de TI hacia la organización
- Daño a la imagen del negocio (mala reputación)
- Riesgos relacionados con la calidad no detectados que impactan al negocio
- Incremento de costos retrasos debido a un control pobre sobre calidad
- Aseguramiento de calidad no aplicado
- Inconsistencias en la calidad a través de la organización
- Desempeño del negocio reducido

Aspectos por evaluar en la gestión de TI

Aspectos a considerar en la auditoría sobre la estrategia de TI:

Disponer de la siguiente información:

- Lineamientos asociados a la gestión de TI
- Diseño de estructura organizacional
- Perfiles de puesto
- Descripción de procesos y funciones

Aspectos a considerar en la auditoría sobre la estrategia de TI:

Evaluar:

- Existencia lineamientos formales y comunicados para la gestión de TI
- Ubicación en la organización que le facilite la independencia en la entrega de servicios

- Una estructura acorde a los servicios y requerimientos de la organización

Roles y responsabilidades claramente establecidos

REFERENCIAS

Foro de Seguridad. (s.f.). *Conozca la ley Sarbanes-Oxley.* Obtenido de Foro de Seguridad: http://www.forodeseguridad.com/artic/segcorp/7217.htm

ISACA. (2012). *COBIT® 5.* Obtenido de ISACA Chapter Costa Rica: www.isaca.org

Svarzman, M. (1 de agosto de 2004). *Basilea II: un gran incentivo a la gestión de riesgos.* Obtenido de Basilea 2: http://www.basilea2.com.ar/Articulos.asp?id=1

techtarget.com. (agosto de 2014). *Gestión de TI.* Obtenido de Tech Target: https://searchdatacenter.techtarget.com/es/definicion/Gestion-de-TI