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

PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

Ana Virginia Pérez Girón
Asesorada por la Inga. Ada Luz García Colindres

Guatemala, noviembre de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ANA VIRGINIA PÉREZ GIRÓN
ASESORADA POR LA INGA. ADA LUZ GARCÍA COLINDRES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERA EN CIENCIAS Y SISTEMAS

GUATEMALA, NOVIEMBRE DE 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Edgar Estuardo Santos Sutuj
EXAMINADOR	Ing. José Alfredo González Cosenza
EXAMINADOR	Ing. Marlon Francisco Orellana López
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

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

PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha agosto de 2013.

Ana Virginia Pérez Girón

Guatemala, Octubre 28 de 2013

Ingeniero
Carlos Alfredo Azurdia Morales
Coordinador de Privados y Revisión de Tesis
Escuela de Ciencias y Sistemas

Estimado Ingeniero:

Por medio de la presente, me permito informarle que he asesorado el trabajo de graduación titulado: **PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN,** elaborado por la estudiante Ana Virginia Pérez Girón, a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo.

Agradeciéndole de antemano la atención que le preste a la presente, me suscribo de usted,

Atentamente,

Inga. Ada Luz García Colindres

Ada Luz García Colindres
ING. EN CIENCIAS Y SISTEMAS
Colegiado No. 8199

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

Guatemala, 6 de Noviembre de 2013

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

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación de la estudiante **ANA VIRGINIA PÉREZ GIRÓN,** con carné **95-16345,** titulado: **"PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

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

Atentamente,

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

ESCUELA DE CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN",*** *realizado por la estudiante ANA VIRGINIA PÉREZ GIRÓN, aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

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

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

Guatemala, 25 de noviembre 2013

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.841-2013

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ciencias y Sistemas, al trabajo de graduación titulado: **PRÁCTICAS INTERNACIONALES PARA LA AUDITORÍA DE GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN,** presentado por la estudiante universitaria: **Ana Virginia Pérez Girón,** procede a la autorización para la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

DECANO
FACULTAD DE INGENIERIA

Guatemala, noviembre de 2013

/cc

ACTO QUE DEDICO A:

Dios	Por su infinita bondad y amor, al haberme permitido lograr mis objetivos.
María Santísima	Quien me ha acompañado e iluminado en cada decisión que he tomado en mi vida.
Mi madre	Eluvia Girón Figueroa, por todo el amor y apoyo incondicional que me ha brindado a lo largo de mi vida; gracias a ella soy lo que soy.
Mi hermano	Marco Antonio Pérez Girón, quien siempre ha estado acompañándome para poder alcanzar mis metas.
Mi familia	Tíos, tías, primos y primas; uno de los mejores regalos de Dios para mi vida.
Mis amigos	Por su amistad y por tantos buenos momentos compartidos.
Mi asesora	Ada Luz García, por todo el apoyo brindado; por su tiempo y guía permanente para poder desarrollar este trabajo.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Base de datos Es una colección de información organizada de forma que un programa de ordenador pueda seleccionar rápidamente los fragmentos de datos que necesite.

Firewall Es un sistema de defensa basado en el hecho de que todo el tráfico de entrada o salida a la red debe pasar obligatoriamente por un sistema de seguridad capaz de autorizar, denegar, y tomar nota de todo aquello que ocurre, de acuerdo con una política de control de acceso entre redes.

Framework Es una estructura conceptual y tecnológica de soporte definido, normalmente con artefactos o módulos de software concretos, que puede servir de base para la organización y desarrollo de software.

Gateway Es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación.

Gobierno de TI Ayuda a garantizar que la TI soporte las metas del negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociados a la TI.

Granja de servidores	Formado por un grupo de servidores interconectados que a su vez actúan como un único servidor.
Hardware	Engloba a todos los componentes de un ordenador, significando entonces todas las partes duras y físicas que se encuentran en un equipo.
Log	Es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué un evento ocurre para un dispositivo en particular o aplicación.
Mesa de servicio	La principal función es brindar un soporte a los usuarios en relación con los requerimientos de ayuda, en la utilización de servicios computacionales.
Outsourcing	La subcontratación, externalización o tercerización (del inglés *outsourcing*) es el proceso económico en el cual una empresa mueve o destina los recursos orientados a cumplir ciertas tareas hacia una empresa externa por medio de un contrato.
Proxy	Es un equipo intermediario situado entre el sistema del usuario e internet.
Red	Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos

Router	Su función principal consiste en enviar paquetes de datos de una red a otra.
Servidor	Suelen utilizarse para almacenar archivos digitales. Los usuarios, por lo tanto, se conectan a través de la red con el servidor y acceden a dicha información.
Sistema operativo	Es el software básico de una computadora que provee una interfaz entre el resto de programas del ordenador, los dispositivos de hardware y el usuario.
Software	Programas o aplicaciones instaladas en una computadora que tienen una funcionalidad específica y ayuda al usuario a interactuar con el computador.
TI	Siglas utilizadas para resumir la palabra tecnología de la información.
TIC	Siglas utilizadas para resumir la palabra tecnología de la información y la comunicación.
VPN	Es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada como internet.

RESUMEN

Hoy en día uno de los activos más importantes para una organización es la tecnología y su información, por lo que es necesario protegerla y administrar los riesgos de múltiples intrusos o problemas internos; para ello existe una serie de estándares, protocolos, métodos, reglas, herramientas y políticas, para minimizar los posibles riesgos que afecten a la organización.

Los estándares fueron creados para la administración de las tecnologías de la información con el propósito de crear un conjunto de herramientas de apoyo que permita a los administradores cerrar la brecha existente entre requerimientos de control, cuestiones técnicas y riesgos del negocio.

Es prioridad asegurar la información que abarca software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore como activo y signifique un riesgo si esta información llega a perderse o bien no está disponible en el momento de tomar decisiones importantes para la organización. Por lo que es necesario incluir dentro de la corporación una auditoría informática que evalúe constantemente la gestión de los sistemas, redes de comunicaciones, servidores y posterior a ello, describa las vulnerabilidades que se encuentren en dichas revisiones.

Las auditorías de sistemas de información permiten conocer en el momento de su realización cuál es la situación exacta de los activos de información en cuanto a protección, control y medidas de seguridad.

Un buen sistema de gestión de información de sistemas es para una organización el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, minimizando a la vez los riesgos de seguridad de la información.

OBJETIVOS

General

Proveer a los auditores de tecnología de la información, lineamientos con base en prácticas internacionales, para la realización de una auditoría de gestión a las tecnologías de información.

Específicos

1. Mejorar el proceso de evaluación de la gestión informática con base en estándares internacionales en los diversos tipos de organizaciones, siendo este, el primer paso para que se pueda realizar una planificación estratégica de tecnología de información, integrada a las demás funciones de la organización.

2. Proponer una metodología alineada a los estándares internacionales más importantes para la auditoría de la gestión de las tecnologías de información y mejorar el proceso general de la auditoría, enlazándola e integrándola con estándares internacionales, de manera que se logren evaluaciones integrales mucho más acertadas y se contribuya al logro de los objetivos organizacionales.

INTRODUCCIÓN

Hoy en día una de las mayores preocupaciones de las organizaciones es la implementación de tecnologías de información, probablemente es porque no ven que las inversiones realizadas den soluciones inmediatas, tangibles y medibles; y allí donde se veía una oportunidad de mejora, realmente están creando un problema difícil de administrar, controlar y caro de mantener.

La auditoría informática se constituye en una herramienta que gestiona la tecnología de la información en las organizaciones. A través de auditorías informáticas se pretende medir los riesgos y evaluar los controles en el uso de las tecnologías de información, haciendo uso de estándares internacionales, técnicas y estrategias de análisis, que permitan que la auditoría informática se convierta en una real y eficiente herramienta de gestión de tecnologías de información, a beneficio de la organización.

Los estándares internacionales para la gestión de la tecnología de la información son guías generales dictadas por expertos en tecnología, con el objetivo de promover una buena administración de los recursos de la organización en un marco adecuado en la estructura del control interno. Estas normas establecen las pautas básicas y guían el accionar de los altos directivos que dirigen las organizaciones.

1. AUDITORÍA Y GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

La auditoría de gestión a las tecnologías de información y comunicaciones, consiste en el examen de carácter objetivo (independiente), crítico (evidencia), sistemático (normas) y selectivo (muestral) de las políticas, normas, funciones, actividades, procesos e informes de una entidad, con el fin de emitir una opinión profesional (imparcial) con respecto a :eficiencia en el uso de los recursos informáticos, validez y oportunidad de la información, efectividad de los controles establecidos y la optimización de los recursos tecnológicos."[1]

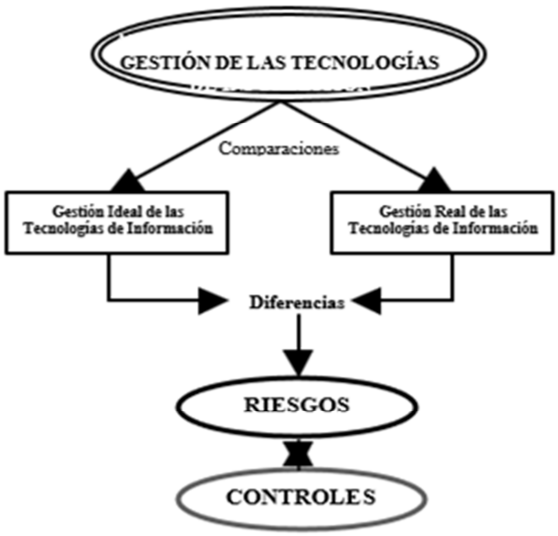
Este enfoque es totalmente compatible con las prácticas y controles contenidos en COBIT, ITIL, estándares de seguridad de la información (ISO 27000) entre otros, que hacen referencia a las pistas de auditoría en los sistemas informáticos, controles de acceso a los sistemas, bases de datos, áreas de tecnología de la información y comunicaciones (TIC´s) área de servidores, codificación de la información, prevención de virus, fraude, detección y mitigación de intrusos, entre otros; estos estándares no proporcionan un criterio legal aplicable si no han sido adoptados por la entidad, pero sí procedimientos de auditoría para examinar la gestión tecnológica en las diferentes organizaciones.

La tecnología de la información ayudada por los distintos estándares, permite identificar riesgos y controles para brindar apoyo al logro de los

[1]http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf. Consulta: 5 de agosto de 2013.

objetivos de la organización, para el cumplimiento de sus metas estratégicas, como se muestra en la siguiente figura.

Figura 1. **Esquema de auditoría informática de la gestión de tecnologías de la información**



Fuente:http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf. Consulta: agosto de 2013.

1.1. Objetivos de la auditoría de gestión de las tecnologías de la información

- Objetivo general: evaluar la eficiencia, efectividad y confiabilidad de la información, para la toma de decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación."[2]

[2]http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf. Consulta: 8 de agosto de 2013.

- Objetivos específicos:

    - Asegurar la integridad, confidencialidad, confiabilidad y oportunidad de la información.

    - Minimizar existencias de riesgos en el uso de tecnología de información en los procesos sistematizados.

    - Conocer la situación actual del área informática para el logro de objetivos estratégicos y operativos de la institución.

    - Apoyar al área de tecnología de información y comunicaciones y a las metas y objetivos de la organización.

    - Asegurar la utilidad, confianza, privacidad y disponibilidad en el ambiente tecnológico.

1.2. Definición del problema

Las organizaciones inician grandes inversiones en tecnología de información numerosas veces, sin evaluar el impacto que realmente tienen en la generación de valor de las mismas. Existen estándares de calidad que han sido propuestos por entidades a nivel mundial.

Estas normas ilustran de manera amplia y ordenada sobre los elementos que se deben tener en cuenta para una adecuada gestión informática. Estas normas no orientan de manera específica sobre los procedimientos a seguir, para una evaluación integral de la gestión informática orientada al logro de los objetivos de un plan estratégico organizacional.

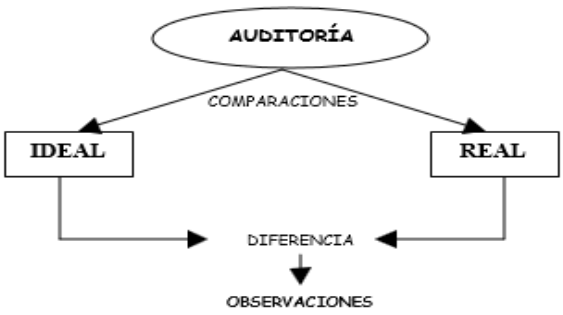
Las normas se miden sobre la base de indicadores de gestión y resultados a alcanzar establecidos para toda la organización, lo que sería el primer paso a seguir, si se quiere lograr una planificación estratégica de la tecnología de información, orientada hacia el logro de los objetivos organizacionales.

1.3. Definición de términos

A continuación se definirá una serie de términos importantes para la correcta comprensión del documento como: auditoría, auditoría de sistemas, riesgo, control, control interno informático, hallazgo, evaluación del proceso de software, metodología, proceso, proceso de software y tecnología de información.

- Auditoría: es la actividad que consiste en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y cumple las condiciones que le han sido prescritas.

Figura 2. **Esquema del concepto clásico de auditoría**



Fuente: elaboración propia.

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

- Riesgo: se define como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

- Control: establece medidas implementadas en las entidades con la finalidad de reducir los riesgos existentes y proteger los activos más importantes para la organización.

- Control interno informático: es el que 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. 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.

- Hallazgo: es el resultado de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría. Los hallazgos de auditoría pueden indicar tanto conformidad o no conformidad con los criterios de auditoría como oportunidades de mejora.

- Evaluación del proceso del software: la medición permite que se mejoren los procesos del software, la planificación, seguimiento y control de un proyecto de software; así como evaluar la calidad del producto que se produce. Las medidas de los atributos del proyecto y del producto se utilizan para calcular las métricas del software, las cuales se pueden analizar para proporcionar indicadores que guían acciones de gestión y técnicas.

- Metodología: la metodología hace referencia al conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen en una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos.

- Proceso: es un conjunto de prácticas relacionadas entre sí, llevadas a cabo a través de roles y por elementos automatizados, que utilizando recursos y a partir de insumos producen un satisfactor de negocio para el cliente.

- Proceso de software: es un conjunto de actividades, métodos, prácticas y transformaciones que los profesionales usan para desarrollar y mantener software y los productos asociados (por ejemplo: planes de proyecto, documentos de diseño, código, casos de prueba, y manuales de usuario).

- Tecnología de la información: comprende tanto al hardware de computadoras, redes y comunicaciones, así como al software de base (sistemas operativos, servidores proxy, manejadores de bases de datos, servidores web, etc.) y los sistemas de información (sistemas que soportan procesos relacionados con el manejo de la información en las organizaciones), así como los servicios relacionados, que se usan en las

organizaciones para el logro de sus objetivos, tanto dentro de ellas como en sus interrelaciones con otros miembros de las cadenas de suministros con las cuales realizan transacciones.

1.4. Gestión de la tecnología de la información

Consiste en la aplicación de los procesos de la administración (planificación, ejecución, seguimiento y control) a los diversos aspectos que tienen relación con los bienes y servicios de tecnología de información, incluyendo los siguientes aspectos:

- Gestión de procesos que tienen que ver con la infraestructura de tecnología de información
- Gestión de proyectos de infraestructura de tecnología de información
- Gestión de proyectos de desarrollo de sistemas de información
- Gestión de requerimientos relacionados con los sistemas de información en producción.

La gestión de la tecnología de la información se lleva a cabo mediante la adopción de buenas prácticas, ampliamente usadas, que proceden de diversas fuentes como son los estándares ISO 9000, 27001, COBIT, ITIL, entre otros.

El control interno informático debe estar comprendido dentro de las labores del área encargada de la gestión de tecnología de información, examinando diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares, y normas fijadas por la dirección de organización y/o la dirección de informática, así como los requerimientos legales.

1.4.1. Problemas en la gestión de la tecnología de la información

En la actualidad existe un alto índice de proyectos tecnológicos que fracasan, debido a la mala dirección de los responsables pues pierden el objetivo del proyecto. El éxito de un proyecto suele ser muy simple: lograr la satisfacción del cliente finalizando el proyecto a tiempo y dentro del presupuesto inicialmente previsto. Sin embargo, en la práctica, los problemas a los que se enfrenta el responsable del proyecto cuando intenta cumplir con estos requisitos son complejos.

A continuación se dan a conocer los inconvenientes que un directivo de Tecnología de la Información puede enfrentar durante su administración para evitar su fracaso.

- Problemática de los proyectos tecnológicos: la falta de planeación, el inadecuado dimensionamiento, costos y tiempos subestimados en un proyecto de tecnología, se convierten en los grandes impedimentos al momento de su implementación.

- Control y gestión de proyectos tecnológicos: el objetivo de la gestión tecnológica se centra en el desarrollo de destrezas y herramientas para la adquisición y generación continua de conocimientos dentro de la organización. Para lo cual es necesario crear capacidades específicas en**:**

    - Adquisición de datos
    - Procesamiento y análisis de los datos adquiridos
    - Difusión interna de conocimiento

- Conservación de la información: estas capacidades requieren de la creación de determinadas condiciones de índole organizativas y operativas, dirigidas a crear un ambiente organizacional que estimule la creatividad y la incorporación de personal idóneo con las herramientas de trabajo necesarias para el desempeño de sus funciones. La gestión tecnológica en busca de un mejor desempeño se apoya en las cuatro funciones gerenciales**:** planeación, organización, dirección y control.

La correcta utilización de estas funciones facilitará la dirección del crecimiento tecnológico de la organización. Las principales causas por las que fracasan los proyectos tecnológicos se muestran en la siguiente tabla.

Tabla I. **Factores de falla o cancelación en los proyectos**

Factores de daño o cancelación	**Porcentaje (%)**
Requerimientos incompletos	13,1
Deficiencia en el involucramiento del usuario	12,4
Deficiencia de recursos	10,6
Expectativas no realistas	9,9
Deficiencia en soporte ejecutivo	9,3
Cambios en los requerimientos y especificaciones	8,7
Deficiencia en la planeación	8,1
Ya no se necesita más	7,5
Deficiencia en administración de TI	6,2
Desconocimiento en tecnología	4,3
Otros	9,9

Fuente: www.acis.org.co/fileadmin/Articulos/Andres_Salinas.pdf.
Consulta: agosto de 2013.

Según investigaciones realizadas, los factores que llevan al fracaso un proyecto tecnológico son los siguientes:

- Falta de compromiso con el proyecto, en el establecimiento de cronogramas, presupuestos y objetivo de desempeño técnicos.

- Falta de retroalimentación de la organización patrocinadora.

- Falta de retroalimentación por parte del cliente.

- Estructura de la organización adecuada al equipo del proyecto.

- Participación del equipo del proyecto en la determinación del cronograma y los presupuestos.

- Entusiasmo del patrocinador.

- Procedimiento de control adecuado, especialmente en relación con los cambios.

A continuación se describen algunos de los obstáculos y las posibles soluciones que deben tenerse en cuenta, durante el desarrollo de proyectos tecnológicos:

- Conocimiento del negocio: el no conocer del negocio es uno de los mayores problemas en el inicio de un proyecto de tecnología. El equipo de trabajo debe conocer el funcionamiento de la empresa, ya que es indispensable saber cómo funciona y cuáles son sus procesos; todo esto debe ser analizado detenidamente antes de iniciar con el desarrollo de un

proyecto tecnológico. Uno de los factores del éxito de un proyecto es que el equipo de trabajo esté conformado por personas que conozcan el funcionamiento de la empresa y los procesos que van a ser sistematizados, sin importar que desconozcan las herramientas tecnológicas; de este modo evitarán llegar al fracaso. El conocedor del negocio debe ser parte de los líderes del proyecto.

- Conocimiento de los objetivos específicos: los líderes y miembros del equipo deben de tener una idea clara del objetivo del proyecto, saber cómo debe de operar el negocio una vez culmine el desarrollo del proyecto y qué cambios benéficos se verán en la empresa. Los líderes del proyecto deben de estar preparados tanto en el tema técnico como en lo administrativo, calcular el costo del inicio del proyecto y el costo que se tendrá si no se llegara a terminar con éxito.

- Es importante que todo el equipo comprenda las consecuencias que se tendrán para la empresa y el grupo, en caso de que el proyecto llegara a fallar. Para evitar confusiones se debe de tener identificado cada grupo de trabajo y su participación en el resultado del proyecto, preparar reuniones con ellos, con el fin de explicar el objetivo y las herramientas para lograrlo. Se debe vender una visión del futuro deseado para la organización al culminar el proyecto.

- Resistencia al cambio y desestimación: siempre existirán usuarios que se resistan al cambio en todos los niveles de la organización; esto debido a las malas experiencias que se han afrontado en proyectos pasados, pues no se consiguieron los resultados que se esperaban. La comparación entre el sistema tecnológico antiguo y el nuevo, puede hacer que los usuarios finales estén en contra del nuevo sistema al primer fallo que

ocurra. Un cambio exitoso requiere de líderes de proyecto con iniciativa y sean firmes con la gente que no pone de su parte para lograr que el proyecto sea un éxito.

- Para evitar la desestimación del proyecto, el directivo de tecnología de información debe comprender lo que se requiere para la realización del proyecto, y de ser necesario, revisar y ajustar las metas, analizar los requerimientos solicitados y el equipo de trabajo, con el fin de asegurarse que las personas están enfocadas en los resultados del negocio y no se conformen simplemente con que el sistema funcione.

- Equipo de trabajo y sobrecarga: las condiciones del equipo de trabajo y sobrecarga son las más difíciles de manejar, ya que se dan casi siempre en la mitad o por finalizar el proyecto; es por ello que se debe asegurar que el equipo de trabajo tenga la gente adecuada con el conocimiento necesario, tanto administrativo como operativo. En ciertos casos es necesario contratar temporalmente personal experto, que oriente al grupo de trabajo en los vacíos que posee. Tener credibilidad y claridad sobre lo que se está realizando fortalece el proyecto y ante las falencias, capacitar al grupo de trabajo no es un error, es una ganancia oculta.

- Para manejar la sobrecarga de trabajo, es necesario encontrar alternativas y establecer prioridades, haciendo ver que los requerimientos que no fueron dados a tiempo, deben esperar a una segunda fase del proyecto. De no ser posible, es necesario exponer de manera escrita los nuevos requerimientos, dejando indicado que lo solicitado no fue incluido dentro del plan inicial y modificar las fechas de entrega, sin alterar las porciones del proyecto.

- Cultura organizacional: los líderes del proyecto en muchas ocasiones no han considerado en su planificación la cultura de la organización como factor clave. En la mayoría de casos, cuando el cambio está en conflicto con la cultura, la cultura prevalece. Aún los proyectos más populares pueden causar incomodidad. Para un usuario final salir de su zona de *confort* es difícil, ya que para él, el proyecto es algo nuevo y desconocido, sin tener en cuenta el beneficio que produce. Para evitar este factor, es necesario imaginar las actitudes y comportamientos necesarios en las personas, para que el proyecto cierre esa brecha cultural de manera paulatina. En el caso de un proyecto grande, es recomendable empezar entregando partes pequeñas.

- El desarrollo de un proyecto de tecnología, no es una tarea fácil, pero es un reto que las empresas deben enfrentar, para lograr ser competitivas en el mercado, ya que el recurso sistemático permite manejar adecuadamente la información y de esta forma, lograr una toma de decisiones efectiva.

1.4.2. Evolución de la gestión de la tecnología de información

La gestión de la tecnología de información,¡ ha evolucionado muy rápido en las últimas décadas. Las empresas requieren de una alta capacidad para adaptarse a los permanentes y acelerados cambios de la tecnología en las áreas de la informática, sistemas y telecomunicaciones.

La capacidad para desarrollar y utilizar nuevas tecnologías ha permitido automatizar de forma gradual tareas que anteriormente eran realizadas manualmente.

Las ventajas que ofrecen las tecnologías de la información dependen del punto de vista que establece la organización, sobre qué espera de ellas. La unión de la tecnología con el uso de los recursos hace que sea permisible una continua revisión de las ventajas tecnológicas.

En la actualidad, las empresas que no se encuentran involucradas con la tecnología no pueden ser competitivas, ya que una pieza fundamental en cualquier organización es la automatización de sus procesos. La globalización permite estar mejor informados, tanto con las empresas, como con los clientes y proveedores.

Durante mucho tiempo, dentro de las organizaciones, la informática fue considerada una herramienta para soportar funciones operativas.

Actualmente es vista como área de oportunidad para lograr ventajas en los negocios, permiten mejorar la competitividad del negocio, incremento en las ventas, mejora el nivel de servicio al cliente, incrementa la productividad y reduce los costos.

El implementar las tecnologías de la información en las organizaciones no es sencillo, la evolución que han tenido, así como el entorno de la empresa crean retos para su implementación y su funcionamiento. La misión principal de las tecnologías de la información es apoyar a las empresas a automatizar sus procesos, haciéndolas competitivas.

La buena gestión de las tecnologías de información en una organización depende de la armonía entre estrategias, infraestructura y procesos del negocio, asociados con los recursos tecnológicos.

La evolución de las tecnologías de la información exige a que se examinen a conciencia las estrategias de los negocios.

Las organizaciones interesadas en aplicar las tecnologías de la información deben revisar sus estrategias de comercialización, producción y distribución, para implementar una adecuada estructura, que tome en cuenta las tendencias tecnológicas y la visión de lo que se quiere en el futuro.

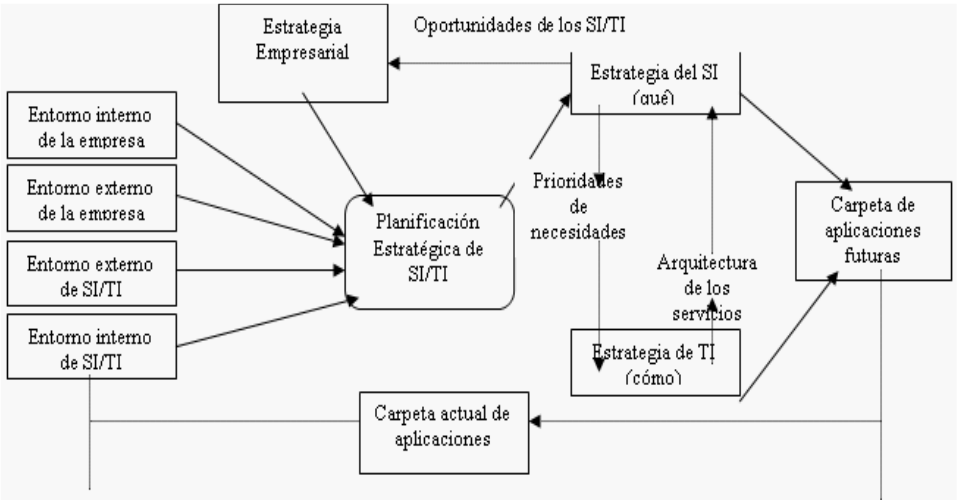
Se debe especificar cómo se van a satisfacer las necesidades con base en las prioridades de la estrategia de los sistemas de información y la tecnología de información precisa para desarrollar y operar las aplicaciones actuales y futuras.

Esto implica establecer la forma en que han de desarrollarse las aplicaciones y cómo se van a alcanzar, utilizar, controlar y gestionar los recursos tecnológicos y humanos necesarios para satisfacer las necesidades de la empresa.

La estrategia de las tecnologías de información dentro de la organización debe estar fundamentada en las necesidades del negocio.

Dicha estrategia debe dar prioridad a la demanda de acuerdo con las necesidades planteadas, y luego asegurar que se gestiona la oferta de recursos y de tecnología, de la mejor forma posible para satisfacer la demanda.

Figura 3. **Estrategia de las tecnologías de información**



Fuente: http://ocw.uoc.edu/informatica-tecnologia-ymultimedia/fundamentos-de-sistemas-de-informacion/Course_listing. Consulta: julio de 2013.

2. ESTÁNDARES INTERNACIONALES DE CALIDAD RELACIONADOS CON LA GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

A continuación se dará una pequeña descripción de los estándares internacionales de calidad más importantes, relacionados con la gestión de las tecnologías de información.

2.1. COBIT 4.0

Se refiere al objetivo de control para información y tecnologías relacionadas**.** "Es una guía de mejores prácticas presentado como un marco de trabajo, dirigida a la gestión de tecnología de la información (TI). Fue propuesto por ISACA (en inglés: Information Systems Audit and Control Association); tiene una serie de recursos que pueden servir de modelo de referencia para la gestión de TI, incluyendo un resumen ejecutivo, un marco de trabajo, objetivos de control, mapas de auditoría, herramientas para su implementación y principalmente, una guía de técnicas de gestión"[3]

Es el estándar más completo, ya que engloba los diversos conceptos expresados en las normas ISO, CMM y PMBOK. Permite evaluar los diversos elementos que integran la gestión de la tecnología de información.

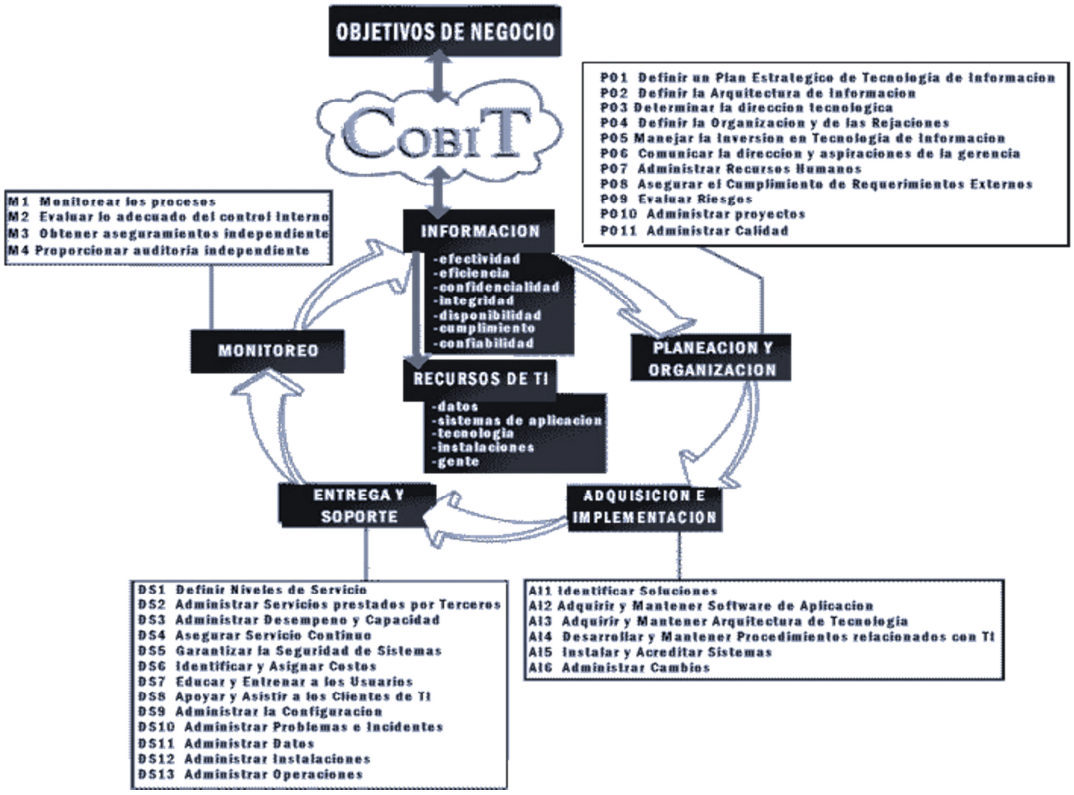
[3]http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas. Consulta: 14 de agosto de 2013.

COBIT ayuda a corregir las brechas existentes entre riesgos de negocios, necesidades de control y aspectos técnicos. Proporciona prácticas a través de un marco referencias (framework) de dominios y procesos, presenta actividades en una estructura manejable y lógica. Las prácticas de COBIT representan el consenso de expertos que ayudarán a los profesionales a optimizar la inversión en la información, representando aquello sobre lo que serán juzgados si las cosas salen mal.

COBIT se enfoca a la orientación de negocios, está diseñado para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio. Proporciona las herramientas para los procesos propios del negocio que provee 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 que se encuentran agrupados.

COBIT posee un conjunto de 34 objetivos de control 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 todo 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.

Figura 4. **Objetivos de control de COBIT**



Fuente: ISACA. ISACA. http://www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Auditing-Spanish-.aspx. Consulta: agosto de 2013.

COBIT está diseñado para ser utilizado para tres audiencias:

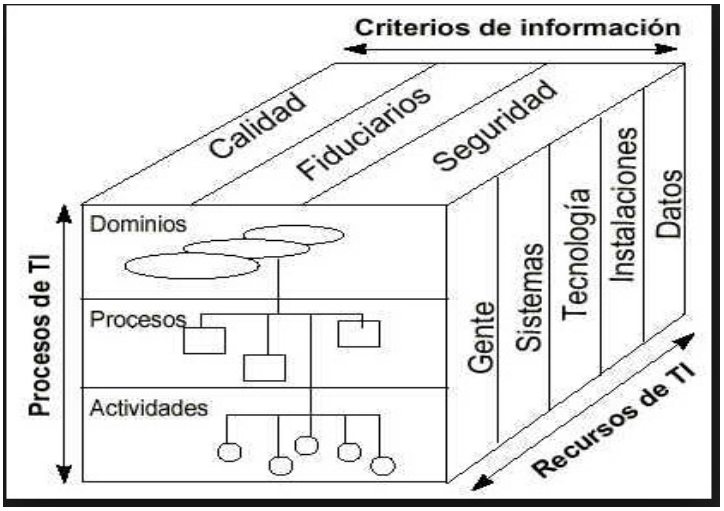
- Administración: para ayudarlos a lograr un balance entre riesgos e inversiones, controlando el ambiente de tecnología de información frecuentemente impredecible.

- Usuarios: para obtener una garantía en cuanto a la seguridad y controles de los servicios de tecnología de información.

- Auditores de sistemas de información: para dar soporte a las opiniones mostradas a la administración sobre los controles internos y las necesidades de la audiencia inmediata de la alta gerencia.

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. A los gerentes de la empresa les interesa un enfoque de calidad, seguridad o fiduciario. Un gerente de TI desea considerar recursos de TI por los cuales es responsable. Los auditores se enfocan en 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 5. **Cubo de COBIT**



Fuente: ISACA. http://www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Auditing-Spanish-.aspx. Consulta: agosto de 2013.

Los dominios son identificados manejando el léxico que la gerencia utilizaría en las actividades cotidianas de la organización (y no vocabulario utilizado por el auditor). Por lo tanto, cuatro grandes dominios son identificados: planificación y organización, adquisición e implementación; entrega y soporte, y monitorización.

2.1.1. Planificación y organización

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

Entre los objetivos de control de este grupo están los siguientes procesos:

- PO1. Definición de un plan estratégico: lograr un balance óptimo entre las oportunidades de tecnología de información y los requerimientos de TI de negocio.

- PO2. Definición de la arquitectura de la información: satisfacer los requerimientos de negocio y organizar de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio.

- PO3. Determinación de la dirección tecnológica: aprovechar al máximo de la tecnología disponible o emergente, satisfaciendo los requerimientos del

negocio, a través de la creación y mantenimiento de un plan de infraestructura tecnológica.

- PO4. Definición de la organización y de las relaciones de TI: esto se realiza por medio de una organización conveniente en número y habilidades, con tareas y responsabilidades definidas y comunicadas.

- PO5. Manejo de la inversión: tiene como finalidad la satisfacción de los requerimientos de negocio, asegurando el financiamiento y el control de desembolsos de recursos financieros.

- PO6. Comunicación de la dirección y aspiraciones de la gerencia: asegura el conocimiento y comprensión de los usuarios sobre las aspiraciones de la gerencia, se concreta a través de políticas establecidas y transmitidas a la comunidad de usuarios, necesitándose para esto estándares para traducir las opciones estratégicas de reglas de usuario prácticas y utilizables.

- PO7. Administración de recursos humanos: maximizar las contribuciones del personal a los procesos de TI, satisfaciendo así los requerimientos de negocio, a través de técnicas sólidas para administración de personal.

- PO8. Asegurar el cumplimiento con los requerimientos externos: cumplir con obligaciones legales, regulatorias y contractuales; para ello se realiza una identificación y análisis de los requerimientos externos en cuanto a su impacto en TI, llevando a cabo las medidas apropiadas para cumplir con ellos.

- PO9. Evaluación de riesgos: asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI; para ello se logra la participación de la propia organización en la identificación de riesgos de TI y el análisis de impacto.

- PO10. Administración de proyectos: establecer prioridades y entregar servicios oportunamente y de acuerdo con el presupuesto de la inversión.

- PO11. Administración de calidad: satisfacer los requerimientos del cliente; para ello se realiza una planeación, implementación y mantenimiento de estándares y sistemas de administración de calidad por parte de la organización.

2.1.2. 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 caminos y el mantenimiento realizados a sistemas existentes.

Entre los objetivos de control de este grupo están los siguientes procesos:

- AI1. Identificación de soluciones: asegurar un enfoque efectivo y eficiente para satisfacer los requerimientos del usuario, posibilitado por una identificación y análisis, objetivos y claros, de las oportunidades alternativas medidas en contraposición con los requerimientos del usuario.

- AI2. Adquisición y mantenimiento de aplicaciones: proveer funciones automatizadas que soporten efectivamente el proceso del negocio, posibilitado por una definición de declaraciones específicas de requerimientos funcionales y operativos, y una implementación por fase con productos claros.

- AI3. Adquisición y mantenimiento de la infraestructura tecnológica: proveer las plataformas apropiadas para soportar las aplicaciones del negocio, mediante adquisición juiciosa de hardware, estandarización sobre el software, evaluación del rendimiento del hardware y del software, y administración consistente del sistema.

- AI4. Facilidad de uso: asegurar el debido uso de las aplicaciones y de las soluciones tecnológicas establecidas, posibilitados por un enfoque estructurado del desarrollo de manuales de procedimiento de usuario y de operaciones, requerimientos de servicio y materiales de entrenamiento.

- AI5. Obtención de recursos tecnológicos**:** proveer recursos de TI, incluyendo personas, hardware, software y servicios cuando sea necesario, a través de la definición de procesos de aprovisionamiento, la selección adecuada de proveedores y la configuración de condiciones contractuales.

- AI6. Gestión de cambios: minimizar la probabilidad de interrupción, alteraciones no autorizadas y errores, mediante el análisis, la implementación y el seguimiento de todos los cambios solicitados y hechos a la infraestructura existente de TI.

- AI7. Instalación y acreditación de soluciones y cambios: verificar y confirmar que la solución es adecuada para el propósito que se pretende, mediante una instalación, migración, conversión y plan de aceptación, bien formalizados.

2.1.3. Entrega de servicio y soporte

Este dominio hace referencia a la entrega de servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad.

Entre los objetivos de control de este grupo están los siguientes procesos:

- DS1. Definir y administrar los niveles de servicio: asegurar la alineación de los servicios claves de TI con la estrategia del negocio, enfocándose en la identificación de requerimientos de servicio, el acuerdo de niveles de servicio y el monitoreo del cumplimiento de los niveles de servicio.

- DS2. Administrar los servicios de terceros: brindar servicios satisfactorios de terceros, con transparencia acerca de los beneficios, riesgos y costos, enfocándose en el establecimiento de relaciones y responsabilidades bilaterales con proveedores calificados de servicios tercerizados y el monitoreo de la prestación del servicio, para verificar y asegurar la adherencia a los convenios.

- DS3. Administrar el desempeño y la capacidad: optimizar el desempeño de la infraestructura, los recursos y las capacidades de TI, en respuesta a las necesidades del negocio. Enfocándose en cumplir con los

requerimientos de tiempo de respuesta de los acuerdos de niveles de servicio, minimizando el tiempo sin servicio y haciendo mejoras continuas de desempeño y capacidad de TI, a través del monitoreo y la medición.

- DS4. Garantizar la continuidad del servicio: asegurar el mínimo impacto al negocio, en caso de una interrupción de servicios de TI. Enfocándose en el desarrollo de resistencia (*resilience*) en las soluciones automatizadas y desarrollando, manteniendo y probando los planes de continuidad de TI.

- DS5. Garantizar la seguridad de los sistemas: asegurar la información contra uso no autorizado, divulgación, modificación, daño o pérdida, implementando controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas esté restringido a usuarios autorizados.

- DS6. Identificar y asignar costos: transparentar y entender los costos de TI y mejorar la rentabilidad a través del uso bien informado de los servicios de TI, enfocándose en el registro completo y preciso de los costos de TI, un sistema equitativo para asignación acordado con los usuarios de negocio, y un sistema para reportar oportunamente el uso de TI y los costos asignados.

- DS7. Educar y entrenar a los usuarios: hacer uso efectivo y eficiente de soluciones y aplicaciones tecnológicas y el cumplimiento del usuario con las políticas y procedimientos, enfocándose en un claro entendimiento de las necesidades de entrenamiento de los usuarios de TI, la ejecución de una efectiva estrategia de entrenamiento y la medición de resultados.

- DS8. Administrar la mesa de servicio y los incidentes: permite el efectivo uso de los sistemas de TI, garantizando el análisis de las consultas de los usuarios finales, incidentes y preguntas.

- DS9. Administrar la configuración: optimizar la infraestructura, recursos y capacidades de TI, y llevar registro de los activos de TI, enfocándose en establecer y mantener un repositorio completo y preciso de atributos de la configuración de los activos y de líneas base y compararlos contra la configuración actual.

- DS10. Administrar los problemas**:** garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio, reducir el retrabajo y los defectos en la prestación de los servicios y de las soluciones. Enfocándose en registrar, rastrear y resolver problemas operativos; investigar las causas raíz de todos los problemas relevantes y definir soluciones para los problemas operativos identificados.

- DS11. Administrar los datos**:** optimizar el uso de la información y garantizar la disponibilidad de la información cuando se requiera, enfocándose en mantener la integridad, exactitud, disponibilidad y protección de los datos.

- DS12. Administrar el ambiente físico: proteger los activos de cómputo y la información del negocio, minimizando el riesgo de una interrupción del servicio. Enfocándose en proporcionar y mantener un ambiente físico adecuado para proteger los activos de TI contra acceso, daño o robo.

- DS13. Administrar las operaciones: un procesamiento completo y apropiado de información requiere de una efectiva administración del

procesamiento de datos y del mantenimiento del hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procesamiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware.

2.1.4. Monitoreo y control

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

- ME1. Monitorear y evaluar el desempeño de TI: incluye definición de indicadores de desempeño relevantes, y la realización de reportes sistemáticos y oportunos acerca de los mismos.

- ME2. Monitorear y evaluar el control interno: este proceso se encarga de monitorear las actividades de control interno de la organización relacionadas con TI, y además identifica las acciones de mejoramiento posibles.

- ME3. Garantizar el cumplimiento regulatorio: identifica leyes y regulaciones aplicables, con el fin de reducir riesgos relacionados con el no cumplimiento de los requerimientos del negocio.

- ME4. Aplicación del gobierno de TI: satisface la integración del gobierno de TI con los objetivos corporativos. Por otra parte, alinea el cumplimiento de las metas del negocio con las leyes y regulaciones existentes.

2.2. ISO 12207

Es una estándar que provee una serie de objetivos de control para la gestión de los proyectos de desarrollo de software, para un desempeño ideal de las áreas de desarrollo de sistemas de información.

Este estándar comprende 17 procesos, los cuales son agrupados en tres categorías principales de apoyo y de organización, que se muestran en la siguiente gráfica:

Figura 6. **ISO 12207 procesos del ciclo de vida del software**

Fuente: http://normasiso-iec.blogspot.com/2009/10/normas-isoiec-12207.html. Consulta: agosto de 2013.

2.2.1. Procesos principales

Los procesos principales son cinco, los cuales brindan servicio a las partes principales durante el ciclo de vida del software. Estos son:

- Adquisición: define las actividades del adquiriente, es decir, la organización que adquiere un sistema, producto, software o servicio de software.

- Suministro: se relaciona con las actividades del proveedor, organización que proporciona sistema, producto o servicio de software al adquiriente.

- Desarrollo: define las actividades que tiene que llevar a cabo el desarrollador, organización que define y desarrolla el producto software.

- Operación: define las actividades del operador, organización que proporciona el servicio de operar un sistema informático en su entorno real.

- Mantenimiento: define las actividades del responsable de mantenimiento o la organización que se encarga de esta función; es decir, la gestión de las modificaciones al producto, para mantenerlo actualizado y operativo.

2.2.2. Procesos de apoyo

Este proceso soporta y coordina el desarrollo y el ciclo de vida de las actividades primarias. Apoya a otros procesos para llevar a cabo una función especializada.

Está compuesto por 8 procesos:

- Documentación**:** este proceso define las acciones necesarias para registrar toda la información generada por los procesos del ciclo de vida.

- Gestión de la configuración: este proceso evalúa las configuraciones, así como la administración de versiones.

- Aseguramiento de la calidad: asegura objetivamente que los productos de software satisfagan los requerimientos especificados y se ajusta a los planes establecidos.

- Verificación: verifica los productos y servicios de software.

- Validación: valida los productos de software del proyecto del software.

- Revisión conjunta: se enfoca tanto en revisiones técnicas como administrativas, para evaluar el estado de los productos producidos.

- Auditoría: define las acciones para establecer el cumplimiento de los requerimientos, planes y contratos.

- Solución de problemas: define el proceso para resolver los problemas que sean encontrados, sin interesar su naturaleza, durante la ejecución del desarrollo, operación, mantenimiento y otros procesos.

2.2.3. Procesos organizativos

Este proceso apoya la administración de todo el ambiente de desarrollo, está comprometido en seguir cuatro procesos:

- Administración: el objetivo de este proceso es proveer administración a todos los procesos del proyecto, incluyendo administración del producto y del proyecto.

- Infraestructura: este proceso resguarda el hardware, software, herramientas, técnicas y estándares que se necesitan para la ejecución de los otros procesos.

- Mejora de procesos: este proceso define las acciones que una organización realiza para establecer, medir, controlar y mejorar los procesos de su ciclo de vida.

- Recursos humanos: define las actividades para proveer personal capacitado adecuadamente.

2.3. ISO 17799

Es una norma que provee una serie de objetivos de control para la gestión de procesos y proyectos de infraestructura de tecnología de información.

También incluye secciones relacionadas con la seguridad en el desarrollo de sistemas de información y la gestión de la continuidad del negocio. Incluye los siguientes grupos de objetivos de control.

2.3.1. Política de seguridad

Entre los objetivos de control de este grupo están:

- Documento de política de seguridad de la información
- Revisión y evaluación

2.3.2. Aspectos organizativos de la seguridad

Entre los objetivos de control de este grupo están:

- Estructura para la seguridad de la información: comité, recursos, responsabilidades, asesoría de expertos, colaboración entre organizaciones y evaluación independiente.

- Seguridad en los accesos de terceras partes

- *Outsourcing*

2.3.3. Clasificación y control de activos

Entre los objetivos de control de este grupo están:

- Responsabilidades sobre los activos
- Clasificación de la Información

2.3.4. Seguridad ligada al personal

Entre los objetivos de control de este grupo están:

- Seguridad en la definición del trabajo y recursos
- Formación y capacitación en seguridad de la información
- Respuesta ante incidencias y malos funcionamientos de la seguridad

2.3.5. Seguridad física y del entorno

Entre los objetivos de control de este grupo pueden mencionarse:

- Áreas seguras
- Seguridad de los equipos
- Controles generales

2.3.6. Gestión de comunicaciones y operaciones

Entre los objetivos de control de este grupo están:

- Procedimientos y responsabilidades de operación
- Planificación y aceptación del sistema
- Protección contra software malicioso
- Gestión Interna de respaldo y manipulación
- Gestión de redes
- Uso y seguridad de los medios de información
- Intercambio de Información y software

2.3.7. Control de accesos

Entre los objetivos de control de este grupo pueden citarse:

- Requisitos de negocio para el control de accesos
- Gestión de acceso a usuarios
- Responsabilidades de los usuarios
- Control de acceso a la red
- Control de acceso al sistema operativo
- Control de acceso a las aplicaciones
- Seguimiento de accesos y usos del sistema
- Informática móvil y teletrabajo

2.3.8. Desarrollo y mantenimiento de sistemas

Entre los objetivos de control de este grupo están:

- Requisitos de seguridad en los sistemas
- Seguridad de las aplicaciones
- Controles criptográficos
- Seguridad de los archivos del sistema
- Seguridad en los procesos de desarrollo y soporte

2.3.9. Gestión de la continuidad del negocio

Entre los objetivos de control de este grupo pueden citarse:

- Planificación
- Prueba

- Mantenimiento y reevaluación de los planes de continuidad

2.3.10. Cumplimiento

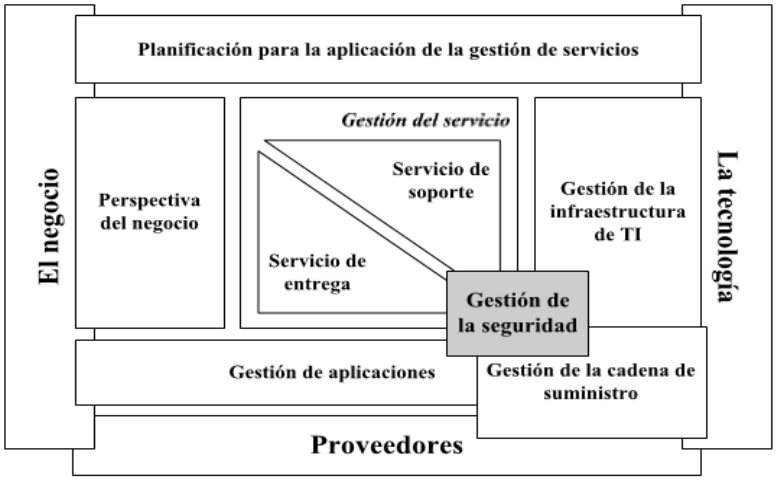
Entre los objetivos de control de este grupo están:

- Cumplimiento de los requisitos legales
- Revisiones de la política de seguridad y la conformidad técnica
- Consideraciones sobre la auditoría de sistemas

2.4. ITIL

Provee de una metodología para la gestión de los requerimientos de desarrollo que tienen que ver con los sistemas en producción (los sistemas que ya están utilizando los usuarios de las diversas áreas de la organización).

Figura 7. **Marco de trabajo de ITIL**



Fuente: ITSMF LIBRARY. Fundamentos de gestión de servicios de TI basado en ITIL. p. 26.

Una organización que adopta las buenas prácticas de la gestión de servicios de tecnología de información de ITIL, mejora significativamente la velocidad de atención de requerimientos de desarrollo de sistemas de información.

A continuación se detalla la gestión de la atención de requerimientos de ITIL:

- Previo a la atención, se han definido o desarrollado:
    - Criterios para determinar qué requerimientos se pueden atender por el operador que atiende en la mesa de servicio (*service desk*), quien es el ente que canaliza los diversos requerimientos, tanto que tengan que ver con procesos de desarrollo de sistemas de información como con procesos de gestión de infraestructura de tecnología de información.
    - Niveles de servicio
    - Criterios para determinar los siguientes niveles de servicio en función de la complejidad y naturaleza del requerimiento, además de las competencias de los recursos disponibles. Comúnmente los criterios están en función del perjuicio que podría ocasionar la ausencia de los servicios de tecnología de información, afectándose a:
        - Clientes externos y clientes internos
        - Solo clientes externos
        - Solo clientes internos

- Un sistema de información para soporte de transacciones y para la gestión del conocimiento de las transacciones registradas en la mesa de servicio.

- Todos los requerimientos de atenciones sobre las tecnologías de información en producción, se realizan a través del *service desk*, ya sea por teléfono, sistema de información o correo electrónico. Los requerimientos al inicio son considerados “incidentes”; es decir, interrupciones a la operación normal de los servicios de tecnología de información.

- Los requerimientos reportados son ingresados a la gestión de incidentes, de acuerdo con los niveles de servicio previamente definidos.

- La gestión de problemas aparece para solucionar las causas de incidentes comunes que han sido registrados en el *service desk.* Ello a su vez, generará nuevos requerimientos.

- La gestión de incidentes o la gestión de problemas pueden provocar:

  - Que se inicie la gestión de cambios (cualquier cambio por mínimo que parezca debe ser registrado con los correspondientes efectos en la gestión de versiones y la gestión de configuraciones).

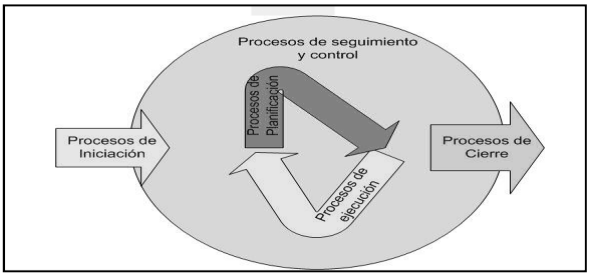
  - Que se inicie la gestión de versiones (gestión de versiones de documentos, código fuente, ejecutables, etc.).

  - Que se inicie la gestión de configuraciones (configuraciones en hardware, software de base y sistemas de información).

2.5. Procesos del PMBOK

El PMBOK “Project management body of knowledge”, o Guía de los fundamentos de la dirección de proyectos, es una síntesis de los diversos conceptos y metodologías de la gestión de proyectos, agrupados bajo un enfoque de procesos. Permite la comprensión de la gestión de proyectos, a través de la interacción de un grupo de procesos, los cuales se pueden observar en la siguiente figura.

Figura 8. **Representación de grupos de procesos en PMBOK**



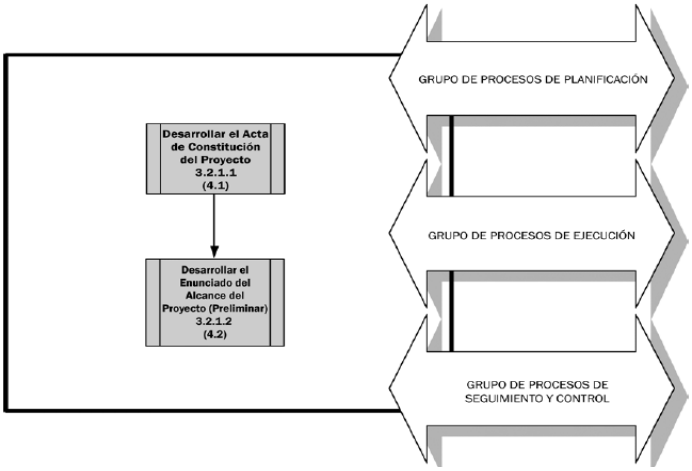
Fuente: <http://www.ehu.es/Degypi/PMBOK/cap3PMBOOK.htm>.Consulta: agosto de 2013.

2.5.1. Proceso de iniciación

El proceso de iniciación refina la descripción del alcance inicial y los recursos que la organización está dispuesta a invertir. Si aún no hubiera sido designado, se elegirá al director del proyecto. También se documentarán las restricciones y asunciones iniciales. Esta información se refleja en el acta de constitución del proyecto y, una vez aprobado, queda oficialmente autorizado. Si bien el equipo de dirección del proyecto puede ayudar a redactar el acta de constitución del mismo, la aprobación y financiación se realizan fuera de los límites del proyecto.

Como parte del grupo de procesos de iniciación, muchos proyectos grandes o complejos pueden dividirse en fases. La revisión de los procesos de iniciación al comienzo de cada fase permite mantener el proyecto enfocado en los objetivos de negocio que pretende satisfacer, como se puede observar en la siguiente figura

Figura 9. **Grupo de procesos de iniciación**

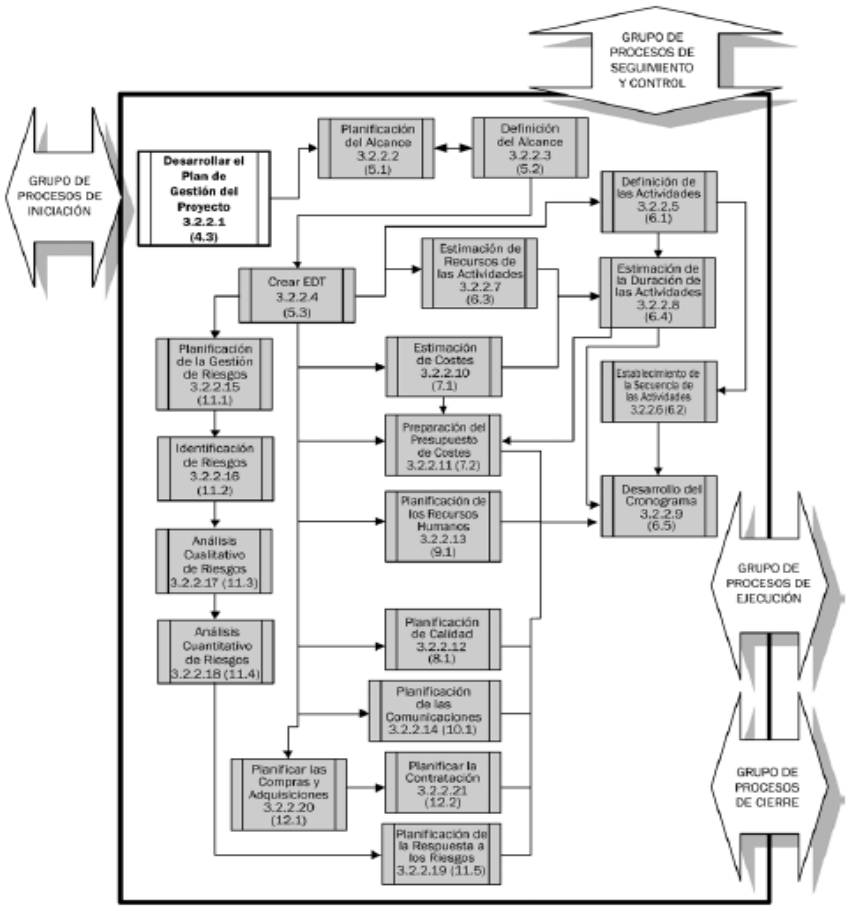


Fuente: GLOBAL STANDARD. Guía de los fundamentos de la dirección de proyectos. p.44.

2.5.2. Proceso de planificación

El grupo de procesos de planificación ayuda a recoger información de varias fuentes de diverso grado de completitud y confianza. Los procesos de planificación desarrollan el plan de gestión del proyecto. Estos procesos también identifican, definen y maduran el alcance y el coste del proyecto y planifican las actividades que se realizan dentro del mismo. A continuación se muestra dicho proceso.

Figura 10. **Grupo de procesos de planificación**

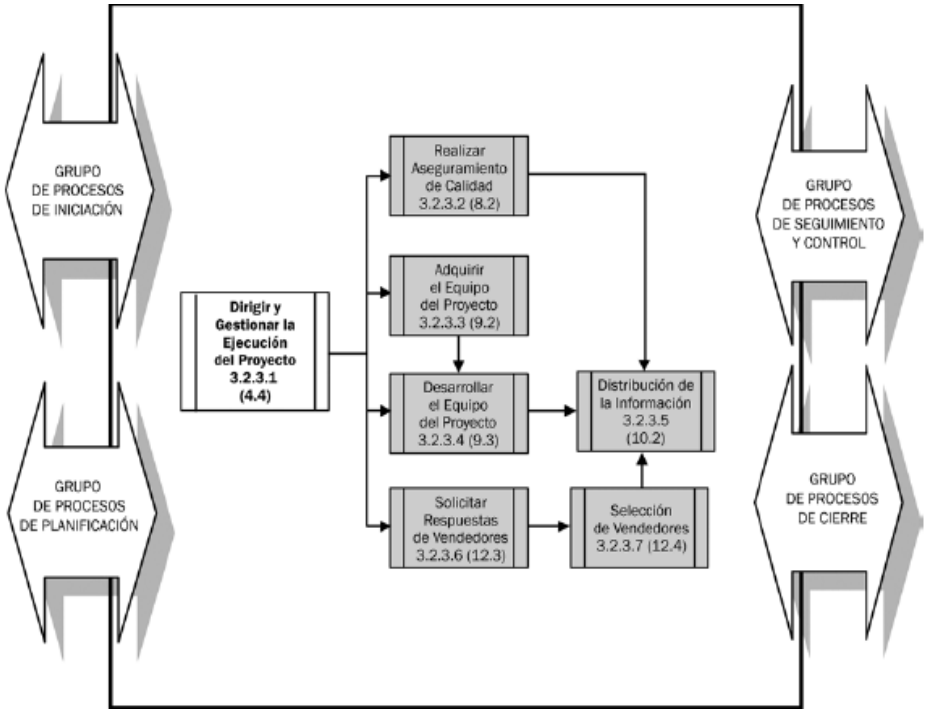


Fuente: GLOBAL STANDARD. Guía de los fundamentos de la dirección de proyectos. p.46.

2.5.3. Proceso de ejecución

Este grupo de procesos implica coordinar personas y recursos, así como integrar y realizar las actividades del proyecto, de acuerdo con el plan de gestión del mismo. Este grupo de procesos también aborda el alcance definido en el enunciado del alcance del proyecto e implementa los cambios aprobados, como se muestra en la siguiente figura.

Figura 11. **Grupo de procesos de ejecución**



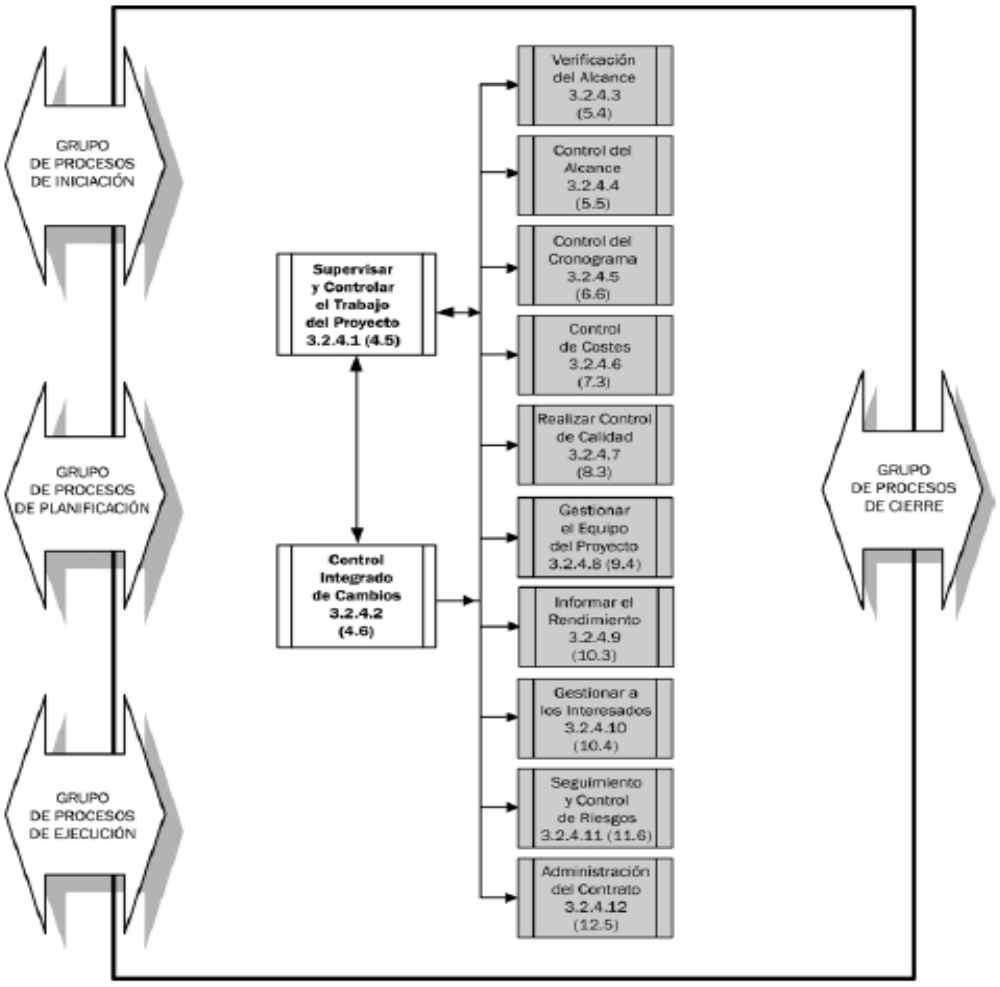
Fuente: GLOBAL STANDARD. Guía de los fundamentos de la dirección de proyectos. p. 55.

2.5.4. Proceso de seguimiento y control

El beneficio clave de este grupo de procesos es que el rendimiento del proyecto se observa y se mide regularmente para identificar las variaciones respecto del plan de gestión del mismo.

El grupo de procesos de seguimiento y control también incluye controlar los cambios y recomendar acciones preventivas como anticipación de posibles problemas. A continuación se muestra la gráfica de dicho proceso.

Figura 12. **Grupo de procesos de seguimiento y control**

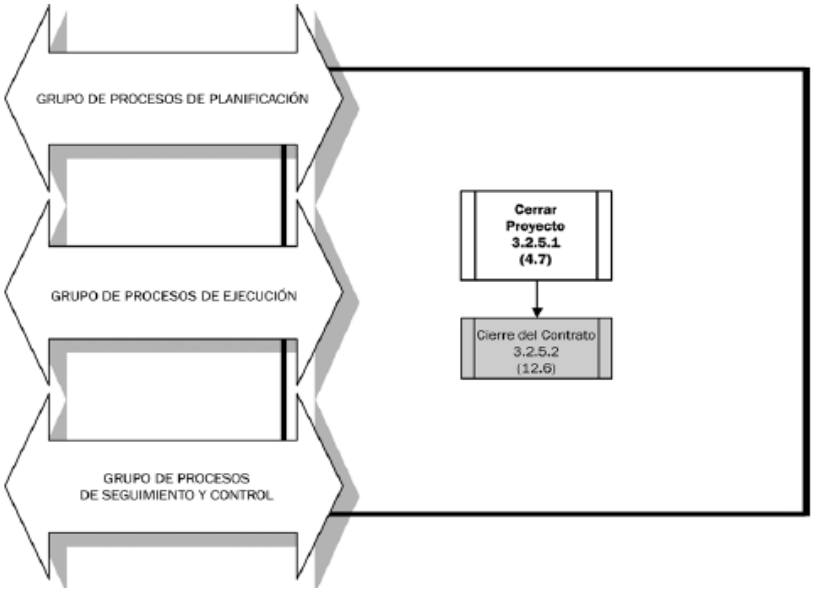


Fuente: GLOBAL STANDARD. Guía de los fundamentos de la dirección de proyectos. p.60.

2.5.5. Proceso de cierre

Este grupo de procesos, una vez completado, verifica que los procesos definidos se completen dentro de todos los grupos de procesos para cerrar el proyecto o una fase de él, según corresponda, y establece formalmente que se ha finalizado un proyecto o fase del mismo. A continuación se muestra la gráfica de dicho proceso.

Figura 13. **Grupo de proceso de cierre**



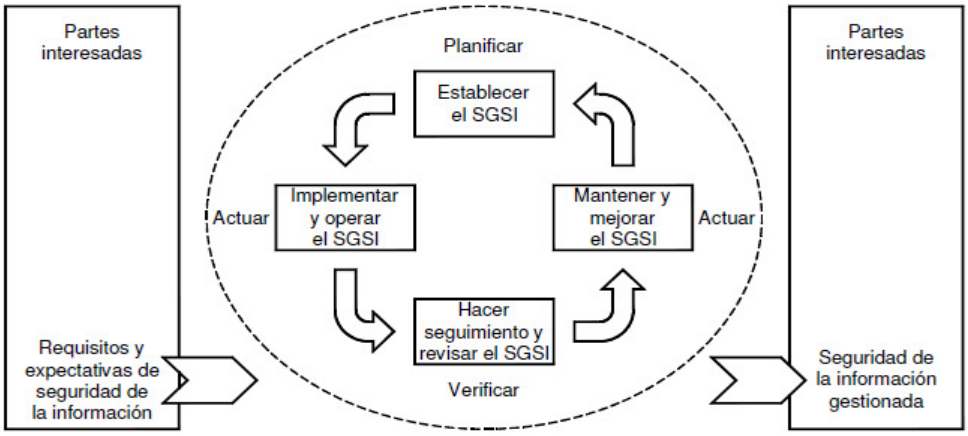
Fuente: GLOBAL STANDARD. Guía de los fundamentos de la dirección de proyectos. p.66.

2.6. ISO 27001

Esta norma adopta el modelo de procesos “planificar-hacer-verificar-actuar”, que se aplica para estructurar todos los procesos del seguridad de la gestión de la seguridad de la información. Se toman como elementos de entrada los requisitos de seguridad de la información y las expectativas de las partes interesadas, y a través de las acciones y procesos necesarios, se producen resultados de seguridad de la información, que cumplen estos requisitos y expectativas.

Esta norma brinda un modelo robusto para implementar los principios en aquellas directrices que controlan la evaluación de riesgos, diseño e implementación de la seguridad, gestión y reevaluación de la seguridad.

Figura 14. **Modelo aplicado a los procesos de SGSI**



Fuente: Norma técnica Colombiana NTC-ISO/IEC 27001.
http://www.ehu.es/Degypi/PMBOK/cap3PMBOOK.htm#3.1_Procesos_de_Dirección_de_Proyectos>. Consulta: junio de 2013.

- Planificar: establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes a las políticas y objetivos globales de una organización.

- Hacer: implementar y operar la política, los controles, procesos y procedimientos del SGSI.

- Verificar: evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

- Actuar: emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

3. METODOLOGÍA PARA NORMALIZAR LOS DIFERENTES ESTÁNDARES INTERNACIONALES DE CALIDAD, RELACIONADOS CON LA GESTIÓN DE LA TECNOLOGÍA DE LA INFORMACIÓN

3.1. Importancia de normalizar los estándares

Los estándares proporcionan un conjunto de criterios que se deben tomar en cuenta al momento de realizar una auditoría de la gestión de tecnología de información; pero, no dan procedimientos enmarcados en una metodología que permita auditar de manera integral la gestión de la tecnología de información, alineada al logro de objetivos estratégicos organizacionales.

Si no se tiene una metodología integral, no se puede llegar a un análisis profundo que permita encontrar las causas de los problemas y por ende, realizar un diagnóstico que realmente sirva para realizar una planificación estratégica de tecnología de información alineada a la planificación estratégica organizacional, y las auditorías podrían verse limitadas a la evaluación de decenas o cientos de aspectos aislados cuya solución realmente no beneficiaría de la mejor manera a la organización.

La metodología para la auditoría integral de la gestión de las tecnologías de la información (MAIGTI) enlaza los numerosos conceptos de las buenas prácticas de la gestión de las tecnologías de información (COBIT), la gestión de los procesos del ciclo de vida de desarrollo de software (ISO/IEC 12207), las buenas prácticas de la gestión de la seguridad de la información (ISO/IEC 17799), la gestión de servicios de tecnología de información (ISO/IEC 20000 o

ITIL), así como la gestión de proyectos del Project Management Institute (PMBOK), sobre la base de una simplificación del proceso general de auditoría.

3.2. Proceso de desarrollo de la metodología

Como se mencionó anteriormente, una mala gestión en la tecnología de la información representa alrededor del 65 % de los problemas en las organizaciones, no solo hay que gestionar correctamente para lograr un resultado positivo para la empresa, sino que también hay que aplicar las técnicas adecuadas para el éxito.

El tratar de seguir al pie de la letra una determinada metodología para todos los proyectos de una compañía no es del todo acertada; cada proyecto es diferente, cada uno tiene distintos alcances, presupuestos y tiempos distintos. Por ende, usar una sola metodología para todos no es lo más óptimo.

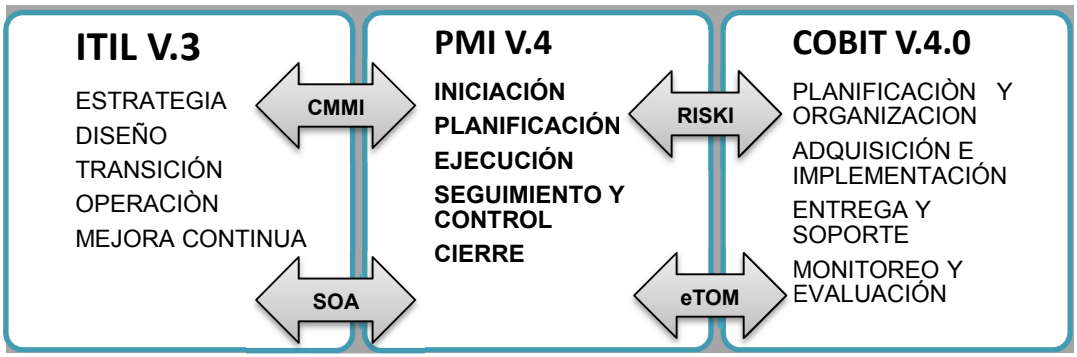
Asimismo, la falta de compromiso del equipo con la metodología elegida hace la tarea más difícil y genera mayores dificultades, ya que los involucrados no harán lo que se supone deben hacer. Muchas veces esto se da por una falta de entrenamiento adecuado o por una resistencia al cambio de las personas.

Se debe determinar cómo los diversos estándares que existen hoy en día pueden ayudar a resolver los problemas de las empresas, recalcando que para cada uno de los problemas, hay más de un modelo aplicable para gestionar dichas problemáticas. Es decisión de cada compañía determinar el que mejor se adapte a sus necesidades y políticas empresariales. Los estándares no siempre encajan el uno con el otro, cada uno de ellos fue creado por distintas personas, distintos tiempos, distintos lugares y con propósitos distintos.

Por ello, a pesar de que pueda haber varios estándares que den solución a determinada problemática, cada uno de ellos fue creado para resolver un matiz específico de dicha problemática, con un enfoque específico y con un nivel de granularidad distinto. El reto se encuentra en saber qué partes de cada estándar o modelo pueden ser para cada compañía.

Es de primordial importancia el saber elegir las mejores prácticas, procesos y estrategias entre todos estos estándares y poder generar a partir de estas partes seleccionadas, un modelo personalizado y adaptado totalmente para una organización en particular. En la siguiente figura se muestra la integración de los diferentes estándares.

Figura 15. **Integración de buenas prácticas y estándares**



Fuente: http://es.scribd.com/doc/115518531/Buenas-Practicas-Gobierno-Ti. Consulta: junio de 2013.

Esta variedad de estándares, la necesidad de analizarlos y elegir lo mejor entre ellos para el uso dentro de la compañía, plantea distintos retos que deben saber afrontarse:

- Integrar dichos estándares es muchas veces un rompecabezas; se debe saber elegir las partes que más convengan a la empresa, de cada uno de estos estándares.

- Elegir y construir un propio marco de trabajo basado en diversos estándares; se debe evitar el riesgo de querer incluir más de la cuenta dentro de dicho marco de trabajo. Lograr y mantener un marco de trabajo simple y eficaz es a lo que se debe apuntar.

- Se debe evaluar también el costo de implantar determinado estándar y determinada combinación de ellos. Si no se establece un presupuesto claro, se corre el riesgo de fracasar en la puesta en marcha de este proyecto.

- La falta de compromiso y apoyo de la alta gerencia puede conllevar a un resultado negativo. Sin una fuerza de soporte de la alta gerencia, el proyecto no tomará el vuelo que requiere y quedará a medio camino.

- Definir un cronograma es crucial; se debe realizar una implantación de estándares de gobierno de las TI de tal manera que permita una adopción veloz, y a la vez una adecuada institucionalización de los procesos relacionados con dichos estándares. La implantación por fases podría ser una buena alternativa en caso los tiempos para una implantación total sean muy largos para las expectativas de la compañía.

- Muchas veces se obvia la correcta capacitación y entrenamiento del personal que estará a cargo de los procesos implantados. Esto conlleva a una resistencia al cambio y a una falta de institucionalización de las

- prácticas implantadas. Para eliminar este problema, la concientización y entrenamiento a los empleados y demás involucrados es necesaria.

- Finalmente, un reto relevante es encontrar el momento ideal para proponer e implantar determinado estándar. Muchas veces estas iniciativas son rechazadas por la alta gerencia debido al mal momento en que fueron propuestas. Se debe saber escoger el momento ideal en el que dicha propuesta tendrá la mayor acogida posible. Lógicamente esto se debe sopesar con las necesidades y prioridades de la organización.

A continuación se muestra cada uno de los estándares mencionados en el capítulo anterior, cada uno de ellos en contexto y cómo ellos se interrelacionan entre sí para crear un marco global para el gobierno de TI.

Figura 16. **Interrelación entre los diferentes estándares para crear un marco de gobierno de TI**

Fuente:http://es.scribd.com/doc/115518531/Buenas-Practicas-Gobierno-Ti.
Consulta: julio de 2013.

A continuación se detalla los principales elementos en común y diferencias entre cada uno de estos estándares para una mejor elección del estándar a utilizar, según las necesidades de la empresa.

- ITIL versus CMMI: el modelo ITIL se aplica al ciclo de vida completo de TI, pero se enfoca en los procesos operacionales (postimplementación de un determinado servicio o infraestructura TI). De allí proviene el gran problema de ITIL, que no cubre adecuadamente las fases de desarrollo de software ni la gestión de proyectos asociada a esa fase de construcción de activos software. Por otro lado, CMMI generalmente se aplica al desarrollo del servicio o infraestructura en TI (durante el diseño y la implantación). Sin embargo ambos tienen un punto común: la gestión de la entrega. Ambos modelos poseen actividades recomendadas para la gestión de la entrega de nuevos elementos de software e infraestructura.

  Analizando ambos modelos, se puede observar que CMMI se centra en garantizar la calidad en el desarrollo de software mientras que ITIL garantiza la explotación del producto. Por ello, muchas empresas consideran que ambas metodologías no son excluyentes, sino complementarias, embarcándose en proyectos de análisis y definición de procesos que permitan encajar ambas filosofías de trabajo (en conjunto abarcan desde el desarrollo del software hasta la gestión del mantenimiento y servicios del mismo).

- ITIL versus PMBOK: los entregables de un proyecto trabajado con el modelo PMBOK (PMI) pueden ser gestionados también usando el modelo ITIL para gestión de servicios. La gestión de servicios brinda un conjunto de procesos para garantizar el correcto funcionamiento de la infraestructura TI de la organización. Esta gestión de servicios involucra

- manejar adecuadamente los fallos que puedan suceder (gestión de incidentes) que conllevan a realizar ajustes en dichos servicios e infraestructura. Dichos ajustes no solo ni más ni menos que proyectos de actualización de los servicios TI, que pueden ser manejados siguiendo los procesos estándar de PMBOK o con aquellos que el mismo modelo ITIL propone. Por ello el principal punto de intersección entre ITIL y PMBOK se encuentra en el proceso de gestión del cambio y la creación de nuevos servicios. Los términos y nomenclaturas, usando por cada uno de estos estándares para esta gestión del cambio, varían en cada modelo.

- Finalmente, ambos poseen actividades similares para realizar dicha gestión del cambio. El enfoque de ITIL para el manejo del cambio es orientado a garantizar la disponibilidad y operatividad del servicio dentro del contexto de un determinado acuerdo de nivel de servicio firmado con el cliente del servicio. Por otro lado, el enfoque de PMBOK respecto de esta gestión de cambios es garantizar la calidad dentro del marco, la triple restricción que todo proyecto debe considerar: costo, tiempo, calidad y riesgos. Puede decirse entonces que estos dos estándares son complementarios a la vez, dependiendo del enfoque que quiera dar la organización en los procesos de intersección. Se pueden usar ambos modelos en conjunto, para gestionar servicios basado en ITIL y gestionar los cambios en dichos servicios usando PMBOK.

- ITIL versus COBIT: quizá sea COBIT quien más puntos presente frente a ITIL, aunque se presenten como complementarias. Incluso COBIT puede que tenga mayor alcance que ITIL, ya que abarca todo el espectro de actividades de IT, mientras que ITIL está centrado solo en "*service management*" (gestión del servicio).

Ambos modelos son también complementarios y se pueden usar juntos: ITIL para lograr efectividad y eficiencia en los servicios TI y COBIT para verificar la conformidad en cuanto a disponibilidad, rendimiento, eficiencia y riesgos asociados de dichos servicios con los objetivos y estrategias de la compañía, usando para ello métricas claves y cuadros de mando que reporten dicha información.

La razón para usar estos estándares y realizar una integración entre ellos, es ayudar a la organización a cumplir sus objetivos de negocio.

Hay muchos estándares, y la lista seguirá creciendo; todas pueden usarse en conjunto; esto crea retos de integración por resolver. Pero se pueden adaptar piezas de cada estándar y usarlas de manera personalizada en cada organización.

Por otro lado, no hay una manera única de hacerlo; no hay recetas mágicas para decidir qué usar y cómo usarlo, pero si hay guía y mucha documentación de ayuda y soporte.

3.3. Arquitectura de la metodología

La estructura de objetivos de control compone la metodología, la cual a su vez está basada en el modelo de procesos, sobre la base del proceso general de auditoría de la ISO 19011:2002 (lineamientos sobre auditorías de gestión de calidad), como se ve en la figura.

Figura 17. **Estructura para la metodología integral de la gestión de la tecnología de información**

Fuente: ALFARO PAREDES, Emigdio Antonio.
<http://www.tesislatinoamericanas.info/index.php/record/view/48709. Consulta: mayo de 2013.

La metodología resultante comprende los elementos siguientes: la finalidad de la auditoría, el alcance, es decir el detalle de lo que está incluido y lo que no está incluido como parte de la auditoría, requerimientos de información, proceso de evaluaciones a realizar y las salidas como papeles de trabajo e informe de auditoría, con los hallazgos o evidencias de la ejecución del proceso.

4. ENFOQUES DE LA AUDITORÍA DE LA TECNOLOGÍA DE LA INFORMACIÓN

4.1. Enfoque a la seguridad

La seguridad informática puede llegar a entenderse solamente para equipos y entornos técnicos, como si la información en otros ambientes no requiriera protección, cuando son las propias operaciones de la entidad, las que requieren protección.

Si no existen medidas y adecuada protección, se puede perder información vital, o por lo menos no estar disponible en el momento requerido y se puedan tomar decisiones erróneas.

Debe de evaluarse en la auditoría si los modelos de seguridad están en armonía con las nuevas arquitecturas y las distintas plataformas de la organización.

Al realizar una auditoría enfocada a la seguridad, deben de tomarse los siguientes aspectos:

- Fundamentos de seguridad: políticas, planes, funciones; etc.
- El desarrollo de las políticas
- Amenazas físicas y externas
- Control de accesos (físicos, lógicos)

Para evaluar riesgos hay que pensar, entre otros elementos, el tipo de información almacenada procesada y transmitida, la criticidad de las aplicaciones, la tecnología usada, el marco legal y la organización misma. Para ello es necesario evaluar las vulnerabilidades que existen, ya que la cadena de protección se podrá romper con mayor probabilidad por los eslabones más débiles, que serán los que preferentemente intentarán usar de forma no autorizada.

En un proceso de auditoría, se evaluará todos estos aspectos mencionados además de otros; por ejemplo, si la seguridad es realmente una preocupación a nivel de la corporación, no es suficiente que exista presupuesto para ello, es necesaria una cultura de seguridad y que exista un comité que fije y apruebe los objetivos correspondientes. Si la organización auditada está en medio de un proceso de implementación de la seguridad, la evaluación se centrará en los objetivos, los planes, proyectos que hay en curso y los medios usados o previstos.

Cuando se habla de seguridad siempre se refiere a sus tres dimensiones clásicas y son las siguientes:

- La confidencialidad: se cumple cuando solo las personas autorizadas pueden conocer los datos o la información correspondientes.

- La integridad: consiste en que solo el usuario autorizado puede variar los datos (deben quedar pistas para control posterior y para auditoría.)

- La disponibilidad: se alcanza si las personas autorizadas pueden acceder a tiempo a la información.

Entre las fases de la auditoría de seguridad se encuentran:

- Auditoría de la seguridad física: se evalúan las resguardos físicos de datos, programas, instalaciones, equipos redes y soportes, y por supuesto habrá que considerar a las personas, que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no estén expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector.

- Auditoría de la seguridad lógica: es necesario verificar que cada usuario únicamente pueda acceder a los recursos que autorice el propietario, según su función, y con las posibilidades que el propietario haya fijado: consulta, modificación, eliminación y ejecución; lo que se representaría en una matriz de accesos.

En cuanto a autenticación, el método más usado es la contraseña, cuyas características estarán acordes con las normas y estándares que la organización establezca, que podrían contemplar la criticidad de los recursos que serán accedidos.

4.2. Enfoque a la información

La protección de los datos puede tener varios enfoques respecto de las características citadas: la confidencialidad, disponibilidad e integridad. Puede haber datos críticos en cuanto a su confidencialidad, u otros datos cuya criticidad viene dada por la disponibilidad; si se pierden, pueden causar perjuicios graves; o en los casos más extremos, pueden poner en peligro la corporación.

Finalmente, pueden existir otros datos críticos atendiendo a su integridad, especialmente cuando su pérdida no puede detectarse fácilmente o una vez detectada, no es fácil reconstruirlos.

Los datos pueden provenir tanto, dentro o fuera de la organización, y pueden incluir preparación, autorización e incorporación al sistema, ya sea por el cliente, por empleados, o bien ser captado por otra forma; debe revisarse cómo se verifican los errores.

Al realizar una auditoría enfocada a la información, deben de tomarse en cuenta los siguientes aspectos:

- Proceso de los datos: controles de validación, integridad y almacenamiento; que existan copias suficientes, sincronizadas y protegidas.

- Salida de resultados: controles en transmisiones, impresión y distribución.

- Retención de la información y protección en función de su clasificación: destrucción de los diferentes soportes que la contengan cuando ya no sea necesaria, o bien su desmagnetización.

- Designación de propietarios: clasificación de los datos, restricción de su uso para pruebas, inclusión de muestras para poder detectar usos no autorizados.

- Clasificación de los datos e información: debe revisarse quién la ha realizado y según qué criterios y estándares; no suele ser práctico que haya más de cuatro o cinco niveles.

- Cliente-servidor: es necesario verificar los controles en varios puntos, y no solo en uno central como en otros sistemas, y a veces en plataformas heterogéneas, con niveles y características de seguridad muy diferentes, y con posibilidad de transferencia de ficheros o de captación y exportación de datos, que pueden perder sus protecciones al pasar de una plataforma a otra.

4.3. Enfoque a la infraestructura tecnológica

Se debe conocer, comprender y analizar de manera global la gestión en tecnología de la información, su infraestructura o plataforma tecnológica y los sistemas de información aplicados a la organización, tales como:

- Granja de servidores y sus características
- Seguridad perimetral
- Estructura de redes
- Sistemas operativos
- Software y hardware de seguridad
- Inventario de hardware y software (con el propósito de establecer el nivel de obsolescencia o actualización)
- Adquisiciones (Inversiones) en recursos de tecnología de la información
- Infraestructura eléctrica

4.4. Enfoque al software de aplicación

Todos los desarrollos deben estar autorizados a distinto nivel según la importancia del desarrollo a abordar, incluso autorizados por un comité, si los costes o los riesgos superan unos umbrales.

Al realizar una auditoría enfocada al software de aplicación, deben de tomarse en cuenta los siguientes aspectos:

- Revisión de programas por parte de técnicos independientes, o bien por auditores preparados: a fin de determinar la ausencia de “caballos de Troya”, bombas lógicas y similares, además de verificar la calidad del programa.

- Protección de los programas: a menos desde dos perspectivas, de los programas que sean propiedad de la entidad, realizados por el personal propio o contratado de su desarrollo a terceros, como el uso adecuado de aquellos programas de los que se tenga licencia de uso.

4.5. Enfoque a las comunicaciones y redes

En las políticas de la organización debe reconocerse que los sistemas, redes y mensajes transmitidos y procesados son propiedad de la organización y no deben usarse para otros fines no autorizados, por seguridad y por productividad. Los usuarios tendrán restricción de accesos según dominios, únicamente podrán cargar los programas autorizados, y solo podrán variar las configuraciones y componentes los técnicos autorizados. Se revisarán especialmente las redes cuando existan repercusiones económicas, ya se trate de transferencia de fondos o comercio electrónico. Al realizar una auditoría enfocada a las comunicaciones y redes, deben de tomarse en cuenta los siguientes aspectos:

- Tipos de redes y conexiones

- Tipos de transacciones

- Tipos de terminales y protecciones: físicas, lógicas, llamadas de retorno.

- Transferencia de ficheros y controles existentes.

- Consideración especial respecto de las conexiones externas, a través de pasarelas (*gateway*) y encaminadores (*routers*).

- Internet e intranet: separación de dominios e implantación de medidas especiales, como normas y cortafuegos (*firewal*l), y no solo en relación con la seguridad, sino por accesos no justificados por la función desempeñada, como a páginas de ocio o eróticas..

- Correo electrónico: tanto por privacidad y para evitar virus, como para que el uso del correo sea adecuado y referido a la propia función, y no utilizado para fines particulares.

- Protección de programas: tanto la prevención del uso no autorizado de programas propiedad de la entidad o de los que tengan licencia de uso.

- Control sobre las páginas web: quién puede modificar y desde dónde; finalmente preocupan también los riesgos que pueden existir en el comercio electrónico.

5. PRÁCTICA DE LA AUDITORÍA DE TECNOLOGÍA DE LA INFORMACIÓN Y SU DESARROLLO

5.1. Etapas para la realización de una auditoría de sistemas

- Etapa de planeación de la auditoría: este es el primer paso para determinar cómo se va a ejecutar la auditoría; se deben identificar las razones por las que se quiere a realizar la auditoría, establecer el objetivo de la misma, el diseño de métodos, técnicas y procedimientos necesarios para llevarla a cabo y para la solicitud de documentos que servirán de apoyo para la ejecución; terminando con la elaboración de la documentación de los planes, programas y presupuestos para llevarla a cabo. Para poder llevar a cabo la etapa de planeación es necesario realizar:

    - Identificar el origen de la auditoría: esto es necesario para poder dar inicio a su planeación; en esta se debe determinar por qué surge la necesidad o inquietud de realizar una auditoría.

    - Visita preliminar al área informática: este es el segundo paso en la planeación de la auditoría, que consiste en realizar una visita preliminar al área de informática en la que se llevará a cabo la revisión, luego de conocer el origen de la auditoría y antes de iniciarla formalmente; el propósito es el de tener un primer contacto con el personal asignado a dicha área, conocer la distribución de los sistemas y dónde se localizan los servidores y equipos terminales en el centro de cómputo, sus características, las medidas de seguridad y

otros aspectos relacionados con las problemáticas que se presentan en el área auditada.

- Establecer el objetivo general de la auditoría, con el fin de indicar lo que se pretende alcanzar con el desarrollo de la auditoría informática; mas en él se plantean todos los aspectos que se pretende evaluar.

- Establecer los objetivos específicos: especificar los fines individuales que se pretenden para el logro del objetivo general, donde se señalan específicamente los sistemas, componentes o elementos concretos que serán evaluados.

- Determinar los puntos que serán evaluados: luego de determinar los objetivos de la auditoría se deben relacionar los aspectos que serán evaluados, y para esto se debe considerar aspectos específicos del área informática y de los sistemas computacionales tales como: la gestión administrativa del área de informática, el cumplimiento de las funciones del personal informático y usuarios de los sistemas, los sistemas en desarrollo, la operación de los sistemas en producción, los programas de capacitación para el personal del área y usuarios de los sistemas, protección de las bases de datos, datos confidenciales y accesos a las mismas, protección de las copias de seguridad y la restauración de la información, entre otros aspectos.

- Elaborar el plan y programa de auditoría: para realizar la planeación formal de la auditoría informática y de sistemas, en la cual se concretan los planes, programas y presupuestos para llevarla a cabo; se deben elaborar los documentos formales para el desarrollo de la

auditoría, donde se delimiten las etapas, eventos y actividades y los tiempos de ejecución para el cumplimiento del objetivo, anexando el presupuesto con los costos de los recursos que se utilizarán para llevarla a cabo.

- Algunos de los aspectos a tener en cuenta para elaborar el plan de auditoría serán: las actividades que se van a realizar, los responsables de realizarlas, los recursos materiales y tiempos, el flujo de eventos que sirven de guía, la estimación de los recursos humanos, materiales e informáticos que serán utilizados, los tiempos estimados para las actividades y la auditoría, los auditores responsables y participantes de las actividades, y otras especificaciones del programa de auditoría.

- Identificar y seleccionar los métodos y herramientas para la auditoria: en este se determina la documentación y medios necesarios para llevar a cabo la revisión y evaluación en la organización, seleccionando o diseñando los métodos, procedimientos, herramientas, e instrumentos necesarios de acuerdo con los planes, presupuestos y programas establecidos anteriormente para la auditoría. Para ello se deben considerar los siguientes puntos:

  - Establecer la guía de ponderación de cada uno de los puntos que se debe evaluar

  - Elaborar una guía de la auditoría

  - Elaborar el documento formal de la guía de auditoría

- Determinar las herramientas, métodos y procedimientos para la auditoría de sistemas

- Diseñar los sistemas, programas y métodos de pruebas para la auditoría.

- Asignar los recursos para la auditoría: con la asignación de los recursos humanos, informáticos, tecnológicos y de cualquier otro tipo, se llevará a cabo la auditoría.

- Etapa de ejecución de la auditoría: al terminar la etapa de la planeación de la auditoría, se continúa con la ejecución de la misma, la cual está determinada por las características propias, los puntos elegidos y los requerimientos estimados en la planeación.

- Etapa de dictamen de la auditoría: la tercera etapa, luego de la planeación y ejecución, es emitir el dictamen; este es el resultado final de la auditoría, donde se presentan los siguientes puntos:

  - Elaboración del informe de las situaciones que se han detectado
  - La elaboración del dictamen final
  - Presentación del informe de auditoría

  Para poder llevar a cabo esta etapa es necesario analizar la información y elaborar un informe de las situaciones detectadas, a lo que se le llamará hallazgo; las partes en que se divide son las siguientes:

  - Sumilla: es el título o encabezamiento que resume la observación

- Condición: este término se refiere al hecho irregular o deficiencia determinada, cuyo grado de desviación debe ser demostrada y sustentada con evidencias.

- Criterio: es la norma o estándar técnico profesional, alcanzable en el contexto evaluado, que permite al auditor tener la convicción de que es necesario superar una determinada acción u omisión de la organización en procura de mejorar la gestión. Los criterios más comunes a utilizar en la auditoría son: normas técnicas, estándares internacionales, políticas internas de la organización y elementos de la estructura del control interno.

- Causa: es la razón fundamental por la cual ocurrió la condición, o el motivo por el que no se cumplió el criterio o norma.

- Efecto: es la consecuencia real o potencial cuantitativo o cualitativo que ocasiona la observación, indispensable para establecer su importancia y recomendar a la administración que tome las acciones requeridas para corregir su condición.

- Elaborar el informe final: el auditor debe terminar la elaboración del informe final de auditoría y complementarlo con el dictamen final, para después presentarlo a los directivos del área auditada, para que conozcan la situación actual del área, antes de presentarlo al representante o gerente de la empresa.

- El informe debe contener los siguientes puntos: introducción, objetivos (general, específicos), alcance de la auditoria, antecedentes

(base legal de la organización), hallazgos, observaciones, conclusiones, recomendaciones y anexos.

- Una vez comentadas las debilidades encontradas con los auditados, se elabora el informe final, lo cual es garantía de que los auditados ya aceptaron las debilidades encontradas y que luego se plasman en documentos formales.

- Elaborar el Informe formal: el último paso es presentar formalmente el informe y el dictamen de la auditoría al más alto de los directivos de la organización, donde se informa de los resultados de la misma. Tanto el informe como el dictamen deben presentarse en forma resumida, correcta y profesional.

Tabla II. **Etapas de una aditoría de sistemas**

ETAPAS	PASOS A REALIZAR
Planeación de la Auditoria de Sistemas	1. Identificar el origen de la auditoria 2. Realizar una visita preliminar al área que será evaluada 3. Establecer los objetivos de la auditoria 4. Determinar los puntos que serán evaluados en la auditoria 5. Elaborar planes, programas y presupuestos para realizar la auditoria 6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoria 7. Asignar los recursos y sistemas computacionales para la auditoria
Ejecución de la Auditoria de Sistemas	1. Realizar las acciones programadas para la Auditoria 2. aplicar los instrumentos y herramientas para la auditoria 3. Identificar y elaborar los documentos de oportunidades de mejoramiento encontradas 4. Elaborar el dictamen preliminar y presentarlo a discusión 5. Integrar el legajo de papeles de trabajo de la auditoria
Dictamen de la Auditoria de Sistemas	1. Analizar la información y elaborar un informe de situaciones detectadas 2. Elaborar el Dictamen final 3. Presentar el informe de auditoria

Fuente: http://auditordesistemas.blogspot.com/2011/11/metodologia-para-realizar-auditoria.html. Consulta: agosto de 2013.

5.2. Técnicas para la auditoría informática

Las técnicas de auditoría son métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que sustente sus observaciones y recomendaciones; su empleo se basa en su criterio, según las circunstancias. Dentro de las técnicas utilizadas en una auditoría informática se pueden mencionar:

- Cuestionarios: las auditorías informáticas se realizan recabando información y documentación de todo tipo. Los informes finales dependen de analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del consiste en lograr obtener toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias. Estos cuestionarios deben de ser muy específicos para cada situación, y se debe de tener cuidado en su fondo y forma. Sobre esta base, se estudia y analiza la documentación recibida, de modo que tal análisis determine a su vez la información que deberá elaborar el propio auditor. El cruce de información es una de las bases fundamentales de la auditoría.

- Entrevistas: es una de las actividades personales más importante que realiza el auditor; en ellas, se acumula información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas en cuestionarios. La entrevista entre auditor y auditado se basa fundamentalmente en el concepto interrogatorio. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente a una serie de preguntas sencillas y variadas. Sin embargo,

esta sencillez es solo aparente, tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso en particular.

- Lista de chequeo: el auditor deberá aplicar la técnica de la lista de chequeo, de modo que el auditado responda claramente a las preguntas que se tengan formuladas. Se deberá interrumpir lo menos posible a este, solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta. En algunas ocasiones, se hará necesario para que responda con amplitud un tema concreto.

- Trazas y/o huellas: con continuidad, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas y no otras. Para ello se apoya en productos de software, que entre otras funciones, rastrean los caminos que siguen los datos a través del programa.

- Software para auditoría: se utilizan productos de software llamados “paquetes de auditoría”, estos sirven para la obtención de muestreos estadísticos que permitan la elaboración de una hipótesis de la situación real. En la actualidad, los productos de Software especiales para la auditoría informática, se orientan principalmente hacia la extracción de datos de ficheros y bases de datos de la organización auditada.

- Peritaje informático: se conoce como peritaje informático a los estudios e investigaciones orientados a la obtención de una prueba informática de aplicación en un asunto judicial, para que sirva a un juez en la toma de decisiones sobre la culpabilidad o inocencia del involucrado.

- Observación: esta técnica consiste en examinar los diferentes aspectos que intervienen en el funcionamiento del área informática y los sistemas de software.

6. APLICACIÓN DE LAS PRÁCTICAS INTERNACIONALES PARA LA GESTIÓN DE TECNOLOGÍA DE LA INFORMACIÓN EN UNA AUDITORÍA A LAS DE REDES PRIVADAS VIRTUALES –VPN-

Se desarrollará a base de ejemplo una auditoría basada en redes privadas virtuales debido a su incremento en los últimos años en todo el mundo, ya que se hace necesaria la búsqueda de nuevas formas de conexión en cualquier momento y en todo lugar; el ser humano siempre busca nuevas formas de poder realizar sus actividades de una forma fácil, en ello se muestra la necesidad de utilizar una red privada virtual.

No obstante ante el incremento de esta necesidad, surgen ciertos mecanismos engañosos que afectan el entorno de estas redes y su seguridad; por ende a la información que estas respaldan.

Estos mecanismos engañosos, en su mayoría de casos afectan la seguridad, acarreando como consecuencia diferentes riesgos informáticos, generando un gran impacto negativo si no se tiene el control respectivo dentro de dicha entidad.

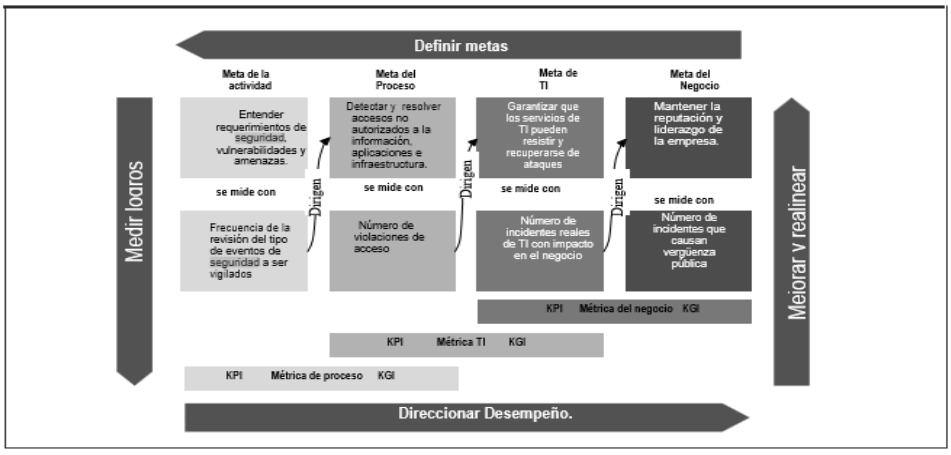
Para mitigar o eliminar estos riesgos se deben definir controles informáticos como la seguridad de los sistemas de información, la cual se define como la disciplina que trata de los riesgos informáticos, en donde la auditoría se involucra en este proceso de protección y preservación de la información y de sus medios de proceso.

Tomando en cuenta este concepto, si los controles informáticos son llevados de manera inadecuada, surge una nueva necesidad, la de auditar dicho control para determinar las amenazas, vulnerabilidades y riesgos que tiene el servicio informático relacionados con las redes privadas virtuales.

.

Se propone realizar una auditoría basada en COBIT 4.0, con el proceso DS5, para auditar la seguridad de las redes privadas virtuales, con el fin de mejorar la disponibilidad, confiabilidad, confidencialidad, cumplimiento e integridad de la información, ya que estas buenas prácticas son genéricas y están previstas a ser aplicables y adaptables en cualquier organización independiente del tipo, tamaño o naturaleza. Están enfocadas a los dominios de diseño, administración y seguridad, adecuado a su realidad, ya que el objetivo de las buenas prácticas es alinear la tecnología con el negocio, como se puede ver en la siguiente figura.

Figura 18. **Relación entre procesos, metas y métricas (DS5)**



Fuente: ISACA. http://www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Auditing-Spanish-.aspx. Consulta: agosto de 2013.

De acuerdo con estas consideraciones, las buenas prácticas propuestas evalúan de forma completa los dominios de diseño, administración y seguridad de la red inalámbrica, relacionados con las metodologías, estándares y normas internacionales.

El proceso DS5 (garantizar la seguridad de los sistemas) busca garantizar la seguridad que satisface el requisito de negocio de TI para mantener la integridad de la información y de la infraestructura de procesamiento, y minimizar el impacto de las vulnerabilidades e incidentes de seguridad, enfocándose en la definición de políticas, procedimientos y estándares de seguridad de tecnología y en el monitoreo, detección, reporte y resolución de las vulnerabilidades e incidentes de seguridad.

Esto se logra con:

- El entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.

- La administración de identidades y autorizaciones de los usuarios de forma estandarizada.

- Probando la seguridad de forma regular.

Y se mide con:

- El número de incidentes que dañan la reputación con el público.

- El número de sistemas donde no se cumplen los requerimientos de seguridad.

- El número de violaciones en la segregación de tareas.

Asimismo, se utilizarán también las buenas prácticas de TI, ISO 17799, enfocadas a la seguridad en el desarrollo de sistemas de información y a la gestión de la continuidad del negocio. Tomando los objetivos de control como políticas de seguridad, control de accesos, seguridad física y del entorno, entre otros.

A continuación se desarrollará el caso basado en redes privadas virtuales –VPN- , en donde se pretende ejemplificar los pasos a realizar en una auditoría.

Antes de iniciar con el plan y programa de auditoría, se debe de realizar una visita preliminar para conocer la forma en que el área de informática de la organización administra la red privada virtual, sus procedimientos, políticas, configuraciones, accesos, entre otros. Por lo que se debe de concertar una cita con la persona encargada de su administración.

Ya obtenido el primer acercamiento con el área informática y los insumos necesarios para llevar a cabo la revisión, se procede a realizar el plan y programa de la auditoría.

CONCLUSIONES

1. La auditoría de gestión a las tecnologías de información apoyan en la revisión y evaluación de los controles, sistemas, procedimientos informáticos, su utilización, eficiencia y seguridad, a fin de que por medio del señalamiento se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones.

2. La gestión de tecnología de información evalúa los sistemas de información en general, desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información, contribuyendo con la dirección al logro de una administración eficaz.

3. Los estándares ayudan a definir los requisitos para una buena gestión de la seguridad de la información, ya que se han concebido para garantizar la selección de controles genéricos, para que todo tipo de organización pueda implementarlas.

4. El uso de estándares en la gestión de la tecnología de la información posibilita la toma de decisiones adecuadas que garanticen las relaciones costo-beneficio y la optimización de su uso.

RECOMENDACIONES

1. Las organizaciones deben de adoptar estándares internacionales para basar sus evaluaciones sobre el nivel de cumplimiento de los procesos utilizados para dirigir y controlar la organización, hacia el logro de sus objetivos.

2. Debe aplicarse la gestión de tecnología de información, utilizando adecuadamente los recursos tecnológicos de la organización, para lograr los beneficios esperados.

3. El uso de una metodología, apoyada de un conjunto de buenas prácticas, ayuda a una organización a planificar, diseñar, ejecutar y evaluar los planes de tecnología de la información necesarios para el cumplimiento de los objetivos establecidos.

BIBLIOGRAFÍA

1. ALFARO PAREDES, Emigdio Antonio. *Metodología para la auditoría integral de la gestión de la tecnología de la información.* Pontificia Universidad Católica de Perú. [en línea]. <http://www.tesislatinoamericanas.info/index.php/record/view/48709> [Consulta: mayo de 2013].

2. Colombia. *Norma técnica colombiana NTC-ISO/IEC 27001*. [en línea]. http://www.ehu.es/Degypi/PMBOK/cap3PMBOOK.htm#3.1_Procesos _de_Dirección_de_Proyectos>[Consulta: junio de 2013].

3. GLOBAL STANDARD. *Guía de los fundamentos de la dirección de proyectos.* 4a ed. Pennsylvania: Project Management Institute, 2008. 393 p.

4. GUITART HORMIGO, Isabel. *Fundamentos de sistemas de información.* Universidad de Cataluña, España. [en línea]. <http://ocw.uoc.edu/informatica-tecnologia-ymultimedia/fundamentos-de-sistemas-de-informacion/Course_listing> [Consulta: julio de 2013].

5. ISACA. *Estàndares.* [en línea]. <http://www.isaca.org/Knowledge-Center/Standards/Pages/Standards-for-IS-Auditing-Spanish-.aspx> [Consulta: agosto de 2013].

6. ISTMF LIBRARY. *Fundamentos de gestión de servicios TI basados en ITIL.* USA: Van Harem Publishing, 2004. 250 p.

6. *Manual de auditoría de gestión a las tecnologías de información y comunicaciones.* [en línea]. <http://bibliotecavirtual.olacefs.com/gsdl/collect/guasyman/archives/HASH0155.dir/ManualAuditoriaGestionTICs.pdf>[Consulta: agosto de 2013].

6. OLALDE AZKORRETA, Karle. *Introducción a los procesos de DP para un proyecto.* [en línea]. <http://www.ehu.es/Degypi/PMBOK/cap3PMBOOK.htm>. [Consulta: agosto de 2013].

7. SALINAS DUARTE, Andrés Ernesto. *Obstáculos en la gestión de proyectos en tecnologías de información y comunicación y posibles soluciones.* [en línea]. <http://www.acis.org.co/fileadmin/Articulos/Andres_Salinas.pdf>. [Consulta: agosto de 2013].

8. SLIDESHARE. *Mejores prácticas para el manejo de tecnología de información en las organizaciones*. [en línea]. <http://www.slideshare.net/rosmelys/mejores-practicas-para-el-manejo-de-tecnologa-de-informacin-en-la-organizaciones> [Consulta: junio de 2013].

9. VILCHES, Ernesto. *Guía de gestión de servicios basada en fundamentos de ITIL.* [en línea]. http://albinogoncalves.files.wordpress.com/2011/03/itil-v3-2010.pdf>. [Consulta: junio de 2013].

10. WIKIPEDIA. *Objetivos de control para la información.* [en línea]. http://es.wikipedia.org/wiki/Objetivos_de_control_para_la_informaci%C3%B3n_y_tecnolog%C3%ADas_relacionadas> [Consulta: julio de 2013].

APÉNDICES

Apéndice 1. **Planificación de la auditoría**

Apéndice 1a. **Revisión a la gestión de conexiones de red privada virtual –VPN-**

1. Objetivo general: evaluar la efectividad y aseguramiento de la gestión de conexiones de red privada virtual –VPN-

2. Objetivos específicos:

- Evaluar el control interno establecido para la gestión de conexiones de red privada virtual.

- Evaluar la administración de accesos a la red privada virtual y la confidencialidad de la información brindada a través de la misma.

- Evaluar el registro de las pistas de auditoría en conexiones a la red privada virtual.

3. Alcance: la evaluación comprenderá el ambiente de control relacionado, correspondiente al año 2013.

4. Criterios: las pruebas se enfocarán en el análisis de la información recabada de acuerdo con su importancia relativa, y otros criterios que el auditor, a su juicio profesional considere conveniente, de conformidad al alcance definido.

5. Informe: resultado de la ejecución de la auditoría conforme a la programación formulada, evidenciada en documentación que sustente resultados conforme a los objetivos establecidos; se espera un informe de auditoría a rendir ante las autoridades de la institución.

6. Presupuesto de tiempo: de conformidad con los recursos disponibles, el alcance de la auditoría y programación de pruebas, se asignará el tiempo efectivo conforme a las actividades que se resumen a continuación:

Apéndice 1b. **Asignación de tiempo para las actividades**

Actividad	Tiempo asignado
Familiarización	2 semanas
Evaluación preliminar de Control interno	1 semana
Definición de plan y programa de auditoría	1 semana
Ejecución de auditoría	1 semana
Elaboración y presentación de proyecto de informe	Dos días

Fuente: elaboración propia.

7. Recursos:

- Personal nombrado: auditores de sistemas de información
- Elaborado por: auditores de sistemas de información
- Aprobado por: jefe del departamento de auditoría de sistemas de información y estudio

Apéndice 2. **Programa de la auditoría**

Revisión a la gestión de conexiones de red privada Virtual -VPN-

- Definición: evaluar los controles informáticos asociados al registro, autorización y monitoreo de usuarios y sus gestiones realizadas mediante conexiones –VPN-, a fin de establecer la efectividad de los mismos.

.

- Objetivos específicos:

    - Evaluar el control interno establecido para la gestión de conexiones de red privada virtual.
    - Evaluar la administración de accesos a la red privada virtual.
    - Evaluar el registro de las pistas de auditoría para conexiones a la red privada virtual.

- Alcance: el examen comprenderá la evaluación del ambiente de control relacionado, correspondiente al año 2013 y otros que el auditor considere necesarios para las pruebas de la auditoría.

- Selección de la muestra: la muestra se enfocará en el análisis de la información registrada en las bitácoras de conexiones -VPN-, correspondientes al año 2013 y otros datos que el auditor considere necesarios para las pruebas de la auditoría.

Apéndice 2a. **Trabajo a desarrollar**

Núm.	DESCRIPCIÓN	REFERENCIA P/T	HECHO POR	REVISADO POR
1	**Para cumplir con el objetivo 1:** Evaluar el control interno establecido para la gestión de conexiones de red privada virtual. **Elaborar lo siguiente:** • Con base en los resultados de la familiarización y evaluación preliminar de control interno, efectuar una revisión al marco de control, definido para la gestión de conexiones de red privada virtual. • Identificar y evaluar los lineamientos formales implementados que refieren las actividades de control actuales. • Solicitar las reglas del Firewall incluyendo IP´S para -VPN- • Analizar y concluir al respecto.	**PT.1** **PT.3** **PT.1** **PT.3** **PT.2** **PT.3**	**AUDITORES**	**SUPERVISOR**

Continuación del apéndice 2a.

Núm.	DESCRIPCIÓN	REFERENCIA P/T	HECHO POR	REVISADO POR
2	**Para cumplir con el objetivo 2:** Evaluar la administración de accesos a la red privada virtual. **Elaborar lo siguiente:** • Solicitar al área de informática listado de usuarios que poseen acceso a la red privada virtual. • Del listado obtenido de usuarios que tienen acceso a la red privada virtual realizar lo siguiente: o Generar un listado de usuarios con acceso a la red privada virtual y revisar que coincida con el listado proporcionado. o Revisar la existencia de usuarios genéricos y su función. • Analizar y concluir al respecto.	**PT.2** **PT.4** **PT.4**	**AUDITOR**	**SUPERVISOR**

Continuación del apéndice 2a.

Núm.	DESCRIPCIÓN	REFERENCIA P/T	HECHO POR	REVISADO POR
3	**Para cumplir con el objetivo 3:** Evaluar el registro de las pistas de auditoría para conexiones a la red privada virtual. **Elaborar lo siguiente:** • Solicitar al área informática los log´s de acceso a la red privada virtual. • De los log´s proporcionados seleccionar una muestra y realizar lo siguiente: o Revisar que los usuarios que tienen operaciones registradas, se encuentran en el listado de accesos autorizados que proporcionó el área Informática. Realizar consultas a las bitácoras de base de datos, para verificar si los usuarios identificados anteriormente tienen operaciones en horario inhábil.	**PT.2** **PT.2** **PT.5** **PT.2**	**AUDITOR**	**SUPERVISOR**

Fuente: elaboración propia.

Apéndice 3. **Cuestionario de control interno *PT. 1***

Revisión a la gestión de conexiones de red privada virtual -VPN-

Datos generales: **Fecha:_____**

Nombre y puesto que desempeña:_____

Favor responder las preguntas en los espacios correspondientes y adjuntar la documentación que corresponde.

NÚM.	PREGUNTAS	SÍ	NO	COMENTARIOS
	Objetivo: Evaluar los controles informáticos asociados al registro, autorización y monitoreo de usuarios y sus gestiones realizadas mediante conexiones a la red privada virtual -VPN-			
1	¿Se cuenta con políticas, procedimientos y/o manuales relacionados con la administración y uso de las conexiones de la red privada virtual –VPN-? En caso afirmativo, favor indicar el nombre completo de la política, procedimientos y/o manuales aplicables y proporcionar una copia. En caso negativo, favor describir en comentarios las actividades que realizan para la administración y uso de las conexiones de la red privada virtual –VPN.	X		GUÍA PARA VPN
2	¿Se cuenta con normas, políticas o procedimientos para la gestión de altas, bajas o modificación de accesos de los usuarios de conexiones -VPN-?	X		Administración para solicitudes de accesos VPN.

Continuación del apéndice 3.

NÚM.	PREGUNTAS	SÍ	NO	COMENTARIOS
	En caso afirmativo, favor indicar el nombre completo de la norma, política o procedimiento y proporcionar una copia. En caso negativo, favor describir en comentarios las actividades que realizan para administrar la gestión de altas, bajas o modificación de accesos de los usuarios para el uso de conexiones –VPN-			
3	¿Cuáles son los medios utilizados para la autenticación de usuarios en conexiones VPN? Explique.			
4	¿Se cuenta con pistas de control (log's) que permitan revisar las actividades realizadas por un usuario a través de una conexión –VPN-?	X		Existe un conector entre el servidor de VPN y el servidor de autenticación.
	En caso afirmativo: Indicar si existen actividades de monitoreo de estos log's.	X		
	En caso negativo, favor describir en comentarios las acciones que realizan para monitorear las actividades realizadas por un usuario a través de una conexión –VPN-?	X		Existe monitoreo por medio de log´s.

Continuación del apéndice 3.

NÚM.	PREGUNTAS	SÍ	NO	COMENTARIOS
5	¿Se cuenta con un documento o referencia donde se tengan definidos los siguientes aspectos?	X		Conexiones VPN
	• Tiempo máximo de conexión a –VPN-	X		
	• Protocolos autorizados a ser utilizados en conexiones VPN.	X		
	• Días y horarios permitidos de conexión.	X		
	• Clasificación de la información que no es permitido operar a través de este medio.	X		

Respondido por: _____ Firma y sello

Fuente: elaboración propia.

Apéndice 4. **Requerimiento Núm. 01** ***PT. 2***

Para: Persona encargado del área Informática

De: Auditor de sistemas

Asunto: Requerimiento de información

Derivado a la revisión a la gestión de conexiones de red privada virtual –VPN- y para efectos de la ejecución de la auditoría solicito se sirva proporcionar la siguiente información:

- Listado de cuentas de usuarios con acceso a -VPN- .
- Reglas del Firewall incluyendo IP´S para -VPN- .
- Log´s de acceso a la red privada virtual del año 2013.

Atentamente,

Auditor de sistemas.

Apéndice 5. **Ejecución de la auditoría. Actividades para cumplir con los objetivos** ***PT. 3***

Actividades para cumplir con el objetivo 1

Objetivo 1: evaluar el control interno establecido para la gestión de conexiones de red privada virtual.

- Se identificaron y evaluaron los lineamientos formales implementados que refieren las actividades de control actuales por medio del cuestionario de control interno. Los lineamientos identificados son los siguientes:
    - Para administración, monitoreo cuentan con la guía para VPN.
    - Para la gestión de altas, bajas o modificación de acceso cuentan con la política de administración para solicitudes de accesos VPN.
    - Existe monitoreo por medio de Log sobre la utilización de la red VPN.
    - Se tienen reglas establecidas del firewall.
- Se solicitaron las reglas del firewall incluyendo IP´S para -VPN-

De lo cual se concluyó: existen lineamientos para poder evaluar el control interno establecido para la gestión de conexiones de red privada virtual.

Actividades para cumplir con el objetivo 2 ***PT. 4***

Objetivo 2: evaluar la administración de accesos a la red privada virtual.

- Se solicitó al área informática el listado de usuarios que poseen acceso a la red privada virtual.

- Se generó listado de usuarios con acceso a VPN desde la línea de comando, con la instrucción NET GROUP /DOMAIN.

- Se verificó la existencia de usuarios genéricos en los perfiles de VPN.

De lo cual se concluyó: existen usuarios genéricos para el uso de la red privada virtual –VPN- y accesos –VPN- asociados a usuarios de soporte externo con contrato expirado.

Actividades para cumplir con el objetivo 3 ***PT. 5***

Objetivo 3: evaluar el registro de las pistas de auditoría para conexiones a la red privada virtual.

- Log´s proporcionados por la gerencia de informática.

- Se generó listado de usuarios con acceso a VPN desde la línea de comando con la instrucción NET GROUP /DOMAIN.

- De los log´s proporcionados se observó lo siguiente:

    - Usuarios que no se encuentran en el listado proporcionado por la gerencia de informática.

- Usuarios sin registro de información dentro de la institución.

De lo cual se concluyó: falta de disponibilidad de registros históricos de las conexiones -VPN-

Apéndice 6. **Informe de auditoría. Revisión a la gestión de conexiones de red privada virtual -VPN-**

A. Hallazgo 1: falta de disponibilidad de registros históricos de conexiones VPN. Durante la ejecución de la auditoría, se determinó que existe dificultad para obtener información específica, relacionada con las conexiones VPN de los usuarios a través de la bitácora del firewall, debido al gran volumen de datos registrados y la cantidad de trabajo que conlleva extraerlos.

- Criterios:

  - Las políticas internas de la organización establecen que es conveniente dejar por escrito, los procedimientos de autorización, registro, custodia y control oportuno de todas las operaciones. Los procedimientos de registro, autorización y custodia son aplicables a todos los niveles de organización, independientemente de que las operaciones sean financieras, administrativas u operativas; deben contar con la definición de su campo de competencia y el soporte necesario para rendir cuenta de las responsabilidades inherentes a su cargo.

- La norma internacional ISO 17779 indica que se deben establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes.

- Causa: la bitácora del firewall integra todos los registros históricos de conexiones, incluyendo las conexiones VPN en un solo repositorio; por lo que es necesario manejar grandes volúmenes de información, para separar los registros correspondientes a conexiones específicas de VPN.

- Efecto: se dificulta poder determinar las fechas y horas en que un usuario realizó conexiones VPN hacia los sistemas de la organización, con el propósito de brindar trazabilidad de sus operaciones realizadas en dichos sistemas.

- Recomendaciones:

  - Considerar la incorporación de un servidor de bitácoras que permita la administración efectiva de diferentes archivos de log´s y garantice su disponibilidad cuando se requiera.

  - Considerar la incorporación de herramientas de generación de reportes que faciliten la gestión de los log´s, al momento de revisiones de control o de requerimientos de seguridad.

B. Hallazgo 2: accesos VPN activos asociados a usuarios de soporte externo con contrato expirado. En bitácoras proporcionadas para el año 2013, se identificaron conexiones VPN, que corresponden a usuarios que prestaron

sus servicios para la organización, sin embargo se verificó que el contrato de estas personas no se encuentra actualmente vigente.

Apéndice 6a. **Usuarios y fechas en que realizaron conexiones**

No.	Usuario	Fechas en las que realizaron conexiones en bitácoras proporcionadas
1	Luis Fernando Romero	18-sep-13
2	María Luisa Pimentel	10-oct-13
3	Ricardo Morataya	12-oct-13

Fuente: elaboración propia.

El personal referido pertenecía a un grupo de asesores de una empresa externa a la organización; sin embargo, esta empresa brindó servicios de soporte y desarrollo especializado para un sistema de información gerencial en el año 2009, según contrato CONTRATO-700-2009, mismo que se encuentra expirado.

- Criterios:
    - La norma internacional Cobit 4.0 indica que se debe proporcionar una protección adecuada contra accesos no autorizados, modificaciones y envíos incorrectos de información sensitiva durante la transmisión de datos.
    - La norma ISO 17779 indica que se requiere un conjunto de controles para lograr y mantener la seguridad de las redes informáticas. Los

administradores de redes deben implementar controles para garantizar la seguridad de los datos en la misma, y la protección de los servicios conectados contra el acceso no autorizado.

- Causa: falta de remoción oportuna de los accesos otorgados por el área Informática al personal externo, al término de su relación contractual con la organización.

- Efecto: el acceso de VPN vigente para estos usuarios, les permite conectarse a los servidores y equipos donde figuran como administradores locales, a través del uso del escritorio remoto, teniendo plena libertad de operar en estos servidores y equipos.

- Riesgo: que el acceso sea utilizado para obtener información sensible de la organización y ser enviados a sitios externos.

- Recomendación: que el área informática coordine la remoción inmediata de los accesos referidos en el hallazgo, y a la vez se implemente una revisión sobre la totalidad de los usuarios con acceso a VPN, con el fin de depurar los accesos asignados a los mismos, conforme al puesto y funciones que desempeñan.

C. Hallazgo 3: cuentas no personales (genéricas) con acceso activo a redes VPN. Se identificaron cuentas activas con acceso activo a VPN, que no identifican de forma individual al personal que las usa, condicionando la trazabilidad de lo ejecutado con dichas cuentas.

- Criterio: la buena práctica de tecnología de la información COBIT 4.0, establece que para una buena administración de accesos, debe

considerar el uso de una identificación personal de usuario de tal manera que este pueda ser localizado y sea responsable de sus acciones. El uso de identificadores para un grupo de usuarios no debe permitirse.

- Causa: debilidad en las actividades de supervisión y monitores de accesos.

- Efecto: condiciona la identificación de la persona responsable de las conexiones realizadas con esta cuenta, en operaciones específicas para efectos de la rendición de cuentas.

- Recomendación: proceder a remover el acceso VPN de las cuentas no personales que figuran en los perfiles de VPN y a brindar el acceso a las cuentas específicas del personal que lo necesite según su función y puesto de trabajo.