INSTITUTO POLITÉCNICO NACIONAL

ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA
UNIDAD ZACATENCO

SECCIÓN DE ESTUDIOS DE POSGRADO E INVESTIGACIÓN
PROGRAMA DE POSGRADO EN INGENIERÍA DE SISTEMAS
MAESTRÍA EN CIENCIAS EN INGENIERÍA DE SISTEMAS

"METODOLOGÍA PARA EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL COMO UN MEDIO DE SEGURIDAD EN EL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN".

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRO EN CIENCIAS EN INGENIERÍA DE SISTEMAS.

PRESENTA:

LIC. DIANA MARISOL PRADO OSEGUERA.

DIRECTOR DE TESIS:

M. en C. LEOPOLDO A. GALINDO SORIA.

MÉXICO D.F., JUNIO DE 2009.

SIP-14

INSTITUTO POLITECNICO NACIONAL

SECRETARIA DE INVESTIGACION Y POSGRADO

ACTA DE REVISION DE TESIS

En la Ciudad de México, D. F. siendo las 17:00 horas del día 25 del mes de Junio del 2009 se reunieron los miembros de la Comisión Revisora de Tesis designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de la E.S.I.M.E. ZAC para examinar la tesis de grado titulada:

"METODOLOGÍA PARA EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL COMO UN MEDIO DE SEGURIDAD EN EL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN"

Presentada por el alumno:

PRADO	OSEGUERA	DIANA MARISOL
Apellido paterno	materno	nombre(s)

Con registro:

A	0	7	0	3	6	9

aspirante al grado de:

MAESTRO EN CIENCIAS EN INGENIERÍA DE SISTEMAS

Después de intercambiar opiniones los miembros de la Comisión manifestaron ***SU APROBACIÓN DE LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director de tesis

M. EN C. LEOPOLDO ALBERTO GALINDO SORIA

Presidente

DR. LUÍS MANUEL HERNÁNDEZ SIMÓN

Segundo Vocal

M. EN C. JORGE ARTURO REYES BONILLA

Tercer Vocal

M. EN C. ENRIQUE UGALDE MIRANDA

Secretario

DRA. CLAUDIA HERNÁNDEZ AGUILAR

Suplente

M. EN C. EFRAÍN JOSÉ MARTÍNEZ ORTIZ

EL PRESIDENTE DEL COLEGIO

DR. JAIME ROBLES GARCÍA

SECCION DE ESTUDIOS DE POSGRADO E INVESTIGACION

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA DE CESIÓN DE DERECHOS

En la Ciudad de México, D. F., el día 15 de Junio de 2009, la que suscribe Diana Marisol Prado Oseguera, egresada del Programa de Maestría en Ingeniería de Sistemas, con número de registro A070369, adscrito a la Sección de Estudios de Posgrado e Investigación de la ESIME, Unidad Profesional "Adolfo López Mateos", manifiesto que es autor intelectual del presente Trabajo de Tesis, bajo la dirección del M. en C. Leopoldo Alberto Galindo Soria y cede los derechos del trabajo titulado:

"METODOLOGÍA PARA EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL COMO UN MEDIO DE SEGURIDAD EN EL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN".

Al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información, no deben de reproducir el contenido textual, gráficas o datos del trabajo, sin el permiso expreso del autor y/o director de trabajo.

Este puede ser obtenido, a la siguiente dirección electrónica:

mayma_2000@yahoo.com

Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Diana Marisol Prado Oseguera.

Nombre y Firma

RESUMEN.

“METODOLOGÍA PARA EL ESTABLECIMIENTO DE OBJETIVOS DE CONTROL COMO UN MEDIO DE SEGURIDAD EN EL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN”.

Para la mayoría de las empresas, la información y las tecnologías que la soportan, representan recursos de gran valor para las mismas. Por ello, la seguridad de estos elementos debería de ser notable. Actualmente, la seguridad de la información en las Tecnologías de Información (TI), no se le ha dado la importancia necesaria; dado a que existe una falta de conocimiento en esta materia.

Por lo tanto, éste trabajo de tesis, se realizó con la finalidad de proponer una metodología dirigida para aquellas empresas que quieren mejorar ó evitar una situación de riesgo, por tener un escaso conocimiento en seguridad de la información de esta área.

Su propósito es que mediante el establecimiento de objetivos y de actividades que permitan alcanzar éstos, sea posible crear un medio ambiente de seguridad en la información contenida en las Tecnologías de Información.

Durante el desarrollo de este proyecto de tesis, se detallará cada una de las fases que integran la metodología propuesta y se explicarán las actividades que las complementan, al final de este trabajo escrito, se presenta un ejemplo de su aplicación.

ABSTRACT.

"METHODOLOGY FOR THE ESTABLISHMENT OF CONTROL OBJECTIVES AS A WAY OF SECURITY IN THE AREA OF TECHNOLOGIES OF INFORMATION".

ABSTRACT.

For the majority of the companies, the information and the technologies that it support, they represent resources of great value for the same ones. For it, the safety of these elements should be notable. Nowadays, the safety of the information in the Information Technology (IT), It does not have the necessary importance; given to that exists an absence of knowledge in this matter.

Therefore, this work of thesis, it was realized with the purpose of proposing a methodology directed for those companies that want to improve or to avoid a situation of risk, for having an insufficient knowledge in safety of the information of this area.

Its intention is that by means of the establishment of objectives and activities that allow to reach these, is possible to create a safety environment in the information contained in the Information Technology.

During the development of this project of thesis, there will be detailed each of the phases that integrate the proposed methodology and will be explained the activities that complement them, at the end of this written work, there appears an example of its application.

ÍNDICE GENERAL.

ÍNDICE GENERAL.

ÍNDICE GENERAL.

ÍNDICE GENERAL.

ÍNDICE DE TABLAS.

ÍNDICE DE TABLAS.

Índice de Figuras

Índice de Figuras

Índice de Figuras

SIGLAS, ABREVIATURAS Y ACRÓNIMOS.

ARO	Determinación de la frecuencia anual.
ALE	Determinación de la expectativa de pérdida anual.
BS7799	Estándar creado por British Standards Institute (BSI) titulado "Information Security Management Systems" (Administración de seguridad en sistemas de información).
CEO	Chief Executive Officer (Director General).
CFO	Chief Financial Officer (Director Financiero).
CIO	Chief Information Officer (Director de Información).
CMM	Capability Maturity Model (Modelo de Capacidad y Madurez).
COBIT	Control Objectives for Information and related Technology (Objetivos de Control para la Información y Tecnología relacionada).
COCO	Canadian Criteria of Control Committee (Modelo de Control Interno COCO)
CONTROL TURNBULL	Internal Control Guidance for Directors on the Combined Code-UK (Guía de Control Interno para directores).
COSO	Internal Control - Integrated Framework del Committee of Sponsoring Organizations of the Treadway Commission (Estándar de Control Interno desarrollado por el Comité de Organizaciones patrocinadoras de la comisión Treadway).
DFD	Data Flow Diagram (Diagrama de Flujo de Datos).
ERP	Enterprise Resource Planning (Software integral -Planeación de Recursos Empresariales)
ISACA	Information Systems and Audit Control Association (Asociación de Auditoria y Control de Sistemas de Información).
ISO	International Organization for Standardization (Organización Internacional para la Estandarización).
ITGI	Information Technology Governance Institute (Comité de Investigación del Instituto de Gobierno de TI).
ITIL	Information Technology Infrastructure Library (Conjunto de mejores prácticas para las Tecnologías de la Información).
LAN	Local Area Network (Red de área local).
PYME	Pequeña y mediana empresa.
RACI-RASCI	Responsible, Accountable, Supportive, Consulted, Informed
ROSI	Rendimiento de la inversión en seguridad.
SAC	Systems Audit ability and Control del Institute of Internal Auditors Research Foundation (Sistemas de Auditoria y Control).
SAP	Systeme, Anwendungen und Produkte (Sistemas, Aplicaciones y Productos),
SOX	Ley Sarbanes Oxley
SLE	Determinación de la expectativa de pérdida simple.
TI	Tecnologías de Información.
WAN	World Area Network (Red de Área Mundial)

GLOSARIO.

-A-

ACTIVIDADES DE CONTROL: Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que la respuesta a los riesgos sea correctamente efectuada. Las actividades de control ocurren en todos los niveles y funciones de la organización. [Santillana, 2003]

ACTIVO: Cualquier elemento de valor para una organización, como componentes de hardware, software, datos, personas y documentos. [Microsoft, 2004]

ADMINISTRACIÓN: La palabra "Administración" se forma del prefijo *"ad"*, que significa hacia, y de *"ministratio"*, que viene a su vez de *"minister"*, vocablo compuesto de *"minus"*, comparativo de inferioridad, y del sufijo *" ter"*, que sirve como término de comparación. [Reyes, 1992]. Conjunto de técnicas sistemáticas que permite que las organizaciones sociales logren sus fines. Acción de planear, controlar y dirigir los recursos de una organización con el fin de lograr los objetivos deseados. [Hernández, Ballesteros, 1990].

ADMINISTRACIÓN DE RIESGO: Esfuerzo global de administrar el riesgo hasta alcanzar un nivel aceptable en la empresa. Y le evaluación del riesgo es el proceso de identificar y asignas propiedades a los riesgos para le empresa. [Microsoft, 2004].

ADQUIRIR E IMPLEMENTAR (AI): Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia: • ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio? • ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto? • ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados? • ¿Los cambios afectarán las operaciones actuales del negocio? [COBIT, 2005].

AMBIENTE DE CONTROL: El ambiente de control sirve de base para todos los otros componentes de la gestión de riesgos, proporcionando la disciplina y la estructura. Influye en la estrategia y en los objetivos establecidos, estructurando las actividades del negocio, identificando, evaluando e interpretando los riesgos. Es decir, que el ambiente de control incide sobre el funcionamiento de las actividades de control, la información, los sistemas de comunicación y las actividades de supervisión. [Santillana, 2003]

AMENAZA: Evento o circunstancia capaz de causar daño, existen tres fuentes comunes para las amenazas, y pueden ser clasificadas como naturales, humanas o ambientales.

-B-

BRECHAS DE OPERACIÓN: Son aquellos lugares o situaciones en donde las operaciones reales fallan en dar los resultados esperados.

-C-

COBIT: (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Foundation. COBIT (1996) es una estructura que provee una herramienta para los propietarios de los procesos del negocio para descargar eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos. [Fernández, 2003].

CONTROL: Cualquier medida que tome la dirección, el consejo y otros, para mejorar la gestión de riesgo y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección, planifica, organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas. [Santillana, 2003]

CONTROL FINANCIERO Y CONTABLE: Son los medios que comprenden el plan de organización y todos los métodos y procedimientos cuya misión es la salvaguarda de los bienes activos y la fiabilidad de los registros contables. [Reyes, 1992]

CONTROL INTERNO: Un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos. [Santillana, 2003]

-D-

DOCUMENTACIÓN DE PROCESOS: Un método estructurado que utiliza un preciso manual para comprender el contexto y los detalles de los procesos clave. Siempre que un proceso vaya a ser rediseñado o mejorado, su documentación es esencial como punto de partida. Lo habitual en las organizaciones es que los procesos no estén identificados y por consiguiente, no se documenten ni se delimiten.

-E-

EFECTIVIDAD: La efectividad es la capacidad de lograr un efecto deseado o esperado. [Reyes, 1992]

EFICACIA: Medida normativa para alcanzar resultados; la eficacia de una organización se refiere a su capacidad de satisfacer una necesidad social mediante el suministro de productos, bienes o servicios. Su preocupación es hacer correctamente las cosas y de la mejor manera posible; el logro de objetivos mediante los recursos disponibles. [Reyes, 1992]

EFICIENCIA: Medida normativa para la utilización de recursos en un proceso; es una relación técnica entre las entradas y salidas, esta enfocada hacia la búsqueda de la mejor manera de cómo las cosas deben hacerse o ejecutarse, con el fin de que los recursos se utilicen con el modo más racional posible. Su preocupación son lo medios, métodos y procedimientos más adecuados para un óptimo empleo de los recursos. [Reyes, 1992]

EMPRESA PYME: La categoría de microempresas, pequeñas y medianas empresas (PYME) esta constituida por empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede 50 millones de euros o cuyo balance general no excede 43 millones de euros. [Comisión Europea, 2006].

ENTREGAR Y DAR SOPORTE (DS): Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia: •¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio? •¿Están optimizados los costos de TI?•¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura? •¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad? [COBIT, 2005].

ESTRUCTURA Y ORGANIZACIÓN FORMAL: Entiéndase como estructura y organización formal a aquellas empresas que cuentan con una distribución planeada que establece un patrón de las relaciones de los elementos (organigrama), y por consecuencia funciones y procesos definidos.

EVALUACIÓN DE RIESGOS: La evaluación de riesgos permite a la organización considerar los potenciales acontecimientos que pudieran afectar el logro de los objetivos. La probabilidad representa la posibilidad que un acontecimiento ocurra, mientras que el impacto representa su efecto. La metodología de evaluación de riesgos de una organización normalmente comprende una combinación de técnicas cualitativas y cuantitativas. [Microsoft, 2004]

EVIDENCIA: presentación de elementos (documentos, fotografías, correos electrónicos, etc.) que se agrega y usa para probar que el proceso y la actividad de control se están llevando a cabo adecuadamente.

-G-

GARANTÍA RAZONABLE: El control interno, independientemente de su buen diseño y operación, sólo puede proporcionar a la gerencia y directorio una garantía razonable, en relación al logro de los objetivos de una entidad. La probabilidad de éxito se afecta por limitaciones inherentes a todo sistema de control interno.

Estas limitaciones pueden incluir una errada toma de decisiones con respecto al establecimiento o diseño de controles, la necesidad de considerar tanto costos como beneficios, desautorización por parte de la gerencia, el fracaso de los controles mediante la colusión o simples errores y confusiones. Además, los controles se

pueden eludir mediante la colusión de dos o más personas. Finalmente, la gerencia tiene la capacidad de ignorar el sistema de control interno. [Fernández, 2003].

GESTIÓN DE RIESGO: Un proceso para identificar, evaluar, manejar y controlar acontecimientos o situaciones potenciales, con el fin de proporcionar un aseguramiento razonable respecto del alcance de los objetivos de la organización.

-I-

INFORMACIÓN Y COMUNICACIÓN: La información, tanto interna como externa, debe ser identificada, captada y comunicada en tiempo y forma para poder así evaluar los riesgos y establecer la respuesta a los mismos. Dado que la información se origina en diversas fuentes (internas, externas) y tiene diferentes características (cualitativa, cuantitativa), se genera un gran desafío que es el de contar con un gran volumen de información, del que deberá ser captada la información relevante, procesada y trasmitida de tal modo que llegue oportunamente a todos los sectores, permitiendo asumir las responsabilidades individuales. [Santillana, 2003]

-M-

MADUREZ: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.[COBIT, 2005]

MAPEO DE PROCESOS: Una aproximación que define la organización como un sistema de procesos interrelacionados. El mapa de procesos impulsa a la organización a poseer una visión más allá de sus límites geográficos y funcionales, mostrando cómo sus actividades están relacionadas con los clientes externos, proveedores y grupos de interés. Tales “mapas” dan la oportunidad de mejorar la coordinación entre los elementos clave de la organización. Así mismo dan la oportunidad de distinguir entre procesos clave, constituyendo el primer paso para seleccionar los procesos sobre los que actuar.

MARCO DE CONTROL: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

MEDIANA EMPRESA: Se considera microempresa aquella empresa que cuenta con un plantilla menor a 250 empleados, tiene un volumen de negocios menor o igual a 50 millones de euros y un balance menor o igual a 43 millones de euros. [Comisión Europea, 2006].

METODOLOGÍA: del griego (metà "más allà" odòs "camino" logos "estudio"). Se refiere a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia. Aun cuando el término puede ser aplicado a las artes cuando es necesario efectuar una observación o análisis más riguroso o explicar una forma de interpretar la obra de arte. En resumen son el conjunto de métodos que se rigen en una investigación científica o en una exposición doctrinal. Método es el procedimiento para alcanzar los objetivos y la metodología es el estudio del método. [Web 1, 2009]

METODOLOGÍA SUAVE: Los sistemas "flexibles" están dotados con características conductuales, son vivientes y sufren un cambio cuando se enfrentan a su medio. Los sistemas "flexibles" típicamente serían del dominio de las ciencias de la vida y las ciencias conductual y social. En vez de basarnos exclusivamente en el análisis y la deducción, necesitamos sintetizar y ser inductivos. En vez de basarnos estrictamente en métodos formales de pensamiento, debemos tomar en cuenta lo siguiente:

1. Los procesos de razonamiento informales, como el juicio y la intuición.
2. El peso de los datos comprobados, derivados de unas cuantas observaciones y muy poca oportunidad de réplica.
3. Las predicciones basadas en datos comprobados endebles, más que en explicaciones.
4. Mayor discontinuidad de dominio y la importancia del evento único.

Metodología basada en sistemas para enfrentar problemas del mundo real en los cuales los fines que se sabe son deseables no se pueden tomar como dados. [Van Gigch, 2008]

***MÉTRICA*:** Un estándar para medir el desempeño contra la meta. [COBIT, 2005]

MICROEMPRESA: Se considera microempresa aquella empresa que cuenta con un plantilla menor a 10 empleados y tiene un volumen de negocios o balance menor o igual a 2 millones de euros. [Comisión Europea, 2006].

MONITOREAR Y EVALUAR (ME): Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia: •¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde? •¿La Gerencia garantiza que los controles internos son efectivos y eficientes? •¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio? •¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño? [COBIT, 2005].

-O-

OBJETIVOS: Declaraciones generales establecidas por los auditores que definen los logros pretendidos del trabajo. [COBIT, 2005].

OUTSOURCING / SUBCONTRATACIÓN: La subcontratación es el proceso económico en el cual una empresa determinada mueve o destina los recursos orientados a cumplir ciertas tareas, a una empresa externa, por medio de un contrato.

-P-

PLANEAR Y ORGANIZAR (PO): Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas.

Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia: • ¿Están alineadas las estrategias de TI y del negocio? • ¿La empresa está alcanzando un uso óptimo de sus recursos? • ¿Entienden todas las personas dentro de la organización los objetivos de TI? • ¿Se entienden y administran los riesgos de TI? • ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio? [COBIT, 2005].

PEQUEÑA EMPRESA: Se considera microempresa aquella empresa que cuenta con un plantilla menor a 50 empleados y tiene un volumen de negocios o balance menor o igual a 10 millones de euros. [Comisión Europea, 2006].

-R-

RENDIR CUENTAS: Significa "la responsabilidad termina aquí", esta es la persona que provee la autorización y direccionamiento a una actividad. [COBIT, 2005]

RIESGO: Es la probabilidad de que un acontecimiento pueda afectar el alcance de los objetivos. El riesgo se mide en términos de impacto y probabilidad de ocurrencia. [COBIT, 2005].

-S-

SEGURIDAD: Situación del que está al amparo de algún riesgo o peligro. De seguridad se dice de lo que no ofrece riesgo. [Gran Diccionario Enciclopédico Ilustrado 1982].

SEGURIDAD EN LA INFORMACIÓN*:* Relativo a la seguridad informática, consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. [Web 2, 2008].

-T-

TECNOLOGÍAS DE INFORMACIÓN: Corresponde con metodologías, sistemas complejos, técnicas y herramientas; de: software, hardware, telecomunicaciones, bases de datos y servicios de apoyo; que se agrupan e interactúan para proporcionar soluciones integrales o completas en diversos ámbitos de la administración, finanzas, producción y automatización; en los diferentes niveles de funcionamiento de la organización. [Galindo, 2007].

-V-

Vulnerabilidades: Debilidades que la empresa podría tener.

INTRODUCCIÓN Y PRESENTACIÓN AL PROYECTO DE TESIS.

0.1 PRESENTACIÓN DEL PROYECTO DE TESIS.

La seguridad es un concepto que todos podemos entender como una necesidad básica, pero que no cuenta con una definición formal, teniendo significados diferentes a diferentes personas en diferentes contextos. Para la mejor comprensión de este texto, se entenderá el concepto de seguridad como: “la situación del que está al amparo de algún riesgo o peligro” [Gran Diccionario Enciclopédico Ilustrado, 1982].

La influencia de este concepto ha alcanzado actualmente, tales dimensiones en los diversificados aspectos de la vida cotidiana; que van desde sistemas de alarma computarizados y centralizados, sistemas de detección y comunicación de siniestros, medidas de seguridad el manejo de alimentos, aditamentos de seguridad en vestimentas de trabajo, hasta la seguridad de la información entre muchos otros.

Este último, la seguridad de información, ha tomando un auge especialmente, ya que la sociedad se encuentra envueltas en una era donde la información y el conocimiento cuentan con un valor incalculable. Sin embargo, la ausencia de conocimiento en este tópico es evidente, ya que muchas empresas y personas, han sufrido daños irreparables, que se han convertido en grandes pérdidas económicas.

Por lo tanto, el siguiente trabajo tiene como objetivo la propuesta de una metodología que proporcione mejorar la situación de escaso conocimiento mediante la aplicación de controles ó actividades de control y sus objetivos que permitan un ambiente de seguridad en el área de Tecnologías de Información (TI), para todas aquellas empresas que quieran adquirir una confianza razonable en su información.

0.2 MARCO METODOLÓGICO PARA EL DESARROLLO DE LA TESIS.

Ahora, se muestra el marco sistémico y metodológico, en el se describen una serie de actividades a emplear, sus correspondientes técnicas, herramientas y productos a obtener para realizar el desarrollo del proyecto de tesis:

Tabla 0.1 Marco metodológico integral para el desarrollo del proyecto de tesis.

MARCO METODOLÓGICO			
ACTIVIDADES (¿Qué Hacer?)	**TÉCNICAS (¿Cómo hacerlo?)**	**HERRAMIENTA (¿Con qué hacerlo?)**	**METAS (¿Qué Obtener?)**
1. Definir el tema.	-Observación -Investigación	-Método científico	Especificar la oportunidad ó problemática que se puede considerar como tema de estudio.
2. Recopilar información del tema.	-Investigación. -Recopilación bibliográfica.	-Libros -Revistas -Periódicos -Internet.	Identificar y aislar la problemática ó oportunidad para obtener una visión sistémica del tema de estudio.
3. Desarrollar el marco Metodológico.	-Definición del marco metodológico mediante una tabla.	-Procesador de palabras.	Definir las actividades que se tienen que hacer para realizar el proyecto de tesis.
4. Definir el marco Conceptual.	-Observación -Investigación. -Recopilación bibliográfica. -Definición del marco Conceptual	-Libros del tema -Diccionarios -Enciclopedias -Pirámide Conceptual. -Procesador de palabras.	Delimitar los conceptos y describir los términos generales empleados en el proyecto de tesis.
5. Identificar y analizar la situación actual. 5.1 Definir la justificación. 5.2 Definir Objetivo general y específicos.	-Definir una visión global del tema en cuestión a tratar. -Conocer conceptos básicos para la definición de Objetivos. - Elaborar tabla de ventajas y desventajas.	-Libros, -Revistas -Internet. -Procesador de palabras.	Obtener un análisis de las ventajas y desventajas de la metodología propuesta y modelos existentes en el mercado. A partir del análisis, hacer una justificación lógica que defienda el estudio del proyecto en cuestión. Definir los alcances o resultados a obtener.
6. Desarrollar la metodología.	-Investigación. -Analizar, Identificar y definir la metodología de desarrollo.	-Libros -Revistas -Internet -Periódicos	Obtener un conjunto de actividades que conformen la metodología a desarrollar.
7. Construcción de un modelo.	-Definir las partes que conformaran el modelo a seguir.	-Procesador de palabras.	Concebir un modelo a seguir con el conjunto de actividades definidas anteriormente.
8. Implementar en forma real el modelo.	-Aplicar modelo en una empresa.	-Hoja de cálculo	Adquirir una aplicación en el mundo real, del uso del modelo.
9. Redactar el documento de tesis.	-Conocer la metodología para el desarrollo y redacción de un proyecto de tesis de maestría	-Procesador de textos -Editor de imágenes -Hoja de cálculo	Obtener un documento escrito del proyecto de tesis.
10. Presentar el examen de grado.	-Investigar los lineamientos institucionales de SEPI-ESIME para presentar el examen de grado.	-Internet -Entrevista	Conseguir el grado de Maestro en ciencias en ingeniería de sistemas.

0.3 PRESENTACIÓN DEL DOCUMENTO DEL PROYECTO DE TESIS.

A continuación, se presenta el siguiente esquema que muestra la estructura general del documento de tesis; en esta imagen se plantea el medio ambiente general para proponer una mejora en el área de Tecnologías de Información (TI) de una empresa de comunicaciones móviles y de rastreo:

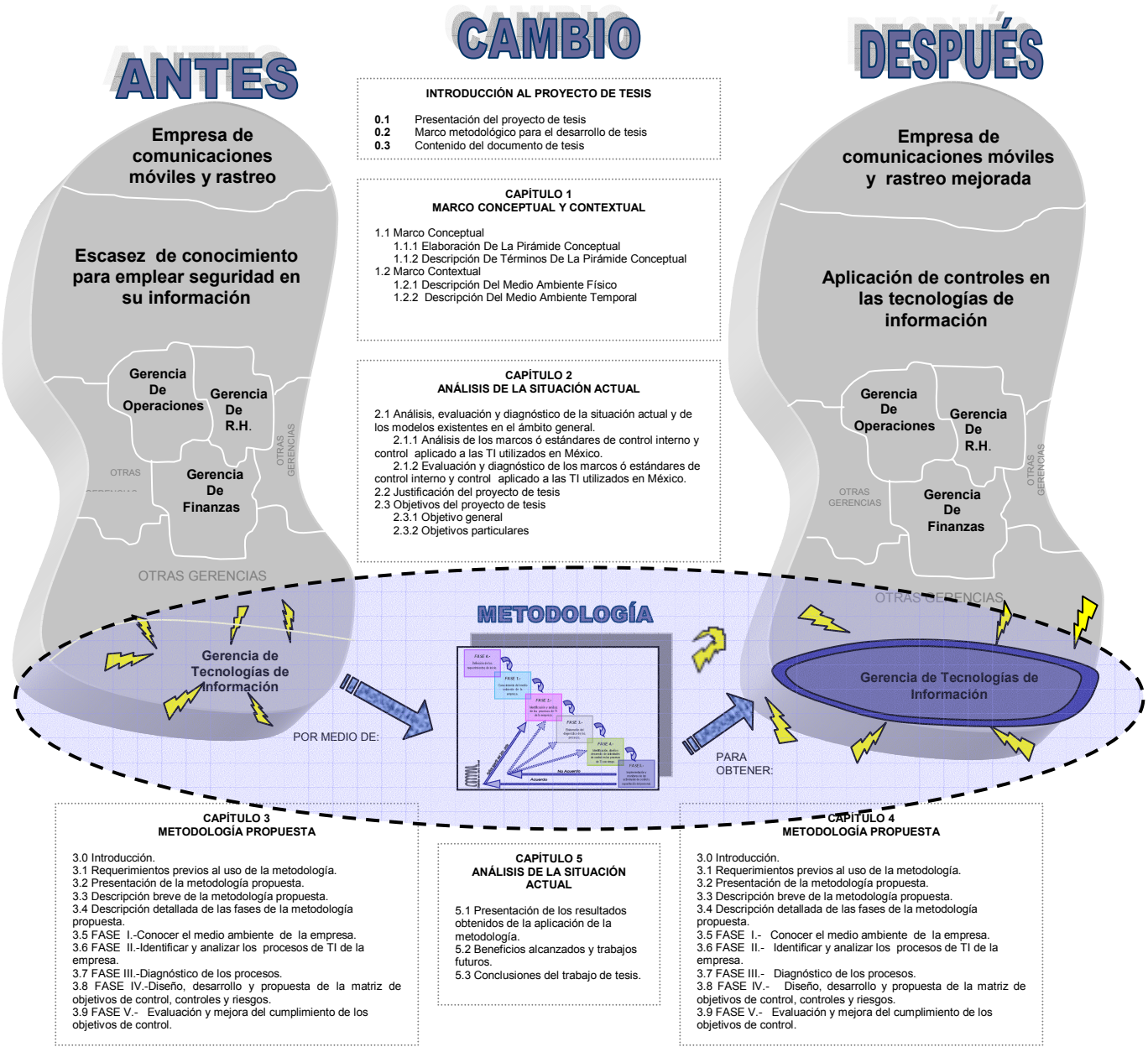


Figura 0.1 Estructura del documento del proyecto de tesis.

CAPÍTULO 1.- MARCO CONCEPTUAL Y CONTEXTUAL.

1.0 INTRODUCCIÓN.

El siguiente capítulo, comprende el Marco Conceptual que consta de las definiciones necesarias y representadas sombreadamente en una pirámide conceptual, para el desarrollo de esta tesis, de igual manera contiene el Marco Contextual que describe la situación actual de la seguridad de la información y de la empresa en que se implantará la metodología al inicio de este proyecto.

1.1 MARCO CONCEPTUAL.

1.1.1 ELABORACIÓN DE LA PIRÁMIDE CONCEPTUAL.

La siguiente representación gráfica llamada “Pirámide Conceptual” [Galindo, 2002] tiene por objeto mostrar los elementos conceptuales involucrados en el proyecto de tesis y en sí, define el título del mismo y se presentan de los más generales en su base, a los más particulares en su cúspide y serán empleados durante el desarrollo de la tesis y el trabajo escrito:

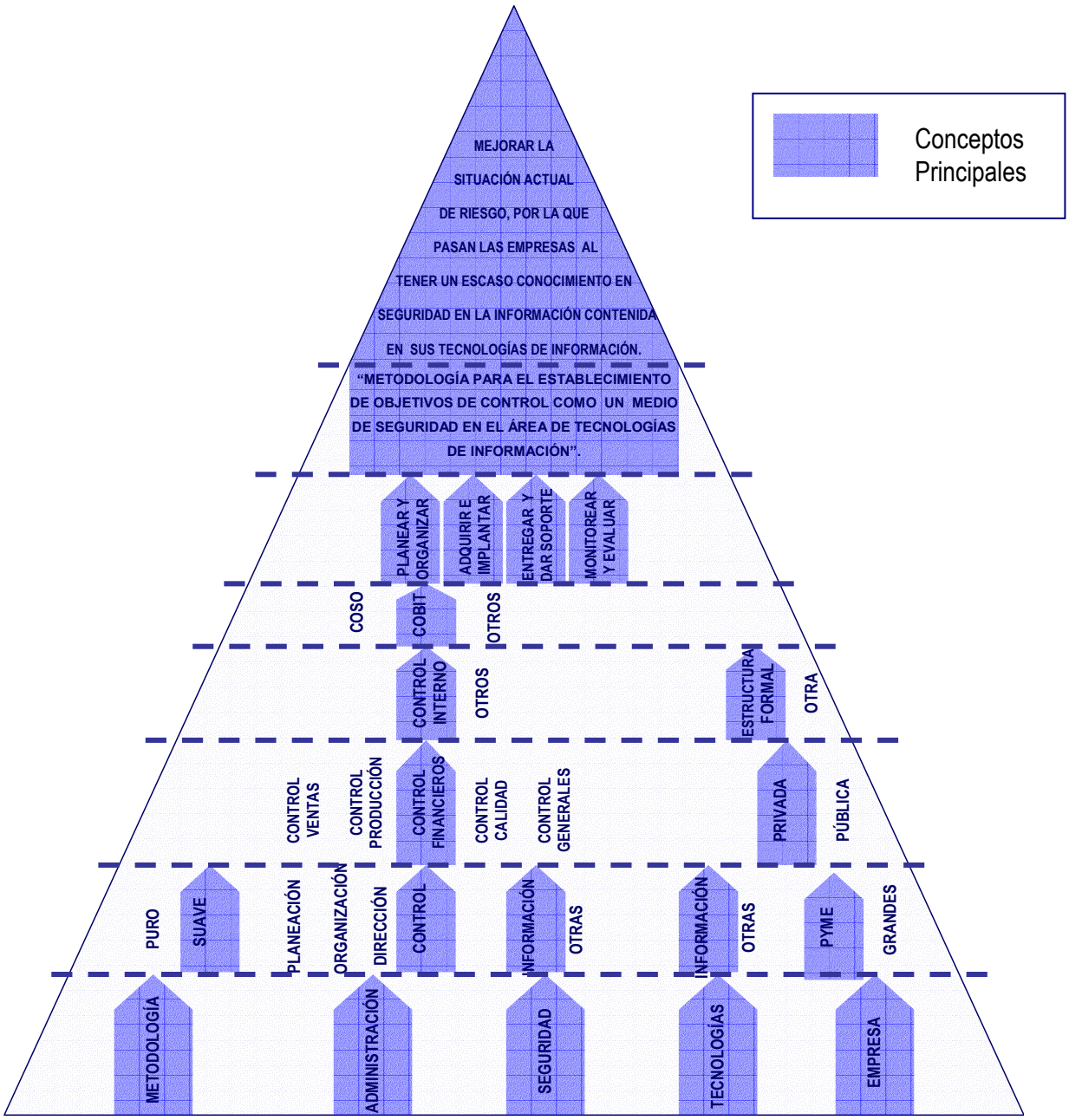


Figura 1.1 Pirámide conceptual de los elementos que interviene en el desarrollo del modelo y metodología.

A continuación, se describirán de manera detallada los conceptos de esta pirámide:

1.1.2 DESCRIPCIÓN DE LOS TÉRMINOS PRINCIPALES DE LA PIRÁMIDE CONCEPTUAL.

En seguida, se encuentra una breve descripción de los principales términos conceptuales que se utilizarán en este proyecto de tesis, basados en los presentados en la “Pirámide Conceptual:

METODOLOGÍA: del griego (metà "más allà" odòs "camino" logos "estudio"). Se refiere a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia. Aun cuando el término puede ser aplicado a las artes cuando es necesario efectuar una observación o análisis más riguroso o explicar una forma de interpretar la obra de arte.

En resumen son el conjunto de métodos que se rigen en una investigación científica o en una exposición doctrinal. Método es el procedimiento para alcanzar los objetivos y la metodología es el estudio del método. [Web 1, 2009]

METODOLOGÍA SUAVE: Los sistemas “flexibles” están dotados con características conductuales, son vivientes y sufren un cambio cuando se enfrentan a su medio. Los sistemas “flexibles” típicamente serían del dominio de las ciencias de la vida y las ciencias conductual y social. En vez de basarnos exclusivamente en el análisis y la deducción, necesitamos sintetizar y ser inductivos. En vez de basarnos estrictamente en métodos formales de pensamiento, debemos tomar en cuenta lo siguiente:

5. Los procesos de razonamiento informales, como el juicio y la intuición.
6. El peso de los datos comprobados, derivados de unas cuantas observaciones y muy poca oportunidad de réplica.
7. Las predicciones basadas en datos comprobados endebles, más que en explicaciones.
8. Mayor discontinuidad de dominio y la importancia del evento único.

Metodología basada en sistemas para enfrentar problemas del mundo real en los cuales los fines que se sabe son deseables no se pueden tomar como dados. La metodología de sistemas suaves se basa en una postura fenomenológica. [Van Gigch, 2008].

ADMINISTRACIÓN: La palabra "Administración" se forma del prefijo *"ad"*, que significa hacia, y de *"ministratio"*, que viene a su vez de *"minister"*, vocablo compuesto de *"minus"*, comparativo de inferioridad, y del sufijo *" ter"*, que sirve como término de comparación. [Reyes, 1992]. Conjunto de técnicas sistemáticas que permite que las organizaciones sociales logren sus fines. Acción de planear, controlar y dirigir los recursos de una organización con el fin de lograr los objetivos deseados. [Hernández, Ballesteros, 1990].

CONTROL: Las políticas, procedimientos, practicas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados. [COBIT, 2005].

CONTROL FINANCIERO Y CONTABLE: Son los medios que comprenden el plan de organización y todos los métodos y procedimientos cuya misión es la salvaguarda de los bienes activos y la fiabilidad de los registros contables. [Reyes, 1992]

CONTROL INTERNO: Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una garantía razonable de que los objetivos de negocio se alcanzarán y de que los eventos indeseables serán prevenidos o detectados [COBIT, 2005].

COBIT: (Control Objectives for Information and related Technology) de la Information Systems Audit and Control Foundation. COBIT (1996) es una estructura que provee una herramienta para los propietarios de los procesos del negocio para descargar eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos. [Fernández, 2003].

PLANEAR Y ORGANIZAR (PO): Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada. Este dominio cubre los siguientes cuestionamientos típicos de la gerencia: • ¿Están alineadas las estrategias de TI y del negocio? • ¿La empresa está alcanzando un uso óptimo de sus recursos? • ¿Entienden todas las personas dentro de la organización los objetivos de TI? • ¿Se entienden y administran los riesgos de TI? • ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio? [COBIT, 2005].

ADQUIRIR E IMPLEMENTAR (AI): Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia: • ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio? • ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto? • ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados? • ¿Los cambios afectarán las operaciones actuales del negocio? [COBIT, 2005].

ENTREGAR Y DAR SOPORTE (DS): Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales. Por lo general aclara las siguientes preguntas de la gerencia: •¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio? •¿Están optimizados los costos de TI?•¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura? •¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad? [COBIT, 2005].

MONITOREAR Y EVALUAR (ME): Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno. Por lo general abarca las siguientes preguntas de la gerencia:

•¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde? •¿La Gerencia garantiza que los controles internos son efectivos y eficientes? •¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio? •¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño? [COBIT, 2005].

SEGURIDAD: Situación del que está al amparo de algún riesgo o peligro. De seguridad se dice de lo que no ofrece riesgo. [Gran Diccionario Enciclopédico Ilustrado 1982].

SEGURIDAD EN LA INFORMACIÓN*:* Relativo a la seguridad informática, consiste en asegurar que los recursos del sistema de información (material informático o programas) de una organización sean utilizados de la manera que se decidió y que el acceso a la información allí contenida así como su modificación sólo sea posible a las personas que se encuentren acreditadas y dentro de los límites de su autorización. [Web 2, 2008].

TECNOLOGÍAS DE INFORMACIÓN: Corresponde con metodologías, sistemas complejos, técnicas y herramientas; de: software, hardware, telecomunicaciones, bases de datos y servicios de apoyo; que se agrupan e interactúan para proporcionar soluciones integrales o completas en diversos ámbitos de la administración, finanzas, producción y automatización; en los diferentes niveles de funcionamiento de la organización. [Galindo, 2007].

EMPRESA: Es una entidad que ejerce una actividad económica, independientemente de su forma jurídica. Así, pueden considerarse empresas los trabajadores autónomos, las empresas familiares, las sociedades colectivas y las asociaciones que ejercen regularmente una actividad económica. [Comisión Europea, 2006].

EMPRESA PYME: La categoría de microempresas, pequeñas y medianas empresas (PYME) esta constituida por empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede 50 millones de euros o cuyo balance general no excede 43 millones de euros. [Comisión Europea, 2006].

MICROEMPRESA: Se considera microempresa aquella empresa que cuenta con un plantilla menor a 10 empleados y tiene un volumen de negocios o balance menor o igual a 2 millones de euros. [Comisión Europea, 2006].

PEQUEÑA EMPRESA: Se considera microempresa aquella empresa que cuenta con un plantilla menor a 50 empleados y tiene un volumen de negocios o balance menor o igual a 10 millones de euros. [Comisión Europea, 2006].

MEDIANA EMPRESA: Se considera microempresa aquella empresa que cuenta con un plantilla menor a 250 empleados, tiene un volumen de negocios menor o igual a 50 millones de euros y un balance menor o igual a 43 millones de euros. [Comisión Europea, 2006].

ESTRUCTURA FORMAL: Entiéndase como "estructura formal", aquellas empresas que cuentan con una descripción de cargos, funciones y procesos definidos.

1.2 MARCO CONTEXTUAL

La seguridad es un tema trascendental para las empresas que quieren ofrecer servicio o productos de calidad para el consumidor, ya que en ella se encuentra alojada la confianza y garantía que la compañía ofrece; pero la seguridad es un tema muy amplio y por lo tanto, es aplicable a distintos asuntos empresariales, que van desde la seguridad industrial hasta las seguridad en la información.

Esta último, la seguridad de la información, se ha vuelto uno de los tópicos más relevantes en la actualidad, ya que la información representa uno de los activos más valiosos de las empresas, y como ésta se encuentra alojada en los sistemas de información de las mismas, ha convirtiendo a las tecnologías de información en los soportes principales de las operaciones empresariales.

Pero este tema se ha deja un tanto a la suerte, ya que la mala implementación de normas, políticas y procedimientos que apoyan a las tecnologías de información; originadas por la ausencia de cultura preventiva y la falta de planes de seguridad, a ocasionado que auditores, jefes de seguridad y personal relacionado, busquen soluciones de seguridad que les permitan crear y/o fortalecer los sistemas de control a manera apoyar la toma de decisiones oportuna.

Estas soluciones de seguridad deben contar elementos que permitan controlar y evaluar los diferentes aspectos de la tecnológica de la información, principalmente lo relacionado con la seguridad, ya que se reconoce como factor crítico para el éxito y la supervivencia de las organizaciones, que su infraestructura en tecnologías de información sea administrada efectivamente. (Ver Anexo A, acerca de La importancia de la Seguridad en la Información para conocer más acerca del tema).

Debido a esto, se han desarrollado nuevas regulaciones como COBIT (Control Objectives for Information and related Technology) y la ley SOX (Ley Sarbanes-Oxley) que mediante su cumplimiento han reconocido aumento de procesamientos, disminución del riesgo, diseño y/o transformación de los controles e incremento del valor de la empresa. Estas mejoras podrían no sólo ayudar a que la institución se desempeñe de acuerdo a las mejores prácticas, sino también a reforzar fundamentalmente el propósito primario del ordenamiento regulatorio (la ley o equivalentes), el mejoramiento de la transparencia en la administración de la empresa y refuerzo para la confianza del inversionista y del mercado.

Con el fin de implementar buenos controles (que nos permitan una seguridad razonable) en tecnologías de información, es preciso contar con una metodología para su desarrollo, basada en las mejores prácticas en el tratamiento de control interno aplicado a las TI, como lo ofrece el Marco Referencial COBIT. Por la situación anteriormente mencionada, este proyecto de tesis, propone tal metodología que permita crear un medio ambiente de seguridad de la información alojada en las TI y como complemento de su explicación será aplicada en una empresa de comunicaciones que se prestó para la implantación de ésta en algunos de sus procesos.

Enseguida se hará la presentación de esta empresa:

1.2.1 Descripción del medio ambiente temporal.

La empresa objeto de estudio en la cual se aplicará el proyecto de tesis, es una organización del ramo de las comunicaciones localización de unidades móviles vía satélite. Para fines prácticos a lo largo del documento de tesis, se le denominará "La empresa".

A continuación, se empieza a detallar como parte de la descripción del medio ambiente:

"La empresa", surge en noviembre de 1988, como una alternativa de comunicación y localización de unidades móviles vía satélite.

Durante sus primeros años, se encarga de hacer las inversiones necesarias, para cumplir con sus expectativas de crecimiento, y es así, como en 1995 adquiere su propio Centro de Operaciones cuyo costo de inversión fue superior a 1.5 millones de dólares.

En esos momentos, "La empresa" contaba con el apoyo de otra empresa internacional en comunicaciones como su proveedor tecnológico. Sin embargo, por razones de estrategia financiera, en 1997 se consolida la alianza con esta institución para beneficiar entre otras cosas, con crecimiento empresarial, al contar con recursos frescos y soporte técnico de excelencia.

Actualmente, "La empresa" sigue aliada con este socio comercial mundial en comunicaciones móviles y rastreo y gracias a este respaldo, está en constante desarrollo, involucrando directamente a su capital humano; y destacando en el desarrollo de soluciones logísticas, diseñadas "a la medida" de los mercados.

A continuación, se muestra una imagen con los productos, a manera de ejemplo, que ofrece la empresa:

Figura 1.2 Productos ofrecidos por "La empresa".

1.2.2 Descripción del medio ambiente organizacional.

“La empresa” es parte de una de las 3 sub empresas que conforman al socio líder en comunicaciones en México y se compone de la siguiente manera:

Figura 1.3 Organigrama general de “La empresa”.

Luego entonces, “La empresa” cuenta con elementos correspondientes que integran las tecnologías de información y los cuales, tienen que ser revisados y soportados por el área de TI; en este caso en particular, el departamento de Sistemas Administrativos, por lo tanto, la aplicación de esta metodología se llevará a cabo en aquello que tenga que ver directamente con los sistemas y las tecnologías de información y será supervisado por el área ya mencionada.

En el capítulo siguiente, se analizarán, evaluarán y diagnosticarán la situación actual de algunos estándares y marcos referenciales existentes, definiendo los que son utilizados en México, con la finalidad de observar cuales ellos son los que pueden servir de apoyo para el propósito del desarrollo de la metodología aquí propuesta.

CAPÍTULO 2.- ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA SEGURIDAD DE LAS TI.

2.0 INTRODUCCIÓN.

Una vez que se han definido los conceptos y el contexto en que se desenvuelve la problemática, es preciso fundamentar y justificar mediante un análisis, cuáles son los marcos, modelos y estándares que permiten disminuir el escenario de escasez de conocimiento en seguridad de la información, identificando y determinando los que cuentan con una metodología para su aplicación y los que son utilizados en México; con el fin de delimitar y señalar los más aptos para la resolución de este condición.

Ya que el fin principal de esta tesis es: ***proponer una solución que reduzca la situación de baja seguridad por la que pasan las tecnologías de información y la información contenida en éstos***; y dado que las TI se encuentran inmersas en todos los aspectos de la empresa, es conveniente comprender los beneficios y daños por los que podría transitar la empresa en el uso adecuado e inadecuado de estas tecnologías; por ello y a continuación se agregado un cuadro comparativo con estos argumentos que permita aclarar y reconocer la importancia del buen tratamiento de la información en las TI y su suceso contrario.

Tabla 2.1 Cuadro comparativo de los beneficios y daños del uso de las Tecnologías de Información. [Fuente propia]

Beneficios y daños del USO de las Tecnologías de Información	
Eficaz y adecuado:	**Ineficaz e incorrecto:**
• Facilita la información exacta oportuna y relevante acerca de la empresa a todos los niveles, desde el personal operativo hasta la dirección administrativa. • Permite el procesamiento sin obstáculos de cada aspecto de los procesos del negocio, de ese modo mejora la productividad y eficacia de todo el personal operativo. • Va más allá del proceso transaccional y de la administración de la información para generar ventajas competitivas para la empresa de varias maneras. • Evitar gastos innecesarios en TI.	• Puede causar un daño significativo a los negocios por perdida de ventaja competitiva. • Ineficiencia que termina en un servicio pobre a los clientes. • Incremento de costos. • Aumento en los ciclos de procesos. • Tiempos muertos.

Ahora, que se ha informado de las ventajas y desventajas que se producen del uso de las TI, a continuación se presentará ***un análisis, evaluación y diagnóstico de estándares, marcos y modelos*** que proponen medidas importantes y mejores prácticas al permitir dar un buen uso a las TI y salvaguardar la información contenida en éstas; afinando como resultado, un medio ambiente de seguridad correcto.

2.1 ANÁLISIS, EVALUACIÓN Y DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DE LOS MARCOS EXISTENTES EN EL ÁMBITO GENERAL.

Entonces, en base a lo comentado son anterioridad, en el siguiente esquema, se muestran modelos, marcos y estándares utilizados para el control interno y control interno aplicados a las TI; para así delimitar el tema. Por lo tanto, se encuentran sombreados aquellos más cercanos y utilizados en México:

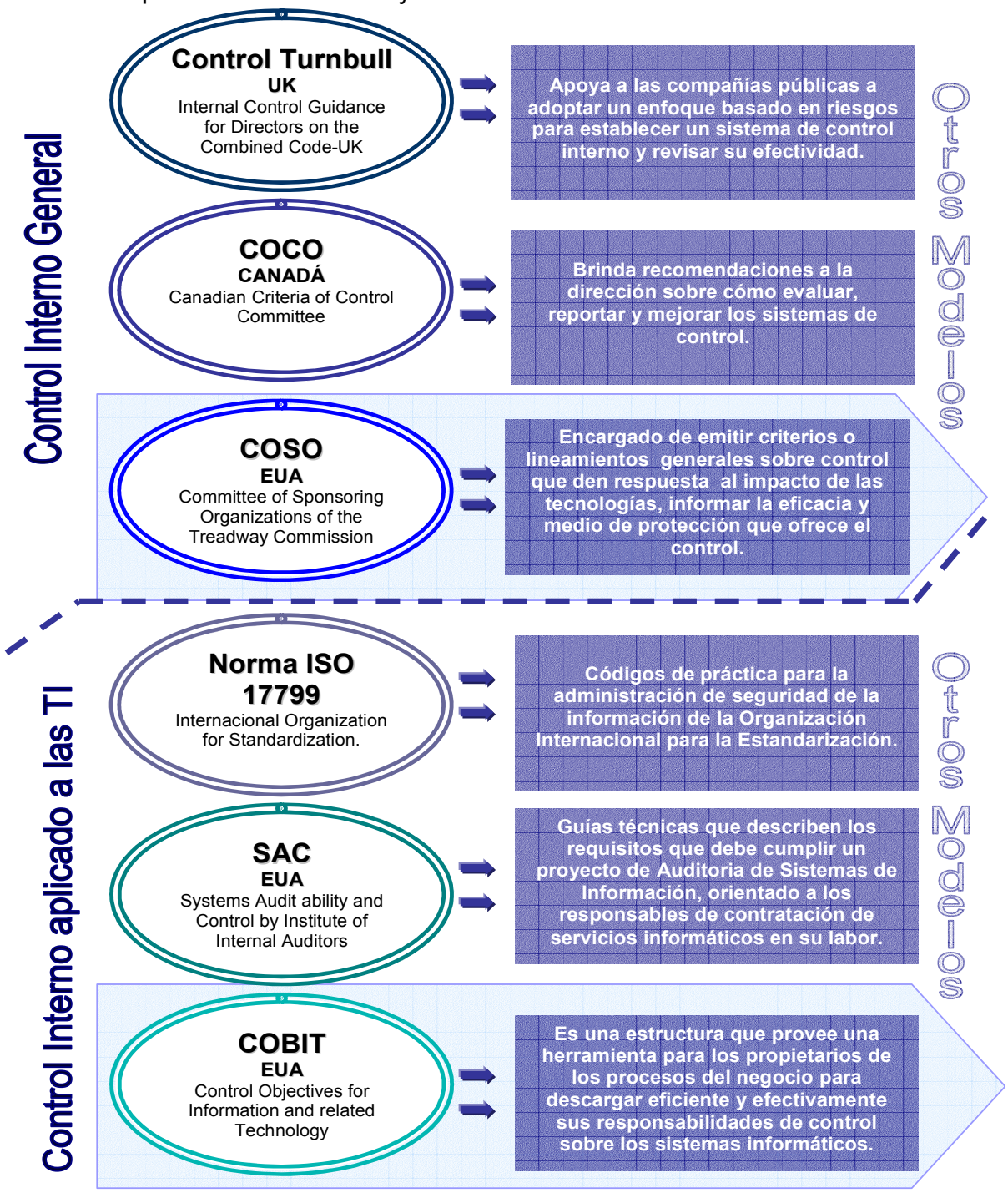


Figura 2.1 Marcos, Modelos y Estándares del Control Interno y Control Interno aplicado a las Tecnologías de Información.

2.1.1 ANÁLISIS DE LOS MARCOS DE CONTROL INTERNO Y CONTROL INTERNO APLICADO A LAS TI MÁS UTILIZADOS EN MÉXICO.

Definidos los estándares ó marcos que contienen las mejores prácticas más comúnmente utilizados en México; ahora, como una breve síntesis se presenta el siguiente cuadro comparativo, que muestra el modelo **COSO** (usado para el Control Interno, en general) y el marco **COBIT** (utilizado para el Control Interno en las TI); se ha adicionado en a éste cuadro, el conjunto de medidas para las tecnologías **SAC** como referencia; debido a que el marco COBIT surge de la suma del COSO y el SAC, lo que permite considerarlo como un marco referencial más completo e integral.

Tabla 2.2 Análisis comparativo de los marcos y estándares de referencia de control usados en México (Inicio) [Fuente Propia].

ANÁLISIS COMPARATIVO DE LOS MARCOS DE CONTROL INTERNO Y CONTROL INTERNO APLICADO A LAS TI CON RELEVANCIA EN MÉXICO.			
MARCO DE CONTROL INTERNO	***CONTROL INTERNO.***	***TECNOLOGIAS DE INFORMACIÓN***	***CONTROL INTERNO APLICADO A LAS TECNOLOGÍAS DE INFORMACIÓN.***
	COSO (Committee of Sponsoring Organizations of the Treadway Commission).	**SAC (Systems Auditability and Control).**	**COBIT (Control Objectives for Information and related Technology).**
DESCRIPCIÓN:	COSO - Internal Control - Integrated Framework del Committee of Sponsoring Organizations of the Treadway Commission. Publicado en EUA en 1992 en respuesta a las inquietudes que planteaba la diversidad de conceptos y definiciones e interpretaciones existentes entorno al control interno.	SAC (Systems Auditability and Control) del Institute of Internal Auditors Research Foundation. SAC (1991, revisado en 1994) ofrece asistencia a los auditores internos sobre el control y auditoria de los sistemas y tecnología informática.	COBIT (Control Objectives for Information and related Technology) of Information Systems Audit and Control Foundation. COBIT (1996) es una estructura que provee una herramienta para los propietarios de los procesos del negocio para descargar eficiente y efectivamente sus responsabilidades de control sobre los sistemas informáticos.
DIRIGIDO A:	Auditores Internos.	Dirección, usuarios,auditores de Sistemas de Información.	Auditores Internos.
SE REFIERE AL CONTROL INTERNO COMO:	Procesos.	Conjunto de procesos, subsistemas y personas.	Conjunto de procesos incluyendo políticas, procedimientos, prácticas estructuras organizacionales.

Tabla 2.2 Análisis comparativo de los marcos de referencia de control usados en México (Final) [Fuente Propia].

ANÁLISIS COMPARATIVO DE LOS MARCOS DE CONTROL INTERNO Y CONTROL INTERNO APLICADO A LAS TI CON RELEVANCIA EN MÉXICO.			
MARCO DE CONTROL INTERNO	***CONTROL INTERNO.***	***TECNOLOGIAS DE INFORMACIÓN.***	***CONTROL INTERNO APLICADO A LAS TECNOLOGÍAS DE INFORMACIÓN.***
	COSO (Committee of Sponsoring Organizations of the Treadway Commission).	**SAC (Systems Auditability and Control).**	**COBIT (Control Objectives for Information and related Technology).**
OBJETIVOS Ó PROPÓSITOS:	*Operaciones Efectivas y eficientes. *Informes financieros confiables. *Cumplimiento de las leyes y regulaciones.	*Operaciones Efectivas y eficiente. *Informes financieros contables. *Cumplimiento de las leyes y regulaciones.	***Operaciones efectivas y eficientes. *Confidencialidad, Integridad y disponibilidad de información. *Cumplimiento de las leyes y regulaciones.**
ESTRUCTURA:	Componentes: -Supervisión -Ambiente de Control -Administración de Riesgos -Actividades de Control -Información y Comunicación	Componentes: -Ambiente de Control -Manual y Automatizado -Procedimientos de -Control de Sistemas	Dominios: -Planeamiento y organización -Adquisición e implementación -Entrega y soporte -Monitoreo y evaluación
ENFOCADO A:	Toda la Entidad.	Tecnología Informática.	Tecnología Informática.
EVALUACIÓN DE LA EFECTIVIDAD DEL CONTROL INTERNO:	En un momento dado.	Por un período de tiempo.	Por un período de tiempo.
RESPONSABLE POR EL CONTROL INTERNO:	Dirección.	Dirección.	Dirección.
TAMAÑO:	353 páginas en cuatro volúmenes.	1193 páginas en 12 módulos.	187 páginas en cuatro documentos.

2.1.2 EVALUACIÓN Y DIAGNÓSTICO DE LOS MARCOS Ó ESTÁNDARES DE CONTROL INTERNO Y CONTROL INTERNO APLICADO A LAS TI MÁS UTILIZADOS EN MÉXICO.

Como se observa en el análisis anterior, acerca de los marcos de referencia de control interno, tecnologías de información y su unificación, se muestran sus objetivos ó sistema ó modelo a conseguir; es decir, los productos a obtener (nótese en la parte rayada en el cuadro), ***pero no indican las actividades o procesos metodológicos para llegar a ellos.***

Por consecuencia, de lo anterior, se puede dar el siguiente diagnóstico:

Algunas de estas actividades que se podrán realizar y que no se proponen o contemplan en el modelo a conseguir son las siguientes:

- Identificar o adquirir el medio ambiente general y particular de TI, así como el conocimiento detallado de sus procesos como apoyo para el diseño de actividades y objetivos de control para TI.
- Detallar el desarrollar una estructura de controles para llevar un registro y evaluación de éstos.
- Explicar y aplicar de manera adecuada algunas de las técnicas particulares de apoyo para crear un ambiente de seguridad.

Por lo tanto, existe una necesidad de proponer una ***Metodología para el establecimiento de objetivos de control y sus actividades correspondientes,*** la cual será el producto principal del proyecto de tesis, y que permita lograr lo siguiente:

Figura 2.2 Representación del modelo a conseguir para crear un medio ambiente de seguridad en las Tecnologías de Información.

2.2 JUSTIFICACIÓN DEL PROYECTO DE TESIS.

Del anterior análisis, evaluación, diagnóstico y modelo a conseguir; entonces, en el proyecto de tesis, se propone una Metodología que permita obtener un Sistema o Medio Ambiente a través de la utilización de objetivos de control y sus actividades para crear un medio de seguridad de la información, que es operada por las Tecnologías de Información para la empresas o Instituciones.

Esto implica en particular, para un ambiente como el de México, que la metodología se pueda aplicar en empresas que cuente con una estructura formal (Entiéndase como estructura y organización formal a aquellas empresas que cuentan con una distribución planeada que establece un patrón de las relaciones de los elementos [organigrama], y por consecuencia funciones y procesos definidos), independientemente de su tamaño.

Ahora con estos antecedentes, se definen los siguientes objetivos:

2.3 OBJETIVOS DEL PROYECTO DE TESIS.

2.3.1 OBJETIVO GENERAL.

Proponer una metodología para obtener un sistema ó medio ambiente basado en objetivos de control y sus actividades correspondientes para crear un medio de seguridad de la información operada por las Tecnologías de Información para aquellas empresas que cuenten con una estructura y organización formal.

2.3.2 OBJETIVOS PARTICULARES.

- Identificar y conocer el medio ambiente general para determinar el marco contextual y conceptual de la situación en estudio.

- Analizar, evaluar y diagnosticar la situación actual con respecto a los marcos de referencia y control interno para obtener un sistema que cree un medio ambiente de seguridad de la información que es operada por las Tecnologías de Información.

- Proponer la metodología para el uso de objetivos de control y sus actividades como medio de seguridad de la información albergada en las tecnologías de información con la finalidad de reducir el escaso conocimiento en esta materia.

- Implementar la metodología en algunos procesos de “La empresa” y evaluar el desempeño de las actividades de control y sus objetivos ya aplicados.

En el siguiente capítulo, se presentará la metodología propuesta y se explicará cada una de las Fases.

CAPÍTULO 3.- METODOLOGÍA PROPUESTA.

3.0 INTRODUCCIÓN.

En el siguiente capítulo, se pretende describir en forma detallada la metodología propuesta, explicando cómo establecer los objetivos de control y sus actividades para introducirse en un medio ambiente de seguridad de la información en las TI.

Esta metodología se apoyará acorde al diagnóstico, términos y recomendaciones que hace el marco de referencia COBIT, ya que cuenta con los elementos necesarios para fortalecer los argumentos de esta tesis; a consecuencia de ello es recomendable tener presente este marco de referencia.

3.1 PRESENTACIÓN DE LA METODOLOGÍA PROPUESTA.

El siguiente esquema es la representación visual de las fases de la metodología propuesta y que posteriormente se describirán detalladamente.

Esta metodología está basada en una integración de las siguientes metodologías: “Una Metodología Básica para el Desarrollo de Sistemas” [Galindo, 2007], Metodología para crear la”Tabla Metodológica ó Tabla Solución Integral” como Apoyo al Desarrollo de Sistemas [Galindo, 2008], la “Metodología ORCA” [PWC, 2006]; y el uso de diversas técnicas particulares complementarias.

Esta combinación se realizó con el propósito de contar con una metodología sistémica que permitiera cumplir los requerimientos necesarios para asegurar la confidencialidad, integridad y disponibilidad de la información y las tecnologías de información que las contienen, mediante el uso de objetivos y el desarrollo e implementación de sus actividades de controles.

Y a continuación, se presenta en este esquema:

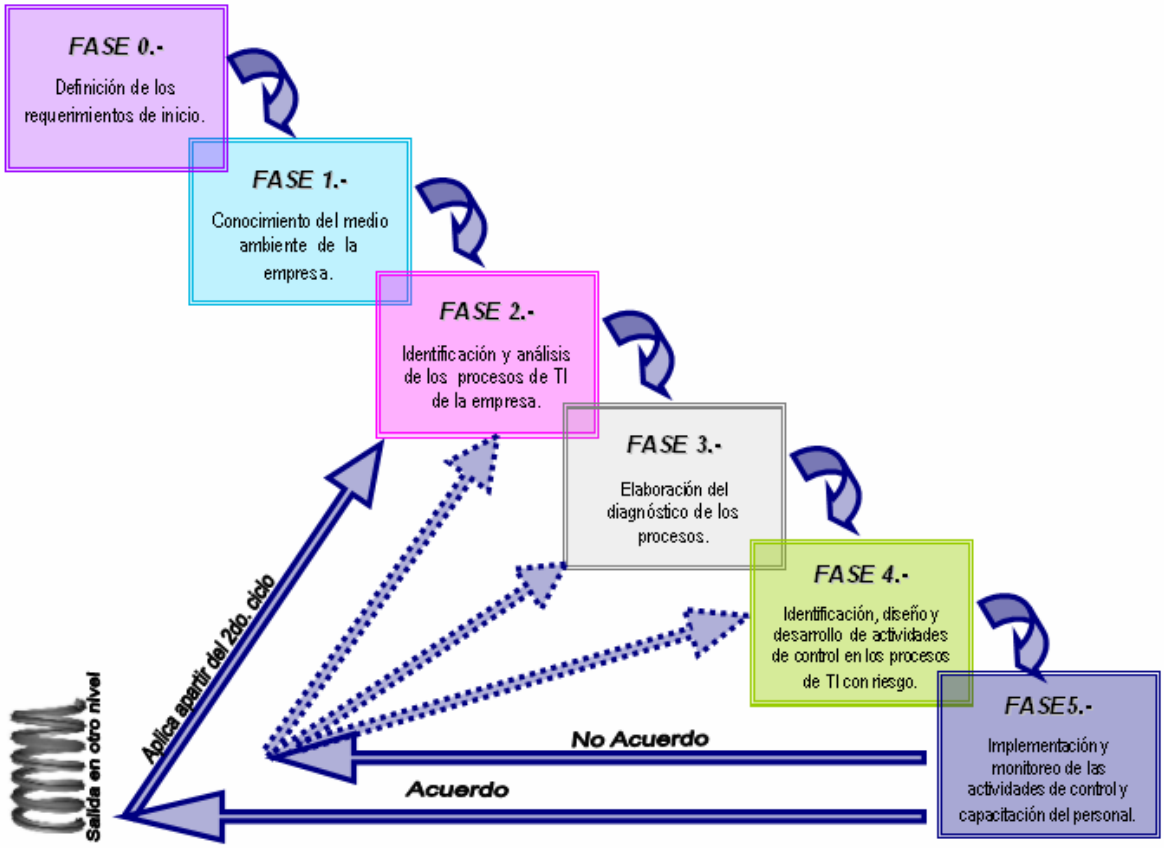


Figura 3.1 Metodología para el establecimiento de objetivos de control como medio de seguridad en el área de Tecnologías de Información.

En seguida, se expresa una explicación breve acerca de cada una de las fases que conforman la metodología propuesta.

3.2 DESCRIPCIÓN BREVE DE LA METODOLOGÍA PROPUESTA.

FASE 0.- DEFINICIÓN DE LOS REQUERIMIENTOS DE INICIO:

En esta primera fase es necesario contar con requisitos que hay que tomar en cuenta antes de iniciar con el uso de la metodología, como son el apoyo de la dirección y el personal adecuado.

FASE 1.- CONOCIMIENTO DEL MEDIO AMBIENTE DE LA EMPRESA:

En esta fase se conocerá la ubicación, visión, misión, políticas, etc., de la empresa; es decir, se conocerá el medio ambiente en general y particular de esta misma.

FASE 2.- IDENTIFICACIÓN Y ANÁLISIS DE LOS PROCESOS DE TI DE LA EMPRESA:

Una vez conocidos los datos generales de la empresa, se debe conocer y analizar los procesos del área en particular, con la finalidad de encontrar aquellos en los que se puede estar en riesgo.

FASE 3.- ELABORACIÓN DEL DIAGNÓSTICO DE LOS PROCESOS DE TI CON BRECHAS OPERACIONALES DE LA EMPRESA:

Al conocer los procesos, es necesario identificar los riesgos contenidos en éstos; estos riesgos se evalúan y analizan para darles prioridad de solución; de acuerdo a esta prioridad se elige la acción que se va a tomar con respecto a cada riesgo, en particular la acción de mitigar, la cuál, e la que permite disminuir el riesgo.

FASE 4.- IDENTIFICACIÓN, DISEÑO Y DESARROLLO DE ACTIVIDADES DE CONTROL EN LOS PROCESOS DE TI CON RIESGO:

Una vez seleccionado el tratamiento que se le va a dar a cada riesgo, la acción de mitigar permite implantar los objetivos de control y se diseñan sus actividades para el área tecnologías de información mediante el desarrollo de una propuesta de matriz.

FASE 5.- IMPLANTACIÓN Y MONITOREO DE LAS ACTIVIDADES DE CONTROL Y CAPACITACIÓN DEL PERSONAL:

En esta fase se dan a conocer las actividades de control, para que se pongan en operación y se presta la capacitación respectiva al personal para el cumplimiento y ejecución de éstas. Se puede implementar una evaluación de actividades de control (monitoreo) para verificar qué se estén ejerciendo y cumplan con sus objetivos; en caso contrario, se pueden mejorar los existentes ó implementar actividades de control complementarias.

Ahora, a continuación, se presenta otra forma de percibir la metodología:

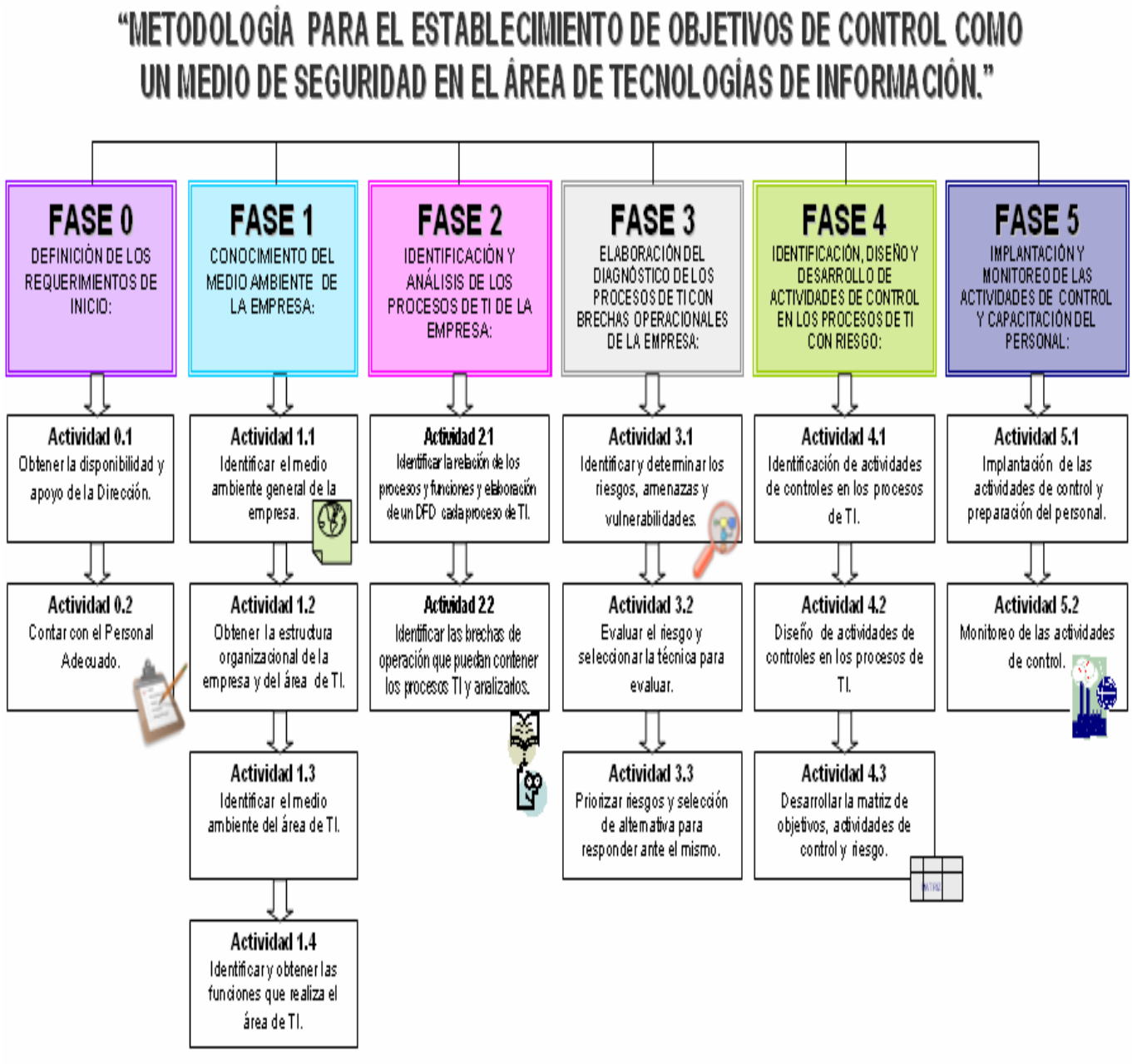


Figura 3.2 Descripción breve de la metodología propuesta.

3.3 DESCRIPCIÓN DETALLADA DE LAS FASES DE LA METODOLOGÍA PROPUESTA.

3.4 FASE 0.- DEFINICIÓN DE LOS REQUERIMIENTOS DE INICIO:

Es preciso mencionar que esta metodología fue creada con la intención de ayudar a aquellas empresas que deseen mejorar su situación actual de seguridad en el área de TI y que tengan una estructura formal como es contar con organigrama, descripción de cargos y funciones y documentación de procesos que permitan iniciar con el uso de objetivos e implantación de actividades de control, que es el propósito principal de este proyecto de tesis.

Cuándo las empresas deciden integrar iniciativas nuevas como lo es esta metodología, deben existir algunas recomendaciones o requerimientos previos con los que se debe contar para que se obtenga el resultado deseado.

Las cuales se presentan en la que se llamará “Fase 0” mostrada en esta imagen y cuyas actividades se describirán a continuación:

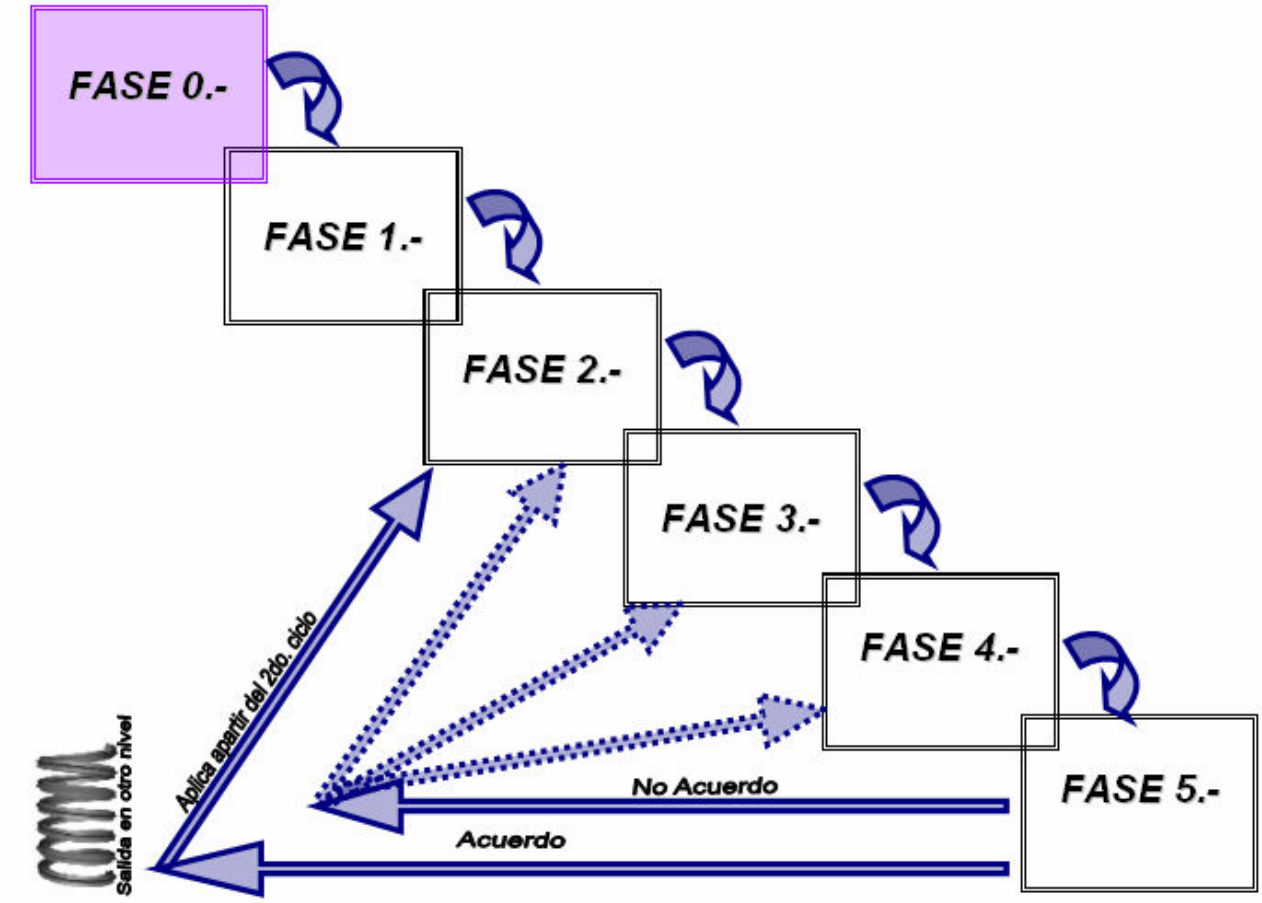


Figura 3.3 Representación de la metodología propuesta en la Fase 0.

3.4.1 Actividad 0.1 *Obtener la disponibilidad y apoyo de la Dirección.*

Para iniciar con la metodología, hay que contar con el respaldo y sustento de la Dirección, dado que es necesario su aceptación y soporte para todos los requisitos de la metodología.

La Dirección debe apoyar de forma precisa y consistente el proceso de insertar iniciativas nuevas a la empresa, es decir, dar su apoyo en lo necesario (incluyendo toda clase de recursos), para colaborar y participar desde la petición de los requerimientos hasta la aceptación y participación total de la implementación y usos de nuevas medidas de seguridad; para que el personal involucrado en estos cambios pueda entender el significado e incluirse en la oportunidad de realizar un trabajo más seguro a través del uso de objetivos y actividades de control.

Así mismo, sí este apoyo no es firme ni claro, es posible que los involucrados en este cambio no lo tomen enserio y no cumplan con las actividades necesarias para tener un medio ambiente de seguridad dejando la puerta abierta a que el riesgo se materialice y dejando el uso de este proyecto como un intento fallido, por eso, es indispensable el cumplimiento de este punto.

3.4.2 Actividad 0.2 *Contar con el Personal Adecuado.*

En muchas empresas, no se tiene un responsable de la seguridad de la información, por ello, es recomendable contar con por lo menos una persona que se dedique a esta función y el cual no dependa directamente del área de TI (dado que, quien evalúa no debe ser participe en la evaluación) y en seguida se presentan algunas condiciones para su mejor selección.

La falta de una figura encargada de coordinar, planear y promover las actividades que tengan que ver con la parte de seguridad informática genera una situación que se ve reflejada en el crecimiento de problema de seguridad que se presentan dentro de las empresas; esto, aunado a la ignorancia de no saber cuales son las capacidades necesarias y suficiente en conocimientos, formación y habilidades, así como las responsabilidades y deberes de la figura encargada de la seguridad de la empresa, hacen que sea difícil el poder seleccionar a la persona indicada que se encargue de ver lo referente a la seguridad informática dentro de las instituciones.

El propósito de tener una figura denominada: ***Oficial de Seguridad Informática (OSI)*** es tener a alguien al cual se pueda recurrir en caso de algún problema de seguridad, un **encargado de difundir las alertas, así como el proponer y definir esquemas que reduzcan los incidentes de seguridad que se presenten**. (Ver anexo D, acerca del Oficial de Seguridad Informática para saber más del tema)

Tomando en cuenta estos puntos se obtendrá un buen funcionamiento de la metodología aquí propuesta.

3.5 FASE 1.- CONOCIMIENTO DEL MEDIO AMBIENTE DE LA EMPRESA:

En esta fase, lo que se pretende es identificar y conocer el medio ambiente ó analizar la situación actual de la empresa, es decir, realizar una investigación preeliminar acerca de la misma en particular.

En la siguiente figura se muestra donde se encuentra ubicada la fase dentro de la metodología propuesta:

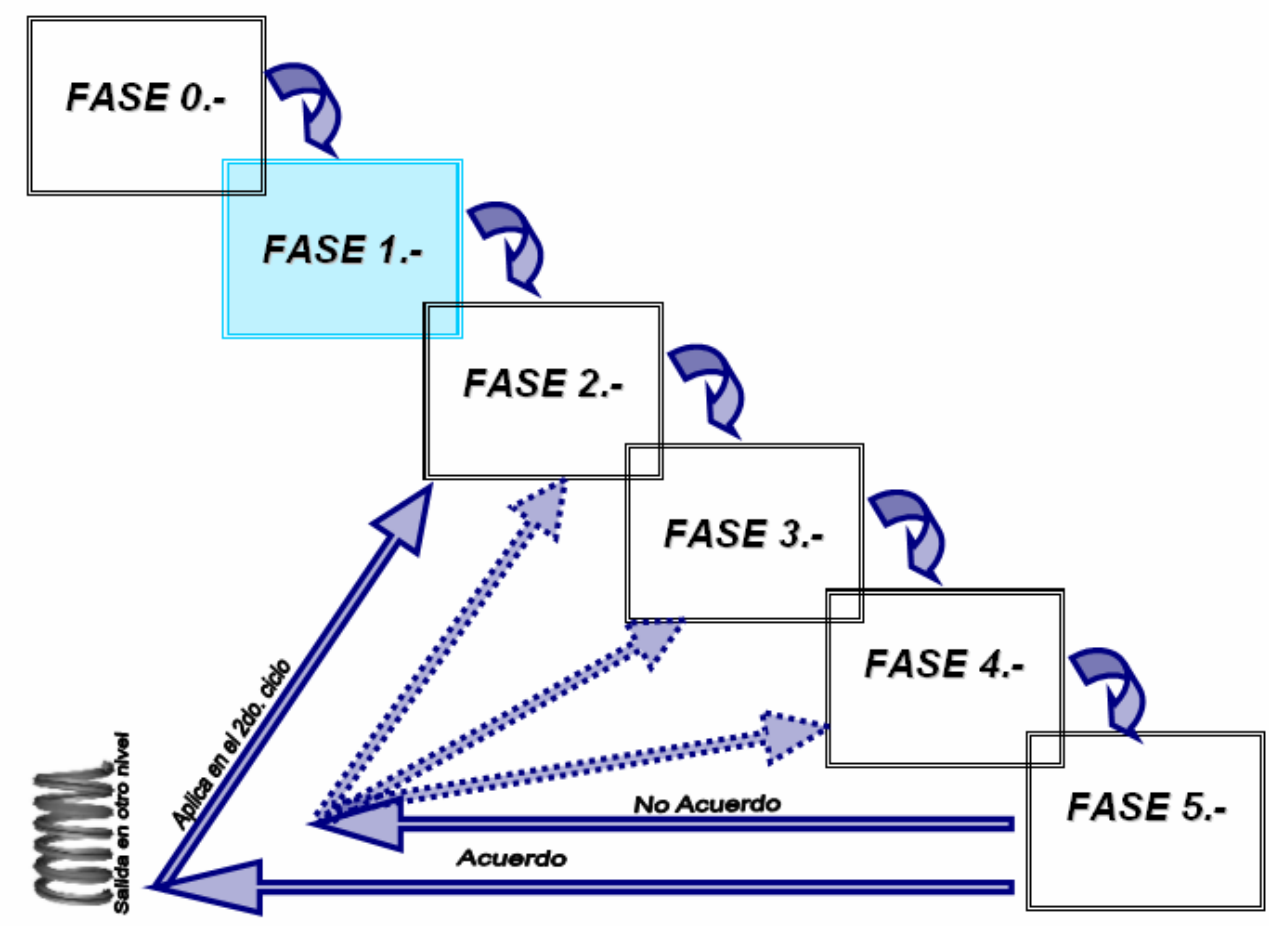


Figura 3.4 Representación de la metodología propuesta en la Fase 1.

3.5.1 Actividad1.1 *Identificar y obtener: la visión, misión, políticas, planes, estrategias, objetivos y actividades de la empresa en general.*

Para la implantación de actividades de control que estén involucrados con las tecnologías de información es necesario conocer los términos generales, y reconocer la situación actual; en la cual se encuentra la empresa; lo cual nos permitirá **conocer el medio ambiente y las áreas de la empresa**; así como elementos y relaciones fundamentales con el objetivo de estudio.

Algunos puntos a **conocer de la compañía son: sus orígenes, razón de ser, su marco normativo, a dónde se dirige, qué espera hacer, qué hace y cómo lo hace.** Es decir, se requiere conocer su: visión, misión, políticas sus planes correspondientes, los objetivos a cumplir para esos fines, las funciones que definen lo qué se hace y sus correspondientes procesos que permiten hacerlo.

El propósito de esta Actividad es comprender el entorno general de la empresa. Las técnicas que se puede emplear son la observación, entrevistas y para integrar todos estos elementos y tener una visión global es el mapa mental.

3.5.2 Actividad 1.2 *Obtener u elaborar la estructura organizacional de la empresa y del área de tecnologías de información.*

Un aspecto fundamental en el conocimiento del medio ambiente es: **identificar la estructura organizacional de la empresa y del área particular.** Esto ayudará a ubicar las áreas que se ven involucradas con los procesos del área de tecnologías de información.

El conocer el marco organizacional u organigrama de la empresa y del área de tecnologías de información proporcionará conocer los departamentos relacionadas con el área en particular, así como las dependencias de los cargos.

3.5.3 Actividad 1.3 *Identificar y obtener: las políticas, planes, estrategias y objetivos del área de tecnologías de información.*

Una vez identificado el medio ambiente general de la empresa, es necesario **conocer el medio ambiente particular**, en este caso, el área de tecnologías de información, en la cual se desean implantar las actividades de control, con el fin de identificar la razón de ser de sus planes y estrategias, además de sus objetivos.

Es decir, se debe definir, **identificar y obtener los planes, estrategias, políticas, funciones, actividades y procesos en general del área de tecnologías de información.** Por lo tanto, se debe determinar el entorno del área particular.

Para aquellas empresas que ya cuentan con procedimientos más específicos del área de TI, se puede solicitar lo siguiente:

- ☑ Políticas y procedimientos de TI, especialmente las políticas y procedimientos de seguridad.
- ☑ Plan de recuperación en caso de desastres o plan de continuidad de negocios.
- ☑ Plan estratégico de TI.
- ☑ Diagrama de la infraestructura de TI, indicando los servidores, la localización y uso de los mismos, y el software de base utilizado.
- ☑ Diagrama de la red.
- ☑ Metodología de desarrollo/implantación de sistemas.
- ☑ Procedimientos de mantenimiento/cambios a sistemas.
- ☑ Informe de control gerencial de las actividades de sistemas (por ejemplo, indicadores clave de rendimiento, estadísticas de operación, análisis de incidencias, control de proyectos, etc).
- ☑ Inventario de software aplicativo, en el cual se señale cual es el crítico para la empresa. Puede incluir:

    - Nombre del software y aplicativos (versión sí aplica)
    - Nombre de los Sistemas Operativos y versión
    - Nombre del software (versión sí aplica)
    - Características de los Sistema Operativos y versión
    - Lenguaje y versión
    - Base de datos y versión
    - Tiempo de funcionamiento
    - Planes de modificaciones en los sistemas.
    - Paquete, ¿Desarrollo interno o externo?
- ☑ Si han existido incidente de seguridad, solicitar reporte.

Las técnicas que se puede emplear son las de: observación, las entrevista y para tener una visión global de esta actividad puede ser la creación de mapas mentales.

El propósito de esta Actividad es examinar la evidencia disponible (por ejemplo, la documentación, los reportes, planes, etc., que utiliza la empresa), para identificar qué procedimientos de continuidad son requeridos para corroborar manifestaciones y obtener la seguridad que el ambiente de sistemas requiere para ser confiable.

3.5.4 Actividad 1.4 *Identificar y obtener u elaborar las funciones que se realizan en el área de tecnologías de información.*

Ya que se conoce el entorno particular y general de la empresa, hay que definir de forma detallada las funciones; como éstas son elementos que por lo común, no dependen de los cambios de las personas en los cargos, son un buen parámetro para conocer las estructuras funcionales de la empresa y del área en particular.

Además, es conveniente **conocer las funciones para tener una idea de que personas se involucran en éstas, así como identificar que conjunto de actividades son necesarias para el desarrollo de un proceso determinado**.

En el caso de que no se cuente con una descripción de cargos con claridad, un medio de apoyo para definir quienes deben realizar determinadas funciones en un proceso son las gráficas RACI ó RASCI (Responsible, Accountable, Supportive, Consulted, Informed), proporcionadas por el marco de referencia COBIT; esta técnica permite entender los roles y responsabilidades del personal involucrado. Es decir, ilustra genéricamente y de acuerdo a cada proceso quién es el responsable, quién debe rendir cuentas, a quien se debe consultar e informar dentro de un marco de trabajo organizacional estándar.

Estas gráficas proporcionan entendimiento para cada proceso, qué actividades son necesarias para este proceso y qué personas están encargadas de realizar estas actividades. (Ver anexo E, acerca de la Gráfica RACI para saber más del tema)

3.6 FASE 2.- IDENTIFICACIÓN Y ANÁLISIS DE LOS PROCESOS DE TI DE LA EMPRESA:

Dado que ya se identificaron las funciones especificadamente, de la misma manera se debe hacer con los procesos; por eso, en esta fase se tiene que identificar los procesos de TI en los que se aplicarán las actividades de control, en este caso, debido a que el uso de las actividades de control es respecto a la salvaguardar los recursos informáticos; el reconocimiento de procesos tendrá que encontrarse involucrados directamente con las tecnologías de información.

Todo esto se hace con el propósito de identificar de qué función proviene el proceso y las actividades que intervienen en cada uno.

En la siguiente figura se muestra donde se encuentra ubicada la fase dentro de la metodología propuesta:

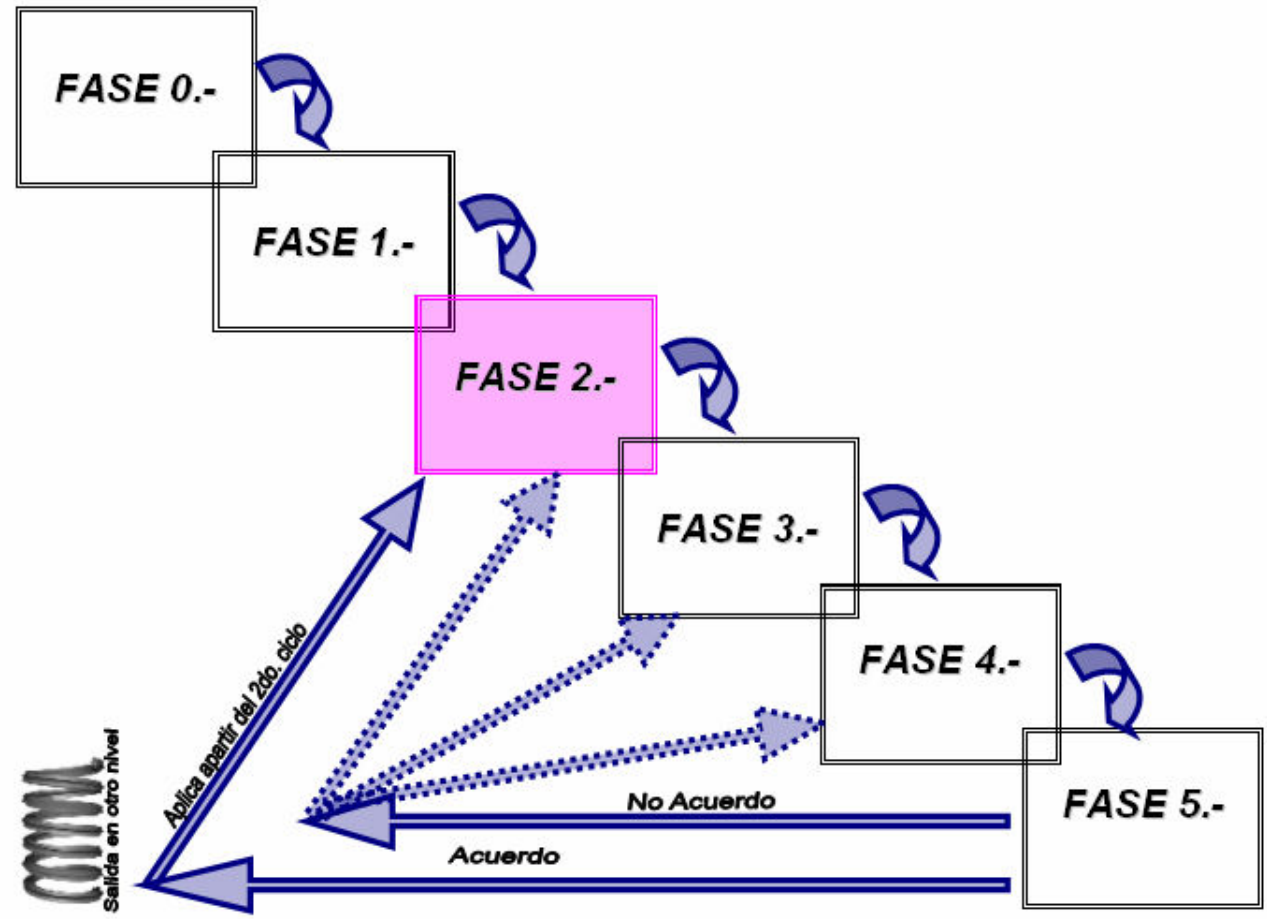


Figura 3.5 Representación de la metodología propuesta en la Fase 2.

3.6.1 Actividad 2.1 *Identificar la relación de los procesos y funciones y elaboración de un Diagrama de Flujo de Datos (DFD) cada proceso de TI.*

Una vez que se han determinado en forma general las funciones de TI, es el momento de **identificar los procesos que intervienen en el desarrollo de cada uno de las funciones** en el área en sí, de tal manera que puedan ser representados en forma gráfica como lo es un diagrama de procesos.

En esta actividad, se puede crear, de acuerdo a la información previamente obtenida en las actividades anteriores, una tabla en la cual se colocarán las funciones y los procesos que intervienen para la realización de cada una estas funciones; el desarrollo de ésta, ayudará a entender la procedencia de cada proceso y también, concebir el por qué están integradas por los pasos ó actividades que la conforman; a fin de obtener una perspectiva más amplia a cerca de lo que es cada proceso y así poder evaluarlo.

Para complementar esta perspectiva, se puede elaborar un Diagrama de Flujo de Datos (DFD) ó también conocido como Mapeo de Procesos, que se refiere a un diagrama básico ó detallado (de acuerdo a como se considere necesario), por cada proceso y también, podría hacerse, si es viable, un diagrama general en donde involucre todos los procesos del área como una visión colectiva.

El objetivo, es realizar una apreciación elemental de cada proceso, para identificar definidamente cuales son éstos, así como, iniciar con el reconocimiento de las actividades ó pasos que los conforman y funciones que intervienen; con la finalidad de determinar posteriormente cuales de estos procesos se podrían estar llevando a cabo erróneamente.

Para ello, se requiere solicitar toda la información indispensable como documentación, narrativas, manuales, etc., para puntualizar cada proceso.

Algunas técnicas que se pueden emplear son la observación, investigación y entrevista para recopilar la información necesaria.

Para la elaboración del Diagrama de Procesos se propone desarrollarlo con la técnica de Diagrama de Flujo de Datos (DFD), para visualizar de manera general los procedimientos y actividades. (Ver Anexo F, acerca del DFD y su simbología para saber más del tema).

A continuación, se mencionarán algunos consejos y cómo es que se debe desarrollar en general este diagramado.

Como primer paso es preciso determinar límites, es decir, puntos de inicio y final del proceso; al igual que los pasos principales que ocurren entre los puntos de inicio y parada del proceso, además de identificar las entidades involucradas (origen o destino de los datos) en el mismo y especificar los resultados del proceso.

Algunas recomendaciones que se pueden tomar en cuenta en el momento de iniciar con el diagramado o trazado son:

- ☑ Determine el nivel del mapa de proceso a elaborar y elija un nombre que identifique el proceso,
- ☑ Inicie con un borrador utilizando la simbología propuesta en el anexo F.
- ☑ Trace los limites (el inicio y el fin del proceso) y coloque las actividades intermedias que permiten crear ese proceso.
- ☑ Para definir estas actividades intermedias divida el proceso en pasos, cada paso será una actividad necesaria para el desarrollo de este.
- ☑ Asegúrese que cada paso ó círculo de retroalimentación tenga un escape al siguiente paso para que no se convierta en un círculo sin fin.

El **diagrama debe proporcionar el proceso "real", el que se lleva en el ejercicio**, que no siempre es el mismo que el proceso "ideal" el que se encuentra en los manuales, sí es que se cuenta con éstos.

De tal forma que esta técnica permitirá documentar los procesos o sí ya se cuenta con documentación, rectificar que se estén llevando a cabo de acuerdo a los manuales, de no ser así, ayuda a determinar la inserción de actividades de control para habilitar la efectividad de estos procesos.

Como observaciones finales de esta actividad, se debe tomar en cuenta:

- ☑ Analizar el diagramado para encontrar posibles problemas,
- ☑ Sí ya se cuenta con documentación previa de los procesos, se debe comparar las diferencias y similitudes en estos dos estados, en términos de procesos, actividades de control utilizados, trayectorias, flujos de tareas, etc.
- ☑ Y separar las actividades con problemas para identificar las soluciones de éstas, e implementar los cambios necesarios para que el proceso cambie del estado "como está" y sea igual al estado del proceso de "como debería estar".

Se deja a consideración el nivel de detalle del diagrama de flujo, ya que se puede realizar de acuerdo a las necesidades de conocimiento que se quiera alcanzar de cada proceso.

Afín de dar continuidad al tema y realizar una selección de procesos de TI que puedan contener algún problema, como primera instancia, se sugiere la actividad siguiente:

3.6.2 Actividad 2.2 *Identificar las brechas de operación que puedan contener los procesos TI y analizarlos.*

Bien, ahora que se conocen las funciones y los procesos que las integran, es necesario identificar si estos procesos cuentan con brechas operacionales.

*Las **brechas operacionales,** son aquellos lugares o situaciones en donde las operaciones reales fallan en dar los resultados esperados*; para esto hay que visualizar ampliamente el contexto en el que operan, en este caso, las situaciones operacionales relacionadas con el área TI.

Conociendo esto, y para **hacer una selección adecuada, hay que determinar los procesos que se vinculan a estas brechas*;*** esto va a ser posible***,*** mediante el apoyo de la observación, entrevistas y recopilación de información acerca de las brechas de operación que permita llegar a una selección de los procesos que se encuentren vinculados a situaciones inusuales que originen resultados no deseados.

Para ello, se requiere reunir la información suficiente (documentación, manuales, descripciones y narrativos) y se aconseja buscar como apoyo al personal adecuado, acorde a la delimitación de cargos realizada anteriormente y con las siguientes características:

- ☑ Que tengan conocimiento acerca del proceso,
- ☑ Brinden perspectivas funcionales,
- ☑ Estén interesados en mejorar el proceso,
- ☑ Estén dispuestos y motivados a permanecer con el proyecto hasta su culminación
- ☑ Sean lo suficientemente influyentes para facilitar la implementación de los cambios acordados al proceso.

Entonces, de no contar con la información y medios suficientes para determinar las brechas, será necesario efectuar una revisión detallada que vaya de proceso en proceso y actividad por actividad para identificar el flujo de las transacciones operacionales, además de cómo es su realización la empresa; todo esto con la finalidad de encontrar la oportunidad de analizar procesos o actividades que afecten en el cumplimiento de objetivos organizacionales.

Se recuerda que el objetivo general de esta fase es obtener toda la información necesaria sobre cómo los procesos se inician, registran, procesan y reportan, es decir,

entender el flujo de las transacciones operacionales de los proceso donde pueden ocurrir errores.

Una vez determinados los procesos vinculados con las brechas y hacer una revisión detallada de los mismos, la conclusión que se va obtener de cada proceso, se puede colocar en una tabla a manera de resultado de la observación e investigación de éstos, con el fin de poder comenzar con la determinación de sus posibles riesgos.

3.7 FASE 3.- ELABORACIÓN DEL DIAGNÓSTICO DE LOS PROCESOS DE TI CON BRECHAS OPERACIONALES DE LA EMPRESA:

Una vez reconocidos los procesos y su actividades, hay que identificar los riesgos contenidos en ellos, con la finalidad de evaluarlos, priorizarlos y darles solución a través de la implantación de objetivos y diseño de actividades de control.

La siguiente imagen se muestra la posición de ubicación la fase dentro de la metodología propuesta:

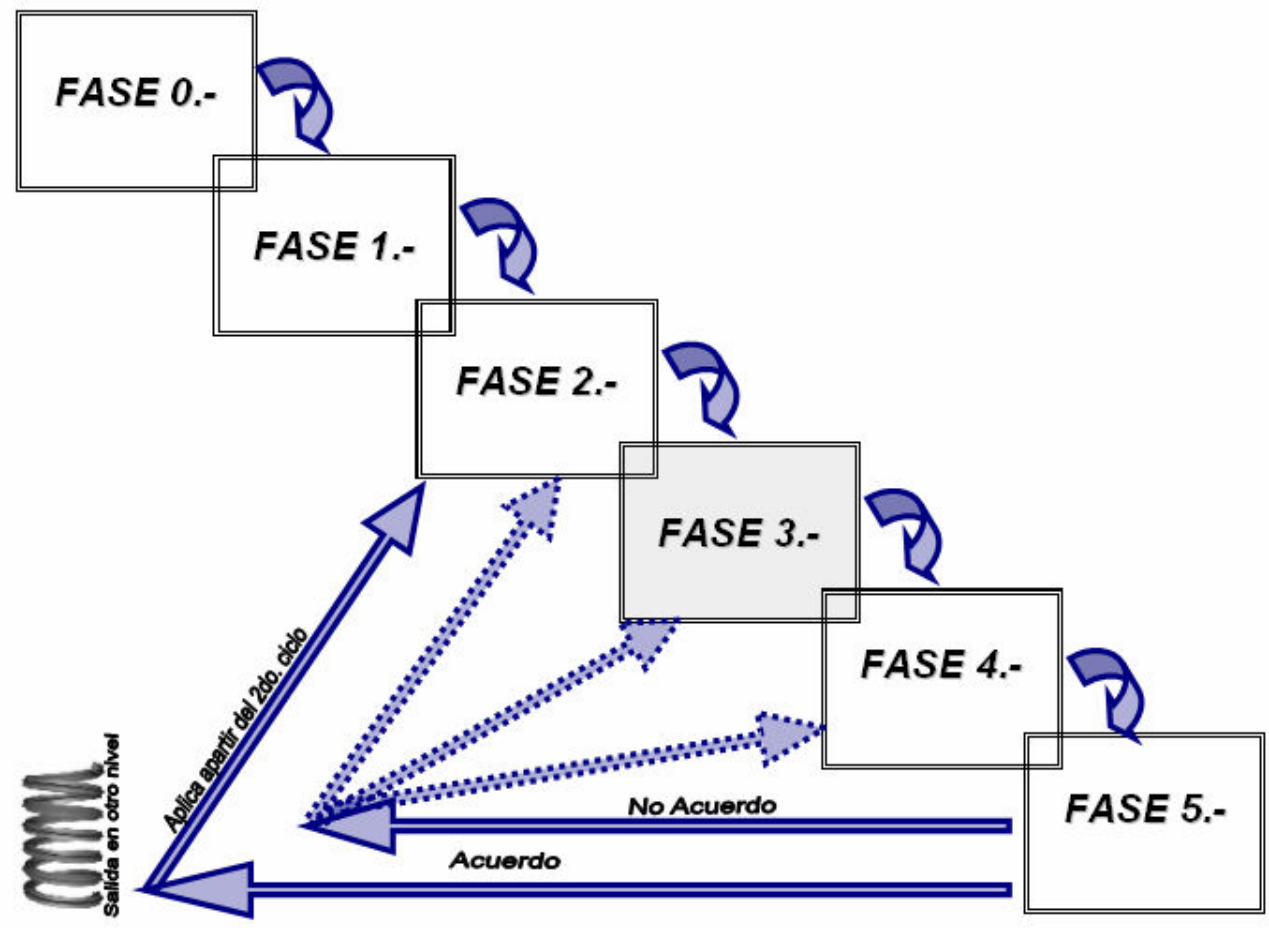


Figura 3.6 Representación de la metodología propuesta en la Fase 3.

3.7.1 Actividad 3.1 *Identificar y determinar los riesgos, amenazas y vulnerabilidades.*

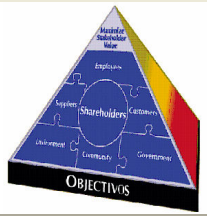
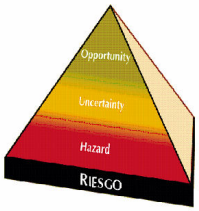
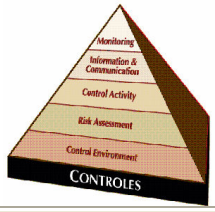
De los procesos previamente seleccionados, es decir, los que pueden tener algún problema, es preciso **identificar y determinar definidamente los conceptos como son: los riesgos, amenazas (sucesos nocivos) y las vulnerabilidades (fragilidades con las que cuenta la empresa);** con la finalidad de reconocer las definiciones y adquirir las nociones elementales para emplear la metodología ORCA que será la técnica que se utilizará para la elaboración de actividades de control.

Como una explicación introductoria, se presenta la ***Metodología ORCA*** (nombrada así por las iniciales de Objetivos, Riesgos, Controles y Alineación), la cual es un desarrollo de la firma de auditoria y consultoría PricewaterhouseCoopers empleada para la identificación y evaluación de riesgos a través de la alineación de procesos, actividades de control y riesgos.

En seguida, se presenta un cuadro en el que se explica en síntesis cada uno de los conceptos que la conforman:

ORCA (Objetivos, Riesgos, Controles ó actividades de control y Alineación)

Tabla 3.1 Elementos de la metodología ORCA [PWC, 2006]

Objetivos		La definición y comunicación de los objetivos de una organización al personal es un paso esencial para su logro.
Riesgos		Es importante determinar si los riesgos son cuantificables y si no evaluarlos, en términos cualitativos a fin de priorizarlos.
Controles ó Actividades de Control		La actitud y respuestas de la Dirección para evitar oportunidades, incertidumbres y peligros, es un factor esencial.

Alineación		Sólo la alineación de los reportes, políticas y sistemas de información permitirá lograr las metas de una organización.

El enfoque ORCA, ayuda a identificar los eventos que destruyen valor, y con base en los eventos y riesgos identificados, ayuda a definir las actividades de control que la Dirección debe ejecutar para asegurar que los objetivos sean alcanzados.

Este enfoque sirve como punto de partida para crear una cultura del Riesgo en toda la institución.

La metodología ORCA, se utiliza cuando:

- ☑ Se deseé fortalecer las actividades de control en la empresa.
- ☑ No se tienen correctamente identificados los riesgos que puedan afectar la efectividad de las operaciones de la empresa.
- ☑ Se desee definir y conocer las actividades que la Dirección debe ejecutar para asegurar que los objetivos sean alcanzados.

A continuación, y por motivos de comprensión, se explican más ampliamente cada uno de los elementos de la metodología ORCA de la siguiente manera, Riesgo, Control ó Actividad de control, Objetivo y Alineación.

***R**iesgo:* *Es la probabilidad de que un acontecimiento pueda afectar ó impactar el alcance de los objetivos*. Por lo general se mide por medio de una combinación del impacto y la probabilidad de ocurrencia [COBIT, 2005]. Algunos ejemplos son: fraude, robo, pérdida de activos fijos, deficiencia en logro de objetivos, etc.

Sin embargo, no son tan fácilmente identificables, dado que ***el riesgo es inherente***, es decir, innato e implícito ya que al realizar cualquier operación, actividad o proceso empresarial o no, se corren riesgos desde el momento que se ejecuta; las causas que proporcionan su aparición, pueden ser múltiples y de índole diversa y una misma causa puede generar más de un riesgo.

Entonces, para la identificación de los riesgos que enfrente una empresa en el logro de sus objetivos, hay que tomar en cuenta que puede ser de origen interno, es decir, provocados por la entidad teniendo en cuenta la actividad específica o sus características internas en el funcionamiento, como externos que son los elementos fuera de la organización que afectan, en alguna medida, el cumplimiento de sus objetivos.

Para identificar el riesgo puede seguir los pasos siguientes:

a) Escoger uno de los procesos previamente seleccionados.

b) Identificar las actividades principales del proceso y las eventualidades a las cuales están expuestas internas y externas. Tome como base las siguientes preguntas:

¿Cómo se podría producir cierto suceso dañino? y ¿Qué puntos débiles de la empresa provocaría que ese suceso existiera?; es posible que cada evento maligno puede comprender varias debilidades. Los puntos débiles más importantes suelen producirse por procesos mal definidos.

b.1) Sí no se conocen estas eventualidades por alguna razón, se puede recurrir a la búsqueda de incidencias anteriores registradas tal vez en una bitácora interna ó se pueden revisar algunos gacetas o informaciones publicadas de problemas de seguridad ya conocidos.

c) Este conjunto de eventualidades puede ser clasificado como riesgos, amenazas y vulnerabilidades.

Entiéndase por:

Riesgo: se refiere a la ausencia de seguridad que se puede estimar a través de la probabilidad y el alcance de los daños que podría ocasionar el suceso dañino.

Amenazas: Son los eventos ó causas que pueden producir daños y ocasionan que el riesgo sea eminente. Estos pueden ser ocasionados por fenómenos naturales, personas o maquinas / equipos. Materializado

Vulnerabilidades: Son las debilidades que la empresa puede tener y dar paso a que una amenaza ataque.

Ejemplo:

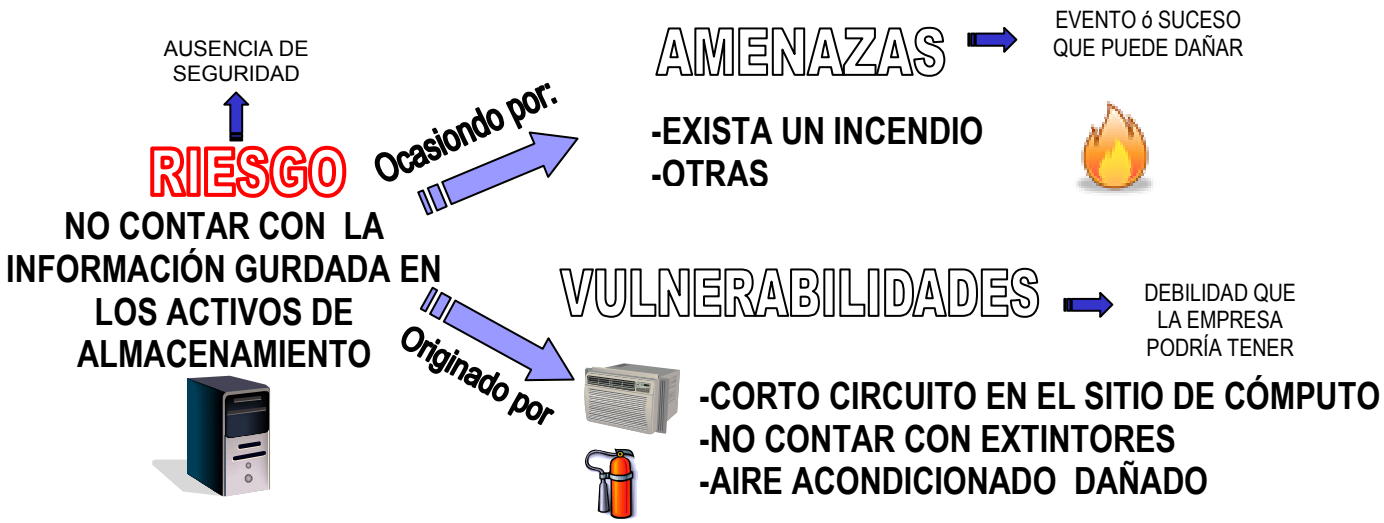


Figura 3.7 Ilustración del Riesgo, Amenazas y Vulnerabilidades.

d) Para comprender por completo los conceptos mencionados, se puede crear una tabla que se llamará: “Tabla de Identificación del Riesgo”, donde se detallen las amenazas que provocaría ese riesgo y las debilidades o vulnerabilidades que la empresa podría tener para que ese suceso se materialice.

Tabla 3.2 Ejemplo de la clasificación de las amenazas, vulnerabilidades y riesgos.

IDENTIFICACIÓN DEL RIESGO			
PROCESO	**AMENAZA** (Suceso maligno que lo ocasionó)	**DESCRIPCIÓN DE LAS VULNERABILIDADES** (¿Qué ocasionó ese suceso?)	**RIESGO** (¿En qué puede afectar?)
El “Proceso Z” previamente identificado, debido a su inadecuada realización, da paso a lo siguiente:	Incendio en el que se perdieron los activos de almacenamiento.	-Corto circuito en el sitio de cómputo.	*No contar con la información almacenada en esos activos cuando sea requerida.*
		-No contar con extintores.	
		-Aire acondicionado dañado.	

Ahora, que ya se conocen los eventos dañinos y las debilidades que pueden materializar el riesgo y perjudicar a los procesos de TI, se les puede dar un valoración con la finalidad de identificarlos y priorizarlos para darles solución con la implementación de actividades de control que permitirán a la empresa alcanzar una seguridad razonable en su información y logro de objetivos.

3.7.2 Actividad 3.2 *Evaluar el riesgo y seleccionar la técnica para evaluar.*

En seguida, se dará una explicación sobre el tema de evaluación de riesgo a nivel general ó resumen, ya que este tópico es muy extenso y debido a que las intenciones de este trabajo de tesis recaen esencialmente en el uso de objetivos de control y el desarrollo e implantación de sus actividades; por tal motivo, no se profundizará en el tema.

Para dar una valoración a los riesgos existe la evaluación de riesgos, que permite a la organización considerar los potenciales acontecimientos que pudieran afectar el logro de los objetivos. Esta generalmente **se mide a través de la probabilidad** que representa la posibilidad que un acontecimiento ocurra, **y el impacto** representa su efecto.

Pero la evaluación del riesgo no es un tópico que se tome a la ligera, ya que el cálculo del riesgo es muy incierto, debido a que **no se cuenta con una métrica universal** que refleje una medición de la información disponible. A consecuencia de lo anterior mencionado, las organizaciones siguiendo un punto de vista preventivo (antes de que se materialice el riesgo), utilizan dos tipos de evaluación de riesgo para su valoración: las evaluaciones cuantitativas y las evaluaciones cualitativas que a continuación se expondrán.

Existen dos tipos de evaluación de riesgo utilizados comúnmente por las empresas o personal que han deseado evaluar o valorar el riesgo, estas son:

La evaluación cualitativa *que es aquella donde la probabilidad del incidente y la magnitud de sus consecuencias se expresa en términos cualitativos como alta, media y baja***,** mientras que

La evaluación cuantitativa *los resultados se expresan en cifras.*

Entonces, para determinar la evaluación de riesgo más conveniente para una empresa, es preciso conocer el estado actual de la empresa y los acontecimientos por las que ésta, esta pasando, ya que ningún evaluación de riesgo es aplicable a todas las situaciones y que, según las circunstancias, una evaluación puede convenir más que otro; por tal motivo, más adelante se presenta un tabla comparativa que ayude a su selección.

Sin embargo, las evaluaciones de riesgo cualitativo y cuantitativo tienen sus ventajas y desventajas. Determinadas situaciones pueden demandar que las organizaciones adopten un enfoque cuantitativo.

Por el contrario, las organizaciones de pequeño tamaño o con recursos limitados, normalmente, encontrarán más adecuado el enfoque cualitativo.

En la siguiente tabla se resumen las ventajas y desventajas de cada uno de este tipo de evaluaciones de riesgo:

Tabla 3.3 Ventajas y desventajas de las evaluaciones cuantitativas y cualitativas. [Microsoft, 2004].

	CUANTITATIVO	CUALITATIVO
Ventajas	– Se asignan prioridades a los riesgos según las repercusiones financieras; se asignan prioridades de los activos (como servidores, equipos de cómputo, etc.) según los valores financieros.	– Permite la visibilidad y la comprensión de la clasificación de riesgos.
	– Los resultados facilitan la gestión del riesgo por el rendimiento de la inversión en seguridad.	– Resulta más fácil lograr el consenso.
	– Los resultados se pueden expresar en terminología específica de administración (por ejemplo: los valores monetarios y la probabilidad expresada como un porcentaje específico).	– No es necesario cuantificar la frecuencia de las amenazas.
	– La precisión tiende a ser mayor con el tiempo a medida que la organización crea un registro de historial de los datos mientras gana experiencia.	– No es necesario determinar los valores financieros de los activos.
		– Resulta más fácil involucrar a personas que no sean expertas en seguridad o en informática
		– Es sencillo y económico, no requiere de un análisis más profundo ó cuando no se existe la información suficiente para cuantificar parámetros.
Desventajas	– Los valores de repercusión asignados a los riesgos se basan en las opiniones subjetivas de los participantes.	– No hay una distinción suficiente entre los riesgos importantes.
	– El proceso para lograr resultados creíbles y el consenso es muy lento.	– Resulta difícil invertir en la implementación de actividades de control porque no existe una base para un análisis de costo-beneficio.
	– Los cálculos pueden ser complejos y lentos.	– Los resultados dependen de la calidad del equipo de evaluación de riesgos que los creo.

	– Los resultados sólo se presentan en términos monetarios y pueden ser difíciles de interpretar por parte de personas sin conocimientos técnicos. – El proceso requiere experiencia, por lo que los participantes no pueden recibir cursos durante el mismo.	

En seguida, se describirán ambas evaluaciones, haciendo énfasis en la evaluación cualitativa, ya que es la que se ha seleccionado para esta metodología, de acuerdo a que es más fácil y sencilla de usar, no requiere de personal especializado, ni de datos históricos y financieros para su aplicación.

La Evaluación Cuantitativa en su representación más básica, emplea la siguiente expresión matemática [Microsoft, 2004]:

$$PE = F \times V$$

Donde:

PE **=** **P**erdida **E**sperada, expresada en pesos y en forma semestral o anual.

F **= F**recuencia, veces probables en el que el riesgo se concreta en el semestre o año.

V **= V**aloración estimada que se podría perder para cada caso en que el riesgo se concrete, expresada en pesos.

La ***Frecuencia,*** hace uso de datos históricos, es decir, se debe de contar con una bitácora donde se haya registrado las veces que se ha presentado este evento para determinar su probabilidad; de no ser así, requiere de estimaciones estadísticas más elaboradas que requiera de personal con este conocimiento.

La ***Valoración estimada*** requiere de los siguientes elementos: una estimación monetaria acerca los activos, una lista de las amenazas importantes, el potencial de pérdida para cada empresa, por amenaza en 12 meses, protecciones, actividades de control y acciones recomendadas. (Ver Anexo G, acerca de la Evaluación del Riesgo: Uso de la técnica cuantitativa propuesta Por Microsoft, para saber más del tema).

Para el uso de esta evaluación se requiere más que iniciativa propia para su manejo adecuado. La empresa que opte por esta alternativa tendrá que tomar en cuenta que requiere un análisis ampliamente detallado de los riesgos y que esto implicaría una inversión considerable en tiempo y dinero.

Para la ***Evaluación Cualitativa***, ***hay que definir el impacto y la probabilidad de los riesgos de acuerdo a las percepciones de las personas que conocen los procesos y los riesgos que contienen***. Para ello, y dando continuidad a la

identificación previamente hecha de los riesgos y el uso de esta alternativa es preciso enlistarlos.

En base a esta lista se elaborará un cuestionario que se aplicará a este personal, dado a que pueda aportar algún conocimiento de los riesgos, con la finalidad de obtener información necesaria para determinar la valorización de los mismos.

Para esto, se debe establecer una serie de cuestionamientos donde se pregunte acerca de estos riesgos y del nivel que este personal considera que sucede y que impacta o daña a la empresa. Se propone las siguientes escalas a utilizar y su descripción, con el fin de que cada persona aplique el mismo nivel de medida a través de los siguientes parámetros:

Niveles para la **probabilidad:**

- **Alta:** es muy posible que el hecho se presente.
- **Media:** es posible que el hecho se presente.
- **Baja:** es muy poco posible que el hecho se presente.

Ese mismo esquema puede aplicarse para la escala de medida para el **Impacto,** ejemplo:

- **Alto:** Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.
- **Medio:** Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.
- **Bajo:** Si el hecho llegara a presentarse tendría bajo efecto en la entidad.

Ahora para integrar los resultados de los cuestionarios se puede hacer a través de una tabla que concentre los resultados y un gráfico, en donde se traslapen el impacto y la probabilidad y se de un valor a los riesgos en una visión integral.

Tabla 3.4 Cuadro de ejemplo que concentra los niveles de impacto y ocurrencia del riesgo evaluado. [Fuente Propia]

Entrevista aplicada a 50 personas	"RIESGO T"		
NIVEL / OCURRENCIA / IMPACTO	BAJO / Casi nunca	MEDIO / Algunas veces	ALTO / Siempre sucede
¿Qué nivel de *Ocurrencia* considera que este riesgo aparece en la empresa?	10	35	5

¿Qué nivel de *Impacto* causaría el surgimiento de este riesgo en la empresa?	35	12	3

VALORES DEL RIESGO ACORDE A LA PROBABILIDAD / IMPACTO				
1 Intrascendente	**2** Baja	**3** Media	**4** Moderado	**5** Alta

3.7.3 Actividad 3.3 *Priorizar riesgos y selección de alternativa para responder ante el mismo.*

Conforme al los valores asignados al impacto y la probabilidad, es posible obtener un valor general de ambos, facilitando la determinación de asignarle un nivel de prioridad a cada riesgo. A continuación se propone una tabla que unifica el valor de impacto y el de la probabilidad de ocurrencia en uno solo.

La valorización de esta tabla consiste en asignar a los riesgos calificaciones dentro de un rango, *que podría ser por ejemplo de 1 a 5,* dependiendo de la combinación entre impacto y probabilidad. Esto, se expresa de la siguiente manera:

Tabla 3.5 Cuadro de la prioridad del riesgo acorde al impacto y probabilidad del mismo. [Fuente Propia]

Impacto	Probabilidad	Valor	Prioridad
Bajo	Bajo	1	Intrascendente
Medio	Bajo	3	Media
Alto	Bajo	4	Moderada
Bajo	Medio	2	Baja
Medio	Medio	3	Media
Alto	*Medio*	5	Alta
Bajo	Alto	4	Moderada
Medio	*Alto*	5	Alta
Alto	Alto	5	Alta

Para graficar un conjunto de riesgos el siguiente ejemplo será de gran ayuda. En la siguiente representación, se puede observar un esquema de valorización de riesgos en función de la probabilidad e impacto de tipo numérico con escala:

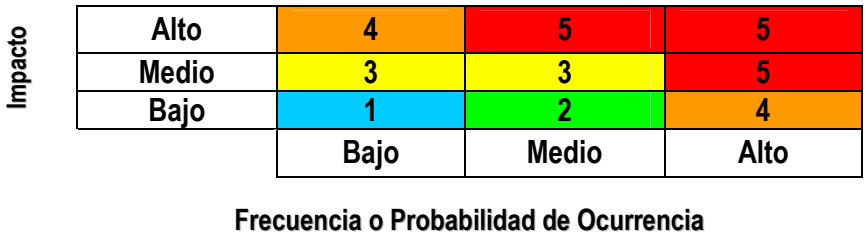


Figura 3.8 Gráfica del Impacto y Probabilidad de los riesgos. [Fuente Propia]

De esta manera, se puede identificar rápidamente que los riesgos de más bajo nivel se encuentran en la parte inferior izquierda, los riesgos de nivel medio se encuentran en la parte central y los niveles de más alto riesgo se encuentran en la parte superior derecha.

También, se puede utilizar una escala de colores como lo ilustra el anterior ejemplo para una localización más ágil visualmente.

Ahora bien, una vez entendida la valoración y la manera de darle prioridad a los riesgos, también se debe tomar en cuenta que un riesgo con gran magnitud de pérdida o daño y una mediana probabilidad de ocurrencia debe ser tratado en forma distinta que un riesgo con una media magnitud de pérdida o daño y una alta probabilidad de ocurrencia. En teoría los dos riesgos indicados poseen una idéntica prioridad para su tratamiento, pero en la práctica es muy difícil darles solución cuando se hace frente a limitaciones en los recursos disponibles.

Por consiguiente, es recomendable que se elabore un nuevo comparativo que ayude a realizar una selección más adecuada a las posibilidades y disposiciones de la empresa.

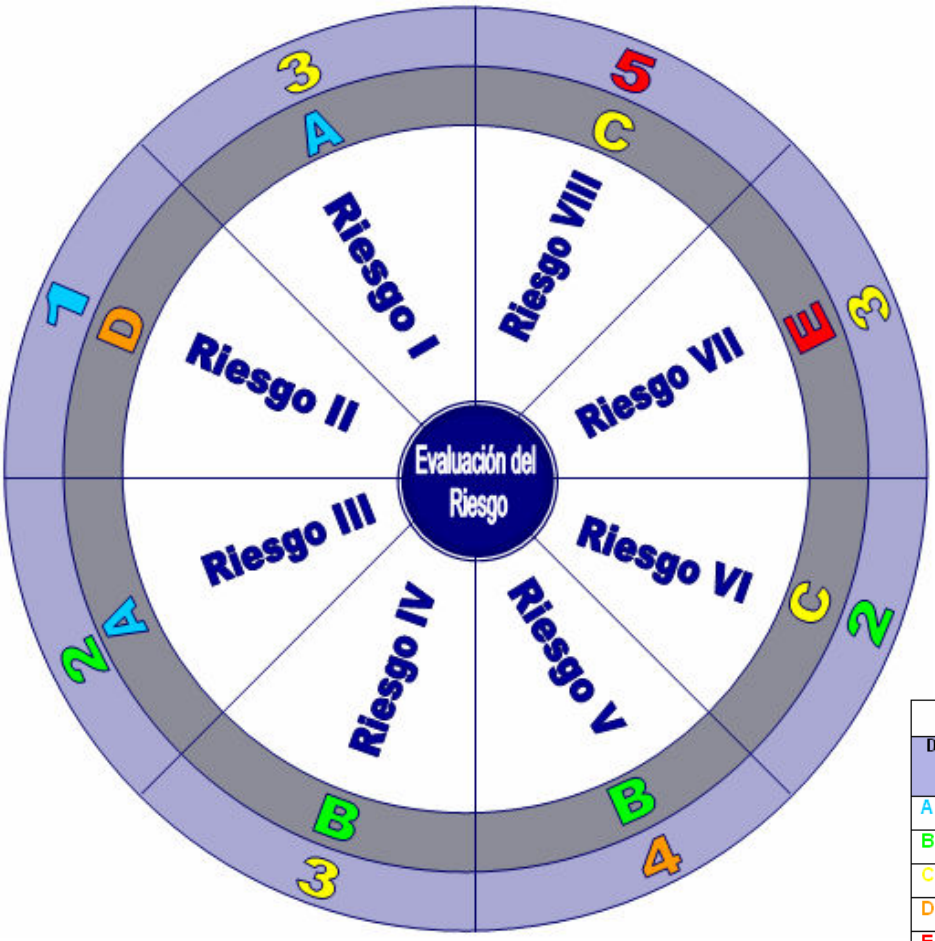
Este comparativo se puede hacer mediante otra gráfica en donde se traslapen las prioridades de los riesgos con respecto a la disponibilidad de recursos con los que cuenta la Dirección para enfrentar los riesgos.

Por ejemplo, supongamos que se tiene un conjunto de 8 riesgos *(I – VIII)*, cualesquiera ya valorados y con sus respectivas disposiciones de recursos. A continuación se presenta el cuadro comparativo con cada la disponibilidad de recursos y prioridad del riesgo de cada uno de los riesgos obtenidos.

Tabla 3.6 Cuadro comparativo de los Riesgos, la Disponibilidad de Recursos y la Prioridad del Riesgos. [Fuente Propia]

Cuadro Comparativo Riego / Recursos / Prioridad		
Lista de Riesgos	Disponibilidad de Recursos	Prioridad del Riego
I	A	3
II	D	1
III	A	2
IV	B	3
V	B	4
VI	C	2
VII	E	3
VIII	C	5

Luego entonces, la graficación de estos dos términos (Recursos y Probabilidad de riesgo) quedaría de la siguiente forma:



Simbología	
Disponibilidad de Recursos	**Prioridad del Riesgo**
A Mínimo	1 Intrascendente
B Limitado	2 Baja
C Regular	3 Media
D Muy Bueno	4 Moderado
E Excelente	5 Alta

Figura 3.9 Gráfica comparativa de la Disponibilidad de Recursos y la Prioridad de los Riesgos. [Fuente Propia]

Ahora bien, la selección deberá realizarse **con forme al nivel de riesgo (entre mas alto sea, más prioridad de resolución deberá tener) y la disponibilidad de recursos que ofrezca la dirección de la compañía (entre más recursos disponibles será mejor) según sea el caso**; ahora, es el momento para iniciar con una estrategia para dar una solución a estas debilidades que afectan el área de TI.

Continuando con la evaluación cuantitativa, los resultados obtenidos, van a permitir aplicar alguna de las alternativas para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para responder ante los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos.

Existen 4 estrategias o formas de responder ante los riesgos [Santillana, 2003]:

- **Tolerar**: Es cuando el riesgo se acepta, si el costo de superar un riesgo es mayor que el del riesgo mismo, o si superar dicho riesgo absorberá recursos que se utilizarán para superar un riesgo mucho más serio, la medida más conveniente es limitarse a aceptar el riesgo.

- **Transferir**: Se transfiere el riesgo a un tercero como a una compañía de seguros (contrato de outsourcing, póliza de seguro).

- ***Mitigar***: Reducir el riesgo mediante la implementación de contramedidas que adoptan los equipos de seguridad como es el establecimiento de una serie de actividades de control que permiten mitigar o limitar el riesgo a unos niveles aceptables.

- **Eliminar**: Terminar con el riesgo, existen situaciones en las que el nivel de riesgo y el costo de superarlo son simplemente inaceptables. En tales casos, resulta más conveniente evitar el riesgo, ya sea al retirar el sistema ó proceso afectado ó simplemente no implementarlo.

En este caso de estudio, lo que se desea es darle continuidad a la alternativa de ***Mitigar*** ya que es la que va a permitir superar o aminorar las debilidades que se han detectado en la empresa, mediante el uso de actividades de control.

Una vez que se conoces los eventos que pueden provocar la efectividad de los riesgos, es el momento para iniciar con el tema de actividades de control y por consiguiente objetivos de control.

3.8 FASE 4.- IDENTIFICACIÓN, DISEÑO Y DESARROLLO DE ACTIVIDADES DE CONTROL EN LOS PROCESOS DE TI CON RIESGO:

Ya que se ha identificado y estimado el nivel de riesgo, ahora, deben adoptarse las medidas para enfrentarlo; en esta fase, se continuará con la explicación de los conceptos restantes de la metodología ORCA que son el conocimiento soporte para poder identificar las actividades de control existentes y diseñar complementarias; así como, la selección de objetivos que deben ser cumplidos por estas actividades de control; plasmándolo en el desarrollo de una matriz que contenga la integración de estos elementos.

A continuación, la siguiente representación muestra e lugar en donde se encuentra esta fase dentro de la metodología propuesta:

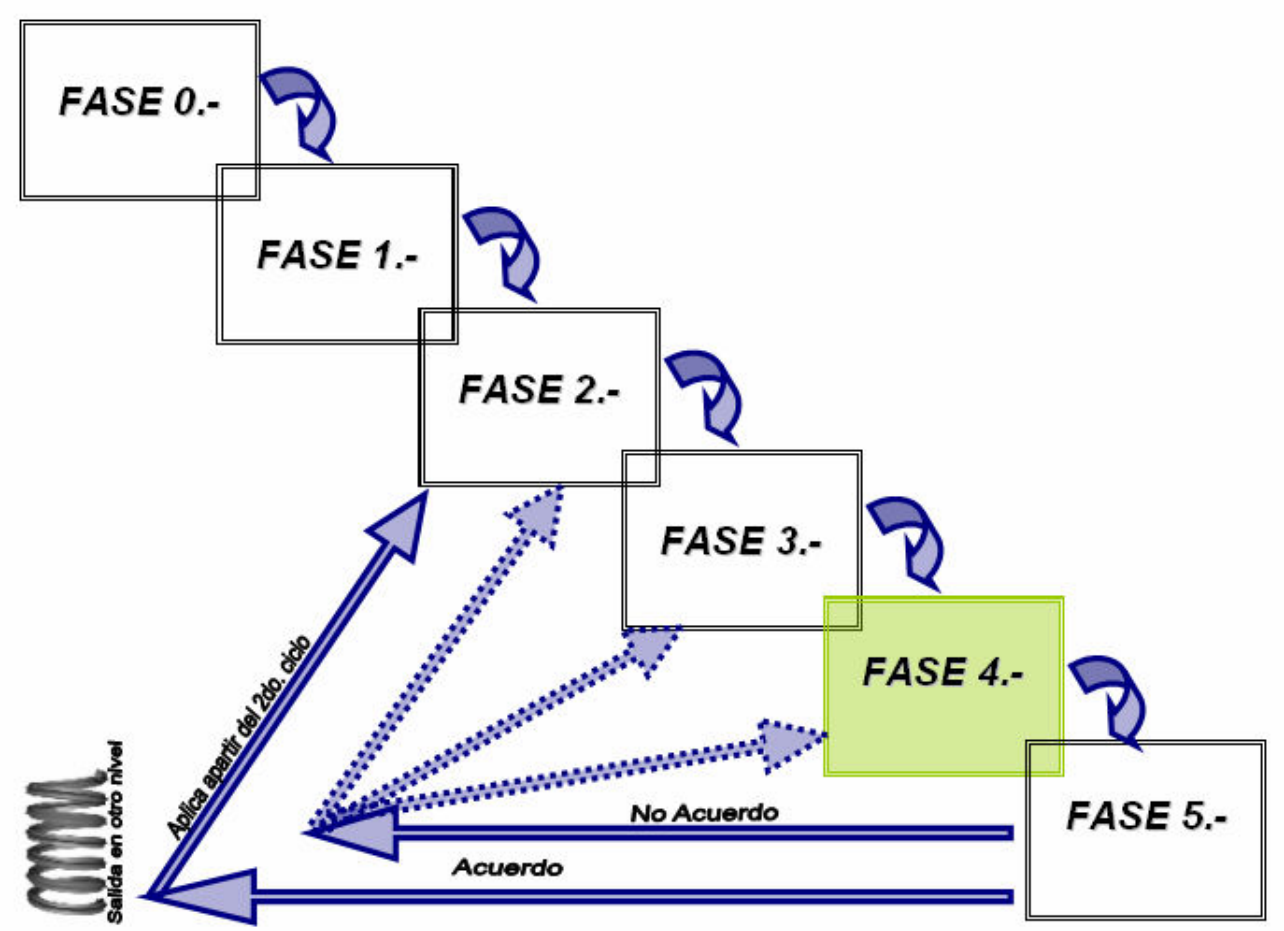


Figura 4.1 Representación de la metodología propuesta en la Fase 4.

3.8.1 Actividad 4.1 *Identificación de actividades de controles en los procesos de TI.*

Una vez que se conocen con detalle los procesos previamente seleccionados del área de TI; es necesario identificar cuales de ellos cuentan con actividades de control. Para asimilar lo que es una actividad de control en la empresa se utilizará el siguiente ejemplo:

Cualquier compañía, ¿A qué peligro se expondría, al dejar de hacer respaldos de la información continuamente? El riesgo sería notable y esta vulnerabilidad de la empresa provocaría la amenaza continua de perder información, lo que permitiría que no se cuente con una fuente de información confiable, que pudiera llevar el negocio hasta la quiebra.

Ahora bien, para contra restar esto, existen los ***Controles ó actividades de control:*** *que son las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados.*

Para una identificación más viable se propone **realizar una lista con las posibles actividades de control ó contramedidas para cada riesgo;** un buen apoyo podría ser nuevamente del personal involucrado en los procesos de TI anteriormente seleccionados, para realizarles entrevistas y aplicares un cuestionario que ayude a obtener información acerca de las soluciones posibles para elaborar este listado.

A continuación, se presentan las siguientes preguntas de apoyo:

- ☑ ¿Qué medidas debe adoptar la empresa para impedir la aparición del riesgo?
- ☑ ¿Qué puede hacer la empresa para recuperarse del riesgo una vez detectado?
- ☑ ¿Qué medidas puede adoptar para detectar la aparición de riesgos?
- ☑ ¿Cómo se puede supervisar la actividad de control para garantizar que se continué aplicando?
- ☑ ¿Existen otras acciones que se puede llevar a cabo para afrontarlo?

Los resultados de estas entrevistas y cuestionarios ayudarán identificar actividades de control ya existentes e identificar algunas propuesta de medidas para diseñar nuevas actividades.

Pero es posible que en esta parte se pueda sufrir el riesgo de detección, en donde la persona encargada de efectuar esta metodología no detecte un error importante, debido a que en el transcurso de averiguación de las actividades de control, no se cuente con la suficiente información; por ello, se recomienda conseguir material suficiente (evidencia) que proporcione el convencimiento y soporte acerca de la necesidad de implementar una ó varias actividades de control en un proceso. (Ver Anexo H, acerca de Categorías, clasificación y condiciones de las actividades de control de acuerdo al desarrollo del Control Interno para saber más del tema).
Una vez que se han identificado las posibles actividades de control dentro de la empresa, a continuación, se la relación que tiene con los objetivos de control para el diseño nuevas actividades.

3.8.2 Actividad 4.2 *Diseño de actividades de controles en los procesos de TI.*

Para el diseño de actividades, primero se requiere conocer el objetivo que se desee alcanzar, el propósito que se quiere cumplir y que es afectado por la aparición del riesgo**.**
Por ello, y retomando el concepto de actividades de control dice, que los controles van asociados con ***el cumplimiento de objetivos;*** éstos están profundamente relacionados ya que se necesitan mutuamente para que se obtenga el resultado deseado. La empresa es un conjunto de actividades y procesos, y cada uno de estos cumple un objetivo dentro de ella, la sumatoria de todos los objetivos lleva a la compañía a cumplir un objetivo global.

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

Las características con las que deben contar los objetivos son las siguientes:

- ☑ Posibles y razonables,
- ☑ Definidos claramente por escrito,
- ☑ Útiles,
- ☑ Aceptados y usados,
- ☑ Flexibles,
- ☑ Comunicados al personal y
- ☑ Controlables.

En resumen, este objetivo o proposición lo que hace, es decir el producto que se quiere obtener con la aplicación de una acción.

Ahora se presenta un ejemplo:

Tabla. 3.7 Ejemplo de Objetivo de control y actividad de control.

Acción que se debe tomar para que el objetivo se cumpla.

OBJETIVO DE CONTROL	CONTROL Ó ACTIVIDAD DE CONTROL
Facilitar la operación correcta de las aplicaciones y el uso de la infraestructura de TI.	Verificar la existencia de manuales de usuario y material de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitoso de las aplicaciones.

Por lo tanto, mediante las técnicas de observación, indagación, entrevistas, solicitud de documentación y sentido común es posible lograr detectar y crear actividades de control con el que ya podría contar la empresa. Entonces, para crear el entorno de seguridad en las TI se establece un conjunto de objetivos de control los cuales deben ser cumplidos o alcanzados por las actividades de control ó controles y estos últimos, **se diseñan de acuerdo al cumplimiento del propósito al riesgo que se desee evitar.**

Subrayando que el diseño de la actividad de control se hará de acuerdo al impacto del objetivo que se quiera salvaguardar, por ejemplo, “el almacenamiento de la información”; sí la información es muy importante, los respaldos que se harán de ésta, serán más a menudo que los respaldos de la información de menor categoría. Las categorías de la información serán proporcionadas por cada empresa, ya que ella decide cual es la información de mayor y menor importancia para la misma.

Una manera de disponer con objetivos que contengan todas estas características mencionadas y que satisfagan las necesidades de un ambiente de seguridad en la información, es basarse en objetivos de en un marco referencial que brinde buenas

prácticas y permita el acceso accesible a su realización, de tal forma, que se aconseja emplear el estándar COBIT que tiene gran aceptación y contiene todos estos requisitos. (Ver Anexo I, acerca del Marco Referencial COBIT para saber más del tema).

Otro definición que interviene para vincular los conceptos de control ó actividad de control y objetivo de control es la ***Alineación***: *esta concepción se refiere a que los objetivos de control seleccionados deben estar acorde y dentro de los objetivos generales del negocio.*

Los objetivos de control deben ser objetivos particulares que ayuden a conseguir el objetivo general de la empresa, es decir, deben estar sincronizados de tal forma que trasladen su efecto a los niveles superiores provocando una cascada de cumplimiento de metas brindada por la alineación entre éstos, proporcionando transparencia para las operaciones y procesos que se verá reflejado en mejores resultados de desempeño en el negocio.

Por lo tanto, la noción y relación del **O**bjetivo de control, el **R**iesgo, el **C**ontrol ó actividad de control y su **A**lineación, permiten comprender la correspondencia de estos términos y solución que se puede alcanzar para identificar, evaluar y modificar un mal proceso de TI.

En la siguiente Actividad, se desarrollará una matriz basada en los conceptos ya vistos.

3.8.3 Actividad 4.3 *Desarrollar la matriz de objetivos de control, actividades de control y riesgo.*

Ahora bien, ya que se ha identificado que la empresa puede correr riesgo al permitir vulnerabilidades que dan entrada a sucesos dañinos; que es posible que cuente con acciones de control que las mitiguen y que a falta de éstas actividades es posible crearlas, asociarla y alinearlas con el cumplimiento de objetivos de control y objetivos del negocio, entonces, es tiempo de continuar con el desarrollo de ***una matriz que se***

llamará "<u>Matriz de Objetivos de Control, Actividades de Control y Riesgos</u>"en la cual se concentran esta definiciones.

Esta matriz será dividida en dos, l***a primera parte, usará los términos de la metodología ORCA*** que ya fueron vistos en las actividades 3.9, 4.1 y 4.2, y será complementada por otros conceptos que adicionales que hacen referencia a éstos; como a continuación se muestra:

Tabla. 3.8 Cabecera de la matriz de objetivos de control, actividades de control y riesgos (Inicio). [Fuente Proipia]

1) Objetivo de control	2) Descripción del Riesgo	3) Actividades de Control	4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Evidencia, Supervisión y autorización)	5) Periodicidad de la actividad de control	6) Clasificación de la actividad de control Manual /Automático

La **segunda parte** que en seguida se muestra**, será abordada más adelante en la Fase V** dado que esta parte restante **trata de la evaluación y monitoreo de las actividades de control.**

Tabla. 3.9 Cabecera de la matriz de objetivos de control, actividades de control y riesgos (Final). [Fuente Proipia]

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia

Entonces, contemplando lo anterior, inmediatamente, se iniciará con los elementos restantes de la primera parte de la matriz, recordando que los primeros 3 términos ya fueron abordados en actividades posteriores:

4) DESCRIPCIÓN DE LA ACTIVIDAD DE CONTROL:

1) Objetivo de control	2) Descripción del Riesgo	3) Actividades de Control	4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Evidencia, Supervisión y autorización)	5) Periodicidad de la actividad de control	6) Clasificación de la actividad de control Manual /Automático

En esta columna se da una **explicación de la actividad de control** dentro de la empresa y se puede responder con las preguntas siguientes: ¿Qué actividad de control se está aplicando para este objetivo?, ¿Cómo se lleva acabo esta actividad?, ¿Quién realiza esta actividad?, ¿Dónde se realiza esta actividad?, ¿Cuándo se realiza la

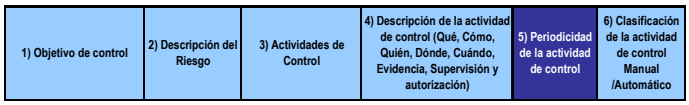
actividad de control?, ¿Qué evidencia produce esta actividad de control?, ¿Quién supervisa esta actividad? ¿Quién autoriza la realización de la actividad de control?, etc.

Ejemplo:

Tabla. 3.10 Ejemplo de objetivo de control, actividad de control y descripción de la actividad de control.

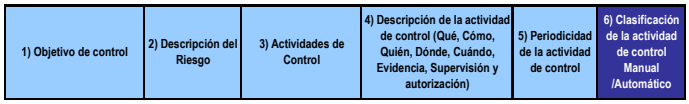
Acción que se debe tomar para que el objetivo se cumpla. **Situación de la empresa con respecto a esta actividad de control.**

OBJETIVO DE CONTROL	CONTROL Ó ACTIVIDAD DE CONTROL	DESCRIPCIÓN DEL CONTROL EN LA EMPRESA.
Facilitar la operación correcta de las aplicaciones y el uso de la infraestructura de TI.	Verificar la existencia de manuales de usuario y material de entrenamiento para transferir el conocimiento necesario para la operación y el uso exitoso de las aplicaciones.	El área de TI de la empresa cuenta con documentación acerca de los aspectos de operación y niveles de servicio.



5) PERIODICIDAD:

Se refiera a la **cantidad de veces con la qué se aplica esta actividad de control,** puede ser varias veces al día, semanal, quincenal, mensual, anual, etc.



6) CLASIFICACIÓN DE LA ACTIVIDAD DE CONTROL:

Esta columna trata acerca de la clasificación de la actividad de control ó control de acuerdo a la forma en que se lleva acabo éste; es decir, sí son ***Automáticos***, se refiere a que *son soportados por los sistemas de aplicación e involucra una comparación efectuada por el sistema de determinada información relativa a una transacción con una serie de parámetros pre-establecidos.*

Ejemplo: La aplicación verifica que el nombre de usuario y contraseña son válidos para acceder al mismo. Cuando se realicen verificaciones del funcionamiento de estos controles, se recomienda que sólo se prueben una vez, ya que la aplicación si esta programada correctamente siempre funcionará bien, de lo contrario siempre habrá errores.

Y sí son ***Manuales***: *Son aquellos llevados a cabo por los funcionarios de la organización y su efectividad está sujeta a la responsabilidad, capacidad, experiencia del funcionario que los realiza y la segregación de funciones.*

Ejemplo: Para realizar una modificación a un programa o sistema, se requiere de una solicitud formal de cambio por parte del dueño de la información hacia el área de

desarrollo, debido a que los desarrolladores no deben realizar alteraciones a las aplicaciones sin el consentimiento de este dueño. [Reyes, 1992].

Luego entonces, la matriz de objetivos de control, actividades de control y riesgos en su primera parte y agregando un ejemplo, se conformará de las siguientes columnas que quedarán de esta manera:

Tabla 3.11 Matriz de objetivos de control, actividades de control y riesgos (Inicio). [Fuente Propia]

Dado que significa un reto para las pequeñas y medianas empresas poseer y mantener un sistema de seguridad efectivo en las TI, a continuación se ha agregado una lista que plantea los controles mínimos con los que podrían contar estas empresas, siendo los tres primeros los más importantes para que una pequeña empresa mejore notablemente su seguridad.

Tabla 3.12 Lista de actividades de control para TI, aplicables para las pequeñas y medianas empresas [Fuente propia].

	1) Objetivo de control	2) Descripción del Riesgo	3) Actividades de Control	4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Evidencia, Supervisión y autorización)	5) Periodicidad de la actividad de control	6) Clasificación de la actividad de control Manual /Automático
DOMINIO ENTREGAR Y DAR SOPORTE	Brindar un servicio continuo de TI requiere de la administración de un sitio de almacenamiento externo a las instalaciones, donde se guarden los respaldos de información necesarios para la recuperación de TI y para los planes de continuidad de la empresa. La Gerencia de TI debe asegurarse de que este sitio cuente con las políticas y procedimientos indispensables para recuperar, mantener y conservar la información empresarial. (Referencia COBIT-DS4)	No contar con respaldos de información que pueda ser requerida en cualquier momento, puede provocar perder la disponibilidad de la información. (Nivel medio **3**)	Tener un proceso para el acceso a los medios de respaldo (cintas, Discos Compactos y medios removibles).	"La empresa" no cuenta con un formato manual o automatizado donde el dueño de la información y la Gerencia de TI supervisen y autoricen el uso e instalación de la información respalda en cintas, Discos Compactos y medios removibles.	Anual	Manual

ACTIVIDADES DE CONTROL DE TI PARA PEQUEÑAS Y MEDIANAS EMPRESAS

1. **Protección contra Virus y spyware.**
2. **Seguridad en redes, firewalls, Conexión inalámbrica segura.**
3. **Procedimientos de respaldos.**
4. Controles de privilegios de acceso a archivos.
5. Plan de recuperación de desastres y continuidad de TI.
6. Controles que permitan a TI ser parte de los planes a corto y largo

Conocidas las Actividades de control y demás términos relacionados con su conformación, en la siguiente fase se mostraran algunos otros elementos que se deben tomar en cuenta para la evaluación y monitoreo, además de algunos seguimientos para la implantación de las actividades de control y capacitación del personal.

3.9 FASE 5.- IMPLANTACIÓN Y MONITOREO DE LAS ACTIVIDADES DE CONTROL Y CAPACITACIÓN DE PERSONAL:

Antes de continuar con la segunda parte de la tabla, primero se explicará cómo se deben implantar los controles ó actividades de control y que capacitación se le debe

dar al personal involucrado, para que una vez implantados entonces ahora sí puedan ser evaluados y monitoreados, elementos que conforman la segunda parte de la tabla.

En la siguiente figura se muestra donde se encuentra ubicada la última fase de la metodología propuesta:

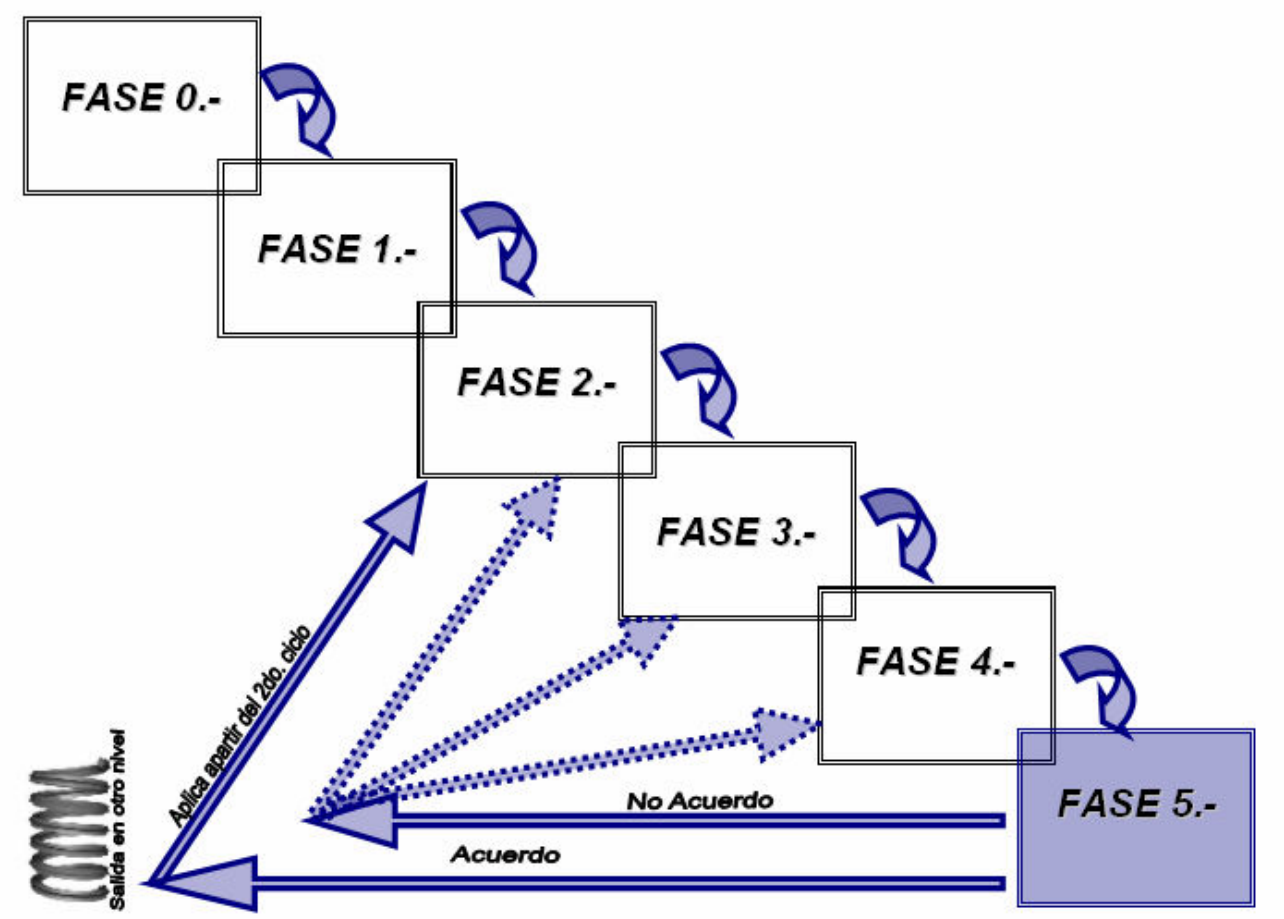


Figura 3.11 Representación de la metodología propuesta en la Fase 5.

3.9.1 Actividad 5.*1 Implantación de las actividades de control y preparación del personal.*

El responsable del cumplimiento de esta metodología, tendrá que iniciar una importante labor, primero tiene que **dar a conocer las actividades de control exhortando a la**

concienciación y convencimiento hacia a la Dirección, personal de TI y demás involucrado, para que comprendan y sigan los procedimientos, normas, políticas y prácticas nuevas que le ayudarán a realizar su trabajo. (Ver Anexo J, acerca de la Seguridad de la información y el factor humano de acuerdo a ISACA, para saber más del tema)

Haciendo énfasis en la oportunidad de gozar de la ayuda que se obtendrán al implantar esta actividades de control. Esto es, tratar de disminuir la resistencia al cambio. El cambio es positivo pero temeroso, por lo que es aconsejable ser prudente, avanzar poco a poco, impartir la mayor cantidad de información posible, tener contacto con el personal, **explicando las ventajas y beneficios** que generará el implantar las actividades de control, no solo para la entidad, sino para el personal en sí. Estar preparados a atender consultas, recibir sugerencias, ser participativo y transparente. (Ver Anexo K, acerca de del Proceso de cambio de acuerdo a ISACA, para saber más del tema)

Debe hacer conocer al personal que están participando en la creación de un ambiente de seguridad, que están aportando y apoyando en la viabilidad del mismo.

Para **generar motivación y cooperación del personal** en la efectiva implantación de los controles, es necesario hacerle conocer las "metas alcanzadas" y agradecerles por su aporte importante, como también, insinuarles su compromiso para su continuidad.

Los objetivos alcanzados no solo se refieren al cumplimiento de las actividades periódicas programadas, sino a los resultados alcanzados con dichas actividades.

Por ejemplo; el personal ahora muestra compromiso con la entidad, aporta con ideas, replica la filosofía de la Dirección de implantar una efectiva actividad de control en las TI, la imagen de la entidad es mejorada, por el cambio de actitud del personal, ahora es mas atento y oportuno en su atención, etc.

La concienciación y los pasos mencionados, anteriormente, no es una actividad "temporal", deberá ser recurrente para **producir un cambio de actitud en el personal,** de manera que se arraigue el control de las TI en la empresa.

Una buena práctica es **establecer entrenamiento y capacitación de seguridad** continua para el todo el personal involucrado, así como publicar anuncios de seguridad que recuerden a los usuarios sus responsabilidades y restricciones, junto con una advertencia de las medidas que se pueden tomar contra los infractores.

Para asegurarse que los controles ó actividades de control se están llevando acabo, se requerirá realizar procedimientos que monitoreen para detectar errores de proceso e identificar fallos de seguridad de forma sencilla. Este monitoreo concederá adoptar acciones correctivas y preventivas proveyendo al sistema o medio ambiente de seguridad de mantenimiento y mejora continua.

3.9.2 Actividad 5.2 *Monitoreo de las actividades de control.*

Ahora, para el monitoreo y evaluación de las actividades de controles y retomando los pasos vistos, anteriormente, se hará uso de la metodología ORCA, expuesta a continuación:

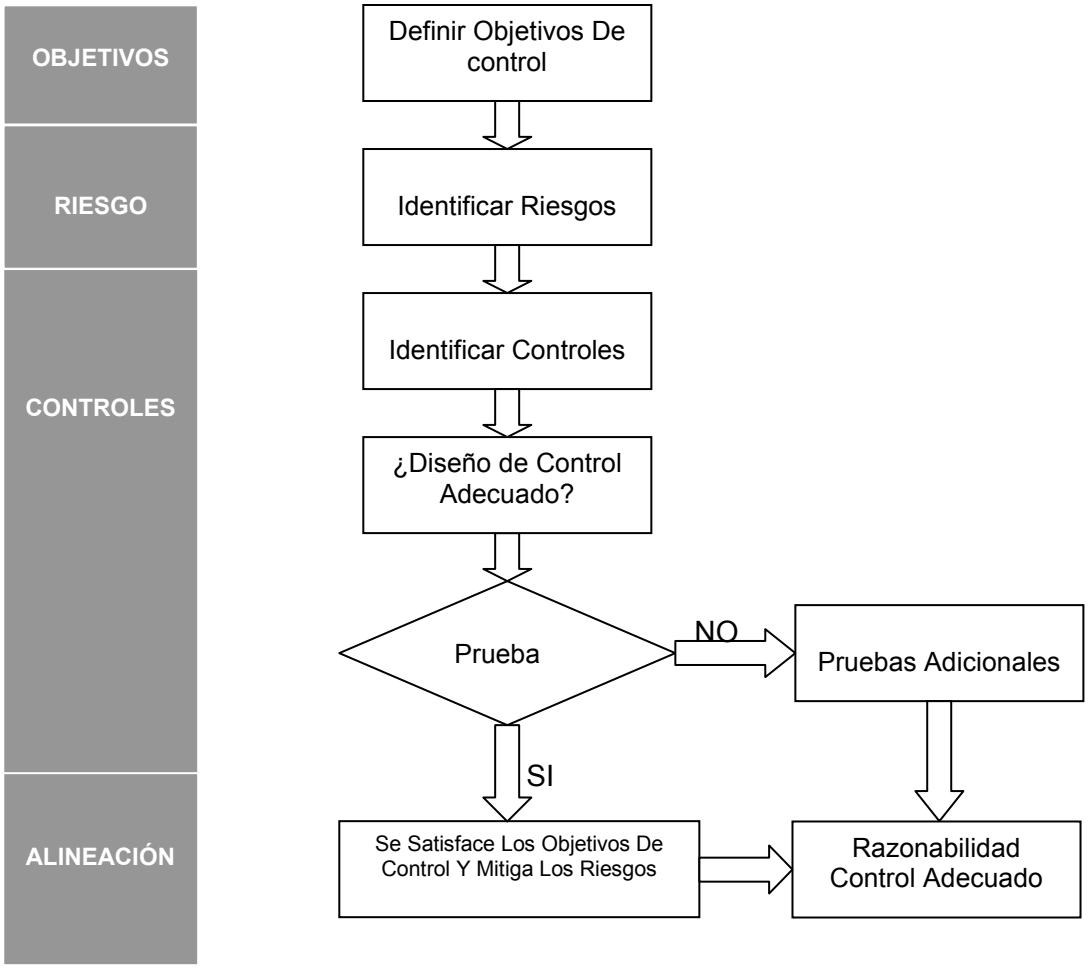


Figura 3.12 Metodología ORCA [PWC, 2006]

En resumen, la metodología ORCA propone definir en primera instancia, los objetivos de control, después identificar los riesgos y los controles y por último, evaluar sí la actividades de control son adecuadas al cumplir con el objetivo definido en un pricipio.

La metodología propuesta en este proyecto de tesis, utiliza estos conceptos, pero a diferencia de la metodología ORCA, cuenta con una serie de pasos que explican a que se refieren estos términos y cómo es que se pueden definir, identificar y evaluar estos mismos.

A continuación, se muestra nuevamente la imagen de la metodología ORCA pero ahora, contrastandola con las fases de la metodología propuesta en este trabajo escrito:

Comparativo con la metodología propuesta

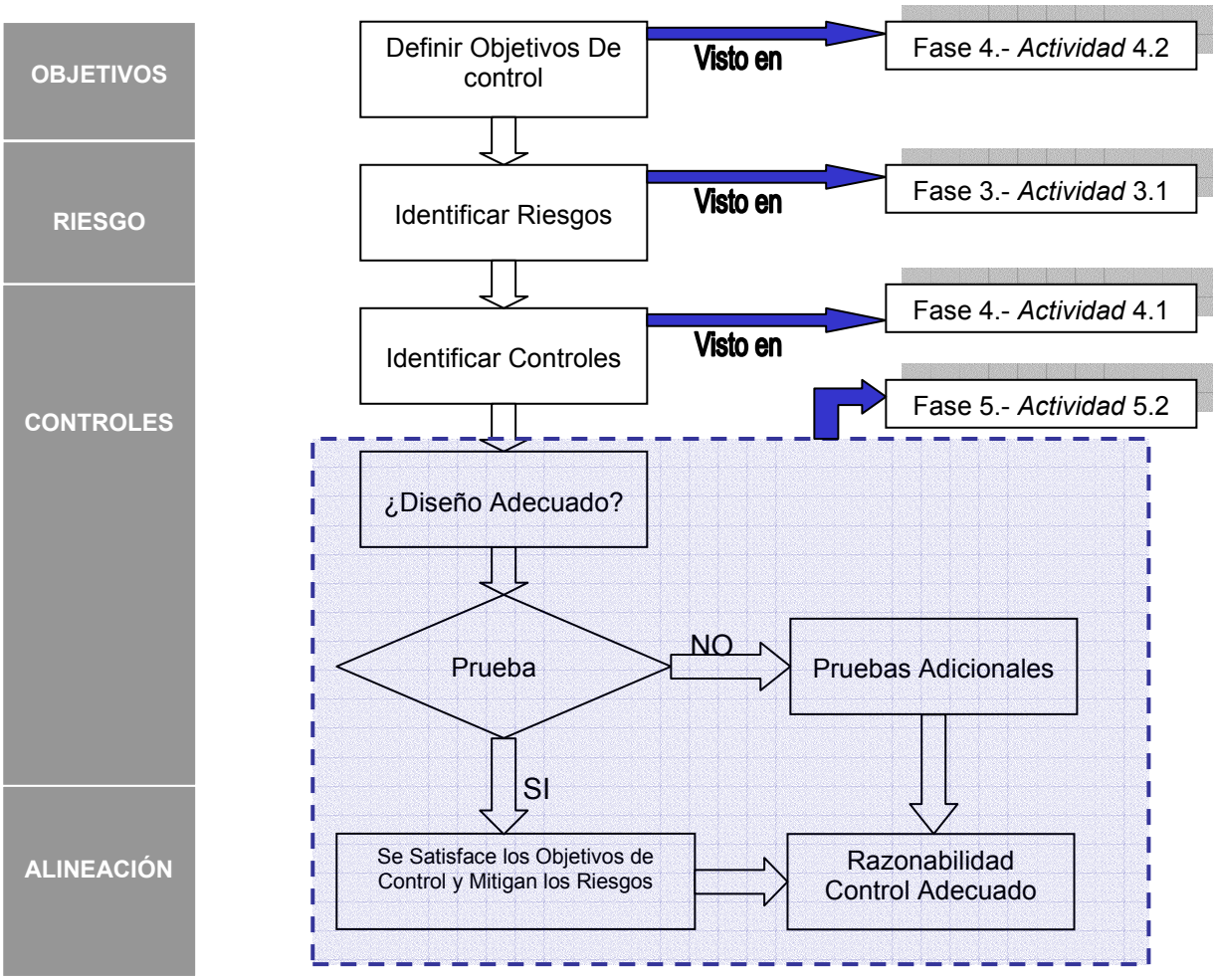


Figura 3.13 Comparativo de la metodología ORCA y la metodología propuesta en este proyecto.

Continuando con el desarrollo de esta fase, la sección sombreada de esta imagen, es la que se refiere a la parte de la evaluación y monitoreo de las actividades de control, en este apartado lo primero que se debe ver es el diseño de éstas.

Para determinar sí el diseño de las actividades de control es el adecuado, hay que contestar las siguientes preguntas:

- ☑ ¿Cómo se supone que deben operar las actividades de control?
- ☑ ¿Están realmente en operación?
- ☑ ¿Son suficientes para satisfacer los objetivos de control?
- ☑ ¿Se revisa el 100% de la transacción en la que opera la actividad de control?
- ☑ ¿O se toma una muestra?
- ☑ ¿En este último caso, la muestra es representativa?

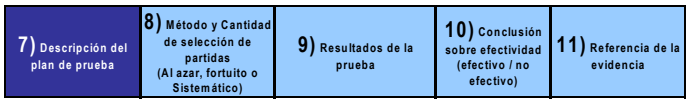
El objetivo en esta etapa es **determinar sí las actividades de control operan de manera efectiva para prevenir errores.** Consiste en verificar que las actividades de control funcionan y han funcionado durante todo el período bajo análisis de acuerdo a su diseño. Esto puede realizarse a través de el uso de un Plan de Prueba, para ello hay que determinar el tamaño de la muestra de acuerdo a la frecuencia de la ejecución de la actividad de control, además de la técnica que se va a utilizar para hacer esta prueba y solicitar evidencia que permita comprobar la ejecución de la actividad, de tal forma, que se pueda obtener un resultado que permita dar una valoración acerca de la misma.

Todos estos elementos que se han mencionado y que en seguida se muestran, forman la segunda parte de la matriz de objetivos de control, actividades de control y riesgos que serán comentados particularmente más adelante:

Tabla. 3.13 Cabecera de la matriz de objetivos de control, actividades de control y riesgos (Final). [Fuente Propia]

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia

Ahora, se comienza con la descripción de la columna 7 de esta segunda parte:



7) PLAN DE PRUEBA:

Trata de la descripción del procedimiento que se va ejecutar para **revisar que la actividad de control se este efectuando correctamente**, este debe incluir la técnica que se usó. Se propone el empleo de las siguientes técnicas:

- ***Indagación***

Por ejemplo: Entrevistar al administrador de una aplicación como SAP para consultarlo sobre cómo se controla y registran los usuarios de la aplicación. Indagando en detalle sobre la información utilizada para efectuar el control, la oportunidad, periodicidad y acciones que se toman sobre el alta, baja y cambio de usuarios.

¿Luego confirmar nuestra impresión relatando la actividad de control realizado al administrador de la aplicación y re - preguntando para identificar posibles inconsistencias.

¿Resulta suficiente este método de prueba? No.

¿Cual es su principal limitación? Si el funcionario que indagamos es lo suficientemente hábil, nos puede contar una bonita historia que podría resultar ser incorrecta.

- ***Observación.***

Ejemplo: Presenciar las actividades de control de seguridad física del centro de cómputo.

¿Resulta suficiente este método de prueba? ¿Existe otra alternativa para probarlo? En algunos casos sólo existirá la alternativa de observar un procedimiento de la actividad de control para efectuar la prueba.

¿Cuales son sus principales desventajas? Resulta ineficiente porque es necesaria nuestra presencia en diferentes oportunidades para que la muestra seleccionada sea representativa. Nuestra presencia condiciona el comportamiento de los funcionarios.

- ***Inspección de documentos y registros.***

Ejemplo: Solicitar la bitácora de respaldo de las bases de datos y verificar:

- ☑ Que se encentran firmados por el funcionario a cargo de la actividades de control
- ☑ Que existe evidencia de que el reporte fue analizado (anotaciones)
- ☑ Que existe evidencia del seguimiento de las excepciones (por ejemplo, correos electrónicos, referencia a llamadas telefónicas, impresiones de pantalla sobre la resolución de la excepción, etc.)
- ☑ Que existe evidencia de que las excepciones hayan sido resueltas

- ***Reproducción.***

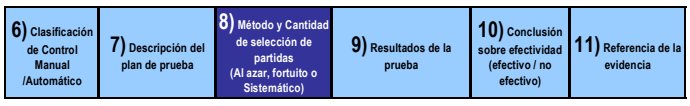
Por ejemplo: Reproducir los registros de los usuarios para confirmar quienes tienen acceso a cierta aplicación.

¿Cual es la gran ventaja de este método? Da el mayor nivel de confort.

¿Cual es su principal desventaja? Requiere demasiado tiempo para su ejecución.

El método a utilizar depende del nivel de confort que se deseé alcanzar, esto depende de la importancia del objetivo de control que soporta y también del tiempo que se quiera invertir. Es muy común que se utilice una combinación de los diferentes métodos para probar adecuadamente una actividad de control.

8) MÉTODO Y CANTIDAD DE SELECCIÓN DE PARTIDA



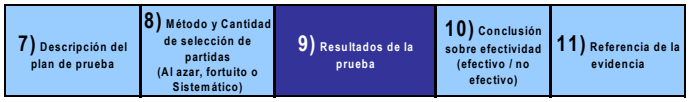
El método se refiere a la forma en que se realizó la selección de partida ó muestra (ejemplo: azar ó sistemática) para verificar si se a efectuado la actividad de control en un periodo de días, semanas ó meses, según se requiera.

En seguida, se muestra una tabla para el método sistemático que puede usarse para determinar el tamaño de la muestra de acuerdo a la frecuencia de la actividad de control.

Tabla 3.14 Selección del tamaño de muestra de acuerdo a la frecuencia de la actividad de control [PWC, 2006].

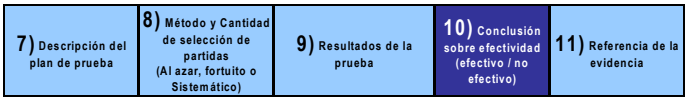
FRECUENCIA DE LA ACTIVIDAD DE CONTROL	TAMAÑO DE MUESTRA
Anual	1
Trimestral	2
Mensual	2 a 5
Semanal	5, 10, 15
Diario	20, 30, 40
Varias veces al día	25, 30, 45, 60

9) RESULTADOS DE LA PRUEBA



En esta parte se tiene que describir los resultados obtenidos de la experiencia que se tuvo con el método de prueba utilizado.

10) CONCLUSIÓN SOBRE LA EFECTIVIDAD



En esta columna es donde se coloca **el grado de cumplimiento de la actividad de control**, esta graduación puede estar compuesta por varios niveles, puede ir desde el más conciso valorando sí es efectiva la actividad de control o no es efectiva.

Sí se requiere una escala más específica para evaluar el cumplimiento de la actividad de control se puede utilizar los modelos de madurez que ofrece en cada uno de los objetivos de control el marco referencial COBIT. (Ver Anexo J, acerca del Marco Referencial COBIT para saber más del tema).

Este marco ofrece 6 niveles de madurez que van desde el nivel 0 No existente hasta el 5 Optimizado y que a continuación serán abordados:

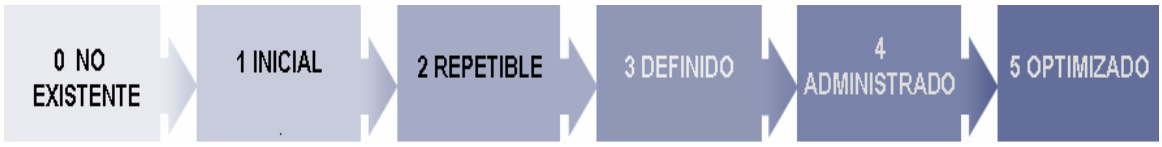


Figura 3.14 Modelo de Madurez [COBIT, 2005].

0 No existente. Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.

1 Inicial. Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar en su lugar existen enfoques *ad hoc* que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la Dirección es desorganizado.

2 Repetible. Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido. Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

4 Administrado. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada o fragmentada.

5 Optimizado. Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.

El modelo de madurez también es utilizado como una técnica de auto – evaluación del área de TI, al conseguir el promedio de todas las escalas de medición de los procesos, se permite responder los siguientes cuestionamientos:

1. El desempeño real de la empresa - ¿Dónde se encuentra la empresa hoy?
2. El estatus actual de la industria - La comparación.
3. El objetivo de mejora de la empresa - ¿Dónde desea estar la empresa?

Figura. 3.15 Representación gráfica del modelo de madurez. [COBIT, 2005]

Además de los elementos anteriores, para que se considere una actividad de control efectiva y segura, tendría que cumplir con las siguientes consideraciones:

- ☑ ***Actualizada*** (por que puede cambiar el proceso y volverse obsoleto el control),
- ☑ ***Autorizada*** (por el responsable de TI y el dueño de la información) y
- ☑ ***Difundida*** (para que todos los involucrados los conozcan y los cumplan).

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia

11) REFERENCIA DE LA EVIDENCIA

Aquí se coloca el nombre y **las pruebas obtenidas** como documentación, correos electrónicos, impresiones de pantalla, etc., que permiten soportar el resultado de la prueba.

Luego entonces, la segunda parte de la matriz de objetivos de control, actividades de control y riesgos y continuando con el ejemplo de la primera parte, se conformará de la siguiente manera:

Tabla 3.15 Continuación de la matriz de Objetivos de control, Actividades de control y Riesgos. [Fuente Propia]

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia

Solicitar el procedimiento para el acceso a los medios de respaldo y evidencia de su realización verificando que estuviese autorizado por la gerencia.	Sistemático / 1	Se encontró evidencia y documentación de que el procedimiento para el acceso a los medios de respaldo se lleva acabo.	Efectivo Nivel de Madurez **5**	1. Proceso de acceso a los respaldos.doc 2.Correos electrónicos de la solicitud y autorización al acceso de los medios de almacenamiento.

Ahora que ya se conocen los elementos que integran por completo la matriz, es preciso comentar que para manejar un conjunto de objetivos de control de forma sencilla es necesario organizarlos; el marco referencial COBIT plantea agruparlos en 4 conjuntos ó dominios: Planear y Organizar (PO), Adquirir e implementar (AI), Entregar y Dar Soporte (DS) y Monitorear y Evaluar (ME).

A continuación, se presenta ambas partes de la matriz, incluyendo una primera columna donde se coloca dominio que pertenece cada objetivo y la referencia de éste dentro del marco referencial (DS4).

Tabla 3.16 Matriz completa de Objetivos de control, Actividades de control y Riesgos. [Fuente Propia]

DOMINIO	1) Objetivo de control	2) Descripción del Riesgo	3) Actividades de Control	4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Evidencia, Supervisión y autorización)	5) Periodicidad de la actividad de control	6) Clasificación de la actividad de control Manual /Automático
ENTREGAR Y DAR SOPORTE	Brindar un servicio continuo de TI requiere de la administración de un sitio de almacenamiento externo a las instalaciones, donde se guarden los respaldos de información necesarios para la recuperación de TI y para los planes de continuidad de la empresa. La Gerencia de TI debe asegurarse de que este sitio cuente con las políticas y procedimientos indispensables para recuperar, mantener y conservar la información empresarial. (Referencia COBIT-DS4)	No contar con respaldos de información que pueda ser requerida en cualquier momento, puede provocar perder la disponibilidad de la información. (Nivel medio **3**)	Tener un proceso para el acceso a los medios de respaldo (cintas, CD y medios removibles).	"La empresa X" no cuenta con un formato manual o automatizado donde el dueño de la información y la Gerencia de TI supervisen y autoricen el uso e instalación de la información respalda en cintas, CD y medios removibles.	Anual	Manual

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia
Solicitar el procedimiento para el acceso a los medios de respaldo y evidencia de su realización verificando que estuviese autorizado por la gerencia.	Sistemático / 1	Se encontró evidencia y documentación de que el procedimiento para el acceso a los medios de respaldo se lleva acabo.	Efectivo Nivel de Madurez **5**	1. Proceso de acceso a los respaldos.doc 2.Correos electrónicos de la solicitud y autorización al acceso de los medios de almacenamiento.

Los resultados que muestra esta matriz pertenecen al momento en que ya se cuenta con el proceso de acceso a medios de almacenamiento, por lo tanto, la conclusión muestra es un proceso efectivo, por que ya cumple con el objetivo fijado y se le ha asignado un nivel de madurez 5 (Optimizado) de acuerdo al marco de referencia COBIT.

Como punto final de esta actividad se ha agregado el siguiente cuadro guía que resumen y explica el contenido de cada una de las columnas:

Tabla 3.17 Cuadro guía para llenar la matriz de Objetivos de control, Actividades de control y Riesgos. [Fuente Propia]

<table>
<tr><th>Columna</th><th>Explicación</th></tr>
<tr><td>Nombre del Dominio (opcional)</td><td>Nombre del dominio de COBIT del cual fue obtenido el objetivo de control.</td></tr>
<tr><td>1) Objetivo de Control</td><td>Es una declaración del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI. Responde a la pregunta ¿Qué propósito se quiere cumplir.</td></tr>
<tr><td>2) Descripción del Riesgo</td><td>Se describe el acontecimiento pueda afectar ó impactar el alcance de los objetivos. Reponde a la pregunta ¿Qué propósito se quiere cumplir?</td></tr>
<tr><td>3) Actividad de control</td><td>Se trata de son las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados. Responde a la Acción que se debe tomar para cumplir ese propósito.</td></tr>
<tr><td>4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Supervisión y autorización)</td><td>Descripción a detalle de la actividad que la empresa realiza para cubrir el objetivo de control. Puede responder con las preguntas siguientes: ¿Qué actividad de control se está aplicando para este objetivo?, ¿Cómo se lleva acabo esta actividad?, ¿Quién realiza esta actividad?, ¿Dónde se realiza esta actividad?, ¿Cuándo se realiza la actividad de control?, ¿Qué evidencia produce esta actividad de control?, ¿Quién supervisa esta actividad? ¿Quién autoriza la realización de la actividad de control?, etc.,</td></tr>
<tr><td>5) Periodicidad del control (sólo para controles manuales)</td><td>Frecuencia de la ejecución de la actividad de control, Se refiera a la cantidad de veces con la qué se aplica esta actividad de control, puede ser varias veces al día, semanal, quincenal, mensual, anual, etc.</td></tr>
<tr><td>6) Clasificación de la Actividad de control (automático/manual)</td><td>Documentar el tipo de control:
-Controles automáticos:
Son aquellos soportados por los sistemas de aplicación.
-Controles manuales:
Son aquellos llevados a cabo por los funcionarios de la organización.</td></tr>
<tr><td>7) Descripción del plan de prueba</td><td>Trata de la descripción del procedimiento que se va ejecutar para revisar que la actividad de control se este efectuando correctamente, este debe incluir la técnica que se usó. Se propone el empleo de las siguientes técnicas:
▪ Indagación, Observación, Inspección de documentos y registros y Reproducción.</td></tr>
<tr><td>8) Metodo y Cantidad de selección de partidas (Al azar, fortuito o Sistematico)</td><td>Se refiere a la forma en que se realizó la selección de partida ó muestra para verificar si se a efectuado la actividad de control en un periodo de días, semanas ó meses, según se requiera.

El método de selección:
Casual o fortuito: Seleccionados manualmente sin sesgo consciente
Al azar: Utilizando tablas o software para generar números al azar
Sistemático: Seleccionando manualmente considerando un intervalo fijo entre los individuos de la población a ser incluidos en la muestra.
<table>
<tr><th>Frecuencia de la Actividad de Control</th><th>Tamaño de Muestra</th></tr>
<tr><td>Anual</td><td>1</td></tr>
<tr><td>Trimestral</td><td>4</td></tr>
<tr><td>Mensual</td><td>12</td></tr>
<tr><td>Semanal</td><td>52</td></tr>
<tr><td>Diario</td><td>250</td></tr>
<tr><td>Varias veces al día</td><td>Más de 250</td></tr>
</table>
</td></tr>
<tr><td>9) Resultados de la prueba</td><td>En esta parte se tiene que describir los resultados obtenidos de la experiencia que se tuvo con el método de prueba utilizado</td></tr>
<tr><td>10) Conclusión sobre efectividad (efectivo / no efectivo)</td><td>En esta columna es donde se coloca el grado de cumplimiento de la actividad de control, esta graduación puede estar compuesta por varios niveles, puede ir desde el más conciso valorando si es efectiva la actividad de control o no es efectiva. Si se requiere una escala más específica para evaluar el cumplimiento de la actividad de control se puede utilizar los modelos de madurez que ofrece en cada uno de los objetivos de control el marco referencial COBIT.</td></tr>
<tr><td>11) Referencia de evidencia</td><td>Aquí se coloca el nombre y las pruebas obtenidas como documentación, correos electrónicos, impresiones de pantalla, etc., que permiten soportar el resultado de la prueba.</td></tr>
</table>

Algunas cuestiones que no se deben olvidar son:

- ☑ Para la generar un ambiente de seguridad en TI, se debe contar con un **responsable de la seguridad** de la información y de las actividades de control implementadas, para asegurar de su cumplimiento.

- ☑ El **apoyo de la Dirección** debe ser absoluto para que se pueda contar con los recursos necesarios en la generación de un sistema o medio ambiente de seguridad de la información.

- ☑ **Conocer** las cuestiones generales de **la empresa e involucrarse en el desarrollo de los procedimientos** de TI **para poder identificar y producir las actividades de controles** que ayuden a mitigar los **riesgos** que padece.

- ☑ La empresa debe **mantener la documentación de todas las actividades de control** (las aceptadas, las derivadas a terceros y las mitigadas) y evidencia de pruebas. El desarrollo y mantenimiento de documentación y material de prueba son un elemento clave de actividades de controles efectivas.

- ☑ La **evaluación** de las actividades de control **debe basarse en** los procedimientos que garanticen **el funcionamiento en el diseño y la efectividad operacional de cada actividad de control.**

- ☑ El área de TI debe de **contar con una segregación de funciones adecuada**. Ninguna persona o departamento debe manejar todos los aspectos o fases de una misma transacción desde el comienzo hasta el final. Toda transacción debe ser realizada en cuatro etapas: aprobación, autorización, ejecución y registro, cuya actividad de control debe correr a cargo de empleados o departamentos relativamente independientes. Esta segregación de funciones se hace con la finalidad de poder detectar los errores para que ninguna persona se halle en posición de poder cometer un desfalco y ocultar su acción por medio de la falsificación de documentos, sin confabularse con otros miembros de la empresa.

Observación importante: Ya que se ha empleado la metodología por primera vez, puede ser aplicada tantas veces se desee (esto es, de manera cíclica y a partir de la segunda fase, ya que no es necesarios volver a conocer el entorno de la empresa y los requerimientos de la metodología), para seguir evaluando, monitoreando y rediseñando actividades de control y mantener un ambiente de seguridad.

En el siguiente capítulo se presentará un ejemplo de la implantación de la metodología propuesta en esta tesis.

CAPÍTULO 4.- APLICACIÓN DE LA METODOLOGÍA PROPUESTA EN UNA PYME DE COMUNICACIÓN.

4.0 INTRODUCCIÓN.

El siguiente capítulo se trata de la implantación de la metodología en un caso real. Para esta situación, se aplicarán en una empresa dedicada a las comunicaciones móviles y rastreo; a modo de ejemplo sólo serán usados dos procesos de TI, con el fin de reconocer cuál de éstos cumple con los objetivos de control y puede ser considerado como un proceso que ofrece seguridad razonable.

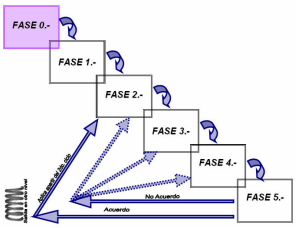
Por consiguiente y como recordatorio, cuando se tenga que hacer referencia a el nombre de la empresa solo se mencionará como:" La empresa".

4.1 APLICACIÓN DE LA METODOLOGÍA.

Dado que “La empresa” es un socio comercial (sub-empresa) de una empresa mayor internacional en comunicaciones móviles y de rastreo, es preciso, delimitar la aplicación de esta metodología que sólo se aplicará en los procesos de TI de la “La empresa”.

A continuación, se explica de acuerdo a cada fase y actividad que integran la metodología, ¿qué es lo que se debe hacer para cumplir esta actividad?, ¿qué técnicas se pueden usar?, ¿que herramientas se pueden utilizar? y ¿qué resultado se deben en esta actividad? para cada una:

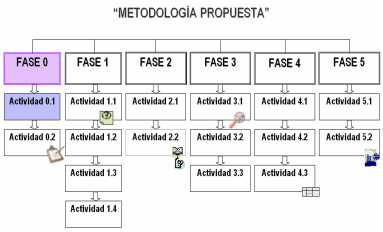
4.2 FASE 0.- DEFINICIÓN DE LOS REQUERIMIENTOS INICIO:



Objetivo general de la Fase 0:

Contar con requisitos que hay que tomar en cuenta antes de iniciar con el uso de la metodología, como son el apoyo de la Dirección y el personal adecuado.

4.2.1 Actividad 0.1 Obtener la disponibilidad y apoyo del Consejo de Administración.



¿Qué hacer?

Para iniciar con la implantación de esta metodología es necesario, que la Dirección, identifique que “La empresa” puede sufrir diversos riesgos que afecten la información contenida en las tecnologías de información de la misma.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que se pueden emplear son la persuasión y concienciación para que la Dirección reconozca que se deben aplicar contra medidas que permitan la mitigación de estos riesgos con el fin de lograr una organización más segura.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas de apoyo que se pueden emplear son el generador de presentaciones y el procesador de palabras.

RESULTADOS
¿Qué obtener?

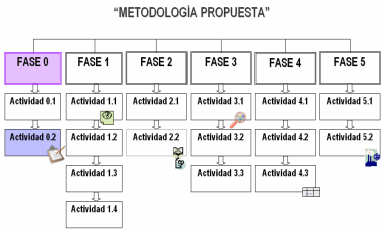
A través de presentaciones y pláticas con la Dirección, esta debe de establecer su participación y apoyo claramente, comprendiendo que al iniciar con este proyecto se va

a requerir de la asignación de recursos suficientes para la implantación de los objetivos y sus controles en la organización.

4.2.2 Actividad 0.2 Contar con el personal adecuado.

¿Qué hacer?

Realizar concienciación a la Dirección para la aprobación de conforma un equipo de trabajo dirigido por un Oficial de Seguridad Informática, quienes no deberán depender directamente de la Gerencia de TI, si no, ser parte de un área de staff, ya que no pueden formar parte del área que se evaluará.



TÉCNICAS APLICADAS
¿Cómo hacer?

La técnica que se pueden emplear es la concienciación para que la Dirección reconozca que se requiere de un equipo de trabajo que se encargue de la seguridad de la información.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar son el trabajo de persuasión y convencimiento hacia la Dirección.

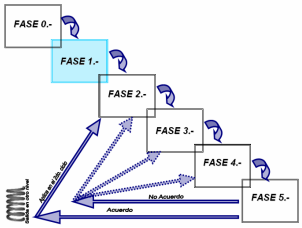
RESULTADOS
¿Qué obtener?

Obtener personal adecuado capaz de identificar, analizar y diagnosticar los procesos de TI y determinar sí se cuenta con alguna clase de control en estos procesos, así como definir nuevas maneras de controlarlos y verificar que se efectúen correctamente.

En conclusión de esta fase, lo que se pretender es persuadir a la Dirección para que reconozca que "La empresa", puede tener o ya estar pasando por diversos riesgos que podrían convertirse en oportunidades para mejorar y que para que esto suceda se requiere de personal adecuado y capaz de manejar la seguridad de la información.

Una vez concluidas las actividades de la fase 0, ahora, se presentaran las actividades de la fase:

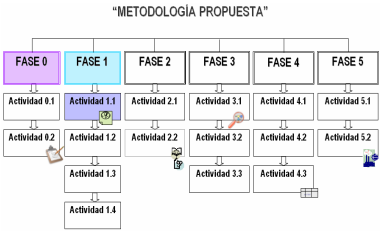
4.3 FASE 1.- CONOCER EL MEDIO AMBIENTE DE LA EMPRESA:



Objetivo general de la Fase 1:

Conocer la ubicación, visión, misión, políticas, etc., de la empresa; es decir, se identificar el medio ambiente en general y particular de esta misma.

4.3.1 Actividad 1.1 Conocer el media ambiente general de la empresa



¿Qué hacer?

Solicitar la información necesaria para identificar la visión, misión, políticas, planes, estrategias, objetivos, funciones y actividades generales de "La empresa".

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que se pueden emplear son la observación, entrevistas y mapas mentales.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

La herramienta que se puede usar es el procesador de palabras.

RESULTADOS
¿Qué obtener?

"La empresa" surge en México en 1988 como socio comercial de una corporación líder mundial que ofrece comunicaciones y localización de unidades móviles vía satélite a través del Sistema innovador. Cuenta aproximadamente con 200 empleados.

A continuación se presenta, a manera de ejemplo algunos de los productos que ofrece esta empresa:

Este producto que ofrec la empresa, es una terminal de comunicaciones integral que realiza la comunicación entre el operador y la central de despacho. También, proporciona la ubicación del vehiculo, por medio de Sistema de navegación de Posición Global (por sus siglas en inglés GPS).

Figura 4.1 Antena de comunicaciones GPS.

Este segundo producto es una unidad de teclado que permite crear mensajes escritos. Con 63 diferentes opciones de mensajes. De esta forma, se puede controlar el ciclo de carga de un embarque.

Figura 4.2 Teclado de comunicaciones.

Ahora se presenta un diagrama tipo “Mapa Mental”, en donde se muestran los básicos de la empresa:

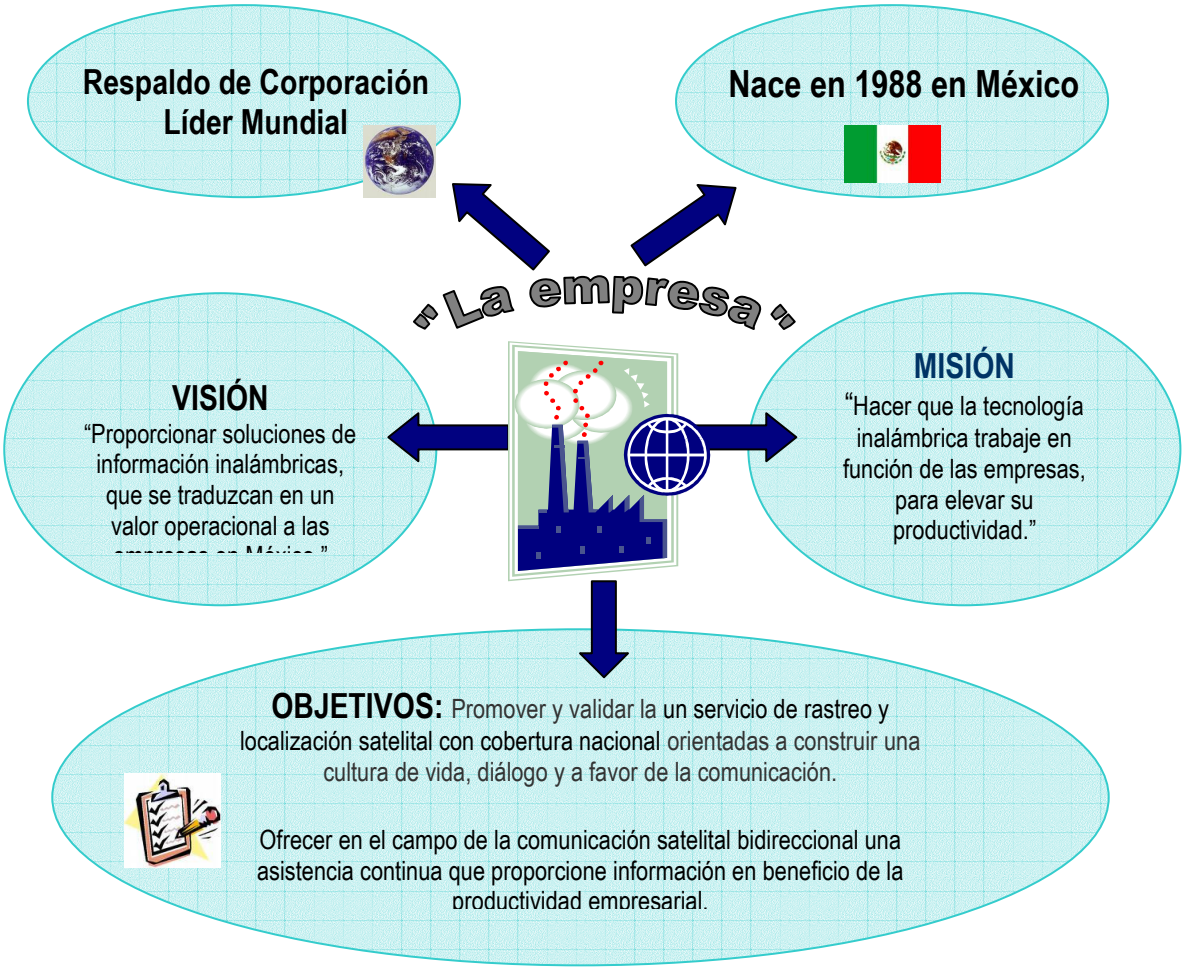


Figura 4.3 Mapa mental del entorno de “La empresa”.

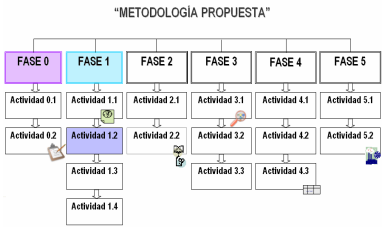
Beneficios del Sistema innovador que ofrecen:

- ☑ Servicio de rastreo y localización satelital con cobertura nacional y ubicación a nivel calle.
- ☑ Comunicación bidireccional que ofrece información en línea de su operación, para beneficio de su productividad.
- ☑ Respaldo tecnológico y financiero de una corporación líder.
- ☑ Estación terrenal única en México y regulada por Secretaría de Comunicaciones y Transporte (SCT) para seguridad de su información.
- ☑ Servicio personalizado 24 horas los 365 días del año.
- ☑ Capacidad de adaptación a las necesidades logísticas y financieras de cada cliente.

4.3.2 Actividad 1.2 *Obtener u elaborar: la estructura organizacional de la empresa y del área de tecnologías de información.*

¿Qué hacer?

Solicitar el organigrama para identificar la estructura organizacional de la empresa y del área particular.



TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que se pueden emplear son la observación y la entrevista.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

La herramienta que se puede usar es el procesador de palabras.

RESULTADOS
¿Qué obtener?

Como resultado, se presentan 4 organigramas, el primero es acerca de la división general de la empresa líder, en donde una de sus sub divisiones es la empresa abordada en este ejemplo y en donde se muestra su posición en la siguiente imagen:

Figura 4.4 Organigrama de la división general de la empresa líder para ubicar "La empresa".

En seguida, se presenta el organigrama general e interno de “la empresa” que se tomo como ejemplo. El área resaltada con línea punteada corresponde a la Gerencia de TI.

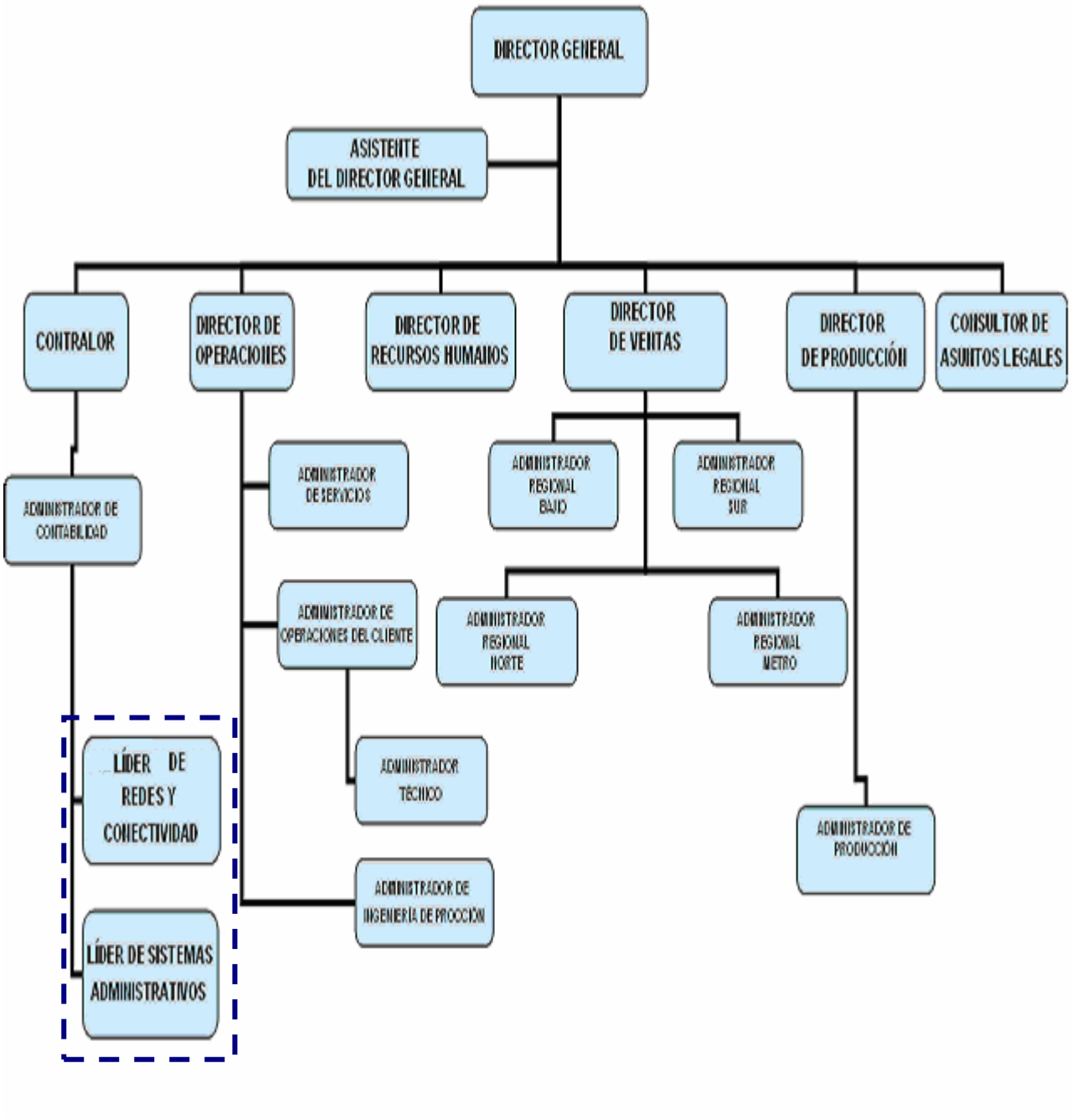


Figura 4.5 Organigrama general de “La empresa”.

Por último, se presentan los organigramas de las áreas que conforman la Gerencia de TI.

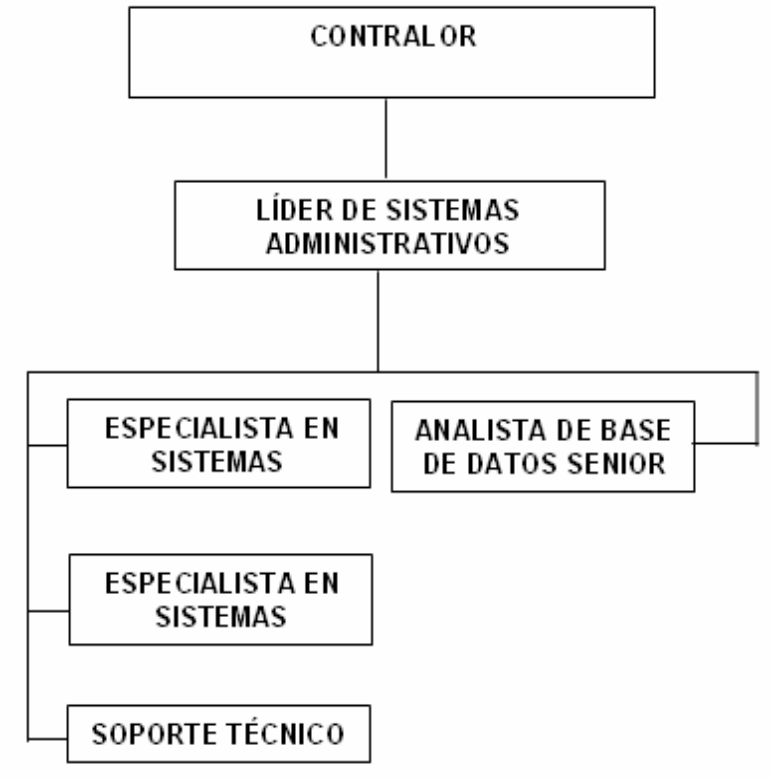
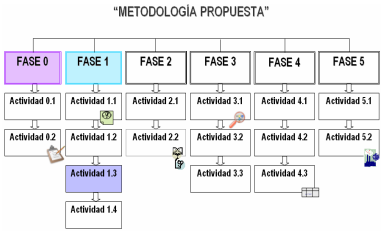


Figura 4.6 Organigrama de la Administración de Sistemas de “La empresa”.

Figura 4.7 Organigrama del área de Conectividad y Redes de “La empresa”.

4.3.3 Actividad 1.3 *Identificar y obtener: las políticas, planes, estrategias y objetivos del área de tecnologías de información.*

¿Qué hacer?



Solicitar la información necesaria para identificar y obtener los planes, estrategias, políticas, funciones, actividades y procesos del área de tecnologías de información.

Para obtener información especificar del área de TI se puede solicitar lo siguiente:
(Nota: La información remarcada en negro es la que se proporcionó y se encuentra en la parte posterior de esta actividad)

- ☑ **Políticas y procedimientos de TI, especialmente, las políticas y procedimientos de seguridad.**
- ☑ Plan estratégico de TI.
- ☑ Plan de recuperación en caso de desastres o plan de continuidad de negocios.
- ☑ **Diagrama de la infraestructura de TI, indicando los servidores, la localización y uso de los mismos.**
- ☑ **Diagrama de la red.**
- ☑ Metodología de desarrollo/implantación de sistemas.
- ☑ **Informe de control gerencial de las actividades de la Gerencia de TI (por ejemplo, indicadores clave de rendimiento, estadísticas de operación, análisis de incidencias, control de proyectos, etc.).**
- ☑ **Inventario de software aplicativo, en el cual se señale cual es el crítico para la empresa. Puede incluir:**
  - **Nombre del software y aplicativos (versión sí aplica)**
  - **Nombre de los Sistemas Operativos y versión**
  - Lenguaje y versión
  - **Base de datos y versión**
  - Tiempo de funcionamiento
  - **Planes de modificaciones en los sistemas.**
  - **Paquete, ¿Desarrollo interno o externo?**
- ☑ **Mapeo de sistemas (Diagrama de interfaces entre los diferentes sistemas aplicativos y plataformas)**
- ☑ Si han existido incidente de seguridad, solicitar reporte.
- ☑ **Procedimientos de mantenimiento/cambios a sistemas.**

TÉCNICAS APLICADAS
¿Cómo hacer?

La técnica que se pueden emplear son la observación, indagación y entrevistas.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

La herramienta que se puede usar es el procesador de palabras.

RESULTADO
¿Qué obtener?

Dando que no fue permitido usar toda la información requerida, a continuación se presenta algunos de los puntos propuestos y que están remarcados en negro en la lista pasada, empezando con:

- ☑ **Políticas y procedimientos de TI, especialmente, las políticas y procedimientos de seguridad.**

Políticas de Seguridad de Tecnología de Información.

Objetivo.

El objetivo de estas políticas es describir el uso adecuado de los servicios, aplicativos y equipos de computación y las redes dentro de las instalaciones de "La empresa". Estas reglas buscan proteger a la información, las personas y a la empresa.

Es importante hacer notar que el uso inapropiado de los recursos tecnológicos expone a la empresa a riesgos innecesarios como ataque de virus, compromiso de las redes y sistemas, problemas de índole jurídico nacionales, regionales e internacionales.

Alcance.

Estas políticas están dirigidas a los empleados, consultores, personal temporal y al personal vinculado con firmas que prestan servicios a la empresa que utilicen tecnología de información. Estas políticas aplican a los equipos propios o arrendados que tiene la empresa y a los equipos propiedad de externos que sean conectados a las redes de la empresa. La garantía del cumplimiento de esta política será responsabilidad de cada miembro de la empresa pues su contravención afecta a toda la empresa.

Políticas de seguridad.

La Gerencia de TI está conformada por dos departamentos Sistemas Administrativos, Conectividad y Redes. Estos se encargan de brindar servicio directo al usuario, por el ámbito de competencia que tiene cada uno de ellos en materia de informática, desde el equipamiento, instalación, alteración, cambio de lugar, programación, etc. Por lo que ha sido necesario emitir políticas particulares para la Red, que es el nombre oficial de un conjunto de recursos y facilidades informáticas, de la infraestructura de telecomunicaciones y servicios asociados a ellos, provistos por la Gerencia de TI. Así pues este apartado contiene una clasificación de estas políticas, y son:

Del Equipo.

De la instalación de equipo de cómputo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, impresoras y equipo accesorio), que esté o sea conectado a la Red, o aquel que en forma autónoma se tenga y que sea propiedad de la empresa debe de sujetarse a las normas y procedimientos de instalación que emite el departamento de Conectividad y Redes de la Gerencia de TI.
2. La Gerencia de TI en coordinación con la Gerencia de Contabilidad (Activo Fijo), deberá tener un registro de todos los equipos propiedad de la empresa.
3. El equipo de la empresa que sea de propósito específico y tenga una misión crítica asignada, requiere estar ubicado en un área que cumpla con los requerimientos de: seguridad física, las condiciones ambientales, la alimentación eléctrica, así como su acceso que la Gerencia de TI tiene establecido en su normatividad de este tipo.
4. Los responsables de apoyo interno del departamento de Conectividad y Redes deberán dar cabal cumplimiento con las normas de instalación, y notificaciones correspondientes de actualización, reubicación, reasignación, y todo aquello que implique movimientos en su ubicación, de adjudicación, sistema y misión.
5. La protección física de los equipos corresponde a quienes en un principio se les asigna, y corresponde notificar los movimientos en caso de que existan, al responsable de salvaguardar los registros que tiene el departamento de Conectividad y Redes.

Del mantenimiento de equipo de cómputo.

1. Al departamento de Conectividad y Redes de la Gerencia de TI, corresponde la realización del mantenimiento preventivo y correctivo de los equipos, la conservación de su instalación, la verificación de la seguridad física, y su acondicionamiento específico a que tenga lugar. Para tal fin debe emitir las normas y procedimientos respectivos.
2. En el caso de los equipos atendidos por terceros la Gerencia de TI deberá normar al respecto.
3. Corresponde al departamento de Conectividad y Redes dar a conocer las listas de los proveedores, que puedan tener acceso a los equipos y brindar los servicios de mantenimiento básico.
4. Queda estrictamente prohibido dar mantenimiento a equipo de cómputo que no es propiedad de la empresa.

De la actualización del equipo.

1. Todo el equipo de cómputo (computadoras, estaciones de trabajo, impresoras y equipo accesorio), y los de telecomunicaciones que sean propiedad de la empresa debe procurarse sea actualizado tendiendo a conservar e incrementar la calidad del servicio que presta, mediante la mejora sustantiva de su desempeño.

De la reubicación del equipo de cómputo.

1. La reubicación del equipo de cómputo se realizará satisfaciendo las normas y procedimientos que el departamento de Conectividad y Redes emita para ello.
2. El equipo de cómputo a reubicar sea de la empresa o bien externo se hará únicamente bajo la autorización por escrito del responsable contando el lugar a donde se hará la ubicación con los medios necesarios para la instalación del equipo.

Del Control de Accesos.

Del acceso a áreas críticas.

1. El acceso de personal se llevará acabo de acuerdo a las normas y procedimientos que dicta la Gerencia de TI.
2. En concordancia con la política de la empresa y debido a la naturaleza de estas áreas se llevará un registro permanente del tráfico de personal, sin excepción.
3. La Gerencia de TI deberá proveer de la infraestructura de seguridad requerida con base en los requerimientos específicos de cada área.
4. Bajo condiciones de emergencia o de situaciones de urgencia manifiesta, el acceso a las áreas de servicio crítico estará sujeto a las que especifiquen las autoridades superiores de la empresa.

Del control de acceso al equipo de cómputo.

1. Todos y cada uno de los equipos son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
2. Las áreas donde se tiene equipo de propósito general cuya misión es crítica estarán sujetas a los requerimientos que la Gerencia de TI emita.
3. Las áreas de cómputo de las oficinas de la empresa donde se encuentre equipo cuyo propósito reúna características de imprescindible y de misión crítica, deberán sujetarse también a las normas que establezca la Gerencia de TI.
4. Los accesos a las áreas críticas deberán de ser clasificados de acuerdo a las normas que dicte la Gerencia de TI de común acuerdo con el comité de seguridad informática.
5. Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la Gerencia de TI tiene la facultad de acceder a cualquier equipo de cómputo que esté conectado a la Red, por cuestiones de administración de las aplicaciones.

Del control de acceso local a la red.

1. El departamento de Conectividad y Redes de la Gerencia de TI es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
2. El departamento de Sistemas Administrativos de la Gerencia de TI es responsable de proporcionar a los usuarios el acceso a los sistemas administrativos.
3. La Gerencia de TI es la responsable de difundir el reglamento para el uso de la red y de procurar su cumplimiento.
4. Dado el carácter unipersonal del acceso a la Red, el departamento de Conectividad y Redes verificará el uso responsable, de acuerdo al Reglamento para el uso de la red.
5. El acceso lógico a equipo especializado de cómputo (servidores, ruteadores, bases de datos, etc.) conectado a la red es administrado por la Gerencia de TI.
6. Todo el equipo de cómputo que esté o sea conectado a la Red, o aquellas que en forma autónoma se tengan y que sean propiedad de la empresa, debe de sujetarse a los procedimientos de acceso que emite la Gerencia de TI.

De control de acceso remoto.

1. La Gerencia de TI es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles a usuarios, que así lo requieran y justifiquen la necesidad del requerimiento.
2. El acceso remoto podrá ser otorgado a personas ajenas a la empresa solo cuando sea aprobado por la Gerencia de TI y la Gerencia solicitante.
3. El acceso remoto que realicen personas ajenas a la empresa deberá cumplir las normas que emite la Gerencia de TI.

4. Cualquier acceso remoto a la Red será monitoreado en todo momento siguiendo el procedimiento que así lo indique el departamento de Conectividad y Redes.

De acceso a los sistemas administrativos.

1. Tendrán acceso a los sistemas administrativos solo los usuarios que tengan una cuenta vigente en cada sistema y se restringirán a los permisos previamente otorgados.
2. La creación, modificación o baja de una cuenta se realizará por personal del departamento de Sistemas Administrativos de la Gerencia de TI, siguiendo el procedimiento señalado para cada caso.
3. El manejo de información administrativa que se considere de uso restringido deberá ser cifrada con el objeto de garantizar su integridad. La Gerencia de TI proporcionará los elementos necesarios para cifrar la información cuando así se le solicite.
4. La instalación y uso de los sistemas de información se rigen por el reglamento de uso de la Red y por las normas y procedimientos establecidos por la Gerencia de TI.
5. Los servidores de bases de datos son dedicados, por lo que se restringe el acceso solo a aquellos usuarios que así lo requieran y tengan autorización por escrito de la Contraloría y/o Dirección General. El acceso será otorgado siguiendo el procedimiento que estipule la Gerencia de TI.

De utilización de los recursos de la red.

1. Los recursos disponibles a través de la Red serán de uso exclusivo para asuntos relacionados con las actividades sustantivas de la empresa.
2. La Gerencia de TI es la responsable de emitir y dar seguimiento al Reglamento para el uso de la Red.
3. Corresponde a la Gerencia de TI administrar, mantener y actualizar la infraestructura de la Red.
4. La Gerencia de TI debe propiciar el uso de las tecnologías de la información con el fin de contribuir con las directrices económicas y ecológicas de la empresa.
5. Dado el carácter confidencial que involucra el correo electrónico la Gerencia de TI emite su reglamentación.

Del Software.

De la adquisición de software.

1. Del presupuesto de los proyectos que se otorga a las diferentes áreas de la empresa una cantidad deberá ser aplicada para la adquisición de software con licencia.
2. La Gerencia de TI promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.
3. La Gerencia de TI será la única autorizada de adquirir nuevo software para el uso en un área en particular o en toda la Red, previa autorización del Grupo Líder de la empresa.
4. La Gerencia de TI deberá seguir los lineamientos que establezcan las políticas de adquisición de bienes de la empresa, así como de lineamientos específicos del corporativo de la empresa líder. Deberá estar informada sobre los convenios que tenga La empresa líder con fabricantes de software para las nuevas adquisiciones.

De la instalación de software.

1. Corresponde al departamento de Conectividad y Redes de la Gerencia de TI emitir las normas y procedimientos para la instalación y supervisión del software básico para cualquier tipo de equipo.

2. En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo, únicamente se permitirá la instalación de software con licenciamiento apropiado y de acorde a la propiedad intelectual.
3. El departamento de Conectividad y Redes será el responsable de brindar asesoría y supervisión para la instalación de software informático de uso común o más generalizado, así como para el software de telecomunicaciones.
4. El departamento de Sistemas Administrativos será el responsable de brindar asesoría y supervisión para la instalación de software informático relativo a aplicaciones administrativas (Solomon, NOM2001, etc.).
5. La instalación de software que desde el punto de vista de la Gerencia de TI pudiera poner en riesgo los recursos de la empresa no está permitida.
6. Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, y otros que se apliquen).
7. La protección lógica de los sistemas corresponde a quienes en un principio se les asigna y les compete notificar cualquier movimiento al departamento de Conectividad y Redes de la Gerencia de TI
8. Todo software instalado deberá ser usado exclusivamente para asuntos relacionados con las actividades de la empresa.

De la actualización de software.

1. La adquisición y actualización de software para equipo especializado de cómputo y de telecomunicaciones se llevará a cabo de acuerdo a la calendarización que anualmente sea propuesta por la Gerencia de TI.
2. Corresponde a la Gerencia de TI autorizar cualquier adquisición y actualización del software.
3. Las actualizaciones del software de uso común o más generalizado se llevarán a cabo de acuerdo al plan de actualización desarrollado por la Gerencia de TI.
4. El departamento de Conectividad y Redes de la Gerencia de TI administrará los diferentes tipos de licencias de software y vigilará su vigencia en concordancia con la política informática.

De la auditoria de software instalado.

1. El departamento de Conectividad y Redes es el responsable de realizar revisiones periódicas para asegurar que sólo programación con licencia esté instalada en las computadoras de la empresa.
2. La Gerencia de TI propiciará la conformación de un grupo especializado en auditoría de sistemas de cómputo y sistemas de información.
3. Corresponderá al grupo especializado dictar las normas, procedimientos y calendarios de auditoría.

Del software propiedad de la empresa.

1. Cualquier software adquirido por la empresa sea por compra, donación o cesión es propiedad de la empresa y mantendrá los derechos que la ley de propiedad intelectual le confiera.
2. El departamento de Conectividad y Redes en coordinación con la Gerencia de Contabilidad (Activos Fijos) deberá tener un registro de todo el software propiedad de la empresa.
3. Todos los sistemas informáticos (programas, bases de datos, interfaces, etc.) desarrollados con o a través de los recursos de la empresa se mantendrán como propiedad de la empresa respetando la propiedad intelectual del mismo.

4. Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la empresa que debe preservarse.
5. Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la empresa deben estar resguardados.
6. Corresponderá al Departamento de Conectividad y Redes de la Gerencia de TI promover y difundir los mecanismos de respaldo y salvaguarda de los datos.

Generales.

1. Debido al carácter confidencial de la información, todo el personal de la empresa deberá de conducirse de acuerdo a los códigos de ética profesional y normas y procedimientos establecidos.

2. Cualquier violación a las políticas y normas de seguridad deberá ser reportada de acuerdo al procedimiento de reporte de incidentes para cada caso, según aplique.

Sanciones.

1. Las sanciones pueden ser desde una llamada de atención o informar al usuario hasta la rescisión de contrato dependiendo de la gravedad de la falta y de la malicia o perversidad que ésta manifiesta.
2. Corresponderá al Grupo Líder hacer las propuestas finales sobre las sanciones a quienes violen las disposiciones en materia de informática de la empresa.
3. Todas las acciones en las que se comprometa la seguridad de la Red y que no estén previstas en esta política, deberán ser revisadas por la Dirección General y la Gerencia de TI para dictar una resolución sujetándose al estado de derecho.

Vigencia.

La presente política entrará en vigencia a partir de la fecha de publicación. Cualquier excepción a esta política o procedimiento debe ser aprobada por el Gerente de Sistemas y el Director General.

Con este plan se puede determinar que la empresa cuenta con políticas que se aplican en las tecnologías de información y describen el uso adecuado de los servicios, aplicativos, equipos de computación y las redes dentro de las instalaciones. Los temas que abarca son:

- Objetivo del plan,
- Alcance del plan,
- Políticas de seguridad,
- Temas del equipo de cómputo (Instalación, Mantenimiento, Actualización y Reubicación),
- Temas de control de acceso (a Áreas criticas, al Equipo de cómputo, a la Red local, Acceso remoto),
- Temas de software (Adquisición, Instalación, Actualización, Auditoria y Propiedad),
- Generales,
- Sanciones,
- Y Vigencia

En base al anterior plan de Políticas de Seguridad de las Tecnologías de Información, surgen los siguientes procedimientos a generar por “La empresa”:

PROCESOS A GENERAR A PARTIR DE LA POLITICIA DE SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Tabla 4.1 Cuadro de procesos que debe generar la Gerencia de TI, a partir de la política de seguridad informática.

DESCRIPCION	RESPONSABLE
Proceso de instalación de equipo Hardware.	Departamento de Conectividad y Redes
Proceso de mantenimiento de Hardware. Debe incluir la lista de proveedores que realizan el mantenimiento ya sea correctivo o preventivo.	Departamento de Conectividad y Redes
Proceso para la reubicación de Hardware.	Departamento de Conectividad y Redes
Proceso de acceso a áreas críticas del sitio de cómputo.	Departamento de Conectividad y Redes
Proceso del registro permanente de acceso al sitio de cómputo.	Departamento de Conectividad y Redes
Creación de un comité de seguridad en informática.	Departamento de Conectividad y Redes
Reglamento del uso de la Red.	Departamento de Conectividad y Redes
Proceso de acceso a la Red.	Departamento de Conectividad y Redes
Proceso y reglamente de acceso remoto a la Red	Departamento de Conectividad y Redes
Proceso de modificación de cuentas en sistemas administrativos.	Departamento de Sistemas Administrativos
Procedimiento de cifrado de información.	Departamento de Conectividad y Redes
Proceso de asignación de cuentas en Bases de datos de Sistemas administrativos.	Departamento de Sistemas Administrativos
Reglamento de uso de correo electrónico.	Departamento de Conectividad y Redes
Políticas de adquisición de bienes en Empresa.	Contraloría
Proceso de instalación de software de uso común (Windows, Office, antivirus, etc.)	Departamento de Conectividad y Redes
Calendario de actualización de Software de uso crítico (Servidores, etc.)	Departamento de Sistemas Administrativos
Plan de actualización de Software de uso común	Departamento de Sistemas Administrativos
Creación de un comité de Auditoría de sistemas quien dictará normas, procedimientos y calendarios de Auditoría.	Departamento de Sistemas Administrativos
Procesos de respaldo y salvaguarda de datos.	Departamento de Conectividad y Redes
Proceso de respaldo de Base de datos.	Departamento de Sistemas Administrativos

Como parte final de este punto, se proporcionan los factores por cuales se están retrazando la realización de los procesos propuestos en la tabla 4.1.

FACTORES QUE RETRASARON LAS ACTIVIDADES:

- Se solicitó de manera urgente la creación de la empresa Inc. esto retrasó las tareas de Mejoras al proceso de depósitos en garantía y enganches, Proceso de reclamo de seguros y la Captura de Gastos con Detalle para declaración SAT.

- Las actividades de 50 cursores en pantalla Clientes y 50 cursores en pantalla Órdenes de Venta por ser de baja prioridad fueron retrasados para darle prioridad a la liberación de Contratos Re manufacturado y el folio automático en creación de facturas desde AR

- La Corrección checkbox “Extranjero” Pantalla de Clientes, está retenido porque estamos en espera de respuesta del proveedor que entregue el código fuente de una adaptación realizada hace algún tiempo.

- La actividad “Permitir el registro de descuentos a nivel Kit” se encuentra detenida porque hace falta la validación final por parte de administración y finanzas.

Dando continuidad a los puntos propuestos, en seguida se muestra el siguiente:

☑ **EL diagrama de la infraestructura de TI, indicando los servidores, la localización y uso de los mismos.**

DIAGRAMAS DE LA INFRAESTRUCTURA DE TI Y DE LA RED.

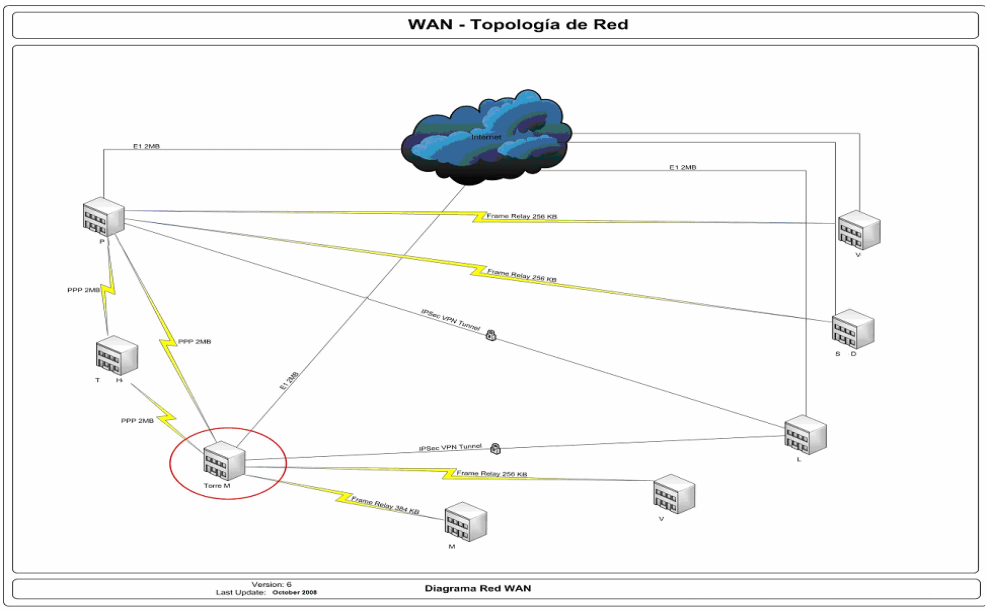


Figura 4.8 Topología de la red tipo WAN (World Area Network) de “La empresa”.

La Infraestructura de la red es de tipo WAN, dado a que es de alcance amplio; está integrada y distribuida por varias redes locales que son las que integran la red total del la empresa líder en comunicaciones a la que pertenece esta empresa que se tomó como ejemplo.

De acuerdo a la segunda parte del punto anterior, aquí se presenta la configuración de los servidores y su localización:

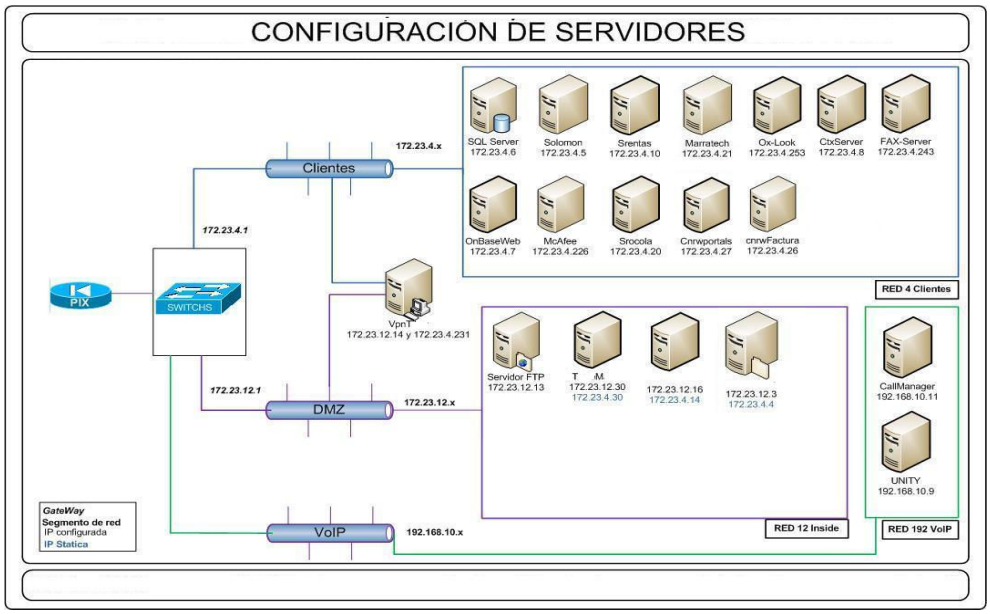


Figura 4.9 Configuración de los servidores de “La empresa”.

En esta imagen preliminar, se puede ver la distribución y dirección de cada servidor que integran la red local de la empresa, los cuales se encuentran ubicados en el Edificio Principal.

Retomando los puntos mencionados en esta actividad, en seguida, se presenta el punto que habla del:

☑ **Diagrama de la red.**

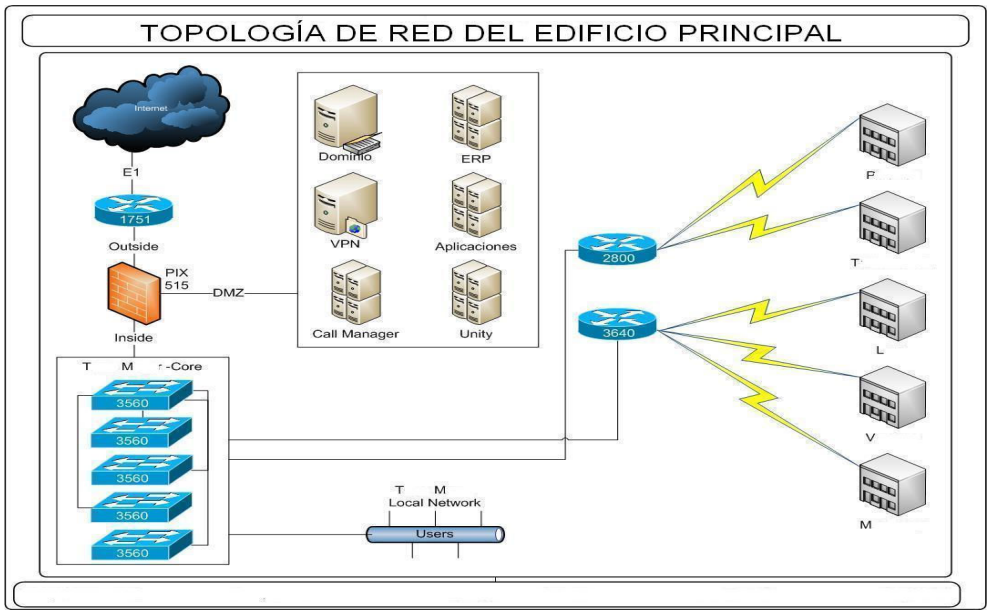


Figura 4.10 Topología de Red de “La empresa”.

El diagrama anterior de red, indica como se distribuyen los datos, así como se controlan las comunicaciones mediante un dispositivo denominado Cortafuegos (Firewall), quien es el que permite o prohíbe la entrada a la red.

Nuevamente siguiendo el listado de puntos de esta actividad, se presenta:

- ☑ **Informe de control gerencial de las actividades de la Gerencia de TI (por ejemplo, indicadores clave de rendimiento, estadísticas de operación, análisis de incidencias, control de proyectos, etc.).**

RESUMEN EJECUTIVO MENSUAL.

INFORME DE AVANCE Periodo: mes 1-mes 2-año.

Estatus por requerimiento:

Tabla 4.2 Informe de control gerencial de los requerimientos solicitados a la Gerencia de TI.

Nuevos	• Crear y parametrizar compañía en Solomon. • Parametrizar. en NOM2001. • Facturación a plazos desde Módulo de Servicios.
Concluidos	• Folio automático en creación de facturas. • Contratos Re manufacturado. • Modificaciones al reporte de Requerimientos de Efectivo. • Reporte de Balanza con información de Visto Bueno. • Mostrar cursor en pantalla SD.203.00.
En Proceso	• Conversión de Estados Financieros. • Considerar precio real y artículo en el proceso Arbor. • Habilitar comentarios Mantenimiento por terminación de contrato. • Eliminar detalles estéticos en cotización de Ventas. • Captura de gastos con detalle para declaración en Hacienda.
Retrasados	• Completar proceso de automatización InstalCampo. • Contratos T2 • 50 cursores en pantalla de Clientes. • 50 cursores en pantalla de Órdenes de Venta. • Mejoras al proceso de depósitos en garantía y enganches. • Publicación de factura a plazos. • Modificaciones al formato de Cotización de Servicios. • Emisión automática de enmiendas. • Proceso de reclamo de seguros.
Retenidos	• Corrección de Pantalla de Clientes en la parte de “Extranjero” • Permitir el registro de descuentos a nivel Kit.

Dado el informe anterior, inmediatamente se expone un gráfico, dentro del mismo informe, donde se localiza el porcentaje de los estatus en que se encuentra los requerimientos solicitados a la Gerencia de TI mencionados en la tabla anterior:

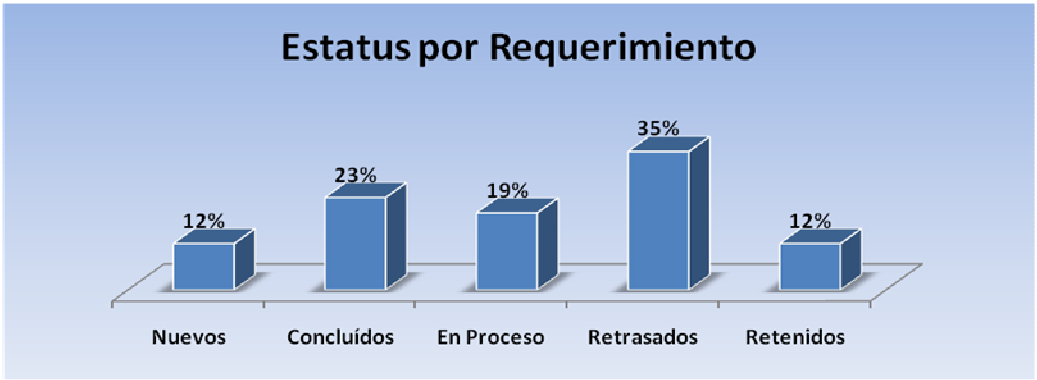


Figura 4.11 Gráfica de porcentajes de los estatus de los requerimientos de la Gerencia de TI de "La empresa".

Como parte del informe de control gerencial, también, contiene una gráfica con las solicitudes de soporte técnico por departamento / área.

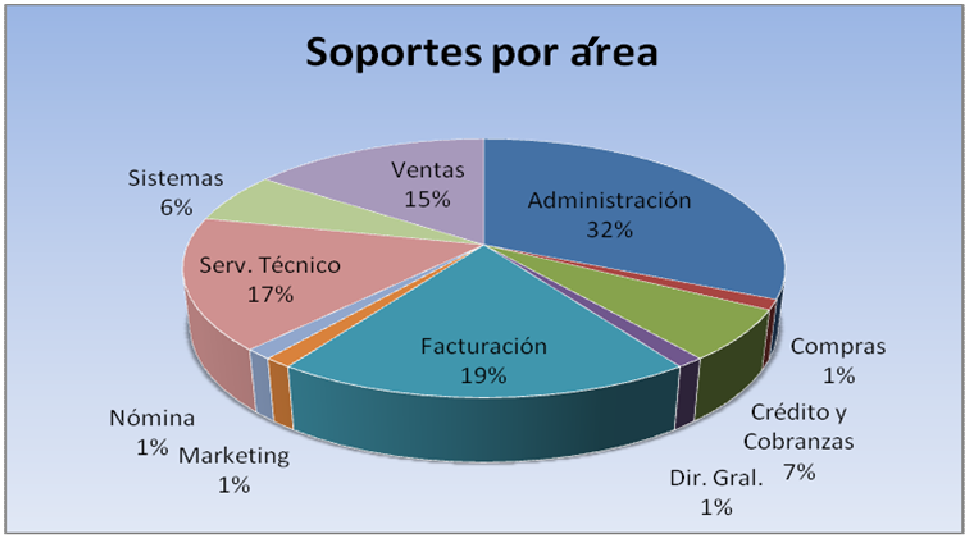


Figura 4.12 Gráfica de las solicitudes atendidas de soporte técnico por la Gerencia de TI de "La empresa"

Además, se incluye un cuadro donde se informa el estatus de las solicitudes, ofreciendo un tiempo promedio de respuesta a estas solicitudes.

Soportes	*Cantidad*
Total Recibidos	*79*
Concluidos	*67*
En Proceso	*12*
Tiempo Promedio de respuesta	*4.9 horas*

Tabla 4.3 Concentrado de las solicitudes de Soporte Técnico de "La empresa".

Como última parte de este informe gerencial, se presenta una tabla con las actividades y procesos que se realizarán a futuro

PROCESOS A DESARROLLAR PRÓXIMO PERIODO:

Tabla 4.4 Procesos a realizadas por la Gerencia de TI de “La empresa” (Inicio).

RETRASADOS				
1	**Completar proceso de automatización InstalCampo**			
	Resp.	**Etapa**	**Descripción**	**% Avance**
	M A	*Pruebas Usr.*	Documentación de pruebas con usuario	100%
	M	*Producción*	Liberación en producción	100%
2	**Contratos T2**			
	Resp.	**Etapa**	**Descripción**	**% Avance**
	C.	*Desarrollo*	Desarrollo de adaptación	60%

Tabla 4.5

3	**50 cursores en pantalla Clientes**			
4	**50 cursores en pantalla Ordenes de Venta**			
5	**Mejoras al proceso de depósitos en garantía y enganches**			
	Resp.	**Etapa**	**Descripción**	**% Avance**
	M	*Análisis*	Revisar requerimiento con usuario	100%
	C	*Desarrollo*	Desarrollo de adaptación (Externo)	25%
6	**Publicación de Factura a Plazos**			
	Resp.	**Etapa**	**Descripción**	**% Avance**
	A	*Análisis*	Revisar requerimiento con usuario	100%
	C	*Desarrollo*	Desarrollo de adaptación	100%
	A	*Pruebas Int.*	Documentación de pruebas internas	100%
	A.	*Pruebas Usr.*	Documentación de pruebas con usuario	100%
	M	*Producción*	Liberación en producción	100%
7	**Modificación al formato de Cotización de Servicios**			
	Resp.	**Etapa**	**Descripción**	**% Avance**
	A	*Análisis*	Revisar requerimiento con usuario	100%
	C	*Desarrollo*	Desarrollo de adaptación	100%
	A	*Pruebas Int.*	Documentación de pruebas internas	100%
	A	*Pruebas Usr.*	Documentación de pruebas con usuario	100%
	M	*Producción*	Liberación en producción	100%
8	**Emisión automática de enmiendas**			
9	**Proceso de reclamo de seguros de TMC**			
	Resp.	**Etapa**	**Descripción**	**% Avance**
	M	*Análisis*	Revisar requerimiento con usuario	100%

Tabla 4.5 Procesos a realizadas por la Gerencia de TI de “La empresa” (Final).

EN PROCESO			
10 Conversión de Estados Financieros			
Resp.	**Etapa**	**Descripción**	**% Avance**
M	*Pruebas Usr.*	Documentación de pruebas con usuario	100%
M	*Producción*	Liberación en producción	100%
11 Captura de Gastos con detalle para declaración SAT			
Resp.	**Etapa**	**Descripción**	**% Avance**
M	*Análisis*	Revisar requerimiento con usuario	20%
INICIO			
12 Considerar precio real y artículo en el proceso Arbor			
Resp.	**Etapa**	**Descripción**	**% Avance**
M	*Análisis*	Revisar requerimiento con usuario	100%
13 Habilitar comentarios en Mtto Antenas por terminación de contrato			
Resp.	**Etapa**	**Descripción**	**% Avance**
M	*Análisis*	Revisar requerimiento técnico.	100%
M	*Desarrollo*	Desarrollo de la adaptación	100%
M	*Pruebas Int.*	Documentación de pruebas internas	100%
M	*Pruebas Usr.*	Documentación de pruebas con usuario	100%
M	*Producción*	Liberación en producción	100%
14 Eliminar detalles estéticos en cotización de Venta			
Resp.	**Etapa**	**Descripción**	**% Avance**
A	*Análisis*	Revisar requerimiento con usuario	100%
C	*Desarrollo*	Desarrollo de adaptación	100%
A	*Pruebas Int.*	Documentación de pruebas internas	100%
A	*Pruebas Usr.*	Documentación de pruebas con usuario	100%
M	*Producción*	Liberación en producción	100%

A través de este informe y de los elementos que lo componen, se puede reconocer que la empresa mantiene seguimientos acerca de los procesos y actividades que se desarrollan en la Gerencia de TI, así como de los proyectos futuros para esta área.

Y como última punto que se verá será:

- ☑ **Inventario de software aplicativo, en el cual se señale cual es el crítico para la empresa.**

En relación al inventario, se proporcionó información de los aplicativos (programas especializados) y los sistemas operativos con los cuales se trabaja en la empresa:

CARACTERISTICAS DE LOS APLICATIVOS.

Tabla 4.6 Características generales de los aplicativos usados en “La empresa”.

Nombre Aplicativo	Infraestructura				
	Nombre del servidor	Sistema Operativo (Tipo y versión)	Funcionalidad del servidor (application, database, etc)	Base de Datos (Tipo, versión y nombre de las instancias)	Ubicación Física del Servidor
Dynamics SL-Solomon IV	HP Proliant DL 380	WIN 2003 SERVER	Aplicación-Base de Datos	SQL 2000	Edificio Principal
NOM2001	HP Proliant DL 380	WIN 2003 SERVER	Aplicación- Base de Datos	SQL 2000	Edificio Principal

Las aplicaciones que se emplean en “La empresa” son NOM2001, utilizada para realizar la Administración del Personal y la Nómina y Dynamics SL que es un software integral que contiene diversos módulos como son:

CARACTERISTICAS DE LOS APLICATIVOS.

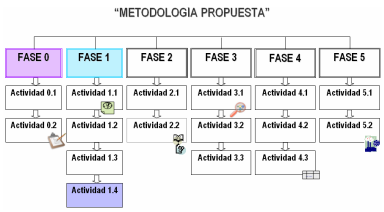
Tabla 4.7 Características detalladas de los aplicativos usados en “La empresa”.

	Nombre Aplicativo	*Dynamics SL-Solomon IV*	*NOM 2001*
Características	**Proveedor**	Microsoft	GCG
	Versión	5.5	2001
	Propósito y funcionalidad del aplicativo	ERP Integral Con los siguientes modulos: Cuentas por cobrar, Cuentas por pagar, Tesorería, Facturación, Declaraciones financieras, Generador de cuentas, Compras, Administración avanzada de embarques, Generador de Balances Financieros, Inventario, Administración de órdenes de venta, Servicios de Contratos, Herramientas de desarrollo y Adaptaciones de control.	Administracón del Recurso humano y pago de nomina
	Tipo de tecnología (Web / Cliente Servidor, Centralizado / Descentralizado, Standalone)	Cliente-Servidor	Cliente-Servidor
	Cantidad de locaciones en que se encuentra instalado	1	1
	Interfases relevantes	NOM, W FACTURA	Solomon
	Volumen de transacciones procesadas anualmente	ALTA	ALTA
	Cantidad de usuarios	45	4
	Mantenimiento dado durante el último año (mínimo 0-3, promedio 4-12, alto más de 12)	Promedio	Promedio
	Cambios relevantes en el año	Los cambios dentro de la manipulación de BD fueron los siguientes: • Comercialización del nuevo producto T2. • Pantallas nuevas para generación de reporte. • Adaptación en formato de contratos. • Creación de reportes nuevos. • Optimización de procesos manuales. • Instalación de SP4 en SQL ambiente de producción. • Actualización de sistema operativo Win2003.	• Cambios en el cálculo del ISR por las nuevas reformas fiscales.
	Problemas conocidos	Sin problemas significativos en todo 2008.	
	Proyectos para el próximo año	• Mejoras de procesos y optimización de recursos. • Nuevo proceso de facturación de servicios.	

Mediante el análisis de la información anterior, se puede concluir que “La empresa”cuenta con políticas formales que cubren los temas principales de seguridad, las cuales se encuentran disponibles para todo el personal en la Intranet de la misma.

4.3.4 Actividad 1.4 *Identificar y obtener u elaborar las funciones que se realizan en el área de tecnologías de información.*

¿Qué hacer?



Conocer las funciones para tener una idea de que personas se involucran en éstas, así como identificar que conjunto de actividades son necesarias para el desarrollo de un proceso determinado.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que se puede emplear son la observación y la entrevista. (Ver anexo L para saber más acerca de la entrevista que se aplicó).

HERRAMIENTAS DE APOYO
¿Con qué hacer?

La herramienta que se puede usar es el procesador de palabras.

RESULTADO
¿Qué obtener?

Haciendo referencia a los cargos vistos en el organigrama de la Gerencia de TI en la actividad 1.2 de esta fase; sea elaborado un cuadro con los roles y responsabilidades de algunos puestos para identificar las actividades que intervienen en cada proceso.

Tabla 4.8 Funciones de algunos cargos de "La empresa".

FUNCIONES DE LOS CARGOS			
Administrador de Datos, Red y Voz	***Líder de Sistemas Administrativos***	***Analista de Base de Datos Senior.***	***Líder de Conectividad y Redes***
• Responsable del buen funcionamiento de la red interna. • Garantizar la calidad de los recursos para clientes internos. • Revisión y análisis de servidores, red interna, enlaces de conexión con usuarios internos. • Soporte técnico a usuarios. • Actualización de equipos de cómputo (Hardware y Software). • Control de acceso a red. • Administración de servicios de voz.	• Responsable de cumplir con los programas de trabajo. • Supervisar empleados encargados de la estructura del software para el procesamiento de la información. • Ofrecer soluciones automatizadas a usuarios de varias áreas de la empresa. • Supervisar las funciones especializadas de análisis, diseño, desarrollo y modificaciones de sistemas y soporte técnico.	• Administrar la base de datos mediante la creación de procesos de auditoria. • Optimización de los recursos del servidor y respaldo. • Control en medios magnéticos de almacenamiento de datos. • Administración de privilegios y accesos. • Realizar diseño de sistemas nuevos, modificados, sistemas existentes nuevas aplicaciones, utilizando métodos, técnicas y herramientas de Software.	• Cumplir con los programas de supervisión a los encargados de la Red de área local (LAN) y la de área mundial (WAN) de la empresa. • Optimizar el funcionamiento de las redes a través de herramientas de gestión de red. • Coordinar el soporte a usuarios de la red. • Control de acceso, alta y baja de usuarios de red.

En seguida, se presenta los documentos que sirven de evidencia para determinar las características de cada cargo/puesto de la Gerencia de TI utilizados para elaborar el cuadro anterior:

EVIDENCIA OBTENIDA PARA CONOCER LAS FUNCIONES DE CADA PUESTO.

DESCRIPCIÓN DE PUESTO

Organización: Fecha: Octubre- 08

Departamento/ Área: Conectividad /Operaciones

Título de Posición: Administrador Red, Datos y Voz Aprobar:

Ocupante de Posición: Aprobar:

Superior: *Líder de conectividad*

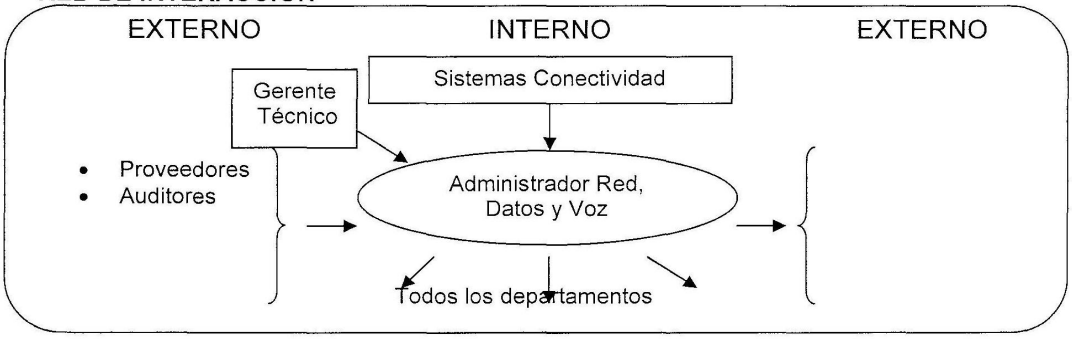
PROPÓSITO (¿Por qué existe la posición, dentro de qué límites y con qué objetivos?)

Responsable del buen funcionamiento de la red interna (Datos y Voz), garantizando la calidad de los recursos para nuestros Clientes internos, entre las diferentes actividades por mencionar son: revisión y análisis Servidores y red interna, enlaces de conexión con usuarios internos (locales y foráneos), soporte técnico a usuarios, actualización de equipos de computo (HW y SW), control de accesos a la red, administración del servicio de voz (Call Manager).Soporte a nuestros usuarios internos de las diferentes oficinas (

ALCANCE Y MARCO DE REFERENCIA

FINANCIERA	NO - FINANCIERA Organización Total: Subordinados Indirectos: 0 Subordinados directos: 0 Categoría: Gerentes:___ Especialistas:___ Otros:___

RED DE INTERACCIÓN



REQUERIMIENTOS MÍNIMOS

Educación: Ingeniería en Comunicaciones (Cursos en sistemas operativos (versiones de Windows y Linux), paquetería, Curso en redes.
Experiencia Laboral: 4 años Administrador de Voz y Datos. (conocimientos de hardware)
Conocimientos Específico: Ingles, Sistemas operativo Windows, Linux, Telefonía (Conmutadores PBX y Call Manager voz/IP), paquetería, Redes en cableado estructurado, Aplicaciones de Antivirus, Programación básica y certificaciones deseables
Conocimiento del Negocio: Empresa multinacional (conocimientos de redes, administración de voz y datos).

Figura 4.13 Descripción del puesto del Administrador de Red, Datos y Voz.

DESCRIPCIÓN DE PUESTO

Organización: Fecha: 2008

Departamento / Área: Sistemas/Finanzas

Título de Posición: ***Líder de Sistemas Administrativos*** Aprobar:

Ocupante de Posición: Aprobar:

Superior: *Contralor*

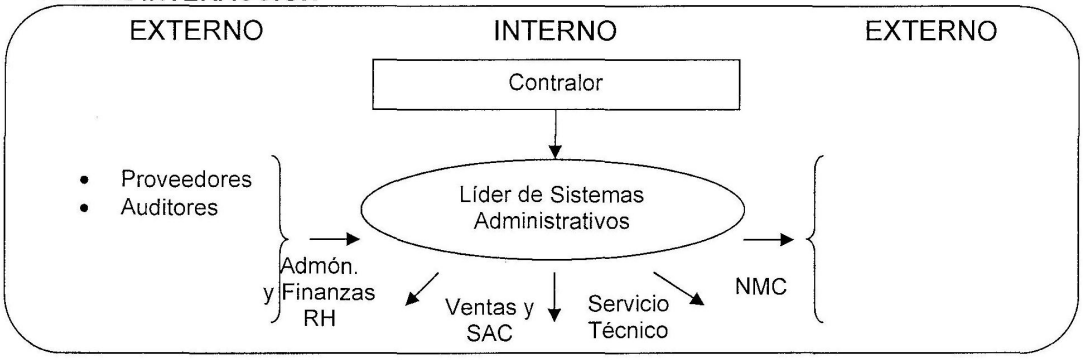
PROPÓSITO (¿Por qué existe la posición, dentro de qué límites y con qué objetivos?)

Es responsable de cumplir con los programas de trabajo, supervisando a un grupo de empleados encargados de proveer a la compañía con la infraestructura de software para el procesamiento de información, ofrecer soluciones automatizadas a usuarios de varias áreas de la empresa, supervisar las funciones especializadas de análisis, diseño y desarrollo de sistemas, soporte técnico, modificaciones a sistemas existentes. Con el objeto de darle continuidad a la operación administrativa y generar una diferencia competitiva de la empresa.

ALCANCE Y MARCO DE REFERENCIA

FINANCIERA	NO - FINANCIERA
	Organización Total: Subordinados Indirectos: 0 Subordinados directos: 4 Categoría: Gerentes:_0_ Especialistas:_4_ Otros:_0_

RED DE INTERACCIÓN



REQUERIMIENTOS MÍNIMOS

Educación: Lic. Informática Administrativa , Ingeniería en Sistemas o similar

Experiencia Laboral: 4 o 5 años.

Conocimientos Específicos: Inglés 100%, Solomon, Certificación en administración de proyectos PMPI, SOX, manejo de personal, conocimientos amplios en aplicaciones ofimáticas, lenguajes de programación, bases de datos, redes, metodologías de programación (UML).

Conocimiento del Negocio: Operación administrativa en empresa multinacional.

Figura 4.14 Descripción del puesto del Líder de Sistemas Administrativos.

DESCRIPCIÓN DE PUESTO

Organización: Fecha: 2008

Departamento/Área: Sistemas/Finanzas

Título de Posición: **Analista de Bases de Datos *SR.*** Aprobar:

Ocupante de Posición: Aprobar:

Superior: *Líder de sistemas administrativos ST600*

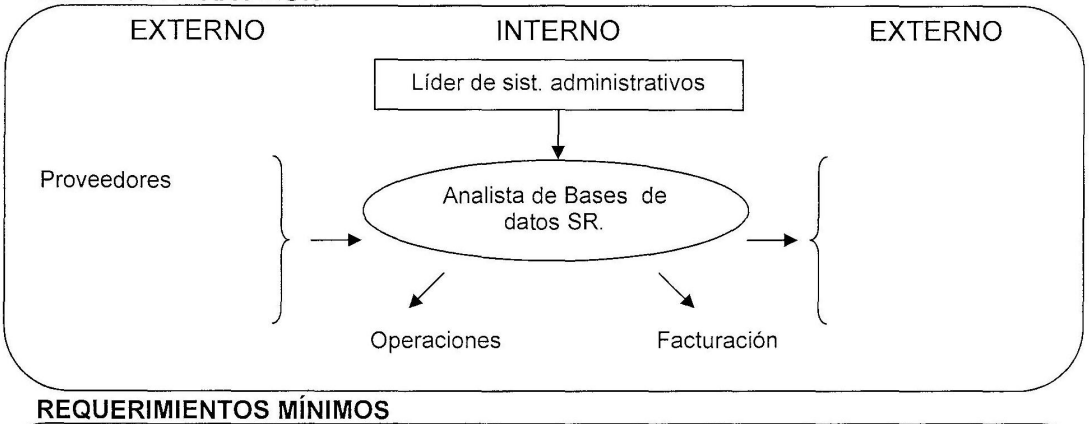
PROPÓSITO (¿Por qué existe la posición, dentro de qué límites y con qué objetivos?)

Administrar la base de datos mediante la creación de procesos de auditoria, optimización de los recursos del servidor, respaldos y control en medios magnéticos de almacenamiento de datos, administración de privilegios y accesos a fin de asegurar la operación de los sistemas. Realiza el diseño de sistemas nuevos y/o modificaciones a sistemas existentes y/o nuevas aplicaciones, utilizando métodos, técnicas y herramientas de software.

ALCANCE Y MARCO DE REFERENCIA

FINANCIERA	NO - FINANCIERA
	Organización Total: 0
	Subordinados Indirectos: 0 Subordinados directos: 0
	Categoría: Gerentes: 0 Especialistas: 0 Otros: 0

RED DE INTERACCIÓN



REQUERIMIENTOS MÍNIMOS

Educación: Ingeniería en computación, Sistemas, Cibernética ó Licenciatura en Sistemas Administrativos

Experiencia Laboral: 2 años como analista de sistemas y 2 Años en puesto similar

Conocimientos Específicos: Programación (store procedures, triggers, views, jobs, etc.) y Administración (backups, parametrización, tunning, etc.) de SQL Server, Bases de datos, Redes de cómputo, sistemas operativos (PDC, DNS, Jobs, etc.), Programación orientada a objetos, Visual .Net, C++, Crystal reports. Inglés deseable.

Conocimiento del Negocio: Trabajo bajo presión, Analítico, Pro activo, Enfoque al cliente, Actitud de Servicio, Comunicación Efectiva

Figura 4.15 Descripción del puesto del Analista de Datos Senior.

DESCRIPCIÓN DE PUESTO

Organización: Fecha: 2008

Departamento /Área : Conectividad/Operaciones

Título de Posición: ***Líder de conectividad y sistemas*** Aprobar:

Ocupante de Posición: Aprobar:

Superior: *Gerente Técnico*

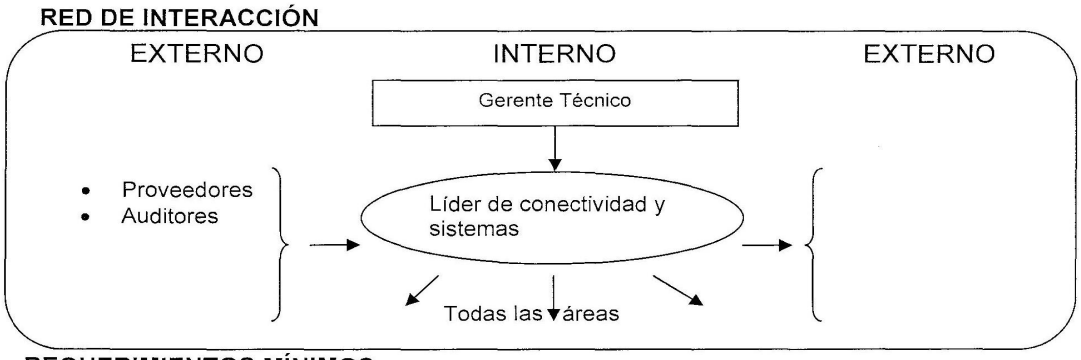
PROPÓSITO (¿Por qué existe la posición, dentro de qué límites y con qué objetivos?)

Responsable de cumplir con los programas de trabajo supervisando a un grupo de ingenieros, encargados de la eficiente administración de la red de cómputo Lan y Wan de CNR, optimizándola en su funcionamiento y a través de herramientas de gestión de red.
Coordina el soporte a los usuarios de la red, lo que incluye control de accesos, alta y baja de usuarios de la misma.

ALCANCE Y MARCO DE REFERENCIA

FINANCIERA	NO - FINANCIERA
	Organización Total:
	Subordinados Indirectos: Subordinados directos: 2
	Categoría: Gerentes:___ Especialistas:__x_ Otros:___

RED DE INTERACCIÓN



REQUERIMIENTOS MÍNIMOS

Educación: : Ingeniería en Telecomunicaciones o Tecnologías de la Información (Cursos en sistemas operativos (versiones de Windows), paquetería administrativa y de cómputo, Curso en redes CISCO.

Experiencia Laboral: Mínimo de 5 años en administración de redes Lan y Wan en puesto similar.

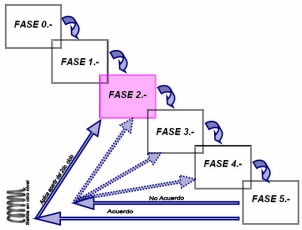
Conocimientos Específicos: Administración de Linux, Windows a nivel avanzado, seguridad informática, Diseño de redes, Bases de datos, administración de firewalls, Manejo de personal.

Conocimiento del Negocio: Empresa multinacional (conocimientos de redes, administración de voz y datos sobre IP.)

Figura 4.16 Descripción del puesto del Líder de Conectividad y Sistemas.

Como resumen de esta Fase 1, se ha conocido el medio ambiente general de "La empresa", se ha identificado la estructura organizacional general y particular de la Gerencia de TI, así como los procesos, funciones y planes de esta área en particular, con la finalidad de comprender el entorno para familiarizarse principalmente con los procesos de TI, que se analizarán en la Fase siguiente.

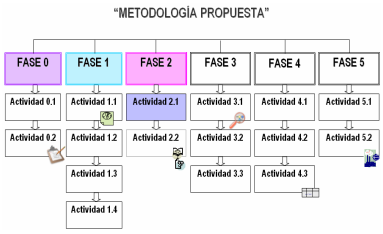
4.4 FASE 2.- IDENTIFICAR Y ANALIZAR LOS PROCESOS DEL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN:



Objetivo general de la Fase 2:

Conocer y analizar los procesos del área de TI, con la finalidad de encontrar aquellos en los que se puede estar en riesgo.

4.4.1 Actividad 2.1 *Identificar la relación de los procesos y funciones y elaboración de un Diagrama de Flujo de Datos (DFD) cada proceso de TI.*



¿Qué hacer?

Determinar e identificar en forma general los procesos de TI que intervienen en el desarrollo de cada uno de las funciones del área de TI.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que se pueden emplear son la observación, investigación, entrevista, elaboración de DFD y tabla de la relación función procesos.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar: el procesador de palabras y software de dibujo.

RESULTADO
¿Qué obtener?

Como ya se mencionó, debido a que se cuenta con información limitada de "La empresa"; el análisis sólo se llevará a cabo en dos funciones y en los procesos de TI que las integran, con el fin de reconocer cuál de estos procesos cumple con los objetivos de control.

Se realizó una entrevista al Líder de Sistemas Administrativos y el Líder de Conectividad y Redes acerca de sus funciones, políticas y procedimientos (anteriormente ya vistas en las actividades 1.3 y 1.4), diseñados para preservar la integridad de las aplicaciones, sistemas operativos y sus datos que intervienen en éstas, del cual se obtuvo el siguiente cuadro:

Tabla 4.9 Relación entre Funciones de TI y los Procesos de TI de la “Empresa X”.

RELACIÓN ENTRE FUNCIONES DE TI Y PROCESOS DE TI	
Función de TI	**Procesos de TI contenidos en la función**
Control de Alta, Modificación de privilegios y Baja de usuarios de red. Encargado: Líder de Conectividad y Redes.	☑ Proceso de Alta de usuario de red. ☑ Proceso de Modificación de privilegios de usuario de red. ☑ Proceso de Baja de usuario de red.
Control en medios magnéticos de almacenamiento de datos. Encargado: Líder de Conectividad y Redes.	☑ Proceso para el acceso a los medios de respaldo (cintas, Discos Compactos y medios removibles).

En este cuadro, se muestra la relación entre las funciones y los procesos que se deben llevar a cabo para cumplirlas; y una vez que se conoce su asociación, es preciso, iniciar con el análisis cada uno de estos procesos y para ello, a continuación se presenta los diagramas de primer nivel de cada uno:

PROCESO DE ALTA DE USUARIO DE RED.

Figura 4.17 Diagrama de Flujo de Datos básico del proceso de Alta de usuarios de red de “La empresa”.

El diagrama de flujo muestra, en general, la entrada del flujo de datos que sería una solicitud de Alta de usuario de la red, después viene el proceso en sí, que se refiere a el alta de usuario a la red y por último, la salida o resultado del proceso, que es obtener una cuenta de ingreso a la red.

PROCESO DE MODIFICACIÓN DE PRIVILEGIOS DEL USUARIO DE RED.

Figura 4.18 Diagrama de Flujo de Datos básico del proceso de la Modificación de privilegios de usuarios de red de “La empresa”.

Este segundo diagrama de flujo, muestra la entrada del flujo de datos que sería una solicitud de Modificación de privilegios de usuario de la red, después viene el proceso para llevar acabo esta acción y finalmente, la salida o resultado del proceso, que es obtener una cuenta modificada de la red.

PROCESO DE BAJA DE USURIO DE RED.

Figura 4.19 Diagrama de Flujo de Datos básico del proceso de Baja de usuarios de red de “La empresa”.

En este diagrama de flujo muestra, en general lo mismo que los anteriores, la entrada del flujo de datos que sería una solicitud de Baja de usuario de la red, después viene el proceso en sí, que se refiere a dar de baja a un usuario de la red y por último, la salida o resultado del proceso, que es obtener una cuenta eliminada de la red.

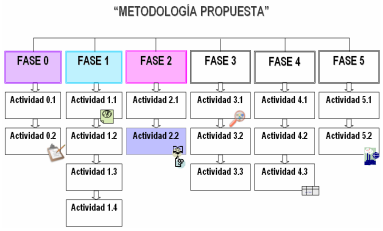
PROCESO PARA EL ACCESO A LOS MEDIOS DE RESPALDO.

Figura 4.20 Diagrama de Flujo de Datos básico del proceso para solicitar acceso a los medios de respaldo de “La empresa”.

Este último diagrama de flujo muestra la entrada del flujo de datos que sería una solicitud de acceso a un medio de respaldo, después se inicia el proceso para dar este acceso, y para terminar, la salida o resultado que se debe obtener es una cuenta de ingreso a la red.

Conocer los diagramas de flujo, permite entender como es que se realizan los proceso en este caso, de alta, baja, modificaciones de privilegios y acceso a los medios de respaldo en su forma básica y que elementos (como la entrada, proceso y salida) los integran fundamentalmente.

4.4.2 Actividad 2.2 *Identificar las brechas de operación y análisis los procesos que se vinculan a estas brechas.*



¿Qué hacer?

Determinar en cada proceso, sí contiene brechas operacionales, es decir; lugares o situaciones en donde las operaciones reales fallan en dar los resultados esperados.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que pueden emplear son la observación, entrevistas, recopilación de información y elaboración de tabla de resultado de análisis de los procesos.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

La herramienta que se puede usar es el procesador de palabras.

RESULTADO
¿Qué obtener?

Conforme a la información obtenida con antelación, se realizó un análisis paso a paso de los procesos de alta, baja y modificación de usuarios de red y el proceso para el acceso a los medios de respaldo, obteniendo las siguientes descripciones:

PROCESO DE ALTA DE USUARIO DE RED.

Paso 1: El Gerente o el Supervisor del área donde será adscrito el nuevo usuario, debe enviar un correo al Gerente de Contabilidad solicitando la creación de esta cuenta nueva, en ese correo debe informar el nombre completo del usuario y el alcance de la cuenta, dependiendo de las actividades que este nuevo usuario realizará dentro de la Red, este correo debe incluir los números de cada pantalla y/o reportes así como el nivel de acceso a éstas que el usuario tendrá para la realización de sus actividades dentro de la Red.

Paso 2: El Gerente de Contabilidad envía el correo original de solicitud al Administrador de Cuentas y al Líder de Sistemas Administrativos informando de su aprobación para la creación y configuración apropiada de la cuenta mencionada.

Paso 3: El Administrador de Cuentas realiza la creación y la configuración de la cuenta nueva.

Paso 4: El Administrador de Cuentas deberá emitir un reporte en un archivo de computadora dado, como evidencia de la creación y configuración de la cuenta nueva.

Paso 5: A la cuenta se le asigna una clave de acceso genérica, la cual es entregada personalmente al usuario, en el mismo proceso de entrega de la clave de acceso, se le indica como personalizar ésta y se le informa que a partir de este momento es solo su responsabilidad el uso que se de a la cuenta creada.

PROCESO DE MODIFICACIÓN DE PRIVILEGIOS DEL USUARIO DE RED.

Paso 1: El usuario que necesita la modificación a su cuenta, debe enviar un correo su Gerente o Supervisor de su área, informando del requerimiento para sus actividades dentro de red. Este correo debe incluir los números de cada pantalla y/o reportes así como el nivel de acceso a éstas que el usuario tendrá.

Paso 2: El Gerente o Supervisor de dicho usuario, debe enviar el correo original de solicitud al Gerente de Contabilidad solicitando su aprobación para la modificación de la cuenta del usuario solicitante. Indicando el detalle de las pantallas y/o reportes a los que el usuario esta solicitando acceso, en el mismo correo se debe especificar el motivo por el cual el usuario está realizando dicho requerimiento.

Paso 3: El Administrador de Cuentas debe emitir un reporte en un archivo de computadora dado, como evidencia de la configuración de la cuenta del usuario solicitante antes y después de dicha modificación.

Paso 4: Ambos archivos se agregan a la respuesta del correo de solicitud, para su envío al Gerente de Contabilidad y al resto de los involucrados en la solicitud.

PROCESO DE BAJA DE USURIO DE RED.

Paso 1: El Gerente de Recursos Humanos, envía un correo al Gerente de TI y al Líder de Sistemas Administrativos informando que algún empleado causó baja en la empresa y solicita se eliminen las cuentas que este usuario utilizaba para sus actividades dentro de la red.

Paso 2: El Líder de Sistemas Administrativos, envía un correo al Administrador de Cuentas y al Gerente de Contabilidad informando de la baja de la cuenta de dicho usuario.

Paso 3: El Administrador de Cuentas emite un reporte del estado actual de la cuenta del usuario a eliminar,

Paso 4: El Administrador de Cuentas realiza un respaldo de la configuración de dicha cuenta en un archivo copiando todos los derechos de acceso que tiene el usuario.

Paso 5: El Administrador de Cuentas elimina dicha cuenta y se documenta como evidencia la baja definitiva de la cuenta del usuario en la ruta del servidor de red H:\Compartir\Sistemas\Baja.

Paso 6: Dicha documentación es agregada a la respuesta del correo de solicitud, para su envío al Líder de Sistemas Administrativos.

PROCESO PARA EL ACCESO A LOS MEDIOS DE RESPALDO.

Los respaldos de información de la base de datos de las aplicaciones se realizan en Discos gravables y son almacenados en cajas identificadas por mes y año, las cuales se encuentran resguardadas en una gaveta dentro de las instalaciones de la empresa.

Los discos son rotulados por número, mes y año y cualquier persona posee acceso a la gaveta donde se encuentran los respaldos; pero no existe evidencia de que tenga un proceso para realizar una solicitud formal para hacer uso de los respaldos.

Como deducción del análisis de los procesos de TI presentados se concluyó las siguientes observaciones:

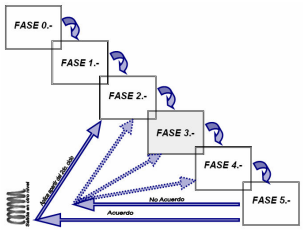
Tabla 4.10 Relación entre Funciones de TI y los Procesos de TI de la "Empresa X".

RESULTADO DEL ANÁLISIS DE LOS PROCESOS	
Procesos Efectivos	**Procesos No efectivos**
☑ Proceso de Alta de usuario de red. ☑ Proceso de Modificación de privilegios de usuario de red. ☑ Proceso de Baja de usuario de red.	☑ Proceso para el acceso a los medios de respaldo (cintas, Discos Compactos y medios removibles).
Conclusión: Como resultado del análisis se concluyó que los procesos arriba mencionados, se encuentran detallados paso a paso, son comprensibles, cuenta con evidencia de su realización, con autorización de uno o varios superiores y son conocidos por el personal.	**Conclusión:** Como resultado del análisis del proceso mencionado arriba, se obtuvo que no existe evidencia de que se cuenta con un proceso detallado y por escrito que permita al personal hacer una solicitud formal de los medios de respaldo.

Por lo tanto, **el proceso que se va a diagnosticará evaluando y priorizando sus riesgos será el proceso para el acceso a los medios de respaldo (cintas, discos compactos y medios removibles),** ya que es evidente, que **es un proceso indefinido**, el cual **puede provocar la materialización de algunos riesgos como perder los discos de respaldo** ya que cualquier persona de la empresa puede tener acceso a ellos.

En resumen, en esta Fase 2, se identificaron los procesos de TI de acuerdo a las funciones anteriormente proporcionadas y se analizaron para saber cuales de ellos podrían contener situaciones de falla, con el propósito de comenzar con la evaluación, diagnóstico y asignación de prioridad de solución de los mismos; estas últimas tres actividades son las que conforman la Fase 3 y que a continuación se iniciará.

4.5 FASE 3.- ELABORACIÓN DEL DIAGNÓSTICO DE LOS PROCESOS DE TI CON BRECHAS OPERACIONALES DE LA EMPRESA:

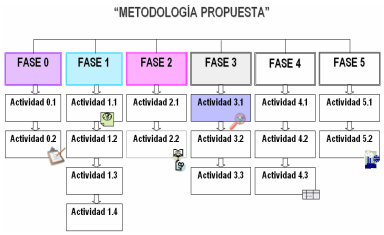


Objetivo general de la Fase 3:

Identificar los riesgos contenidos en los procesos, evaluarlos y darles prioridad de solución.

4.5.1 Actividad 3.1 *Identificar y determinar los riesgos, amenazas y vulnerabilidades.*

¿Qué hacer?



Identificar y determinar definidamente los conceptos como son: los riesgos, amenazas y las vulnerabilidades en los procesos de TI previamente seleccionados.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que pueden emplear son recopilación, análisis de la información y elaboración de tabla para la identificación del riesgo, amenaza y vulnerabilidad.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

La herramienta que se puede usar es el procesador de palabras.

RESULTADO
¿Qué obtener?

En el siguiente cuadro se han colocado el proceso previamente seleccionado con sus riesgos, amenazas y vulnerabilidades correspondientes.

Para llenar este cuadro, hay que tener muy en cuenta las preguntas que vienen en el encabezado de mismo, ya que éstas son las que van a permitir resolverlo que es un riesgo, amenaza y vulnerabilidades,

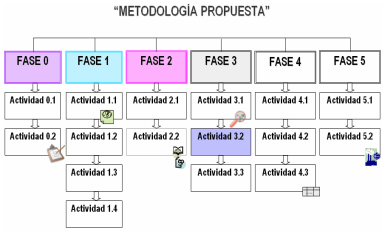
Tabla 4.11 Identificación del Riesgos, Amenazas y Vulnerabilidades de los procesos de TI de la "Empresa X".

IDENTIFICACIÓN DEL RIESGO			
PROCESO	**AMENAZA** (Suceso maligno que lo ocasionó)	**DESCRIPCIÓN DE LAS VULNERABILIDADES** (¿Qué ocasionó ese suceso?)	**RIESGO** (¿En qué puede afectar?)
Proceso para el acceso a los medios de respaldo (cintas, discos gravables y medios removibles).	Perdida de la información respaldada debido al nulo aseguramiento de acceso a la misma.	-No contar con restricciones de acceso a los medios de respaldo para el personal.	*No contar con respaldos de información que pueda ser requerida.*
		-Mantener la información en un lugar dentro de la misma empresa.	
		-No contar con un sitio seguro, como una gaveta con llave en donde almacenarlos.	

Una vez identificado los riesgos, así como las amenazas y vulnerabilidades que los integran, es momento de **darle un valor** con el propósito de reconocer entre los ellos, cuál es el más impacta a la empresa y que con más frecuencia se da, además de saber con quede disponibilidad de recursos cuenta cada uno para su resolución.

4.5.2 Actividad 3.2 *Evaluar el riesgo y seleccionar la técnica para evaluar.*

¿Qué hacer?



Seleccionar una técnica de evaluación de riesgos (entre la evaluación cuantitativa ó cualitativa), para dar una valoración a los riesgos.

TÉCNICAS APLICADAS
¿Cómo hacer

Las técnicas que pueden emplearse son las de evaluación de riesgos cuantitativa y cualitativa y la elaboración de gráficos como concentrados de la valoración.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar son el procesador de palabras y la hoja de cálculo.

RESULTADO
¿Qué obtener?

Ahora bien, **considerando que "La empresa" es de tamaño pequeño**, que es una compañía que **recién quiere iniciar en un ambiente de seguridad para su informa**ción y que **cuenta con recursos limitados para este comienzo**; dado estas condiciones, la técnica se escoge es la **evaluación cualitativa.**

Para determinar el impacto y la probabilidad de ocurrencia del riesgo se aplicó un cuestionario acerca de estos dos temas al personal de TI involucrado directamente con el proceso y su riesgo.

El personal que participó fue de 5 individuos y lo que se obtuvo en resumen, es lo siguiente:

Tabla 4.12 Cuadro que concentra los niveles de impacto y ocurrencia del riesgo evaluado en la "Empresa X".

Cuestionario aplicado a 5 personas	**RIESGO: No contar con respaldos de información que pueda ser requerida.**		
NIVEL DE IMPACTO / Ocurrencia	**BAJO / Casi nunca**	**MEDIO / Regularmente**	**ALTO / Siempre sucede**
¿Qué tan a menudo considera que ocurre este riesgo en la empresa?	0	4	1
¿Qué nivel de *Impacto* causaría el surgimiento de este riesgo en la empresa?	1	3	1

De acuerdo a los resultados del cuadro anterior, la mayoría de los participantes en el cuestionario considera que la ocurrencia de este riesgo sucede regularmente.

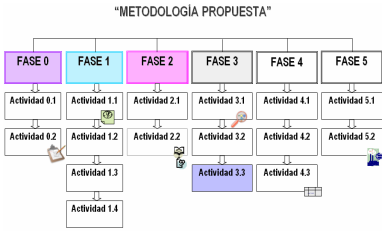
Y que el impacto que causa a la empresa también se considera en un nivel regular o medio.

Por lo tanto, y **como resultado** de esta última tabla, se puede determinar que **la Ocurrencia tiene** un nivel **MEDIO** y **el impacto** también, **tiene un nivel MEDIO.**

A continuación, y de acuerdo a estos niveles obtenidos en esta actividad, se verá como se debe priorizar el riesgo.

4.5.3 Actividad 3.3 *Priorizar riesgos y selección de alternativa para responder ante el mismo.*

¿Qué hacer?



Dar prioridad a los riesgos de acuerdo al impacto, probabilidad y disponibilidad de recursos, además de seleccionar una alternativa para el tratamiento de cada riesgo.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que pueden emplear son recopilación y análisis de la información.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar son el procesador de palabras y la hoja de cálculo.

RESULTADO
¿Qué obtener?

Dado que, el resultado obtenido en la anterior actividad determina que el riego se evaluó conforme a la Probabilidad de Ocurrencia del mismo en un nivel MEDIO y el impacto que puede tener en la empresa con un nivel MEDIO también, en seguida, se presenta la siguiente tabla que propone unifica las anteriores valorizaciones en una sola, a fin de facilitar la asignación del nivel de prioridad:

Tabla 4.13 Cuadro de la prioridad del riesgo acorde al impacto y probabilidad del mismo.

VALORES DEL RIESGO ACORDE A LA PROBABILIDAD DE OCURRENCIA / IMPACTO				
1 Intrascendente	2 Baja	3 Media	4 Moderado	5 Alta

Impacto	Probabilidad de Ocurrencia	Valor	Prioridad
Bajo	Bajo	1	Intrascendente
Medio	Bajo	3	Media
Alto	Bajo	4	Moderada
Bajo	Medio	2	Baja
Medio	**Medio**	3	**Media**
Alto	Medio	5	Alta
Bajo	Alto	4	Moderada
Medio	Alto	5	Alta
Alto	Alto	5	Alta

De acuerdo a los valores de impacto y probabilidad anteriores, se puede deducir con esta tabla que la **prioridad de resolución** que se le debe dar a este riesgo **es Media y tiene un valor de 3.**

Ya que este ejemplo no cuenta con un conjunto de riesgos para darles prioridad entre ellos, sí se tuviera el caso contrario, los valores numéricos que propone la tabla preliminar, serán de mucha ayuda, ya que facilitará tomar la decisión de cual riesgo resolver primer, comenzando con los de valor 5 hasta llegar al 1.

Otro punto que hay que y tomar en cuenta para una mejor manera de priorizar es la disponibilidad de los recursos, esta dependerá de dos cuestiones, la primera de acuerdo a el riesgo que se quiera mitigar serán los recursos que se soliciten y la segunda es referente a la cantidad de recursos con que cuente la empresa.

Entonces conforme a los resultados obtenidos, se deberá seleccionar la acción que se va a tomar con respecto a ese riesgo.

A continuación, se presenta un cuadro que puede revisarse para seleccionar una forma de tratar al riesgo:

Tabla 4.14 Cuadro de las acciones a tomar para tratar el riesgo de la "Empresa X".

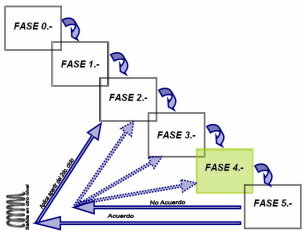
TRATAMIENTO DEL RIESGO			
Acción a tomar	**Descripción de Acción**	**Efecto en la empresa**	**Efectividad**
Tolerar	Soportar el riesgo y no tomar ninguna acción.	No ofrece ninguna mejora y sigue afectando a la empresa.	✗
Mitigar	Reducir el riesgo mediante la implementación de medidas.	Se implantan objetivos de control que nos aseguran que se esta llevando a cabo las actividades de un proceso determinado. Puede ser realizada por el personal de la empresa.	✓
Eliminar	Terminar con el riesgo, retirando el proceso.	No se puede eliminar, ya que es un proceso útil y necesario para contar con información disponible y confiabilidad.	✗
Transmitir	Transferir el riesgo a un tercero.	Es una solución costosa para la empresa.	✗

Como resultado de la revisión de estas alternativas, se puede asumir que tolerar no es una opción que nos permita disminuir el riesgo; la alternativa eliminar no es posible, ya que este proceso es indispensable para "La empresa", transmitir podría ser una solución siempre y cuando la empresa tenga los recursos suficientes para mantener esta opción y por último **mitigar**, que **es la alternativa que permitiría reducir este riesgo al implementar objetivos y sus actividades correspondientes para mantener este proceso bajo control.**

En síntesis, esta Fase 3 se pudo dar valor a la probabilidad de ocurrencia y al impacto que podría causar el riesgo encontrado en la fase anterior, así como unificar el valor de estos dos términos con el propósito de darle prioridad al riesgo de mayor nivel ante los demás riesgos. Por lo tanto, la siguiente Fase pretende diseñar contramedidas que permitan reducir este riesgo.

4.6 FASE 4.- IDENTIFICACIÓN, DISEÑO Y DESARROLLO DE ACTIVIDADES DE CONTROL EN LOS PROCESOS DE TI CON RIESGO:

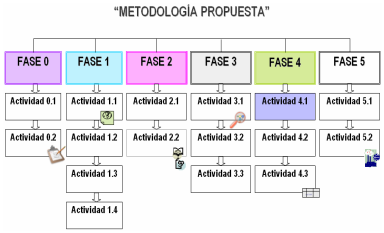
Objetivo general de la Fase 4:



Mitigar los riesgos a través del uso de objetivos de control y el diseño de sus actividades para el área tecnologías de información mediante el desarrollo de una propuesta de matriz.

4.6.1 Actividad 4.1 *Identificación de actividades de controles en los procesos de TI.*

¿Qué hacer?



Identificar cuales de los procesos con riesgos, cuentan ó contienen actividades de control.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que pueden emplear son entrevistas, cuestionarios y recopilación y análisis de la información.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

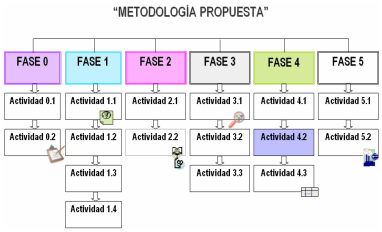
La herramienta que se puede usar es el procesador de palabras.

RESULTADO
¿Qué obtener?

En este caso en particular, al no contar con un proceso defino y detallado para el acceso a medios de almacenamiento, no es posible la existencia de alguna actividad de control.

Lo que sí es posible es diseñar alguna actividad que permita mitigar el riego y que se realizará en la siguiente actividad:

4.6.2 Actividad 4.2 *Diseño de actividades de controles en los procesos de TI.*



¿Qué hacer?

Se requiere conocer el objetivo que se desee alcanzar, es decir; el propósito que se quiere cumplir y que es afectado por la aparición del riesgo, para poder diseñar la actividad que genere una disminución en el efecto de éste.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que pueden emplear son la observación, indagación, entrevistas y elaboración de tabla con los objetivos y actividades de control.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar son el procesador de palabras y el marco referencial COBIT.

RESULTADO
¿Qué obtener?

Retomado cual es el proceso y el riesgo que lo afecta y recordando tomar en cuenta las preguntas que se deben responder para facilitar el llenado de esta tabla, se elaboró lo siguiente:

Tabla 4.15 Cuadro del uso y diseño de los objetivos y actividades de control de la "Empresa X".

EL OBJETIVO DE CONTROL Y DISEÑO DE SUS ACTIVIDADES.			
PROCESO	**RIESGO** (¿En qué puede afectar?)	**OBJETIVO DE CONTROL** (¿Qué propósito se quiere cumplir?)	**ACTIVIDAD DE CONTROL** (Acción que se debe tomar para cumplir ese propósito)
Proceso para el acceso a los medios de respaldo (cintas, discos gravables y medios removibles).	No contar con respaldos de información que pueda ser requerida.	Brindar un servicio continuo de TI requiere de la administración de un sitio de almacenamiento externo a las instalaciones, donde se guarden los respaldos de información necesarios para la recuperación de TI y para los planes de continuidad de la empresa. La Gerencia de TI debe asegurarse de que este sitio cuente con las políticas y procedimientos indispensables para recuperar, mantener y conservar la información empresarial. Referencia COBIT 2005 (DS4)	Establecer un formato manual o automatizado donde el dueño de la información y la Gerencia de TI supervisen y autoricen el uso e instalación de la información respalda en cintas, CD y medios removibles.

Para comenzar con la descripción de este cuadro, como ya se ha explicado las columnas de proceso y riesgo en las actividades 3.1 y 3.2, la siguiente columna, que se refiere al **objetivo de control se puede determinar definiendo cuál sería el propósito general que se debe cumplir ó alcanzar al realizar un proceso de forma efectiva**, está se debe contestar viéndolo desde un punto mayor, es decir; como un meta de la empresa.

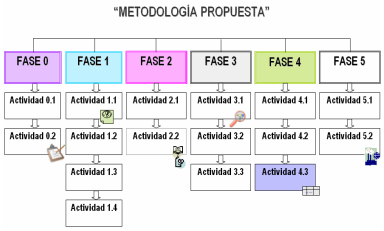
Ciertamente, resulta difícil idear estos objetivos de control, para ello, se recomienda el uso de marco de referencia COBIT, que ofrece cuatro dominios que contienen 34 procesos genéricos que contienen un conjunto de objetivos de controles de Tecnología de Información actualizados, internacionales y generalmente aceptados para ser utilizados diariamente por Gerentes y personal de TI.

El objetivo de control que aquí se incluye fue extraído de este marco de referencia, pertenece al dominio de Entregar y Dar soporte (DS) número 4 que se refiera a: brindar un servicio continuo de TI requiere de la administración de un sitio de almacenamiento externo a las instalaciones, donde se guarden los respaldos de información necesarios para la recuperación de TI y para los planes de continuidad de la empresa.

Con respecto a la última columna que habla de **la actividad de control**, una vez definido el objetivo es más fácil **determinar la acción o actividad que se debe realizar para que ese objetivo sea alcanzado**, en este caso, **si no se cuenta con un procedimiento para el acceso a los medios de respaldo (cintas, discos gravables y medios removibles), la contramedida inmediata sería crear un procedimiento que permita un acceso controlado a estos medios.**

En la siguiente actividad, se propone como una manera de reunir los conceptos y obtener una visión global, el desarrollar una matriz en dos partes; la primera que englobe los términos ya mencionados ya algunos otros asociados como son: Objetivo de control, Descripción del Riesgo, Actividad de control, Descripción de la actividad de control, Periodicidad del control y Clasificación del mismo y la segunda parte compuesta por términos que ayuden a evaluar y monitorear que los objetivos y actividades anteriormente propuestos, se están llevando de la manera en que se describe en la primera parte de la matriz.

4.6.3 Actividad 4.3 *Desarrollar la matriz de objetivos de control, actividades de control y riesgo.*



¿Qué hacer?

Desarrollar una matriz en la cual se concentran los conceptos de objetivo de control, descripción del riesgo, actividad de control, descripción de la actividad de control, periodicidad y clasificación de control.

TÉCNICAS APLICADAS
¿Cómo hacer?

La técnica que puede emplear es la definición de una tabla denominada "Matriz de Objetivos de control, Actividades de control y Riesgos".

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar son el procesador de palabras, hoja de cálculo y el marco referencial COBIT.

RESULTADO
¿Qué obtener?

En seguida, se muestra el resultado de la Matriz de Objetivos de control, Actividades de control y Riesgos (primera parte) que se obtuvo al reunir los términos vistos en las actividades anteriores:

Tabla 4.16 Matriz de Objetivos de control, Actividades de control y Riesgos de la "Empresa X" (Inicio).

DOMINIO	1) Objetivo de control	2) Descripción del Riesgo	3) Actividades de Control	4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Evidencia, Supervisión y autorización)	5) Periodicidad de la actividad de control	6) Clasificación de la actividad de control Manual /Automático
ENTREGAR Y DAR SOPORTE	Brindar un servicio continuo de TI requiere de la administración de un sitio de almacenamiento externo a las instalaciones, donde se guarden los respaldos de información necesarios para la recuperación de TI y para los planes de continuidad de la empresa. La Gerencia de TI debe asegurarse de que este sitio cuente con las políticas y procedimientos indispensables para recuperar, mantener y conservar la información empresarial. (Referencia COBIT-DS4)	No contar con respaldos de información que pueda ser requerida en cualquier momento, puede provocar perder la disponibilidad de la información. (Nivel medio **3**)	Tener un proceso para el acceso a los medios de respaldo (cintas, Discos Compactos y medios removibles).	"La empresa" no cuenta con un formato manual o automatizado donde el dueño de la información y la Gerencia de TI supervisen y autoricen el uso e instalación de la información respalda en cintas, Discos Compactos y medios removibles.	Anual	Manual

Para la elaboración de esta matriz, se utilizó el siguiente cuadro guía que explica el contenido de cada una de las columnas:

Tabla 4.17 Cuadro guía para llenar la matriz de Objetivos de control, Actividades de control y Riesgos (Inicio).

Columna	Explicación
Nombre del Dominio (opcional)	Nombre del dominio de COBIT del cual fue obtenido el objetivo de control.
1) Objetivo de Control	Es una declaración del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI. Responde a la pregunta ¿Qué propósito se quiere cumplir.
2) Descripción del Riesgo	Se describe el acontecimiento pueda afectar ó impactar el alcance de los objetivos. Reponde a la pregunta ¿Qué propósito se quiere cumplir?
3) Actividad de control	Se trata de son las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar una garantía razonable de que los objetivos del negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados. Responde a la Acción que se debe tomar para cumplir ese propósito.
4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Supervisión y autorización)	Descripción a detalle de la actividad que la empresa realiza para cubrir el objetivo de control. Puede responder con las preguntas siguientes: ¿Qué actividad de control se está aplicando para este objetivo?, ¿Cómo se lleva acabo esta actividad?, ¿Quién realiza esta actividad?, ¿Dónde se realiza esta actividad?, ¿Cuándo se realiza la actividad de control?, ¿Qué evidencia produce esta actividad de control?, ¿Quién supervisa esta actividad? ¿Quién autoriza la realización de la actividad de control?, etc.,
5) Periodicidad del control (sólo para controles manuales)	Frecuencia de la ejecución de la actividad de control, Se refiera a la cantidad de veces con la qué se aplica esta actividad de control, puede ser varias veces al día, semanal, quincenal, mensual, anual, etc.
6) Clasificación de la Actividad de control (automático/manual)	Documentar el tipo de control: -Controles automáticos: Son aquellos soportados por los sistemas de aplicación. -Controles manuales: Son aquellos llevados a cabo por los funcionarios de la organización.

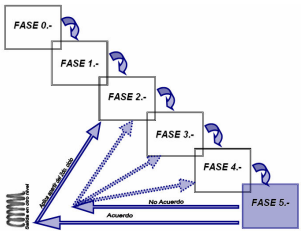
El desarrollo de este cuadro guía se hizo con el fin de contar con una síntesis de los conceptos que se manejan en la Matriz de Objetivos de control, Actividades de control y Riesgos.

Éste, se ha dividido en dos partes, el segmento inicial presentado anteriormente, que se utilizará para llenar la primera parte de la matriz y la segunda corresponde a la parte restante de la misma.

Después, de haber culminado la primera parte de esta Matriz de Objetivos de control, Actividades de control y Riesgos propuesta; a continuación, la siguiente Fase aborda los temas de la implantación de estos objetivos y actividades, así como la forma de evaluar y monitorear estas actividades una vez implantadas.

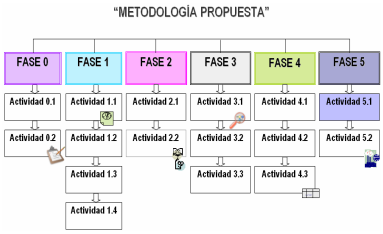
4.7 FASE 5.- IMPLANTACIÓN Y MONITOREO DE LAS ACTIVIDADES DE CONTROL Y CAPACITACIÓN DEL PERSONAL:

Objetivo general de la Fase 5:



Dar a conocer las actividades de control, para que se pongan en operación y se presta la capacitación respectiva al personal para el cumplimiento y ejecución de éstas. Implementar una evaluación de actividades de control (monitoreo) para verificar qué se estén ejerciendo y cumplan con sus objetivos de control.

4.7.1 Actividad 5.1 *Implantación de las actividades de control y preparación del personal.*



¿Qué hacer?

Dar a conocer las actividades de control exhortando a la concienciación y convencimiento hacia a la Dirección, personal de TI y demás involucrado.

TÉCNICAS APLICADAS
¿Cómo hacer?

Las técnicas que pueden emplear son juntas y reuniones para explicar el uso y beneficios de las actividades de control implantadas.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

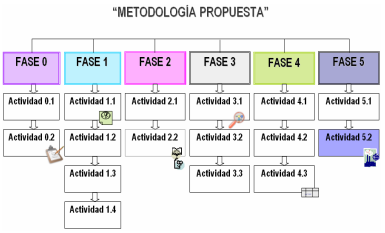
Las herramientas que se pueden usar son equipo de cómputo y proyector para las presentaciones.

RESULTADO
¿Qué obtener?

Presentar los nuevos objetivos y actividades al personal en general. El convencimiento y la concienciación de la dirección, personal de TI y demás involucrados , para que comprendan y sigan los procedimientos, normas, políticas y prácticas nuevas que le ayudarán a realizar mejor su trabajo.

Adquirir motivación y cooperación para producir un cambio de actitud en el personal, de manera que se arraigue el control de las TI en la empresa.

4.7.2 Actividad 5.2 *Monitoreo de las actividades de control.*



¿Qué hacer?

Determinar sí las actividades de control implantadas operan de manera efectiva para prevenir errores.

TÉCNICAS APLICADAS
¿Cómo hacer?

La técnica que puede emplear es la definición de una tabla denominada matriz de control.

HERRAMIENTAS DE APOYO
¿Con qué hacer?

Las herramientas que se pueden usar son el procesador de palabras, hoja de cálculo y el marco referencial COBIT.

¿QUÉ RESULTADO SE DEBEN OBTENER?

En seguida, se muestra el resultado de la Matriz de Objetivos de control, Actividades de control y Riesgos (segunda parte):

Tabla 4.18 Matriz de objetivos de control, Actividades de control y riesgos de la "Empresa X" (Final).

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia
Solicitar el procedimiento para el acceso a los medios de respaldo y evidencia de su realización verificando que estuviese autorizado por la gerencia.	Sistemático / 1	Se encuentró evidencia y documentación de que el procedimiento para el acceso a los medios de respaldo se lleva acabo.	Efectivo Nivel de Madurez **5**	1.Proceso de acceso a los respaldos.doc 2.Correos electónicos de la solicitud y autorización al acceso de los medios de almacenamiento.

Para llenar esta segunda parte, de la Matriz de Objetivos de control, Actividades de control y Riesgos se empleo el segmento correspondiente del cuadro guía creado para facilitar este propósito y que se muestra en seguida:

Tabla 4.19 Cuadro guía para llenar la matriz de Objetivos de control, Actividades de control y Riesgos (Final).

<table>
<tr><th>Columna</th><th>Explicación</th></tr>
<tr><td>7) Descripción del plan de prueba</td><td>Trata de la descripción del procedimiento que se va ejecutar para revisar que la actividad de control se este efectuando correctamente, este debe incluir la técnica que se usó. Se propone el empleo de las siguientes técnicas:
• Indagación, Observación, Inspección de documentos y registros y Reproducción.</td></tr>
<tr><td>8) Metodo y Cantidad de selección de partidas (Al azar, fortuito o Sistematico)</td><td>Se refiere a la forma en que se realizó la selección de partida ó muestra para verificar si se a efectuado la actividad de control en un periodo de días, semanas ó meses, según se requiera.

El método de selección:
Casual o fortuito: Seleccionados manualmente sin sesgo consciente
Al azar: Utilizando tablas o software para generar números al azar
Sistemático: Seleccionando manualmente considerando un intervalo fijo entre los individuos de la población a ser incluidos en la muestra.
<table>
<tr><th>Frecuencia de la Actividad de Control</th><th>Tamaño de Muestra</th></tr>
<tr><td>Anual</td><td>1</td></tr>
<tr><td>Trimestral</td><td>4</td></tr>
<tr><td>Mensual</td><td>12</td></tr>
<tr><td>Semanal</td><td>52</td></tr>
<tr><td>Diario</td><td>250</td></tr>
<tr><td>Varias veces al día</td><td>Más de 250</td></tr>
</table></td></tr>
<tr><td>9) Resultados de la prueba</td><td>En esta parte se tiene que describir los resultados obtenidos de la experiencia que se tuvo con el método de prueba utilizado</td></tr>
<tr><td>10) Conclusión sobre efectividad (efectivo / no efectivo)</td><td>En esta columna es donde se coloca el grado de cumplimiento de la actividad de control, esta graduación puede estar compuesta por varios niveles, puede ir desde el más conciso valorando sí es efectiva la actividad de control o no es efectiva. Sí se requiere una escala más específica para evaluar el cumplimiento de la actividad de control se puede utilizar los modelos de madurez que ofrece en cada uno de los objetivos de control el marco referencial COBIT.</td></tr>
<tr><td>11) Referencia de evidencia</td><td>Aquí se coloca el nombre y las pruebas obtenidas como documentación, correos electrónicos, impresiones de pantalla, etc., que permiten soportar el resultado de la prueba.</td></tr>
</table>

A continuación, se muestra la Matriz de Objetivos de control, Actividades de control y Riesgos completa obtenida con la implantación de esta metodología propuesta:

Tabla 4.20 Matriz completa de Objetivos de control, Actividades de control y Riesgos de la "Empresa X".

DOMINIO	1) Objetivo de control	2) Descripción del Riesgo	3) Actividades de Control	4) Descripción de la actividad de control (Qué, Cómo, Quién, Dónde, Cuándo, Evidencia, Supervisión y autorización)	5) Periodicidad de la actividad de control	6) Clasificación de la actividad de control Manual /Automático
ENTREGAR Y DAR SOPORTE	Brindar un servicio continuo de TI requiere de la administración de un sitio de almacenamiento externo a las instalaciones, donde se guarden los respaldos de información necesarios para la recuperación de TI y para los planes de continuidad de la empresa. La Gerencia de TI debe asegurarse de que este sitio cuente con las políticas y procedimientos indispensables para recuperar, mantener y conservar la información empresarial. (Referencia COBIT-DS4)	No contar con respaldos de información que pueda ser requerida en cualquier momento, puede provocar perder la disponibilidad de la información. (Nivel medio **3**)	Tener un proceso para el acceso a los medios de respaldo (cintas, CD y medios removibles).	"La empresa X" no cuenta con un formato manual o automatizado donde el dueño de la información y la Gerencia de TI supervisen y autoricen el uso e instalación de la información respalda en cintas, CD y medios removibles.	Anual	Manual

7) Descripción del plan de prueba	8) Método y Cantidad de selección de partidas (Al azar, fortuito o Sistemático)	9) Resultados de la prueba	10) Conclusión sobre efectividad (efectivo / no efectivo)	11) Referencia de la evidencia
Solicitar el procedimiento para el acceso a los medios de respaldo y evidencia de su realización verificando que estuviese autorizado por la gerencia.	Sistemático / 1	Se encuentró evidencia y documentación de que el procedimiento para el acceso a los medios de respaldo se lleva acabo.	Efectivo Nivel de Madurez **5**	1.Proceso de acceso a los respaldos.doc 2.Correos electónicos de la solicitud y autorización al acceso de los medios de almacenamiento.

Esta Matriz de Objetivos de control, Actividades de control y Riesgos, permitirá a la empresa manejar en una sola visión diversos temas relacionados con el riesgo.

Con esta matriz se podrá:

- ☑ Describir el riesgo.
- ☑ Asignarle al riesgo una o varias actividades y describirlas para aminorarlo.
- ☑ Fijar objetivos que permitan reconocer si se están cumpliendo con las actividades.
- ☑ Determinar que la clase de actividades de control que se están efectuando (automático o manual).
- ☑ Determinar que tan a menudo se hace ésta actividad de control.

Además, de concentrar una parte que se dedica a la evaluación de las actividades de control que permite:

- ☑ Describir una prueba o varias pruebas para comprobar la efectividad de las actividades de control.
- ☑ Contiene el método que se va a usar para estas pruebas y la cantidad de la muestra que se va emplear para realizarlas.
- ☑ Detallar el resultado obtenido de las pruebas.
- ☑ Colocar la experiencia y conclusión obtenida de las pruebas.
- ☑ Y hacer referencia a la documentación proporcionada para la realización de estas misma.

BIBLIOGRAFÍA.

[Van Gigch, 2008] Van Gigch J. P., "Teoría de general de sistemas", Ed.Trillas, México.

[Gran Diccionario Enciclopédico, 1982] Reader´s Digest (Ed.), "Concepto de Riesgo", (vol. 10), México.

[Chiavenato, 1994] Chiavenato Idalberto, "Administración de Recursos Humanos", Ed. Mc Graw Hill, Colombia.

[Reyes, 1992] Reyes Ponce Agustín, "Administración Moderna", Ed. Limusa, México.

[Hernández, Ballesteros, 1990] Hernández Sergio y Ballesteros Nicolás, "Fundamentos De Administración", Ed. Interamericana, México.

[Santillana, 2003] Santillana Gonzáles Juan Ramón, "Establecimiento de Sistemas de Control Interno", Ed. Thomson, México,

REFERENCIAS.

[Catalán y Rodríguez, 2005] Catalán García Beatriz y Rodríguez Valenzuela,"El reto de la seguridad de la información en México, una estrategia para abordarla", Revista Contaduría Pública, Año 33, Nº 395, México.

[COBIT, 2005] IT Governance Institute (Ed), "Marco de Trabajo de Objetivos de Control para la Información y Tecnologías relacionadas (COBIT)", (ver 4.0), Estados Unidos de América. Disponible en: http://www.isaca.org.mx

[Comisión Europea, 2006] "La nueva definición de PYME", Guía del usuario y ejemplo de declaración, Publicaciones de empresa e industria, Comisión Europea, Disponible en: http://ec.europa.eu/enterprise/enterprise_policy/sme_definition/sme_user_guide_es.pdf

[COSO, 2008] Resumen:"Los nuevos conceptos de Control Interno (Informe COSO)", consultado en la pagina de la Secretaria de la Función Pública de México, [fecha de consulta: 20 de diciembre del 2008]. Disponible en: http://www.funcionpublica.gob.mx/scagp/ucegp/guias/informe_coso_resumen.doc

[Egan, 2005] Egan Mark, "Seguridad de la información en el factor humano", Boletín electrónico de Information Systems Audit and Control Association (ISACA), Bogota, Colombia. Disponible en: http://www.isaca-bogota.net

[Ernst & Young, 2007] Ernst & Young (Ed),"10ª Encuesta Global de Seguridad de la Información de Mancera Ernst & Young" Disponible en: http://www.ey.com/global/assets.nsf/Mexico/EGSI10c/$file/EGSI10c.pdf

[Fernández, 2003] Adriana Fernández Menta, "El Modelo COBIT", Boletín de la Comisión de Normas y Asuntos Profesionales de Instituto de Auditores Internos de Argentina N° 12, (Diciembre de 2003), Disponible en línea en: http://www.iaia.org.ar/publicaciones-normaria.html

[Galindo, 2002] Galindo L. A., "Metodología Para El Apoyo Al Desarrollo Y Redacción Del Proyecto De Tesis De Maestría", Memorias Del 3er. Congresos Internacional De Ingeniería Electromecánica Y De Sistemas, SEPI – ESIME Zacatenco, IPN, Noviembre De 2002, México, D.F.

[Galindo, 2006] Galindo L., "Reporte Técnico: Planeación y Administración de Sistemas de Información", Maestría en Ciencias en Ingeniería de Sistemas, SEPI – ESIME Zacatenco, IPN, 2006, México, D.F.

[Galindo, 2007] Galindo L., "Una metodología Básica para el Desarrollo de Sistemas", Memorias Del 3er. Congresos Internacional De La Ciencia Y De La Investigación Para La Educación, Marzo de 2007, Campeche, México,

[Galindo, 2008] Galindo L., "Metodología para crear la Tabla metodológica o Tabla Solución Integral, como apoyo al desarrollo de sistemas", Maestría en Ciencias en Ingeniería de Sistemas, SEPI – ESIME Zacatenco, IPN, 2008, México, D.F.

[Microsoft, 2004] Microsoft, "Guía de administración de riesgos de seguridad", [fecha de consulta: 3 de febrero del 2009]. Disponible en: http://www.microsoft.com/spain/technet/recursos/articulos/srsgch00.mspx

[Oseni, 2007] Oseni Ezekiel, "Gerencia del cambio en el proceso de cambio", Boletín electrónico de Information Systems Audit and Control Association (ISACA), Bogota, Colombia. Disponible en: http://www.isaca-bogota.net

[Perfil OSI, 2003], CUDI-CDR-Grupo de Seguridad, "Perfil Oficial de Seguridad Informática", [fecha de consulta: 5 de marzo del 2009], Disponible: http://rfc.cudi.edu.mx/drafts/draft2.pdf

[PWC, 2006] PricewaterhouseCoopers (Ed), Manual de Curso "GO SPA 2006", México.

[SOX, 2008] "Sarbanes Oxley: FAQ´s"**,** consultado en la página de Deloitte Chile, [fecha de consulta: 20 de diciembre del 2008]. Disponible en: http://www.deloitte.com/dtt/article/0,1002, cid%253D112807,00.html

[SOX1, 2008] "Ley Sarbanes Oxley" disponible en su versión en inglés, [fecha de consulta: 20 de diciembre del 2008]. Disponible en: http://www.deloitte.com/dtt/cda/doc/content/Ley %20Sarbanes%20Oxley.pdf

[Web 1, 2009] Colaboradores de Wikipedia. "Metodología" [en línea]. Wikipedia, La enciclopedia libre, 2009 [fecha de consulta: 3 de febrero del 2009]. Disponible en http://es.wikipedia.org/w/index.php?title=Metodolog%C3%ADa&oldid=23776209

[Web 2, 2008] Colaboradores de Wikipedia. "Seguridad informática" [en línea]. Wikipedia, La enciclopedia libre, 2008 [fecha de consulta: 27 de diciembre del 2008]. Disponible en http://es.wikipedia.org/w/index.php?title=Seguridad_inform%C3%A1tica&oldid=22866981

LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN.

A.1 LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN.

La información es el objeto de más valor para las empresas, por tal motivo juegan un papel muy importante, ya que es la materia prima de cualquier acción dentro de éstas. Es por ello que la seguridad de esta información deber de ser un asunto de suma consideración.

Lo que actualmente, no se puede apreciar así en la mayoría de los casos. De acuerdo con el Lic. Adrián Palma Castillo, ex presidente de la Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI), grupo de profesionales relacionados con la informática, con el objetivo de reducir los riesgos de del uso de la tecnología de la información en las organizaciones dice:

> *"El gran problema de la seguridad a nivel nacional y Latinoamérica y en algunos casos a nivel internacional es el desconocimiento real de los distintos temas de seguridad, hoy día las organizaciones se enfocan a soluciones puntuales y totalmente reactivas y correctivas además de que la mayoría de las organizaciones se enfoca a la cultura del producto, el problema radica en que las instituciones o empresas no saben realmente cuál es el nivel de seguridad que requiere su organización y esto es por que no se sabe cuáles son realmente los riesgos que pudieran poner en peligro la capacidad de operación, servicio y en algunos casos hasta la supervisión de la organización.*
>
> *Aunado a lo anterior las organizaciones tienen que enfrentar el reto de exigir servicios que realmente cumplan con sus necesidades de seguridad con una alta calidad y a un costo aceptable, la pregunta obligada es: ¿cómo lograrlo? ya que la seguridad se ve desde un punto de vista meramente tecnológico y difícilmente involucran a todas las áreas del negocio".* [Catalán, Rodríguez, 2005]

Figura A.1 Lic. Adrián Palma Castillo, ex-presidente de la Asociación Latinoamericana de Profesionales en Seguridad Informática (ALAPSI).

Conforme a lo anterior citado, podemos ver que la seguridad de información no es un rubro que se consideré de gran importancia para las empresas.

Por consiguiente y para confirmar este supuesto, se ha incluido algunas preguntas y respuestas más representativas para el objeto de interés de esta tesis, de la 10ª Encuesta Global de Seguridad de la Información de Mancera Ernst & Young, firma de auditoría y asesoría de negocios; la cual fue aplicada en el año de 2007 a casi 1,300 organizaciones a nivel mundial pertenecientes a más de 20 diferentes sectores industriales; en la cual, México obtuvo el tercer lugar de participación.

En seguida se muestran algunos de las preguntas representativas realizadas:

1a.- ¿En qué nivel se encuentra integrada la función de seguridad de la información al proceso corporativo de administración de riesgos?

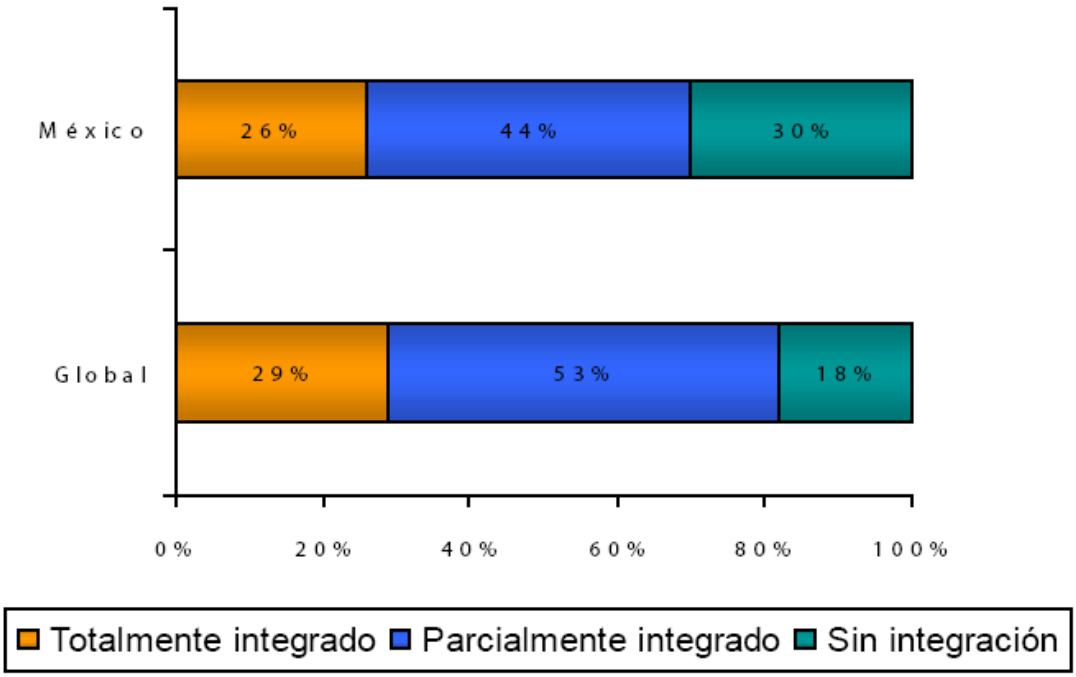


Figura A.2 Gráfica de resultados del nivel de integración de la función de seguridad de la información al proceso corporativo de administración de riesgos.

Los resultados de esta primera pregunta muestran una brecha significativa en el nivel de alineación e integración de la función de seguridad de la información a los objetivos y procesos de negocio.

Por ejemplo, sólo 26% de las organizaciones en México señala que existe una integración total entre la seguridad de la información y el proceso corporativo de administración de riesgos (figura 1.4).

2ª.- ¿Cuál es el principal habilitador de la integración de la seguridad de la información al proceso corporativo de administración de riesgos?

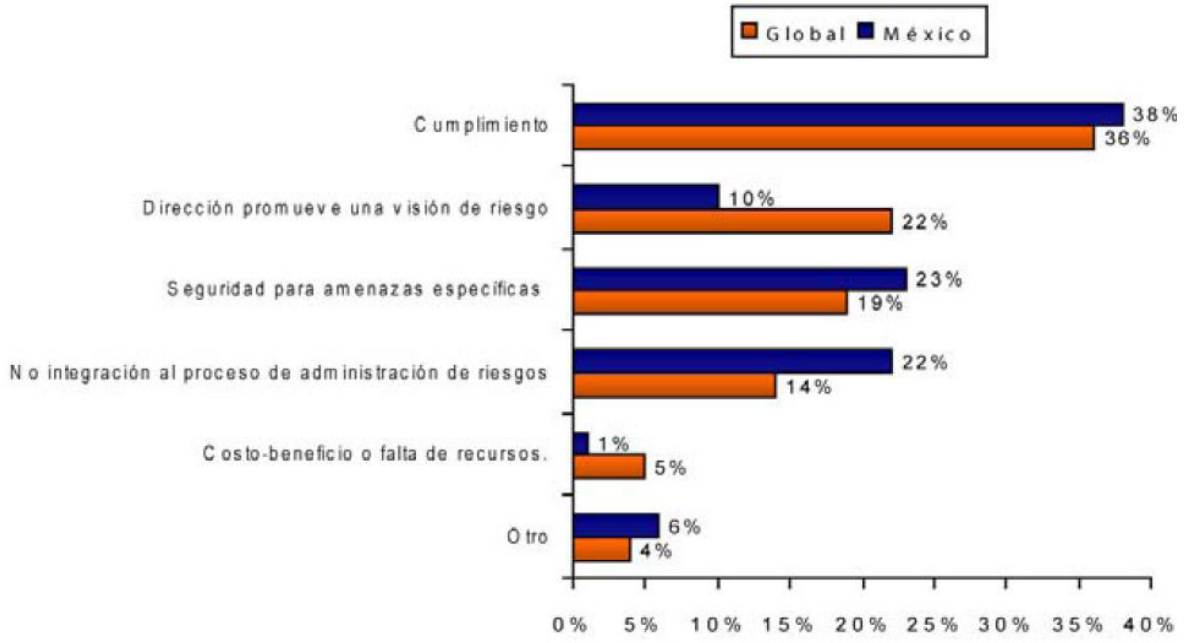


Figura A.3 Gráfica de resultados del principal habilitador de la integración de la función de seguridad de la información al proceso corporativo de administración de riesgos.

De la anterior figura, se puede concluir que el principal habilitador para que se lleve a cabo la seguridad de la información es ***el cumplimiento***, es decir, que se realiza por acatamiento u obligación, y no por el concepto de preocupación (en la toma de acciones preventivas) ó conciencia (como el estado en que la seguridad es parte inherente en el proceso).

3ª.- ¿Cuáles son los habilitadores que han tenido un impacto significativo en las prácticas de seguridad de la información?

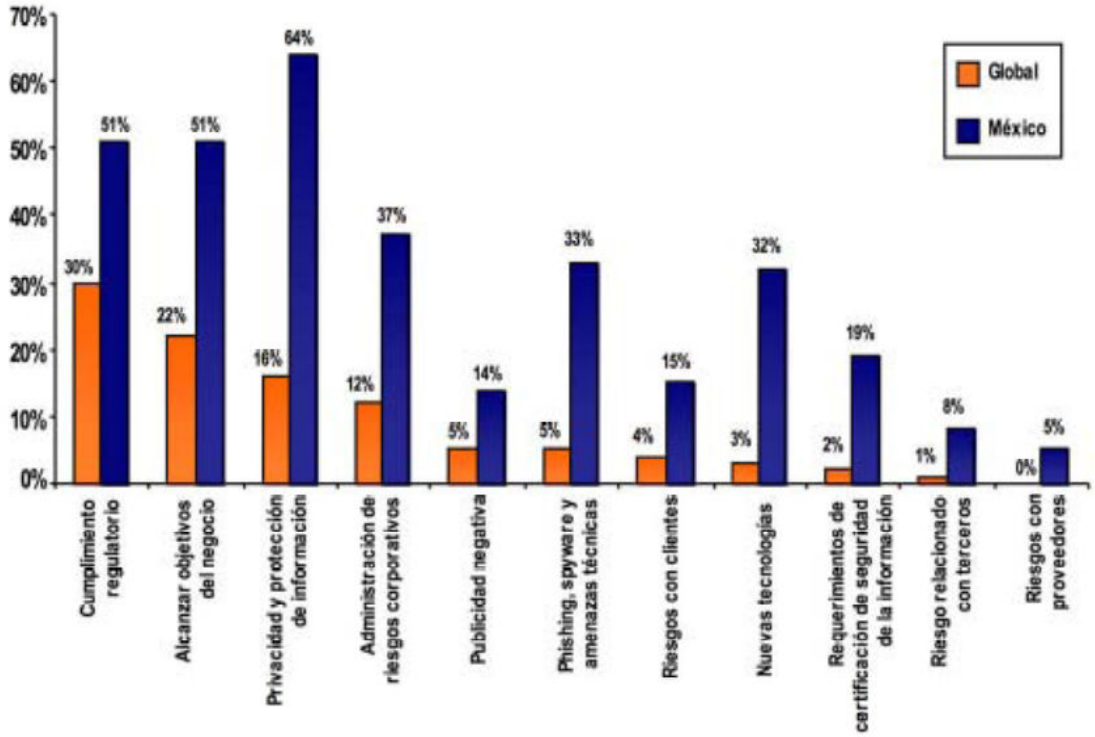


Figura A.4 Gráfica de resultados habilitadores que han tenido un impacto significativo en las prácticas de seguridad de la información.

Por consecuencia de la pregunta anterior, queda en claro que en México y la tendencia mundial en general, que los principales prácticas que habilitan la seguridad de información en el negocio: son ***la privacidad y protección de la información, el cumplimiento regulatorio, y alcance de los objetivos del negocio.***

Con especial énfasis, considerando estos dos últimos, ya que se está reconociendo a la seguridad de la información como una función importante para el negocio, inclusive a nivel de cumplimiento con los objetivos estratégicos.

4ª.- ¿Qué tan importante es la función de seguridad de la información para soportar los siguientes esfuerzos?

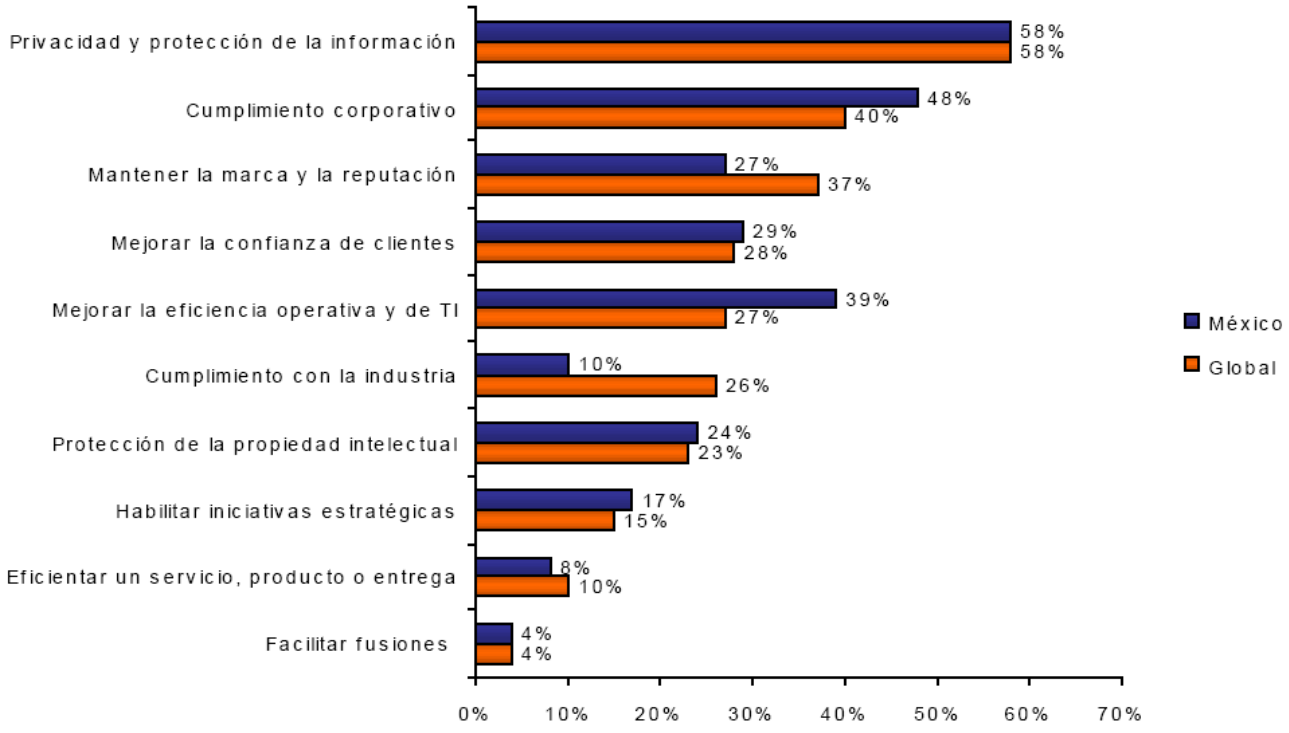


Figura A.5 Gráfica de resultados de la importancia de la función de la seguridad de la información en el apoyo de diversos rubros.

Tanto a nivel global, como en nuestro país, la mayor parte de las organizaciones reconoce que la administración de la privacidad y la protección de la información es el proceso más importante que está siendo soportado por la función de seguridad de la información. Asimismo, es relevante hacer mención que el tercer lugar en México está siendo ocupado por la eficiencia operativa y de TI, lo cual permite romper el paradigma que la seguridad de la información únicamente genera una sobrecarga a las operaciones del negocio.

5ª.- Indique en qué grado está de acuerdo o en desacuerdo con los siguientes planteamientos

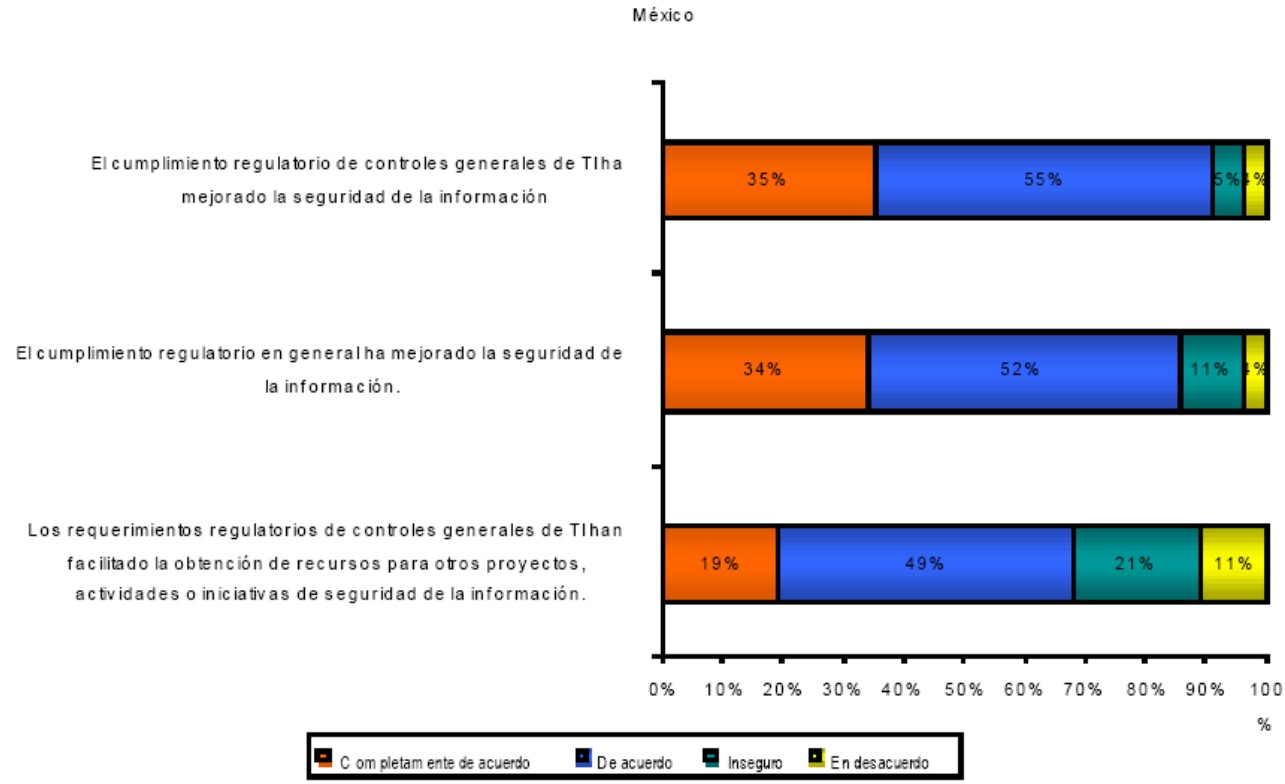


Figura A.6 Gráfica de resultados del grado de acuerdo o desacuerdo con respecto al cumplimiento regulatorio y los controles generales.

Hoy en día se reconoce que el cumplimiento regulatorio si ha beneficiado y ayudado a la mejora de la seguridad de la información. En México, casi 9 de cada 10 participantes en esta encuesta, están de acuerdo con esto (figura 1.8). Inclusive, casi 70% afirma que el cumplimiento regulatorio ha facilitado la obtención de recursos para actividades y/o proyectos relacionados con la seguridad de la información.

6ª.- ¿Cuáles son las regulaciones que más han afectado a las prácticas de seguridad de la información en su organización en los últimos 12 meses?

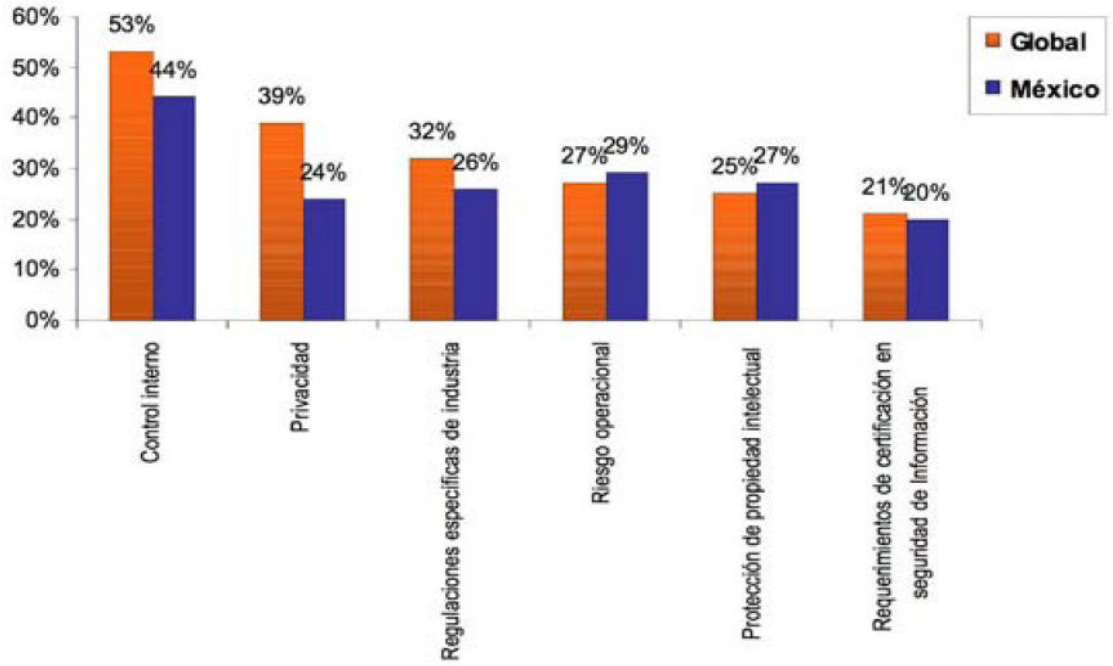


Figura A.7 Gráfica de resultados de las regulaciones que más han afectado a las prácticas de seguridad de la información en su organización en los últimos 12 meses.

Las regulaciones que más han impactado a las prácticas de seguridad de la información son las relacionadas con ***Control Interno,*** por ejemplo: Sarbanes-Oxley. También existen otras regulaciones como aquellas vinculadas con privacidad, las cuales ocupan el segundo lugar en importancia a nivel global, sin embargo, en México ocupan un rezagado quinto lugar a causa de la ausencia de un marco regulatorio robusto en esta materia.

Radica aquí la importancia de contar con una metodología basada en el marco de referencia CobIT; (del cual se basa principalmente la ley del Sarbanes Oxley) como medio de impulsar y robustecer las leyes sobre privacidad que obliguen a las organizaciones a proteger la información personal de empleados y, en general, de los ciudadanos. De tal manera, que permita Iniciar el camino de la prevención para los contiguas exigencia regulatorias en materia de seguridad de información.

7ª.- ¿Cuáles son las actividades que se han identificado como preocupación de seguridad de la información?

Preocupaciones de seguridad	¿Que le preocupa y cuándo lo atendera?							
	Global				México			
	Preocupa	Hoy	Próximos 12 meses	No preocupa	Preocupa	Hoy	Próximos 12 meses	No preocupa
Medios removibles (ej. USB flash drive, portable drives)	52% (1)	27% (1)	23% (1)	8% (1)	62% (1)	35% (1)	18% (1)	21% (1)
Cómputo movil (ej. PDA, smart phones)	40% (2)	24% (2)	18% (2)	6% (2)	37%	19%	17%	14%
Aplicaciones WEB	37% (3)	28% (3)	13% (3)	3% (3)	37%	31%	13%	6%
Redes inalámbricas	35%	24%	15%	4%	60% (2)	13% (2)	23% (2)	8% (2)
Encripción de disco duro	27%	17%	14%	6%	29%	18%	14%	17%
Servicios de mensajería (ej. Instant messaging, email)	26%	19%	9%	4%	29%	14%	13%	8%
Convergencia entre seguridad lógica y física	24%	13%	12%	7%	38% (3)	15% (3)	18% (3)	14% (3)
Servicios WEB	22%	17%	9%	3%	26%	17%	12%	7%
Encripción de correo electrónico	22%	12%	11%	6%	21%	14%	7%	13%
Telefonía por IP	13%	9%	10%	6%	24%	17%	15%	10%
Virtualización de servidores	13%	11%	8%	4%	25%	17%	15%	6%
Nuevos sistemas operativos (ej. Vista)	11%	5%	10%	6%	15%	7%	13%	12%
Administración de patentes y dispositivos digitales	9%	5%	7%	9%	8%	5%	6%	19%
Identificación de radio frecuencia (RFID)	4%	2%	4%	12%	5%	4%	8%	19%

Primer lugar (1)
Segundo lugar (2)
Tercer lugar (3)

Figura A.8 Gráfica de resultados de las actividades que son una preocupación para la seguridad de la información.

Por otro lado, las tres preocupaciones para la seguridad de la información de las organizaciones mexicanas son, en orden de relevancia: ***medios removibles, redes inalámbricas y la convergencia entre seguridad lógica y física***.

Sin embargo, a nivel global, además de los medios removibles, el cómputo móvil y las ***aplicaciones web*** representan las mayores preocupaciones. Por lo cual, las organizaciones mexicanas deben de colocar atención en la tendencia global, ya que hoy en día las aplicaciones web están siendo muy utilizadas para el soporte a procesos de negocio, por lo que el diseño, evaluación y monitoreo de seguridad de las mismas se vuelve indispensable. Además, es cada vez más común el robo de información a través de cómputo móvil.

8ª.- ¿Cómo se está evaluando la postura de la seguridad de la información en su organización?

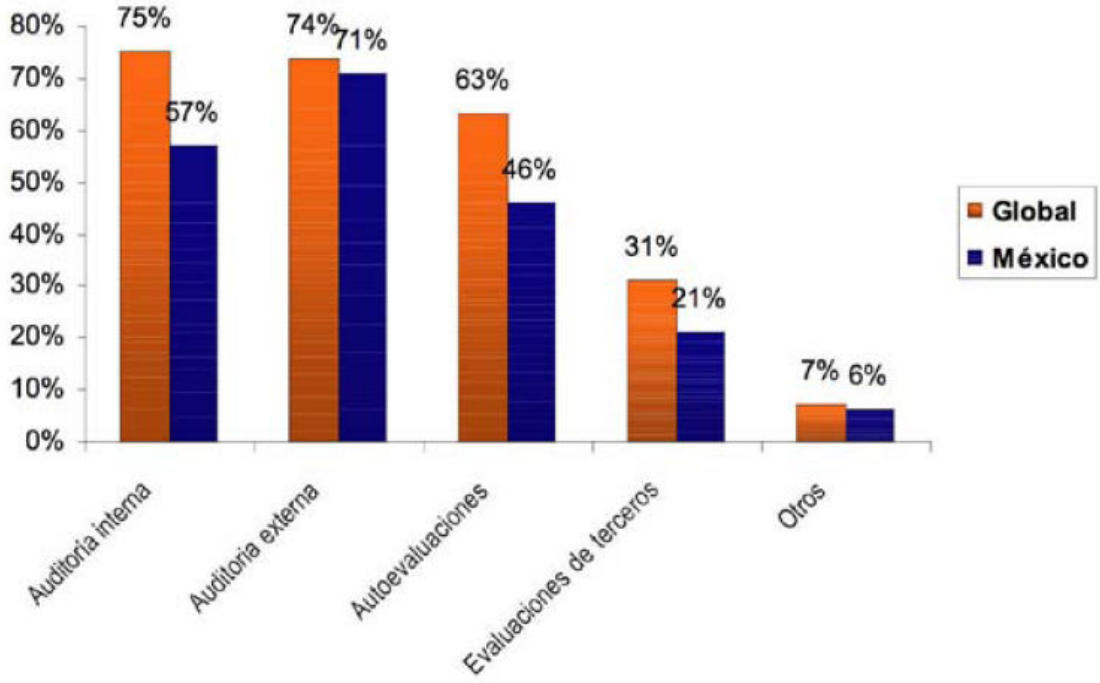


Figura A.9 Gráfica de resultados de las posturas de evaluación para la seguridad de la información en las organizaciones.

Los resultados muestran que las organizaciones están buscando formas de evaluar y administrar la seguridad de la información de manera más efectiva. La postura de seguridad en las organizaciones está siendo evaluada principalmente por ***auditoría interna o externa***. Sin embargo, ambas funciones realizan evaluaciones ***con un enfoque orientado más a temas financieros*** que operativos y/o estratégicos y cuyo objetivo principal es la integridad de la información, pero no necesariamente la confidencialidad y disponibilidad de la misma. Por lo anterior, es muy probable que la seguridad de la información no esté siendo evaluada en forma integral y con la profundidad requerida.

Es importante reiterar que un adecuado análisis de riesgos de seguridad de la información es el principal insumo para diseñar e implementar una estrategia de seguridad de la información, alineada a los objetivos del negocio, que permita la protección de los activos de información relevantes para la organización.

9ª.- ¿Cuáles son los beneficios aportados a su organización como resultado de la adopción de estándares de seguridad de la información?

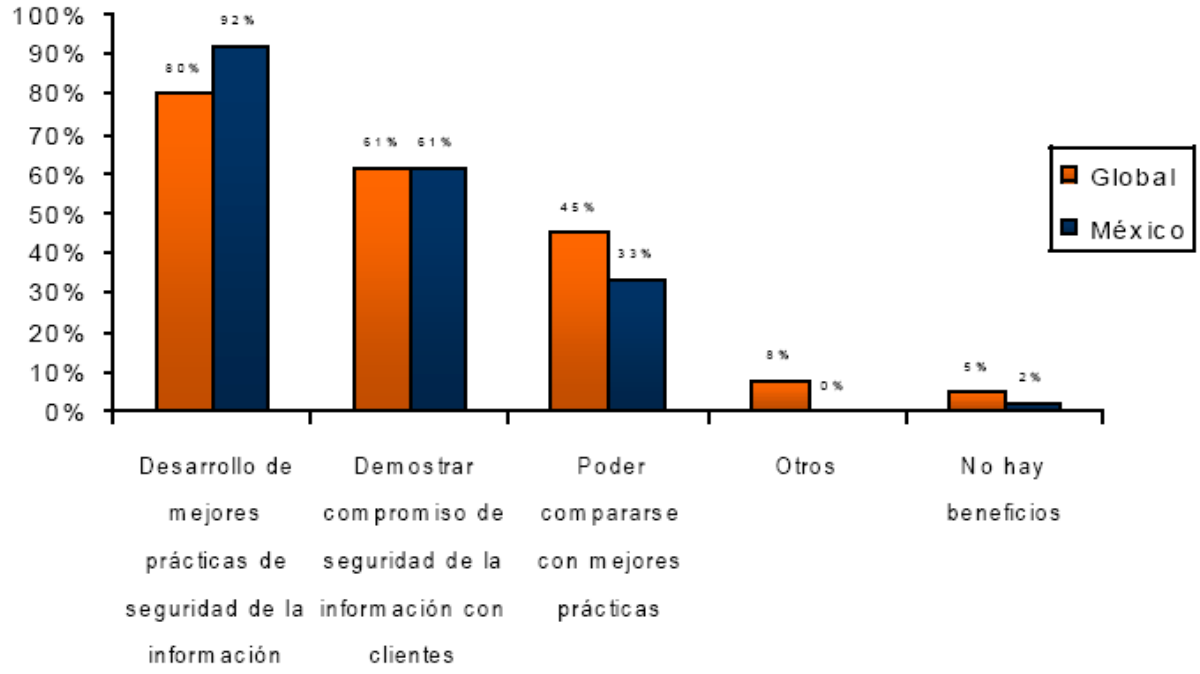


Figura A.10 Gráfica de resultados de los beneficios obtenidos por la adopción de estándares para la seguridad de la información.

Y para concretar; la adopción y alineamiento con estándares de seguridad, va en incremento, ya que se reconocen los beneficios de los mismos, siendo los principales: desarrollo de mejores prácticas y demostrar el compromiso con la seguridad de la información a los clientes y/o socios de negocio [Ernst & Young, 2007].

En síntesis, y acorde a las interrogantes anteriores; se puede asumir que la información representa uno de los activos más valiosos de las empresas, y como ésta se encuentra alojada en los sistemas de información de las mismas, ha convirtiendo a las TI en los soportes principales de las operaciones empresariales, por ello, es preciso que las empresas ofrezcan un ambiente de seguridad a está área.

LEY SARBANES – OXLEY.

B.1 SÍNTESIS DE LA LEY SARBANES – OXLEY.

La seguridad no es considerada como una necesidad primordial para algunas instituciones, ya que con excesiva frecuencia la conforman de manera informal y no generan procedimientos, manuales y políticas que permitan llevar de manera seria las funciones y responsabilidades de la organización.

Esta escasez de seguridad a originado grandes escándalos financieros contables de algunas empresas estadounidenses como son WorldCom, Enron entre otras, en las cuales se cometieron fraudes al presentar información falsa que favorecía la situación de capital líquido de la empresa; afectando sensiblemente la confianza de los accionistas; fue así requerida la producción de una nueva ley que diera transparencia a las actividades empresariales devolviendo la fiabilidad de la información e imponiendo nuevas prácticas corporativas.

Esta ley denominada Sarbanes - Oxley, SOx ó SarbOx debido a sus creadores, fue producida el 30 de julio del 2002 en los Estados Unidos, está conformada por 11 apartados que abarcan desde responsabilidades adicionales a las ya existentes para los comités de auditoria, hasta penas de cárcel por fraude.

Figura. B.1 Fotografía de Paul S. Sarbanes y Michael G. Oxley

El ***contenido*** principal de esta ley se agrupa en seis grandes áreas que afectan a todas las empresas cotizadas en los mercados americanos.

1. Mejora en la calidad de la información pública y en los detalles de la misma.
2. Reforzamiento de responsabilidades en el Gobierno Corporativo de las sociedades.
3. Mejora en las conductas y comportamientos éticos exigibles: mayores exigencias de responsabilidad en los temas de gestión indebida de información confidencial.
4. Aumento de la Supervisión a las actuaciones en los mercados cotizados.
5. Incremento del régimen sancionador asociado a incumplimientos.
6. Aumento de exigencia y presión sobre la independencia efectiva de los auditores.

[SOX, 2008]

Su ***objetivo*** es monitorear a las empresas que cotizan en bolsa de valores de Estados Unidos, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad no solo es regular los aspectos financieros o contables, ***busca que el proceso operativo de la empresa sea transparente y que haya consistencia entre las cifras y la información.*** Obligando a las empresas a implementar un estricto control interno en sus operaciones.

Mantenerse dentro de los márgenes de la Ley Sarbanes-Oxley requiere que toda la información financiera sea precisa, esté actualizada y sea completamente verificable por lo tanto, el departamento de TI y sus sistemas son los responsables de generar, soportar y mantener esa información. En consecuencia, esos mismos sistemas garantizarán la validez y disponibilidad de los datos.

Cumplir la Ley Sarbanes-Oxley y mantenerse ahí, demanda que las organizaciones evalúen sus controles internos y demuestren su efectividad a través de la generación de informes fiscales correspondientes.

Los ***aparatos*** que están relacionadas con ***el control interno*** son las siguientes:

Sección 302: En el artículo 302 de la Ley habla acerca de los funcionarios que firmaran y darán validez a los procedimientos internos con el fin de asegurar la transparencia financiera.

Sección 404*:* el artículo 404 de la Ley Sarbanes-Oxley habla acerca de la exigencia de redactar un informe de control interno al final de cada ejercicio fiscal. Dentro de este informe de control interno se establece la responsabilidad del equipo directivo de tener una estructura de control interno adecuada. Anteriormente esta exigencia no existía y ahora el equipo directivo es responsable ante posibles fraudes.

Sección 906: El artículo 906 de la Ley Sarbanes-Oxley establece una nueva disposición en el código penal donde se especifican las multas y penas para los responsables legales de infracción de los requerimientos expuestos en la Ley Sarbanes-Oxley. [SOX1, 2008]

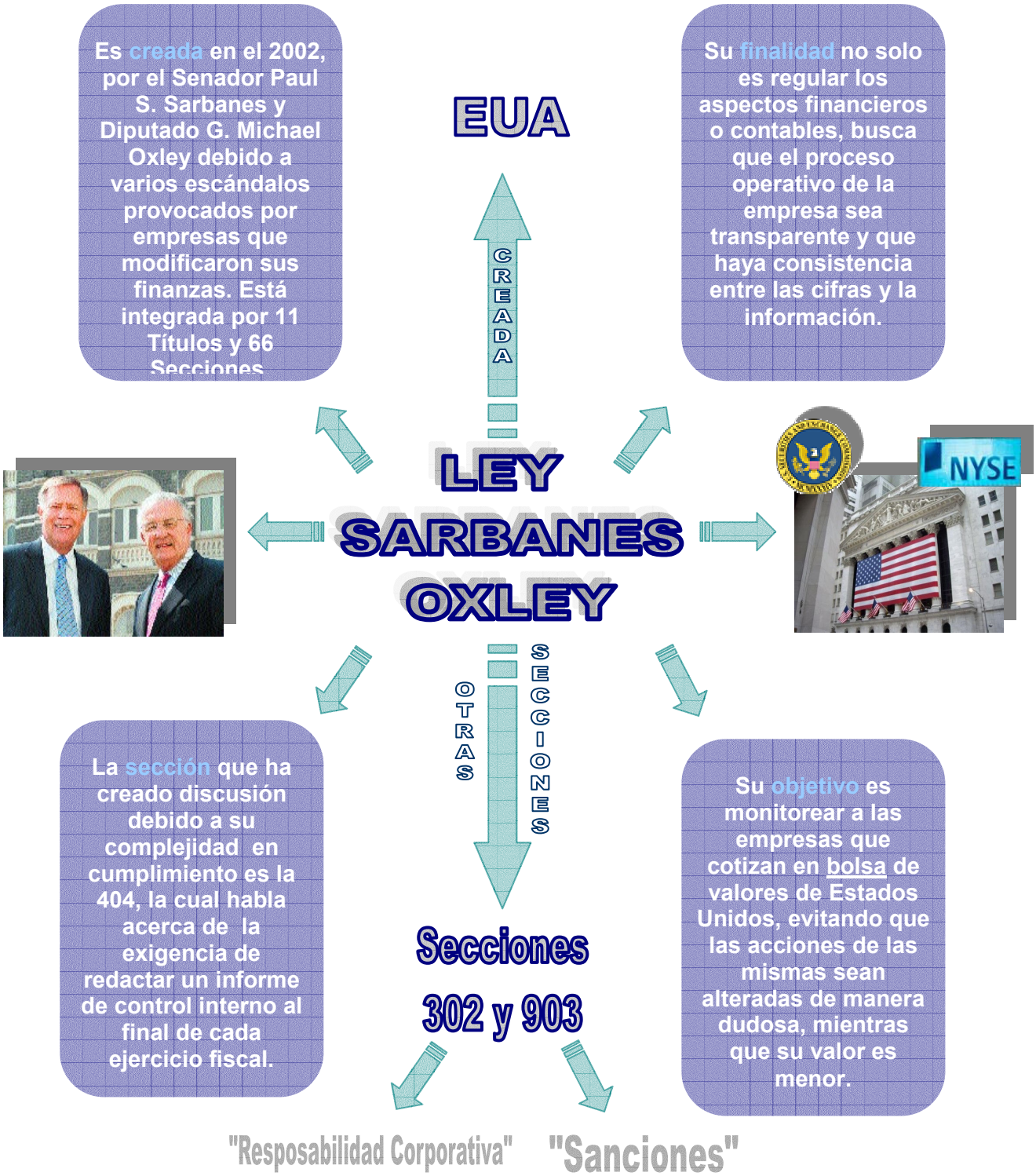


Figura. B.2 Mapa mental de la Ley Sarbanes – Oxley [Fuente propia].

CONTROL INTERNO.

Para comprender con claridad los temas a tratar durante el desarrollo de ésta tesis, es necesario conocer una diversidad los conceptos que serán abordados, comenzando con el Control Interno.

C.1 DEFINICIÓN DE CONTROL INTERNO.

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos.

Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

No todas las personas entienden lo mismo por "Control Interno", esto se agrava cuando sin estar claramente definido se utiliza en la normatividad.

En sentido amplio, se define como: ***un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:***

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes y normas aplicables.

La anterior definición refleja ciertos conceptos fundamentales:

- El Control Interno es un ***proceso,*** un medio utilizado para la consecución de un fin, no un fin en sí mismo.
- El Control Interno lo llevan a cabo las ***personas***, no se trata solamente de manuales de políticas e impresos, sino de ***personas*** en cada nivel de la organización.
- El Control Interno sólo puede aportar un ***grado de seguridad razonable,*** no la seguridad total, a la Dirección y al Consejo de Administración de la Entidad.
- El Control Interno esta pensado para facilitar la consecución de ***objetivos*** propios de cada entidad.

C.2 LA ESTRUCTURA DEL CONTROL INTERNO.

Otra definición de el Control Interno de acuerdo al autor Juan Ramón Santillana Gonzáles “comprende el plan de organización y todos los métodos y procedimientos que en forma cotidiana son adoptados por una entidad para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera y la complementaria administrativa y operacional, promover eficiencia operativa y estimular la adhesión a las políticas preescritas por la administración” [Santillana, 2003].

El Control Interno **consta de cinco componentes relacionados entre sí,** se derivan de la manera en que la dirección dirige la empresa y están integrados en el proceso de dirección, los componentes del Control son:

1. El Ambiente De Control
2. La Evaluación De Riesgos
3. Los Sistemas De Información Y Comunicación
4. Los Procedimientos O Actividades De Control
5. Supervisión Ó Vigilancia

Los cuales se detallan a continuación:

1.- Ambiente de control.

El ambiente de control sirve de base para todos los otros componentes de la gestión de riesgos, proporcionando la disciplina y la estructura.

El ambiente de control influye en la estrategia y en los objetivos establecidos, estructurando las actividades del negocio, identificando, evaluando e interpretando los riesgos. Es decir, que el ambiente de control incide sobre el funcionamiento de las actividades de control, la información, los sistemas de comunicación y las actividades de supervisión.

Como parte del ambiente de control, la dirección establece filosofía de gestión de riesgos, determinando el grado de riesgo que asumirá la organización. Se entiende como grado de riesgo que la organización está dispuesta a aceptar para el logro de su objetivo.

2.- Evaluación de riesgos.

La evaluación de riesgos permite a la organización considerar los potenciales acontecimientos que pudieran afectar el logro de los objetivos. La probabilidad representa la posibilidad que un acontecimiento ocurra, mientras que el impacto representa su efecto.

La metodología de evaluación de riesgos de una organización normalmente comprende una combinación de técnicas cualitativas y cuantitativas. En aquellos casos donde los riesgos no son cuantificables, o cuando no se poseen datos suficientes y creíbles para evaluaciones cuantitativas, a menudo se utilizan solo técnicas de evaluación cualitativa, sin embargo, no se debe olvidar que la cuantificación brinda mayor precisión en la evaluación de riesgos.

Al momento de evaluar los acontecimientos no se debe realizar individualmente, sino que se debe tener en cuenta la correlación que pudiera existir entre distintos acontecimientos y las secuencias de acontecimientos que se combinan e interactúan para crear los impactos sobre la organización.

3.- Sistemas de información y comunicación.

La información, tanto interna como externa, debe ser identificada, captada y comunicada en tiempo y forma para poder así evaluar los riesgos y establecer la respuesta a los mismos.

Dado que la información se origina en diversas fuentes (internas, externas) y tiene diferentes características (cualitativa, cuantitativa), se genera un gran desafío que es el de contar con un gran volumen de información, del que deberá ser captada la información relevante, procesada y trasmitida de tal modo que llegue oportunamente a todos los sectores, permitiendo asumir las responsabilidades individuales.

4.- Actividades de control.

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que la respuesta a los riesgos sea correctamente efectuada. Las actividades de control ocurren en todos los niveles y funciones de la organización.

5.- Supervisión ó Vigilancia.

La gestión de riesgos deber ser supervisado, y tal supervisión puede hacerse en tiempo real o a posteriori, siendo la primera forma la más eficaz.

Una vez que tenemos un enfoque acerca de lo que es el control interno, podemos retomar que es una actividad que comúnmente se lleva a cabo en las empresas, y que a través de la implementación, desarrollo y cumplimiento de objetivos se efectúa. Este puede estar inherente, es decir, que se encuentra ahí por naturaleza, simplemente por que existe algún tipo de control dentro de la empresa; o puede estar de manera formal, en el cual se pude encontrar ampliamente documentado mediante políticas, procedimientos, manuales, descripciones, entre otras formas de documentación.

El control interno es aplicable para todos los niveles y áreas de la organización; ya que en todas estas áreas se realizan actividades y procesos recurrentes, quienes se ejecutan para cumplir con metas y objetivos, los cueles son monitoreados para evaluar su nivel de desempeño, basándose en políticas y planes y deben existir dueños de cada actividad y proceso quienes se han responsables de la ejecución de estos mismos.

Estos últimos términos son mencionados con el fin de dar a conocer que cada proceso que se desarrolla en cualquier entidad empresarial se desenvuelve de esta manera.

Algunas áreas donde se efectúa el control interno son Compras, Ventas, Capital Humano, Almacén, Inventarios, Tecnologías de Información, etc; este último, jugando un papel muy importante en la actualidad, ya que soportan gran parte de la información que se maneja dentro de la empresa [COSO, 2008].

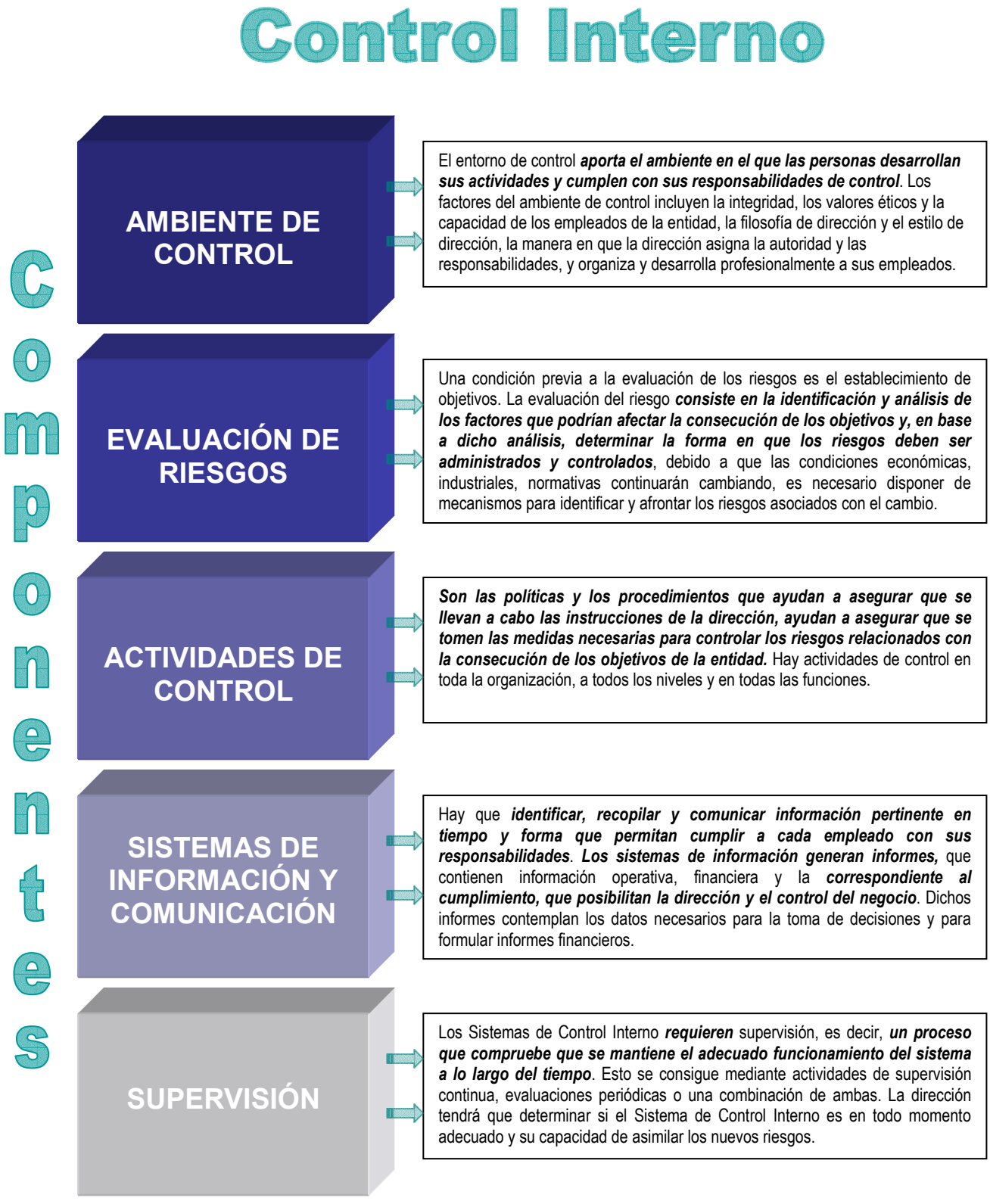


Figura. C.1. Mapa mental del Control Interno [Fuente propia].

EL OFICIAL DE SEGURIDAD INFORMÁTICA.

D.1 DEFINICIÓN.

El Oficial de seguridad informática (OSI), es la persona responsable de planear, coordinar y administrar los procesos de seguridad informática en una organización

D.2 MISIÓN.

El Oficial de seguridad informática tiene la función de brindar los servicios de seguridad en la organización, a través de la planeación, coordinación y administración de los procesos de seguridad informática, así como difundir la cultura de seguridad informática entre todos los miembros de la organización.

D.3 OBJETIVOS.

- ☑ Definir la misión de seguridad informática de la organización en conjunto con las autoridades de la misma.

- ☑ Aplicar una metodología de análisis de riesgo para evaluar la seguridad informática en la organización.
- ☑ Definir la Política de seguridad informática de la organización.
- ☑ Definir los procedimientos para aplicar la Política de seguridad informática.
- ☑ Seleccionar los mecanismos y herramientas adecuados que permitan aplicar las políticas dentro de la misión establecida.
- ☑ Crear un grupo de respuesta a incidentes de seguridad, para atender los problemas relacionados a la seguridad informática dentro de la organización.
- ☑ Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad informática dentro de la organización.
- ☑ Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad en la organización.
- ☑ Crear un grupo de seguridad informática en la organización.

D.4 FORMACIÓN.

- ☑ Licenciatura en el área de cómputo.

- ☑ Contar con conocimientos sólidos en el ámbito de la informática en:

    - Equipos de cómputo,
    - Redes y arquitectura,

- Servidores,
- Sistemas Operativos,
- Sistemas de administración de Bases de Datos,
- Protocolos de Comunicación y
- Lenguajes de Programación.

☑ Nociones en:

- Ambiente de Seguridad,
- Cultura y Auditoría de TI,
- Herramientas y Mecanismos de Seguridad y
- Estándares y Legislaciones.

[Perfil OSI, 2003]

GRÁFICA RACI ó RASCI.

E.1 SÍNTESIS DE LAS GRÁFICAS RACI.

En el caso de que no se conozcan las funciones con claridad, un medio de apoyo para definir cada proceso y sus funciones son las gráficas RACI proporcionadas por el marco de referencia COBIT, esta técnica permite entender los roles y responsabilidades del personal involucrado, es decir, ilustra genéricamente y de acuerdo a cada proceso quién es el responsable, quién debe rendir cuentas, a quien se debe consultar e informar dentro de un marco de trabajo organizacional estándar. (Rendir cuentas significa “la responsabilidad termina aquí”, esta es la persona que provee la autorización y direccionamiento a una actividad).

Estas gráficas proporcionan entendimiento para cada proceso, qué actividades son necesarias para este proceso y qué personas están encargadas de realizar estas actividades.

Los pasos para su elaboración son loa siguientes:

1. Identifique todos los procesos / actividades implicados y enumérelos en el lado izquierdo del gráfico (Filas).

2. Identifique todos lo roles / responsabilidades y enumérelos en el lado superior del gráfico. (Columnas)

3. Complete las celdas del gráfico: identifique quién tiene el rol / responsabilidad de a cuerdo a las iniciales R, A, S, C, I para cada proceso.

R = Responsible (encargado). La persona que realiza la actividad.

A = Accountable. Es ante quien "R" debe reportarse, quien debe firmar o aprobar la actividad o rol antes de que sea ACEPTADO.

S = Supportive (puede ser de apoyo). Puede proporcionar recursos o puede desempeñar un papel al apoyar la puesta en práctica. (Puede que exista o no este rol).

C = Consulted (es quien debe ser consultado). Tiene la información y/o la capacidad necesaria para terminar la actividad/ proceso.

I = Debe ser informado. Debe ser notificado de los resultados, pero no necesita ser consultado.

Estos tres últimas roles (Apoyo, Consultado e informado) garantizan que todas las personas que son requeridas están involucradas y dan soporte al proceso.

4. Resuelva los traslapes. Cada proceso en el mapa de roles de responsabilidad debe contener solamente un "R" para indicar un dueño único del proceso. En el caso que resulten múltiples "R", hay necesidad de detallar aún más los procesos secundarios, para separar las responsabilidades individuales.

5. Resolución de separaciones. Donde no se ha identificado ningún rol "R" par un proceso, se debe identificar quien tiene la autoridad para la definición del rol y se deberá determinar la existencia del rol y el nuevo responsable.

La Gráfica RACI requiere de actualizaciones continuas y de clarificar e informar los roles para que cada individuo asuma su responsabilidad.

Esta técnica proporciona un enfoque consistente de funciones y responsabilidades. Reduce duplicación de esfuerzos y contradicciones, y mejora los resultados al eliminar confusiones.

Gráfica RACI Funciones

Actividades	CEO	CFO	Ejectivo del negocio	CIO	Prop. de proceso del negocio	Jefe de operaciones	Arquitecto en jefe	Jefe de desarrollo	Jefe de administración de TI	PMO	Cumplimiento, auditoria riesgo y seguridad
Crear y mantener modelo de información corporativo / empresarial		C	I	A	C		R	C	C		C
Crear y mantener diccionario de datos corporativo				I	C		A/R	R			C
Establecer y mantener esquema de clasificación de datos	I	C	A	C	C	I	C	C			R
Brindar a los propietarios procedimientos y herramientas para clasificar sistemas de información	I	C	A	C	C	I	C	C			R
Usar el modelo de información, el diccionario de datos y el esquema de clasificación para planear los sistemas optimizados de negocio	C	C	I	A	C		R	C			I

Una gráfica RACI identifica quién es Responsable, quién debe rendir cuentas (A), quién debe ser Consultado y/o Informado

Figura. E.1 Ejemplo de la Gráfica de RACI [COBIT, 2005]

DIAGRAMA DE FLUJO DE DATOS.

F.1 SÍNTESIS DE LA ELABORACIÓN DE UN DIAGRAMA DE FLUJO DE DATOS.

El Diagrama de Flujo de Datos (DFD), es una representación gráfica del "flujo" de datos a través de un sistema de información. Cuando se sigue su flujo a través de los procesos del negocio, que es el propósito del análisis de flujo de datos, le proporciona a los analistas una gran cantidad de información, sobre como se esta llevando a cabo las funciones, las actividades y objetivos de la compañía.

La clasificación general que puede ser empleada de acuerdo al detalle de los procesos es la siguiente:

Nivel 0 Diagrama de contexto: En el diagrama de contexto solo se dibuja el proceso principal y los flujos entre este y sus entidades externas.

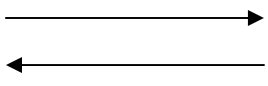
Nivel 1 Diagrama de nivel superior: En el diagrama de nivel superior se plasman todos los procesos que describen al proceso principal. En este nivel los procesos no pueden interrelacionarse directamente, sino que entre ellos siempre debe existir algún almacenamiento o entidad externa que los una.

Nivel 2 Diagrama de detalle o expansión: A partir del nivel 2 de detalle, los procesos pueden interrelacionarse directamente, sin necesidad de almacenamiento que los una. Cabe destacar que en el nivel 1 y 2 siempre los procesos deben tener las entradas y las salidas dadas en el diagrama de contexto.

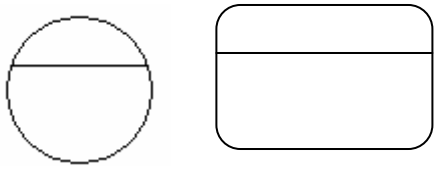
Los DFD, al ser una técnica que emplea conceptos gráficos, su fundamento es el uso de símbolos iconográficos cuyo formato se presenta a continuación:

FLUJO DE DATOS: Los datos cambian o se procesan o transforman o se usan o consultan, en una dirección especifica desde su origen hasta su destino, en forma de un documento, carta, llamada telefónica o cualquier otro medio.

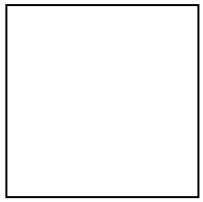
El flujo de datos es un “paquete” o “grupo” de datos y se representan por medio de flechas, que se etiquetan con el nombre de datos o grupo de datos.



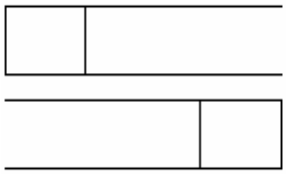
PROCESOS: El personal, procedimientos o dispositivos, utilizan, producen o transforman datos. Aquí no se identificará el componente físico, que realiza la transformación. Los procesos se representan por medio de círculos o recuadros redondeados.



ORIGEN O DESTINO DE LOS DATOS: El origen externo o interno, o destino de los datos, los cuales pueden ser: individuos, programas, procesos, empresas u otras entidades, interactúan con el sistema, pero están fuera de su límite, en cierta forma determinan la frontera del sistema o subsistema o del proceso. Se representa por medio de un rectángulo o cuadro.



LUGAR DE ALMACENAMIENTO DE DATOS: Los datos se almacenan o se hace referencia a ellos a través de un proceso dentro del sistema. Este símbolo, puede o no representar dispositivos de computadoras, es más bien el concepto de almacenamiento de la información. Se representan por un símbolo, en forma de rectángulo sin una arista.



En el diagrama, cada componente: flujo de datos, procesos, origen o destino y lugar de almacenamiento de datos, se etiqueta con un nombre descriptivo. Los procesos y los lugares de almacenamiento se identifican además, con un número que se realiza para propósitos de identificación. Este número no necesariamente, representa la secuencia del proceso.

A continuación se presentan las actividades a desarrollar para elaborar un diagrama de flujo de datos:

1. Revisar la documentación previa de apoyo, estudiando las operaciones y procesos en marcha.

2. Identificar como se procesan los datos al manejar las transacciones y terminar las tareas.

3. Seguir el flujo de datos:

    - Entrada.
    - Proceso.
    - Almacenamiento.
    - Recuperación.
    - Salida.

Añadir gradualmente, detalles a los niveles inferiores (procesos descendentes) [Galindo, 2006]

El DFD es una técnica que puede ayudar a comprender:

- ☑ Las actividades, tares y pasos que conforman cada proceso.
- ☑ De estas actividades, se puede identificar las que pueden darle un valor agregado a la empresa o aquellos que están ocasionando un problema.
- ☑ Y en general, obtener un panorama integral de los procesos y la interconexión entre estos.

En la figura siguiente se muestra un diagrama de flujo de datos nivel 0:

Figura. F.1 Ejemplo de un diagrama de flujo de datos Nivel 0.

EVALUACIÓN DEL RIESGO: USO DE LA TÉCNICA CUANTITATIVA PROPUESTA POR MICROSOFT.

G.1 INTRODUCCIÓN.

El siguiente anexo está basado en la guía de administración de riesgos que propone Microsoft [Microsoft, 2004], y trata acerca de la evaluación de riesgo cuantitativa la cual se verá a nivel resumen, ya que este tópico es muy extenso y debido a que las intenciones de este trabajo de tesis recaen esencialmente en el uso, desarrollo e implantación de los controles, por lo tanto, no se profundizará en el tema.

G.2 LA EVALUACIÓN CUANTITATIVA.

En las evaluaciones de riesgos cuantitativas, el objeto es intentar calcular valores numéricos en donde se estima el valor verdadero de cada activo del negocios en función de lo que costaría reemplazarlo, lo que costaría en pérdida de productividad, lo que costaría en reputación de marca y en otros valores de negocios directos e indirectos.

Existen algunos puntos débiles importantes que son inherentes a esta evaluación y que no se pueden solventar fácilmente:

a) No existe un modo formal y riguroso de calcular de forma eficaz los valores de los activos y de los controles.

b) Las organizaciones que han intentado aplicar meticulosamente todos los aspectos de la gestión de riesgos cuantitativa han comprobado que el proceso es excesivamente costoso, suelen tardar mucho tiempo en completar su primer ciclo completo y normalmente implican a muchos miembros del personal con discusiones acerca de cómo se han calculado los valores fiscales específicos.

c) En organizaciones con activos de alto valor, el costo de exposición puede ser tan alto que se gastaría una enorme cantidad de dinero en mitigar los riesgos a los que estuvieran expuestas. Pero esto no es realista, una organización no gastaría todo su presupuesto en proteger un solo activo, ni siquiera los cinco principales.

G.2.1 Detalles del enfoque cuantitativo.

En esta parte se examinan algunos de los factores y valores que normalmente se evalúan durante una evaluación de riesgos cuantitativa, como la valoración de activos, el costo de los controles, la determinación del rendimiento de la inversión en seguridad

(ROSI) y el cálculo de valores para la expectativa de pérdida simple (SLE), la frecuencia anual (ARO) y la expectativa de pérdida anual (ALE). No se trata en absoluto de un examen exhaustivo de todos los aspectos de la evaluación de riesgos cuantitativa, sino de un breve examen de algunos detalles de dicho enfoque para que compruebe que las cifras que conforman la base de todos los cálculos son subjetivas en sí mismas.

G.2.1.1 Valoración de activos.

La determinación del valor monetario de un activo es una parte importante. A menudo, los directores se basan en el valor de un activo como orientación para determinar el dinero y tiempo que deben invertir para protegerlo. Muchas organizaciones conservan una lista de valores de los activos como parte de los planes de continuidad de negocios. (Ver el tema G.3 en este anexo, acerca de una propuesta de lista de valores de activo).

No obstante, las cifras calculadas en realidad son estimaciones subjetivas: no existe ninguna herramienta o método para determinar el valor de un activo. Para asignar un valor a un activo, se deben calcular los tres factores principales siguientes:

- El valor global del activo en la organización. Calcule o estime el valor del activo en términos financieros directos. Consideremos el ejemplo simplificado de las repercusiones de la interrupción temporal de un sitio Web de comercio electrónico que normalmente funciona siete días a la semana, 24 horas al día, y que genera un promedio de 2.000 dólares por hora en ingresos procedentes de los pedidos de los clientes. Puede establecer con seguridad que el valor anual del sitio Web en términos de ingresos por ventas es de 17.520.000 dólares.

- La repercusión financiera inmediata de la pérdida del activo. Si simplificamos deliberadamente el ejemplo anterior y suponemos que el sitio Web genera una tasa constante por hora y el mismo sitio Web deja de estar disponible durante seis horas, la exposición calculada es de un 0,000685% por año. Al multiplicar este porcentaje de exposición por el valor anual del activo, podrá predecir que las pérdidas directamente atribuibles en este caso serían de 12.000 dólares. En realidad, la mayoría de los sitios Web de comercio electrónico generan ingresos con unas tasas muy distintas según la hora del día, el día de la semana, la estación, las campañas de publicidad y otros factores. Además, algunos clientes pueden encontrar un sitio Web alternativo que prefieran al original, por lo que dicho sitio Web puede tener una pérdida de usuarios permanente. En realidad, calcular la pérdida de ingresos resulta bastante complejo si se quiere ser preciso y tener en cuenta todos los tipos posibles de pérdida.

- La repercusión de negocios indirecta de la pérdida del activo. En este ejemplo, la empresa estima que gastará 10.000 dólares en publicidad para contrarrestar la propaganda negativa de una incidencia. Asimismo, la empresa también estima una pérdida de un 0,01% a un 1% de ventas anuales, o 17.520 dólares. Mediante la combinación de los gastos de publicidad adicionales y de la pérdida ingresos por ventas anuales, en este caso se puede predecir un total de 27.520 dólares en pérdidas indirectas.

G.2.1.2 Determinación de la expectativa de pérdida simple (SLE).

La expectativa de pérdida simple es la cantidad total de ingresos que se pierde por una única incidencia del riesgo. Se trata de un importe monetario que se asigna a un único suceso que representa la cantidad de pérdida potencial de la empresa, en caso de que una amenaza específica aproveche una vulnerabilidad. (La expectativa de pérdida simple es similar a la repercusión de un análisis de riesgos cualitativo.) Calcule dicha expectativa multiplicando el valor del activo por el factor de exposición. Dicho factor representa el porcentaje de pérdida que una amenaza realizada podría suponer para un determinado activo. Si un conjunto de servidores Web tiene un valor de activo de 150.000 dólares y un incendio provoca daños estimados en el 25% de su valor, en este caso la expectativa de pérdida simple será de 37.500 dólares. No obstante se trata de un ejemplo muy simplificado, ya que es necesario tener en cuenta otros gastos.

G.2.1.3 Determinación de la frecuencia anual (ARO).

La frecuencia anual es la cantidad razonable de veces que se espera que ocurra el riesgo durante el año. La elaboración de estas estimaciones resulta muy difícil; existen muy pocos datos actuariales disponibles. Lo que se ha recopilado hasta ahora parece ser información privada que poseen unas pocas empresas de seguros de bienes. Para estimar la frecuencia anual, recurra a sus experiencias anteriores y consulte a expertos en gestión de riesgos, además de consultores de negocios y de seguridad. La frecuencia anual es similar a la probabilidad de un análisis de riesgos cualitativo y va del 0% (nunca) al 100% (siempre).

G.2.1.4 Determinación de la expectativa de pérdida anual (ALE).

La expectativa de pérdida anual es la cantidad total de dinero que la organización perderá en un año si no se toman medidas para mitigar el riesgo. Para calcular este valor multiplique la expectativa de pérdida simple por la frecuencia anual. La expectativa de pérdida anual es similar al intervalo relativo de un análisis de riesgo cualitativo.

Por ejemplo, si un incendio en el conjunto de servidores Web de la misma empresa provoca daños valorados en 37.500 dólares y la probabilidad, o frecuencia anual, de que se produzca un incendio tiene un valor 0,1 (lo que indica una vez cada diez años), en este caso el valor de frecuencia anual sería 3.750 dólares (37.500 x 0,1 = 3.750).

La expectativa de pérdida anual proporciona un valor con el que la organización puede trabajar para presupuestar cuánto costará establecer controles o protecciones para prevenir este tipo de daño (en este caso, 3.750 dólares o menos al año) y brindar un nivel adecuado de protección. Es importante cuantificar la posibilidad real de un riesgo y el daño, en términos monetarios, que puede causar la amenaza para determinar la cantidad que se puede destinar en la protección contra la posible consecuencia de la amenaza.

G.2.1.5 Determinación del costo de los controles.

Determinar el costo de los controles requiere estimaciones precisas de cuánto costará adquirir, probar, implementar, poner en funcionamiento y mantener cada control. Dichos costos deben incluir la compra o desarrollo de la solución de control, la implementación y configuración de la solución de control, el mantenimiento de la misma, la notificación de nuevas directivas o procedimientos relacionados con el nuevo control a los usuarios, los cursos para usuarios y personal de TI acerca de cómo utilizar y dar soporte al control, supervisarlo y combatir la pérdida de comodidad o productividad que el control pueda imponer. Por ejemplo, para reducir el riesgo de que un incendio dañe el conjunto de servidores Web, la organización ficticia puede implementar un sistema de extinción de incendios automatizado. Será necesario contratar a un contratista para que diseñe e instale el sistema y, después, se tiene que supervisar continuamente. También será necesario comprobar el sistema periódicamente y, en ocasiones, recargarlo con los retardantes químicos que utilice.

G.2.1.6 Rendimiento de la inversión en seguridad (ROSI).

Estime el costo de los controles mediante la siguiente ecuación:

(Expectativa de pérdida anual antes del control) – (Expectativa de pérdida anual después del control) – (Costo anual del control) = Rendimiento de la inversión en seguridad

Por ejemplo, la expectativa de pérdida anual de la amenaza de que un pirata informático inutilice un servidor Web es de 12.000 dólares y después de implementar la protección sugerida se valora en 3.000 dólares. El costo anual del mantenimiento de la protección es de 650 dólares, por lo que el rendimiento de la inversión en seguridad es de 8.350 dólares al año, tal como se expresa en la siguiente ecuación: 12.000 - 3.000 - 650 = 8.350.

G.2.2 Resultados de los análisis de riesgos cuantitativos.

Los elementos de entrada de los análisis de riesgos cuantitativos proporcionan objetivos y resultados claramente definidos. Los siguientes elementos normalmente se derivan de los resultados de los pasos anteriores:

- Valores monetarios asignados de los activos.
- Una lista completa de amenazas importantes.
- La probabilidad de que cada amenaza ocurra.
- El potencial de pérdida para la empresa, por amenaza, cada 12 meses.
- Protecciones, controles y acciones recomendados

Ha podido comprobar que todos estos cálculos se basan en estimaciones subjetivas. Las cifras clave que proporcionan los resultados no se obtienen de ecuaciones objetivas o de conjuntos de datos actuariales bien definidos sino de las opiniones de los que realizan la evaluación.

El valor del activo, la expectativa de pérdida simple, la frecuencia anual y el costo de los controles son cifras que incorporan los propios participantes (normalmente después de mucho debate y compromiso).

G.3 PROPUESTA DE LISTA VALORES DE ACTIVOS.

En este apéndice se enumeran los activos del sistema de información que se encuentran habitualmente en organizaciones de varios tipos. Esta lista no pretende ser exhaustiva y es improbable que represente todos los activos del entorno único de su organización. Por lo tanto, es importante que personalice la lista durante la fase de evaluación de riesgos de su proyecto. Se proporciona como una lista de referencia y un punto de partida para ayudar a su organización a empezar.

Tabla G.1 Activos comunes del sistema de información

Clase de activo	Entorno de TI global	Nombre del activo	Clasificación de activo
	Máximo nivel de descripción del activo	*Definición de siguiente nivel (si es necesario)*	*Clasificación de valor de activo, consulte la ficha Definición de grupo (1-5)*
Tangible	Infraestructura física	Centros de datos	5
Tangible	Infraestructura física	Servidores	3
Tangible	Infraestructura física	Equipos de escritorio	1
Tangible	Infraestructura física	Equipos móviles	3
Tangible	Infraestructura física	PDA	1
Tangible	Infraestructura física	Teléfonos móviles	1
Tangible	Infraestructura física	Software de aplicación de servidor	1
Tangible	Infraestructura física	Software de aplicación de usuario final	1
Tangible	Infraestructura física	Herramientas de desarrollo	3
Tangible	Infraestructura física	Enrutadores	3
Tangible	Infraestructura física	Conmutadores de red	3
Tangible	Infraestructura física	Equipos de fax	1
Tangible	Infraestructura física	PBX	3
Tangible	Infraestructura física	Medios extraíbles (por ejemplo, cintas, disquetes, CD-ROM, DVD, discos duros portátiles, dispositivos de almacenamiento PC Card, dispositivos de almacenamiento USB, etc.)	1
Tangible	Infraestructura física	Fuentes de alimentación	3
Tangible	Infraestructura física	Sistemas de alimentación ininterrumpida	3
Tangible	Infraestructura física	Sistemas contra incendios	3

Clase de activo	Entorno de TI global	Nombre del activo	Clasificación de activo
Tangible	Infraestructura física	Sistemas de aire acondicionado	3
Tangible	Infraestructura física	Sistemas de filtrado de aire	1
Tangible	Infraestructura física	Otos sistemas de control medioambiental	3
Tangible	Datos de intranet	Código fuente	5
Tangible	Datos de intranet	Datos recursos humanos	5
Tangible	Datos de intranet	Datos financieros	5
Tangible	Datos de intranet	Datos de publicidad	5
Tangible	Datos de intranet	Contraseñas de empleados	5
Tangible	Datos de intranet	Claves de cifrado privadas de empleado	5
Tangible	Datos de intranet	Claves de cifrado de sistema informático	5
Tangible	Datos de intranet	Tarjetas inteligentes	5
Tangible	Datos de intranet	Propiedad intelectual	5
Tangible	Datos de intranet	Datos de requisitos normativos (GLBA, HIPAA, CA SB1386, Directiva de protección de datos de UE, etc.)	5
Tangible	Datos de intranet	Números de seguridad social de empleados de EE.UU.	5
Tangible	Datos de intranet	Números de licencia de conducir de empleados	5
Tangible	Datos de intranet	Planes estratégicos	3
Tangible	Datos de intranet	Informes de crédito al consumo de los clientes	5
Tangible	Datos de intranet	Registros médicos de los clientes	5
Tangible	Datos de intranet	Identificadores biométricos de los empleados	5
Tangible	Datos de intranet	Datos de contacto de negocios de empleados	1
Tangible	Datos de intranet	Datos de contacto personales de empleados	3
Tangible	Datos de intranet	Datos de pedidos	5
Tangible	Datos de intranet	Diseño de infraestructura de red	3
Tangible	Datos de intranet	Sitios Web internos	3
Tangible	Datos de intranet	Datos etnográficos de empleados	3
Tangible	Datos de extranet	Datos de contratos con socios	5
Tangible	Datos de extranet	Datos financieros de socios	5

Clase de activo	Entorno de TI global	Nombre del activo	Clasificación de activo
Tangible	Datos de extranet	Datos de contacto de socios	3
Tangible	Datos de extranet	Aplicación de colaboración con socios	3
Tangible	Datos de extranet	Claves de cifrado de socios	5
Tangible	Datos de extranet	Informes de crédito de socios	3
Tangible	Datos de extranet	Datos de pedidos de socios	3
Tangible	Datos de extranet	Datos de contratos con proveedores	5
Tangible	Datos de extranet	Datos financieros de proveedores	5
Tangible	Datos de extranet	Datos de contacto de proveedores	3
Tangible	Datos de extranet	Aplicación de colaboración con proveedores	3
Tangible	Datos de extranet	Claves de cifrado de proveedores	5
Tangible	Datos de extranet	Informes de crédito de proveedores	3
Tangible	Datos de extranet	Datos de pedidos de proveedores	3
Tangible	Datos de Internet	Aplicación de ventas de sitio Web	5
Tangible	Datos de Internet	Datos de publicidad de sitio Web	3
Tangible	Datos de Internet	Datos de tarjeta de crédito de clientes	5
Tangible	Datos de Internet	Datos de contacto de clientes	3
Tangible	Datos de Internet	Claves de cifrado públicas	1
Tangible	Datos de Internet	Notas de prensa	1
Tangible	Datos de Internet	Notas del producto	1
Tangible	Datos de Internet	Documentación de producto	1
Tangible	Datos de Internet	Materiales de cursos	3
Intangible	Reputación		5
Intangible	Buena voluntad		3
Intangible	Moral de empleados		3
Intangible	Productividad de empleados		3
Servicios de TI	Mensajería	Correo electrónico/programación (por ejemplo, Microsoft® Exchange)	3
Servicios de TI	Mensajería	Mensajería instantánea	1
Servicios de TI	Mensajería	Microsoft Outlook® Web Access	1

Clase de activo	Entorno de TI global	Nombre del activo	Clasificación de activo
		(OWA)	
Servicios de TI	Infraestructura básica	Microsoft Active Directory®	3
Servicios de TI	Infraestructura básica	Sistema de nombres de dominio (DNS)	3
Servicios de TI	Infraestructura básica	Protocolo de configuración dinámica de host (DHCP)	3
Servicios de TI	Infraestructura básica	Herramientas de administración empresarial	3
Servicios de TI	Infraestructura básica	Uso compartido de archivos	3
Servicios de TI	Infraestructura básica	Almacenamiento de datos	3
Servicios de TI	Infraestructura básica	Acceso telefónico remoto	3
Servicios de TI	Infraestructura básica	Telefonía	3
Servicios de TI	Infraestructura básica	Acceso a red privada virtual (VPN)	3
Servicios de TI	Infraestructura básica	Servicio de nombres de Internet de Microsoft Windows® (WINS)	1

CATEGORÍAS, CLASIFICACIÓN Y CONDICIONES DE LAS ACTIVIDADES DE CONTROL DE ACUERDO A EL DESARROLLO DEL CONTROL INTERNO.

H.1 DEFINICIÓN DE CONTROL.

Para el mejor entendimiento de este texto se iniciará con el término de Control ó también conocida como actividad de control.

Control ó Actividad de Control: "Es cualquier medida que tome la dirección, el Consejo y otros, para mejorar la gestión de riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos. La dirección planifica organiza y dirige la realización de las acciones suficientes para proporcionar una seguridad razonable de que se alcanzarán los objetivos y metas." [Fernández, 2003].

Los controles o actividades de control son medidas aplicables para todo el entorno de la empresa y generalmente se conocen como controles generales, pero dentro de estas actividades de control se encuentran aquellos que se han especificado y son aplicables a una sola área como es la de tecnologías de información.

A continuación se mencionarán categorías, clasificaciones y condiciones con las que deben de cumplir los controles ó actividades de control.

H.2 CATEGORÍAS, CLASIFICACIÓN Y CONDICIONES DE LOS CONTROLES Ó ACTIVIDADES DE CONTROL.

H.2.1 Categorías de los controles generales de acuerdo a COSO.

Los ***Controles*** son los medios diseñados para contrarrestar los riesgos identificados y pueden ser clasificados de acuerdo al Control Interno general y al marco referencial COSO en:

- ☑ **Controles de monitoreo** – actividades de control que ayudan a la gerencia a validar de manera periódica las acciones que se ejecutan en determinado proceso del negocio tales como los márgenes, número de cuentas nuevas, número de facturas procesadas, etc. para identificar errores originados por la falta o funcionamiento incorrecto de controles a nivel de transacciones, y monitorear el logro de las metas financieras y operacionales.

- ☑ **Controles a nivel de transacciones** – actividades de control dirigidas a asegurar que los datos (órdenes, facturas, cobranza, etc.) estén completos, sean válidos y exactos, y para cumplir con los objetivos de control establecidos para los diferentes procesos.

- ☑ **Controles de Salvaguarda de Activos** – actividades de control referidos a la custodia de los activos e incluyen controles y medidas de seguridad diseñadas para asegurar que el acceso a los activos se limite sólo al personal autorizado, como son: bienes muebles e inmuebles, efectivo o documentos al cobro y registro de datos.

- ☑ **Controles de Segregación de Funciones** – actividades de control diseñadas para prevenir que una persona esté en posición de controlar distintas etapas del procesamiento de una transacción sin que otra persona detecte errores o irregularidades, si los mismos se producen.

- ☑ **Controles Generales de Tecnologías de Información** – actividades de control que ayudan a asegurar el acceso a programas y datos (Seguridad física y lógica), comprobar operaciones computacionales, verificar mantenimiento y cambio de programas y revisar el desarrollo de programación. [PWC, 2006]

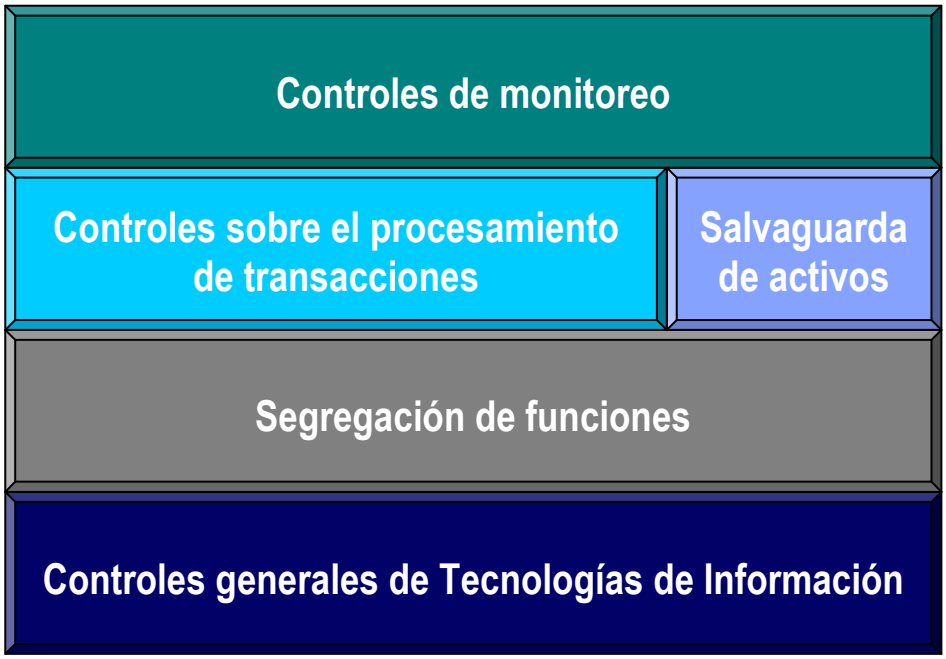


Figura H.1 Controles ó Actividades de control.

Con la anterior clasificación, se puede captar en que parte de acuerdo al COSO se ubican los Controles Generales de Tecnologías de Información. Conforme a esta imagen, se puede ver que son los controles que sirven de base para los demás debido a su naturaleza de soporte, ya que las Tecnologías de Información, son las que contiene la gran mayoría de la información operacional de la empresa a través de sus sistemas de información, redes, bases de datos, servidores, equipos de cómputo, etc., de ahí radica la importancia de que se requiera proteger esto bienes.

H.2.2 Clasificación de los controles.

Ahora bien, los controles generales y los controles de TI en su contexto general, pueden tener los siguientes clasificaciones a de acuerdo a su naturaleza de origen y a la forma en que se lleva a cabo. Estos controles son aplicables a cualquier tipo de control en cualquier nivel de la organización.
Los controles se dividen en:

a. Acorde a su aplicación sobre el riesgo: ***Preventivos y Detectivos.***

b. Acorde a la forma en que se llevan acabo en: ***Automáticos y Manuales.***

a. *Preventivos y Detectivos.*

1. *Preventivos*.- Están diseñados para evitar el procesamiento de transacciones con errores o irregularidades, identificándolas y rechazándolas antes de completar el procesamiento.

Ejemplo: Contar con un formato de alta de usuarios para el acceso a las aplicaciones, debidamente autorizado por la gerencia de la cual proviene. Previniendo así que las altas de usuarios se realicen sin permiso.

2. *Detectivos*.- Están diseñados para identificar errores o irregularidades, una vez ocurrido el proceso.

Ejemplo: Realizar un monitoreo remoto de instalaciones de software en equipos de usuario. Este control detecta que software se instalado sin autorización.

b. *Automáticos y Manuales.*

1. *Automáticos*.- Son aquellos soportados por los sistemas de aplicación e involucra una comparación efectuada por el sistema de determinada información relativa a una transacción con una serie de parámetros pre-establecidos.

   Ejemplo: La aplicación verifica que el nombre de usuario y contraseña son válidos para acceder al mismo. Cuando se realicen verificaciones del funcionamiento de estos controles, se recomienda que sólo se prueben una vez, ya que la aplicación si esta programada correctamente siempre funcionará bien, de lo contrario siempre habrá errores.

2. *Manuales*.- Son aquellos llevados a cabo por los funcionarios de la organización y su efectividad está sujeta a la responsabilidad, capacidad, experiencia del funcionario que los realiza y la segregación de funciones.

   Ejemplo: Para realizar una modificación a un programa o sistema, se requiere de una solicitud formal de cambio por parte del dueño de la información hacia el área de desarrollo, debido a que los desarrolladores no

deben realizar alteraciones a las aplicaciones sin el consentimiento de este dueño. [Reyes, 1992]

H.2.3 Condiciones para los controles.

Las circunstancias con las que deben disponer los controles para proporcionar una seguridad razonable son expuestas a continuación:

- ☑ **Proporcionar efectividad y eficiencia en las operaciones**– A causa de que el uso de controles disminuye el riego, por consecuencia los procesos son más efectivos y eficientes. Este es uno de los objetivos de negocio básicos de una entidad, incluyendo las metas de desempeño y de rentabilidad. Esto incluye la protección de los activos, tangibles e intangibles.

- ☑ **Suministrar confiabilidad de los reportes financieros** – En la aplicación de controles, podemos asegurarnos que la información sea completa, exacta y valida, viéndose reflejado en reportes arrojados por las aplicaciones. Y a su vez, en la preparación confiable de reportes financieros presentados de manera razonable y en conformidad con Principios de Contabilidad Generalmente Aceptados (GAAP) u otros principios apropiados diferentes a GAAP.

- ☑ **Cumplir con leyes y regulaciones aplicables** – Incluye cumplimiento con las reglas de la SEC (Securities and Exchange Commission) reglas del mercado de valores y reglas de pago de impuestos sobre utilidades, las cuales tienen un impacto financiero. [PWC, 2006]

MARCO DE REFERENCIA COBIT.
[COBIT, 2005]

I.1 INTRODUCCIÓN AL MARCO DE REFERENCIA COBIT.

COBIT es un marco de referencia aceptado internacionalmente como una buena práctica de control de la información, desarrollado por la Information Systems Audit and Control Association (ISACA) y el IT Governance Institute (ITGI) con un equipo de conformado por más de 100 expertos alrededor del mundo (miembros de ISACA y otros industrias) y es utilizado para implementar el gobierno de TI y mejorar los controles de TI. Se trata de un marco compatible y que incorpora aspectos fundamentales de otros estándares y modelos relacionados (COSO, CMM, ISO 27002 y BS7799).

I.2 ANTECEDENTES.

- ☑ 1992: comenzó la actualización de los objetivos de control de ISACA.
- ☑ 1996: ISACA proporcionó a los profesionales de TI un marco de prácticas control de la TI generalmente aplicables y aceptadas.
- ☑ 1998: fue actualizado y se publicó una segunda versión.
- ☑ 1999: se publicaron los “Objetivos de Control para redes”.
- ☑ 2000: se publicó la 3ra. Edición.
- ☑ 2004: ante las regulaciones internacionales, ISACA publica IT Control Objectives for Sarbanes – Oxley.
- ☑ 2005: se publica COBIT 4.0, fortaleciendo el enfoque de Marco de Gobernabilidad de TI.
- ☑ 2007: La última versión COBIT 4.1 es una síntesis de la versión anterior, aumentando nuevas prácticas y el mejoramiento de procesos.

I.3 MISIÓN DEL COBIT.

Su misión es investigar, desarrollar publicar y promover un conjunto de objetivos de controles de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser utilizados diariamente por Gerentes de negocio y personal de TI.

1.4 CÓMO SATISFACE COBIT LA NECESIDAD DEL CONTROL DE TI.

1.4.1 Componentes de COBIT.

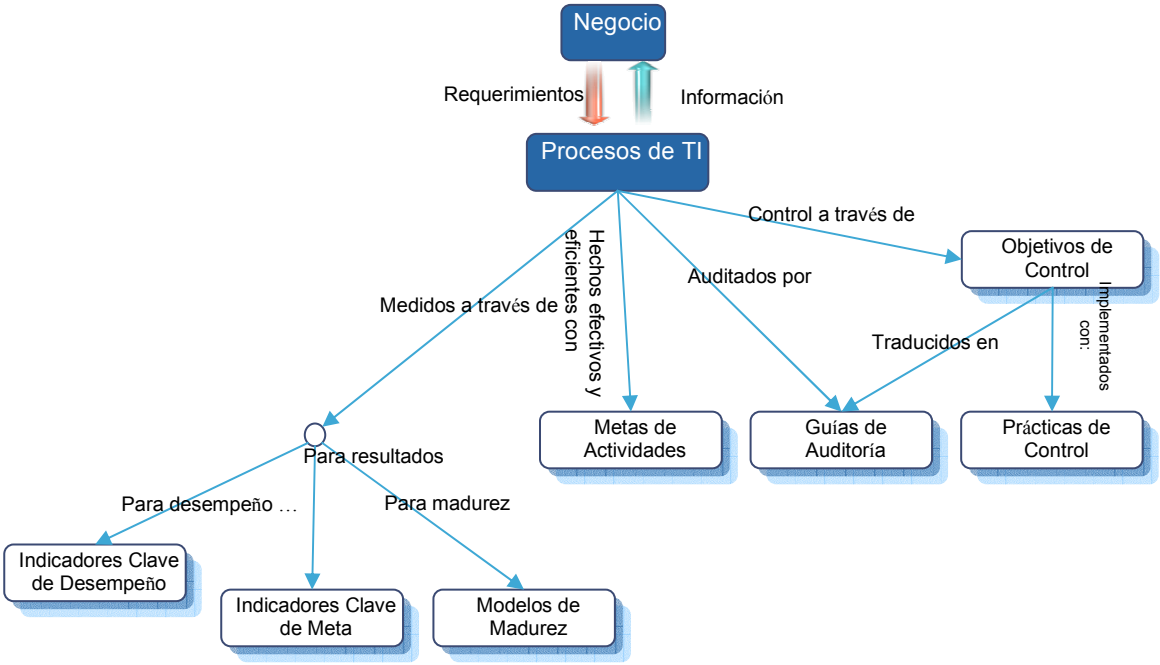


Figura. I.1 Componentes que maneja COBIT.

El negocio esta conformado por muchos procesos que manejan información a través de diferentes medios como son las TI; para asegurarse de que esta información es segura y de que estos procesos son realizados con efectividad y eficacia se fijan metas generales y objetivos determinados que utilizan prácticas ó actividades de control para ser cumplidos. Para testificar que este cumplimiento se esta llevando acabo, las empresas hacen uso de guías de auditoria.

Algunas técnicas para medir el cumplimiento de estas actividades, objetivos y metas de control son los modelos de madurez que permiten determinar en qué situación se encuentra la empresa actualmente (indicador del estado actual), en qué situación se encuentran las demás empresas (comparación con el indicador promedio de empresas similares) y qué meta alcanzable se puede fijar la empresas para el futuro (el objetivo de mejora de la empresa).

I.4.2 Principios básicos de COBIT.

Para satisfacer esta necesidad COBIT se creó con las características principales de ser ***orientado a negocios, orientado a procesos, basado en controles e impulsado por mediciones***.

La ***orientación a negocios*** es el tema principal de COBIT. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como consejero para la gerencia y para los propietarios de los procesos de negocio.

El marco de trabajo COBIT se basa en el siguiente principio (figura I.2): proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información. El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

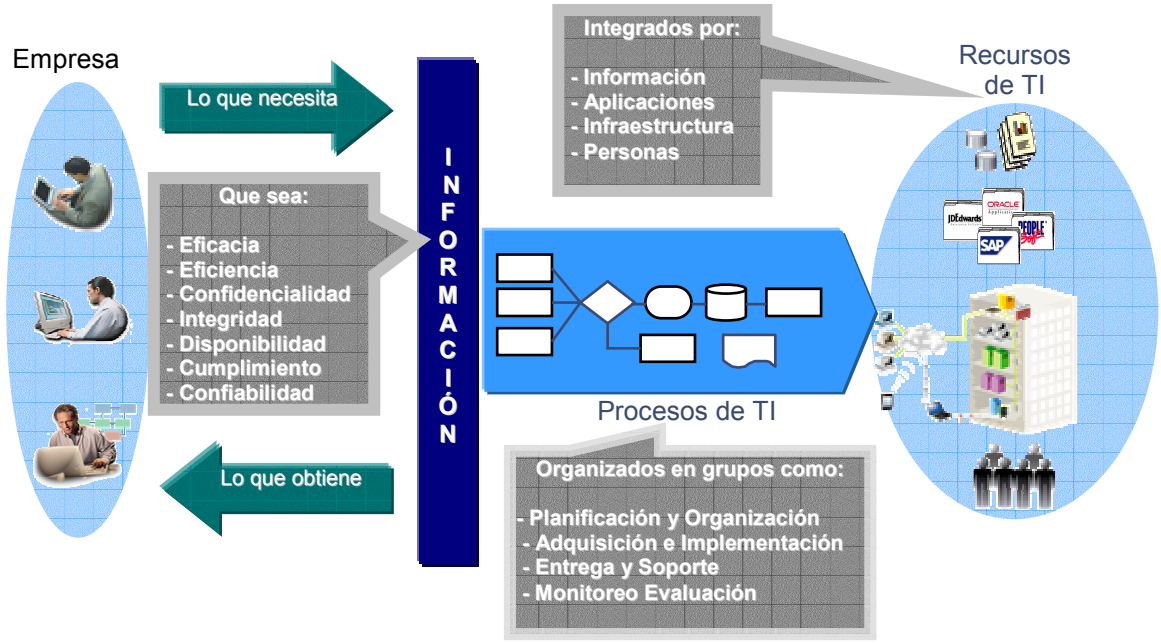


Figura. I.2 Conceptos usados por COBIT.

Con respecto a ***orientado a procesos*** COBIT define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son:

Integrados por 34 procesos de

- ☑ Planear y Organizar (PO),
- ☑ Adquirir e Implementar (AI),
- ☑ Entregar y Dar Soporte (DS) y
- ☑ Monitorear y Evaluar (ME)

Cada proceso se tiene cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso.
Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear. El marco de trabajo de COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que cada uno en la empresa visualice y administre las actividades de TI. La incorporación de un modelo operacional y un lenguaje común para todas las partes de un negocio involucradas en TI es uno de los pasos iniciales más importantes hacia un buen gobierno.

También brinda un marco de trabajo para la medición y monitoreo del desempeño de TI, comunicándose con los proveedores de servicios e integrando las mejores prácticas administrativas. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

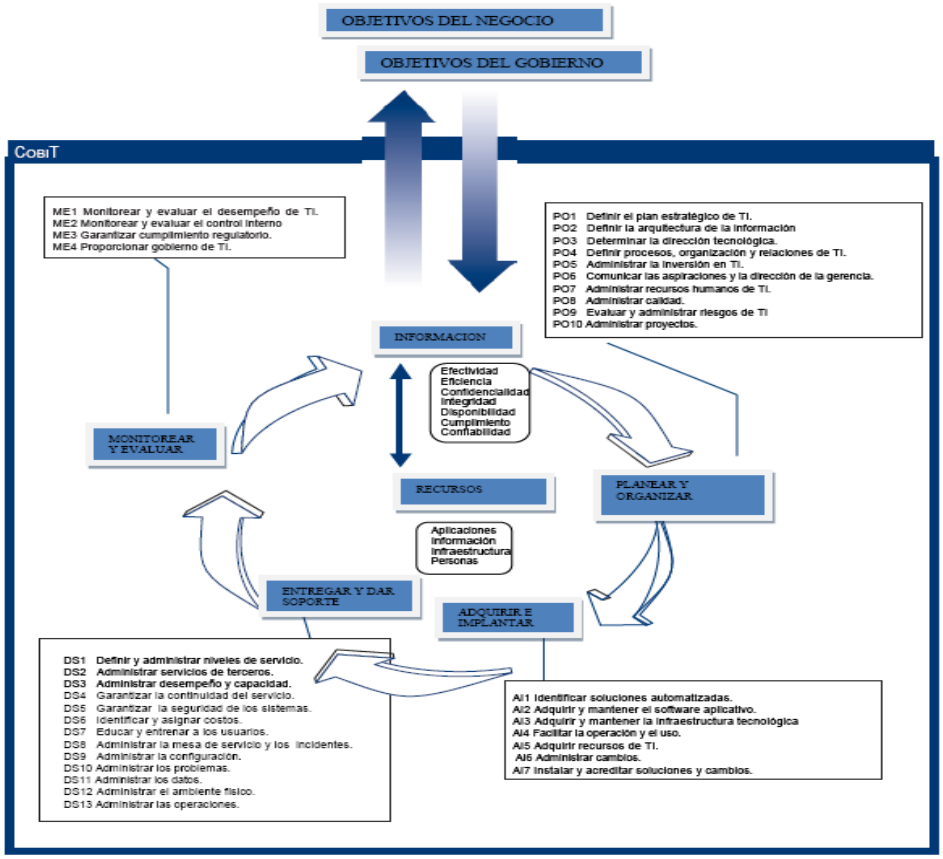


Figura I.3 Estructura del marco COBIT

En la parte que esta ***Basado en controles,*** se refiere a que los procesos requieren controles; control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos. Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT.

La guía se puede obtener del modelo de control estándar mostrado en la figura 1.4. Sigue los principios que se evidencian en la siguiente analogía: cuando se ajusta la temperatura ambiente (estándar) para el sistema de calefacción (proceso), el sistema verificará de forma constante (comparar) la temperatura ambiente (inf. de control) e indicará (actuar) al sistema de calefacción para que genere más o menos calor.

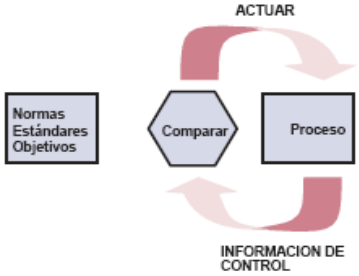


Figura I.4 Modelo de control.

La gerencia operacional usa los procesos para organizar y administrar las actividades de TI en curso. COBIT brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia operacional de TI y para la gerencia administrativa. Para lograr un gobierno efectivo, los gerentes operacionales deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de COBIT están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobierno de TI, los procesos de TI y los controles de TI.

Una necesidad básica de toda empresa es entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar la empresa. La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. ¿Qué se debe medir y cómo? Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. Para decidir cuál es el nivel correcto, la gerencia debe preguntarse a sí misma: ¿Qué tan lejos debemos ir, y está justificado el costo por el beneficio? COBIT atiende estos temas para ***Generar Mediciones*** por medio:

- ☑ Modelos de madurez que facilitan la evaluación por medio de benchmarking y la identificación de las mejoras necesarias en la capacidad.

- ☑ Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades del negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios de un marcador de puntuación balanceado (balanced scorecard).

- ☑ Metas de actividades para facilitar el desempeño efectivo de los procesos.

1.5 LOS 3 PANORAMAS DE COBIT.

A continuación se muestra el cubo COBIT en donde se presenta tres panoramas de cómo es que puede ser visto el uso de este marco referencial.

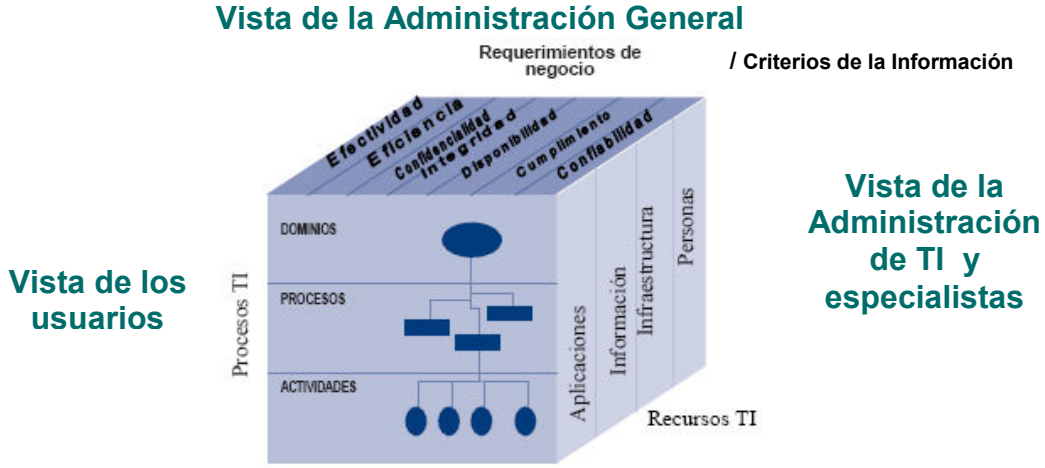


Figura I.5 Las diferentes vistas de COBIT.

1.5.1 Requerimientos del Negocio / Criterios de Información.

Efectividad: Información relevante y pertinente para el negocio, provista de manera oportuna, correcta, consistente y utilizable.
Eficiencia: Tratar la información a través del uso óptimo de recursos (productivo y económico).
Confidencialidad: La información sensible protegida de revelación no autorizada.
Integridad: Exactitud, completitud y validez de la información.
Disponibilidad: Actual y futura, salvaguarda de los recursos necesarios.
Cumplimiento: Adhesión al marco legal y de política.
Confiabilidad: Propiedad de la información que se usará en la toma de decisiones.

1.5.2 Recursos de TI.

Aplicaciones Se refiere a la suma de programas de aplicación, funciones de procesamiento y procedimientos manuales
Información Datos en todas sus formas (insumos, procesados, salidas de los sistemas de información) que sean utilizados por el negocio.
Infraestructura Tecnología y facilidades (hardware, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc., y el ambiente que los soporta), y que permiten el funcionamiento de las aplicaciones.
Gente Personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas de información y servicios. Considerando personal interno ó subcontratado.

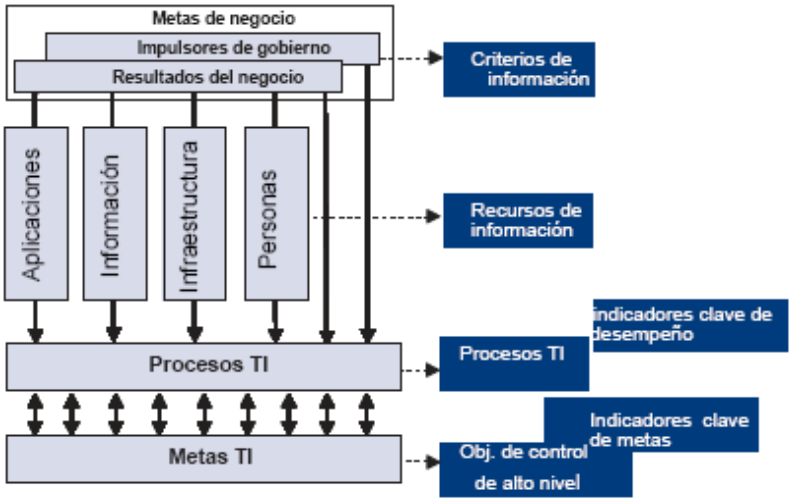


Figura I.6 Recursos de TI.

1.5.3 Modelo de los procesos.

☑ Agrupamiento lógico de procesos, a menudo se concibe como dominios de responsabilidad dentro de una estructura y encuadra en el ciclo de vida aplicable a los procesos de TI.
☑ Una serie de actividades o tareas vinculadas con cortes (de control) naturales.
☑ Son necesarias para lograr un resultado mensurable. Son las acciones que deben realizarse para que el proceso cumpla con su objetivo.

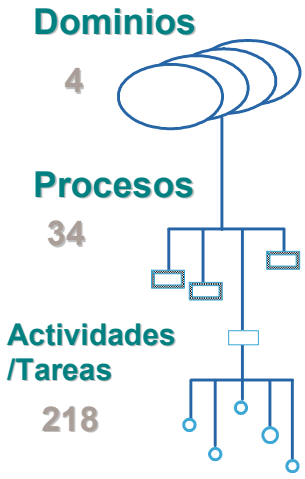


Figura I.7 Modelo de los procesos de COBIT.

1.6 BENEFICIOS DEL COBIT.

Algunos de los beneficios que se obtienen al implementar COBIT son los siguientes:

- ☑ Mejor alineación, con base en su enfoque de negocios.
- ☑ Una visión, entendible para la gerencia, de lo que hace TI.
- ☑ Propiedad y responsabilidades claras, con base en su orientación a procesos.
- ☑ Aceptación general de terceros y reguladores.
- ☑ Entendimiento compartido entre todos los participantes, con base en un lenguaje común.
- ☑ Cumplimiento de los requerimientos COSO para el ambiente de control de TI. [COBIT, 2005]

SEGURIDAD DE LA INFORMACIÓN Y EL FACTOR HUMANO DE ACUERDO A ISACA.
[Egan, 2005]

J.1 SEGURIDAD DE LA INFORMACIÓN Y EL FACTOR HUMANO.

El siguiente artículo, se agregó con el fin de ampliar el criterio a cerca de la intervención del factor humano ante la seguridad de la información. Éste fue publicado en julio de 2005 por Information Systems Audit and Control Association (ISACA) en el boletín electrónico para Colombia. [Egan, 2005]

ACTUALIDAD

SEGURIDAD DE LA INFORMACION Y EL FACTOR HUMANO

Por Mark Egan
Tomado de Information System Control Journal (JOnline), Volumen 3, 2005

Traducido por
José Manuel Gutiérrez Gonzáles-IS/EAS.

Si la tecnología por si sola fuera suficiente para mantener una organización segura, las amenazas de Internet serían poco más que una reflexión para muchas empresas.

La mayoría de negocios y la misma industria han aprendido, al menos que las tecnologías de seguridad son apoyadas por sólidas políticas de seguridad y procedimientos corporativos y que incluso la más robusta solución no llega a proporcionar la protección adecuada contra la rápida evolución de las amenazas de hoy.

Políticas y procedimientos complementan las tecnologías de seguridad. Ellos representan las recomendaciones practicas que identifican los pasos que se deben seguir para evitar acciones inseguras que pongan en riesgo la confidencialidad, integridad y disponibilidad de los datos.

Sin embargo, aunque tecnología y procesos, sean partes fundamentales de la estructura de seguridad de la información corporativa, un tercer componente es necesario para completar el cuadro: **las personas**.

No se trata solo de que las personas hagan funcionar la seguridad tecnológica, o que crean y sigan políticas de seguridad, procedimientos y procesos críticos.

Teniendo el personal adecuado en el Lugar correcto, se puede compensar las diferencias en procesos y tecnología.

Ciertamente, las personas pueden ser el eslabón más débil o más fuerte en la cadena de la seguridad. Hacer de ellos el último, es posible con el involucramiento ejecutivo, con la colaboración de profesionales en seguridad, a través de entradas funcionales corporativas y revisiones independientes programadas.

Operando a Nivel-C

La información es el combustible de los negocios. En cualquier industria, desde servicios financieros y manufactura hasta el cuidado de la salud, la información es supremamente importante. Lo mismo se cumple para cada departamento funcional de una compañía; la información dirige los recursos humanos, desarrollo de productos, ventas, comercialización, administración de la relación con los clientes y mucho más.

Como resultado, la información debe permanecer accesible pero segura.

La protección de la información, a su vez debe convertirse en la prioridad del negocio, en lugar de considerarse solo un asunto más de tecnología.

Es aquí, donde intervienen el director ejecutivo, el oficial de información y el oficial operativo. Para que un programa de seguridad de la información sea adoptado como una iniciativa importante para el negocio, este debe tener el soporte y atención continua de los ejecutivos a nivel corporativo. Los proyectos de seguridad de la información requieren financiación y recursos. Asegurando la información del negocio se impacta a cada individuo, proceso y cada componente de hardware o software en una empresa. Además la seguridad de la información o incluso la falta de esta, puede tener un alto impacto en la satisfacción del cliente, en la marca corporativa o en la reputación de la misma.

Dentro o Fuera

En el pasado los problemas de seguridad podían ser manejados casi por cualquier profesional de TI. La expansión de las amenazas fue relativamente lenta y eran fácilmente identificadas, erradicadas y controladas.

Esto no duró por mucho tiempo. Las amenazas de Internet alcanzaron niveles incomparables de complejidad, y la velocidad con que aparecen y se propagan pueden incluso superar a la mayoría de organizaciones sabias en tecnología. Quizás lo más importantemente, es que las vulnerabilidades del software se están descubriendo y explotando tan rápidamente que aplicar medidas preventivas es prácticamente imposible, especialmente cuando al personal de TI se le asignan mas responsabilidades con menos recursos.

Esto es porque tener una organización de seguridad de la información dedicada es fundamental para entender y encontrar los desafíos en seguridad de la información de hoy y de mañana. Por cada 1000 empleados, al menos un profesional en seguridad de

la información debe estar en el lugar de quien tiene las credenciales y experiencia requerida para reconocer y responder ante cualquier cosa que amenace la seguridad y disponibilidad de la información corporativa. Un líder a nivel ejecutivo es quien reporta al CEO, CIO o COO, este podría ser el líder del equipo de seguridad de la información.

Por su puesto, que para muchas organizaciones dejar en outsorcing alguna o todas las funciones de seguridad de la información es otra alternativa. Debido a que la seguridad de la información es critica y compleja, contratar expertos para administrar dicha seguridad puede dar como resultado un ahorro considerable en los costos y una postura de seguridad mucho más fuerte.

Este requiere de pocas personas

Un buen gobierno corporativo es el sello de cualquier organización exitosamente rentable. Esto ayuda a establecer el horizonte de la compañía y asegura que la misma este siempre en la dirección correcta. El gobierno corporativo refleja el interés de un amplio grupo de asociados de compañías, de la gerencia, de la junta directiva y de los accionistas.

La seguridad de la información también requiere la dirección de una junta de gobierno. Porque la seguridad de la información impacta la totalidad de la empresa. Una junta de gobierno de la seguridad de la información debe incluir lideres de unidades de negocios claves y departamentos funcionales. Estos departamentos típicamente incluyen el área legal, instalaciones, recursos humanos y TI. Además, solo la junta de gobierno corporativo es considerada la responsable por la dirección de la compañía y por el programa de seguridad de la información de la misma.

Una mirada atrás

Puesto que el propósito de las iniciativas de la seguridad de la información es mantener la seguridad y disponibilidad de la misma, llevar a cabo revisiones independientes periódicas de las políticas de seguridad de la información, procedimientos y soluciones son una necesidad. Mientras las revisiones internas pueden agregar valor descubriendo prácticas inefectivas o tecnología defectuosa, las auditorias desarrolladas por un equipo de auditores de sistemas certificados (CISA's), por ejemplo, puede suministrar un análisis mucho más detallado sobre el nivel de conformidad con varias industrias y regulaciones gubernamentales.
Las revisiones independientes dan a las organizaciones la forma de medir la efectividad de sus programas de seguridad contra mejores practicas de la industria, además porque su experiencia es basada en la interacción con múltiples negocios y organizaciones, los auditores independientes pueden hacer mucho más que identificar problemas, ellos pueden ofrecer verdaderas recomendaciones para instruir sobre controles y prácticas para llevar a cabo mejoras considerables. En el mundo de los negocios no es posible pasar la seguridad de la información a una pantalla de radar. De hecho cuando la tecnología de información esta aun más estrechamente relacionada con las operaciones diarias de las organizaciones de un lado a otro entre industrias y continentes, esta permanecerá como una prioridad en las salas de reuniones

Por consiguiente, las iniciativas criticas de seguridad de la información serán conducidas e implementadas por ejecutivos corporativos, que trabajan junto con profesionales de seguridad de la información, quienes mantendrán un especial cuidado en los recursos de información y en posibles amenazas que se puedan presentar. Más que la mayoría de tecnologías emergentes, o que las mejores prácticas intentadas y comprobadas, este factor humano demostrará ser la mejor defensa que una organización posee contra cualquiera que pueda acechar alrededor de la esquina digital.

Mark Egan
es oficial de seguridad de la información en Symantec Corp. Egan es el autor de The Executive Guide to Information Security, publicado por Symantec Press.

PROCESO DE CAMBIO DE ACUERDO A ISACA.
[Oseni, 2007]

K.1 GERENCIA DEL CAMBIO EN EL PROCESO DE CAMBIO.

El siguiente artículo fue publicado en el boletín marzo / abril de 2007 por Information Systems Audit and Control Association (ISACA) para Colombia. [Oseni, 2007].Se agregó como anexo con el fin de tener una perspectiva del procesos de cambio.

brindada por algunos de ustedes hace casi 2 años y medio, y ratificada hace casi año y medio, para dirigir el Capítulo de ISACA Bogotá. Para mí ha sido una muy buena experiencia que me ha permitido lograr muchas cosas, pero la principal, ha sido la de conocerlos a muchos de ustedes, no solo en el ámbito académico sino en el personal. Desde este espacio he conseguido muchos amigos, y por ellos la dedicación entregada ha valido la pena. Me despido de este cargo, con la satisfacción del deber cumplido, y con el ánimo de seguir apoyando a esta Asociación en cualquiera de las múltiples labores que se realizan. Agradezco también a los demás miembros de la Junta Directiva y a todos aquellos que conformaron los diferentes Comités organizadores de los eventos realizados, por todos sus esfuerzos, ya que sin ellos no habríamos alcanzado los objetivos establecidos.

Saludos especiales.

FERNANDO FERRER O., CISA
Presidente ISACA – Capítulo Colombia

PALABRAS DEL EDITOR

Dos grandes retos, dos grandes logros. Dos eventos importantes se han realizado por el Capítulo en el último año, lo cual genera muchas expectativas para el futuro. Contando con la colaboración de los asociados se lograrán grandes cosas. La invitación es a participar activamente de todas las iniciativas de la asociación y del capítulo. Mucha información llega a nuestras manos de parte de la asociación y del capítulo, saquemos el máximo provecho de esto.

LUIS ALEJANDRO BECERRA FRANCO
Coordinador de Publicaciones

ARTICULO CENTRAL

GERENCIA DEL CAMBIO EN EL PROCESO DE CAMBIO

Por Ezekiel Oseni, CISA, ACA, ACIP, ACS
Traducido por: Luis Alejandro Becerra F.
Publicado en: Journal Online - ISACA

Se sabe que el cambio es la única situación permanente en la vida pero, asombrosamente, esta es una decisión que la gerencia encuentre difícil de hacer e implementar – y cuando el cambio esta hecho, por lo general es una de las decisiones mas resistidas por los empleados. Sin embargo, el cambio es inevitable; por lo tanto, para ser eficaz, la gerencia debe anticiparse y prepararse para esto.

Retos del cambio

El cambio es la partida de un proceso existente o una forma de hacer algo a un nuevo proceso o una forma diferente de hacer la misma cosa. Un proceso de cambio puede ser una enmienda a un proceso existente, una introducción a un nuevo proceso o ambas. Por ejemplo, un proceso manual puede ser redefinido o automatizado, o un proceso automatizado puede ser actualizado, complementado o reemplazado completamente por nuevos paquetes. Estos cambios pueden ser conocidos también como procesos de reingeniería de negocios (business process reengineering BPR).

De cualquier forma los cambios están orientados a mejorar la organización en el corto, mediano o largo plazo. Sin embargo, no importa como las ideas de cambio sean presentadas, éstas pueden ser frustradas a propósito o sin intención si no son bien gerenciadas durante todas las etapas. Un gerenciamiento pobre a menudo genera grandes inversiones en el proceso de cambio y las altas expectativas que vienen con las ideas se convierten en grandes fracasos.

Algunos cambios son introducidos con fanfarria, pero no a lo largo después de iniciar su

implementación, se encuentran impedimentos que podrían haber sido evitados o minimizados si los hubiesen identificado y gerenciado oportunamente en las primeras etapas. Los casos abundan donde cuentas de las organizaciones siguen siendo irreconciliables debido a la automatización, a la mejora del sistema o a la introducción de procesos de paquetes enteramente nuevos. No hay duda que un proceso de cambio en el punto de concepción, evaluación y/o puesta en práctica requiere recursos financieros y tiempo de la gerencia y conduce a las altas expectativas. Sin embargo, cualquier falla puede ser desastrosa. Para prevenir tal falta, la atención se debe dar a la gerencia del cambio en

3. **Cómo puede ocurrir este cambio?** Esta pregunta es tan relevante como las dos primeras. Algunos procesos de cambio loables (que responden satisfactoriamente las dos primeras preguntas) terminan en desastre, y se pierden todos los tiempos de gerencia e inversión porque la pregunta de cómo hacer el cambio no ha sido adecuadamente resuelta. Cualquier acercamiento que se adopte para efectuar el cambio debe direccionar la forma de asegurar la mínima interrupción al sistema y debe efectuar el cambio con un costo mínimo.
4. **Cómo puede ser sostenido el cambio?** Esta pregunta debería ser la más crítica de las cuatro. La pregunta, si es adecuadamente contestada, justifica la sabiduría tras del cambio. Las tres primeras preguntas pueden ser contestadas de forma correcta, pero si la pregunta de cómo sostener el cambio no está bien orientada, todos los esfuerzos son simplemente una pérdida a largo plazo. Ésta es la etapa donde muchos procesos de cambio hacen frente a tormentas turbulentas y, cuando fallan, se dice que podían "no estar preparados para la prueba del tiempo."

Etapas del proceso de cambio

Las tres etapas de la realización de un proceso de cambio son preimplementación, implementación y postimplementación.

Etapa de Pre-implementación

Esta etapa puede ser resumida en tres partes:

1. **Concepción de la idea de cambio**- Esta etapa es donde se identifica la necesidad del proceso de cambio. La necesidad del cambio puede ser originada por una deficiencia en el presente sistema; la necesidad de reducir costos; el deseo de mejorar el servicio de entrega, logros contra la competencia o mejoramiento tecnológico (cambio proactivo); o la necesidad de cumplir con directivas gubernamentales o regulatorias (cambio reactivo o de cumplimiento).
2. **Evaluación de la idea** - Se identifican y evalúan las alternativas contra criterios predeterminados en esta fase. Las beneficios y

niveles bajo, medio y alto de gerencia, dependiendo de las circunstancias y el nivel de autoridad de cada nivel.

Entendiendo el Proceso de Cambio

En describiendo la psicología del cambio, la publicación "Field Theory in Social Science"[1] identifica tres etapas del proceso de cambio: descongelamiento (superación de la inercia y desmontaje del estado mental existente), implementación (cuando el cambio ocurre – típicamente un periodo de confusión) y recongelamiento (el nuevo estado mental se cristaliza y el nivel de comodidad regresa a los

costos (insuficiencias) de las alternativas se identifican. Excepto cuando es un cambio forzado, el nuevo proceso propuesto debe ofrecer beneficios mucho mas altos que los proveidos por el proceso existente.

3. **Aprobación eventual de la gerencia para introducir el proceso de cambio** – En cada una de las subetapas, especialmente en los puntos en donde se evalúa y aprueba la idea de cambio, posible resistencia por parte de usuarios y beneficiarios del proceso existente debe ser identificada. El grado y las formas de resistencia deben ser diagnosticados.

En la etapa de pre-implementación, hay disponibles tres opciones principales para manejar la resistencia al proceso de cambio propuesto:

1. **Ignorar la resistencia y adelantar el programa de proceso de cambio.** La decisión de ignorar la resistencia debe tomarse solo si el impacto de esta resistencia es insignificante y/o el costo de prevenir o realizar acciones contra la resistencia es excesivamente alto comparado con los beneficios.
2. **Terminar la resistencia previniéndola.** Para que esto sea efectivo, el grado y las formas de resistencia consideradas al proceso del cambio se deben comprobar con tanta precisión como sea posible antes de la puesta en práctica. Cabe anotar aquí que la resistencia emergería en etapa de pre-implementación, especialmente en el momento de la evaluación de la idea del cambio. Se debe dar la bienvenida a la resistencia constructiva en todas las etapas, especialmente antes de la aprobación final del proceso de cambio. Este tipo de resistencia aumenta la calidad del cambio y la aceptación cuando esta orientado a la satisfacción de todos las partes. Se asume que todas las formas de resistencia y crítica en esta etapa son constructivas, teniendo en cuenta que todas las partes involucradas en la toma de decisiones buscan lo mejor para la organización. La segunda opción es viable solo si los beneficios de prevenir la resistencia son más grandes que los costos.

3. **Implementar gerencia de crisis**. Esta es la opción de contra-resistencia, lo que implica que la resistencia al proceso de cambio no puede ser prevenida, pero los efectos son tan significativos que no pueden ser ignorados. Los

pre-implementación se ejecuten sin ningún problema. Autores del proceso del cambio, vendedores y consultores del proceso de cambio no pueden considerar todos los problemas probables que ocurran durante la etapa de la puesta en práctica o pueden, por cualquier razón, no desear divulgarlos hasta que la gerencia haya abordado el ejercicio.

Muchos proyectos de proceso de cambio han sido abandonados a mitad de la implementación luego de que enormes fondos y el tiempo de la gerencia han sido utilizados. Es un hecho que algunas de las organizaciones con esta clase de experiencia deplorable no se han recuperado completamente de la inversión perdida o han dejado de existir. Para citar como ejemplo, los esfuerzos de automatizar las operaciones de varios ministerios y agencias federales del estado en Nigeria están lejos de ser realizados a pesar de las cantidades enormes de dinero y tiempo que se han dedicado a estas tareas en el tiempo. Muchos de los proyectos se han abandonado y hay apenas algún ministerio del gobierno en Nigeria automatizado completamente. Otro ejemplo es el programa nacional del documento de identidad iniciado por el gobierno nigeriano hace más de dos décadas. El cambio fue resistido pero el gobierno insistió. Sin embargo, a pesar de todo el proyecto fué abandonado y todos los recursos económicos, financieros y otros comprometidos se han perdido.

La etapa de pre-implementación es la base para la etapa de implementación. Los programas de pre-implementación defectuosos culminan a menudo en problemas serios que truncan el proceso de cambio en la etapa de implementación

Es necesario que la gerencia instale un Comité permanente para ser proactivo en la identificación de problemas y resistencia durante la implementación y encontrar soluciones inmediatamente. Cuando no puede prevenir problemas y resistencia, debe por lo menos encontrar soluciones eficaces. El Comité permanente debe estar compuesto por todos los departamentos afectados por el proceso de cambio

cambio sean invitados en la etapa de la evaluación para evaluar, entre otras cosas, la conveniencia y la compatibilidad del proceso propuesto.

La interrupción del servicio es otro problema crítico

y debe reunirse de forma regular y cuando se requiera para discutir problemas y soluciones.

Todos los *stakeholders* (internos y externos) en el sistema deben estar involucrados durante el proceso de implementación para una mejor comprensión y cooperación.

Etapa de Post-implementación

La etapa de post-implementación se refiere básicamente a asegurarse de que el proceso de cambio alcanza los objetivos predeterminados y que los problemas de la etapa del post-implementación son identificado y eliminados rápidamente. Uno no espera que la oposición al proceso de cambio sea tan feroz en esta etapa como puede ocurrir en las etapas del pre-implementación y de implementación.

Si se presentan problemas, será muy probablemente debido a:

- ✓ **Carencia de o entrenamiento inadecuado para permitir a usuarios del nuevo proceso hacer el uso máximo del nuevo proceso** – la mayoría de la gente es renuente a aprender nuevas formas, especialmente donde se requieren tiempo y concentración profunda. Por ejemplo, la gente que está más familiarizada con una aplicación particular es más probable que encuentre razones para criticar la nueva aplicación. La gerencia debe asegurarse de que todos los miembros del personal afectados por el proceso de cambio tomen el entrenamiento necesario en todas las etapas de implementación del proceso de cambio. El personal y otros *stakehoders* deben sentirse importantes (porque lo son) en la acertada implementación del proceso de cambio.
- ✓ **Choque cultural** - En una situación donde organizaciones que han estado funcionando independientemente con procesos distintos, la visión, la creencia y otras cualidades específicas se funden juntas como entidad bajo un proceso, una visión y creencia comunes, es probable que se experimente un choque cultural. Esto puede durar hasta que los

pre-implementación se ejecuten sin ningún problema. Autores del proceso del cambio, vendedores y consultores del proceso de cambio no pueden considerar todos los problemas probables que ocurran durante la etapa de la puesta en práctica o pueden, por cualquier razón, no desear divulgarlos hasta que la gerencia haya abordado el ejercicio.

Muchos proyectos de proceso de cambio han sido abandonados a mitad de la implementación luego de que enormes fondos y el tiempo de la gerencia han sido utilizados. Es un hecho que algunas de las organizaciones con esta clase de experiencia deplorable no se han recuperado completamente de la inversión perdida o han dejado de existir. Para citar como ejemplo, los esfuerzos de automatizar las operaciones de varios ministerios y agencias federales del estado en Nigeria están lejos de ser realizados a pesar de las cantidades enormes de dinero y tiempo que se han dedicado a estas tareas en el tiempo. Muchos de los proyectos se han abandonado y hay apenas algún ministerio del gobierno en Nigeria automatizado completamente. Otro ejemplo es el programa nacional del documento de identidad iniciado por el gobierno nigeriano hace más de dos décadas. El cambio fue resistido pero el gobierno insistió. Sin embargo, a pesar de todo el proyecto fué abandonado y todos los recursos económicos, financieros y otros comprometidos se han perdido.

La etapa de pre-implementación es la base para la etapa de implementación. Los programas de pre-implementación defectuosos culminan a menudo en problemas serios que truncan el proceso de cambio en la etapa de implementación

Es necesario que la gerencia instale un Comité permanente para ser proactivo en la identificación de problemas y resistencia durante la implementación y encontrar soluciones inmediatamente. Cuando no puede prevenir problemas y resistencia, debe por lo menos encontrar soluciones eficaces. El Comité permanente debe estar compuesto por todos los departamentos afectados por el proceso de cambio y debe reunirse de forma regular y cuando se requiera para discutir problemas y soluciones.

Todos los *stakeholders* (internos y externos) en el sistema deben estar involucrados durante el proceso de implementación para una mejor comprensión y cooperación.

Etapa de Post-implementación

La etapa de post-implementación se refiere básicamente a asegurarse de que el proceso de cambio alcanza los objetivos predeterminados y que los problemas de la etapa del post-implementación son identificado y eliminados rápidamente. Uno no espera que la oposición al proceso de cambio sea tan feroz en esta etapa como puede ocurrir en las etapas del pre-implementación y de implementación.

Si se presentan problemas, será muy probablemente debido a:

- ✓ **Carencia de o entrenamiento inadecuado para permitir a usuarios del nuevo proceso hacer el uso máximo del nuevo proceso** – la mayoría de la gente es renuente a aprender nuevas formas, especialmente donde se requieren tiempo y concentración profunda. Por ejemplo, la gente que está más familiarizada con una aplicación particular es más probable que encuentre razones para criticar la nueva aplicación. La gerencia debe asegurarse de que todos los miembros del personal afectados por el proceso de cambio tomen el entrenamiento necesario en todas las etapas de implementación del proceso de cambio. El personal y otros *stakehoders* deben sentirse importantes (porque lo son) en la acertada implementación del proceso de cambio.
- ✓ **Choque cultural** - En una situación donde organizaciones que han estado funcionando independientemente con procesos distintos, la visión, la creencia y otras cualidades específicas se funden juntas como entidad bajo un proceso, una visión y creencia comunes, es probable que se experimente un choque cultural. Esto puede durar hasta que los

miembros del personal estén listos para dejar su vieja manera de hacer las cosas y el trabajo bajo nueva cultura. La gerencia debe asegurarse que las diferencias culturales sean identificadas y minimizadas en cuanto sea posible. También, el personal debe ser orientado a adoptar el nuevo proceso.

Para asegurar la gerencia del cambio acertada, es crítico tener un plan de recuperación y contingencia de desastres en todas las etapas del proceso de cambio, especialmente durante las etapas de implementación y de post-implementación. Estos planes ayudan a asegurarse de que la organización puede continuar sus operaciones con un mínimo o ninguna interrupción si falla la implementación del proceso de cambio.

Según una fórmula de cambio desarrollada por Richard Beckhard y David Gleicher, llamada en ocasiones fórmula de Gleicher, la combinación (producto) del descontento de organización; visión para el futuro; y la posibilidad de acción táctica inmediata, debe ser más fuerte que la resistencia dentro de la organización para que ocurra un cambio significativo. Exactamente qué tan eficaz es la fórmula debe ser determinada. Ninguna organización ha salido a declarar la adopción del fórmula y atribuir el éxito del proceso de cambio a ella (la fórmula). Los ingredientes del modelo están concebidos para tratar la experiencia previa, las expectativas futuras y las acciones actuales contra resistencia pero una cosa es segura: no hay regla dura y rápida a poner programas de cambio en ejecución. Como los cambios difieren, mas allá de métodos y aproximaciones, una combinación de la determinación, de cuidadosa planeación y de la unión entre todos los *stakeholders* producirán siempre buenos resultados.

Conclusiones

El cambio puede ser costoso, financieramente y de otras formas, pero también puede ser grande la recompensa si es pensado e implementado cuidadosamente. Partiendo de que grandes recursos financieros y humanos se requieren para efectuar algunos cambios de proceso, se requieren planes de calidad para asegurarse de que el nuevo proceso se implemente, los inconvenientes se identifican puntualmente y se derivan soluciones factibles. Es la responsabilidad de la alta gerencia asegurar un proceso de cambio exitoso.

Para maximizar el éxito, la gerencia debe estar bien equipada para manejar el ambiente (empleados, clientes, proveedores, competidores y otros *stakehoders*) afectado directa o indirectamente por el proceso de cambio.

Referencias

Beckhard, R.; Organization Development: Strategies and Models, Addison-Wesley, Massachusetts, USA, 1969

Notas

[1] Lewin, K.; Field Theory in Social Science, Harper and Row, New York, USA, 1951

Ezekiel Oseni, CISA, ACA, ACIP, ACS
Es cabeza de la Division de Control y Auditoría en *Bank of Industry*, Lagos, Nigeria.

COBIT USER CONVENTION EN BOGOTA

Nuevamente con gran éxito el Capítulo Bogotá – Colombia llevó a cabo un evento internacional de gran magnitud: en esta ocasión el I Cobit User Convention en Latinoamérica.

El evento que se llevó a cabo en el Hotel Cosmos 100 de Bogotá durante la semana del 9 al 13 de Abril estuvo dividido en 3 etapas, así:

Preconferencia - 9 de Abril. La Preconferencia fue conducida por los expositores Sergio y Ricardo Flores Grijalva del Capítulo ISACA de México D.F., quienes presentaron a 65 asistentes una breve inducción a Cobit.

ENTREVISTAS APLICADAS.

L.1 CUESTIONARIO 1.

Preguntas de la entrevista que se realizó para obtener la información acerca de los sistemas son (Actividad 1.3):

1. ¿Cuáles son los sistemas que se considera más importantes para la empresa? ¿Qué tan bien satisfacen los requerimientos de la misma?

2. En general, los sistemas del cliente ¿han sido desarrollados internamente o son paquetes estándar? En el caso de paquetes, ¿qué nivel de adaptación se ha hecho? ¿Quién realiza los cambios (el proveedor o la empresa)?

3. ¿Cuán antiguos son los sistemas? ¿Requerirán cambios relevantes en el futuro cercano?

4. ¿Cuáles son las principales locaciones de procesamiento? ¿Cuáles son los principales ambientes de hardware y software de base?

5. ¿Son confiables los sistemas? ¿Proveen información integra, exacta y útil para la gestión y control del negocio?

6. ¿Cómo están conectados los diversos ambientes TI? ¿Cuáles son las conexiones principales con redes externas (por ej. EDI, EFT e Internet)?

7. ¿Se utilizan proveedores externos de servicios (outsourcing)? Si es así, qué actividades y componentes han sido tercerizados,¿Cuáles son los contactos clave?
8. ¿Está cualquier parte de la infraestructura de TI de la compañía compartida o conectada con la estructura de TI de una compañía relacionada o no relacionada?

9. ¿Existen aplicaciones de E-Business en uso?

Si es así:

- ☑ Identificar partes de terceros más significativas que están conectadas a los sistemas de la empresa ¿Cuáles son sus principales roles y qué nivel de acceso tienen a los sistemas de la compañía?

- ☑ ¿Qué mecanismos de seguridad se han establecido, tales como firewalls?

- ☑ ¿Han existido incidentes de seguridad relacionados con E-Business, por ejemplo, hackeo en el sitio web?

L.2 CUESTIONARIO 2.

Preguntas de la entrevista que se realizó para obtener la información acerca de la organización del personal (Actividad 1.4):

1. ¿Cuál es la estructura organizativa de TI?

2. ¿Cuál es el nivel de dependencia respecto al personal superior?

3. ¿Está el número y experiencia del staff de TI alineado con las necesidades de la operación?

4. ¿Están claramente definidos los roles y responsabilidades de TI?

5. ¿Se han producido cambios significativos en la estructura organizativa de TI durante el ejercicio?

6. ¿Quién es el responsable máximo de TI? ¿A quién le reporta?

7. ¿Existe un Comité de TI? ¿Cómo se determinan y alinean las prioridades de TI con la estrategia y prioridades del negocio?

8. ¿Quiénes son los contactos claves en el departamento de TI?

9. ¿Existen actividades informáticas significativas fuera de la función de TI?

10. ¿En caso operativo, tienen las personas que administran dichas actividades los conocimientos y experiencia apropiados?

11. ¿Se tienen establecidos programas adecuados de entrenamiento?

12. ¿Existe una adecuada segregación de tareas dentro de la función de TI?

[Fuente Propia]