



Universidad Nacional Mayor de San Marcos

Universidad del Perú. Decana de América

Facultad de Ingeniería de Sistemas e Informática

Escuela Académico Profesional de Ingeniería de Sistemas

“Propuesta de un marco de trabajo para la administración de riesgos de TI basado en COBIT y PMBOK aplicado a la empresa TELECOM”

TESINA

Para optar el Título Profesional de Ingeniera de Sistemas

AUTORES

Milagros CANCHO ESPINOZA

Milagros MORALES FLORES

ASESOR

Jorge PANTOJA

Lima, Perú

2010



Reconocimiento - No Comercial - Compartir Igual - Sin restricciones adicionales

<https://creativecommons.org/licenses/by-nc-sa/4.0/>

Usted puede distribuir, remezclar, retocar, y crear a partir del documento original de modo no comercial, siempre y cuando se dé crédito al autor del documento y se licencien las nuevas creaciones bajo las mismas condiciones. No se permite aplicar términos legales o medidas tecnológicas que restrinjan legalmente a otros a hacer cualquier cosa que permita esta licencia.

Referencia bibliográfica

Cancho, M & Morales, M. (2010). *Propuesta de un marco de trabajo para la administración de riesgos de TI basado en COBIT y PMBOK aplicado a la empresa TELECOM*. Tesina para optar el título de Ingeniera de Sistemas. Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de Ingeniería de Sistemas e Informática, Universidad Nacional Mayor de San Marcos, Lima, Perú.

Este trabajo está dedicado a toda
nuestra familia en especial a nuestros
padres que nos impulsaron
constantemente a seguir adelante.

AGRADECIMIENTOS

A las personas que nos asesoraron, por su orientación y dedicación para que este trabajo cumpla con los objetivos trazados.

A nuestros colegas y amigos por sus observaciones y porque en todo momento nos incentivaron para que culminemos este trabajo.

A todas aquellas personas que indirectamente nos ayudaron para culminar este trabajo y que muchas veces constituyen un invalorable apoyo.

Y por encima de todo damos gracias a Dios.

Ficha Catalográfica

CANCHO ESPINOZA, Milagros
MORALES FLORES, Milagros

Propuesta de un Marco de Trabajo para la Administración de Riesgos de TI basado en COBIT
y PMBOK aplicado a la Empresa TELECOM

Gestión de Proyectos
(Lima 2010)

(UNMSM, Pregrado, Ingeniería de sistemas e Informática)

Tesina, Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e
Informática

**PROPUESTA DE UN MARCO DE TRABAJO PARA LA ADMINISTRACIÓN DE RIESGOS DE TI
BASADO EN COBIT Y PMBOK APLICADO A LA EMPRESA TELECOM**

Milagros Cancho Espinoza
Paola Milagros Morales Flores

FEBRERO – 2009

Asesor : **Jorge Pantoja**
Grado : **Ingeniero de Sistemas**

La Gestión de Riesgos es parte fundamental de la Gestión de Proyectos de Tecnología de Información. Hoy en día es importante poder plantear respuestas a situaciones inesperadas, para así poder tener una mejor respuesta a los incidentes que podrían presentarse, además se debe tener un nivel de alineamiento entre los objetivos de TI y los objetivos del negocio de toda entidad. En el presente trabajo propondremos un marco de trabajo para dicha gestión utilizando los estándares COBIT y PMBOK y luego realizando una aplicación en la realidad de la empresa TELECOM.

Para nuestra aplicación tomaremos como muestra uno de los procesos de la empresa, donde haremos una Gestión de Riesgos utilizando las fortalezas del COBIT 4.1 y PMBOK Tercera Edición planteadas en el marco de trabajo propuesto.

La aplicación de este marco de trabajo tiene como objetivo alcanzar los siguientes

resultados: Administrar los riesgos en los procesos de la empresa, implementar medidas de mitigación de los riesgos de tecnología de información, clasificar los procesos críticos de negocio y alcanzar resultados económicos, sociales y operativos positivos.

Palabras claves: COBIT

PMBOK

Procesos.

Administración de Riesgos.

Alineamiento Estratégico.

ABSTRACT

PROPUESTA DE UN MARCO DE TRABAJO PARA LA ADMINISTRACIÓN DE RIESGOS DE TI BASADO EN COBIT Y PMBOK APLICADO A LA EMPRESA TELECOM

Milagros Cancho Espinoza

Paola Milagros Morales Flores

FEBRERO – 2009

Asesor : Jorge Pantoja
Grado : Ingeniero de Sistemas

Risk Management is a fundamental part of the Project Management of Information Technology. Today it is important to bring responses to unexpected situations, so you can get a better response to incidents that may occur, in addition you must have a level of alignment between IT goals and business objectives of any entity. In this paper we propose a framework for such management using COBIT and PMBOK standards and then performing an actual implementation of the company TELECOM.

For our sample application we will take as one of the processes of the company where we will have a Risk Management using the strengths of the COBIT 4.1 and PMBOK Third Edition raised under the proposed work. The implementation of this framework aims to achieve the following results: Managing risks in business processes, implement measures to mitigate the risks of

information technology, classifying critical business processes and achieve economic results, social and positive operating.

Palabras claves: COBIT

PMBOK

Processes.

Risk Management.

Strategic Alignment.

INTRODUCCIÓN

El objetivo de la presente investigación es aplicar una metodología basada en los estándares COBIT 4.0 y PMBOK Tercera Edición para mejorar la Gestión de Riesgos en el Desarrollo de Proyectos de TI en la Empresa TELECOM.

Esta investigación se realizó en búsqueda de una mejora de la Gestión de Riesgos en la empresa TELECOM para lo cual se esperaba aplicar un marco de trabajo que mostrara buenos y consistentes resultados en los procesos de la empresa, así como un eficiente plan de contingencia que actúe de la manera más acertada en caso de efectuarse alguna incidencia.

Teniendo la Gestión de Proyectos como punto principal cuyo eje más importante es la planificación, la ejecución y el seguimiento y control, es necesario conocer las actividades que puedan ayudar para tal fin; de manera ordenada y aplicada dentro de un contexto real. Esta investigación pretende ser consultada y utilizada para aquellas personas que reconozcan al PMBOK como marco de trabajo en el desarrollo de sus proyectos y además apoyándonos en las fortalezas de COBIT para la Gestión de Riesgos, enriqueceremos la aplicación de una metodología basada en ambos estándares de trabajo.

En el pasado ya se ha enfatizado la importancia de la Gestión de Riesgos como uno de los puntos más resaltantes en la Gestión de Proyectos, es por eso que se ha venido haciendo investigaciones para la mejora de este con diferentes metodologías, hoy planteamos un marco de trabajo, el cual consideramos que

asegurará buenos resultados.

Este trabajo está dividido en cinco capítulos, los cuales se describen a continuación.

En el **primer capítulo** se describe las pautas generales de la investigación aplicada, empezando por el planteamiento y formulación del problema suscitado en la empresa TELECOM, el tipo de investigación que se realizará, las relaciones con otros proyectos similares, los objetivos que se alcanzaron con la investigación, las variables e indicadores que se miden y el área específica de aplicación.

En el **segundo capítulo** se describe el marco referencial donde se aclara algunos conceptos e ideas acerca de la Gestión de Riesgos, el proceso y la importancia de este, además de se describe las metodologías que actualmente dan soporte a la gestión de riesgos.

En el **tercer capítulo** se desarrolla la propuesta de marco de trabajo, se definen los procesos, y se detallan su uso.

En el **cuarto capítulo** se hace una aplicación del marco de trabajo propuesto, y se evalúan sus resultados.

En el **quinto capítulo** se observa todas las conclusiones y recomendaciones devenidas de esta implementación y nuestra opinión en base a los resultados obtenido en la aplicación de la metodología.

LISTA DE FIGURAS

Figura 2.1. Ciclo de la Gestión de Riesgos

Figura 3.1. Fases de la Propuesta Metodológica

Figura 4.1: Macroprocesos de La Empresa.

Figura 4.2: Proceso de Ventas - Postpago

Figura 4.3: Proceso de Ventas – Prepago

Figura 4.4: Nivel de Cumplimiento de Objetivos de Control

Figura 4.5 Diagrama de flujo del Procedimiento de Venta Fullfilment en el Proceso de Ventas

Figura 4.5 Total de vulnerabilidades identificadas

Figura 4.6. Nivel de Incidentes E2E

Figura 4.7. Nivel de Incidentes UAT

Figura 4.9. Comparación de nivel de incidencias

LISTA DE CUADROS

Cuadro 3.1. Descripción de las Fases de la Propuesta Metodológica

Cuadro 3.2: Descripción de Campos del Anexo 1.

Cuadro 3.3: Descripción de Campos del Anexo 2.

Cuadro 3.4: Marco de Control

Cuadro 3.5: Nivel de Cumplimiento del Objetivo de Control

Cuadro 3.6: Mapeo de Procesos

Cuadro 3.7: Descripción de Campos del Anexo 6.

Cuadro 3.8: Planificación de la Gestión de Riesgos

Cuadro 3.9: Matriz de Probabilidades

Cuadro 3.10: Matriz de Impacto

Cuadro 3.11: Nivel de Riesgo

Cuadro 3.12: Nivel de Prioridad

Cuadro 3.13: Evaluación Cualitativa de Riesgos

Cuadro 3.14: Plan de Respuesta a Riesgos

Cuadro 3.15: Acciones Correctivas

Cuadro 3.16: Informe del Rendimiento de Trabajo

Cuadro 4.1: Nivel de Incidentes E2E

Cuadro 4.2: Nivel de Incidentes UAT

Cuadro 4.3: Comparación de nivel de incidencias

Cuadro 4.4: Total de vulnerabilidades identificadas

ÍNDICE

Lista de Figuras.....	xi
Lista de Cuadros.....	xii
CAPÍTULO I.....	4
PLANTEAMIENTO METODOLÓGICO.....	4
1.1. EL PROBLEMA	5
1.2 TIPOS Y NIVEL DE INVESTIGACIÓN.....	7
1.3 ANTECEDENTES DE LA INVESTIGACIÓN	8
1.4 JUSTIFICACIÓN.....	10
1.5 OBJETIVOS.....	11
1.6 VARIABLES E INDICADORES	12
1.7 DISEÑO DE EXPERIMENTOS	13
1.8 RECURSOS	13
CAPÍTULO II.....	15
MARCO REFERENCIAL	15
2.1 MARCO TEÓRICO.....	16
2.1.1 METODOLOGÍA	16
2.1.2 RIESGO	16
2.1.3 CALIFICACIÓN Y CUANTIFICACIÓN DE UN RIESGO.....	17

2.1.4	CONCEPTO DE RIESGO DE TECNOLOGÍA DE INFORMACIÓN	19
2.1.5	GESTIÓN DE RIESGOS	20
2.1.6	CICLO DE LA GESTIÓN DE RIESGOS	22
2.1.7	ESTRATEGIAS DE RIESGOS.....	28
2.2	METODOLOGÍAS DE GESTIÓN DE RIESGOS.....	28
2.2.1	GUÍA DEL PMBOK.....	28
2.2.2	CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY (COBIT).....	29
2.2.3	RATIONAL UNIFIED PROCESS (RUP)	30
2.2.4	CAPABILITY MATURITY MODEL INTEGRATED (CMMI)	32
2.3	ESTADO DEL ARTE.....	32
2.3.1	ESTÁNDAR PMBOK	32
2.3.2	ESTÁNDAR COBIT	34
CAPÍTULO III		36
PROPUESTA DEL MARCO DE TRABAJO BASADO EN COBIT Y PMBOK.....		36
CAPÍTULO IV.....		75
APLICACIÓN DE LA METODOLOGÍA PROPUESTA.....		75
4.1	SITUACIÓN ACTUAL DE LA EMPRESA.....	76
CAPÍTULO V.....		114
CONCLUSIONES Y RECOMENDACIONES		114

REFERENCIAS BIBLIOGRÁFICAS	117
ANEXOS Y APÉNDICES	119

CAPÍTULO I

PLANTEAMIENTO METODOLÓGICO

1.1. El Problema

1.1.1 Realidad Problemática

En la actualidad en muchas empresas se observa poca o ninguna administración de riesgos al momento de hacer frente y resolver toda clase de incidencias producidas durante la gestión de un proyecto, cuyas consecuencias se ven reflejadas en el desempeño de los procesos de negocio de las empresas mismas causando varios efectos en las respuestas de los procesos de negocio, como son retrasos, ineficiencias y además descontento por parte de los cliente y de los stakeholders.

Los reportes periódicos de la cantidad de incidencias encontrados en los procesos muestran que el control de riesgos, no solo es deficiente, sino que en algunos casos no existen un control como tal en la Gestión de los Proyectos.

Además de los problemas propios del sistema de control interno, todo esto origina una afectación presupuestal mayor a la planificada. Eso quiere decir que el control interno no se encuentra entrelazado con las actividades de ejecución presupuestal, y por lo tanto no influye en la optimización de la administración de Gestión de Riesgos en el desarrollo de proyectos de software de TI.

Si los riesgos del proyecto se hacen realidad es probable que la planificación temporal del proyecto se retrase y que los costos aumenten.

Los riesgos técnicos amenazan la calidad y la planificación temporal del software que hay que producir, en el caso de que un riesgo técnico se convierta en realidad, la implementación puede llegar a ser difícil o imposible. Los riesgos técnicos identifican problemas potenciales de análisis, diseño, desarrollo, verificación y de mantenimiento. Además las ambigüedades de especificaciones, incertidumbre técnica, técnicas anticuadas y las tecnologías punta son también factores de riesgo.

Cabe señalar que los riesgos amenazan fuertemente el buen desenvolvimiento de los procesos del negocio, podemos citar algunos riesgos observados:

- Construir un producto o sistema excelente pero que no tiene un buen desenvolvimiento en el mercado.
- Realizar un producto que no está alineada con la estrategia comercial de la compañía.
- Tener o contemplar un recorte en el presupuesto inicial.

1.1.2 Enunciado del Problema

¿En qué medida el marco de trabajo planteado basada en los estándares COBIT y PMBOK mejorará la Gestión de Riesgos de TI en la Empresa TELECOM?

1.1.3 Delimitación de la Investigación

1.1.3.1 Delimitación Espacial

El estudio se realizará en la empresa de telecomunicaciones TELECOM.

1.1.3.2 Delimitación Temporal

La investigación será desarrollada en los meses de agosto 2009 –febrero del 2010.

1.1.3.3 Delimitación Social

- Las investigadoras.
- El asesor.
- El jurado.

1.2 Tipos y Nivel de Investigación

1.2.1 Tipo de Investigación

El tipo de investigación a realizar es aplicada ya que se hará uso de los conocimientos adquiridos durante nuestra investigación en la propuesta planteada.

Además también es una investigación correlacional ya que existe una asociación causal entre las variables independientes y dependientes planteadas en el diseño de experimentos.

1.2.2 Nivel de Investigación

La presente investigación será del nivel descriptivo, ya que se tiene por finalidad llegar a conclusiones generales construida por medio de abstracciones los cuales dan cuenta de los hechos observados en la realidad dentro del universo.

1.3 Antecedentes de la Investigación

1.3.1 AUTOR: MORALES PINTO Irma Estela

TÍTULO: REDUCCIÓN DEL IMPACTO DE LOS RIESGOS EN PROYECTOS TI

RESUMEN:

En este trabajo se demostró que los riesgos pueden prevenirse mediante adecuada gestión de los mismos.

Se realizó dos casos de estudio:

Sistema de seguimiento de Proyectos (PASA PERÚ-CE)

Implementación Del Registro Nacional de Proveedores (RNP) en CONSUCODE.

En este proyecto de investigación se aplicó el marco de trabajo COBIT para la gestión de riesgos, lo cual produjo una serie de resultados positivos para la reducción del impacto de los riesgos, esto serviría como antecedente para nuestra investigación ya que se demuestra que el estándar COBIT produjo mejoras en la Gestión de Riesgos de los Proyectos de TI en aplicación.

1.3.2 AUTOR: CONDORI ARI Cesar Alberto

GONZALES AQUINO Oriel

TÍTULO: METODOLOGÍA DE LA GESTIÓN DE RIESGOS DE TECNOLOGÍA DE INFORMACIÓN EN UNA INSTITUCIÓN FINANCIERA

RESUMEN:

El objetivo de este trabajo fue alcanzar buenos resultados en: Administración de los riesgos estructurales y coyunturales, a los que está expuesta la institución evaluada, cumplir la regulación vigente y alcanzar resultados económicos y operativos positivos.

En este proyecto de investigación se planteó un estado del arte en el que se menciona al PMBOK como una buena alternativa para la gestión de riesgos de tecnología de información, en este trabajo se eligió otra metodología ya que se aplicaba mejor al tipo de empresa a aplicar y sus procesos respectivos.

1.4 Justificación

1.4.1. Justificación de carácter práctico

La presente investigación será aplicada sobre proyectos reales buscando identificar los puntos críticos en la gestión de riesgos de cada proyecto, en caso este haya sido aplicado y la forma de mitigar cada riesgo que haya sido identificado para poder optimizar los objetivos del proyecto y su respectivo alcance.

1.4.2. Justificación de carácter metodológico

La investigación se basará en las mejores prácticas de la guía del Project Management Body of Knowledge (PMBOK) y Control Objectives for Information and related Technology (COBIT). Esta integración es una de las más efectivas ya que ayudara a mitigar los riesgos del proyecto y así mismo ver la importancia que se tiene al Gestionar los Riesgos.

1.4.3. Justificación de carácter teórico

La investigación permitirá conocer los conceptos acerca de los proyectos y la gestión de los mismos. Se identificarán las mejores prácticas en un marco extenso para el área de gestión de riesgos, y los procesos que estos incluyen.

1.5 Objetivos

1.5.1 Objetivo General

Proponer un marco de trabajo basada en los estándares COBIT y PMBOK para mejorar la Gestión de Riesgos en la empresa TELECOM

1.5.2 Objetivos Específicos

- Estudiar los principales estándares y metodologías para la elección de la mejor metodología para la gestión de riesgos.

- Hacer uso de los estándares PMBOK y COBIT para una óptima Gestión de Riesgos de TI.
- Exponer una mejor alternativa de marco de trabajo en la Gestión de Riesgos en la empresa TELECOM.
- Proponer un marco de trabajo para la gestión de riesgos para su aplicación en la empresa TELECOM.
- Plantear estrategias proactivas ante posibles incidencias suscitadas en los procesos de la empresa TELECOM.
- Proteger el logro de los objetivos de TI de la empresa TELECOM.
- Establecer claridad sobre el impacto en el negocio de los riesgos a los objetivos y recursos de TI.

1.6 Variables e Indicadores

1.6.1 Variables

1.6.1.1 Variable Independiente

Metodología basada en los estándares COBIT y PMBOK

1.6.1.2 Variable Dependiente

Gestión de Riesgos en los proyectos de Tecnología de Información.

1.6.2 Indicadores

Para esta investigación los indicadores que utilizaremos para el caso de aplicación:

- Indicadores del negocio
- Indicadores claves de desempeño:
- Indicadores claves de procesos:
- Indicadores claves de metas de TI:

Para mayor detalle ver Capítulo: Aplicación del Marco de Trabajo.

1.7 Diseño de Experimentos

1.7.1 Objeto de Estudio

Nuestro objeto de estudio es la gestión de Riesgos en los procesos de la Empresa TELECOM.

1.8 Recursos

1.8.1 Humanos

- Tesistas
- Asesor asignado.

A fin de recopilar información se realizaron entrevistas a las siguientes personas:

- Analistas de Sistemas de la empresa TELECOM.
- Developers de la empresa TELECOM.
- Analistas de Test de la empresa TELECOM.

- Jefes de Proyecto de la empresa TELECOM.

1.8.2 Materiales

- Laptops.
- Guías, normas y estándares referentes a la Gestión de Proyectos.
- Información proporcionada por la empresa TELECOM.
- Libros y tesis relacionados con el tema de Gestión de Riesgos.

1.8.3 Técnicos

Contamos con acceso a algunas bibliotecas tanto de la UNMSM como de otras universidades las cuales cuentan con una infraestructura optima para el desarrollo de nuestra investigación.

Así mismo contamos con equipos de cómputo portátiles para la rápida recopilación de data.

CAPÍTULO II

MARCO REFERENCIAL

2.1 Marco Teórico

2.1.1 Metodología

Metodología es el procedimiento o conjunto de procedimientos que se utilizan para obtener conocimientos [5]. También se le puede entender como los pasos que se han seguido en:

- Una indagación determinada
- La designación de los modelos concretos de trabajo que se aplican en una determinada disciplina o especialidad.
- La referencia de procedimientos y recomendaciones que se desea a transmitir.

La metodología dependerá de los postulados que el investigador considere como válidos; de aquello que considere objeto de la ciencia y conocimiento científico; pues será a través de la acción metodológica, como recolecte, ordene y analice la realidad estudiada.

2.1.2 Riesgo

Según la Real Academia Española, RAE, un riesgo es:

“Contingencia o proximidad de un daño.”

Un riesgo es la posibilidad grande o pequeña de que un daño o un resultado adverso se produzca de un peligro en particular.

Un riesgo es un problema potencial, que podría suceder o tal vez no.

Pero independientemente del resultado, es una buena práctica en la Gestión de Proyectos identificarlo, evaluar su probabilidad de ocurrencia, estimar su impacto, y establecer un plan de contingencia si el problema realmente se produce. [WWW 01]

Asimismo, al hablar de riesgos comúnmente relacionamos este concepto con las siguientes palabras: amenaza, emergencia, urgencia, apuro, etc.

Entonces podemos definir un riesgo de la siguiente manera: Un Riesgo es aquel evento que genera incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.3 Calificación y Cuantificación de un Riesgo

Son también variadas las formas y métodos para medir un riesgo, se presume que según el tipo de riesgo en análisis, existen distintas maneras de medir el nivel de riesgo al que está expuesto el proceso o servicio en evaluación.

Al hablar de calificación, se puede considerar los objetivos del negocio, por ejemplo para los clientes de una entidad financiera, la calificación de riesgo para acceder a un crédito se mide en términos de clasificar al cliente a quien se otorga un préstamo (por ejemplo, normal, deficiente, potencial pérdida, etc.).

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para describir la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran, estas escalas pueden ser ajustables para adaptarlas a las circunstancias que el análisis establezca. El análisis cualitativo se utiliza:

- Como una actividad inicial para identificar los riesgos que requieren de un análisis más detallado.
- Cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo y
- Cuando los datos numéricos son inadecuados para un análisis cuantitativo.

Al hablar de cuantificación, el objetivo es medir numéricamente la probabilidad de que un evento de riesgo se concrete, asimismo se mide el impacto que generaría en términos monetarios, de imagen institucional, social hacia la organización, etc. Es necesario asimismo tener en cuenta las medidas que la organización adopte para mitigar en cualquier forma la ocurrencia de algún evento de riesgo.

En este contexto, es factible relacionar los niveles de calificación con la cuantificación de un riesgo a ello se denomina análisis semi cuantitativo, por ejemplo un riesgo que tiene una probabilidad de ocurrencia de 40 en 100 casos y que genera una pérdida de 200 nuevos soles cada vez que ocurre podría considerarse como un Riesgo Alto [EDP 01]. Considerando el mismo ejemplo y conociendo que la organización ha implementado un mecanismo de control que reduce las pérdidas de 200 a 15 nuevos soles, y una ocurrencia de 12 en 100 casos, el riesgo puede adoptar un nivel de Riesgo Medio. Este ejemplo muestra una de las maneras de tratar un riesgo y ese es uno de los retos de la Administración de Riesgos.

2.1.4 Concepto de Riesgo de Tecnología de Información

La definición de los riesgos de tecnología de información, está sustentado en dos pilares fundamentales, el primero de ellos enlazado a los riesgos de operación y el segundo a las definiciones internacionales de riesgo en SI.

En el primer pilar, los riesgos de tecnología de información son componentes de los riesgos de operación, entiéndase por riesgos de operación a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos.

Esta primera definición, está sustentada en la declaración de Basilea

II, la misma que propone diez principios para una adecuada administración de los riesgos de operación, estos principios incluyen la adecuada estructura organizacional, la participación de la alta gerencia, la sujeción a revisión de auditoría, la generación de políticas de mitigación de riesgos y un proceso de gestión de los riesgos.

En el segundo pilar, los riesgos de tecnología de información se definen además como aquellos asociados a actividades con soporte en recursos de tecnología de información, sistemas informáticos y tecnología inherente a estos sistemas, los mismos que afectan el desarrollo de las actividades del negocio contra los principios de integridad, confidencialidad y disponibilidad de la información.

Como todo componente de riesgo, los asociados a tecnología de información están inmersos dentro de aquellos eventos que generan incertidumbre o pérdida en términos económicos, sociales, profesionales o de imagen.

2.1.5 Gestión De Riesgos

Proceso efectuado por un grupo designado por el gestor de Proyectos de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización,

gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre la consecución de objetivos de la entidad.

Su propósito es integrar, en la gestión y manejo de los objetivos estratégicos, los riesgos asociados a fin de mejorar el desempeño corporativo.

La gestión del riesgo tiene implícitas ciertas definiciones que cada organización se da a si misma respecto del riesgo:

Apetito al riesgo: Nivel de riesgo que cada organización está preparada para tolerar en sus negocios

Capacidad de riesgo: Nivel de riesgo que cada organización no está financieramente capacitada para exceder

Como consecuencia de ello, la gestión del riesgo es propia para cada organización.

A continuación revisaremos algunas consideraciones que apoyan a las organizaciones a una adecuada gestión de sus riesgos.

Objetivos de Gestión de Riesgos:

- Conectar el concepto de Riesgo con la Estrategia Corporativa de la entidad.
- Liderar la gestión del riesgo desde el más alto nivel de la entidad.
- Gestionar el riesgo en forma integral y no en forma de “silos”

Características de Gestión de Riesgos:

- Aplicación amplia (control interno, KPI, planes de incentivos, estructuración de reportes gerenciales, etc.).
- Herramienta de Gobierno Corporativo.
- Apoyo relevante frente a las tendencias de autorregulación.
- Focalizado en riesgos relevantes

2.1.6 Ciclo De La Gestión De Riesgos

Figura 2.1. Ciclo de la Gestión de Riesgos



Como se menciona en [WWW 02] la Gestión de riesgos tiene 6 fases principales.

- Identificar los riesgos
- Evaluar los riesgos

- Identificar las respuestas respectivas a los riesgos
- Seleccionar
- Planes y Recursos
- Monitoreo y Reportes

a) Identificar los Riesgos

En este paso se identifican los riesgos potenciales que enfrenta un proyecto. Es importante no juzgar la probabilidad de un riesgo en esta fase temprana. Esto se hace de una manera controlada en una fase posterior.

Una vez identificados, los riesgos están inscritos en el registro del riesgo. Esta contiene detalles de todos los riesgos, su evaluación, los propietarios y el estado. El registro de riesgos es una herramienta de control para el administrador del proyecto, proporcionando una referencia rápida de los riesgos clave que enfrenta el proyecto, qué actividades de seguimiento deben tener lugar y por quién.

b) Evaluar los Riesgos

Se refiere a la evaluación de la probabilidad y el impacto de los riesgos individuales, teniendo en cuenta las interdependencias o de otros factores fuera del ámbito de aplicación inmediata en la investigación.

La probabilidad es la posibilidad de evaluar un resultado en particular ocurriendo (incluyendo un examen de la frecuencia con que los resultados puedan surgir). Por ejemplo, grandes daños a un edificio es relativamente poco probable que suceda, pero tendría un impacto enorme en la continuidad del negocio. Por el contrario, de vez en cuando personal rota en las áreas esto es bastante probable que suceda, pero no suelen tener un gran impacto en el negocio como el ejemplo anterior.

El impacto es el efecto de una incidencia ya ocurrida a q està sucediendo. El impacto idealmente debe ser considerado bajo los elementos de:

- Tiempo
- Costos
- Calidad
- Beneficio
- Personas / recursos

c) Identificar respuestas a los riesgos

Se muestran 5 tipos de respuesta a los riesgos:

Prevención

Eliminar el riesgo, haciendo los procesos de manera diferente se elimina el riesgo. Las contramedidas se ponen en el lugar

que sea para detener la amenaza o el problema o evitar que tengan algún impacto en el proyecto o negocio.

Reducción

Tratar el riesgo, tomar medidas para controlar de alguna manera el riesgo, las acciones o bien reducen la probabilidad de que el riesgo se desarrolle o limitar el impacto en el proyecto a niveles aceptables.

Transferencia

Esta es una forma especializada de la reducción de riesgos en la gestión del riesgo se transfiere a un tercero a través de, por ejemplo, una póliza de seguros o cláusula penal, de tal manera que el impacto del riesgo ya no es un problema para la salud del proyecto. No todos los riesgos pueden ser transferidos de esta manera.

Aceptación

Tolerar el riesgo, tal vez porque nada se puede hacer a un costo razonable para mitigar o la probabilidad y el impacto de los riesgos se producen a un nivel aceptable.

Contingencia

Se trata de acciones planificadas y organizadas para entrar en vigencia siempre y cuando el riesgo se produce.

d) Seleccionar

Selección de las acciones de riesgo para tener un equilibrio. Para cada acción posible es cuestión de equilibrar el coste de tomar la acción en contra de la probabilidad y el impacto de permitir que el riesgo se produzca. Hay muchos elementos que deben tenerse en consideración.

Puede haber varias acciones de riesgo posible, cada uno con diferentes efectos. La elección puede ser una de estas opciones o una combinación de dos o más.

e) Planes y Recursos

Una vez hecha la selección, la ejecución de las acciones seleccionadas tendrán una planificación y dotación de recursos y es probable que incluya cambios en los planes, tareas nuevas o modificadas:

Planificación, para las acciones de contramedida detallada durante las actividades de evaluación del riesgo, se compone de:

- Identificar la cantidad y tipo de recursos necesarios para llevar a cabo las acciones.

- Desarrollar un plan de acción detallado, que deberá quedar incluido en los Planes de Etapas y Proyecto ya sea como actividades adicionales o como un plan de contingencia.
- Confirmar la conveniencia de llevar a cabo las acciones identificadas durante la evaluación del riesgo a la luz de cualquier información adicional adquirida.
- Obtener la aprobación de la gestión, junto con todos los demás aspectos de los planes que se producen.

Recursos, servirá para determinar y asignar los recursos reales que se utilizarán para llevar a cabo los trabajos necesarios a través de las acciones, estas asignaciones se muestra en la etapa de proyectos y planes; ya que son acciones que estamos comprometidos a llevar a cabo, las acciones de los contingentes normalmente se financiará con un presupuesto de contingencia.

f) Monitoreo y Reportes

Debe haber mecanismos de seguimiento y presentación de informes sobre las acciones seleccionadas para abordar los riesgos. Algunas de las acciones pueden haber sido sólo para controlar los riesgos identificados en busca de signos de un cambio en su estado.

2.1.7 Estrategias De Riesgos

a) Estrategias Reactivas

Las estrategias reactivas son aquellas que se ponen en ejecución después de haberse producido la amenaza.

Es decir se evalúan las consecuencias cuando este ya se ha producido.

Las consecuencias de esta estrategia es que se pone en peligro el proyecto ya que podría o no mitigarse el riesgo.

b) Estrategias Proactivas

Son aquellas que se hace una evaluación previa y sistemática de todos los posibles riesgos a ocurrir. Se evalúan las consecuencias, se elaboran planes para evitar y minimizar las consecuencias, finalmente se obtendrá un plan de contingencia.

Esta estrategia es recomendable ya que se evade los riesgos y además la reacción se da en un tiempo menor a la anterior.

2.2 Metodologías de Gestión de Riesgos

2.2.1 Guía del PMBOK

La guía del PMBOK de PMI [PRO 04], plantea seis procesos descritos en términos de entradas, herramientas y técnicas y salidas, presentes en la gestión de riesgos, interactuantes entre sí. Cada

proceso tiene lugar por lo menos una vez en cada proyecto, y se realiza en una o más fases del proyecto, si el proyecto se encuentra dividido en fases:

- Planificación de la gestión de riesgos
- Identificación de riesgos
- Análisis cualitativo de riesgos
- Análisis cuantitativo de riesgos
- Planificación de la respuesta a los riesgos
- Seguimiento y control de riesgos

Los anteriores seis procesos descritos ampliamente en la guía del PMBOK, constituyen un enfoque sobre cómo gestionar los riesgos en la administración de proyectos; sin embargo existen otras metodologías que se enfocan específicamente en la gestión de riesgos de proyectos de desarrollo de software.

2.2.2 Control Objectives for Information and related Technology (COBIT)

Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información,(ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

En su cuarta edición, COBIT tiene 34 objetivos de alto nivel que cubren 318 objetivos de control (específicos o detallados) clasificados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y, Supervisión y Evaluación. En inglés: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.

2.2.3 Rational Unified Process (RUP)

Uno de los objetivos de RUP menciona en **[ALF 07]** es asegurar que las expectativas de todas las partes son sincronizadas y consistentes. Esto es asegurado a través de evaluaciones periódicas durante el ciclo de vida del proyecto, y es documentado en el Reporte de Evaluación de Status. Este reporte es utilizado para hacer un seguimiento a información acerca de recursos (humano y financiero), mayores riesgos, progreso técnico medido a través de métricas y resultados de hitos principales. Con RUP hacemos uso de las siguientes clases de métricas:

- Progreso (líneas de código, número de clases, puntos de función por iteración, rehacer)
- Estabilidad (tipo de rehacer, volatilidad de requerimientos o implementación)
- Adaptabilidad (costo de rehacer)
- Modularidad (extensión del impacto de rehacer)

- Calidad (velocidad de descubrimiento de defectos, densidad, profundidad e inherencia, indicador de rehacer).
- Madurez (horas de prueba por falla)
- Perfil de desembolso de recursos (planeados versus actuales)

Los documentos RUP que contienen los planes y compromisos son:

- Casos de Negocio
- Plan de Desarrollo de Software
- Plan de Medición
- Lista de Riesgos
- Plan del Proyecto
- Plan(es) de Iteración
- Evaluación(es) de Iteración, y
- Evaluación(es) de Status

La Lista de Riesgos es un artefacto de RUP que nos provee una visión de todos los riesgos conocidos en el proyecto, y sirve como entrada para la planificación y evaluación del proyecto. Cada riesgo es descrito en función de su impacto, y un plan de contingencia será desarrollado para mitigar el riesgo en cuestión.

La Lista de Riesgos es desarrollada junto con los Casos de Negocio, los cuales formarán la base para la decisión de continuar o no con el proyecto. La Lista de Riesgos es mantenida a través de todo el ciclo de vida del proyecto.

2.2.4 Capability Maturity Model Integrated (CMMI)

Se ha convertido en el nuevo estándar a nivel mundial para la medición de la calidad de los procesos de desarrollo de software y presenta como una de sus PA (Process Area) fundamentales de Nivel 3 la Administración de Riesgos.

2.3 Estado del Arte

2.3.1 Estándar PMBOK

2.3.1.1 Definición

Según [WWW 03] menciona:

“La Guía del PMBOK® es un estándar en la gestión de proyectos desarrollado por el Project Management Institute (PMI). Se encuentra disponible en 11 idiomas: inglés, español, chino simplificado, ruso, coreano, japonés, italiano, alemán, francés, portugués de Brasil y árabe.

En 1987, el PMI publicó la primera edición del PMBOK® en un intento por documentar y estandarizar información y prácticas generalmente aceptadas en la gestión de proyectos. La edición actual, la cuarta, provee de referencias básicas a cualquiera que esté interesado en la gestión de proyectos. Posee un léxico común y una estructura consistente para el campo de la gestión de proyectos.

La Guía del PMBOK es ampliamente aceptada por ser el estándar en la gestión de proyectos.”

2.3.1.2 PMBOK en la Gestión de Riesgos

PLANIFICACIÓN

- Planificación de la Gestión de Riesgos: decidir cómo abordar y planificar las actividades de gestión de riesgos en el proyecto.
- Identificación de Riesgos: determinar cuáles son los riesgos que pueden afectar al proyecto y documentar sus características.
- Análisis Cualitativo de Riesgos: realizar un análisis cualitativo de los riesgos y sus condiciones para priorizar sus efectos sobre los objetivos del proyecto.
- Análisis Cuantitativo de Riesgos: estimar la probabilidad y consecuencias de los riesgos y sus implicaciones sobre los objetivos del proyecto.
- Planificación de Respuestas a los Riesgos: elaborar procedimientos y técnicas para oportunidades de mejora y reducir las amenazas a los objetivos del proyecto.

CONTROL

- Supervisión y Control de Riesgos: supervisar los riesgos residuales, identificar nuevos riesgos, ejecutar planes de Reducción de riesgos, y evaluar su efectividad a lo largo del ciclo de vida del proyecto.

2.3.2 Estándar COBIT

2.3.2.1 Gestión De Riesgos En COBIT

En el proceso PO 9. -Planificar y Organizar-. **Evaluar y Administrar los riesgos de TI:** Se establecen los principios que deben tenerse en cuenta para la gestión de los riesgos.

Se establece que debe crearse y mantenerse un marco adecuado de trabajo para la gestión de riesgos.

Dicho marco de trabajo debe documentar un nivel común y acordado de riesgos TI, estrategias para mitigarlos y riesgos que se acuerden aceptar como residuales.

Cualquier riesgo potencial sobre las metas u objetivos de la organización, causado por algún evento no planificado, se tiene que identificar, analizar y evaluar.

Objetivos de control detallados correspondientes al proceso

PO 9

P9 O.1.- Alineación de la administración o gestión de riesgos de TI con el negocio. Se debe integrar el gobierno, la administración del riesgo y el marco del control de TI, al marco de trabajo de la administración de riesgos de la organización.

PO 9.2.- Establecimiento del contexto del riesgo. Se debe establecer el contexto en el cual el marco de trabajo de la evaluación de riesgo se aplica para garantizar los resultados apropiados.

PO 9.3.- Evaluación de eventos. Identificar aquellos eventos (amenazas y vulnerabilidades) con un impacto potencial sobre objetivos, retos u operaciones de la empresa, aspectos de negocio, regulatorios, legales, tecnológicos, de sociedad comercial, de recursos humanos y operaciones.

PO 9.4.- Evaluación de riesgos TI. Se debe evaluar de forma recurrente la posibilidad de impacto de todos los riesgos identificados, usando métodos cualitativos y cuantitativos.

PO 9.5.- Respuesta a los riesgos. Debemos identificar a los propietarios de los riesgos y a los dueños de los procesos afectados y elaborar y mantener respuestas a los riesgos que garanticen que los controles rentables y las medidas de seguridad mitigan y reducen la exposición a los riesgos de forma continua.

PO 9.6.- Mantenimiento y monitoreo de un plan de acción de riesgos. Debemos asignar prioridades y planear las actividades de control a todos los niveles para implantar las respuestas a los riesgos que sean necesarias, incluyendo costos y beneficios así como la responsabilidad de la ejecución.

CAPÍTULO III

PROPUESTA DEL MARCO DE TRABAJO BASADO

EN COBIT Y PMBOK

3.1 FINALIDAD DEL MARCO DE TRABAJO

La finalidad principal de nuestra propuesta planteada es brindar a cualquier compañía, que gestione proyectos de desarrollo de TI, un marco de trabajo con el cual podrán obtener un proceso adecuado de la Gestión de Riesgos. Nuestro marco de trabajo propuesto está basada en el estándar COBIT 4.0 y la guía PMBOK 3era Edición.

Independiente de la realidad tecnológica de cada caso concreto, COBIT determina, con el respaldo de las principales técnicas internacionales, un conjunto de mejores prácticas para la seguridad, la calidad, la eficacia y la eficiencia de TI que son necesarias para alinear TI con el negocio, identificar riesgos, entregar valor al negocio, gestionar recursos y medir el desempeño, el cumplimiento de metas y el nivel de madurez de los procesos de la organización. Complementando a este concepto con la guía del PMBOK podemos gestionar los riesgos de TI adecuadamente para poder llegar a la obtención de una eficiente gestión de riesgos alineados a los procesos del negocio.

3.2 DIRIGIDO PARA

Este marco de trabajo está dirigido básicamente al Jefe de Proyecto, Coordinador de Proyecto, Encargado del Proyecto o por toda aquella persona que tiene la necesidad de gestionar los riesgos de proyectos de TI. Por otro lado esta metodología está dirigida para apoyar las comunicaciones con la alta gerencia con respecto a los riesgos del proyecto evaluado. De la misma manera apoyará aquellos que toman decisiones de

inversiones, aquellos que deciden con respecto a requerimiento y aquellos que utilizan los servicios de TI.

3.3 DEFINICIÓN DEL MARCO DE TRABAJO

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

La Gerencia está buscando constantemente información condensada y oportuna para tomar decisiones difíciles sobre riesgo y control de manera rápida y exitosa.

En este punto del documento describiremos el marco de trabajo propuesto, el cual gestionará la gestión de riesgos de los proyectos de TI que tienen un impacto ya sea directo o indirecto a la mejora de los procesos.

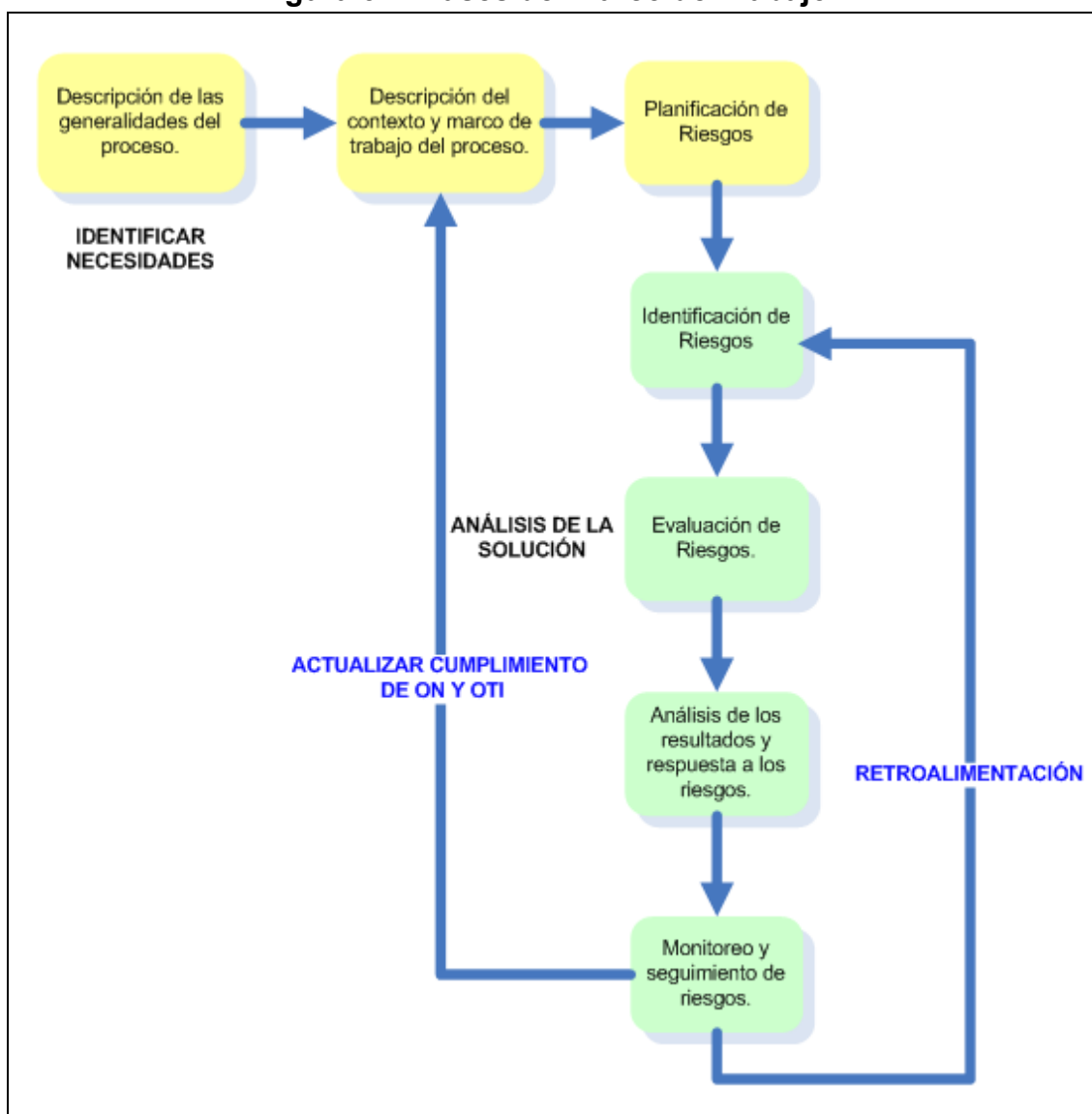
Esta propuesta de marco de trabajo es lo suficientemente general para ser adaptada para cualquier tipo de proceso que esté relacionado con Proyectos de Tecnología de la Información. Fue elaborada considerando muchos aspectos importantes que son necesarios para la recopilación de información relevante para la alta gerencia.

Para este planteamiento se han determinados las siguientes etapas:

- 3.3.1 FASE 1. Descripción del Contexto y Marco de Trabajo de los Procesos.
- 3.3.2 FASE 2. Descripción de las Generalidades de los Procesos.
- 3.3.3 FASE 3. Planificación de Riesgos.
- 3.3.4 FASE 4. Identificación de Riesgos.
- 3.3.5 FASE 5. Evaluación de Riesgos.
- 3.3.6 FASE 6. Análisis de los Resultados de la Evaluación de Riesgos.
- 3.3.7 FASE 7. Monitoreo y Seguimiento de los Riesgos.

En la **Figura 3.1** presentaremos el diagrama en la cual mostraremos como van interactuar las fases de nuestro marco de trabajo:

Figura 3.1: Fases del Marco de Trabajo



En el **Cuadro 3.1** haremos una breve descripción de las fases comprometidas en la propuesta metodológica que estamos realizando, para mayor detalle de las fases involucradas podemos revisar los puntos en los cuales se detalla profundamente que significa y que acciones realizaremos por cada fase.

Cuadro 3.1. Descripción de las Fases de la Propuesta Metodológica

ID	FASE	DESCRIPCIÓN
1	Descripción del Contexto y Marco de Trabajo de los Procesos	En esta primera fase de la propuesta metodológica necesitamos realizar un análisis del proceso(s) de la empresa para de esa forma poder detallar los objetivos del negocio y los objetivos de TI, estos objetivos se recopilarán a través de las entrevistas programadas con la Gerencia General y/o los Jefes de Departamento. Además identificaremos el nivel de implementación del Gobierno de TI en la empresa y realizaremos un análisis del Marco de Control en el cual presentaremos los procesos COBIT y los objetivos de control seleccionados que permitirán el cumplimiento de los objetivos del departamento de sistemas.
2	Descripción de las Generalidades del Proceso	En esta fase identificaremos el proceso a ser evaluado, ya que este nos proporcionará los indicadores del proceso y una visión más realista de cada actividad contemplada de cada proyecto que genere un impacto y un posible riesgo. Es importante que el responsable de gestión de proyecto conozca los procesos relacionados con los proyectos de desarrollo de TI que puede tener a su cargo, ya que a través de estos se están realizando mejoras directamente al proceso del negocio.
3	Planificación de Riesgos	En la fase plan de gestión de riesgos describiremos como se estructurará y realizará la gestión de riesgos en el proyecto. En el plan de gestión de riesgos estamos considerando incluir los siguientes puntos que son importantes: - Metodología de la Gestión de Riesgos. - Roles y Responsabilidades de la Gestión de Riesgos.

		- Periodicidad de la Gestión de Riesgos. Además definiremos los valores de probabilidad, impacto y nivel de riesgo.
4	Identificación de los Posibles Riesgos	En esta cuarta fase de la propuesta metodológica, determinaremos que riesgos pueden afectar al proyecto y se procederá a documentar sus características.
5	Evaluación de Riesgos	En esta quinta fase realizaremos la evaluación de los riesgos identificados para ello se ha contemplado realizar un análisis cualitativo de riesgos en el cual determinaremos la probabilidad, nivel de impacto y nivel de riesgo de los riesgos identificados y que afectación tiene sobre los objetivos de TI asociados.
6	Análisis de Resultados de la Evaluación de Riesgos	En esta fase de la propuesta metodológica realizaremos un análisis de los resultados de la evaluación de riesgos en el cual desarrollaremos opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. Par ello haremos uso de los siguientes documentos: - Plan de Respuesta a Riesgos.
7	Monitoreo de los Riesgos Residuales	La última fase de seguimiento y control se compone de aquellos procesos realizados para el seguimiento de la ejecución del proyecto de forma que se puedan identificar los posibles problemas oportunamente y adoptar las acciones correctivas, cuando sea necesario, para controlar la ejecución del proyecto. El equipo del proyecto debe determinar cuáles de los procesos son necesarios para el proyecto específico del equipo. El beneficio clave de esta última fase es que el rendimiento del proyecto se observa y se mide regularmente para identificar las variaciones respecto del plan de gestión del proyecto. La fase de seguimiento y control también incluye controlar los cambios y recomendar acciones preventivas como anticipación de posibles problemas. Por ello haremos uso de las acciones correctivas e información sobre el rendimiento de trabajo.

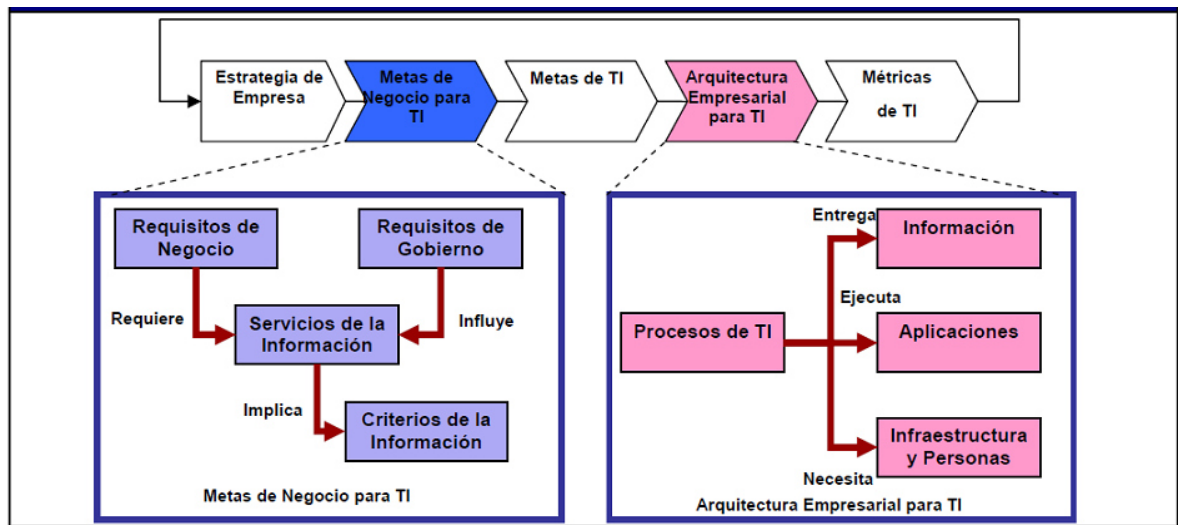
3.3.1 Fase 1: Descripción del Contexto y Marco de Trabajo de los Procesos.

Para este análisis necesitamos detallar los objetivos del negocio y los objetivos de TI, estos objetivos se recopilarán a través de las entrevistas programadas con la Gerencia General y/o los Jefes de Departamento.

La norma COBIT 4.0 nos menciona lo siguiente: Si se pretende que TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio y un claro entendimiento de TI, de cómo y qué debe entregar. La **Figura 3.2** ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos relacionados con iniciativas habilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar, de forma exitosa la parte que les corresponde a TI de la estrategia empresarial.

Para que la alta gerencia de la empresa entienda las metas de los Scorecard de TI, todos estos objetivos y sus métricas asociadas se deben expresar en términos de negocio significativos para la alta gerencia de la empresa, y esto, combinado con la alineación efectiva de la jerarquía de objetos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio.

Figura 3.2



3.3.1.1 Objetivos del Negocio:

En el **Anexo 1** definiremos los objetivos del negocio de la empresa con los cuales podremos cuantificar las aspiraciones que se tienen o conocer las metas a las cuales se quieren llegar, para ello es necesario conocer el negocio, el modelo del negocio, cual es su participación en el mercado y la estrategia de posicionamiento en el mismo.

En el Cuadro 3.2 se detallaran los campos que son necesarios ingresar en el **Anexo 1**.

Cuadro 3.2: Descripción de Campos del Anexo 1.

CAMPO	SUBCAMPO	DESCRIPCIÓN
Control de Versiones	Versión	Versión del documento en el momento, por Ej. 1.0,1.1, etc.
	Hecha por	Nombre del responsable de la creación o modificación del documento.
	Revisado por	Nombre del responsable de revisar la calidad y nivel del documento.
	Aprobado por	Nombre de la persona quien aprueba el documento.
	Fecha	Fecha de creación, modificación, revisión o aprobación del documento.
	Motivo	Descripción del motivo por el cual se realiza la acción.
Cod. ON	Código identificador de los objetivos del negocio, por ej.: ON1, ON2, etc.	
Objetivos del Negocio	Se describirá el objetivo del negocio relacionado con el proceso.	
Indicadores	Se hará mención a los indicadores con los cuales se medirá este objetivo del negocio.	

3.3.1.2 Objetivos del TI:

Un objetivo de TI es la meta a la cual se quiere llegar dentro de las actividades de TI. Se hará uso del **Anexo 2** para identificar y describir todos los objetivos de TI de la empresa. A continuación de detallaran los campos del **Anexo 2**.

Cuadro 3.3: Descripción de Campos del Anexo 2.

CAMPO	DESCRIPCIÓN
Cod. OTI	Código identificador de los objetivos de TI, por ej.: OTI1, OTI2, etc.
Objetivos de TI	Se describirá el objetivo de TI alineados con los objetivos del negocio (Anexo 1).
Indicadores de Medición	Se hará mención a los indicadores que se tienen que cumplir.
Procesos de TI que soporta el objetivo	Se documentará el proceso, procedimiento o actividad que soporta el objetivo de TI.

Es importante que la empresa tenga implementado un Gobierno de TI y que los objetivos de TI estén alineados a los objetivos del negocio. Por ello en el **Anexo 3** se ingresará la descripción del nivel del Alineamiento Estratégico, Entrega de Valor, Administración de Riesgos, Administración de Recursos y Medición de Rendimiento con los cuales cuenta la empresa en cuestión.

3.3.1.3 Necesidad de Implementación de Gobierno de TI

Se considera necesario implementar los dominios de Alineamiento Estratégico, Entrega de Valor, Medición de Rendimiento y Administración de Riesgos basados en COBIT. A continuación describiremos los campos correspondientes al **Anexo 3**, en el cual evaluaremos el nivel de implementación del Gobierno de TI en la empresa.

- 1. Alineamiento Estratégico:** La empresa considera a TI como un área estratégica para el logro de sus objetivos por lo que se requiere un proceso de alineamiento de los objetivos de TI con el negocio. Con este alineamiento cualquier cambio o nuevo requerimiento no contemplado en el plan y presupuesto de TI deberá ser revisado y aprobado por el Comité de Sistemas, en el caso que lo haya.
- 2. Entrega de Valor:** Se requiere valorizar adecuadamente los proyectos de TI, evaluar el costo-beneficio y comprender los beneficios reales.
- 3. Administración de Recursos:** Aquí buscaremos la relación que tiene la Empresa con la inversión óptima y adecuada administración de los recursos críticos de TI: aplicaciones, información, infraestructura y las personas. Problemas claves relacionados a la optimización del conocimiento e infraestructura.
- 4. Administración de Riesgos:** Se requiere crear conciencia sobre los riesgos de tecnologías de información y establecer un sistema de administración de riesgos principalmente en la gestión de proyectos de TI (para ello haremos uso del PMBOK). Ello permitirá asegurar el cumplimiento de los objetivos.
- 5. Medición de Rendimiento:** Se requiere que los resultados obtenidos por el Departamento de Sistemas sean

transparentes y visibles para la alta gerencia vía indicadores de gestión sobre el rendimiento de los procesos y objetivos de TI. Esto apoyara al sustento de cambios y mejoras.

Las actividades de la empresa requieren información de las actividades de TI con el fin de satisfacer los objetivos del negocio. La empresa debe asegurar la interdependencia entre su plan estratégico y sus actividades de TI. TI debe estar alineado y debe permitir a la empresa tomar ventaja total de su información para maximizar sus beneficios, capitalizar oportunidades y ganar ventaja competitiva.

Luego de haber detallado la importancia del porque la empresa debe tener implementado un Gobierno de TI y en caso de que ya lo tenga entonces solo se hará uso de la información que tenga para poder analizarlo. Para esto haremos uso de lo siguiente:

- Marco de Control.
- Mapeo de Procesos.

3.3.1.4 Marco de Control:

La versión de COBIT 4.0 nos menciona que es importante tener un Marco de Control para el Gobierno de TI ya que en este podemos definir las razones de por qué se necesita el Gobierno de TI, los interesados y que se necesita cumplir en el Gobierno de TI.

Sabemos que cada vez más, la alta dirección se está dando cuenta del impacto significativo que la información puede tener en el éxito de una empresa. La dirección espera un alto entendimiento de la manera en que la tecnología de información (TI) es operada y de la posibilidad de que sea aprovechada con éxito para tener una ventaja competitiva. En particular, la alta dirección necesita saber si con la información administrada en la empresa es posible que:

- Garantice el logro de sus objetivos.
- Tenga suficiente flexibilidad para aprender y adaptarse.
- Cuento con un manejo juicioso de los riesgos que enfrenta.
- Reconozca de forma apropiada las oportunidades y actúe de acuerdo a ellas.

Si queremos que la empresa sea parte del grupo de empresas exitosas, entonces esta debe entender los riesgos y aprovechar los beneficios de TI, y encontrar maneras para:

- Alinear la estrategia de TI con la estrategia del negocio.
- Asegurar que los inversionistas y accionistas logran un debido cuidado estandarizado para la mitigación de los riesgos de TI.
- Lograr que toda la estrategia de TI, así como las metas fluyan de forma gradual a toda la empresa.
- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas.

- Crear relaciones constructivas y comunicaciones efectivas entre el negocio y TI, y con socios externos.
- Medir el desempeño de TI.

En este punto del documento presentaremos los objetivos de control seleccionados relacionados con los procesos COBIT a los cuales afecta directamente. Estos objetivos de control nos permitirá el cumplimiento de los objetivos del Área de Sistemas. Para ello en el Cuadro 3.4 describiremos los campos correspondientes al **Anexo 4** en el cual ingresaremos los datos correspondientes al Marco de Control.

Cuadro 3.4: Marco de Control

CAMPO	SUBCAMPO	DESCRIPCIÓN
Cod. OTI		Código identificador de los objetivos de TI, por ej.: OTI1, OTI2, etc. Ver anexo 2.
Objetivos de TI		Se describirá el objetivo de TI alineados con los objetivos del negocio (Anexo 2).
Objetivos de Control		Se describirá el objetivo de control asociado a cada objetivo de TI descrito.
N.C		Ver Cuadro 3.5.
Dominios y Procesos de COBIT		Se hará mención al dominio y proceso de COBIT que se esta afectando.
Objetivos de Control Detallado		Se describirá el objetivo de control detallado asociado a cada dominio o proceso de COBIT.

Nivel de Cumplimiento (N.C): Define el nivel de realización de los objetivos de control identificados; para ello hemos considerado cuatro niveles de cumplimiento:

- Implementado.
- Parcialmente Implementado.
- Pendiente de Implementar.
- N.A.

Cuadro 3.5: Nivel de Cumplimiento del Objetivo de Control

Nivel de cumplimiento		Descripción
	Implementado	El objetivo de control respectivo se encuentra implementado
	Parcialmente implementado	El objetivo de control respectivo se encuentra en proceso de implementación
	Pendiente de implementar	El objetivo de control respectivo no se encuentra implementado ni en proceso de implementación
X	N.A.	El objetivo de control respectivo no aplica a la Compañía

3.3.1.5 Mapeo de Procesos:

En esta parte del documento presentaremos un cuadro para poder presentar el mapeo de procesos COBIT y como ellos soportarían los dominios de Gobierno de TI, los recursos de TI involucrados y los criterios de información.

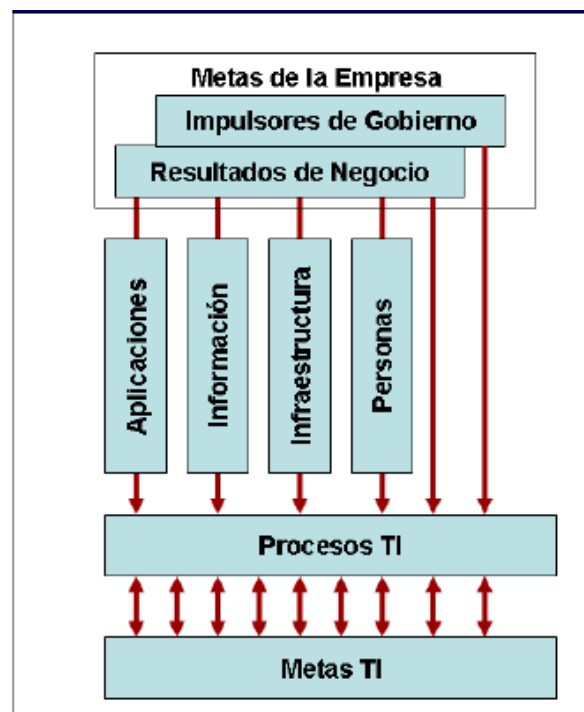
Para detallar el Mapeo de Procesos haremos uso del **Anexo 5**, cuyos campos a ingresar se muestran en la Cuadro 3.6.

Cuadro 3.6: Mapeo de Procesos

CAMPO	SUBCAMPO	DESCRIPCIÓN
Objetivos de Control	Se describirá el objetivo de control asociado a cada objetivo de TI descrito. Ver Anexo 4.	
Dominios y Procesos de COBIT	Se hará mención al dominio y proceso de COBIT que se está afectando. Ver Anexo 4.	
Objetivos de Control Detallado	Se describirá el objetivo de control detallado asociado a cada dominio o proceso de COBIT. Ver Anexo 4.	
Gobierno de TI	Alineamiento Estratégico	La empresa considera a TI como un área estratégica para el logro de sus objetivos por lo que se requiere un proceso de alineamiento de los objetivos de TI con el negocio. Con este alineamiento cualquier cambio o nuevo requerimiento no contemplado en el plan y presupuesto de TI deberá ser revisado y aprobado por el Comité de Sistemas, en el caso que lo haya.
	Entrega de Valor	Se requiere valorizar adecuadamente los proyectos de TI, evaluar el costo-beneficio y comprender los beneficios reales.
	Gestión de Recursos	Aquí buscaremos la relación que tiene la Empresa con la inversión óptima y adecuada administración de los recursos críticos de TI: aplicaciones, información, infraestructura y las personas. Problemas claves relacionados a la optimización del conocimiento e infraestructura.
	Gestión de Riesgos	Se requiere crear conciencia sobre los riesgos de tecnologías de información y establecer un sistema de administración de riesgos principalmente en la gestión de proyectos de TI (para ello haremos uso del PMBOK). Ello permitirá asegurar el cumplimiento de los objetivos.
	Medición y Rendimiento	Se requiere que los resultados obtenidos por el Departamento de Sistemas sean transparentes y visibles para la alta gerencia via indicadores de gestión sobre el rendimiento de los procesos y objetivos de TI. Esto apoyara al sustento de cambios y mejoras.
Recursos de TI	Personas	Son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.
	Información	Son datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.
	Aplicaciones	Incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
	Infraestructura	Hace referencia a las tecnologías y las instalaciones que permiten el proceso de las aplicaciones.
Criterios de Información	Efectividad	Relaciona con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.
	Eficiencia	Consiste en que la información sea generada con el optimo

		uso de los recursos.
	Confidencialidad	Se refiere a la protección de información sensible contra revelación no autorizada.
	Integridad	Está relacionada con la precisión de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
	Disponibilidad	Hace referencia a que la información está disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
	Cumplimiento	Tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.
	Confiabilidad	Hace referencia a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades fiduciarias y de gobierno.

La siguiente figura nos muestra como las metas u objetivos de negocio para TI influyen sobre la forma en que se manejan los recursos necesarios de TI por parte de los procesos de TI para lograr los objetivos o metas de TI.



Para los campos Gobierno de TI, Recurso de TI y Criterios de Información pertenecientes al cuadro 3.6 se consideran los siguientes valores que se deben ingresar:

- P: Nivel Principal.
- S: Nivel Secundario.
- X: Aplica.

3.3.2 Fase 2: Descripción de las Generalidades de los Procesos.

En esta fase es importante entender todos los procesos correspondientes al negocio, ya que este nos proporcionará las variables del sistema como una visión más realista de cada actividad contemplada de cada proyecto que genere un impacto y un posible riesgo.

En esta fase lo que se pretende es conocer también las características más importantes de los procesos del negocio, tales como las entradas, las salidas, los indicadores y toda la información que se considere relevante de carácter informativo para el investigador. Se considera obtener estos datos con checklist de documentos, consulta con los responsables de los procesos y los proyectos relacionados a los procesos.

Es importante que el responsable de gestión de proyecto conozca el proceso relacionado con los proyectos de desarrollo de TI que puede tener

a su cargo, ya que a través de estos se están realizando mejoras directamente al proceso del negocio.

En el documento **Anexo 6** se detallara la descripción del proceso, esto quiere decir que será un documento por cada proceso descrito.

Luego de haber descrito el proceso se procederá a realizar su respectivo diagrama, debemos tener en cuenta que si el proceso es complejo este puede detallarse en uno o más procedimientos para ello lo que se va realizar es un diagrama por cada procedimiento, esto se detalla en el punto “Diagrama del Procedimiento del Proceso” del **Anexo 6**.

En la **Cuadro 3.7** se detallan los campos obligatorios a llenar en el Anexo 6.

Cuadro 3.7: Descripción de Campos del Anexo 6.

CAMPO	SUBCAMPO	DESCRIPCIÓN
Control de Versiones	Versión	Versión del documento en el momento, por Ej. 1.0,1.1, etc.
	Hecha por	Nombre del responsable de la creación o modificación del documento.
	Revisado por	Nombre del responsable de revisar la calidad y nivel del documento.
	Aprobado por	Nombre de la persona quien aprueba el documento.
	Fecha	Fecha de creación, modificación, revisión o aprobación del documento.
	Motivo	Descripción del motivo por el cual se realiza la acción.
Proceso	Nombre de proceso precedido por el acrónimo establecido en la definición de los elementos de la estructura del modelo del proceso.	
Propósito	Objetivos generales medibles y resultados esperados de la implantación efectiva del proceso.	
Objetivos	Objetivos específicos cuya finalidad es asegurar el cumplimiento del propósito del proceso. Los objetivos se identificaran como O1, O2, etc.	
Indicadores	Nº	Código identificador del indicador, por Ej.: I1, I2, etc.

	Tipo	Se ingresaran solo valores de: KGI: Indicadores claves de meta que definen mediciones para informar a la gerencia si un proceso de TI alcanzo los requerimientos del negocio. KPI: Indicadores claves de desempeño que definen mediciones para determinar que tan bien se esta desempeñando el proceso de TI para alcanzar la meta.
	Descripción	Descripción de los indicadores registrados.
Metas Cuantitativas	Valor numérico o rango de satisfacción del indicador.	
Responsabilidad y Autoridad	Responsabilidad es el rol principal responsable por la ejecución del proceso y el cumplimiento de su propósito.	
Procesos Relacionados	Nombre de los procesos relacionados.	
Entradas	Nombre	Nombre del recurso o actividad
	Fuente	Referencia al origen del recurso o actividad.
Salidas	Nombre	Nombre del recurso o actividad
	Descripción	Descripción y característica del recurso o actividad.
	Destino	Referencia al destinatario del recurso o actividad
Vigencia	Inicio	Fecha en la que se inicia el periodo de vigencia de la última versión de la documentación del proceso.
	Revisión	Fecha en la que prevé la revisión de la última versión de la documentación del proceso.
	Fin	Fecha en la finaliza el periodo
Diagrama del Procedimiento del Proceso	ID Procedimiento	Código que identifica un procedimiento (un proceso pueda estar compuesto por uno o varios procedimientos). Esta compuesto por el código identificador del proceso seguido de un número correlativo.
	Titulo del Procedimiento	Nombre del procedimiento
	Tarea o Actividad	Descripción de la actividad a realizar. Cada actividad se documenta como un renglón dentro del cuadro contenido en esta sección.
	Tipo de Tarea	Actividad del procesamiento de algún tipo. Actividad de toma de decisión. Actividad de análisis de entrada y/o emisión de salidas. Actividad de documentación.
	Registro	Nombre del registro generado por la actividad.
	Sección del Registro	Sección en la que se registra algún control definido por la actividad.
	Responsable	Persona encargada e ejecutar la actividad.

3.3.3 Fase 3: Planificación de la Gestión de Riesgos:

El plan de gestión de riesgos describe como se estructura y realizara la gestión de riesgos en el proyecto. En el plan de gestión de riesgos estamos considerando incluir los siguientes puntos que son importantes:

- Metodología de la Gestión de Riesgos: Se definen los métodos o procesos, las herramientas y las fuentes de información que pueden utilizarse para realizar la gestión de riesgos de un proyecto.
- Roles y Responsabilidades de la Gestión de Riesgos: Se define el líder, el apoyo y los miembros del equipo de gestión de riesgos para cada tipo de actividad del plan de gestión de riesgos, se asignaran personas a estos roles y se explicaran las responsabilidades asociadas.
- Periodicidad de la Gestión de Riesgos: Se definen cuándo y con qué frecuencia se realizara el proceso de gestión de riesgos durante el ciclo de vida del proyecto, y establece las actividades de gestión de riesgos que se incluirá en el cronograma del proyecto.

En el Cuadro 3.8 se muestra una descripción de los datos que se han considerado relevantes para realizar las actividades correspondientes a la Planificación de Gestión de Riesgos. Para mayor detalle ver **Anexo 7**.

Cuadro 3.8: Planificación de la Gestión de Riesgos

CAMPO	SUBCAMPO	DESCRIPCIÓN
METODOLOGIA DE KA GESTION DE RIESGOS	Proceso	Nombre del proceso que se va ejecutar.
	Descripción	Descripción del proceso que se va ejecutar
	Herramientas	Herramientas a usar para la ejecución del proceso.
	Fuentes de Información	Responsables de donde se obtuvo la información.
ROLES Y RESPONSABILIDADES DE LA GESTIÓN DE RIESGOS	Proceso	Nombre del proceso que se va ejecutar.
	Roles	Nombre del equivalente a las funciones y/o acciones que realizara una persona,
	Personas	Se ingresan las iniciales de los nombres de las personas responsables.
	Responsabilidades	Se detallan las responsabilidades que tienen las personas según el rol que desempeñan.
PERIODICIDAD DE LA GESTIÓN DE RIESGOS	Proceso	Nombre del proceso que se va ejecutar.
	Momento de Ejecución	Definir en qué momento, fase o actividad del proyecto se ejecutará el proceso.
	Entregable	Documento que se entregara en cada momento de ejecución de cada proceso.
	Periodicidad de Ejecución	Número de veces de ejecución del proceso en un lapso de tiempo.

Dentro de la planificación de gestión de riesgos hemos considerado detallar los indicadores los cuales nos ayudaran a medir el nivel de riesgos. A continuación detallaremos los valores que hemos considerado para poder realizar la medición del nivel del riesgo, probabilidad de ocurrencia e

impacto:

Probabilidad de Ocurrencia: Mide la frecuencia con la que se obtiene un resultado al llevar a cabo un experimento del cual se conocen todos sus resultados posibles.

Cuadro 3.9: Matriz de Probabilidades

Probabilidad	Frecuencia	Puntaje
Insignificante	Improbable que ocurra	0
Muy baja	2-3 veces cada 5 años	1
Baja	Una vez por año	2
Mediana	Una vez cada seis meses	3
Alta	Una vez por mes	4
Muy alta	Más de una vez por mes	5
Extrema	Más de una vez por día	6

Impacto: La escala del impacto, mostrado en el Cuadro 5.9, refleja la importancia del impacto, ya sea positivo por las amenazas que implica o positivo por las oportunidades que genera, sobre cada objetivo del proyecto si se produce un riesgo. Las escalas de impacto son específicas del objetivo que puede verse impactado, el tipo y tamaño del proyecto, las estrategias y el estado financiero de la organización, y la sensibilidad de la organización a impactos específicos.

Cuadro 3.10: Matriz de Impacto

Impacto	Grado	Puntaje
Insignificante	No genera impacto	0
Menor	No se requiere esfuerzo adicional para ser corregido	1
Significativo	Se requiere esfuerzo adicional para ser corregido	2
Perjudicial	Se requiere de esfuerzo y costos adicionales para ser corregido. Daño a la reputación y confianza	3
Serio	Interrupción prolongada y/o pérdida de conexión. Se compromete gran cantidad de datos y servicios.	4
Grave	Interrupción permanente. Se comprometen todos los datos y servicios.	5

Nivel de riesgo

La tabulación del nivel de riesgo indicada en cada observación ha sido elaborada a partir de las siguientes consideraciones:

- Situación actual del entorno sobre el cual se ha identificado el problema u observación.
- Periodicidad con que actualmente ocurren los problemas u observaciones identificadas.
- Impacto estimado en el negocio

Cálculo del Nivel de Riesgo = (Probabilidad de ocurrencia X Impacto)

El nivel de riesgo es el resultado de multiplicar los puntajes de la

probabilidad de ocurrencia y el impacto.

Cuadro 3.11: Nivel de Riesgo

Resultado		Nivel de Riesgo
V	1 – 3	Bajo
A	4 – 7	Medio
N	8 - 14	Alto
R	15 – 30	Crítico

Los niveles de los riesgos indicados en el Cuadro 3.11 forman la base para decidir si se quiere mejorar los controles existentes o implantar unos nuevos, así como la temporización de las acciones. Estos indicadores se aplicaran en el **Anexo 9**.

Prioridad

Definimos la preferencia con la que se va aplicar los planes de contingencia para mitigar los riesgos ya que se empezara mitigando los riesgos de mayor importancia y que por consiguiente requiere de mayor atención.

Cuadro 3.12: Nivel de Prioridad

Prioridad		Descripción
	Alta	La compañía planea implementar el control respectivo en el corto plazo (dentro de los próximos 3 meses) de acuerdo con la recomendación.
	Media	La compañía planea implementar el control respectivo en el mediano plazo (entre los próximos 3 y 12 meses) de acuerdo con la recomendación.
	Baja	La compañía planea implementar el control respectivo en el largo plazo (posterior a los 12 meses) de acuerdo con la recomendación.
X	N.A.	Está relacionado a aquellos objetivos de control que no aplican a la Compañía

3.3.4 Fase 4: Identificación de Riesgos

En esta fase de la propuesta metodológica, determinaremos que riesgos pueden afectar al proyecto y se procederá a documentar sus características.

En el Cuadro 5.8 se detallan los datos que se han considerado importantes obtener; mayor detalle en el **Anexo 8**.

Cuadro 3.13: Identificación de los Posibles Riesgos

CAMPO	DESCRIPCIÓN
Cód. OTI	Código identificador del objetivo de TI. Ver Anexo3.
Objetivos de TI	Se describirá el objetivo de TI alineados con los objetivos del negocio. Ver Anexo 3.
Amenaza	Describe un hecho o la situación actual que puede comprometer un obstáculo en el cumplimiento de los objetivos de TI.
Vulnerabilidad	Describe la debilidad que se tiene a causa de la amenaza latente para cumplir el objetivo de TI.
Cód. Riesgo	Código identificador del riesgo. Ej. R1, R2, etc.
Riesgo	Descripción del riesgo que se podría originar por la explotación de la vulnerabilidad existente.

3.3.5 Fase 5: Evaluación de Riesgos

3.3.5.1 Análisis Cualitativo de Riesgos:

La evaluación de probabilidad de los riesgos investiga la probabilidad de ocurrencia de cada riesgo específico. La evaluación del impacto de los riesgos investiga el posible efecto sobre un objetivo del proyecto, como tiempo, costo, alcance o calidad, incluidos tanto los efectos negativos por las amenazas que implican, como los efectos positivos por las oportunidades que genera.

Para cada riesgo identificado tenemos que evaluar la probabilidad y el impacto. Los riesgos van a ser evaluados en entrevistas o reuniones con participantes seleccionados por su familiaridad con las categorías de riesgos de la orden del día. Entre ellos se incluyen a los miembros del equipo de proyecto y según sea el caso expertos ajenos al proyecto.

Es necesario también contar con el juicio de expertos, ya que es posible que haya poca información sobre los riesgos en la base de datos de la organización de proyectos anteriores. Un facilitador experimentado puede dirigir la discusión, ya que los participantes pueden tener poca experiencia en la evaluación de riesgos.

El nivel de probabilidad de cada riesgo y su impacto sobre cada objetivo se evalúa durante la entrevista o reunión. Los detalles explicativos, incluidas las asunciones que justifican los niveles asignados, también se registran.

En el Cuadro 3.13 se detallan los campos del documento **Anexo 9**, en el cual plasmaremos la evaluación cualitativa de riesgos. Para mayor detalle de los datos ingresados ver **Anexo 9**.

Cuadro 3.13: Evaluación Cualitativa de Riesgos

CAMPO	DESCRIPCIÓN
OTI	Código del objetivo de TI registrado en el Anexo 2.
Cód. Riesgo	Código identificador del riesgo registrado en el Anexo 8.
Descripción del Riesgo	Descripción del riesgo que se podría originar por la explotación de la vulnerabilidad existente. Ver Anexo 8.
Vulnerabilidad	Describe la debilidad que se tiene a causa de la amenaza latente para cumplir el objetivo de TI. Ver Anexo 8.
NC	Nivel de cumplimiento del objetivo de TI identificado en el Anexo 3, el cual está relacionado al riesgo. Ver Cuadro 3.5 para identificar los valores del nivel de cumplimiento.
Probabilidad	Valor del índice de frecuencia. Ver Cuadro 3.9.
Impacto	Valor del impacto calculado.
Prob. X Impacto	Calculo del Nivel de Riesgo = Probabilidad X Impacto
NR	Valor del nivel de riesgo identificado, para identificar los valores ver cuadro 3.11.

3.3.5.2 Análisis Cuantitativo de Riesgos:

Consiste en realizar un análisis cuantitativo a los riesgos priorizados en el análisis cualitativo con el fin de ser más certeros con la probabilidad y el impacto de cada riesgo. Para esto se hacen uso de técnicas avanzadas como Montecarlo, PERT, distribución probabilística, etc.

Para el desarrollo de esta propuesta metodológica no aplica el análisis cuantitativo de riesgos ya que las técnicas a aplicar demandan un análisis más profundo y por ello mayor tiempo.

3.3.6 Fase 6: Análisis de los Resultados de la Evaluación de Riesgos.

En esta parte del documento realizaremos un análisis de los resultados de la evaluación de riesgos en el cual desarrollaremos opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

3.3.6.1 Plan de Respuesta a Riesgos

Existen varias estrategias de respuesta a los riesgos. Para cada riesgo, debemos seleccionar la estrategia o la combinación de estrategias con mayor probabilidad de ser efectiva. Haremos uso de herramientas de análisis de riesgos como la evaluación de probabilidad e impacto de los riesgos, matriz de probabilidad e impacto, categorización de riesgos, etc.

Luego desarrollaremos acciones específicas para implementar esa estrategia. Podemos seleccionar estrategias principales y de refuerzo. También podemos realizar un plan de reserva, el cual únicamente será implementado si la estrategia seleccionada no resulta ser totalmente efectiva o si se produce un riesgo aceptado. Por lo general, se asigna una reserva para contingencia de tiempo y coste. Finalmente podemos desarrollar planes de contingencia, junto con la identificación de las condiciones que disparan su ejecución.

Estamos contemplando tres estrategias que normalmente se ocupan de las amenazas a los riesgos que pueden tener impactos negativos sobre los objetivos del proyecto en caso de ocurrir. Estas estrategias son las siguientes:

- **Evitar:** Evitar el riesgo implica cambiar el plan de gestión del proyecto para eliminar la amenaza que represente un riesgo adverso.
- **Transferir:** Transferir el riesgo requiere trasladar el impacto negativo de una amenaza, junto con la propiedad de la respuesta, a un tercero. Transferir el riesgo simplemente da a otra parte la responsabilidad de su gestión; no lo elimina.
- **Mitigar:** Mitigar el riesgo implica reducir la probabilidad y/o impacto de un evento de riesgo adverso a un umbral aceptable. Adoptar acciones tempranas para reducir la probabilidad de la ocurrencia de un riesgo y/o su impacto sobre el proyecto a menudo es más efectivo que tratar de reparar el daño después de que ha ocurrido el riesgo.

Sugerimos tres respuestas para tratar los riesgos que tienen posibles impactos positivos sobre los objetivos del proyecto. Estas estrategias son explotar, compartir o mejorar como se describe en las siguientes líneas:

- **Explotar:** Se puede seleccionar esta estrategia para los riesgos con impactos positivos, cuando la organización desea asegurarse que la oportunidad se haga realidad. Esta estrategia busca eliminar la incertidumbre asociada con un riesgo del lado positivo en particular haciendo que la oportunidad definitivamente se concrete. Explotar las respuestas directamente incluye asignar recursos más talentosos al proyecto para reducir el tiempo hasta la conclusión, o para ofrecer una mejor calidad que la planificada originalmente.
- **Compartir:** Compartir un riesgo positivo implica asignar la propiedad a un tercero que está mejor capacitado para capturar la oportunidad para beneficio del proyecto. Entre los ejemplos de acciones para compartir se incluyen: formar asociaciones de riesgo conjunto, equipos, empresas con finalidades especiales o uniones temporales de empresas que se pueden establecer con finalidad expresa de gestionar oportunidades.
- **Mejorar:** Esta estrategia modifica el tamaño de una oportunidad, aumentando la probabilidad y/o los impactos positivos, e identificando y maximizando las fuerzas impulsoras clave de estos riesgos de impacto positivo.
- **Aceptar:** Estrategia que se adopta debido a que rara vez es posible eliminar todo el riesgo de un proyecto. Esta estrategia indica que el equipo del proyecto ha decidido no cambiar el plan de gestión del proyecto para hacer frente a un riesgo, o no ha podido

identificar ninguna otra estrategia de respuesta adecuada. Puede ser adoptada tanto para las amenazas como para las oportunidades. Esta estrategia puede ser pasiva o activa.

La aceptación pasiva no requiere acción alguna, dejando en manos del equipo del proyecto la gestión de las amenazas o las oportunidades a medida que se producen.

La estrategia de aceptación activa más común es establecer una reserva para contingencias, que incluya la cantidad de tiempo, dinero o recursos necesarios para manejar las amenazas o las oportunidades conocidas, o incluso también las posibles y desconocidas.

Haremos uso del **Anexo 10** para ingresar la información correspondiente a Plan de Respuesta a Riesgos, cuyos campos se describen en el Cuadro 3.14.

Cuadro 3.14: Plan de Respuesta a Riesgos

CAMPO	DESCRIPCIÓN
Cód. Riesgo	Código identificador del riesgo. Ver Anexo 8.
Objetivos de TI	Se describirá el objetivo de TI alineados con los objetivos del negocio (Anexo 2).
Amenaza	Describe un hecho o la situación actual que puede comprometer un obstáculo en el cumplimiento de los objetivos de TI. Ver Anexo 8.
Vulnerabilidad	Describe la debilidad que se tiene a causa de la amenaza latente para cumplir el objetivo de TI. Ver Anexo 8.

Riesgo	Descripción del riesgo que se podría originar por la explotación de la vulnerabilidad existente. Ver Anexo 8.
NR	Medir los niveles de riesgo para ello ver Cuadro 3.11.
Resp. Del Riesgo	Nombre del responsable quien dará respuesta al riesgo identificado.
Respuestas Planificadas	Describe las respuestas respecto a los riesgos identificados.
Tipo de Respuesta	Estrategia de cómo afrontar el riesgo, teniendo en cuenta si el riesgo es negativo (evitar, mitigar o transferir) o positivo (explotar, compartir o mejorar).
Resp. De la Rta.	Nombre del responsable quien dará respuesta al riesgo.
Fecha Planificada	Fecha en la que se ejecutara la respuesta a los riesgos.
Plan de Contingencia	Descripción del plan de contingencia.

Para mayor detalle ver **Anexo 10.**

3.3.7 Fase 7: Monitoreo y Seguimiento de los Riesgos.

La fase de seguimiento y control son actividades que nos permitirán observar la ejecución del proceso de forma que se puedan identificar los posibles problemas oportunamente y adoptar las acciones correctivas, cuando sea necesario, para controlar la ejecución del proyecto. El beneficio clave de esta última fase es que el rendimiento del proyecto se observa y se mide regularmente para identificar las variaciones respecto del plan de gestión del proyecto. La fase de seguimiento y control también incluye controlar los cambios y recomendar acciones preventivas como anticipación de posibles problemas.

Este seguimiento continuo proporciona al equipo del proyecto una idea acerca de la salud del proyecto y resalta cualquier área que necesite atención adicional. Esta fase de la propuesta metodológica no solamente supervisa y controla el trabajo que se realiza dentro de un Grupo de Procesos, sino que también supervisa todo el esfuerzo del proyecto. En los proyectos de múltiples fases, la fase de seguimiento y control también proporciona retroalimentación entre las fases del proyecto, a fin de implementar acciones correctivas o preventivas para hacer que el proyecto cumpla con el plan de gestión del proyecto. Cuando las variaciones ponen en peligro los objetivos del proyecto, como parte del ciclo modificado planificar-hacer-revisar-actuar. De esta revisión pueden surgir actualizaciones recomendadas para el plan de gestión del proyecto. Por ejemplo, no haber cumplido con la fecha de finalización de una actividad puede requerir ajustes al plan de asignación de personal actual, implementar horas extra o realizar concesiones entre los objetivos de presupuesto y del cronograma.

3.3.7.1 Acciones Correctivas.

Plan realizado por el equipo de TI para canalizar cualquier inconformidad que pueda existir con respecto a los requerimientos desarrollados, además de solucionar cualquier tipo de inconsistencia las cuales conducen a realizar una mejora en la compañía.

Para mayor detalle ver Anexo 11.

Cuadro 3.15: Acciones Correctivas

CAMPO	DESCRIPCIÓN
Proceso	Nombre del proceso evaluado
Proyecto	Nombre del proyecto perteneciente al proceso anterior.
Fase	Fase del Proyecto
Entregable	Lista de Documentos modificados que serán salidas de las acciones correctivas
Actividad	
Definición del Problema	Definir y acotar el problema que se va a resolver, distinguiendo el problema de sus causas y de sus consecuencias.
Reaparición del Defecto	Solución de corto plazo para mitigar la gravedad del problema y/o sus Consecuencias. Especificaciones de qué, quién, cómo, cuándo y dónde.
Identificación de las Causas Raíces	Causas que generan el problema y sus consecuencias
Acción Correctiva a Tomar	Solución de largo plazo que eliminará el problema de raíz, o que lo mitigará hasta un estado controlable. Especificación de qué?, quién?, cómo?, cuando?, donde? y cuanto?
Autorización de Acción Correctiva	Personas que autorizan.

3.3.7.2 Información del Monitoreo de Riesgos

Los riesgos deben monitorearse para poder llevar un registro de sus estados, además de poder ver el nivel del riesgo en el momento y prever algún riesgo que pueda suceder en el futuro. Para mayor detalle ver **Anexo 12**.

Cuadro 3.16: Informe del Monitoreo de Riesgos

CAMPO	SUBCAMPO	DESCRIPCIÓN
Nombre del Proyecto	Nombre de Proyecto	
Siglas del Proyecto	Siglas del Proyecto	
Riesgos Actuales Potenciales	Revisión y Confirmación de Probabilidad e Impacto Estimados Inicialmente.	Resumen de los riesgos con mayor impacto y revisión de sus valores hallados.
	Revisión de Adecuación de Respuestas Planificadas para los Riesgos Identificados Inicialmente.	Resumen de las respuestas a los riesgos antes mencionados
	Revisión de Planes de Contingencia para los Riesgos Identificados Inicialmente.	Resumen y revisión de las respuestas ante los riesgo identificados.
	Verificación de Ejecución de Respuestas Planificadas	Resultados de las respuestas a los riesgos
Riesgos Actuales Sucedidos	Valoración de Impacto Real Vs Impacto Estimado	Evaluar los riesgos sucedidos y determinar su impacto real, comparándolo con el estimado.
	Revisión de Planes de Contingencia para los Riesgos Identificados Inicialmente.	Revisar los planes de contingencia para verificar el resultado de la respuesta al riesgo.
	Elaboración de Planes de Emergencia	Si en caso se necesitara elaborar, planes de emergencia para riesgos con mayor impacto.
	Programación de Ejecución de Planes de Contingencia / Emergencia	Determinar tiempo en el cual se responderá al incidente presentado.
	Evaluación de Necesidades de Acciones Correctivas o Solicitudes de Cambio	Revisión y determinación de que solicitudes de cambios se ordenarán.
Nuevos Riesgos Detectados	Evaluación Cualitativa y Categorización de Riesgos	Evaluación de impacto de los riesgos nuevos detectados
	Definición de Respuestas Planificadas	Determinar respuestas a los riesgos detectados.
	Definición de Planes de Contingencia	Determinar los planes de <u>contingencia</u> para cada riesgo nuevo detectado
	Programación de Ejecución de Respuesta Planificadas	Periodicidad o tiempo para la ejecución de la respuesta planificada.

CAPÍTULO IV

APLICACIÓN DE LA METODOLOGÍA PROPUESTA

4.1 Situación Actual de la Empresa

TELECOM, a quien de aquí en adelante llamaremos "La Empresa", es una Empresa de Telecomunicaciones dedicada a brindar productos y servicios móviles digitales a nivel nacional e internacional. Esta empresa se encuentra comprometida desde su fundación a entregar a sus clientes productos y servicios con la más alta calidad, es decir haciendo uso de sus propias políticas, métodos y procedimientos.

Actualmente "La Empresa" brinda al mercado una única tecnología que permite integrar en un mismo equipo cuatro sistemas de comunicación:

- Conexión directa.
- Interconexión Telefónica.
- Mensajes de Texto.
- Telecom Online

La Empresa a planificado brindar al mercado productos y servicios 3G, uno de los productos es el USB Modem que fue lanzado en diciembre del 2009 el otro producto es el llamado Equipo Móvil Voz el cual se tiene planificado lanzar al mercado en abril del 2010. Para el cumplimiento de estas metas es que se ha está desarrollando el "Proyecto PCS" en las etapas de R 1.0 y R 1.1 respectivamente, con lo cual se tendrá una mejor competitividad en el mercado de las telecomunicaciones con las grandes empresas.

El "Proyecto PCS" es desarrollado para lograr una mejora en los procesos de La Empresa, los cuales en un porcentaje se han estado realizando de

forma manual por lo cual esta mejora hará que se realicen de forma automática. En la figura 4.1 vemos el diagrama de macro procesos de La Empresa.

Figura 4.1: Macroprocesos de La Empresa.



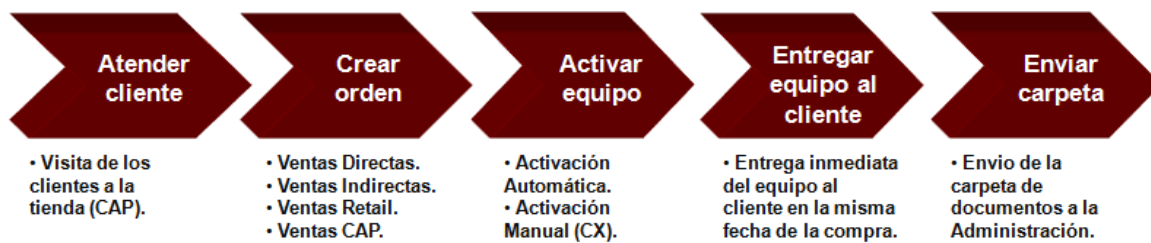
Con la finalidad de mitigar los riesgos en los diferentes proyectos asociados a la mejora de cada proceso hemos planteado aplicar la administración de riesgos, basados en las mejores prácticas de la guía del PMBOK y el marco de control de COBIT 4.1, al Proceso de Ventas en su procedimiento de despacho por el canal de Fulfillment, que de ahora en adelante llamaremos "Proceso Muestra", por ser de mayor complejidad e importancia para La Empresa.

En las figuras 4.2 y 4.3 se muestran como interactúa el "Proceso Muestra".

Figura 4.2: Proceso de Ventas - Postpago



Figura 4.3: Proceso de Ventas - Prepago



Además el Proceso de Ventas está conformado por varios procedimientos como son los siguientes:

- Ventas CAP/CAL.
- Ventas directas e indirectas y CRM para Ventas Nuevas para personas jurídicas.
- Ventas Prepago en CAP
- Venta de equipo Prepago – cadena Retail.
- Despacho en tienda
- Despacho en Fullfilment

El Marco de trabajo aplicado lo veremos con mayor detalle en los siguientes puntos donde se detallarán cada una de las fases del marco de trabajo mencionado.

4.2 FASE 1. Descripción del Contexto y Marco de Trabajo de los Procesos

4.2.1. Objetivos del Negocio.

Se realizaron diversas reuniones con las personas involucradas para consolidar la información. Además se tuvo la facilidad de revisar el Plan Estratégico de La Empresa.

En el siguiente formato describiremos los objetivos del negocio que fueron identificados en esta fase.

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
1.0	MCancho	MMorales	MMorales	23/01/2010

LISTA DE OBJETIVOS DEL NEGOCIO

COD. ON	OBJETIVO DE NEGOCIO	INDICADORES
ON1	Maximizar rentabilidad de la empresa	Este objetivo se medirá en función a la utilidad neta. Reducción de costos operativos.
ON2	Incrementar la calidad de servicio a los clientes	Este objetivo se medirá en función al número de quejas y reclamos de los clientes con respecto a los servicios de la empresa
ON3	Fidelizar a los clientes	Este objetivo se medirá en función a la tasa de retención de clientes.
ON4	Optimizar los procesos del negocio	Este objetivo se medirá en función a los costos operativos por unidades de negocio o departamentos.
ON5	Optimizar los mecanismos de comunicación e información	Reducción de costos de comunicación (paperless)

4.2.2. Objetivos de TI:

De acuerdo al Plan Estratégico de La Empresa, se han logrado identificar objetivos de TI que se deben cumplir, los cuales se encuentran alineados a los objetivos del negocio, además estos se encuentran asociados a sus respectivos indicadores para poder ser medidos.

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
1.0	MCancho	MMorales	MMorales	23/01/2010

LISTA DE OBJETIVOS DE TI

COD. OTI	OBJETIVOS DE TI	INDICADORES DE MEDICIÓN	PROCESOS DE TI QUE SOPORTA EL OBJETIVO
OTI1	Tiempo: Optimizar el desempeño de los sistemas.	Tiempo de respuesta de sistemas.	Mejora continua de la infraestructura de sistemas
OTI2	Integración: Integrar los sistemas de información con los equipos de proyectos y usuarios orientados a mejorar la satisfacción del cliente.	Tiempo de realización de las ventas de productos	Desarrollo de aplicaciones de integración.
OTI3	Presupuesto Garantizar el uso y definición apropiada de presupuestos de sistemas	Presupuesto ejecutado vs. Disponible	Monitoreo mensual del presupuesto
OT4	Incidentes: Reducir incidentes registrados en el Quality Center y Mesa de Ayuda.	Cantidad de incidentes registrados.	Monitoreo mensual de los incidentes registrados.(MA y QC)
OTI5	Valoración de proyectos y cambios Lograr un adecuado análisis y costo beneficio de los proyectos y requerimientos de TI.	Requerimientos del proyecto	Gestión de proyectos de TI. Gestión de cambios
OTI6	Satisfacción Obtener la satisfacción mensual de los servicios de TI para los usuarios, superior al 85%	Nivel de Satisfacción de usuarios.	Monitoreo mensual de los incidentes registrados. (MA y QC).

4.2.3. Necesidad de Implementación de Gobierno de TI

Se realizaron reuniones con la alta gerencia en la cual se concluyo en lo siguiente:

La Empresa debe cumplir con requerimientos de calidad y de seguridad, tanto para su información, como para sus activos. Además la gerencia deberá optimizar el empleo de sus recursos disponibles, los cuales incluyen: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar con sus objetivos, la gerencia debe entender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

COBIT en este caso ayudará a La Empresa a satisfacer sus múltiples necesidades de administración de riesgo estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos.

Las buenas prácticas de COBIT ayudaran a optimizar la inversión de la información por lo cual proporcionaremos un mecanismo de medición que permitirá juzgar cuando las actividades están yendo por el camino equivocado y a qué objetivo de negocio podría estar afectando.

En este caso la gerencia debe asegurar que los sistemas de control interno y el marco referencial están funcionando y soportan los procesos del negocio, y debe ser consciente de cómo cada actividad individual de control satisface los requerimientos de información e impacta los recursos de TI. El impacto sobre los recursos de TI son resaltados en el Marco de

Control **(4.2.4)** junto con los requerimientos del negocio que deben ser alcanzados: eficiencia, efectividad, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información. El control esta incluyendo políticas, estructuras, prácticas y procedimientos organizacionales, las cuales son responsabilidad de la gerencia.

La gerencia mediante este gobierno corporativo, esta asegurando que todos los individuos involucrados en la administración, uso, diseño, desarrollo, mantenimiento u operación de sistemas de información actúen con la debida diligencia.

En el formato de Análisis de Gobierno de TI estamos detallando la situación actual de la madurez del Gobierno de TI que tiene La Empresa.

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
1.0	MCancho	MMorales	MMorales	23/01/2010

ANALISIS DE GOBIERNO DE TI

ALINEAMIENTO ESTRATEGICO
Actualmente TI se encuentra alineado en cinco objetivos de negocio los cuales no están tan estrechamente relacionados a las operaciones de TI. Este alineamiento busca proveer servicios e infraestructura para que los usuarios de los mismos logren incrementar su eficiencia operativa, de esta forma las ventajas competitivas de la institución serán incrementadas. Otro aspecto importantes es la seguridad y confidencialidad de la información, TI tiene la misión de salvaguardar dichos activos y asegurar así la confianza de todos los actores que intervienen en los negocios de la institución, las actuales amenazas tecnológicas ponen en riesgo cumplir este objetivo. TI tiene la responsabilidad de proveer de herramientas de apoyo para que los objetivos del Plan Estratégico sean alcanzados, aunque aún no ha logrado actuar en forma proactiva para identificar y capitalizar oportunidades de negocio que pudieran ser habilitadas por las Tecnologías de Información. Si bien es cierto que las aplicaciones soportan los procesos de negocio aún no se ha logrado cuantificar los costos de operación que se reducirían si se implantarían aplicaciones.

La estructura organizacional carece de elementos relacionados a mejorar los procesos de negocios utilizando las tecnologías de información ya que en algunos casos existe ausencia de conocimientos de las metodologías en gestión de proyectos, gestión de adquisiciones, gestión de servicios de tecnologías de información, gestión de seguridad de información; y en otros casos si bien existe el conocimiento de que tecnologías pueden utilizar en cada caso, no tienen conocimiento de cómo realizar la respectiva aplicación.

ENTREGA DE VALOR

TI tiene como meta principal entregar valor a La Empresa, esto se lograra brindando las herramientas y tecnologías adecuadas para mantener la continuidad de las operaciones y brindar un servicio de primera categoría a los clientes de la institución, las operaciones se vienen realizando con un bajo porcentaje de paralizaciones.

Los accionistas, colaboradores y proveedores deben tener la información necesaria para la toma de decisiones en forma oportuna. Debido a tareas de procesamiento de información algunas operaciones se entregan al día siguiente.

Los clientes buscan seguridad en sus operaciones con La Empresa, esta seguridad está controlada con cada una de sus respectivas agencias, sin embargo el incremento en las nuevas operaciones realizadas por internet genera desconfianza en los clientes.

ADMINISTRACIÓN DE RECURSOS

Actualmente TI cuenta con recursos propios, los cuales se encargan de las operaciones críticas y de negocio además de la realización de tareas de nuevos desarrollos de proyectos que finalmente pasan, la demanda interna de aplicaciones concretas hace que TI tenga que adquirir más productos. Se ha identificado que algunos proyectos no cuentan con la suficiente documentación y control.

El Área de TI no cuenta con indicadores de desempeño para poder sustentar el aumento del costo pero de alguna manera se justifica por el objetivo que deseaban alcanzar y la complejidad de las aplicaciones.

El requerimiento de la Gerencia General es poder optimizar la respuesta ante las incidencias y/o sucesos inesperados, para prever los gastos excesivos de costo y tiempo entre otros.

ADMINISTRACIÓN DE RIESGOS

En el área de TI no existe una cultura de evaluación de riesgos que le permita actuar en forma proactiva a los problemas e incidentes reportados por los usuarios. Asimismo, en el área existe personal con poco o ningún conocimiento y experiencia en metodologías de Identificación, Evaluación y Mitigación de Riesgos.

La mayoría de incidentes reportados por los usuarios podrían evitarse o minimizarse en su impacto si hubiera un proceso de gestión de riesgos de tecnologías de información.

MEDICIÓN DE RENDIMIENTO

Actualmente TI ha definido indicadores para monitorear su rendimiento, estos indicadores permiten administrar ciertos aspectos de TI como son:

Planificación y Organización

Presupuesto por área.

Soporte y Servicios

- Número de contratos que no utilizan términos y condiciones estándares o excepciones autorizadas.
- Número de fallas ocasionadas por capacidad insuficiente o por el desempeño del procesamiento.

Tiempo empleado para resolver problemas de capacidad

- Porcentaje de incrementos de capacidad no planificados sobre el total de incrementos.
- Número de servicios pendientes.
- Tiempo transcurrido entre la detección, reporte y acción sobre incidentes de seguridad.

Monitoreo

- Número de acciones correctivas y sostenibles tomadas como resultado de nuevos hallazgos.
- Tiempo entre la notificación de deficiencias e inicio de acciones.
- Número de procesos monitoreados.

Adquisición e implantación

- Medición de los eventos ocurridos en un período determinado y el impacto de estos eventos, durante la implantación de tecnologías de información.
- El número de quejas y solicitudes adicionales realizadas por los clientes de La Empresa por razón de algún servicio defectuoso ocurrido por problemas que se hayan tenido en los sistemas de información.
- El porcentaje de modificaciones efectivas realizadas a los sistemas de información que soportan los procesos de La Empresa.

4.2.4. Marco de Control:

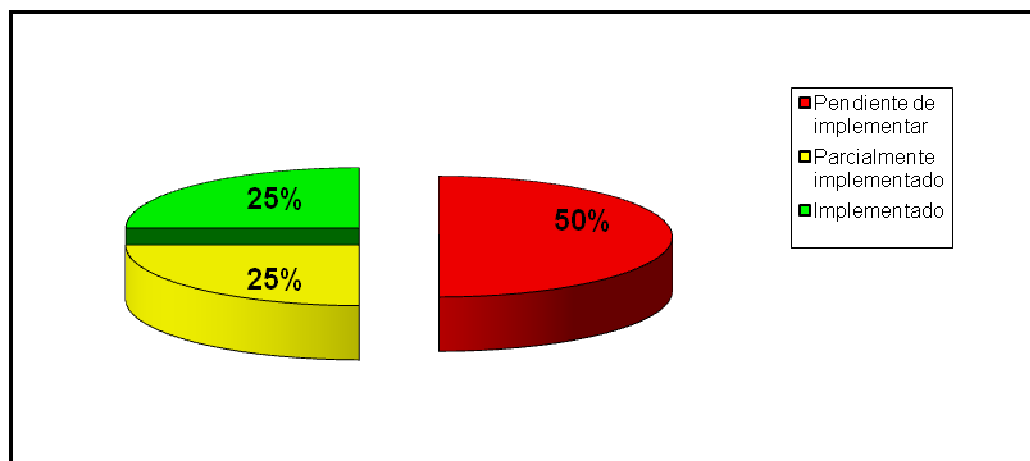
Este marco de control de COBIT en la actualidad, está proporcionando a los procesos de negocio de La Empresa, herramientas que facilitan el cumplimiento de esta responsabilidad. Este marco de control está iniciando con una premisa simple y práctica:

Con el fin de proporcionar la información que La Empresa necesita para alcanzar sus objetivos, los recursos de TI deben ser gestionados mediante un conjunto de procesos de TI agrupados de una forma natural.

El marco de control consta de un conjunto de cuatro Objetivos de Control identificados a alto nivel, uno para cada uno de los Objetivos de TI relacionados.

El siguiente gráfico nos indica el estado actual acerca del nivel de cumplimiento de los cuatro controles identificados, considerando el entorno de TI y la administración de la gestión de riesgos que actualmente se lleva a cabo en La Empresa.

Figura 4.4: Nivel de Cumplimiento de Objetivos de Control



CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
1.0	MCancho	MMorales	MMorales	23/01/2010

MARCO DE CONTROL

COD. OTI	OBJETIVOS DE TI	OBJETIVOS DE CONTROL	N.C	DOMINIOS Y PROCESOS COBIT	OBJETIVOS DE CONTROL DETALLADO
OT11	Tiempo: Optimizar el desempeño de los sistemas.	Realizar un adecuado análisis de costo beneficio que permita sustentar ante la alta gerencia la inversión de proyectos		PO5: Administrar la inversión en TI	PO5.1: Marco de trabajo para la gestión financiera. PO5.2: Prioridades dentro del presupuesto de TI. PO5.3: Proceso presupuestal. PO5.4: Administración de costos de TI PO5.5: Administración de Beneficios.
		Establecer acuerdo de niveles de servicio a los usuarios.		DS1: Definir y Administrar los Niveles de Servicios.	DS1.1: Marco de trabajo de la administración de los niveles de servicio. DS1.2: Definición de servicios. DS1.3: Acuerdos de niveles de servicio. DS1.4: Acuerdos de niveles de operación. DS1.5: Monitoreo y reporte del cumplimiento de los niveles de servicio. DS1.6: Revisión de los acuerdos de niveles de servicio y de los contratos.

OT13	Presupuesto Garantizar el uso y definición apropiada de presupuestos de sistemas	Efectuar adecuado alineamiento de las diferentes áreas hacia los objetivos de negocio que se reflejen en el PETI.		PO5: Administrar la inversión en TI PO1: Definir un Plan Estratégico de TI	PO5.1: Marco de trabajo para la gestión financiera. PO5.2: Prioridades dentro del presupuesto de TI. PO5.3: Proceso presupuestal. PO5.4: Administración de costos de TI PO5.5: Administración de Beneficios. PO1.1: Administración de valor de TI PO1.2: Alineación de TI con el negocio PO1.3: Evaluación de desempeño actual PO1.4: Plan Estratégico de TI	PO5.1: Marco de trabajo para la gestión financiera. PO5.2: Prioridades dentro del presupuesto de TI. PO5.3: Proceso presupuestal. PO5.4: Administración de costos de TI PO5.5: Administración de Beneficios. PO1.1: Administración de valor de TI PO1.2: Alineación de TI con el negocio PO1.3: Evaluación de desempeño actual PO1.4: Plan Estratégico de TI
OT15	Valoración de proyectos y cambios Lograr un adecuado análisis y costo beneficio de los proyectos y requerimientos de TI.	Realizar un adecuado análisis de costo beneficio que permita sustentar ante la alta gerencia la inversión de proyectos.		PO9: Administrar Proyectos	PO10.2: Marco de trabajo para la administración de proyecto PO10.5: Estatuto del alcance del proyecto PO10.6: Inicio de las fases del proyecto. PO10.7: Plan integrado del proyecto PO10.10: Plan de calidad del proyecto PO10.12: Planeación del proyecto y métodos de aseguramiento.	PO10.2: Marco de trabajo para la administración de proyecto PO10.5: Estatuto del alcance del proyecto PO10.6: Inicio de las fases del proyecto. PO10.7: Plan integrado del proyecto PO10.10: Plan de calidad del proyecto PO10.12: Planeación del proyecto y métodos de aseguramiento.

4.2.5. Mapeo de Procesos:

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
1.0	MCancho	MMorales	MMorales	23/01/2010

MAPEO DE PROCESOS

OBJETIVOS DE CONTROL	DOMINIOS Y PROCESOS DE COBIT	OBJETIVOS DE CONTROL DETALLADO	GOBIERNO DE TI				RECURSOS DE TI				CRITERIOS DE INFORMACIÓN						
			Alineamiento Estratégico	Entrega de Valor	Gestión de Recursos	Gestión de Riesgos	Medición y Rendimiento	Personas	Información	Aplicaciones	Infraestructura	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento
Realizar un adecuado análisis de costo beneficio que permita sustentar ante la alta gerencia la inversión de proyectos	PO5: Administrar la inversión en TI	PO5.1: Marco de trabajo para la gestión financiera. PO5.2: Prioridades dentro del presupuesto de TI. PO5.3: Proceso presupuestal. PO5.4: Administración de costos de TI PO5.5: Administración de Beneficios.	S	P	S		S	X		X	X	P	P				S
Efectuar adecuado alineamiento de las diferentes áreas hacia los objetivos de negocio que se reflejen en el PETI.	PO5: Administrar la inversión en TI	PO5.1: Marco de trabajo para la gestión financiera. PO5.2: Prioridades dentro del presupuesto de TI. PO5.3: Proceso presupuestal. PO5.4: Administración de costos de TI PO5.5: Administración de Beneficios.	S	P	S		S	X		X	X	P	P				S

4.3 Fase 2: Descripción de las Generalidades de los Procesos.

4.3.1 Descripción del Proceso.

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha Motivo
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho	05/01/2010

DESCRIPCIÓN DE PROCESOS N°001

PROCESO	
Ventas de Productos y Servicios	
OBJETIVOS	
Lograr la mayor cantidad de ventas logrando la satisfacción del cliente por el servicio que se brinda.	

INDICADORES		
N°	TIPO	DESCRIPCIÓN
I1	KGI	Monto de facturación anual
I2	KGI	Cantidad de operaciones mensuales
I3	KGI	Cantidad de ventas mensuales
I4	KGI	Nivel de satisfacción del cliente
I5	KPI	Eficiencia de empleados de TI
I6	KPI	Nivel de automatización de procesos
I7	KPI	Cantidad de requerimientos de mantenimiento de software
I8	KPI	Cantidad de incidentes reportados
I9	KPI	Satisfacción de usuarios

METAS CUANTITATIVAS	
No aplica	
RESPONSABILIDAD Y AUTORIDAD	
Gerente de ventas	
PROCESOS RELACIONADOS	
- Procesos de Evaluación de créditos - Proceso de activaciones en BSCS	

ENTRADAS	
<i>(Se indica de manera referencial los recursos y/o actividades (precondiciones) requeridas por el proceso.)</i>	
NOMBRE	FUENTE
Comunicación	Haber creado la comunicación con el cliente.
Incidente	Haber creado incidente para la categoría de ventas móviles.
Oportunidad	Haber creado el documento de oportunidad asociado al cliente.
Orden de venta	El usuario crea la orden de venta para el cliente.

SALIDAS		
<i>(Se indica de manera referencial los recursos y/o actividades (postcondiciones) que se obtienen como resultado del proceso.)</i>		
NOMBRE	DESCRIPCIÓN	DESTINO
Generación de documento	Generación de guía de remisión y/o factura en caso aplique	Cliente
Cerrar orden de venta	Orden de venta se cierra después de haber atendido al cliente y haber realizado todo el proceso de venta.	La Empresa
Equipo	Se entrega el equipo con su respectiva activación	Cliente

VIGENCIA		
<i>(Sección que indica la información asociada al periodo de vigencia de la ultima versión del documento del proceso.)</i>		
INICIO	REVISIÓN	FIN
05/01/2010	05/04/2010	30/06/2010

DIAGRAMA DEL PROCEDIMIENTO DEL PROCESO		
ID PROCEDIMIENTO	01-0001	
TITULO DEL PROCEDIMIENTO	Ventas CAP/CAL	
TAREA	Ventas a través de Call Center y tienda	
TIPO DE TAREA: <i>(Sección que indica la información del tipo de actividad.)</i>		Actividad de procesamiento de algún tipo.
		Actividad de toma de decisión.
		Actividad de análisis de entrada y/o emisión de salidas.
		Actividad de documentación.
RESPONSABLE	- Gerente de Ventas - Métodos y procedimientos: Responsable de la actualización del flujo	

	del proceso
--	-------------

4.4 Fase 3. Planificación de la Gestión de Riesgos:

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha Motivo
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho	05/01/2010

PLANIFICACIÓN DE GESTIÓN DE RIESGOS

METODOLOGIA DE LA GESTIÓN DE RIESGOS			
PROCESO	DESCRIPCIÓN	HERRAMIENTAS	FUENTES DE INFORMACIÓN
Planificación de la Gestión de Riesgos	Elaborar el Plan de Gestión de Riesgos.	PMBOK, PMI Compendium.	Sponsor y usuarios. PM y equipo de proyecto.
Identificación de Riesgos	Identificar que riesgos pueden afectar el proyecto y documentar sus características.	Checklist de riesgos.	Sponsor y usuarios. PM y equipo de proyecto, archivos históricos de proyectos.
Análisis de Riesgos	Análisis Cualitativo de Riesgos: Evaluar probabilidad e impacto y establecer el ranking de importancia. Análisis Cuantitativo de Riesgos: No Aplica.	Definición de probabilidad e impacto, matriz de probabilidad e impacto.	Sponsor y usuarios. PM y equipo de proyecto.
Planificación de Respuesta a los Riesgos	Definir respuesta a riesgos, planificar ejecución de respuestas.		Sponsor y usuarios. PM y equipo de proyecto, archivos históricos de proyectos.
Seguimiento y Control	Verificar la ocurrencia de riesgos. Supervisar y verificar la ejecución de respuestas. Verificar aparición de nuevos riesgos.		Sponsor y usuarios. PM y equipo de proyecto.

ROLES Y RESPONSABLES DE LA GESTIÓN DE RIESGOS			
PROCESO	ROLES	PERSONAS	RESPONSABILIDADES
Planificación de Gestión de los Riesgos.	Equipo de G. Riesgos Líder Apoyo Miembros	M.C.E M.M.F	Líder: Se encargará de dirigir la Planificación de riesgos asegurando sus buenos resultados. Miembros: Se encargarán de apoyar y realizar el trabajo técnico para el desarrollo de la Planificación de riesgos.
Identificación de Riesgos	Equipo de G. Riesgos Líder Apoyo Miembros	M.C.E M.M.F	Líder: Se encargará de dirigir la Identificación de riesgos asegurando sus buenos resultados. Miembros: Se encargarán de apoyar y realizar el trabajo técnico para el desarrollo de la Identificación de riesgos.

Análisis de Riesgos	Equipo de G. Riesgos Líder Apoyo Miembros	M.C.E M.M.F	Líder: Se encargará de dirigir la Análisis de riesgos asegurando sus buenos resultados. Miembros: Se encargarán de apoyar y realizar el trabajo técnico para el desarrollo de la Análisis de riesgos.
Planificación de Respuesta a los Riesgos	Equipo de G. Riesgos Líder Apoyo Miembros	M.C.E M.M.F	Líder: Se encargará de dirigir la Planificación de riesgos asegurando sus buenos resultados. Miembros: Se encargarán de apoyar y realizar el trabajo técnico para el desarrollo de la Planificación de riesgos.
Seguimiento y Control de Riesgos	Equipo de G. Riesgos Líder Apoyo Miembros	M.C.E M.M.F	Líder: Se encargará de dirigir la Seguimiento y control de riesgos asegurando sus buenos resultados. Miembros: Se encargarán de apoyar y realizar el trabajo técnico para el desarrollo de la Seguimiento y control de riesgos.

PERIODICIDAD DE LA GESTIÓN DE RIESGOS			
PROCESO	MOMENTO DE EJECUCIÓN	ENTREGABLE	PERIODICIDAD DE EJECUCIÓN
Planificación de Gestión de los Riesgos.	Definir en qué momento, fase o actividad del proyecto se ejecutará el proceso.	Documento de Planificación de riesgos.	1 vez al año
Identificación de Riesgos	Definir en qué momento, fase o actividad del proyecto se ejecutará el proceso.	Matriz de Riesgos.	Inicio de cada proyecto
Análisis de Riesgos	Definir en qué momento, fase o actividad del proyecto se ejecutará el proceso.	- Plan de Respuesta a Riesgos. - Análisis de Brechas. - Nivel de Madurez del Proceso.	Cada punto de control definido.
Planificación de Respuesta a los Riesgos	Definir en qué momento, fase o actividad del proyecto se ejecutará el proceso.	Solicitud de Cambios Aprobadas.	Inicio de cada proyecto
Seguimiento y Control de Riesgos	Definir en qué momento, fase o actividad del proyecto se ejecutará el proceso.	Cuadro de acciones correctivas.	Cada punto de control definido y aprobado por la gerencia.

4.5 Fase 4. Identificación de Riesgos:

Actualmente, La Empresa reconoce la relevancia de sus sistemas y es consciente de los cuidados que deben tomarse para asegurar la integridad, confidencialidad y disponibilidad de su información crítica.

La existencia de diversos escenarios de riesgo que presentan generalmente los sistemas y los componentes tecnológicos han incentivado a La Empresa a iniciar este proyecto de administración de riesgos, a fin de mitigar los riesgos que puedan identificarse para brindar una mayor protección a su información crítica.

En este sentido, La Empresa con la asistencia de nuestro marco de trabajo propuesto, ha desarrollado el inicio de la “Administración de Riesgos”, el cual abarca la situación actual de la empresa entre el periodo de desarrollo del R1.1 que fue de Agosto a Diciembre del 2009.

De acuerdo a los requerimientos de La Empresa, para la identificación de riesgos se han realizado las siguientes actividades:

i. Análisis de Ambientes de TI

Hemos analizado la gestión de riesgos establecida en La Empresa sobre la base de algunos ambientes de TI establecidos, abarcando el entorno de desarrollo de los ambientes de TI y el ciclo de vida que cumplen estos. Los ambientes considerados para la presente evaluación fueron los siguientes:

1. Desarrollo 3G.
2. E2E (End 2 End)
3. UAT (User Accept Testing).

ii. Análisis de Vulnerabilidades

Hemos evaluado los riesgos de algunos proyectos críticos asociados al “Proceso Muestra” que soporta La Empresa, a fin de identificar las vulnerabilidades técnicas que estos proyectos pudieran presentar.

- Sanity Check DR - Local Apps
- Orders.
- Credit System.

Nuestra investigación cubrió principalmente el análisis y la evaluación de las siguientes áreas de riesgos:

- Controlar la calidad de los proyectos.
- Autorización de los Change Request
- Cambios en los cronogramas de proyectos planificados.
- Entorno de conectividad desde y hacia los sistemas.
- Vulnerabilidades técnicas.
- Monitoreo y registro de eventos.

Asimismo, hemos entrevistado a personas de La Empresa que cumplen con los roles relacionados al “Proceso Muestra” los cuales las hacen responsable de brindar soporte técnico al análisis de riesgos que se está realizando.

Tener en cuenta que La Empresa debe realizar las siguientes actividades antes de ejecutar nuestras recomendaciones que se describen en el capítulo de **Conclusiones y Recomendaciones** del presente documento, de ser aplicable:

- Análisis de impacto técnico.
- Análisis de impacto funcional.
- Medidas de marcha atrás en caso de surgir un inconveniente.
- Medidas de backup y restore de los proyectos evaluados.
- Ejecución de la recomendación en equipos de prueba.
- Ejecución de la recomendación en equipos pilotos en un entorno de producción.
- Coordinación con el proveedor del sistema o dispositivo afectado.

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha Motivo
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho	05/01/2010

IDENTIFICACIÓN DE RIESGOS

COD. OTI	OBJETIVOS DE TI	AMENAZA	VULNERABILIDAD	COD. RIESGO	RIESGO
OT1	Tiempo: Optimizar el desempeño de la gestión de proyectos.	Incremento de los costos de horas hombre.	Ausencia del uso de prácticas adecuadas para la estimación de presupuestos. Personal no tiene capacidad para elaborar presupuestos.	R001	No recibir la aprobación de la Gerencia General debido a exceder el monto presupuestado.
		Incremento de tiempos estimados en el cronograma de trabajo según lo planificado.	Ausencia de las buenas prácticas de gestión de proyectos.	R002	No cumplimiento de los tiempos estimados en la planificación del proyecto.
OT2	Integración: Integrar los sistemas de información con los equipos de proyectos y usuarios orientados a mejorar la satisfacción del cliente.	Falta de interés de los integrantes del equipo de proyecto y usuarios.	Ausencia de metodologías formales de gestión de proyectos que requieran la identificación y compromiso del stakeholder.	R003	Retraso en la entrega de las soluciones debido a la usencia de metodologías que aseguren una adecuada gestión del proyecto y calidad del producto.
		Rotación del personal.	Ausencia de criterios priorización de cartera de proyectos. Ausencia de recursos humanos para cubrir las plazas vacantes.	R004	No contribuir con el objetivo de fidelización con la empresa por una inadecuada sustentación y/o evaluación de proyectos.
OT13	Presupuesto: Garantizar el uso y definición apropiada de presupuestos de sistemas	Nuevos requerimientos no planificados por las áreas de negocio.	Ausencia de un proceso de control de cambios.	R005	Nuevos requerimientos del negocio que no sean atendidos oportunamente por al Área de TI debido a la ausencia de un proceso de control de cambios.

OT4	Indicentes: Reducir incidentes registrados en el Quality Center y Mesa de Ayuda.	Analistas de sistemas y líderes de proyecto sin el enfoque de calidad o carencia de conocimientos y/o experiencia apropiada.	No se aplican estándares de calidad o revisiones de calidad en los procesos de implantación de soluciones tecnológicas.	R006	Incremento de incidentes debido a un inadecuado control del servicio de Mesa de Ayuda y Quality Center.
OT15	Valoración de proyectos y cambios Lograr un adecuado análisis y costo beneficio de los proyectos y requerimientos de TI.	Personal sin capacitación apropiada en estimación y monitoreo de beneficios	Ausencia de un proceso de gestión de proyectos que incluya actividades de elaboración de estudios de factibilidad.	R007	Existe el riesgos que los proyectos de TI no entreguen el valor apropiado al negocio debido a la ausencia de procesos eficientes de gestión de proyectos.
OT16	Satisfacción Obtener una satisfacción mensual de servicio de TI superior al 85%	Personal de responsable del soporte a los sistemas no comprometido con la calidad de atención a los usuarios.	Ausencia de un proceso de monitoreo y control del funcionamiento de los sistemas de información que están en producción.	R008	Existe el riesgo de incrementar la cantidad de incidentes, además de poner en puesta a producción sistemas de información que no satisfagan los requisitos del negocio.

4.6 Fase 5. Evaluación de Riesgos:

En esta fase se ha evaluado todos los riesgos mencionados en la fase anterior pero a continuación solo detallaremos el proceso de evaluación del riesgo que tiene mayor nivel de impacto, siendo este el riesgo: **Incremento de incidentes debido a un inadecuado control del servicio de Mesa de Ayuda y Quality Center (R006)** identificado en la fase anterior.

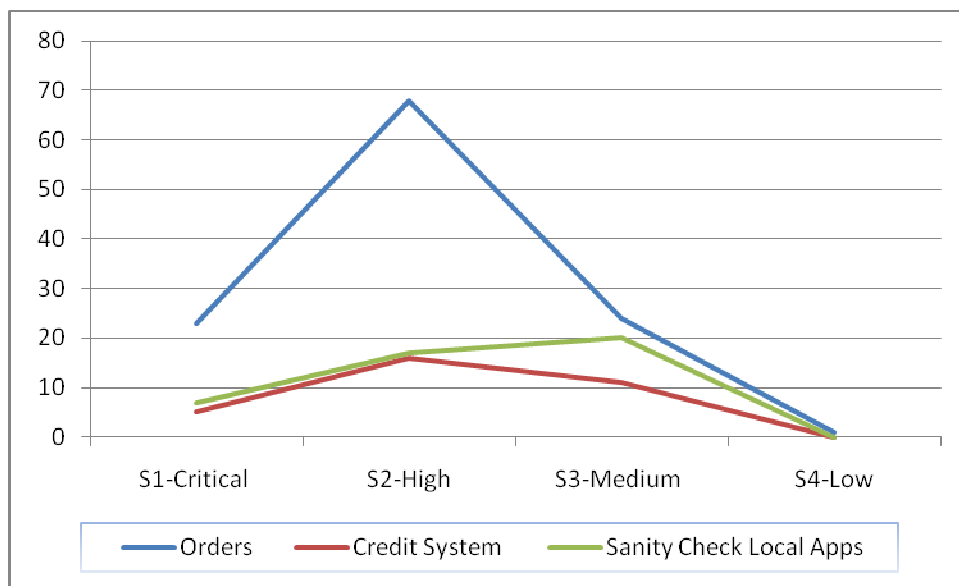
4.6.1 Análisis cualitativo de riesgos

A. Análisis de los Ambientes de TI

Cuadro 4.1: Nivel de Incidentes E2E

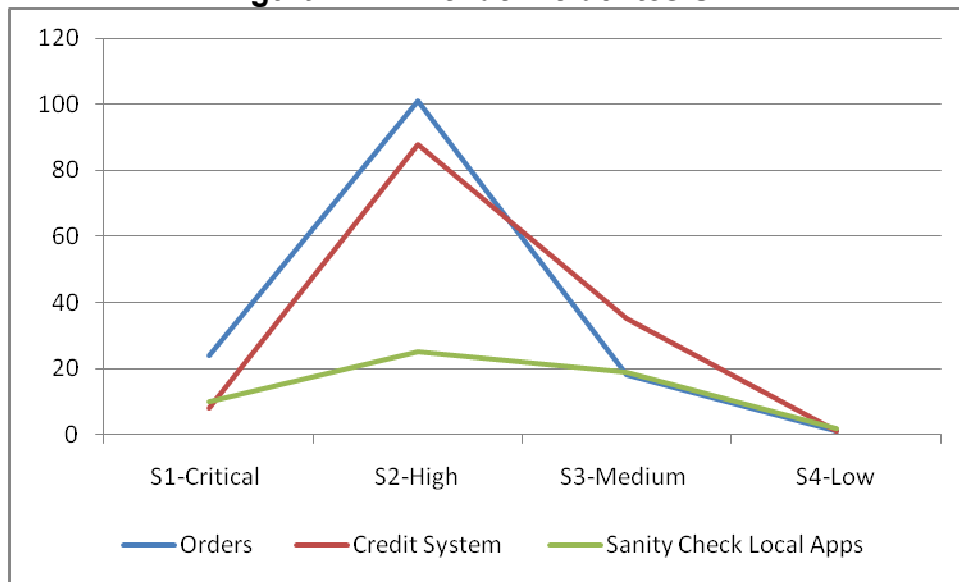
Severidad	Orders	Credit System	Sanity Check Local Apps	Total
S1-Critical	23	5	7	35
S2-High	68	16	17	101
S3-Medium	24	11	20	55
S4-Low	1	0	0	1
Total	116	32	44	192

Figura 4.6. Nivel de Incidentes E2E



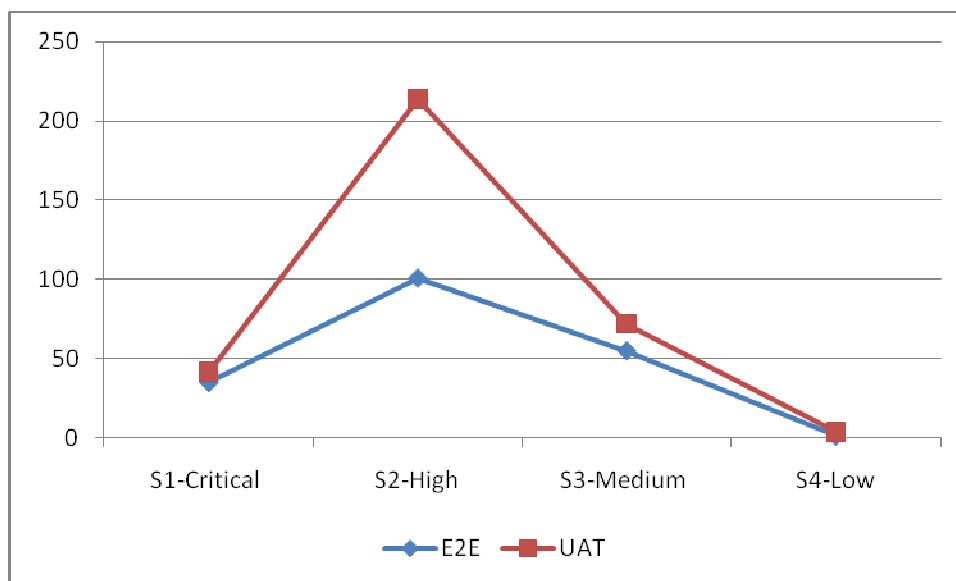
Cuadro 4.2: Nivel de Incidentes UAT

Severidad	Orders	Credit System	Sanity Check Local Apps	Total
S1-Critical	24	8	10	42
S2-High	101	88	25	214
S3-Medium	18	35	19	72
S4-Low	1	1	2	4
Total	144	132	56	332

Figura 4.7. Nivel de Incidentes UAT**Cuadro 4.3: Comparación de nivel de incidencias**

Severidad	E2E	UAT
S1-Critical	35	42
S2-High	101	214
S3-Medium	55	72
S4-Low	1	4
Total	192	332

Figura 4.8. Comparación de nivel de incidencias



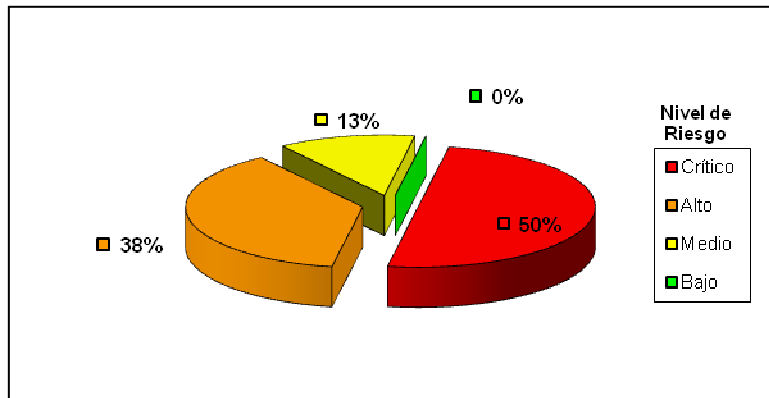
B. Análisis de Vulnerabilidades

El siguiente grafico muestra el total de las vulnerabilidades, según el nivel de riesgo definido en el cuadro 3.11, identificadas en los proyectos de TI que están asociados a la mejora del Proceso Muestra.

Cuadro 4.9: Total de vulnerabilidades identificados

Nivel de Riesgo		Cant.	Porcentaje
Rojo	Crítico	4	50%
Naranja	Alto	3	38%
Amarillo	Medio	1	13%
Verde	Bajo	0	0%
TOTAL		8	100%

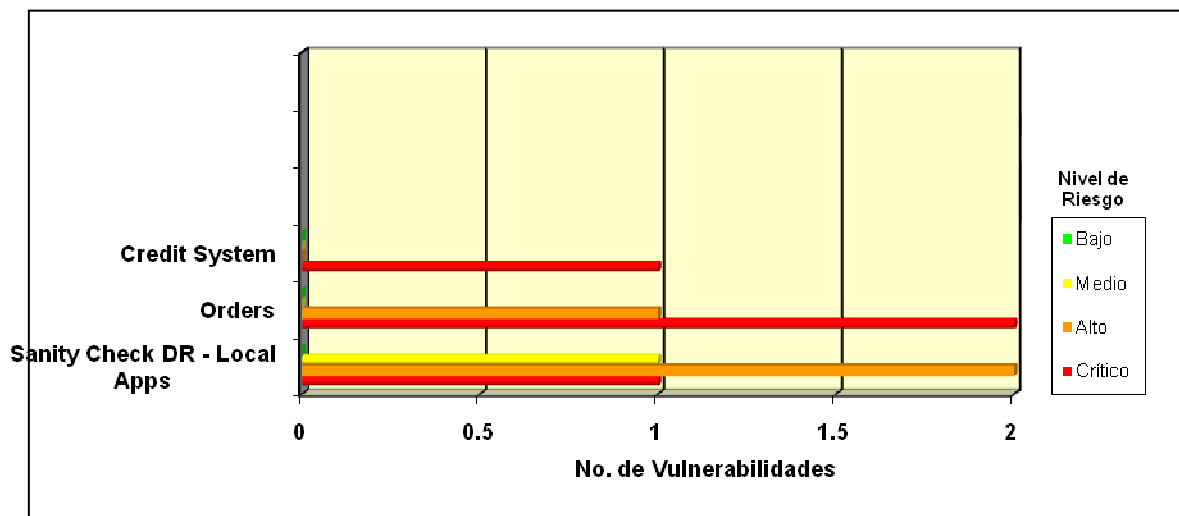
Figura 4.5 Total de vulnerabilidades identificadas



Cuadro 4.4: Número de vulnerabilidades por Nivel de riesgo vs Proyectos de TI

Nivel de riesgo				
	Sanity Check DR - Local Apps	Orders	Credit System	Total
Crítico	1	2	1	4
Alto	2	1		3
Medio	1			1
Bajo				0
Total	4	3	1	8

Figura 4.6 Nivel de Riesgo vs Proyecto de TI



CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha Motivo
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho	05/01/2010

EVALUACIÓN CUALITATIVA DE RIESGOS

OTI	COD. RIESGO	DESCRIPCIÓN DEL RIESGO	VULNERABILIDAD	NC	PROBABILIDAD	IMPACTO	PROB X IMPACTO	NR
OT11	R001	No recibir la aprobación de la Gerencia General debido a exceder el monto presupuestado.	Ausencia del uso de prácticas adecuadas para la estimación de presupuestos. Personal no tiene capacidad para elaborar presupuestos.		3	5	15	
	R002	No cumplimiento de los tiempos estimados en la planificación del proyecto.	Ausencia de las buenas prácticas de gestión de proyectos.		5	5	25	
OT12	R003	Retraso en la entrega de las soluciones debido a la usencia de metodologías que aseguren una adecuada gestión del proyecto y calidad del producto.	Ausencia de metodologías formales de gestión de proyectos que requieran la identificación y compromiso del stakeholder.		2	3	6	
	R004	No contribuir con el objetivo de fidelización con la empresa por una inadecuada sustentación y/o evaluación de proyectos.	Ausencia de criterios priorización de cartera de proyectos. Ausencia de recursos humanos para cubrir las plazas vacantes.		2	3	6	

OTI3	R005	Nuevos requerimientos del negocio que no sean atendidos oportunamente por el Área de TI debido a la ausencia de un proceso de control de cambios.	Ausencia de un proceso de control de cambios.		4	4	16	
OTI4	R006	Incremento de incidentes debido a un inadecuado control del servicio de Mesa de Ayuda y Quality Center.	No se aplican estándares de calidad o revisiones de calidad en los procesos de implantación de soluciones tecnológicas.		5	4	20	
OTI5	R007	Existe el riesgo que los proyectos de TI no entreguen el valor apropiado al negocio debido a la ausencia de procesos eficientes de gestión de proyectos.	Ausencia de un proceso de gestión de proyectos que incluya actividades de elaboración de estudios de factibilidad.		4	3	12	
OTI6	R008	Existe el riesgo de incrementar la cantidad de incidentes, además de poner en puesta a producción sistemas de información que no satisfagan los requisitos del negocio.	Ausencia de un proceso de monitoreo y control del funcionamiento de los sistemas de información que están en producción.		3	2	6	

4.7 Fase 6. Análisis de los Resultados de la Evaluación de Riesgos.

CONTROL DE VERSIONES			
Versión	Hecha por	Revisado por	Aprobado por
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho
			Fecha Motivo
			05/01/2010

PLAN DE RESPUESTA A RIESGOS

OTI	COD. RIESGO	AMENAZA / OPORTUNIDAD	RIESGO	NR	RESPUESTAS PLANIFICADAS	TIPO DE RPTA.	PRIORIDAD	PLAN DE COTINGENCIA
OTI1	R001	AMENAZA	No recibir la aprobación de la Gerencia General debido a exceder el monto presupuestado.	R	Proponer un proceso de evaluación de costo beneficio.	MITIGAR	R	Evaluar el costo planificado vs presupuestado e informar a la gerencia la limitación que se tiene. Tomar medidas correctivas.
					Solicitar feedback de los costos de cada proyecto.	MITIGAR		
	R002	AMENAZA	No cumplimiento de los tiempos estimados en la planificación del proyecto.	R	Solicitar feedback de los tiempos estimados de los proyectos vs los tiempos reales.	MITIGAR	R	Evaluar reprogramación de tiempos estimados. Tomar acciones correctivas.
OTI2	R003	AMENAZA	Retraso en la entrega de las soluciones debido a la ausencia de	A	Solicitar feedback de los participantes del proyecto. Solicitar feedback	MITIGAR	A	Analizar causas. Tomar acciones correctivas. Monitorear resultados.

			metodologías que aseguren una adecuada gestión del proyecto y calidad del producto.			de los usuarios.				
	R004	AMENAZA	No contribuir con el objetivo de fidelización con la empresa por una inadecuada sustentación y/o evaluación de proyectos.	A		Comunicación y coordinación con los usuarios y responsables del proyecto.	MITIGAR	A		Evaluar necesidades. Evaluar impactos contractuales. Tomar acciones correctivas.
OTI3	R005	AMENAZA	Nuevos requerimientos del negocio que no sean atendidos oportunamente por el Área de TI debido a la ausencia de un proceso de control de cambios	R		Solicitar feedback de los usuarios mediante cantidad de requerimientos atendidos. Coordinar requerimientos pendientes entre los usuarios y representantes de equipos de desarrollo.	MITIGAR	R		Evaluar necesidades. Evaluar impactos contractuales. Tomar acciones correctivas.
OTI4	R006	AMENAZA	Incremento de incidentes debido a un inadecuado control del servicio de Mesa de Ayuda y Quality Center.	R		Solicitar feedback de registro de incidentes a los analistas de test. Coordinación continúa de resolución de incidentes.	MITIGAR	R		Evaluar necesidades Evaluar impactos en los tiempos. Evaluación del impacto. Tomar acciones correctivas. Monitorear resultados.

OT15	R007	OPORTUNIDAD	Existe el riesgo que los proyectos de TI no entreguen el valor apropiado al negocio debido a la ausencia de procesos deficientes de gestión de proyectos.	N	Solicitar lista de requerimientos. Programar proceso eficiente de gestión de proyectos.	MITIGAR	A	Analizar causas. Realizar acciones correctivas. Analizar impacto generado.
OT16	R008	AMENAZA	Existe el riesgo de incrementar la cantidad de incidentes, además de poner en puesta a producción sistemas de información que no satisfagan los requisitos del negocio.	A	Solicitar feedback de nivel de satisfacción al cliente mediante encuestas por cada operación. Coordinación y comunicación con los usuarios.	MITIGAR	A	Evaluar necesidades. Analizar impactos del nivel de satisfacción. Monitorear resultados.

4.2.12. Acciones Correctivas

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho	05/01/2010

ACCIÓN CORRECTIVA N ° 001

NOMBRE DEL PROCESO	NOMBRE DEL PROYECTO
PROCESO DE VENTAS – CANAL FULFILLMENT	AUTOMATIZACIONES DE ACTIVACIONES

DEFINICIÓN DEL PROBLEMA:

Se detecto el retraso en la entrega de las activaciones de equipos por parte de los usuarios hacia los clientes.

REPARACIÓN DEL DEFECTO:

- Se mostrara en el list box de seleccionados los SSAA por defecto.
- Se validará, al agregar el ítem a la orden, la existencia de los SSAA por defecto en el template del plan tarifario elegido.
- Se activarán automáticamente los SSAA por defecto junto con la creación y activación del contratos y servicios básicos asociados al template del plan tarifario.
- Si se agrega un SSAA diferente a los que están por defecto, entonces el flujo seguirá su línea manual.

IDENTIFICACIÓN DE LAS CAUSAS RAÍCES

- El tiempo de demora en la activación de un equipo por parte de los usuarios era mayor a lo que se tenía propuesto.
- No se estaban considerando los SSAA propuestos en la oferta comercial versión 10.5.
- La carga de trabajo de los usuarios que tienen el rol de Atención al Cliente es mayor ya que tienen que realizar mas ordenes de Activación y Desactivación de Servicios.

ACCIÓN CORRECTIVA A TOMAR

- La activación manual de los servicios adicionales de una orden de post venta será remplaza por una activación automática que será parte de la misma orden de venta.
- Se limitara las activaciones de los servicios adicionales a solo activar los servicios adicionales por defecto.

AUTORIZACIÓN DE ACCIÓN CORRECTIVA

AUTORIZADO POR :	Release Manager
FECHA:	

4.2.13 INFORME DE MONITOREO DE RIESGOS

CONTROL DE VERSIONES				
Versión	Hecha por	Revisado por	Aprobado por	Fecha
05/01/2010	Milagros Cancho	Milagros Cancho	Milagros Cancho	05/01/2010

INFORME DE MONITOREO DE RIESGOS

NOMBRE DEL PROCESO	NOMBRE DEL PROYECTO
PROCESO DE VENTAS – CANAL FULFILLMENT	AUTOMATIZACIONES DE ACTIVACIONES

RIESGOS ACTUALES POTENCIALES
REVISIÓN Y CONFIRMACIÓN DE PROBABILIDAD E IMPACTO ESTIMADOS INICIALMENTE
- Baja satisfacción de los usuarios, la probabilidad de ocurrencia de incidentes durante las pruebas tiende a subir más del 0.7 estimado. - El no cumplimiento de los tiempos estimados mantiene su probabilidad en 0.84. - El retraso en la entrega de las soluciones propuestas mantiene su probabilidad en 0.2, con tendencia a subir.
REVISIÓN DE ADECUACIÓN DE RESPUESTAS PLANIFICADAS PARA LOS RIESGOS IDENTIFICADOS INICIALMENTE
- A todos los usuarios se solicita el feedback de los incidentes que registran durante sus pruebas en el ambiente de UAT. - Para el cambio de fecha en el cronograma del proyecto se aplico la flexibilidad en cambios por motivos de fuerza mayor aprobados por el comité respectivo.
REVISIÓN DE PLANES DE CONTINGENCIA PARA LOS RIESGOS IDENTIFICADOS INICIALMENTE
- Para los proyectos y riesgos identificados se ha efectuado todos los planes de contingencia previstos. - Para la metodología de gestión de proyectos, se ha evaluado necesidades, los impactos y tomado las acciones correctivas pertinentes.
VERIFICACIÓN DE EJECUCIÓN DE RESPUESTAS PLANIFICADAS
- Para la modificación de cronograma de proyecto se aplico una respuesta planificada. - Para la subida del indicador de incidentes detectados se aplico una respuesta planificada.
RIESGOS ACTUALES SUCEDIDOS
VALORACIÓN DE IMPACTO REAL VS IMPACTO ESTIMADO
- Incumplimiento de los tiempos planificados en el cronograma, inicialmente el impacto estimado fue del 0.24, y el impacto real fue de 0.20. - Registro de incidentes, inicialmente el impacto estimado fue del 0.5, y el impacto real fue de 0.75.
REVISIÓN DE PLANES DE CONTINGENCIA
Para la modificación del cronograma de proyectos, se ha efectuado: - Evaluación del impacto. - Reprogramación de entrega del proyecto. Para mitigar el nivel de registro de incidencia, se ha realizado: - Informar diariamente los resultados de las incidencias registradas. - Tomar las acciones correctivas pertinentes.
ELABORACIÓN DE PLANES DE EMERGENCIA
No aplica.

PROGRAMACIÓN DE EJECUCIÓN DE PLANES DE CONTINGENCIA / EMERGENCIA
No aplica.
EVALUACIÓN DE NECESIDADES DE ACCIONES CORRECTIVAS O SOLICITUDES DE CAMBIO
NUEVOS RIESGOS DETECTADOS
EVALUACIÓN CUALITATIVA Y CATEGORIZACIÓN DE RIESGOS
No se ha detectado nuevos riesgos.
DEFINICIÓN DE RESPUESTAS PLANIFICADAS
No se ha detectado nuevos riesgos.
DEFINICIÓN DE PLANES DE CONTINGENCIA
No se ha detectado nuevos riesgos.
PROGRAMACIÓN DE EJECUCIÓN DE RESPUESTAS PLANIFICADAS
No se ha detectado nuevos riesgos.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El objetivo de utilizar un marco de trabajo en la administración de riesgos es gestionar adecuadamente los riesgos en los proyectos de TI asociados al proceso, predecir los riesgos potenciales y mitigarlos.
- El uso del marco de trabajo propuesto para la administración de riesgos no garantiza el éxito de los proyectos ni mucho menos cumplir con los objetivos propuestos, pero facilita la administración de los riesgos para su respectivo cumplimiento.
- El PMBOK es una guía reconocida a nivel internacional por la aplicación de sus mejores prácticas en la gestión de proyectos, los cuales nos muestra procesos específicos detallados para la gestión de riesgos.
- Las proyecciones de la evaluación de riesgos nos ayudara a visualizar el nivel de cumplimiento de nuestros objetivos de control.
- El inicio de proyectos para la mejora de los procesos sin un correcto alineamiento estratégico provocara que no se cumplan la mejora planificada.
- Habrá una mejor madurez de las comunicaciones para mantener informado y al tanto a la Alta gerencia acerca de los riesgos potenciales en cada proceso.
- Se tendrá informada a la alta gerencia sobre el nivel de cumplimiento de los objetivos para realizar medidas correctivas o preventivas que podría o no tomar para el beneficio de la empresa.

5.2

Recomendaciones

- Se debe considerar que al aplicar una de las áreas del conocimiento de la guía del PMBOK, no es obligatoria seguir con todos los pasos que esta nos recomienda.
- Considerar que la mejora de los procesos se encuentra muy ligada al nivel de alineamiento estratégico en el que se encuentra la compañía.
- Se sugiere tener un cierto nivel de madurez en el desarrollo del gobierno de TI dentro de la compañía.
- Los costos y beneficios pueden verse influenciados por los cambios que pueden haber en los tiempos estimados gracias a las acciones correctivas.
- Es necesario tomar en cuenta que las mejores prácticas de COBIT ayudaran a la compañía a entender sus sistemas de información y decidir el nivel de seguridad y control que es necesario para proteger sus activos.

REFERENCIAS BIBLIOGRÁFICAS

- Bibliografía Especializada.

[CON 06] CONDORI ARI Cesar Alberto y GONZALES AQUINO Oriel, *“Metodología de la gestión de riesgos de Tecnología de Información en una institución financiera”*, Tesis de Pregrado, s.e., Lima 2006.

[ISA 05] Information Systems Audit and Control Association (ISACA), *Control Objectives for Information and related Technology 4.0 (COBIT)*, 2005

[MOR 06] MORALES PINTO, Irma Estela, *“Reducción del impacto de los riesgos en proyectos TI”*, Tesis de Pregrado, s.e., Lima 2006

[PRO 04] Project Management Institute, *“A Guide to the Project Management Body of Knowledge (PMBOK® Guide) - Third Edition”*, 2009.

- Revistas o Papers

[ALF 07] Alfonso Romero B.1, Daniel Lovera D.1, Simeón Yaringaño Y.1, Silvana Flores Ch., Revista del Instituto de Investigaciones FIGMMG Vol. 10, N° 19, 55-61, UNMSM 2007

[EDP 01] EDPACS - The Edp Audit, Control, And Security- A view of international IT Security Standards, Especiallly ISO/IEC17799, Diciembre 2001.

- Direcciones Electrónicas

[WWW 01] <http://www.rspa.com/spi/project-risk.html#resources>

[WWW 01] <http://www.ruleworks.co.uk/riskguide/risk-cycle.htm>

[WWW

02]

http://es.wikipedia.org/wiki/Project_Management_Body_of_Knowledge

ANEXOS Y APÉNDICES

Anexo1. Formato de Objetivos de Negocio

Anexo2. Formato de Objetivos de TI

Anexo3. Formato de Gobierno de TI

Anexo4. Formato de Marco De Control

Anexo 5. Formato de Mapeo de Procesos

Anexo 6. Formato de Ficha de Proceso

Anexo 7. Formato de Planificación de Riesgos

Anexo 8. Formato de Identificación de Riesgos

Anexo 9. Formato de Evaluación de Riesgos

Anexo 10. Formato de Respuesta a los riesgos

Anexo 11. Formato de Acciones correctivas

Anexo 12. Formato de Informe de Monitoreo