AAS5235

UCAB Universidad Católica ANDRES BELLO

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
ÁREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

TRABAJO ESPECIAL DE GRADO

DISEÑO DE HERRAMIENTA PARA MINIMIZAR EL RIESGO TECNOLÓGICO EN EL PROCESO "CONTROL DE CAMBIOS" EN EL BANCO DE DESARROLLO ECONÓMICO Y SOCIAL DE VENEZUELA (BANDES).

Presentado por

GONZALEZ FERREIRA FÁTIMA MARIA

Para optar al título de

Especialista en Gerencia de Proyectos

Asesor
Emmanuel López

Caracas, Marzo de 2013

Caracas, 12 de Marzo de 2013

Directora del Programa Gerencia de Proyectos-ñ

Estudios de Postgrado

Universidad Católica Andrés Bello (UCAB)

Presente.-

Referencia: **Aprobación del Asesor**

Tengo a bien dirigirme a Usted a fin de informarle que he leído y revisado el borrador final del Trabajo Especial de Grado titulado **"DISEÑO DE HERRAMIENTA PARA MINIMIZAR EL RIESGO TECNOLÓGICO EN EL PROCESO "CONTROL DE CAMBIOS" EN EL BANCO DE DESARROLLO ECONÓMICO Y SOCIAL DE VENEZUELA (BANDES)"**, presentado por Fátima María González Ferreira, titular de la cédula de identidad N° 16.700.263, como parte de los requisitos para optar al Título de **Especialista en Gerencia de Proyectos**.

A partir de dicha revisión, considero que el mencionado Trabajo Especial de Grado reúne los requisitos y méritos suficientes para ser sometido a evaluación por el distinguido Jurado que tenga(n) a bien designar.

Atentamente,

Ing. Emmanuel López C.

C. I. Nº 3.189.576

Caracas, 12 de Marzo de 2013

Sres.
UNIVERSIDAD CATÓLICA ANDRÉS BELLO
Postgrado de Gerencia de Proyectos
Cuidad

Nos dirigimos a ustedes para informarles que hemos autorizado a la Ingeniero de Sistemas, Fátima María González Ferreira; C.I. 16.700.263, quien labora en esta organización, a hacer uso de la información proveniente del proceso de Gestión de Control de Cambios Tecnológico que gestiona la Oficina de Requerimiento y Planificación Tecnológica de la Gerencia Ejecutiva Tecnología de la Información, para documentar y soportar los elementos de los análisis estrictamente académicos que conllevarán a la realización del Trabajo Especial de Grado, Diseño de herramienta para minimizar el riesgo tecnológico en el proceso "Control de Cambios" en el Banco de Desarrollo Económico y Social de Venezuela (BANDES); como requisito para optar al título de Especialista en Gerencia de Proyectos, exigidos por la Dirección General de los Estudios de Postgrado de la Universidad Católica Andrés Bello.

Sin más a que hacer referencia, atentamente,

Ing. Juan Federico Barone
Gerente Ejecutivo (E)

DEDICATORIA

El presente Trabajo Especial de Grado se lo dedico...

A Dios, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor. A mis queridos **Padres** quienes con mucho cariño, amor y ejemplo han hecho de mí una persona con valores para poder desenvolverme como: Esposa, Hija y Profesional.

A mi Esposo, Antonio Guevara que ha estado a mi lado dándome cariño, confianza y apoyo incondicional para seguir adelante para cumplir otra etapa en mi vida, y por estar conmigo en aquellos momentos en que el estudio y el trabajo ocuparon todo mi tiempo.

A mi Tutor, el Ingeniero Emmanuel López, por su tiempo compartido y por impulsar el desarrollo de este Trabajo Especial de Grado.

INDICE GENERAL

CARTA DE APROBACIÓN DEL TUTOR ii

DEDICATORIA iv

INDICE GENERAL v

ÍNDICE DE TABLAS viii

ÍNDICE DE FIGURAS ix

ÍNDICE DE GRÁFICAS x

RESUMEN xi

LISTADO DE SIGLAS Y ACRÓNIMOS xii

INTRODUCCIÓN 1

CAPÍTULO I 4
- EL PROBLEMA 4
- Planteamiento del Problema 4
- Objetivos del Estudio 9
  - *Objetivo General* *9*
  - *Objetivos Específicos* *9*
- Justificación del Estudio 9
- Alcance 10
- Limitaciones 11

CAPÍTULO II 12
- MARCO TEÓRICO 12
- Antecedentes de la Investigación 12
- Bases Teóricas 15
  - *Gestión de Proyectos* *15*
  - *Marco de Referencia ITIL V3* *18*
  - *Riesgo* *24*
  - *Valoración del Riesgo* *24*
  - *Identificación del Riesgo* *25*

Clasificación del Riesgo *26*
Análisis del Riesgo *28*
Priorización de los Riesgos *30*
Consideración de Acciones *31*

CAPÍTULO III 33
MARCO METODOLÓGICO 33
Tipo de Investigación 33
Diseño de la Investigación 34
Unidad de Análisis 35
Técnicas e Instrumentos de Recolección de Datos 36
Técnicas para el Procesamiento y Análisis de los Datos 37
Operacionalización de los Objetivos 37
Consideraciones Éticas 40

CAPÍTULO IV 43
MARCO ORGANZACIONAL 43
Contexto Organizacional 43
Misión 44
Visión 44
La Oficina de Requerimiento y Planificación Tecnológica (ORPT) 46

CAPÍTULO V 48
PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS 48

Desarrollo del Objetivo Específico Nro.1. Diagnosticar la situación actual del proceso de control de cambio a fin de determinar los riesgos tecnológicos. 49

Desarrollo del Objetivo Específico Nro.3. Desscribir los elementos relacionados con el riesgo tecnológico, en base al marco referencial Information Technology Infraestructure Library (ITIL) en Bandes. 59

Desarrollo del Objetivo Específico Nro.3. Determinar los niveles de riesgos para el proceso de control de cambio. 62

CAPÍTULO VI 72
LA PROPUESTA 72

Desarrollo del Objetivo Específico .Nro.4. Diseñar la herramienta para la gestión de riesgos en el proceso "Control de Cambios Tecnológicos" para BANDES. 72
Introducción 72
Objetivo 73
Alcance 73
Estructura de la Propuesta 73
Factibilidad de la Propuesta 84
Beneficios de la Propuesta 85

CAPÍTULO VI 86
CONCLUSIONES Y RECOMENDACIONES 86

REFERENCIAS BIBLIOGRÁFICAS 89

ÍNDICE DE TABLAS

Tabla N° **Pág.**

1. Cuadro Operacional de Variables.....38
2. Controles de Cambios Ejecutados.....52
3. Controles de Cambio Fallidos.....57
4. Elementos de Configuración.....60
5. Escala de Probabilidad.....6
6. Escala de Impacto.....64
7. Escala de Urgencia.....67
8. Niveles de Prioridad.....69
9. Niveles de Riesgos.....70
10. Matriz de Prioridad Actual del Proceso de Control de Cambio.....77
11. Identificación y Evaluación Cuantitativa de los Riesgo.....79
12. Gestión de Riesgo.....80

ÍNDICE DE FIGURAS

Figura N° **Pág.**

1. Los Cinco (5) Procesos del Ciclo de Vida del Servicio.....19
2. Asignación de Prioridades.....30
3. Cronograma de Actividades.....39
4. Estructura Organizativa del Bandes 45
5. Ubicación de la ORPT como Unidad Funcional 47
   dentro de la Estructura Organizativa del Bandes
6. Entradas - Actividades – Salidas del Proceso de Control de Cambio.....50
7. Flujo de Gestión del Proceso de Control de Cambio.....74
8. Flujo Actual de Priorización.....77
9. Comparación de Procesos.....79

ÍNDICE DE GRÁFICAS

Gráfica N° **Pág.**

1. Aplicaciones o Elementos de Configuración con Mayor Índice de Cambios.....54
2. Asignación de Prioridad.....69
3. Asignación de Riesgo.....71

UNIVERSIDAD CATÓLICA ANDRÉS BELLO
VICERRECTORADO ACADÉMICO
ESTUDIOS DE POSTGRADO
AREA DE CIENCIAS ADMINISTRATIVAS Y DE GESTIÓN
POSTGRADO EN GERENCIA DE PROYECTOS

DISEÑO DE HERRAMIENTA PARA MINIMIZAR EL RIESGO TECNOLÓGICO EN EL PROCESO "CONTROL DE CAMBIOS" EN EL BANCO DE DESARROLLO ECONÓMICO Y SOCIAL DE VENEZUELA (BANDES).

Autor: Fátima M. González F.
Asesor: Emmanuel López
Fecha: Marzo 2013

RESUMEN

La Oficina de Requerimiento y Planificación Tecnológica (ORPT), es una unidad estratégica adscrita a la Gerencia Ejecutiva de Tecnología de la Información del Banco de Desarrollo Económico y Social de Venezuela (BANDES), cuyas responsabilidades se basan en administrar la gestión de control de cambios tecnológicos, así como lo relativo al diseño e implantación del plan estratégico de tecnología de la información, todo esto con la finalidad de proveer al instituto de una infraestructura tecnológica de vanguardia, de acuerdo con los lineamientos internos y normativas que rigen la materia. Debido a que se ha determinado la existencia de incidentes que afectan la continuidad y productividad del servicio, que es consecuencia de la poca certeza por parte del técnico o desarrollador y del gestor del cambio al momento de determinar el riesgo tecnológico, se realizó el presente con el objetivo de determinar el impacto, la probabilidad de ocurrencia, prioridad y tipo de riesgo que puede suscitar un evento inesperado en la plataforma tecnológica de la institución, como consecuencia de la ejecución de un control de cambio, todo fundamentado en el marco de referencia ITIL. A fin de cumplir con este objetivo se recopiló información sobre una muestra de controles de cambio los cuales fueron analizados para establecer la criticidad de las aplicaciones o servicios de acuerdo a su desempeño y el impacto sobre el negocio. Como producto del estudio se elaboraron matrices para determinar el tipo de impacto, probabilidad, urgencia, prioridad y riesgo, con cinco (5) tipos de niveles de severidad. Por otro lado fueron creados dos (2) formularios para ser completados a fin de establecer el análisis e identificación de riesgo para el proceso de control de cambio.

Palabras clave: Gestión de control de cambios, marco de referencia ITIL, riesgos tecnológicos, gestor de cambios, continuidad del servicio, resiliencia.
Línea de trabajo: Gestión de Riesgos.

LISTADO DE SIGLAS Y ACRÓNIMOS

	SIGLAS Y/O ACRÓNIMOS	DESCRIPCIÓN
1	**BANDES**	Banco de Desarrollo Económico y Social de Venezuela
2	**DSDM**	Dynamic Sistems Developmed Method
3	**DNS**	Domain Name System
4	**DHCP**	Dynamic Host Configuration Protocol
5	**FAS**	Fondo Auto Administrado de Salud
6	**GEBOS**	Sistema de Crédito y Cobranza
7	**GETI**	Gerencia de Tecnología de la Información
8	**ICONTEC**	Instituto Colombiano de Normas Técnicas y Certificación
9	**ITIL**	Information Technology Infraestructure Library
10	**IR**	Identificación de Riesgos
11	**LDAP**	Lightweight Directory Access Protocol
12	**ORPT**	Oficina de Requerimiento y Planificación Tecnológica
13	**PMBOK**	Project Management Body Knowledge
14	**PMI**	Project Management Instistute
15	**RUB**	Racional Unified Process
16	**RFC´S**	Request For Change
17	**ROLLBACK**	Plan de Recuperación
18	**RAE**	Real Academia Española
19	**TI**	Tecnología de la Información
20	**TEG**	Trabajo Especial de Grado
21	**UCAB**	Universidad Católica Andrés Bello

INTRODUCCIÓN

La innovación y el cambio se han vuelto parte esencial de los negocios a un ritmo acelerado. Las organizaciones están haciendo uso de los sistemas de información para crear valor agregado en un mercado altamente competitivo. Hoy en día, son pocos los negocios que no se apoyan en la tecnología. La mayoría de la información administrativa y financiera se encuentra en plataformas de TI que garantizan procesos automatizados para agilizar las tareas rutinarias o en caso contrario sustentan el negocio con robustos sistemas de apoyo en la toma decisiones.

El riesgo tecnológico puede materializarse cuando no hay adecuados planes de gerencia, contingencia, monitoreo del rendimiento tecnológico relacionado a proyectos, productos o servicios. También cuando las organizaciones invierten tarde y, en algunas ocasiones, sin probar adecuadamente las tecnologías. Inmerso en el tema se encuentra la continuidad del servicio, la cual tiene como objetivo asegurar la disponibilidad de los servicios de la plataforma de TI a un 99.9 %; lo cual se debe lograr a través de la identificación y análisis cuantitativo y cualitativo de los posibles riesgos que se pueden presentar ante situaciones inesperadas. Las modificaciones en aplicaciones o sistemas de TI por razón de mejoras, nuevas implementaciones o factores imperativos legales, son posibles consecuencias que pueden atentar contra la continuidad del negocio y se manejan a través de la Gestión de Cambios, las cuales pueden realizarse o acometerse como proyectos dependiendo de la magnitud y envergadura de las actividades a realizar. Es por ello que con la presente investigación se buscó desarrollar una herramienta que abra el panorama de los posibles riesgos que se pueden presentar en los cambios de la plataforma de TI del Banco Económico y Social de Venezuela (BANDES). Para ello fue objeto de

estudio, principalmente, la Guía de los Fundamentos para la Dirección de Proyectos (PMBOK), capítulo de Gestión de Riesgos y el Marco de Referencia ITIL en el sub proceso de Control de Gestión y Cambio.

Este Trabajo Especial de Grado está estructurado en siete (07) capítulos que se describen brevemente a continuación:

Capítulo I. Propuesta de Investigación. Describe la situación que enmarca el contexto y delimitación del problema, objetivo general y objetivos específicos, justificación e importancia, limitaciones, estructura detallada de trabajo, cronograma y presupuesto

Capítulo II. Marco Teórico. Se presentan los antecedentes de la investigación, así como también, los diferentes conceptos que conforman el basamento teórico de la investigación.

Capítulo III. Marco Metodológico. Se define la metodología empleada, el tipo y diseño de la investigación, la unidad de análisis, población, muestra, técnicas e instrumentos de recopilación de información y consideraciones éticas.

Capítulo IV. Marco Organizacional. Se presenta el contexto organizacional del Bandes, su visión, misión, valores y estructura organizativa.

Capítulo V. Presentación y Análisis de los Resultados. Se realizan los análisis de la información recolectada con la aplicación de los instrumentos y la documentación encontrada en la unidad, utilizando como apoyo, gráficos, figura y tablas.

El Capítulo VI. La Propuesta. Contiene la estructura para la Gestión de los Riesgos, de la Gerencia Ejecutiva de Tecnología de la Información., en el proceso de Control de Cambio.

Capítulo VII. *Conclusiones y Recomendaciones. Se presentan los* resultados finales de la investigación.

Por último, se presentan las **Referencias Bibliográficas** utilizadas en el desarrollo de este Trabajo Especial de Grado.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

Las personas se enfrentan todos los días a situaciones que demandan organización, programación y análisis a fin de alcanzar un objetivo particular u organizacional. En un mundo tan fluctuante, solo las organizaciones que se adaptan a las nuevas condiciones del entorno logran asegurar su supervivencia, y es a través de la estructura metodológica de los proyectos que se logra materializar esta adaptabilidad; la clave está en su correcta gestión.

¿Pero qué tipo de proyectos son éstos que se generan en una organización, con la finalidad de satisfacer las necesidades de sus clientes?

La respuesta, está en la alta demanda de los individuos hacia soluciones automatizadas, que logran minimizar cualquier riesgo de error y maximizar el desempeño. Es aquí donde la tecnología hace presencia de la mano de una buena gestión. Es por esto que cada día se hace más necesario el acercamiento de las organizaciones hacia la administración de operaciones automatizadas a fin de asegurar que los servicios de TI se ofrezcan efectiva y eficientemente. El marco de referencia ITIL está basado en las mejores prácticas de procesos en TI y ha desarrollo un conglomerado de "libros" que ofrecen patrones y normas sobre la creación y el manejo de los procesos de TI. Entre estos procesos se encuentra la "Transición de Servicio" que, a su vez, contiene la Gestión de Cambios Tecnológicos y tiene por objetivo controlar todos los cambios durante el ciclo de vida del servicio así como también responder a cambios en los requerimientos de negocio y de tecnología, maximizando valor, reduciendo incidentes de interrupción de los servicios con el mínimo riesgo.

Toda organización que involucra tecnología tiene que añadir valor y garantía dentro del marco de la funcionalidad y utilidad, sobre los servicios prestados, lo cual a su vez, es un activo estratégico y está enmarcado en un ciclo de mejora continua.

Dentro de BANDES, se desempeña la Oficina de Requerimiento y Planificación Tecnológica, la cual es la unidad estratégica de la gerencia, encargada de coordinar las acciones relacionadas con los requerimientos de proyectos tecnológicos, la administración de la gestión de control de cambios, así como lo relativo al diseño e implantación del plan estratégico de tecnología de la información; todo esto con la finalidad de proveer al instituto de una infraestructura tecnológica de vanguardia, de acuerdo con los lineamientos internos y normativas que rigen la materia.

Entre las principales competencias de esta unidad se encuentra la gestión de control de cambios tecnológicos[1], que tiene como finalidad controlar todos los cambios durante el ciclo de vida del servicio, asegurando que estas modificaciones sean registradas y documentadas.

En la actualidad se carece de una herramienta para determinar el riesgo tecnológico para el proceso de control de cambio.

En reiteradas oportunidades se han presentado incidentes con respecto a la continuidad y productividad del negocio a consecuencia de la poca certeza, por parte del técnico o desarrollador, al momento de

---

[1] La gestión de control de cambios tecnológicos está ubicada dentro del proceso de transición, en el esquema del ciclo de vida del servicio en el que se fundamenta el marco de referencia *Information Technology Infraestructure Library* (ITIL) .Este marco de referencia está orientado a la gestión de servicio a través de las mejores prácticas de proceso de TI.

determinar el riesgo tecnológico, entendiéndose como escaso espacio en disco, incompatibilidad de versiones, mal etiquetado, inexistencia de servidores para la instalación de aplicaciones afines, entre otros. Esto ocurre por la inexistencia de una herramienta que contenga la suficiente información que permita analizar y tener un plan de respuesta inmediata para mitigar o eliminar el riesgo en el proceso o sistema objeto del cambio.

La gestión de control de cambio tecnológico está estructurada sobre cinco (5) formularios, en donde se registra desde la solicitud de control de cambio hasta la certificación de los cambios solicitados ya implementados, por parte del usuario funcional y la Coordinación de Seguridad de la Información.

Para que el Comité de Control de Cambio Tecnológico apruebe una solicitud de requerimiento de control de cambio, se tiene que pasar por un proceso, completando un formulario llamado "Solicitud de Control de Cambios Tecnológicos", en donde el área funcional y el área técnica, analizan los posibles efectos del cambio requerido sobre los elementos de configuración y documentación asociada al sistema y/o aplicación, modificación de manuales de usuarios y técnicos en caso de que aplique. Así mismo también se realiza una descripción estimada de las actividades necesarias para la ejecución del control de cambio, y un plan de recuperación estimado, en caso de tener que ejecutar un reverso, si el control de cambio a aplicar, presentara un problema .Se involucra a la Coordinación de Seguridad de la información para ver si el cambio cumple con los parámetros y políticas de seguridad, y se identifica la razón del control de cambio.

En el último análisis de este formulario se encuentra la mayor debilidad de todo el proceso de control de cambio, y no es más, que el

En el último análisis de este formulario se encuentra la mayor debilidad de todo el proceso de control de cambio, y no es más, que el análisis de riesgo del cambio sobre la plataforma tecnológica. Una vez determinado el riesgo, se asigna la prioridad que tiene el control de cambio, y es ésta lo que determina la importancia del cambio .La prioridad se basa en el impacto y la urgencia, aspectos éstos que son usados para identificar los tiempos requeridos para que se tomen acciones. Este último análisis se realiza bajo los siguientes criterios:

- El cambio afecta muchos componentes. Puede afectar la operatividad total del negocio. Riesgo e impacto alto.
- Existe muchas interrelaciones con otros componentes. Puede afectar la operatividad total del negocio. Riesgo e impacto alto.
- El cambio afecta algunos componentes. Puede afectar algunos servicios del negocio. Riesgo e impacto medio.
- El cambio afecta pocos compontes. No afecta la operatividad del negocio. Riesgo e impacto bajo.

Ahora bien el análisis de riesgo es uno de los sub-procesos medulares de la gestión de cambio, ya que se encuentra en la etapa inicial del flujo de cambio, y es allí donde se identifican y evalúan los posibles riesgos sobre la ejecución del cambio; esta información es considerada a la hora de tomar la decisión sobre si se implementará el cambio y, en caso afirmativo, sobre cuándo y de qué manera se llevará a cabo.

En la actualidad, cuando la Oficina de Requerimientos y Planificación Tecnológica (ORPT), recibe una solicitud de control de cambio, el análisis de riesgo es compartido entre el gestor del control de cambio y el área técnica, siendo el criterio de mayor peso, el del área técnica, ya que es ésta la que maneja la información de la estructura y funcionamiento de los sistemas y/o

aplicaciones objeto de cambio, y es allí, entonces, donde se confía en el experto y se toma el riesgo que éste, por su pericia indique. Ello se realiza sin ningún tipo de herramienta que logre extraer, del experto, información que el gestor de cambio pueda tomar y bajo ciertos criterios poder llegar a detectar un riesgo certero.

La solución a esta situación podría ser a través del desarrollo de una herramienta que logre reflejar los resultados cuantitativos y cualitativos del objeto de estudio. Así mismo que permita también el análisis y soluciones oportunas ante los riesgos identificados a fin de mitigarlos o disminuirlos. Esto con el objetivo de reducir incidentes, erradicar las interrupciones en el servicio y culminar toda solicitud de control de cambio con un cien por ciento de eficacia y eficiencia, a causa de la excelente gestión de cambio que realizaría la ORPT a través de la herramienta a desarrollar, cuestión esta que constituye el centro de interés y la problemática a investigar en el presente estudio.

Todo este análisis lleva a las siguientes interrogantes que se consideran deben ser respondidas para realizar el diseño de la herramienta para la Gestión de Riesgo en la plataforma TI de BANDES:

¿Cómo debería ser la herramienta para la gestión de riesgos en el proceso de control de cambio?

¿Cuáles serían los procesos o actividades críticas en cada sistema o aplicación?

¿Cuáles son las debilidades que presentan los proyectos por desarrollado y/o cambio en los sistema o aplicaciones?

¿Qué tipo de variables están asociadas a cada riesgo por procesos tecnológicos?

¿Qué tipos de riesgos están asociados a cada sistema o aplicación?

¿Cuáles serían los elementos que conformarían la herramienta para la gestión de riesgos en el proceso de control de cambios tecnológicos para el BANDES?

Objetivos del Estudio

Objetivo General

Elaborar una herramienta para la gestión de los riesgos, en el proceso "Control de Cambio Tecnológicos" en una organización financiera venezolana.

Objetivos Específicos

1. Diagnosticar la situación actual del proceso de control de cambio a fin de determinar los riesgos tecnológicos.
2. Describir los elementos relacionados con el riesgo tecnológico, en base al marco referencial *Information Technology Infraestructure Library* (ITIL) en Bandes.
3. Determinar los niveles de riesgos para el proceso de control de cambio.
4. Diseñar la herramienta para la gestión de riesgos en el proceso "Control de Cambios Tecnológicos" para BANDES.

Justificación del Estudio

Desde el punto de vista organizacional, los resultados del análisis de riesgo en el proceso de control de cambio tecnológico le permitirán a la Gerencia Ejecutiva de Tecnología de la Información:

- Identificar los grandes riesgos tecnológicos que se pueden presentar con la ejecución de un control de cambio tecnológico.
- Minimizar los incidentes o problemas que ocasionan una suspensión de servicio a consecuencia de una escasa estimación de riesgo-impacto del control de cambio sobre otras aplicaciones inherentes.
- Garantizar el óptimo funcionamiento de todos los servicios que presta la Gerencia Ejecutiva de Tecnología de la Información (GETI), antes los usuarios, cada vez que se realice un control de cambio tecnológico.

La GETI contaría con un nuevo activo: una herramienta para determinar el riesgo tecnológico, para el proceso de control de cambio. Este nuevo activo permitirá el análisis de dichos riesgos y brindará un abanico de soluciones oportunas, que evitará eventos o incidentes cada vez que se realice un control de cambio ya que se tendrán identificados los riesgos y sus posibles consecuencias así como también un plan de mitigación.

A nivel personal, contribuirá a profundizar y enriquecer los conocimientos actuales de gestión de riesgos en proyectos de quien desarrolla este trabajo.

Alcance

El alcance de este estudio comprendió realizar aquellos pasos necesarios para diseñar una herramienta a fin de minimizar los riesgos del proceso "Control de Cambio Tecnológicos" en BANDES, tomando en consideración la identificación, análisis cuantitativo y cualitativo, responsables y acciones recomendadas, de los riesgos por cada proceso

y/o aplicación tecnológica, tomando como base el Área de Gestión de Riesgos indicada en la Guía del PMI y las mejores prácticas en proceso de tecnología de la información ITIL en su versión 3.

El alcance de esta investigación comprende hasta el diseño de la herramienta, no así su, aprobación e implantación por parte de la empresa.

Limitaciones

En cuanto a las limitaciones, Sabino (1992), las define como "*obstáculos que eventualmente pudieran presentarse durante el desarrollo de la investigación*" (p. 38).

Se puede indicar que no se tuvo ninguna limitación para realizar este trabajo ya que las área internas de la Gerencia Ejecutiva de Tecnología de la información prestaron su apoyo para el logro de los objetivos del presente estudio.

CAPÍTULO II

MARCO TEÓRICO

Antecedentes de la Investigación

Al iniciar el presente trabajo de investigación se efectuó una revisión de algunos Trabajos Especiales de Grado (TEG) sobre la línea de gestión de cambios tecnológico bajo el marco de referencia ITIL y riesgos, de manera de poder contar con una base de investigación previa que apoye la temática expuesta. Los TEG que se tomaron como antecedentes de la investigación son los siguientes:

Villamizar (2010) en su Trabajo Especial de Grado para optar al título de Especialista en Gerencia de Proyectos, titulado **"Herramienta para la medición de riesgos en proyectos de implementación del sistema ERP SAP BUSSINES ONE"**. Este trabajo tuvo como objetivo desarrollar el prototipo de una herramienta que permita realizar la medición de riesgos en proyectos de implementación del sistema *ERP SAP Business One*. Como resultado de este proceso de investigación y desarrollo se obtiene una herramienta informática, que integra un conjunto de funciones que permite conocer el nivel de riesgo latente en un proyecto, con la idea de minimizar el impacto negativo de los riesgos presentes en los mismos. De este trabajo de tomó el ejemplo de la matriz de evaluación de probabilidad de riesgo en los tres (3) escenarios posibles (bajo, medio y alto), también se tomó el ejemplo de la matriz comparativa de los resultados obtenidos.

Tomando en cuenta que algunos de las solicitudes de controles de cambios son implementaciones de automatización de nuevos procesos o simplemente nuevos desarrollos, de este trabajo se tomó la categorización

de los riesgos en base a su identificación de un proyecto de software, a fin de contar una guía al momento de identificar los riesgo tecnológicos para solicitudes de cambios del mismo índole.

Marichal (2009) en su Trabajo Especial de Grado para optar al título de Especialista en Gerencia de Proyectos, titulado **"Diseño conceptual de un sistema para la gestión de riesgo en proyectos de desarrollo de software"**. Con la implementación de este diseño se buscó brindar tanto al gerente de proyecto, como también a los *stakeholders* del mismo, la capacidad de gestionar los factores de incertidumbre, bajo un marco de trabajo, conceptualizado y colaborativo de gerencia de riesgo. De esta investigación se tomó la arquitectura del diseño para los factores de incertidumbre y riesgo.

Panfil (2009) en su Trabajo Especial de Grado de Especialista en Gerencia de Proyectos, titulado **"Plan de gestión de riesgos para el proyecto de mejoras de las microcentrales hidroeléctricas ubicadas en la gran sabana operadas por EDELCA"**. El propósito de este plan es identificar, clasificar y analizar cualitativamente los eventos de riesgo que pueden afectar significativamente la adecuada ejecución del proyecto, para luego proponer un plan de gestión de los mismos. De este trabajo se tomó la estructura de la matriz de identificación de eventos, en donde se describe el riesgo, grado de ocurrencia, impacto sobre la plataforma de TI, acciones y estrategias, con nivel de alertas en colores tipo semáforo.

Simonovis (2007) en su Trabajo Especial de Grado para optar al título de Especialista en Gerencia de Proyectos, titulado **"Diseño del proceso de gestión de versiones y liberaciones para la Vicepresidencia de Operaciones de Tecnología de Información de Banesco, basado en mejores prácticas para la gestión de servicios de ITIL"**. Con la

implementación de este diseño se busca garantizar la continuidad y calidad de los servicios tecnológicos, utilizando solo versiones para pases a producción que han sido asignadas de forma organiza, correctamente probadas y autorizadas, objeto de la ejecución de un control de cambio.

De este trabajo se consideraron aspectos relacionados con el proceso de control de cambio tecnológico en base al marco de referencia ITIL, que administra la Vicepresidencia de Operaciones de Banesco, y se establecerá una comparación con la dinámica del proceso actual de gestión de cambio de la GETI.

Vincentelli (2007) en su Trabajo Especial de Grado para optar al título de Especialista en Gerencia de Proyectos, titulado **"Desarrollo de los proceso de gerencia de riesgos para los proyectos estratégicos de C.V.G. Electricidad del Caroní, C.A. –EDELCA-"**. Los procesos como identificación, análisis y posterior gerencia de los riesgos son materia compleja, es por esto que el autor propone el desarrollo de procesos de gerencia de riesgo para proyectos estratégicos en CVG EDELCA, con la finalidad de normalizar un enfoque que permita a la organización tener la certeza que a todos sus proyectos se les aplicaran dichos procesos y de esa forma aumentar la probabilidad de éxito de las iniciativas y cumplimiento de los objetivos estratégicos. De este trabajo se tomó el formato de las tablas para la tabulación o registro de los riesgos en donde se establece una serie de campos que se debe tener en cuenta al momento de identificar riesgos y entre los cuales se tiene, área de riesgo, descripción del riesgo, tipos de consecuencias, probabilidad de ocurrencia, impacto potencial, acción de mitigación, tipo de acción, entre otras. Todas estas variables alimentadas en una matriz para su posterior análisis.

Sosa (2006) en su Trabajo Especial de Grado de Especialista en Gerencia de Proyectos, titulado **"Gestión de riesgos en proyectos de desarrollo de software en una empresa de consultoría venezolana"**. A fin de gerenciar eficientemente y ser más competitivos en el mercado de la consultoría, surge esta propuesta para evitar que los proyectos se tornen inmanejables. Este modelo persigue una gestión de riesgos efectiva en los proyectos de desarrollo de software, a través del análisis de diferentes metodología para desarrollos como Microsoft *Solucions Framework* (MSF), *Dynamic Systems Development Method* (DSDM) *Rational Unified Process* (RUB), entre otros. De este proyecto se tomó una lista de riesgos de proyectos de desarrollo, estructurados en la diferente atapas que describen la metodologías nombradas, y que se evidenciaron en el análisis realizado a una muestra de proyectos de desarrollos.

Bases Teóricas

Como introducción a las base teóricas, se presenta un apartado sobre la Gestión de Proyectos, muy especialmente en la Gestión de Riesgos de la guía de fundamentos del PMI, marco de referencia ITIL y detalle de los conceptos básicos de estás mejores prácticas, y posteriormente adentrarnos en conceptos de riesgos tecnológicos.

Gestión de Proyectos

Chamoun (2002) define un proyecto como "*un conjunto de esfuerzos temporales, dirigidos a generar un producto o servicio único.*" (p. 27). En virtud de lo anterior, la Gestión de Proyectos ha venido a ordenar y normalizar toda serie de esfuerzos que las empresas invierten para sacar adelante esos trabajos "temporales" llamados proyectos.

De ahí que las organizaciones empezaron a especializarse y emprender trabajos que se denominaron "proyectos", que eran y siguen siendo acciones intensivas y temporales que tienen un objetivo final.

Con el pasar de los años, esta técnica de trabajo se fue afinando y se vio la utilidad de normalizarla, de forma tal que su aplicación pudiera hacerse de forma universal.

Así fue como nació la Guía de Fundamentos para la dirección de Proyectos, que contiene el marco conceptual que sirve de norte para tener mayores probabilidades de éxito en cualquier proyecto. Incluye los temas de Ciclo de Vida del Proyecto, Gestión de la Integración del Proyecto, Gestión del Alcance del Proyecto, Gestión del Tiempo del Proyecto, de los Costos, de la Calidad, de los Recursos Humanos, de las Comunicaciones, Adquisiciones y finalmente lo que nos atañe la Gestión de Riesgos.

A continuación se definirán las áreas de conocimientos según la Guía de los Fundamentos para Dirección de Proyectos (2008) Cuarta edición.

- **Gestión de la Integración del Proyecto:** Incluye los procesos requeridos para asegurarse de que los elementos del proyecto sean coordinados correctamente.

- **Gestión del Alcance del Proyecto:** Consiste en determinar los procesos requeridos para asegurarse de que el proyecto incluya todo el trabajo necesario y sólo el necesario para su culminación exitosa.

- **Gestión del Tiempo del Proyecto:** Área de la gerencia de proyectos que incluye los procesos requeridos para asegurar la terminación oportuna del proyecto.

- **Gestión del Costo del Proyecto:** Un subconjunto de la gerencia de proyectos que incluye los procesos requeridos para asegurarse de que el proyecto se termine dentro del presupuesto aprobado.

- **Gestión de la Calidad del Proyecto:** Incluye los procesos requeridos para asegurarse de que el proyecto satisfaga las necesidades para las cuales fue emprendido.

- **Gestión de los Recursos Humanos del Proyecto:** Un componente de la gerencia de proyectos donde se desarrollan los procesos requeridos para hacer el uso eficaz y eficiente de la gente que participa en el proyecto.

- **Gestión de las Comunicaciones del Proyecto:** Procesos requeridos para asegurar la generación oportuna y apropiada, la recolección, la difusión, el almacenamiento (sistemas informáticos), y la utilización efectiva de la información del proyecto, por todos los actores *Stakeholders*.

- **Gestión de los Riesgos del Proyecto:** Es el proceso sistemático de identificar, de analizar y de responder al riesgo del proyecto. Incluye la maximización de la probabilidad de ocurrencia de acontecimientos positivos y de reducir al mínimo de la probabilidad y las consecuencias de acontecimientos adversos de proyectar objetivos.

- **Gestión de las Adquisiciones del Proyecto:** Corresponde a los procesos para la adquisición de los productos y servicios requeridos por el proyecto, así como el aseguramiento de que dichos productos y servicios se dispondrán en forma oportuna y en las mejores condiciones de suministro o almacenamiento temporal.

El presente trabajo está enfocado sobre la Gestión de Riesgo, en la descripción general de sus procesos.

Marco de Referencia ITIL V3

A continuación se reseña la Librería de Infraestructura de Tecnología de la Información ITIL y el proceso de Gestión de Control de Cambio Tecnológicos inmerso en esté.

Cental Computer and Telecommunications Agency. (1989) es el ente que desarrollo el marco de referencia de la Librería de Infraestructura de Tecnología de la Información (ITIL) y recaba las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información. Es un comprendió de cinco (5) libros de procesos de servicios los cuales son:

- Estrategia
- Diseño
- Transición
- Operaciones
- Mejora Continua del Servicio

Todos estos libros están representados en el gráfico del ciclo de vida del servicio que se presenta a continuación.

Los cinco (5) procesos del ciclo de vida del servicio

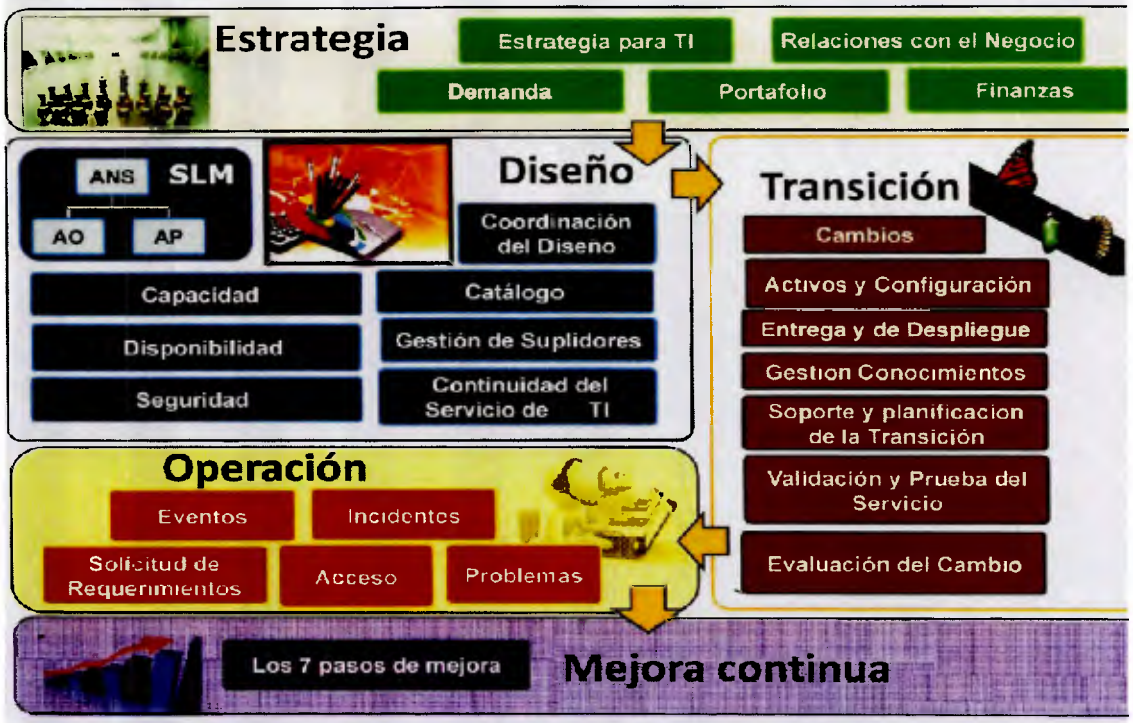


Figura Nro. 1. Los cinco (5) procesos del ciclo de vida del servicio
Fuente: http://www.aitil.com

Dentro de este marco de referencia se detallará la Gestión de Control de Cambio:

El objetivo primordial de la Gestión de Cambios es que se realicen e implementen adecuadamente todos los cambios necesarios en la infraestructura y Servicios TI, garantizando el seguimiento de procedimientos estándar.

La Gestión de Cambios debe trabajar para asegurar que los cambios:

- Están justificados.
- Se llevan a cabo sin perjuicio de la calidad del Servicio TI.
- Están convenientemente registrados, clasificados y documentados.
- Han sido cuidadosamente probados en un entorno de prueba.

- Se ven reflejados en la Base de Datos de Gestión de Configuración (CMDB).
- Pueden deshacerse mediante planes de recuperación en caso de un incorrecto funcionamiento tras su implementación.

A continuación se estable un conjunto de términos que dan apoyo al manejo de la Gestión de Control de Cambio, esto según los Fundamentos de la Gestión de TI en ITIL V3 (2007), los cuales son:

Servicio de TI: Es la vía para generar valor a los clientes/usuarios, apoyándose en obtener sus objetivos de negocios al menor costo riesgo.

Base de Datos de Gestión de Configuración (CMDB): Repositorio usado para almacenar los archivos de Configuración través de su Ciclo de Vida.

Ciclo de Vida: Son las diferentes etapas que ocurren durante la vida de un EC, las cuales se identifican a través del estado.

Elemento de Configuración (EC): Componente de la infraestructura de TI que necesita ser gestionado con el fin de entregar un Servicio de TI.

Solicitud de Control de Cambio: Documento del cambio. Contiene la información acerca del cambio solicitado: qué, quién, cuándo, dónde, por qué y cómo se efectuará el cambio.

Gestor de Cambios: Es el responsable del proceso del cambio y como tal debe ser el último responsable de todas las tareas asignadas a la Gestión de Cambios. En grandes organizaciones el Gestor de Cambios puede disponer de un equipo de asesores específicos para cada una de las diferentes áreas. Sus roles:

- Gestionar la Agenda del Comité de Cambios Tecnológicos (CCT)
- Recibir y revisar RFC´S (*Request for Change* / Solicitudes de Cambios).
- Aprobar Cambios recomendados por el CCT.
- Emitir el cronograma de Cambios.
- Coordinar las Revisiones Post Implementación.
- Cierre de los casos de RFC´s

Comité de Cambios Tecnológicos (CCT): Es un órgano interno, presidido por el Gestor de Cambios, formado principalmente por representantes de las principales áreas de la gestión de servicios TI, así como también, consultores externos, representantes de los colectivos de usuarios y representantes de los principales proveedores de software y hardware.

Sus roles son:

- Evaluar, priorizar y aprobar cambios.
- Incluir representantes de TI y del negocio.
- Reunirse periódicamente

Comité de Cambios Tecnológicos de Emergencia (CCTE): Es un órgano interno, presidio por el Gestor de Cambios, formado principalmente por los representantes del área de gestión de servicio. Su convocatoria es más inmediata

- Evaluar y Aprobar cambios de emergencias de alto riesgo.
- Puede delegar autoridad pero debe ser documentado.

Formularios de Control de Cambio: Documento utilizado para registrar el cambio. Su estructura va a depender del tipo de cambio que se requiera.

Tipos de Controles de cambios:

- **Cambio Estándar:** Son aquellos cambios cotidianos de muy bajo impacto, que no tocan el ambiente de producción y que no son documentados a través de un formulario o solicitud. Como por ejemplo: cambio de mouse de un equipo, instalación de una aplicación en una estación de trabajo de un usuario y en casos más particulares clonaciones o creación de ambientes.
- **Cambio Normal:** Son aquellos que se puede ejecutar bajo las ventanas de cambios establecidas y que siguen el flujo normal establecido para el proceso de Control de Cambio. Este es tratado bajo el formulario de solicitud de cambio normal.
- **Cambios de Emergencia:** Son aquellos que tienen un tratamiento especial debido a la necesidad de sus implantación inmediata, y se generan por la interrupción de un servicio de alto impacto, ya sea por el número de usuarios afectados o porque se han visto involucrados sistemas o servicios críticos para la organización, y se debe de encontrar una respuesta inmediata.
- **Cambios de Alto Impacto:** Son aquellos que se puede ejecutar fuera de las ventanas de cambios establecidas, puesto que no son una emergencia pero tiene un alto impacto sobre el negocio y siguen el flujo normal establecido para el proceso de Control de Cambio. Este también es tratado bajo el formulario de solicitud de cambio normal.

Error conocido: Incidencia con causa conocida.

Incidente: Interrupción no planeada de un Servicio de TI o reducción de calidad de un servicio.

Problema: Incidente sin causa conocida (requiere análisis de causa raíz).

Prioridad: Una categoría usada para identificar la importancia relativa de un Incidente, Problema o Cambio. La prioridad se basa en el impacto y la urgencia que es usada para identificar los tiempos requeridos para que se tome acción.

Plan de Recuperación: plan que documenta todas las acciones que deben tomarse para restaurar el servicio si la implementación de una versión falla total o parcialmente. Los planes alternos pueden contener acciones para una restauración completa del servicio o, en su defecto, para la implementación de planes de contingencia.

Mejores Prácticas: Es un conjunto de estrategias, procesos, procedimientos, actividades y recomendaciones, que al implantarse mejoran la eficacia y eficiencia de un negocio y que han sido probados en diferentes organizaciones, bajo diferentes condiciones y en múltiples oportunidades.
Las mejores prácticas reemplazan:

- El caos con el orden
- Los mejores esfuerzos con calidad fiable.
- Resultados al azar con optimización.

Riesgo

Según el diccionario de la Real Academia Española (RAE):

Riesgo. (del risico o rischio, y éste del ár. clás. rizq, lo que depara la providencia).

1. m. Contingencia o proximidad de un daño.
2. m. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

La Guía del PMBOK (2008) define el riesgo como:

> Un riesgo es un evento o condición incierta que, si sucede, tienen un efecto en por lo menos uno de los objetivos del proyecto. Un riesgo puede tener una o más causas y, si sucede, uno o más impactos. Una causa puede ser un requisito, un supuesto, una restricción o una condición que crea la posibilidad de consecuencias tanto negativas como positivas. (p. 234).

El Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) (2011) define como riesgo *"el efecto de incertidumbre que se tiene sobre el cumplimiento de los objetivos"* (p.18).

Valoración del Riesgo

La valoración del riesgo consta de tres etapas: la identificación, el análisis y la determinación del nivel del riesgo. Estas etapas son de singular interés para desarrollar con éxito la administración del riesgo e implementar una política al respecto; para cada una de ellas se sugiere tener en cuenta la mayor cantidad de datos disponibles y contar con la participación de las

áreas que ejecutan los procesos para lograr que las acciones determinadas alcancen los niveles de efectividad esperados.

Identificación del Riesgo

El proceso de la identificación del riesgo debe ser permanente e interactivo integrado al proceso de planeación y debe partir de la claridad de los objetivos estratégicos de la entidad para la obtención de resultados.

Previa la identificación de los riesgos es importante tener en cuenta tal como se mencionó anteriormente, los factores que pueden incidir en la aparición de los mismos, los cuales pueden ser externos e internos y llegar a afectar la organización en cualquier momento.

Debe considerarse además de los factores previamente citados, factores externos o internos relacionados con la entidad como son: económicos, sociales, de orden público, políticos, legales y cambios tecnológicos, entre otros y como factores internos: la naturaleza de las actividades de la entidad, la estructura organizacional, los sistemas de información, los procesos y procedimientos y los recursos económicos.

Para la identificación se recomienda la aplicación de varias herramientas y técnicas como por ejemplo: entrevistas estructuradas con expertos en el área de interés, reuniones con directivos y con personas de todos los niveles en la entidad, evaluaciones individuales usando cuestionarios, tormentas de ideas con los servidores de la entidad, entrevistas e indagaciones con personas ajenas a la entidad, usar diagramas

de flujo, análisis de escenarios y hacer revisiones periódicas de factores económicos y tecnológicos que puedan afectar la organización, entre otros.

Igualmente pueden utilizarse diferentes fuentes de información de la entidad, tales como registros históricos, experiencias significativas registradas, opiniones de especialistas y expertos, informes de años anteriores, los cuales pueden proporcionar información importante, la técnica utilizada dependerá de las necesidades y naturaleza de la entidad.

Una manera de visualizar los riesgos es a través de la utilización del formato de identificación de riesgos el cual permite hacer un inventario de los mismos, definiendo en primera instancia los riesgos, posteriormente presentando una descripción de cada uno de estos y finalmente definiendo las posibles consecuencias. Es importante centrarse en los riesgos más significativos para la entidad.

Clasificación del Riesgo

Durante el proceso de identificación del riesgo se recomienda hacer una clasificación de los mismos teniendo en cuenta los siguientes conceptos.

- **Riesgo Estratégico:** Se asocia con la forma en que se administra la Entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
- **Riesgos Operativos:** Comprende los riesgos relacionados tanto con la parte operativa como técnica de la entidad, incluye riesgos

provenientes de deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

- **Riesgos de Control:** Están directamente relacionados con inadecuados o inexistentes puntos de control y en otros casos, con puntos de control obsoleto, inoperante o poco efectivo.

- **Riesgos Financieros:** Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, así como su interacción con las demás áreas dependerá en gran parte el éxito o fracaso de toda entidad.

- **Riesgos de Cumplimiento:** Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

- **Riesgos de Tecnología:** Se asocian con la capacidad de la Entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporten el cumplimiento de la misión.

Es importante destacar que para los efectos de las instituciones financieras, el Comité de Supervisión Bancaria de Basilea en la publicación del informe de Convergencia Internacional de Medidas y Normas de Capital Junio (2004), explica que "*existen tres principales tipos de riesgo al que están expuestos los bancos: el de mercado, asociado a las fluctuaciones en*

el precio de los activos; el de crédito, asociado a la incertidumbre en el pago de las obligaciones de los deudores; y el operativo, que está asociado a la posibilidad de error humano, fallas tecnológicas, fraudes y desastres naturales" (p. 156). Para está investigación los riesgos que se evidencian y aplican al área de tecnología, son los riesgos operativos y tecnológicos.

Análisis del Riesgo

El objetivo del análisis es el de establecer una valoración y priorización de los riesgos con base en la información obtenida en el formato de identificación de riesgos elaborados en la etapa de identificación, con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la información sobre el mismo, de su causa y la disponibilidad de datos. Para adelantarlo es necesario diseñar escalas que pueden ser cuantitativas o cualitativas.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

Urgencia: Una medida de cuánto tiempo pasara hasta que un Incidente, Problema o Cambio tenga un impacto significativo en el negocio.

Impacto: Una medida del efecto que tendrá un Incidente, Problema o Cambio en el negocio

A continuación se presentan algunos ejemplos de las escalas que pueden implementarse para analizar los riesgos.

Análisis cualitativo: Se refiere a la utilización de formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de ocurrencia. Se diseñan escalas ajustadas a las circunstancias de acuerdo a las necesidades particulares de cada organización o el concepto particular del riesgo evaluado.

Escala de medida cualitativa de **URGENCIA** se deben establecer las categorías a utilizar y la descripción de cada una de ellas, con el fin de que cada persona que aplique la escala mida a través de ella los mismos ítems, por ejemplo:

ALTA: Es necesario ser atendido inmediatamente.

MEDIA: Es necesario ser atendido con relativa rapidez.

BAJA: Es necesario que se atienda con planificación.

Ese mismo diseño puede aplicarse para la escala de medida cualitativa de **IMPACTO**, estableciendo las categorías y la descripción, por ejemplo:

ALTO: Si el hecho llegara a presentarse, tendría alto impacto o efecto sobre la entidad.

MEDIO: Si el hecho llegara a presentarse tendría medio impacto o efecto en la entidad.

BAJO: Si el hecho llegara a presentarse tendría bajo impacto o efecto en la entidad.

Análisis cuantitativo: Este análisis contempla valores numéricos para los cuales se pueden construir tablas; la calidad depende de lo exactas y completas que estén las cifras utilizadas. La forma en la cual la probabilidad

y el impacto son expresada y las formas por las cuales ellos se combinan para proveer el nivel de riesgo puede variar de acuerdo al tipo de riesgo.

Al igual que para determinar las escalas cualitativas, el diseño de las escalas cuantitativas debe contar con la participación de las personas encargadas de los procesos y con el grupo encargado de liderar la administración del riesgo.

Priorización de los Riesgos

Una vez realizado el análisis de los riesgos con base en los aspectos de urgencia e impacto, se recomienda utilizar la matriz de priorización que permite determinar cuáles requieren de un tratamiento inmediato.

Asignación de Prioridades

Asignación de Prioridades

La **Prioridad** es definida por el **impacto** del negocio y la **urgencia** necesitada

Urgencia	Impacto: ALTO	Impacto: MEDIO	Impacto: BAJO
ALTA	1	2	3
MEDIA	2	3	4
BAJA	3	4	5

Priodidad	Descripción	Solución Esperada
1	Crítica	1 Hora
2	Alta	8 Horas
3	Media	24 Horas
4	Baja	48 Horas
5	Planificación	Plan/Proyecto

Figura Nro. 2. Asignación de Prioridades
Fuente: http://www.aitil.com

Cuando se ubican los riesgos en la matriz, se define cuáles de ellos requieren acciones inmediatas o simplemente pueden tener una holgura de ejecución tipo proyecto.

Para utilizar esta tabla es necesario ubicarse en el nivel de **Urgencia** representado con categorías de **ALTO, MEDIO, BAJO** y desplazarse hacia el **Impacto** ya determinado con **ALTO, MEDIO, BAJO**, esto conllevara a la identificación de una **Prioridad** reflejada en caracteres numéricos del **UNO** (1) al **CINCO** (5) siendo el número uno la prioridad más alta e inmediata con un espectro de respuesta y solución no mayor a una hora, por ende el número cinco está dado por una inmediatez de respuesta más amplia, y puede estar representado con una planificación tipo proyecto.

Consideración de Acciones

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender las cuales deben ser factibles y efectivas, tales como: la implementación de políticas, definición de estándares, optimización de procesos y procedimientos y cambios en software y/o hardware, entre otros.

Se pueden tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

Evitar el riesgo: Es siempre la primera alternativa a considerar. Se logra cuando en el interior de los procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, entre otros.

Reducir el riesgo: Si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.

Dispersar y atomizar el riesgo: Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

Transferir el riesgo: Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros, proveedores externos, esta técnica es usada para eliminar el riesgo de un lugar y pasarlo a otro o de un grupo a otro. Así mismo, el riesgo puede ser minimizado compartiéndolo con otro grupo o dependencia.

Asumir el riesgo: Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidas cuales de las anteriores opciones de manejo del riesgo se van a concretar, estas deben evaluarse con relación al beneficio-costo para proceder a elaborar el mapa de riesgos, el cual permitirá visualizar todo el proceso de valoración, análisis y manejo de los riesgos.

CAPÍTULO III

MARCO METODOLÓGICO

Este capítulo tiene como finalidad describir el marco metodológico establecido por el investigador para el desarrollo del presente proyecto de Trabajo Especial de Grado, considerando la formulación del problema y la definición de sus objetivos. Se describe el tipo y diseño de la investigación, población, muestra, unidades de análisis, técnicas e instrumentos de recopilación de información y el procedimiento empleado.

Tipo de Investigación

La presente investigación tuvo orientada a desarrollar una propuesta de modelo de gestión viable, para satisfacer necesidades y generar un producto de utilidad que contribuya a gestionar los riesgos en el proyecto "Herramienta para Minimizar el Riesgo Tecnológico en el Proceso "Control de Cambios" en el Banco de Desarrollo Económico y Social de Venezuela (Bandes)". En tal sentido, el estudio se enmarcó como Investigación Aplicada, que de acuerdo con la clasificación propuesta por Yáber y Valarino (2003) para investigaciones de Postgrado en Gerencia, específicamente en la disciplina de Gestión de Empresas, relacionadas con su propósito, el tipo de problema que abordan y, definiendo los verbos y la acción que realizan, este trabajo se clasifica como una Investigación y Desarrollo, ya que "*tiene como propósito indagar sobre necesidades del ambiente interno o externo de una organización, para luego desarrollar un producto o servicio que pueda aplicarse en la organización o dirección de una empresa o de un mercado*" (p. 9).

Por la antes expuestos, este enfoque de investigación conviene para ser aplica metodológicamente a la problemática actual de Gerencia Ejecutiva de Tecnología de a información, ya que existe una necesidad organizacional de una propuesta para solucionar la problemática expuesta en el capítulo I.

Además se obtendrá un resultado, el cual será un modelo de herramienta que permitirá la identificación y análisis de los posibles riesgos que se pueden presentar ante la ejecución de un cambio en la plataforma tecnológica de BANDES.

Diseño de la Investigación

Arias, Fidias (2006) define al diseño de la investigación como "La estrategia general que adopta el investigador para responder al problema planteado. En atención al diseño, la investigación se clasifica en: documental, de campo y experimental" (p. 24).

El presente estudio, se realizó para diseñar una herramienta que permita identificar, analizar y minimizar los riesgos tecnológicos en el proceso de Control de Cambio, para ello se llevó a cabo una investigación de campo, y se analizó una situación determinada en un momento dado del flujo de la gestión de cambio. En tal sentido, según lo describe Balestrini (2006), "*los diseños de campo permiten establecer una interacción entre los objetivos y la realidad de la situación de campo; observar y recolectar los datos directamente de la realidad, en su situación natural* "(p. 132).

A su vez, estos diseños de campo se pueden clasificar en diseños experimentales o no experimentales. Para el caso que ocupa en esta investigación, el diseño de campo es de carácter no experimental,

clasificación dentro de la cual se pueden citar las investigaciones descriptivas, exploratorias, evaluativas e incluso los proyectos factibles; donde según Balestrini (2006), *"se observan los hechos estudiados tal como se manifiestan en su ambiente natural, y en ese sentido, no se manipulan de manera intencional las variables*" (p. 132).

En este tipo de investigación se dividen en experimental y no experimental; la primera incluye la manipulación de variables sometiendo a pruebas a una muestra y observar los cambios en este. La investigación no experimental, puede clasificarse de acuerdo a la dimensión temporal en la cual se elabora el trabajo de investigación.

Hay dos tipos de diseños: diseños transversales y longitudinales. Los Diseños Transversales son los que implican la recolección de datos en un solo corte en el tiempo. El presente estudio corresponde a una investigación no experimental transversal ya que se analiza la situación actual en el ahora, tomando en cuenta las referencia previas, para proponer sus mejoras.

Unidad de Análisis

Para el presente estudio es la Oficina de Requerimiento y Planificación Tecnológica (ORPT), unidad que administra el proceso "Control de Cambios", y que impacta directamente sobre los riesgos latentes que pudiesen manifestarse al momento de realizar modificaciones o alteraciones a la plataforma tecnológica de la institución.

La población objeto del estudio, estuvo delimitada por las actividades del proceso "Control de Cambios Tecnológicos" y toda la documentación asociada, que se genera por la demanda de cambios.

Técnicas e Instrumentos de Recolección de Datos

Para Fidias, Arias (2006) se entiende por técnica "*el procedimiento o forma particular de obtener datos o información*" y por instrumento "*un dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información*". (p. 67). En este sentido y con la finalidad de cumplir con los objetivos planteados en esta investigación; así como lograr datos reales y confiables, además de una buena recolección de datos se hace necesaria la aplicación de ciertas herramientas clásicas para la recolección inicial de los datos o información.

Como técnicas se utilizaron la observación directa, consulta de datos históricos y entrevistas no estructuradas y como instrumento se utilizará la hoja de cálculo para el procesamiento de datos. El proceso de recolección de datos inicia con la observación directa del proceso y la recolección de datos a través de los Formularios de Control de Cambio, posteriormente se realizarán entrevistas no estructuras con la finalidad de conocer las actividades realizadas por los involucrados, así como también la revisión de las base de datos y trazas histórica de los controles de cambio ejecutados; a fin de identificar aquellos ejecutados sin éxitos, con plan de recuperación implantados y todos aquellos que reflejaron fallas; luego se identificara y/o clasificara la información para determinar cuál de ella puede ser útil en el desarrollo de la investigación.

Técnicas para el Procesamiento y Análisis de los Datos

Indican la forma como manipular los datos recolectados, a través de los instrumentos mencionados; para ello se divide de forma cuantitativamente y cualitativamente.

- **Técnicas Cuantitativas:** Para Hernández Fernández y Baptista (2003) "Es un técnica de recolección de datos que consiste en el registro, sistemático de datos e información que presentan las características de ser válido y confiable" (p.117), lo cual para el presente estudio permitirá exponer con base las propuestas de mejoras.
- **Técnicas Cualitativas:** Arrojarán la descripción de la información correspondiente con la situación actual, debido a que el resultado es emplear las técnicas como entrevistas no estructuradas, observaciones en el área.

Operacionalización de los Objetivos

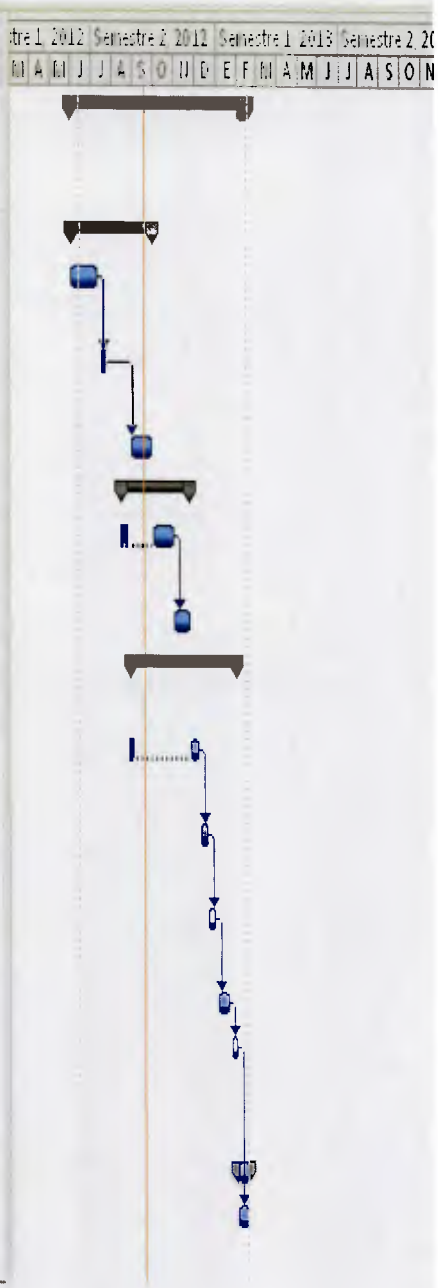
A continuación se presenta una tabla la cual resume la operacionalización de los objetivos de este trabajo de investigación.

Tabla Nro.1. Cuadro de Operacionalización de los Objetivo

OBJETIVOS ESPECIFICOS	VARIABLES	DEFINICIÓN	INDICADOR	TECNICA
Diagnosticar la situación actual del proceso de control de cambio a fin de determinar los riesgos tecnológicos.	Indicadores de Gestión de Desempeño del Proceso Informe de Gestión Mensual	De acuerdo al análisis de la situación actual, se obtendrá una visión exacta de la problemática que se origina por no contar con un análisis de entorno y variables, que incurren en errores o incidentes, repercutiendo en la interrupción del servicio tecnológico, y por ende producen daños al negocio.	• Nro. de controles de cambios no exitoso. • Nro. de aplicaciones críticas para el negocio. • Nro. de controles de cambios con *rollback*. • Nro. de aplicaciones con desarrolla más complejo.	• Observación directa. • Consulta de datos históricos. • Entrevistas no estructuradas.
Describir los elementos relacionados con el riesgo tecnológico, en base al marco referencial *Information Technology Infraestructure Library* (ITIL) en Bandes.		Identificar cada uno de los elementos tecnológicos que conforma la plataforma de TI de la GETI, a fin de determinar su comportamiento ante situaciones de cambios, y estructurar los posibles riesgos que pudieran sufrir estos. Los elementos son aquellos conformados por software y hardware y permitirán elaborar un esquema organizado y más visual de los activos de TI.	• Nro. de elementos o variable afectados por controles de cambios. • Base de datos de conocimientos.	• Grupos de discusión. • Entrevistas no estructuradas. • Revisión de bibliografía.
Determinar los niveles de riesgos para el proceso de control de cambio.		Determinar el manejo de los riesgos, de tal forma que puedan ubicarse en una escala cuantitativa, y a su vez está arroje un nivel de riesgo que se manifieste desde el más alto al más bajo en forma jerárquica, lo cual permitirá establecer prioridades y capacidades de respuestas y soluciones.	• Nro. de controles de cambios con *rollback*. • Niveles establecidos en las metodologías de consulta.	• Revisión de bibliografía. • Entrevistas no estructuradas.
Diseñar la herramienta de riesgos en el proceso de control de cambios tecnológicos para el Banco de Desarrollo Económico y Social de Venezuela (BANDES)		Una vez establecidos los elementos, variables y niveles de riesgos que se ven afectados por el proceso de control de cambio, es indispensable plasmar de forma sistemática esta información, de forma tal que exista un mapa de riesgos y soluciones ante cualquier eventualidad.	• Nro. de controles de cambios con proceso de inicio y fin exitoso.	• Riesgos determinados. • Grupos de discusión.

Figura Nro. 3. Cronograma de Actividades

	Nombre de tarea	Duración	Comienzo	Fin	Predec.
1	**Herramienta para minimizar el riesgo tecnológico en el proceso de control de cambios**	186 días	vie 01/06/12	vie 15/02/13	
2	**Diagnóstico de la situación actual**	**86 días**	**vie 01/06/12**	**vie 28/09/12**	
3	Identificar la poblacion de controles de cambio	27 días	vie 01/06/12	lun 09/07/12	
4	Analizar controles de cambios identificados para identificar los fallidos	1 día	vie 20/07/12	vie 20/07/12	3
5	Identificar las causas	23 días	mié 29/08/12	vie 28/09/12	4
6	**Análisis de los riesgos tecnológicos**	**71 días**	**jue 16/08/12**	**jue 22/11/12**	
7	Identificar cómo las causas afectaron las aplicaciones criticas	25 días	jue 16/08/12	mié 31/10/12	
8	Identificar EC afectados	16 días	jue 01/11/12	jue 22/11/12	7
9	**Determinación de los niveles de riesgos para el proceso de control de cambio en Bandes**	112 días	mar 28/08/12	**mié 30/01/13**	
10	Establecer impacto para cada control de cambio	12 días	mar 28/08/12	mié 05/12/12	
11	Establecer urgencia para cada control de cambio	8 días	vie 07/12/12	mar 18/12/12	10
12	Determinar prioridad de cada control de cambio	8 días	mié 19/12/12	vie 28/12/12	11
13	Identificar la prioridad y urgencia	12 días	mie 02/01/13	jue 17/01/13	12
14	Establecer rangos para aprobacion de controles de cambios con base en los riesgos	8 días	lun 21/01/13	mié 30/01/13	13
15	**Construir Matriz**	**12 días**	**jue 31/01/13**	**vie 15/02/13**	
16	Incorporar todos los factores de riesgos	12 días	jue 31/01/13	vie 15/02/13	14



Consideraciones Éticas

Las consideraciones éticas y legales parten de que ambos términos están vinculados al código de conducta o al sistema de principios morales que el individuo posee, los cuales rigen o guían su actuación durante la ejecución de actividades y manipulación de la información.

Para éste TEG, en vista de que se manejará información confidencial sobre los sistema aplicaciones que conforman los servicios que brinda la GETI al Banco de Desarrollo Económico y Social de Venezuela (BANDES) asociada a procedimientos de funciones internas, documentación relacionada con información tecnológica, y otro tipo de información considerada como "sensible" para el Banco, se deben seguir las premisas establecidas por el Código de Ética del Banco de Desarrollo Económico y Social de Venezuela (2011, p. 3), el cual tiene como objeto "Definir las directrices a cumplir y constituye un conjunto general de normas y estándares de conducta deseados, con fundamento en los valores que junto a los principios y valores del Banco, se han incorporado a la cultura del Instituto".

Así mismo, en base al Código de Ética y Conducta Profesional del PMI, se tomaron en cuenta las siguientes consideraciones:

Del capítulo 2. Responsabilidad

- Únicamente aceptamos aquellas asignaciones que se condicen con nuestros antecedentes, experiencia, habilidades y preparación profesional.
- Cumplimos los compromisos que asumimos: hacemos lo que decimos que vamos a hacer.

- Cuando cometemos errores u omisiones, nos responsabilizamos por ellos y los corregimos de inmediato.
- Cuando descubrimos errores u omisiones realizados por terceros, los comunicamos de inmediato al organismo pertinente.
- Nos hacemos responsables por cualquier problema que se origine a raíz de nuestros errores u omisiones, y de las consecuencias que de ellos resulten.
- Protegemos la información confidencial o de propiedad exclusiva que se nos haya confiado.
- Nos informamos acerca de las políticas, reglas, normativas y leyes que rigen nuestras actividades laborales, profesionales y voluntarias, y las respetamos.

Capítulo 3. Respeto

- Nos informamos sobre las normas y costumbres de los demás, y evitamos involucrarnos en comportamientos que ellos podrían considerar irrespetuosos.

Capítulo 4. Equidad

- Demostramos transparencia en nuestro proceso de toma de decisiones.
- Revisamos constantemente nuestros criterios de imparcialidad y objetividad, y realizamos las acciones correctivas pertinentes.
- Brindamos acceso equitativo a la información a quienes están autorizados a contar con dicha información.

Capítulo 5. Honestidad

- Proporcionamos información precisa de manera oportuna.
- No nos involucramos ni aprobamos comportamientos tendientes a engañar a terceros, entre ellos, realizar declaraciones falsas o engañosas, decir verdades a medias, proporcionar información fuera de contexto o retener información que, si se conociera, convertiría nuestras declaraciones en engañosas o incompletas.
- No nos involucramos en comportamientos deshonestos para beneficio personal ni a costa de terceros. PMI (2008).

CAPÍTULO IV

MARCO ORGANZACIONAL

Contexto Organizacional

El Ejecutivo Nacional crea el Banco de Desarrollo Económico y Social de Venezuela (Bandes) mediante el proceso de transformación del Fondo de Inversiones de Venezuela (FIV), publicado en la Oficial de la República Bolivariana de Venezuela N° 37.194, del 10 de mayo de 2001 y reimpreso en la Gaceta Oficial N° 37.228, del 27 de junio de 2001.

Bandes en un Instituto Autónomo adscrito al Ministerio del Poder Popular de Planificación y Finanzas, el cual actúa como agente financiero del Estado, para atender proyectos orientados hacia la desconcentración económica, estimulando la inversión privada en zonas deprimidas y bajo rendimiento, apoyando financieramente proyectos especiales de desarrollo regional.

Está facultado para ser el ente fiduciario de organismos del sector público, apoyando técnica y financieramente la expansión y diversificación de la infraestructura social y productiva de los sectores prioritarios, a fin de contribuir con el desarrollo equilibrado de las distintas regiones del país, e igualmente para administrar los acuerdos financieros internacionales.

Dentro del Sistema Financiero Público Nacional, el Bandes se convierte en líder al desarrollar su integración, con participación accionaria en la banca del Estado, con el fin de ampliar sus capacidades y apalancar el apoyo financiero al pueblo venezolano.

Respecto al ámbito internacional, el Bandes realiza operaciones de financiamiento internacional con recursos propios o provenientes de terceros, participa en programas bilaterales y cualquier otro acuerdo financiero internacional que establezca el Ejecutivo Nacional, siempre dirigido al bienestar de los pueblos, en el marco de las políticas de Cooperación Internacional para promover la multipolaridad.

Misión

Somos el Banco dirigido a promover el desarrollo económico y social a través del apoyo técnico y financiero a la inversión social y productiva en el ámbito nacional e internacional, bajo los principios de justicia, equidad y solidaridad.

Visión

Ser el Banco de desarrollo líder de la inversión social y productiva, modelo en calidad de servicio y talento humano orientado a la excelencia.

Valores Institucionales

- Honestidad.
- Humildad y sencillez.
- Lealtad.
- Solidaridad.
- Respeto.

- Compromiso.
- Transparencia.
- Responsabilidad.
- Cooperación.

Estructura Organizativa

Figura Nº 4. Estructura Organizativa del Bandes
Fuente: http://www.bandes.gob.ve. (2008)

La estructura organizativa del Bandes está conformada por cuatro ejes básicos: dirección, control y medición, gestión de recursos y apoyo al desarrollo.

La Oficina de Requerimiento y Planificación Tecnológica (ORPT)

La ORPT es encargada de gestionar todos los cambios que involucran un pase o modificación del ambiente de producción, asegurando que éstos sean registrados y documentados para reducir los incidentes y minimizar los riesgos.

El control de cambio se origina en el momento en que se recibe el requerimiento en la Gerencia Ejecutiva de Tecnología de la Información, enviado por la unidad solicitante. Excepto en aquellos casos como mejoras a un servicio existente o nueva implementación, donde el solicitante es la Gerencia Ejecutiva de Tecnología de la Información.

Objetivo

Supervisar y apoyar la gestión de los requerimientos solicitados a la Gerencia Ejecutiva de Tecnología de la Información, con el objetivo de servir de enlace con la OGP de la institución y a su vez, garantizar la atención y ejecución oportuna de dichas solicitudes por parte de todos los supervisores y gerentes de la Gerencia Ejecutiva, de acuerdo al Plan Estratégico definido en el período.

Organigrama de la Oficina de Requerimiento y Planificación Tecnológica (ORPT)

Figura Nro. 5. Ubicación de la ORPT como Unidad Funcional Dentro de la Estructura Organizativa del Bandes
Fuente: http://www.bandes.gob.ve (2009)

CAPÍTULO V

PRESENTACIÓN Y ANÁLISIS DE LOS RESULTADOS

A continuación se presentan, analizan e interpretan los datos obtenidos en la presente investigación, mediante la aplicación de las técnicas e instrumentos explicados en el apartado correspondiente al Capítulo II: Marco Metodológico.

Para Kerlinger (1981) citado por Hurtado, J. (1998) "analizar significa establecer categorías, ordenar, resumir e interpretar los datos" (p. 171). En el mismo orden de ideas, Seltiz, C. y Otros (1976) citado por Balestrini, M. (2002) explican:

> "...el propósito del análisis es resumir las observaciones llevadas a cabo de forma tal que proporcionen respuestas a las interrogantes de la investigación. El análisis implica el establecimiento de categorías, la ordenación y manipulación de los datos para resumirlos y poder sacar algunos resultados en función de las interrogantes de la investigación. Este proceso tiene como fin último, el de reducir los datos de una manera comprensible, para poder interpretarlos, y poner a prueba algunas relaciones de los problemas estudiados..." (p. 169).
>
> En todo caso, el análisis e interpretación de los datos se convierte en la fase de la aplicación de la lógica deductiva e inductiva en el desarrollo de la investigación. Para esta estrategia, los datos, según sus partes constitutivas, se clasifican, agrupándolos, dividiéndolos y subdividiéndolos atendiendo a sus características y posibilidades, para posteriormente reunirlos y establecer la relación que existe entre ellos, a fin de dar respuestas a las preguntas de investigación "(p 170).

A continuación se presentan de acuerdo a los conceptos señalados y los datos recabados, las respuestas a los objetivos de la investigación.

Desarrollo del Objetivo Específico Nro. 1

Diagnosticar la situación actual del proceso de control de cambio a fin de determinar los riesgos tecnológicos.

Todo proceso cuenta con unas características principales como lo son las entradas, actividades y salidas, para ello se detalla la información que alimenta la Gestión de Control de Cambio, objeto de estudio, la cual se presenta en la figura a continuación.

Figura Nro. 6. Entradas - Actividades – Salidas del Proceso de Control de Cambio

Fuente: Flujo de Proceso de Control de Cambio

Dentro de las actividades presentadas en la figura Nro. 6, se encuentra el análisis y evaluación de la factibilidad, que no es más que el diagnostico medular para la aprobación, rechazo o postergación de una solicitud de control de cambio. Es decir a través del resultado que arroje esta actividad, se determinará la factibilidad de la ejecución del cambio.

Dentro de esta actividad de análisis y factibilidad, se encuentra la priorización de la solicitud de control de cambio, para ello es necesario conocer su impacto y urgencia, fase que invita a visualizar el panorama a través de datos históricos, de aquellas aplicaciones o elementos de configuración con índice elevado de ocurrencia a errores por cambios ejecutados, a fin de determinar cuál será la probabilidad y afectación al negocio por los procesos automatizado que estas aplicaciones realizan.

De igual forma para conocer el impacto es preciso determinar la cantidad de controles de cambo fallidos e identificar si la aplicación o servicio está identificado como crítico.

A continuación se presentan la cantidad de controles de cambios ejecutados en el período 2010-2012, a fin de identificar aquellas aplicaciones que sufren modificaciones con más frecuencia e identificarlas como críticas, por ser más vulnerables a cambios.

Tabla Nro. 2. Controles de Cambios Ejecutados.

Aplicaciones	Cantidad
Base de Datos Oracle	7
LDAD	1
Rcppe	1
Switch	2
Active Directory	3
Adobe Flash Player	1
Almacenamuiento IBM DS 8300	1
Aplicaciones Web	6
POA	2
Call Manager	3
Carpetas Compartidas	1
Catalyst	2
Claves Telegráficas	3
Colectores Sentinel	1
Controladores de Dominio	2
Discover	2
Dominio Bandes	1
FAS	14
Firmware	5
Gateway	1
GEBOS	87
IDM	3
Internet Exploret	1
Java	2
Metroethernet	1
Mozilla Firefox	1
Nagios	1
Oracle Financials	13
Ossec	2
PPL Bandes	3
PPL-Sidor	6
Rcppe	5
Reportes Oracle	13
Router	1
RT	3
Safpoa	3
Servidor de Intranet	1

.../...

Aplicaciones	Cantidad
Servidor Lotus	1
SISCOPRO	6
Sistema de Atención al Ciudadano	1
Sistema de Ayuda Social	5
Sistema de Encuestas	1
Sistema de Estacionamiento	1
Sistema de Evaluación	17
Sistema de Formulación Presupuestaria	15
Sistema de Notaria	3
Sistema de Servicio Médico	1
Sistema de Vivienda y Vehículo	28
Sistema Egresados RRHH	1
Sistema fuerte	1
Sistema LA	114
Sistema para Consulta Microcréditos	1
Socredit	3
Switch	6
Tiaca	36
VLAN	2
Total	**448**

Fuente: ORPT. Estadísticas Mensuales de Controles de Cambios (2012)

Tendencia

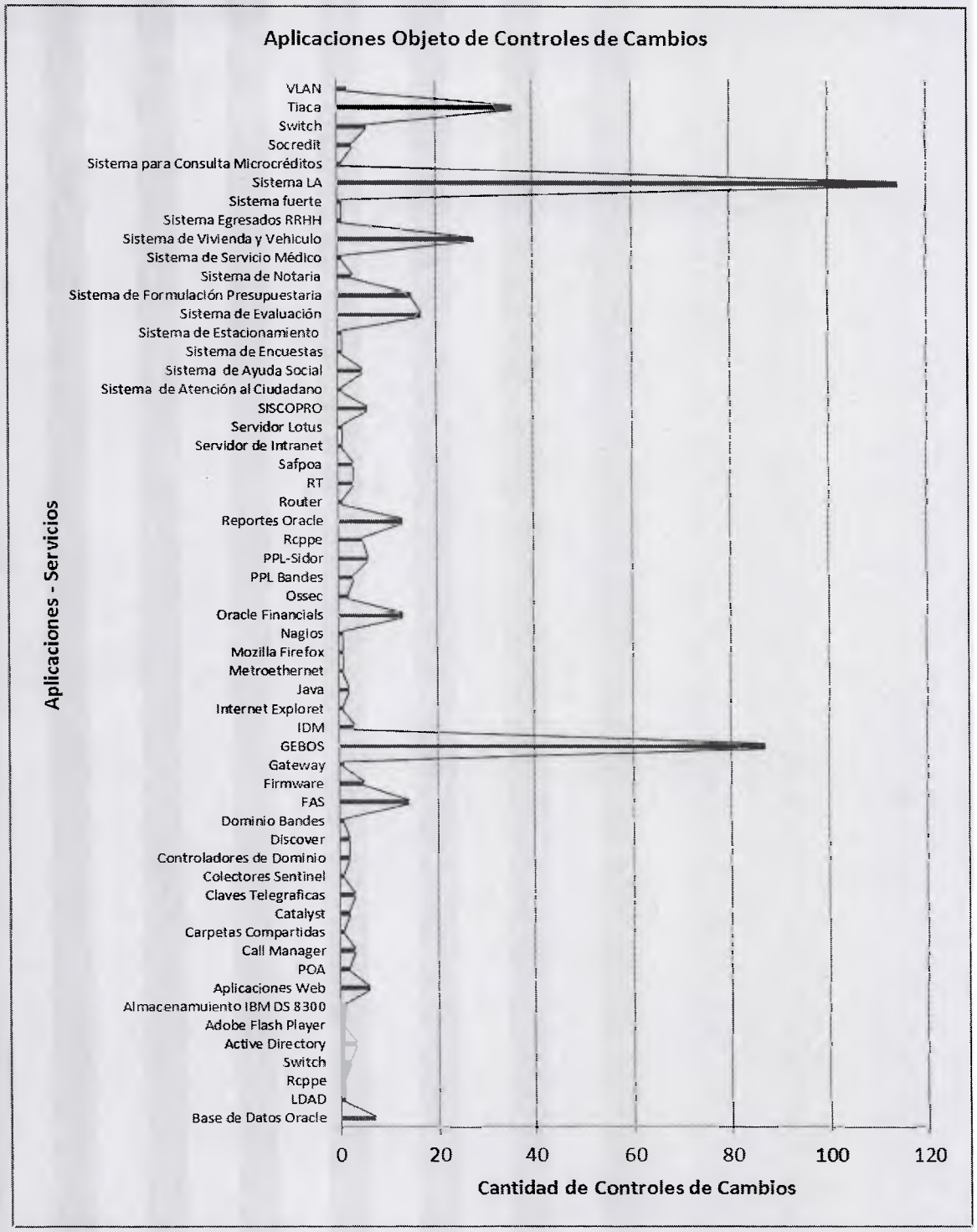


Gráfico Nro. 1. Aplicaciones o Elementos de Configuración con mayor índice de cambios.
Fuente: Estadísticas Mensuales de Controles de Cambios.

El gráfico Nro. 1, muestra los picos con el mayor índice de recurrencia de controles de cambios por aplicación o elemento de configuración, tanto como para aplicar soluciones de errores conocidos, solventar incidencias, o para implantar mejoras.

Se evidencia una tendencia mayor para el Sistema LA sobre cualquier otra aplicación objeto de cambio, así como también para el Sistema de Plan de Financiamiento de Vivienda , Vehículo y Remodelación , Sistema de Evaluación , Sistema de Crédito y Cobranza (Gebos), y en menor cantidad para el Sistema del Fondo Autoadministrado de Salud (FAS),Reportes Oracle y por último Oracle Financials.

En el gráfico se visualizan aplicaciones que no presentan mayor índice de ocurrencia, pero su inesperada suspensión o falla ocasionará, en algunos casos, la falta de continuidad de muchos servicios, debido a que son estos los que sustentan la disponibilidad de otras aplicaciones, el cual es el caso de los elementos de configuración.

Entre los sistemas y/o aplicaciones críticos de infraestructura objeto de cambios que se observan en el gráfico Nro. 1, se encuentran:

- LA Sistemas
- Sistema de Evaluación
- Plan de Financiamiento de Vivienda, Vehículo y Remodelación
- Sistema de Crédito y Cobranza (GEBOS)
- TIACA

- Reportes Oracle
- Oracle Financials

Funcionalidad de los Sistemas Establecidos como Críticos

LA Sistemas: Por ser un banco de inversiones, existen empresas que se apoyan en BANDES para la gestión de sus contratos de fideicomisos, y es allí donde se generan parte de las ganancias de la institución, debido a que se percibe comisiones por la administración de los fondos de dicho contratos. La Suite de LA Sistema es la encargada de procesar todos los tipos de transacciones entorno a los contratos.

Sistema de Evaluación: Es el sistema en donde se cargan los Objetivos de Desempeño Individuales (ODIS), y es a través de estos donde se mide el desenvolvimiento de los funcionarios por cada semestre del año. Este desempeño está ligado una retribución monetaria dependiendo del nivel que cubra el funcionario.

Plan de Financiamiento de Vivienda, Vehículo y Remodelación: Es el sistema encargado de calcular en base al sueldo mensual las tablas de amortización del monto del préstamo asignado para cada funcionario de la institución.

Sistema de Crédito y Cobranza (GEBOS): Es el sistema encargado de gestionar tanto el proceso de liquidación como de cobranza de un crédito asignado, atendiendo a cada una de las modalidades que se puedan presentar en aras de automatizar el movimiento de la cartera del banco.

TIACA: Sistema de Gestión de Recursos Humanos sobre el proceso de nómina y movimiento de los funcionarios en la estructura organizativa.

Reportes Oracle: Sistema encargado de gestionar los reportes necesarios de los procesos administrativos (recibo de pago, cheques, compras).

Oracle Financials: Gestiona los módulos de pago (desembolsos, compras), contabilidad y presupuesto de la institución.

Tabla Nro. 3. Controles de Cambios Fallidos
Requirieron Rollback o Generaron otros Controles de Cambios

Controles de Cambio Fallidos						
Mes	2010	Sistemas	2011	Sistemas	2012	Sistemas
Enero	0		1/5	LA Sistema	0	
Febrero	0		0		0	
Marzo	0		0		0	
Abril	0		0		1/11	Gebos
Mayo	0		1/13	TIACA	1/13	Formulación presupuestaria
Junio	0		1/21	Gebos	0	
Julio	0		0		1/41	Gebos
Agosto	0		0		0	
Septiembre	1/10	Claves Telegráficas	1/13	LA Sistema	0	
Octubre	0		0		0	
Noviembre	0		0		0	
Diciembre	0		0		0	

Fuente: Estadísticas Anuales de Controles de Cambios.

La tabla Nro. 3, muestra aquellos controles de cambios que presentaron fallas en el período 2010-2012, las aplicaciones en color rojo son aquellas establecidas como críticas y las de color amarillo son aquella que presentaron menor estadística y no son críticas, según los resultados arrojados que se muestran en gráfica Nro. 1 de Tendencia, anteriormente presentada.

Estos datos aparentan una pequeña muestra en cuanto a la proporción de controles de cambios ejecutados y los fallidos, sin embargo hay que tener en cuenta que la mayoría de las aplicaciones que presentaron fallas en la liberación del cambio son aquellas identificadas como críticas para el negocio y que pusieron en riesgo la continuidad del servicio.

Tomando en cuenta la premisa fundamental del marco de referencia ITIL, que no es más que mejorar el rendimiento de las empresas con un máximo de eficacia y eficiencia, esta pequeña muestra tendría que reducirse entre 1 y 2 %, a fin contar con un proceso que garantice el mínimo de riesgo en liberación de cualquier cambio y más aún para aquellas aplicaciones críticas.

Se evidencia entonces la existencia de la problemática en el proceso actual de Gestión de Control Cambio, y se visualiza la magnitud de las consecuencias que ocasiona la no identificación oportuna de los riesgos, y como éstos pueden afectar al negocio, comprometiendo el desempeño del manejo de los procesos que administra la Gerencia Ejecutiva de Tecnología de la Información ante la alta gerencia y cuestionando la calidad del servicio que se presta.

Desarrollo del Objetivo Específico Nro. 2

Describir los elementos relacionados con el riesgo tecnológico, en base al marco referencial Information Technology Infraestructure Library (ITIL) en Bandes.

Una vez identificadas aquellas aplicaciones críticas para el negocio, es necesario conocer un poco más, sobre los elementos de configuración que hacen parte de ellas, y que en gran medida su funcionamiento se puede ver se afectado por el desempeño de estos.

Hay que considerar la envergadura y transcendencia de estos componentes, para poder obtener un panorama más amplio de los efectos o consecuencias que se pueden presentarse en caso de falla, como resultado de una modificación o cambio en la aplicación o viceversa de un elemento que afecta alguna aplicación.

Entre los Elementos de Configuración administrados por la Gerencia de Infraestructura y Servicios Tecnológicos, se encuentran: (Ver tabla Nro. a continuación):

Tabla Nro. 4. Elementos de Configuración

Elemento de Configuración	Funcionamiento	Ocasiona
Active Directory	Autenticar y autorizar el ingreso del personal a los sistema que estén integrado con esté. Aprox. 60 % de las aplicaciones.	La autenticación centraliza, en caso de falla no hay ingreso a ninguna aplicación, ya que no valida y niega el acceso a las aplicaciones.
LDAP	Autenticar y autorizar el ingreso del personal a los sistema que estén integrado con esté. Aprox. 38 % de las aplicaciones. Es de plataforma libre.	La autenticación centraliza, si falla no hay ingreso a ninguna aplicación, ya que no valida y niega el acceso.
Servidor web	Acceso directo a la Información corporativa	Página web del Banco y aplicaciones que son ingresadas por esta vía.
Servidor Catalyst	Aloja las aplicaciones de que se encuentran en el portal de aplicaciones (Sistema de Notaría, Sistema de Encuestas, Sistema de Financiamiento de Vivienda y Vehículo, Recibo de Pago, entre otras.	Indisponibilidad de las aplicaciones que son ingresadas por el portal de aplicaciones.
DNS	Convierte los nombres de los host a direcciones de red.	No se pueden resolver los nombres a direcciones de red. Es la base de la conectividad de la institución.
DHCP	Asigna dinámicamente las direcciones de red.	Eventualmente las estaciones de trabajo dejan de recibir las direcciones IP para comunicarse con los servidores.
Correo	Sistema de mensajería electrónica.	Evita la salida de los correo dentro y fuera de la institución.
Antivirus	Centralización del despliegue, alertas, y actualización del sistema de antivirus.	Sistemas vulnerables a ataques.
Virtualizador	Abstrae el particionamiento lógico de los recursos de procesamiento y clústerización el hardware.	Los servicios están corriendo sobre él dejan de funcionar.

.../...

Elemento de Configuración	Funcionamiento	Ocasiona
Bases de datos en producción (Entre 25 bases de datos y esquemas de batos)	Administra, gestiona, controla, recupera, actualiza y optimiza el manejo de la información confidencial de la institución.	Detiene la operatividad del negocio, dependiendo de la base de data afectada y la criticidad del sistema.
Infraestructura de almacenamiento primario y de respaldo y recuperación	**Almacenamiento:** Entorno donde se encuentra el espacio disponible para que puedan operar los diferentes servidores que componen la infraestructura tecnológica de Bandes. **Respaldo:** Resguardo por períodos con frecuencia asociada a una retención, de la infraestructura de tecnología de la información.	No hay disponibles de datos que manejan los sistemas (base de datos, aplicaciones, servidores en producción, pruebas, calidad.
Carpetas compartidas	Punto de almacenamiento para compartir la información que manejan las diferentes áreas del Banco.	Falla el acceso a los documentos que se encuentran en los espacios compartidos.
Central Telefónica (Call Manager)	Direcciona y administra las conexiones de voz y datos de la institución (voz sobre IP).	Interrupción de los servicios de llamadas y Fax.
Corta Fuego	Limita el acceso a partes de red según políticas establecidas.	Bloquea el acceso a las zonas de red donde interviene.
Conectividad de Redes	Gestiona el acceso a la red de internet, red local y sedes alternas (centro alterno de datos, Bandes Uruguay y Nicaragua).	Ocasiona el aislamiento.

Fuente: Información suministrada por el Área de Infraestructura perteneciente a la Gerencia de Tecnología de la Información.

Desarrollo del Objetivo Específico Nro. 3

Determinar los niveles de riesgos para el proceso de control de cambio.

Para el desarrollo de este objetivo se elaboraron diferentes criterios de probabilidad, impacto y urgencia, a través de matrices estructuradas por escalas de menor a mayor, donde el nivel más bajo representa menor grado de severidad y el más alto casos extremos de ocurrencias o situaciones.

Probabilidad

Está basada fundamentalmente en la frecuencia con la que se puede presentar eventos que produzcan riesgos.

Se establecen cinco (5) niveles para contar con un amplio espectro que permita poder determinar la probabilidad con un máximo de opciones. Estos Niveles están estructurados en valores del uno (1) al cinco (5), donde el número 1 por representar a un valor mínimo revela la probabilidad menos ocurrente y el número 5 por representar el valor más alto en la escala, revela la probabilidad de ocurrencia más alta, dado que tendrá más valor un evento cuyo riesgo es casi probable que ocurra y se pueda mitigar a aquellos que casi nunca ocurren y en caso tal de ocurrir son imposibles de controlar. A continuación se muestra la tabla Nro. 5 de Probabilidad:

Tabla Nro. 5. Escala de probabilidad de ocurrencia

Nivel de Probabilidad	Probabilidad	Frecuencia
1	**Raro**	No hay incidentes registrados o la probabilidad de ocurrencia es muy pequeña (circunstancias excepcionales). La probabilidad de que los niveles operativos fallen es muy baja.
2	**Poco Probable**	Muy pocos incidentes registrados o conocidos con alguna oportunidad razonable de ocurrir. Escasa probabilidad de no alcanzar los niveles de operación fuera de lo esperado.
3	**Posible**	Incidentes que no ocurren frecuentemente con alguna oportunidad de ocurrencia. Eventualmente se suscitan situación en la cual, algún elemento involucrado pueden verse afectados.
4	**Muy Posible**	Incidentes registrados sobre una base regular y/o evidencias anecdóticas. Posibilidad alta de que los niveles de desempeño y mantenimiento adecuado de las operaciones se salgan de los márgenes de tolerancia, causando variaciones en la efectividad de los procesos.
5	**Casi Cierto**	Incidentes frecuentes y alta probabilidad de futuras recurrencias. Es común la observación de variaciones sobre el desempeño de los procesos a modificar. Fallas y alta volatizad en el entorno a modificar.

Fuente: Manual de ITIL y Gestión de Continuidad y Contingencia de Negocio (2010)

En la tabla Nro. 5, en el nivel más bajo establecido como Raro, se encuentran las situaciones eventuales en las cuales se necesitan ciertas condiciones especiales para que se puedan presentar, las cuales exceden los límites de control que se puedan tener, en la mayoría de los casos no se tienen eventos registrados.

En el nivel **Poco Probable**, se establecen las situaciones que aunque son probables, se tienen poco eventos registros y se presentan solo cuando no se tiene ni siquiera un mínimo de control y calidad de los procesos.

El tercer nivel catalogado como **Posible**, está dirigido para aquellos incidentes que ocurren frecuentemente, que se tiene conocimiento que suceden, pero no se conoce la causa.

El nivel **Muy Posible**, ubica a aquellos eventos conocidos que están basados es registro o métricas que reflejan su frecuencia de ocurrencia, debido al grado de conciencia que se tiene de que ocurren.

El nivel **Casi Cierto**, es aquél que establece eventos tan conocidos que incurren en la rutina diaria de los procesos.

Impacto

Define el efecto que tendrá un incidente, problema o cambio en el negocio y/o sobre la plataforma tecnológica.

Los diferentes niveles están dados según el aumento o la disminución en indicadores de negocios y tecnológicos. Para la identificación del impacto se tomó el ámbito del negocio, por ende se tocó el área de Finanzas, por tratarse de una institución bancaria y el área de tecnología por ser el área origen del estudio.

Tabla Nro. 6. Escala de Impacto

Nivel de Probabilidad	Severidad	Descripción
1	Mínimo	No hay impacto ni sobre el servicio ni la reputación. Variables: • Pérdida menor a KI% del patrimonio de la institución. • Riesgo remoto de demanda legal. • Pérdida en U.T. ≤ 2.900. • Pérdida en ingresos o incrementos en costo menor al 1 %. • Modificación en los procesos transparente para el usuario. • El cambio no detiene en absoluto la operatividad del servicio • Afecta al menos el 5% de los componentes del servicio tecnológico. • No requiere alertas de suspensión de servicio
2	Menor	Impacto leve sobre el servicio y la reputación Variables: • Perdida de KLi % y KLs % del patrimonio de la institución. • Posible demanda legal. • Pérdida en U.T. entre 3.000 y 6.000. • Pérdida en ingresos o incrementos en costos entre 1.1 % y 3% • Afectación ≤ al 10% de los componentes del servicio tecnológico. • Requiere alertas de suspensión de servicios solo a determinados usuarios.

.../...

Nivel de Probabilidad	Severidad	Descripción
		• Usuarios afectados moderadamente, entre un 15% y un 35% de la organización
3	**Moderado**	Interrupción puntual del servicio crítico no superior a 8 horas Variables: • Perdida entre KLi% y KLs% de la institución. • Se evidencia una situación adversa producto del evento, si embargo es manejable. • Probable(s) demanda(s). • Impacto en factores críticos del proceso. • Afecta los objetivos de la institución. • Pérdida en U.T. entre 6.000 y 15.000. Pérdida de incremento o costo entre 3.1% y 5%. • Afectación ≥ al 15 % de los componentes del servicio tecnológico. • Usuarios afectados en su totalidad, entre un 35% y un 70% de la organización
4	Mayor	Pérdida de servicios críticos hasta más de 1 día. Variables: • Perdida entre KLi% y KLs% del patrimonio de la institución. • Demanda(s) legal(es) esperada(s). • Se evidencia fallas adversas producto del evento la cual no manejable. • Impacto promedio en objetivos de la institución. • Pérdida en U.T. entre 15.001 y 31.000. Pérdida de ingresos o incremento en costo entre 5% y 10 % • Usuarios afectados en su totalidad, entre un 70% y un 85 % de la organización. • Componente críticos afectados.
5	Catastrófico	Pérdida de servicios críticos por más de 2 días. Variables: • Pérdida mayor a KS % del patrimonio de la institución. • Pérdida mayor en U.T a 31.000 • Se espera una demanda (s) legal(es) de envergadura. • Situación adversa segura. • Impacto mayor en el cumplimiento de los objetivos estratégicos y claves en la institución. Pérdida de ingresos o incremento en los costos mayor a 10 %. • Suspensión total de los procesos tecnológicos de la instrucción. • Afectación ≥ al 100% de los componentes del servicio tecnológico.

Fuente: Manual de ITIL y Gestión de Continuidad y Contingencia de negocio (2010)

En la tabla Nro. 6, se tomaron indicadores financieros y se adaptaron a los niveles de impacto establecidos y la descripción correspondiente. Los porcentajes y los límites fueron proporcionados por el área de Finanzas de la institución de acuerdos a lineamientos gerenciales, donde establecen:

KI%: Porcentaje mínimo del patrimonio impactado

KLi%: Límite inferior del porcentaje del patrimonio impactado intermedio

KLs%: Límite superior del porcentaje del patrimonio impactado intermedio

KS%: Porcentaje máximo del patrimonio impactado

Para la Unidad Tributaria (UT) se tomaron valores en un rango entre 2.900 y 31.0000, esto debido a los rangos de valor que de igual forma la Gerencia de Finanzas toma para determinar riesgos financieros de inversión, los cuales fueron distribuidos según el nivel de impacto.

Es importante resaltar que no necesariamente tiene que existir un impacto financiero debido al cambio a ejecutar. Estos indicadores fueron tomados en cuenta como parte de un conglomerado de variables que se tienen que estimar para dar más escenarios y lograr ubicar el impacto, los cuales están orientados hacia aquellos sistemas que manejan transacciones o que repercuten sobre la operatividad del negocio por procesos indirectos de índole de administrativo.

De igual forma se estimó el porcentaje de usuarios afectados, es decir la cantidad de usuarios que hace uso de la aplicación objeto del cambio y la cantidad de elementos de configuración donde este incide.

Urgencia

Establece una medida en cuanto al tiempo de respuesta para establecer una solución ante un incidente o problema.

Está estructurada en valores del uno (1) al cinco (5), donde el número 1, por representar a un valor mínimo, tiene la holgura máxima en cuanto al tiempo establecido para efectuar el cambio y el número 5, el cual es el valor más alto en la escala, revela el nivel de urgencia más inmediato.

Tabla Nro. 7. Escala de Urgencia

Nivel de Probabilidad	Urgencia	Descripción
1	**Acción de Planeación Estratégica**	Tiempo de entrega de solución del incidente, mejora o nueva implantación, ante el usuario, ≥ a dos meses, con razones sustentables: • Solicitud respaldada por un requerimiento formal • Intervención la Oficina de Gestión de Proyectos • Alineados a los objetivos del negocio
2	**Menor**	Tiempo de entrega de solución del incidente ante el usuario, siguiente semana (s), con razones sustentables: • Fecha planeada de entrega con semana(s) de antelación • Acciones preventivas próximas a efectuarse • Mejoras en los proceso
3	**Habitual**	Tiempo de entrega de solución del incidente ante el usuario, entre 2 y 3 días, con razones sustentables: • Fecha planeada de entrega con antelación. • Solicitud respaldada por un requerimiento • Acciones preventivas o correctivas
4	**Moderada**	Tiempo de entrega de solución del incidente ante el usuario, entre 2 y 5 horas, con razones sustentables: • Continuidad en los procesos • Acciones correctivas • Dar respuestas a problemas o eventos inesperados • Minimizar consecuencias o efectos • Acciones preventivas o correctivas inmediata
5	**Acción Inmediata**	Tiempo de entrega de solución del incidente ante el usuario,1 hora, con razones sustentables: • Demandas de la alta gerencia • Incidencias en los procesos financieros • Incidencias en los procesos automatizados de la gestión • administrativa • Imperativos legales • Minimizar perdidas inminentes • Acciones correctivas

Fuente: Manual de ITIL y Gestión de Continuidad y Contingencia de negocio (2010)

En la tabla Nro. 7, se encuentran los factores más importantes que fueron considerados, entre los cuales se tiene el tipo de cambio a ejecutarse, los cuales son:

- Incidencias en los Servicios.
- Soluciones de errores conocidos.
- Nuevos Servicios o Componentes.

- Estrategia empresarial.
- Actualizaciones de software de terceros.
- Mejoras preventivas de los servicios y/o aplicaciones.
- Adquisición de Hardware y/o Software.
- Imperativo Legal.
- Mejoras Reactivas.
- Activar / Desactivar Servicios.
- Otro.

Así mismo se estableció un límite en días y/o horas para dar respuesta ante la falla o evento que suscita el cambio.

Prioridades

La asignación de prioridades identifica la importancia relativa de un incidente o riesgo. La prioridad se basa en el impacto por la urgencia. Estos niveles de prioridades se establecen para identificar y establecer tiempo de atención ante la falla o problema tecnológico que suscita un riesgo, el cual se gestiona a través del proceso de control de cambio. A continuación se muestra la tabla Nro. 8 de Niveles de Prioridad:

Tabla Nro. 8. Niveles de Prioridad

Prioridad	Valoración	Solución Esperada	Valor Numérico
	Planificación	Plan de Proyecto	0.5
	Baja	48 horas	0.10
	Media	24 horas	0.20
	Alta	8 horas	0.40
	Crítica	1 hora	0.80

Fuente: Manual de ITIL y Gestión de Continuidad y Contingencia de negocio

Asignación de Prioridad

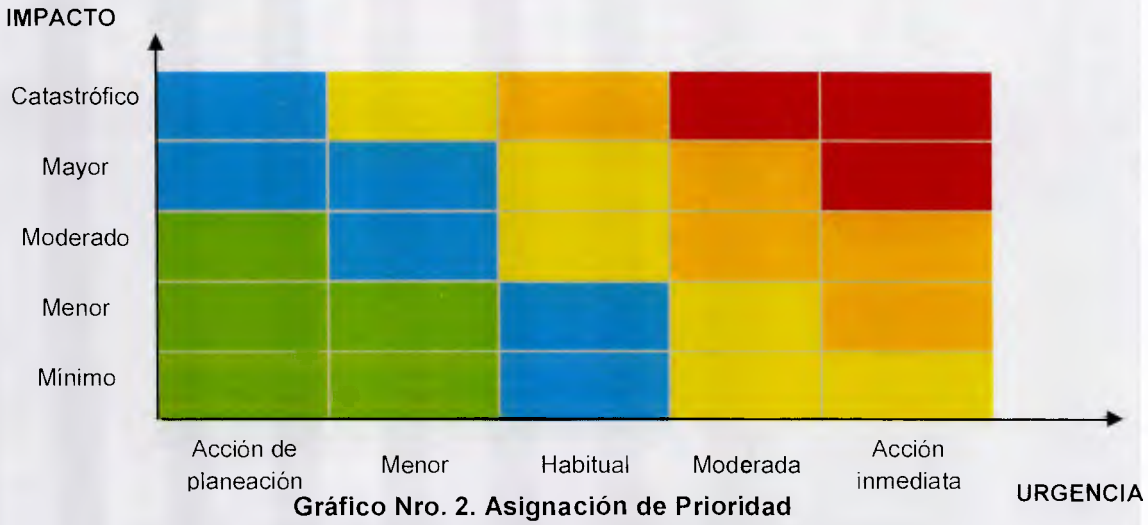


Gráfico Nro. 2. Asignación de Prioridad
Fuente: Manual de Contingencia de Tecnología de la Información

En el gráfico Nro.2, la prioridad se hace mayor a medida que los valores se desplazan hacia la derecha y hacia arriba al mismo tiempo, es decir hacia donde están los valores de impacto y urgencia mayores. Las áreas de color rojo y ladrillo son las que requieren un atención más

inmediata, la de color amarillo tienen holguras cerradas, en cuanto a la azul la holgura es abierta y la verde es una planificación en base a un proyecto de tiempo finito.

Riesgos

Estos niveles se establecen para identificar los tipos de riesgos a los que se expone la plataforma tecnológica al momento de realizar cambios, generados por requerimientos como mejoras, solución de errores, implantaciones de nuevos servicios, entre otros, a fin de establecer los responsables de su atención dada las prioridades gerenciales. El riesgo viene dado por el impacto y la probabilidad.

Tabla Nro. 9. Niveles de Riesgos

Riesgo	Valoración	Descripción	Valor Numérico
	Muy Bajo	No hay preocupación de riesgo por ejecuciones de modificaciones descontroladas o poco estimadas, ya que se cuenta con un plan de trabajo y metodologías para la gestión de las actividades a ejecutar (PMBOK).	Mayor a 0.05
	Bajo	Requiere de seguimiento a nivel de equipo y posible apoyo gerencial, para la toma de decisiones.	Menor a 0.10
	Significante	Responsabilidad gerencial y es fundamental es apoyo del personal operativo. Requiere seguimiento cercano.	Menor a 0.30
	Alto	Requiere atención y acción por la alta gerencia, requiere seguimiento cercano.	Menor a 0.50
	Extremo	Requiere atención inmediata, investigación, planificación y toma de decisiones, por parte de la junta directiva.	Mayor a 0.50

Fuente: Manual de ITIL y Gestión de Continuidad y Contingencia de negocio

Asignación de Riesgo

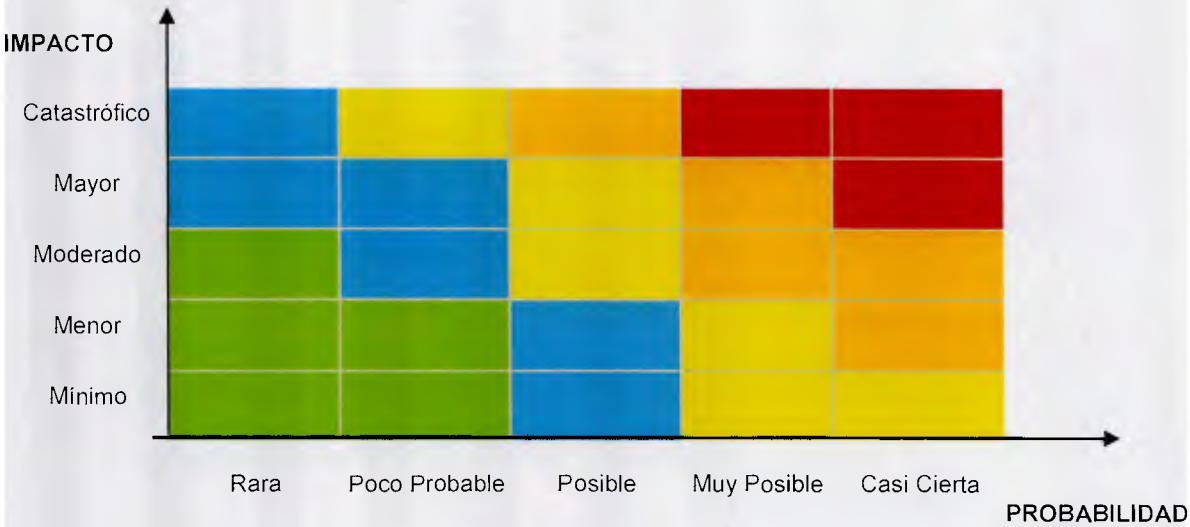


Gráfico Nro.3. Asignación de Riesgo

Fuente: Manual de Contingencia de Tecnología de la Información

En la gráfico Nro. 3, el riesgo se hace mayor a medida que los valores se desplazan hacia la derecha y hacia arriba al mismo tiempo, es decir hacia donde están los valores de impacto y probabilidad mayores. Las áreas de color rojo y ladrillo son las de riesgo alto y extremo, respectivamente, la de color amarillo es la de riesgo significante, la azul es la de riesgo medio y la verde es la de riesgo bajo.

CAPÍTULO VI

LA PROPUESTA

Desarrollo del Objetivo Específico Nro. 4

Diseñar la herramienta para la gestión de riesgos en el proceso "Control de Cambios Tecnológicos" para BANDES.

Título

Diseño de Herramienta para Minimizar el Riesgo Tecnológico en el Proceso "Control de Cambios" en el Banco de Desarrollo Económico y Social de Venezuela.

Introducción

La propuesta de una herramienta para minimizar el riesgo tecnológico en el proceso "Control de Cambios" en el Banco de Desarrollo Económico y Social de Venezuela, busca establecer el proceso para identificar factores como Impacto, Probabilidad y Urgencia, los cuales permiten cuantificar la Prioridad y los Riesgos identificado en cada requerimiento de control de cambio. Esta información es estructurada a través de un instrumento ofimáticos como lo es la hoja de cálculo.

Esta propuesta se elaboró tomando como base el Área de Gestión de Riesgos indicada en la Guía del PMI y las mejores prácticas en proceso de tecnología de la información ITIL en su versión 3.

Objetivo

Brindar una herramienta que permita el manejo de los riesgos en el proceso de Gestión de Control de Cambio, en el cual no sea afectado el alcance, tiempo, costo y calidad, a fin de garantizar la disponibilidad de los servicios en la plataforma tecnológica.

Alcance

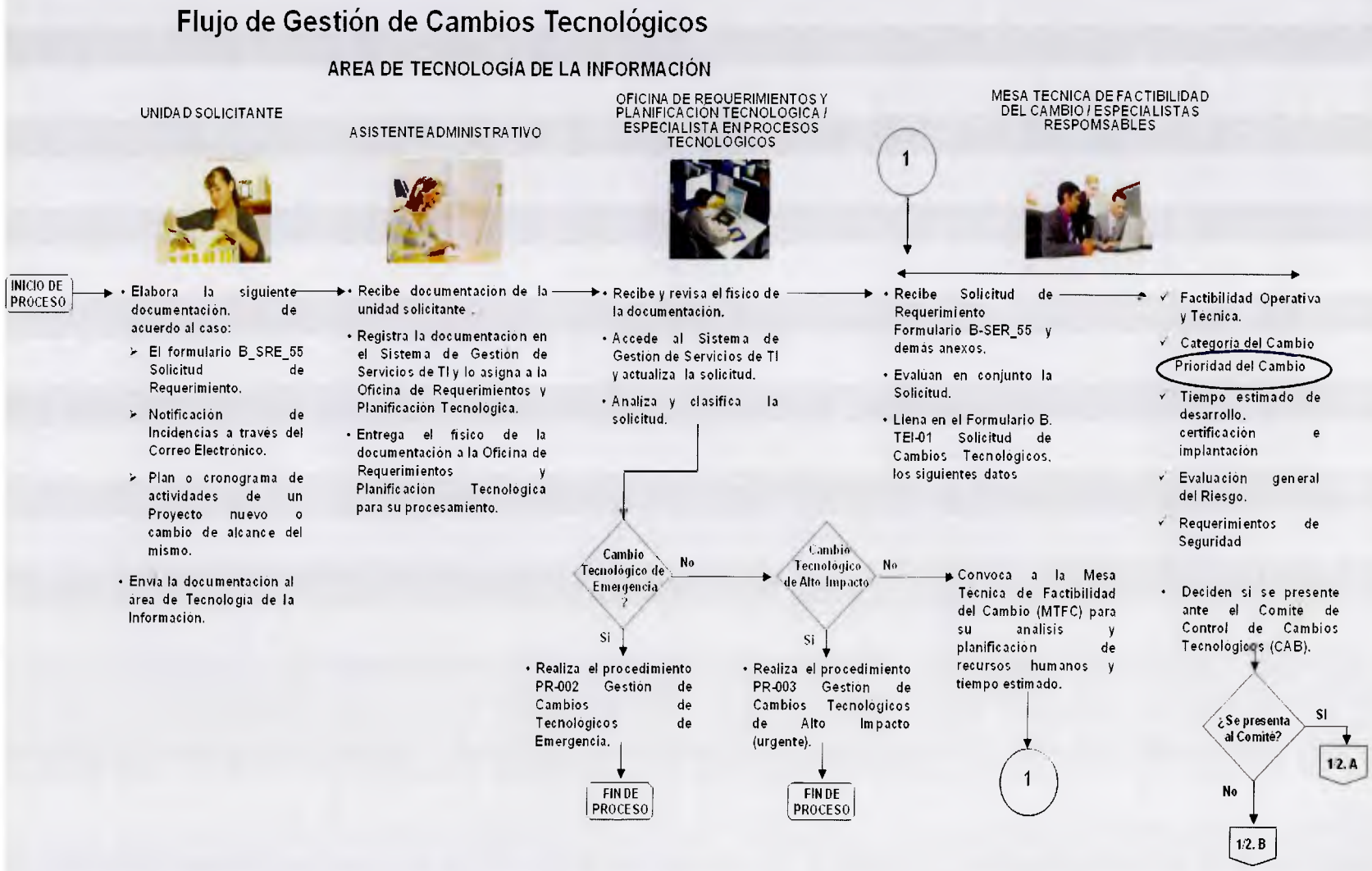
Fundamentar el proceso de control de cambio y las acciones a tomar para obtener una eficaz y proactiva gestión de los riesgos en la Gerencia Ejecutiva de Tecnología de la Información, con la finalidad de asegurar la continuidad de los servicios tecnológicos, buscando minimizar y mitigar los riesgos asociados. Esta propuesta no asegura la reducción absoluta de los riesgos por la aplicación de un control de cambio, esto debido a la existencia de riesgos residuales, los cuales no están contemplados dentro de la estructura de mitigación, sin embargo brinda en gran medida un mayor control sobre los eventos que pueden afectar los objetivos del cambio, permitiendo dar respuesta oportuna ante estos.

Estructura de la Propuesta

Ya identificadas las aplicaciones o servicios establecidos como críticos, los elementos para la identificación de los riesgos y estructuradas las matrices que apoyarán al proceso de control de cambio, se propone:

Flujo de Proceso de Control de Cambio: A continuación se presenta el Flujo de Control de Cambio en la Figura Nro.7, con la finalidad de evidenciar el proceso de priorización que se posee la GETI, para identificar el Impacto y la Urgencia de una solicitud de control de cambio.

Figura Nro. 7. Flujo de Gestión de Control de Cambio (2011)



Priorizar el Cambio: En la Figura Nro. 7 se encuentra la actividad nombrada **Factibilidad Operativa y Técnica** en la cual se prioriza el cambio, y se logra a través de una matriz poco documentada, desarrollada con fundamentos muy básicos, que indiscutiblemente exponen al control de cambio a una probabilidad alta de fallas en la ejecución del mismo.

Tabla Nro. 10. Matriz de Prioridad Actual del Proceso de Control de Cambio

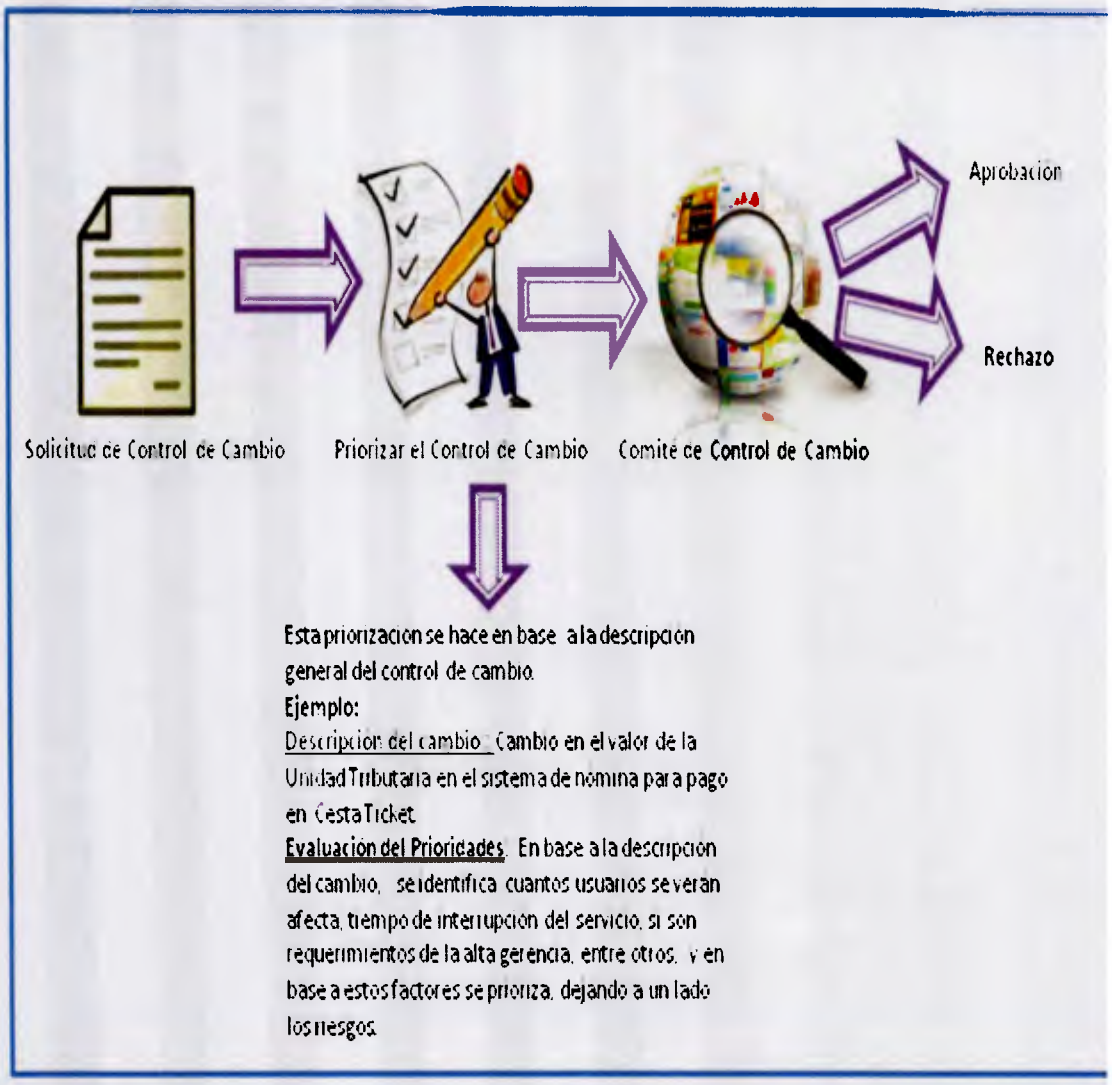
EVALUACIÓN DE PRIORIDADES					
Impacto		Sel.	Urgencia		Sel.
Alto (1)	Afecta totalmente la operatividad del negocio		**Alto (1)**	Servicio interrumpido que debe ser resuelto en un lapso no mayor a 48 horas	
	Riesgo financiero alto				
	El cambio afecta más del 60% de los componentes tecnológicos			Requerimiento de la alta gerencia	
	Usuarios afectados en su totalidad, mayor o igual a un 70 % de la organización				
Medio (2)	Afecta medianamente la operatividad del negocio.		**Medio (2)**	Servicio interrumpido que puede resolverse en un lapso entre 2 días y una (1) una semana	
	Afecta entre un 30% y 60% de los componente tecnológicos				
	Riesgo financiero medio			El incidente puede ser controlado hasta la próxima fecha de aplicación de control de cambio	
	Puede afectar pocos servicios del negocio.				
	Usuarios afectados en su totalidad, entre un 30% y un 70% de la organización				
Bajo (3)	El cambio afecta menos del 30% de los componentes		**Bajo (3)**	Servicio interrumpido que puede resolverse en un lapso mayor a 1 semana	
	Cantidad de Usuarios afectados menor al 30%				
	No afecta la operatividad del negocio			El incidente puede ser controlado por un control de cambio planificado	
	No existe riesgo financiero				

Fuente: Formulario Nro. 2. Solicitud Control Cambios Tecnológicos. (2011)

En la tabla Nro. 10 se muestra el Impacto y la Urgencia con valores del uno (1) al tres (3), donde uno (1) representa el valor más alto y tres (3) el más bajo, la descripción de cada valor carece de información, que asegure el verdadero impacto y urgencia de un control de cambio. Esta evaluación se realiza en base al control de cambio en general, es decir, no se describen cada uno de los riesgos que pueden surgir como consecuencia de la

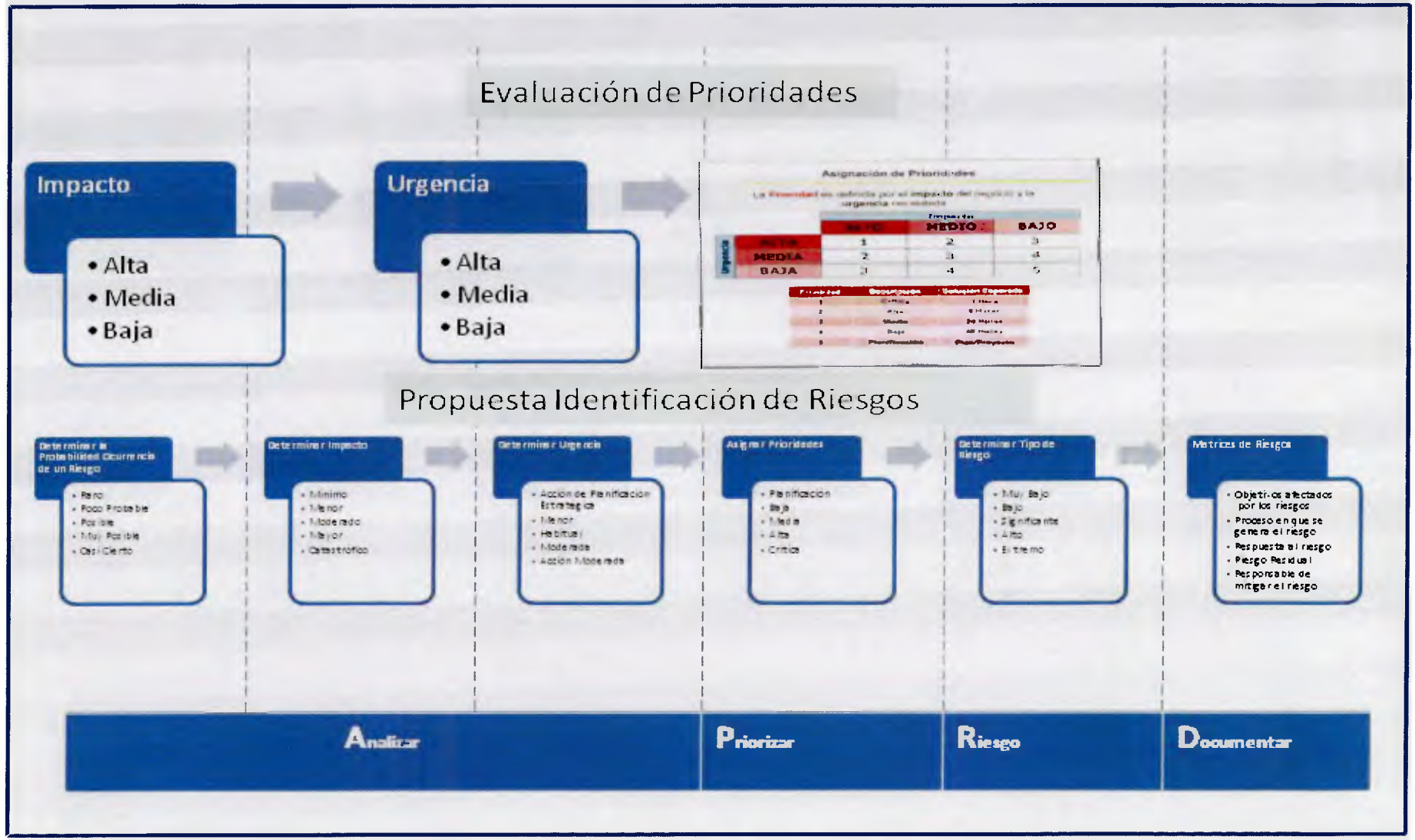
liberación, solo se hace en base a la descripción del cambio. A continuación se muestra una gráfica del proceso actual de priorización en la Gestión de Control de cambio.

Figura Nro. 8 Priorización del Proceso Actual de Control de Cambio



Realizando una comparación entre la figura Nro.8 del proceso actual reflejado en la figura Nro.7, y las tablas Nro. 5,6 y 7, elaboradas para la propuesta de la herramienta para minimizar el riesgo tecnológico en el proceso "Control de Cambios" en el Banco de Desarrollo Económico y Social de Venezuela, se presenta a continuación la figura Nro. 9.

Figura Nro. 9. Flujo Propuesto



Propuesta: En la propuesta a describir se estima un proceso de espectro más amplio, en cuanto al riesgo y la priorización de cada uno de esos riesgo identificados, de forma tal de lograr identificar los tipos de riesgo que se presentan en cada solicitud de control de cambio.

Para ello se desarrollaron formularios a fin de aplicar los criterios de **Probabilidad, Impacto y Urgencia** ya establecidos en el desarrollo del objetivo Nro.3, desarrollados a través de matrices estructuradas por escalas de menor a mayor, por lo cual se elaboraron dos (2) formatos, en donde se disponen los riegos asociados a un control de cambio. Dichos formularios tienen precedencia uno del otro, es decir no se puede llegar a completar el formulario Nro.2 sin haberle suministrado los datos al Nro. 1.

Se propone que inicialmente estos formularios sean aplicados, solo para las solicitudes de cambios que se refieran a los servicios y aplicaciones establecidos como críticos, para luego extenderlo a todas las solicitudes y todos los sistemas.

Estructura de los Formularios: A fin reducir los pases a producción fallidos y fomentar confianza sobre la solución o mejora a implementar en cuanto a la plataforma de tecnología se refiere. A continuación se presentan los formularios.

Tabla Nro. 11. IDENTIFICACIÓN Y EVALUACIÓN CUALITATIVA DE LOS RIESGOS

Descripción del Cambios	
(DC1)Descripción del cambio	
(DC2)Código del control de cambio	
(DC3) Aplicación o servicio objeto del Cambios	

Nro.	Código del Riesgo (CR1)	Descripción del Riesgo (DR2)	Causa (C3)	Efecto de la Causa (EC4)	Impacto (I5)	Urgencia (U6)	Probabilidad (P7)	Impacto por urgencia (Prioridad) (P8)	Tipo de Riesgo (TR9)	Objetivos Afectados (OA10)	
										Alcance	
										Tiempo	
										Costo	
										Calidad	
										Alcance	
										Tiempo	
										Costo	
										Calidad	
										Alcance	
										Tiempo	
										Costo	
										Calidad	
										Alcance	
										Tiempo	
										Costo	
										Calidad	

Tabla Nro. 12. GESTIÓN DE RIESGOS

Código del Riesgo (CR1)	Proceso en que se genera (Pro2)	Elemento de Configuración Afectado (EConf3)	Afecta (A4)	Respuesta al Riesgo (RR5)	Riesgo Residual (RRes6)	Responsable (R7)	Observaciones (O8)

Instrucciones para completar los formularios:

Para la matriz **Identificación de Riesgo** (IR1) se establece:

Identificación y Evaluación Cualitativa de los Riesgos

Descripción del Cambio

(DC1): En este campo se realizará un breve resumen de las especificaciones del cambio describiendo la situación actual y la situación deseada a través de cambio.

(DC2): Se refiere al código asignado por el gestor del cambio una vez que ingresa la solicitud de control de cambio y con el cual se identifica a través de todo el flujo del proceso.

(DC3): Nombre del servicio o aplicación objeto del cambio.

Identificación y Evaluación Cualitativa de los Riesgos

(CR1): Código según nomenclatura, con el fin de listar los riesgos para una situación en específica.

(DR2): Descripción de los posibles riesgos en relación a las situaciones que se pueden presentar debido a la implementación del cambio y la severidad de este.

(C3): Descripción del origen del riesgo identificado, ¿cómo surgen? Razón por la cual se presenta este riesgo. Esto con el fin de identificar posibles fallas en otros elementos de configuración o sistemas que surgen o pueden impactar sobre otro cambio a ejecutarse.

(EC4): Listar las consecuencias que ocasionan las causas de las fallas o eventos ya descritos anteriormente.

(I5): Este campo fue diseño con la finalidad de que el gestor de cambio logre identificar aquellos factores de inciden de forma positiva o negativa sobre el riesgo identificado en la solicitud de cambio analizada, con el fin de establecer el nivel de impacto al cual obedece. Ver pág.62 para asignación de impacto.

(U6): Este campo fue diseño con la finalidad de que el gestor de cambio logre identificar según el riesgo establecido el tiempo de respuesta ante la solicitud de cambio analizada, con el fin de establecer el nivel de urgencia al cual obedece. Ver pág.64 para asignación de Urgencia.

(P7): Este campo fue diseño con la finalidad de que el gestor de cambio logre identificar la probabilidad de ocurrencia o no del riesgo descrito, con el fin de establecer el nivel de probabilidad al cual obedece. Ver pág.60 para asignación de Probabilidad.

(P8): Ésta es establecida por el impacto y la urgencia y determina la importancia del riesgo identificado sobre cualquier otro en el control de cambio analizado. Ver pág.66 para asignación de Prioridad.

(R9): Este campo fue diseño con la finalidad de que el gestor de cambio logre asignar al riesgo identificado según la Probabilidad y el Impacto, el tipo de riesgo al cual este obedece. Ver pág.67 para asignación de riesgo

(OA10): Este campo fue diseñado con la finalidad de identificar según el riesgo ya establecido como afecta este el alcance, tiempo, costo y calidad, a los objetivos de la solicitud de cambio.

Para la matriz **Identificación de Riesgo (IR2)** se establece:

Plan de Gestión de Riesgos

(CR1): Corresponde a cada código utilizado en el formulario Nro.1 para describir los riesgos.

(Pro2): Ubicar el proceso donde se genera el riesgo identificado según su código, dentro la plataforma de tecnología de TI.

(EConf3): Identificar el Elemento de Configuración que ocasiona el riesgo identificado.

(A4): Descripción detallada de cómo afecta al proceso identificado el Elemento de Configuración.

(RR5): Descripción detallada del Plan de acción que mitigara el riesgo en caso de que se presente.

(RRes6): Establecer según la tabla de asignación de riesgo, el nivel que se pueda presentar aun siendo mitigado por el plan de acción. Ver pág.65 para asignación de riesgo.

(R7): Se refiere al personal responsable de que se ejecute el plan de acción para minimizar el riesgo y sus efectos.

(O8): Se refiere a la información adicional que se pueda presentar o que se evidencia a lo largo del análisis y que no puede ser omitida.

Factibilidad de la Propuesta

La propuesta de una herramienta para minimizar el riesgo tecnológico en el proceso "Control de Cambios" en el Banco de Desarrollo Económico y Social de Venezuela, se considera factible bajos los siguientes elementos evaluados:

- **Técnico/Operativo:** La Oficina de Requerimiento y Planificación Tecnología, trabaja dentro del marco de referencia ITIL, por la cual es un equipo orientado a la mejora continua y a la optimización de los procesos tecnológicos y búsqueda de nuevas estrategias que permitan alcanzar los objetivos tazados. La propuesta contempla el manejo del riesgo, a través de la identificación de factores como el Impacto y la Urgencia de un evento, incidente o mejora sobre la plataforma tecnológica del BANDES, también muestra la Priorización y Probabilidad de ocurrencia. Así mismo permite al proceso actual de gestión de control de cambio, ampliarse en las actividades donde se evidencia debilidad, a fin de que garantizar la reducción de los controles de cambios fallidos y asegurar la continuidad de los procesos tecnológicos de la institución. Por lo anteriormente expuesto se considera que se cuenta con el recurso humano disponible y los conocimientos para sustentar la implementación de esta propuesta.

- **Psicosocial:** Se cuenta con un personal en plena conciencia y disposición para realizar las estrategias de mejora continua en el

proceso de implantación, así como también para el cumplimiento de las nuevas actividades y responsabilidades.

Beneficios de la Propuesta

- Reducción de la tasa de fallas en la plataforma tecnológica, a causa de la ejecución de un control de cambio.
- Confianza por parte de nuestros clientes y usuarios en la plataforma tecnológica.
- Mejoras en la ejecución de las tareas y los procesos de la Oficina de Requerimientos y Planificación Tecnológica.
- Detecciones de posibles fallas e implantación de mejoras en los sistemas y/o aplicaciones, debido a la información de los riesgos asociados, por historial documentado a través la herramienta de riesgo.
- Optimización en el rendimiento de los indicadores de gestión.
- Creación de nuevos indicadores de gestión, asociados a riesgo.
- Generación de proyectos a partir de los riesgos identificados a través de la herramienta o instrumento propuesto, a fin de crear un portafolio de proyectos, orientados a reducir las debilidades en los sistemas y/o aplicaciones que evidencian riesgos latentes por sufrir modificaciones o cambios.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

En función de los objetivos planteados inicialmente y considerando los resultados obtenidos, se presentan las siguientes conclusiones:

En base a las reuniones realizadas con las áreas involucradas en el proceso de control de cambio, se lograron elaborar categorías implícitas en el riesgo, como lo es el impacto, la probabilidad y la urgencia, las cuales no tenían precedentes ni estaban en la ocasión de identificar y analizar el riesgo ante las solicitudes de cambios.

Así mismo se construyeron matrices para priorizar el riesgo y asignar el tipo de riesgo para cada cambio, el cual fue valorizado en grados de menor a mayor, siendo de menor prioridad el plan de trabajo y la acción más confortable y planificada, y el nivel más alto con obligación de acciones drásticas e inmediatas por el afecto y las consecuencias negativas sobre el negocio.

Se elaboraron y propusieron formularios para ser implantados en la Oficina de Requerimientos y Planificación Tecnología (ORPT), con la finalidad de proveer un insumo para extraer la información requerida al momento de identificar y listar los riesgos relacionado y su repercusión en el proyecto de cambio sobre el alcance, el tiempo, el costo y la calidad del mismo.

Con la propuesta desarrollada en esta investigación: "Minimizar El Riesgo Tecnológico En El Proceso "Control De Cambios" En El Banco De

Desarrollo Económico Y Social De Venezuela (Bandes)." se cumplió el desarrollo de cada uno de los objetivos planteados inicialmente.

Se logró determinar las carencias que presenta la institución:

La unidad no cuenta con técnicas y/o procedimientos para la identificación y análisis de riesgos para el caso específico de cambios en la plataforma tecnológica del Banco.

Carece de una definición clara de los factores que tienen que ser tomados en cuentas y son tácitos del riesgo.

Como último punto respecto al Análisis de Riesgos, se concluye: que los riesgos que pueden surgir en etapas tempranas se pueden evitar dilucidando muy bien los requisitos, adquiriendo información, optimizando la comunicación entre todos los involucrados y/o obteniendo experiencia. Del mismo modo, tomando acciones anticipadas de manera de reducir la posibilidad de que un riesgo ocurra e impacte sobre un proyecto, a menudo es más positivo que tratar de resarcir el daño después de que el riesgo ha ocurrido y cuando los efectos son irreparables.

Recomendaciones

A partir de lo expuesto anteriormente se efectúan las siguientes recomendaciones:

- Reforzar los conocimientos sobre la gestión de riesgos dentro de la Gerencia Ejecutiva de Tecnología de la Información a fin de fomentar el manejo de herramientas, políticas, procedimientos y estándares dispuestos para ello como lo es; el Comité de Supervisión Bancaria de Basilea, el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC) y la Guía de los Fundamentos para la Dirección de Proyectos (PMBOK) en su módulo de Gestión de Riesgos.

- Es de suma importancia que la Gerencia Ejecutiva de Tecnología de la Información esté en conocimiento constante de los riesgos operativos que se pueden presentar por las fallas o errores que sufra la plataforma tecnológica, es por ello que se necesario contar con un plan de contingencia que sería impulsado por los resultados de la implantación de la propuesta objeto de estudio.

- Es importante la incorporación de métricas e indicadores de riesgos que reflejen la tendencia de los riesgos más significantes por cada área del banco.

- Incluir es la gestión de la ORPT, la elaboración de informes mensuales sobre las fallas o éxitos en la liberación de cada cambios, a fin de que exista una retroalimentación y mejora continua en el proceso de identificación y análisis de los riesgos.

REFERENCIAS BIBLIOGRÁFICAS

Arias, F. (2006). *"El proyecto de investigación. Introducción a la metodología científica".* (5ta ed.). Caracas: Editorial Episteme.

Balestrini, M. (2006). *"Como se elabora el proyecto de investigación".* (7ª ed.). Caracas: BL Consultores Asociados. Servicio Editorial.

Banco de Desarrollo Económico y Social de Venezuela. (2011). Código de Ética del Bandes. Recuperado en Mayo de 2012 de la Intranet: http://intranet.bandes.gob.ve/norproc/general/index.html

Basilea, A. d. (s.f.). http://da.com.ve/. Recuperado el Junio de 2012, de http://www.bis.org/index.htm. Consulta.

Chamoun, Y. (2002). *"Administración profesional de proyectos: La guía".* México D.F. McGraw-Hill / Interamericana editores.

Comité de Supervisión Bancaria de Basilea. (2004*)."Convergencia Internacional de Medidas y Normas de Capital".* Banco de Pagos Internacionales. Suiza.

Fernández, Hernández y Baptista. (2003). *"Metodología de la Investigación".* (3a Ed.). México D.F. Mc Graw –Hill.

Fundamentos de ITIL Versión 3. Recuperado en Junio 2012 de http://www.aitil.com.ve/

Fundamentos de la Gestión TI en ITIL V3. (2007). Recuperado en Mayo de 2012,de http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

Instituto Colombiano de Normas Técnicas y Certificación. ICONTEC. (2011). "*Documentación: Gestión de Riesgos, Principios Restricciones*". NTC 31000. Bogotá, Colombia.

Kerlinger, F. (1981). "*Investigación del Comportamiento*". México: Editorial. McGraw-Hill.

Marichal, C. "*Diseño conceptual de un sistema para la gestión de riesgo en proyectos de desarrollo de software*". Trabajo Especial de Grado presentado ante la Universidad Católica Andrés Bello. Decanato de Estudios de Postgrado, para obtener el título de Especialista en Gerencia de Proyectos. Caracas, Venezuela.

Panfil, J. "*Plan de gestión de riesgos para el proyecto de mejoras de las microcentrales hidroeléctricas ubicadas en la Gran Sabana operadas por EDELCA*". Trabajo Especial de Grado presentado ante la Universidad Católica Andrés Bello. Decanato de Estudios de Postgrado, para obtener el título de Especialista en Gerencia de Proyectos. Caracas, Venezuela.

Project Management Institute. (2006). Project Management Institute Código de Ética y Conducta Profesional. Recuperado en Mayo de 2012 de la Word Wide Web: de la World Wide Web:http://www.zanzivar.com/zzc/index.php?option=com_content&view=article&id=16:el-codigo-de-etica-y-conducta-profesional&catid=7

Project Management Institute. (2008). Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK). (4ta ed.). Pennsylvania: Project Management Institute, Inc.

Sabino, C. (1992). "*El Proceso de Investigación*" (2a ed.). Caracas: Editorial Panapo.

Selltiz, C., Jahoda, M., Deutsch, M. y Cook, S. W. (1976). "*Métodos de investigación en las relaciones sociales*". *(8a Ed.)*. Madrid, España.

Simonovis, E. *"Diseño del proceso de gestión de versiones y liberaciones para la Vicepresidencia de Operaciones de Tecnología de Información de Banesco, basado en mejores prácticas para la gestión de servicios de ITIL"*. Trabajo Especial de Grado presentado ante la Universidad Católica Andrés Bello. Decanato de Estudios de Postgrado, para obtener el título de Especialista en Gerencia de Proyectos. Caracas, Venezuela.

Sosa, C. *"Gestión de riesgos en proyectos de desarrollo de software en una empresa de consultoría venezolana"*. Trabajo Especial de Grado presentado ante la Universidad Católica Andrés Bello. Decanato de Estudios de Postgrado, para obtener el título de Especialista en Gerencia de Proyectos. Caracas, Venezuela.

Velazco, L. (Comp.) (2010). "*Instructivo Integrado para Trabajos Especiales de Grado (TEG)"*. Caracas: Universidad Católica Andrés Bello.

Villamizar, G. "*Herramienta para la medición de riesgos en proyectos de implementación del sistema ERP SAP BUSSINES ONE"*. Trabajo Especial de Grado presentado ante la Universidad Católica Andrés Bello. Decanato de Estudios de Postgrado, para obtener el título de Especialista en Gerencia de Proyectos. Caracas, Venezuela.

Vincentelli, O. *"Desarrollo de los proceso de gerencia de riesgos para los proyectos estratégicos de C.V.G. Electricidad del Caroní, C.A.–EDELCA"*. Trabajo Especial de Grado presentado ante la Universidad Católica Andrés Bello. Decanato de Estudios de Postgrado, para obtener el título de Especialista en Gerencia de Proyectos. Caracas, Venezuela

Yáber, G. y Valarino, E. (2003). *"Tipología, fases y modelo de gestión para la investigación de postgrado en gerencia"*. Caracas, Venezuela.