Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Industrial

DISEÑO DE LA INVESTIGACIÓN DE LA METODOLOGÍA PARA MEDIR EL GRADO DE MITIGACIÓN DEL IMPACTO DE LOS RIESGOS TECNOLÓGICOS EN BANCO INTERNACIONAL

Billy Johann Asturias Rojas
Asesorado por el Msc. Ing. Nery Augusto Paz Barrientos

Guatemala, marzo de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE LA INVESTIGACIÓN DE LA METODOLOGÍA PARA MEDIR EL GRADO DE MITIGACIÓN DEL IMPACTO DE LOS RIESGOS TECNOLÓGICOS EN BANCO INTERNACIONAL

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

BILLY JOHANN ASTURIAS ROJAS
ASESORADO POR EL MSC. ING. NERY AUGUSTO PAZ BARRIENTOS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO INDUSTRIAL

GUATEMALA, MARZO DE 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

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

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

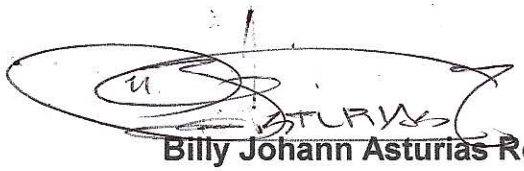
DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Alberto Eulalio Hernández García
EXAMINADOR	Ing. Byron Gerardo Chocoj Barrientos
EXAMINADORA	Inga. Miriam Patricia Rubio de Akú
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

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

DISEÑO DE LA INVESTIGACIÓN DE LA METODOLOGÍA PARA MEDIR EL GRADO DE MITIGACIÓN DEL IMPACTO DE LOS RIESGOS TECNOLÓGICOS EN BANCO INTERNACIONAL

Tema que me fuera asignado por la Dirección de la Escuela de Estudios de Posgrado, con fecha 04 de febrero de 2013.



Billy Johann Asturias Rojas

Universidad de San Carlos
de Guatemala

Escuela de Estudios de Postgrado
Facultad de Ingeniería
Teléfono 2418-9142

AGS-MGIPP-0029-2013

Guatemala, 04 de febrero de 2013.

Director
César Ernesto Urquizú Rodas
Escuela de Ingeniería Industrial
Presente.

Estimado Director:

Reciba un atento y cordial saludo de la Escuela de Estudios de Postgrado. El propósito de la presente es para informarle que se ha revisado los cursos aprobados del primer año y el Diseño de Investigación del estudiante **Billy Johan Asturias Rojas** con carné número **1991-12849**, quien opto la modalidad del **"PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO".**

Y si habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Decimo, Inciso 10.2, del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Sin otro particular, atentamente,

"Id y enseñad a todos"

César Akú Castillo MSc.
INGENIERO INDUSTRIAL
COLEGIADO No. 4,073

Msc. Ing. Nery Augusto Paz Barrientos
Asesor (a)

Ing. Agr. MI. Nery Paz
Colegiado 1967

Msc. Ing. César Augusto Akú Castillo
Coordinador de Área
Gestión y Servicios

Dra. Mayra Virginia Castillo Montes
Directora
Escuela de Estudios de Postgrado

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POST-GRADO
FACULTAD DE INGENIERIA
GUATEMALA

Cc: archivo
/la

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF.DIR.EMI.068.013

El Director de la Escuela de Ingeniería Mecánica Industrial de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el Visto Bueno del Revisor y la aprobación del Área de Lingüística del trabajo de graduación en la modalidad Estudios de Postgrado titulado **DISEÑO DE LA INVESTIGACIÓN DE LA METODOLOGÍA PARA MEDIR EL GRADO DE MITIGACIÓN DEL IMPACTO DE LOS RIESGOS TECNOLÓGICOS EN BANCO INTERNACIONAL,** presentado por el estudiante universitario **Billy Johann Asturias Rojas,** aprueba el presente trabajo y solicita la autorización del mismo.

"ID Y ENSEÑAD A TODOS"

Ing. César Ernesto Urquizú Rodas
DIRECTOR
Escuela de Ingeniería Mecánica Industrial

UNIVERSIDAD DE SAN CARLOS
DIRECCION
Escuela de Ingeniería Mecánica Industrial
FACULTAD DE INGENIERIA

Guatemala, marzo de 2013.

/mgp

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.172-2013

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Industrial, al trabajo de graduación titulado: **DISEÑO DE LA INVESTIGACIÓN DE LA METODOLOGÍA PARA MEDIR EL GRADO DE MITIGACIÓN DEL IMPACTO DE LOS RIESGOS TECNOLÓGICOS EN BANCO INTERNACIONAL,** presentado por el estudiante universitario: **Billy Johann Asturias Rojas,** autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, marzo de 2013

/cc

ACTO QUE DEDICO A:

Dios	Por haberme permitido llegar hasta este momento tan importante en mi vida.
Mis padres	Blanca Lidia Rojas de Asturias (q.e.p.d.) y Alfredo Asturias Divas, por haberme enseñado que las metas se alcanzan con paciencia, constancia y perseverancia; además de nunca olvidar nuestros orígenes, la humildad, la pasión y el amor a Dios.
Mi esposa	Nancy Magaly Cabrera Ibarra, por apoyarme incondicionalmente en todo momento y ser ese soporte en el que siempre puedo confiar.
Mis hijos	Marcelo Andrés Asturias Cabrera y Sebastián Andrés Asturias Cabrera, por ser ese combustible inagotable que siempre me inspiran a seguir adelante.
Mis hermanos	Herbert Estuardo Meza Escobar, Evelyn Carolina Asturias Rojas y Marvin Alfredo Asturias Rojas, por su apoyo y consejos.
Mis amigos	Por su amistad y compartir momentos muy importantes en mi vida.

AGRADECIMIENTO A:

Universidad de San Carlos de Guatemala	Por ser la casa que me brindo los conocimientos necesarios para alcanzar mis metas profesionales.
Facultad de Ingeniería	Por permitirme ser parte de ella y forjarme como un orgulloso integrante de esta facultad.
Escuela de Mecánica Industrial	Por aportar los conocimientos que han servido para representar a la facultad profesionalmente y permitirme realizar este trabajo de graduación.
Ingenieros	Ing. Carlos Olivares, Ing. Alberto Hernandez, Ing. Nery Paz, por compartir sus conocimientos y apoyarme para llevar a cabo este trabajo de graduación.
Todas las personas que hicieron parte de este trabajo de graduación	Por compartir sus conocimientos y consejos para hacer posible el trabajo de graduación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Antropogénico — Se refiere a los efectos, procesos o materiales que son el resultado de actividades humanas a diferencia de los que tienen causas naturales sin influencia humana.

Basilea II — Es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea.

BCP — Plan de Continuidad del Negocio (del inglés Business continuity planning) son los planes logísticos para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre.

Cobit 5 — Es una normativa que proporciona un marco integral que ayuda a las organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la organización.

Comité ALCO	Comité conformado por el área de riesgos de mercado y la Tesorería del Banco llevan un control diario de los riesgos, tanto transaccionales como no transaccionales.
Diagnóstico	Se refiere al análisis que se realiza para determinar cualquier situación y cuáles son las tendencias.
DRP	Es un plan de recuperación ante desastres (del inglés *Disaster Recovery* Plan) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.
Impacto	Es una magnitud que mide el número de repeticiones por unidad de tiempo de cualquier fenómeno o suceso periódico.
Medición	Es el efecto que produce una acción.
Medición	La medición es un proceso básico de la ciencia que consiste en comparar un patrón seleccionado con el objeto o fenómeno cuya magnitud física se desea medir para ver cuántas veces el patrón está contenido en esa magnitud.

Metodología

Hace referencia al conjunto de procedimientos racionales utilizados para alcanzar una gama de objetivos que rigen en una investigación científica, una exposición doctrinal o tareas que requieran habilidades, conocimientos o cuidados específicos. Alternativamente puede definirse la metodología como el estudio o elección de un método pertinente para un determinado objetivo.

Monitoreo

Su origen se encuentra en monitor, que es un aparato que toma imágenes de instalaciones filmadoras o sensores y que permite visualizar algo en una pantalla. El monitor, por lo tanto, ayuda a controlar o supervisar una situación.

Normas

Regla o conjunto de reglas que hay que seguir para llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo.

Política

Es una rama de la moral que se ocupa de la actividad, en virtud de la cual una sociedad libre, compuesta por hombres libres, resuelve los problemas que le plantea su convivencia colectiva, es un quehacer ordenado al bien común.

Reglamentos	Conjunto de normas, reglas o leyes creadas por una autoridad para regir una actividad o un organismo.
Riesgo inherente	Es el riesgo de que ocurran errores importantes generados por las características de la empresa o el organismo.
Riesgos	La probabilidad de que una amenaza, peligro o incertidumbre, a que se ve enfrentada una persona o institución, por efecto o acción relacionada con sus líneas de negocio, operaciones y demás actividades, que pudieran afectar su situación actual.
Risk IT	Es un marco basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión que se ajustan a estos principios.
SIB	Superintendencia de Bancos.
Sostenibilidad	Cualidad por la que un elemento, sistema, o proceso, se mantiene activo con el transcurso del tiempo. Cualidad por la que un elemento se sostiene.
Tolerancia	El término tolerancia puede referirse a la acción y efecto de tolerar o aceptar un riesgo.

Vulnerabilidad	Es la incapacidad de resistencia cuando se presenta un fenómeno amenazante, o la Incapacidad para reponerse después de que ha ocurrido un desastre.

RESUMEN

Las instituciones financieras deben contar con una infraestructura tecnológica lo más actualizada posible, además debe ser lo suficientemente robusta para atender todos los requerimientos que los clientes necesiten, ya que cada día es más fácil tener accesos a sistemas informáticos que faciliten las actividades diarias, lo cual ha venido cambiando aceleradamente en los últimos años. Hoy, los usuarios son más exigentes y tienden a preferir los servicios tecnológicos y por ende a las empresas que se encuentren más actualizadas tecnológicamente.

Lo anterior es de suma importancia, ya que permite identificar debilidades en la administración tecnológica de instituciones financieras como el Banco Internacional, el cual cuenta con una infraestructura tecnológica para soportar toda su funcionalidad y servicio a los clientes, lo que lo coloca en una posición de vulnerabilidad y lo posiciona en un nivel de riesgo alto y la única manera de minimizarlo, es a través de definir estrategias de mitigación, elaborar planes de contingencia, probarlos y saber hasta que punto hemos alcanzado reducir esos riesgos.

Finalmente se utilizará de base, la normativa Cobit 5, la cual proveerá las herramientas necesarias para establecer la metodología que permita medir el grado de mitigación del impacto de los riesgos tecnológicos del Banco Internacional.

Metodología

La metodología que a continuación se describe, consta de 2 etapas, la primera etapa es el estudio del entorno, que a su vez consta de 2 fases, las cuales comprenden la estructura administrativa de riesgo integral y las principales líneas de negocios y la segunda etapa, es la implantación de la solución, que consta de 6 fases, las cuales describen los pasos que se deben cumplir para poder obtener el grado de mitigación de impacto del riesgo tecnológico, lo cual se deberá verificar en las evaluaciones de las 3 fases de la continuidad.

Análisis de entorno

Organización para la administración del riesgo integral

Un aspecto fundamental para la puesta en marcha del sistema de administración de riesgos, es la separación de las unidades de negocio, áreas, departamentos, divisiones que generan los riesgos de aquellas áreas o unidades que monitorean su administración y control. La estructura organizacional de Banco Internacional, S. A. a cargo de la gestión integral de riesgos, se integran por el Consejo de Administración y la alta dirección, el Comité de Riesgo Integral, del cual, el Departamento de Riesgo Integral es un integrante permanente, los que aseguran su independencia y capacidad para supervisar y gestionar los riesgos a que está expuesto el banco.

Implementación de la solución

Gestión integral de riesgos

La gestión integral de riesgos involucra un conjunto de fases o etapas, cuyo objetivo es gestionar y controlar los riesgos a que está expuesto el banco. La metodología que ha dispuesto Banco Internacional, S. A. para la gestión integral de riesgos, se basa en 2 grandes aristas: gestión activa y gestión proactiva.

Identificación de riesgos

Previamente establecidas las líneas de negocio, así como los procesos más críticos, la primera fase de la gestión de riesgos, consiste en identificar los riesgos a que está expuesto el banco, es decir, determinar los eventos internos y externos que pueden tener un impacto negativo sobre los objetivos del banco. Esta etapa exige un análisis meticuloso del proceso, del cual deriva determinado riesgo, dentro del contexto en el que se desenvuelve la institución.

Medición

La medición involucra la ponderación o forma de cuantificar los riesgos, para ello se debe tipificar el efecto negativo o impacto que pueda repercutir en la institución. Para dicha medición, será necesario determinar para cada riesgo, la frecuencia y la intensidad de ocurrencia o impacto, lo que se realiza por medio de una matriz.

Frecuencia

Por frecuencia, se entiende la probabilidad de ocurrencia o el porcentaje de estimación de ocurrencia de un riesgo en un período de tiempo. La escala de frecuencia establecida para Banco Internacional, S. A. va desde el nivel 1 hasta el nivel 5 (en su orden, muy baja, baja, moderada, alta y muy alta).

Impacto

Determinar el impacto previsible de los distintos riesgos, es necesario evaluar las consecuencias estimadas, sin tener en cuenta el impacto de los mecanismos de administración. El impacto se refiere a la trascendencia que tiene la materialización del riesgo para la entidad, ya sea porque tiene un efecto financiero importante o porque afecta la continuidad de operaciones de la institución.

Monitoreo

El monitoreo de los principales riesgos, es una forma de estar presente en todos los niveles de la organización, permitiendo que a través de controles se muestre el desarrollo de los procesos y los problemas que podrían ocurrir en el transcurso de las actividades.

Control y mitigación

Conocidos los riesgos a los que se encuentra sometido el banco en función de las operaciones que realiza, la frecuencia e impacto que eventualmente pueden generar los mismos, así como determinar su importancia

para la institución, es necesario definir los mecanismos de los que se dispone para su adecuada gestión.

Riesgo residual

Es el riesgo resultante luego de tomar en cuenta el efecto del control interno sobre la ponderación de frecuencia e impacto de cada riesgo. Este se calcula de la siguiente forma:

Riesgo residual = (frecuencia * impacto) /control

Riesgo residual

Es el riesgo resultante luego de tomar en cuenta el efecto del control interno sobre la ponderación de frecuencia e impacto de cada riesgo. Este se calcula de la siguiente forma:

Riesgo residual = (frecuencia * impacto) /control

Informes de evaluación de riesgos

El Departamento de Riesgo Integral elaborará en conjunto con los responsables de cada riesgo específico, los informes de exposición al riesgo. El resultado de dicha evaluación debe hacerse del conocimiento del Comité de Riesgo Integral, quien debe analizar la exposición del banco y tomar las decisiones más acertadas para su adecuada gestión.

1. INTRODUCCIÓN

El hombre durante toda su evolución, se ha valido del uso de la tecnología para ser más eficiente y facilitarse la vida, hoy en día, la tecnología es parte de la cotidianeidad y ayuda a obtener bienes o servicios de manera inmediata, además de facilitar el acceso a la información; pero el hacer uso de la tecnología también expone a los riesgos inherentes que esta con lleva, tales como; pérdidas de información, uso indebido de información personal, etcétera. Para evitar o prevenir estos problemas se han diseñado normas y mejores prácticas, con el fin de minimizar estas incidencias o fallas tecnológicas que en el caso de la banca, podría llegar a provocar pérdidas económicas y de reputación.

En lo que respecta a la banca en Guatemala, hasta hace unos años, el ente supervisor del estado para las instituciones financieras, la Superintendencia de Bancos (SIB), ha venido implementando una serie de regulaciones y normas con el fin de obligar a todas estas instituciones a regular la gestión del riesgo operativo, entre estos; el riesgo tecnológico. Estas regulaciones no describen el uso de una normativa en específico, ni mucho menos define una metodología para medir el grado de madurez en la mitigación de dichos riesgos, solo guían a las instituciones financieras a cumplir con ciertas especificaciones, procesos y registros con el fin de poder demostrar que se tiene implementado un sistema de gestión del riesgo.

El poder cumplir con estas regulaciones, han obligado a las instituciones financieras a invertir y definir sus propios esquemas para la gestión del riesgo, basándose en dichas normativas. Uno de los procesos más importantes, es el

de establecer una metodología para medir el grado de mitigación del riesgo al que la institución está expuesta, y con esto poder definir cual es el grado de madurez que se ha alcanzado.

En el presente trabajo se describirá una metodología basada en normas Cobit 5[1] y en análisis de riesgo tecnológico, la cual recopila y ordena los riesgos inherentes del uso de la tecnología, según la línea del negocio con lo que se logra definir el apetito del riesgo y el riesgo residual, que el uso de la tecnología conlleva, para luego poder definir estrategias, elaborar planes de contingencia, probarlos y saber hasta que punto se ha minimizado el riesgo residual, y con esto determinar cual es el grado de madurez en la mitigación de dichos riesgos.

En el capítulo 1, se describen los antecedentes de riesgos que el uso de la tecnología conlleva, también se detallan las justificaciones del por qué se debe analizar un tema como este, con esta información se describen los objetivos generales y específicos, con los cuales se pretende dar respuesta a las interrogantes que se plantean luego de describir la problemática que el uso de la tecnología puede presentar.

En el capítulo 2, se describe que es un riesgo y que tipos de riesgos pueden existir en el área de tecnología, también se definen, que son vulnerabilidades y que tipos de estas pueden existir. Se describen todas las regulaciones, tanto nacionales como internacionales y las que rigen a instituciones bancarias. Se describirá el enfoque de continuidad de negocio y las metodologías de verificación de grado de madurez. Toda esta información servirá de base para el planteamiento de una metodología que permita medir el grado de mitigación del impacto de los riesgos tecnológicos.

1 COBIT5 proporciona un marco integral que ayuda a las Organizaciones a lograr sus metas y entregar valor mediante un gobierno y una administración efectivos de la TI de la Organización.

En el capítulo 3, se describirá la metodología para medir el grado de mitigación del impacto de los riesgos tecnológicos, la cual se dividirá en 2 grandes áreas, en la primera se analiza el entorno tecnológico de las principales líneas de negocio del banco, y en la segunda se detallan las funciones de la gestión integral de riesgos, luego se identificaran los riesgos, se definirá un método de medición, el cual tendrá como variables, la frecuencia, impacto y riesgo inherente, también se definirán métodos de monitoreo, control y mitigación, al final se elaboraran informes sobre cada uno de estos puntos. Este proyecto también contará con un cronograma de actividades y un presupuesto, si este proyecto fuera contratado con soporte externo.

En el capítulo 4, se elabora una serie de informes de los datos obtenidos de las pruebas de certificación basadas en el análisis del entorno tecnológico y la gestión de riesgo integral, los cuales serán analizados por el comité de riesgo tecnológico, el cual evaluará si con esta metodología se obtienen los resultados esperados, con los cuales se pretende crear una ruta que permita identificar el grado de madurez que se ha obtenido durante el tiempo en los esfuerzos de mitigación del riesgo tecnológico.

En el capítulo 5, basados en los informes generados en el capítulo 4 y después del análisis y consenso del comité de riesgo tecnológico, se concluirá, si con el establecimiento de la metodología, permite medir el grado de mitigación del impacto de los riesgos tecnológicos y se establecerán las bases que permitan implementar y validar los resultados de dicha metodología.

2. ANTECEDENTES

Desde hace ya varios años, se han venido tomando medidas de emergencia o prácticas con el fin de tener una alternativa, si se llegase a presentar un incidente en las áreas de tecnología, a partir de los ataques a las torres gemelas de Nueva York en el 2001, se evidenciaron más, algunos de los problemas a los cuales se podrían enfrentar las empresas con el uso de la tecnología, como por ejemplo; la pérdida de información digital, tanto la que está en funcionamiento en los distintos servidores, como las que se tengan en respaldos.

Esto obligó a definir reglas y normas que ayudaran a minimizar el riesgo de perder información electrónica, basados en los 10 principios de Basilea (Comité de Basilea sobre supervisión Bancaria 2002), los cuales pretenden mitigar los riesgos que el uso de la información por medios tecnológicos conlleva y para lo que se crearon 2 institutos que definieran reglas para poder regular estas actividades, además de dirigir y ordenar estos temas de manejo de la información electrónica, estos son el Instituto de Continuidad de Negocio (Business Continuity Institute, creado en el 2007) y el Instituto para la Recuperación de Desastres (Disaster Recovery Institute, DRI International, creado en el 2004), los cuales se dedican a definir las normas de continuidad de negocio y de recuperación de desastres.

Por otro lado, los estados también se han visto en la necesidad de crear instituciones que regulen y velen por el cumplimiento de dichas normativas, esto con el fin de poder presentarse ante inversionistas extranjeros y entidades internacionales de financiamiento, como un país que vela por el aseguramiento

de la información y tecnología. En Guatemala, solo se ha trabajado en algunas áreas, tales como, la hospitalaria, energía, banca y telecomunicaciones, lo cual es demasiado poco, ya que la globalización, el comercio internacional y el acceso a la información son cada día más exigentes, además de que Guatemala está expuesto a muchos riesgos, que en su mayoría son naturales.

El estado se ha visto obligado a crear instituciones que se dediquen a velar, porque se minimicen estos riesgos y se regule este tipo de actividades, en Guatemala para el área de banca y finanzas, es la Superintendencia de Bancos[2], quienes en los últimos años se han dedicado a la implementación de reglamentos de administración de riesgo tecnológico. (JM-102-2011).

Además de aplicar las normativas internacionales, como Cobit 5 y RiskIT[3], las cuales han servido de guía a la Superintendencia de Bancos de Guatemala para definir su manual de riesgo tecnológico, el cual fue aprobado por la Junta Monetaria en el 2012, con la que se pretende normar estas actividades, este reglamento define que se deben crear planes de continuidad de negocio, en los que se deben analizar las medidas de mitigación, a partir del siniestro más catastrófico, el cual se debe analizar en tres etapas, antes, durante y después del incidente.

El riesgo que una entidad bancaria experimente un incidente en el que se pueda perder la información y las actividades transaccionales de un día normal, son bastante altas, ya que su funcionalidad está basada en el uso de la tecnología informática y de telecomunicaciones, esto lo obliga a recuperase de un incidente tecnológico en el menor tiempo posible.

2 La Superintendencia de Bancos organizada conforme a la ley, es el órgano que ejercerá la vigilancia e inspección de bancos, instituciones de crédito, empresas financieras, entidades afianzadoras, de seguros y las demás que la ley disponga.

3 RISK IT es un marco basado en un conjunto de principios y guías, procesos de negocio y directrices de gestión que se ajustan a estos principios.

Hoy en día, con el avance tecnológico, el poder prevenir o minimizar los riesgos que el uso de la tecnología conlleva, se ha convertido en una prioridad, ya que esto permite mantener la continuidad del negocio y evitar pérdidas económica y reputacionales.

3. DESCRIPCIÓN DEL PROBLEMA

Las instituciones financieras deben contar con una infraestructura tecnológica lo más actualizada posible, además debe ser lo suficientemente robusta para atender todos los requerimientos que los clientes necesiten, ya que cada día es más fácil tener accesos a sistemas informáticos que faciliten las actividades diarias, lo cual ha venido cambiando aceleradamente en los últimos años. Hoy, los usuarios son más exigentes y tienden a preferir los servicios tecnológicos y por ende a las empresas que se encuentren más actualizadas tecnológicamente.

Las instituciones financieras en Guatemala, no escapan a los avances tecnológicos, ya que en este país el acceso a la tecnología es bastante alto, lo que coloca a instituciones como el Banco Internacional a la dependencia en un alto grado del uso de tecnología de la información para poder prestar los distintos servicios financieros que ofrece al público, su infraestructura tecnológica es lo suficientemente robusta y actualizada para prestar de manera ágil los servicios a sus clientes, por lo que para esta institución, se hace necesario gestionar adecuadamente el riesgo tecnológico, para asegurar la integridad, disponibilidad, confidencialidad de la información, así como la continuidad de la prestación de sus servicios.

Una institución bancaria con la infraestructura tecnológica como con la que tiene el Banco Internacional y con los servicios que presta en la República de Guatemala, lo coloca en un grado de exposición al riesgo bastante alta, esto sin mencionar los desastres naturales que en un país como este suceden todos los años.

En lo que respecta a la continuidad del negocio, el Banco Internacional debe desarrollar planes de contingencia para poder restablecer sus servicios en el menor tiempo e impacto posible, para lo que debe prepararse en atender las 3 fases de la continuidad en caso de un evento que paralice sus funciones, estas deben definir planes de acción antes, durante y después del incidente o evento.

Actualmente, Banco internacional cuenta con planes de recuperación de desastres, planes de contingencia, infraestructura tecnológica dual y ya ha realizado eventos de contingencia, aún no cuenta con indicadores que le permitan definir tiempos de recuperación y cuál es el grado de madurez que se ha alcanzado en la mitigación del impacto del riesgo tecnológico, lo cual coloca a la institución en un nivel de riesgo muy alto, además de incumplir con la normativas de riesgo tecnológico de la Superintendencia de Bancos de Guatemala, la cual entrará en vigencia a partir del segundo semestre del 2013 y de incumplirse, se tendrán sanciones, lo que podría repercutir en pérdidas económicas y de reputación.

- Interrogantes del problema

¿Cuál deberá ser la metodología que permita medir el grado de mitigación del impacto de los riesgos tecnológicos?

¿Cuáles son las categorías en que se dividen los distintos tipos de riesgos a que se encuentra expuesta la institución bancaria en cada una de sus líneas de negocio, las cuales afectan los procedimientos operativos y tecnológicos de cada una de esas líneas?

¿Cuál es el impacto que los riesgos inherentes y el riesgo residual representan en cada una de las líneas de negocio del banco?

¿Cuál deberá ser la matriz que agrupe los datos del grado de mitigación del impacto del riesgo tecnológico?

4. JUSTIFICACIÓN

Partiendo de que el uso de la tecnología conlleva riesgos inherentes y de que los bancos del Sistema Financiero de Guatemala, basan su funcionalidad como negocio en el uso de tecnologías informáticas, y de que el ente supervisor de todas las instituciones financieras en Guatemala es la Superintendencia de Bancos, quienes recientemente emitieran que en toda actividad financiera se deben administrar los riesgos inherentes que el uso de tecnología conlleva.

Lo anterior es de suma importancia, ya que permite identificar debilidades en la administración tecnológica de instituciones financieras como el Banco Internacional, el cual cuenta con una infraestructura tecnológica para soportar toda su funcionalidad y servicio a los clientes, lo que lo coloca en una posición de vulnerabilidad y lo posiciona en un nivel de riesgo alto y la única manera de minimizarlo, es a través de definir estrategias de mitigación, elaborar planes de contingencia, probarlos y saber hasta qué punto hemos alcanzado reducir esos riesgos.

Por lo que se hace necesario contar con indicadores que ayuden a identificar el nivel de riesgo residual al que se encuentra expuesta la institución, para lo que un sistema de gestión ayudaría a obtener estos datos de manera más eficiente, con la que se podrán definir estrategias de mitigación.

Adicionalmente, se debe proveer un marco de gestión de riesgo tecnológico, el cual le permita a la institución minimizar la exposición al riesgo tecnológico y le permita disminuir potenciales pérdidas económicas y reputaciones, además de cumplir con las nuevas regulaciones de la

Superintendencia de Bancos, tales como; la resolución de Junta Monetaria, JM-102-2011, la cual se debe implementar antes del 28 de febrero del 2014, ya que a partir de ese día serán una obligatoriedad.

Finalmente se utilizará de base, la normativa Cobit 5, la cual proveerá las herramientas necesarias para establecer la metodología que permita medir el grado de mitigación del impacto de los riesgos tecnológicos del Banco Internacional.

5. OBJETIVOS

General

Establecer una metodología que permita medir el grado de mitigación del impacto de los riesgos tecnológicos, basada en las normativas de continuidad de negocio y recuperación de desastres.

Específicos

1. Categorizar los distintos tipos de riesgo a que se encuentra expuesta la entidad por medio de documentar los distintos procesos vinculados al negocio, a fin de que los procedimientos operativos y tecnológicos sean estandarizados y se establezca que deben ser de cumplimiento obligatorio a nivel de toda la organización.

2. Determinar el impacto de los riesgos en distintos escenarios en función del riesgo asociado a la línea de negocio, por medio de la identificación del riesgo inherente y el riesgo residual.

3. Definir una matriz de evaluación del grado de mitigación del impacto del riesgo tecnológico.

6. ALCANCES

Ante la exposición al riesgo y la necesidad de fortalecer los controles y disponer de nuevas metodologías o herramientas para administrar y controlar los riesgos, esta metodología permitirá administrar en forma proactiva y efectiva los riesgos que se toman en la gestión del día a día del negocio. Se analizará el marco teórico, en el que se desarrolla la gestión de riesgos, la cual, apegada a las normas y a las mejores prácticas para la gestión de los diferentes riesgos a los que el banco está expuesto, generará varios benéficos, tales como; una adecuada admiración integral de riesgos y una reducción de pérdidas operacionales y reputacionales.

En esta investigación se establecerá una metodología para medir el grado de mitigación del impacto de los riesgos tecnológicos en el Banco Internacional, la cual pretende resolver el problema que la falta de información del estado de exposición, al riesgo tecnológico conlleva, dicha metodología regulará el ámbito de acción de la gestión de riesgos tecnológicos, y establece pautas para los aspectos técnicos y metodológicos. Se avanzará hasta la definición de una matriz de evaluación del grado de mitigación del impacto del riesgo tecnológico, quedando pendiente la fase de implantación y validación de esta metodología.

7. BOSQUEJO DE TEMAS

ÍNDICE DE ILUSTRACIONES
LISTA DE SÍMBOLOS
GLOSARIO
RESUMEN
INTRODUCCIÓN
ANTECEDENTES
DESCRIPCIÓN DEL PROBLEMA
JUSTIFICACIÓN
OBJETIVO GENERAL Y ESPECÍFICOS
ALCANCES

1. MARCO TEÓRICO
    1.1. Definición de riesgos
    1.2. Tipos de riesgos
    1.3. Definición de vulnerabilidades
    1.4. Regulaciones internacionales
    1.5 . Regulaciones nacionales
    1.6 . Enfoque en instituciones bancarias
    1.7 . Enfoque en continuidad de negocio
    1.8 . Metodología para verificación del grado de madurez

2. METODOLOGÍA
    2.1. Análisis de entorno
    2.2. Implementación de la solución

CRONOGRAMA

PRESUPUESTO

BIBLIOGRAFÍA

8. MARCO TEÓRICO

8.1. Definición de riesgos

- Riesgos

El riesgo en general, está definido como la probabilidad de que una amenaza, peligro o incertidumbre, a que se ve enfrentada una persona o institución, por efecto o acción relacionada con sus líneas de negocio, operaciones y demás actividades, que pudieran afectar su situación actual.

- Riesgos de TI

Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización. Otros de los riesgos a los que una organización se enfrenta; pueden ser estratégicos, ambientales, de mercado, de crédito, riesgos operativos y de cumplimiento.

En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo, por ejemplo, el sector financiero en el marco de Basilea II[4]. Sin embargo, incluso el riesgo estratégico de TI puede tener un componente financiero, especialmente en aquellas organizaciones en las que es el elemento clave de nuevas iniciativas empresariales. Lo mismo se aplica para el riesgo de crédito, donde una política pobre en cuanto a seguridad de la información se refiere, puede conducir a

4 Basilea II es el segundo de los Acuerdos de Basilea. Dichos acuerdos consisten en recomendaciones sobre la legislación y regulación bancaria y son emitidos por el Comité de supervisión bancaria de Basilea.

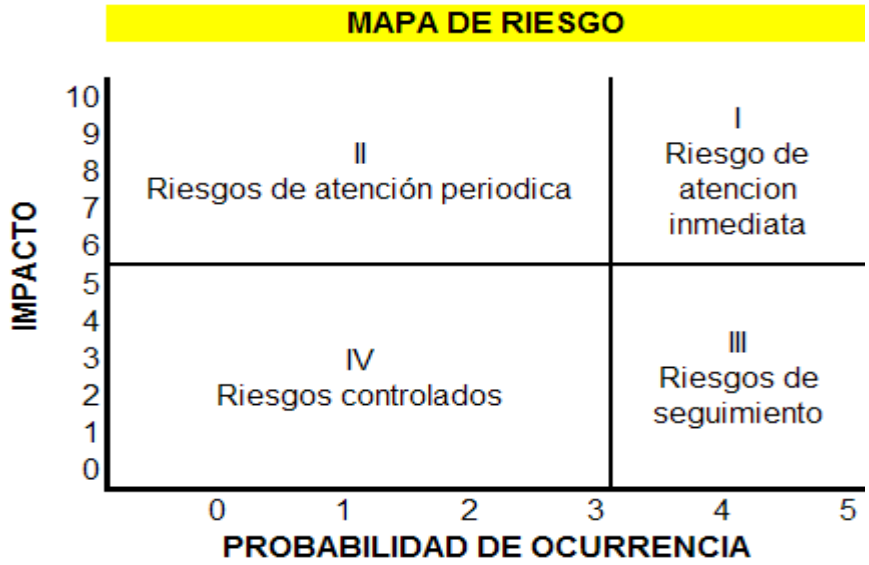
menores calificaciones de crédito. Por esta razón, es mejor no describir los riesgos de TI, con una dependencia jerárquica en una de las categorías de riesgo, sino orientado a la industria financiera.

RISK IT, es el riesgo comercial, es decir, el riesgo de los negocios asociados con el uso, la propiedad, la operación, la participación, la influencia y la adopción de las TI dentro de una organización. Se compone de eventos relacionados con IT que podrían afectar a la organización. Esto incluye tanto la frecuencia y la magnitud incierta, la creación de problemas en el cumplimiento de metas y objetivos estratégicos, así como la incertidumbre en la búsqueda de oportunidades. Los riesgos pueden clasificarse de varias formas.

El valor de los riesgos de TI permitidos, asociado con las oportunidades no aprovechadas para mejorar la eficiencia o efectividad de los procesos de negocio, o la capacidad de soportar nuevas iniciativas, a través del uso de la tecnología. Programas de TI y riesgos en las entregas de proyectos, asociada a la contribución de IT sobre nuevas soluciones de negocio, generalmente en forma de proyectos y programas.

Operaciones de TI y riesgos en las entregas de servicios, asociadas con todos los aspectos relacionados con los servicios y sistemas de TI, los cuales puede producir pérdidas o reducción del valor a la organización. Los riesgos relacionados de TI existen, independientemente de si son descubiertos o reconocidos por una organización. En este contexto es importante identificar y gestionar potencialmente los asuntos importantes de riesgo de TI, a diferencia del resto de riesgos, ya que éste puede no ser rentable. (Marco de Riesgo de TI 2009).

Tabla I. **Mapa de riesgo según el impacto y ocurrencia**



Fuente: elaboración propia.

- Propósito del marco de trabajo de riesgo de TI

La correcta gestión de los riesgos a los que está expuesta la organización, es esencial para la correcta administración de cualquier organización. Casi todas las decisiones de negocio, requieren que la alta dirección o los gerentes sopesen los riesgos y los beneficios.

El uso común y general de las TI puede proporcionar importantes beneficios a una organización, pero también implica riesgos. Debido a su importancia para las organizaciones, los riesgos relacionados con TI deberían ser tratados como los demás riesgos claves organizacionales, tales como el riesgo del mercado, de crédito y otros riesgos operativos.

Dichos riesgos se pueden ubicar por debajo de la categoría más crítica de los riesgos en una organización: el hecho de no lograr los objetivos estratégicos del negocio. Si bien estos riesgos han sido incorporados a las organizaciones en los procesos de toma de decisión, muchos ejecutivos tienden a relegar los riesgos a los especialistas técnicos.

El marco de riesgos de TI, explica los riesgos y permite a los usuarios:

- Integrar la gestión de los riesgos en el ERM de la organización, esto permitirá que se tomen decisiones conscientes sobre el retorno de los riesgos.

- Tomar decisiones con conocimiento acerca de la magnitud del riesgo, el apetito de riesgo y la tolerancia al riesgo de la organización.

- Entender cómo responder a los riesgos. (Marco de Riesgo de TI 2009).

8.2. Tipos de riesgos

- Enfoque en riesgo tecnológico

El riesgo tecnológico, entendido como un elemento constitutivo del amplio conjunto de consideraciones inevitablemente ligadas al devenir científico-tecnológico, emerge como un síndrome de advertencia, de reflexión sobre el nivel de incidencia de la tecnología en las sociedades modernas. Estas últimas, susceptibles de ser interpretadas como “sociedades del riesgo” (Beck, 1998, 2002), se encuentran fuertemente caracterizadas por la proliferación de situaciones socialmente conflictivas, derivadas tanto del progreso

tecnocientífico, como de la propia complejidad de la organización social. (Ramírez, O. J. 2009).

Algunos autores concuerdan en afirmar que el impulso de la investigación contemporánea del riesgo de procesos tecnológicos, en un sentido estricto, estuvo íntimamente relacionada con el desarrollo forzado de la energía nuclear a comienzos de los años 60 y con el conjunto de debates asociados (Rodríguez, 1999; López; Luján, 2000). Desde los años 70 emergió una ola sin precedentes de gran interés público y académico por el estudio del riesgo, lo cual se tradujo en la aparición de numerosas revistas, organizaciones de sociedades profesionales, celebración de congresos, desarrollo de cursos especializados, etcétera, constituyéndose el estudio del riesgo en un importante campo multidisciplinario de investigación y reflexión académica.

Vista desde una perspectiva amplia, la tecnología ha sido una fuerza poderosa en el desarrollo de la civilización occidental, más aún, cuando se ha fraguado su vínculo con la ciencia. Aumentando las posibilidades de incidir y alterar el mundo, el ser humano se ha servido de la tecnología para acondicionar su entorno, a fin de que se adapte mejor a sus necesidades. No obstante, algunos de los resultados de tales intervenciones, son con frecuencia confusos e impredecibles, llegando a incluir no sólo beneficios o costos económicos a mediano y largo plazo, sino también, y especialmente, riesgos con la capacidad de afectar a diferentes grupos sociales en distintos momentos**.**

El riesgo, en este sentido, se ha convertido en la noción clave sobre la que pivota gran parte de los diagnósticos sociales (sean estos económicos, políticos, técnicos, jurídicos o sociológicos), pasando a ocupar tal concepto un lugar relevante dentro de los debates contemporáneos. Gracias a ello, el desarrollo tecnocientífico de las sociedades modernas ha puesto en evidencia

la presencia de riesgos, que van más allá de los naturales conocidos hasta ahora por la humanidad.

A los clásicos riesgos ligados a los elementos naturales, tales como; inundaciones, incendios, sequías, etcétera, se agregan en la actualidad aquellos que son producto exclusivo de la actividad humana, tales como; la energía nuclear, las ondas electromagnéticas, la ingeniería genética, la informática, la nanotecnología, los numerosos procesos basados en la utilización de compuestos químicos y, como parte de estos últimos, la amplia e intensiva utilización de plaguicidas en sistemas agrícolas, entre otros.

Hacer frente a los llamados riesgos tecnológicos de tipo antropogénico[5], permite reconocer cómo de forma simultánea al avance del conocimiento científico se extiende, paradójicamente, enormes vacíos cognitivos y profundas lagunas de ignorancia e incertidumbre.

Si bien, a la luz de una multitud de variables es posible admitir que cuantiosas innovaciones tecnológicas han contribuido efectivamente al mejoramiento de un sin número de circunstancias desfavorables (motivando un papel activo de la sociedad para enfrentar situaciones adversas), también es posible asentir que a la sombra de tales procesos se generan iniciativas nocivas, riesgosas e inciertas con explícitos y potenciales efectos sobre la sociedad.

En palabras de López y Luján: es el nuevo mundo del riesgo asociado a la ciencia y la tecnología actual: cuanto más conocemos los riesgos, mejor apreciamos la gran extensión de nuestra ignorancia; cuanto más hacemos por

5 El término antropogénico se refiere a los efectos, procesos o materiales que son el resultado de actividades humanas a diferencia de los que tienen causas naturales sin influencia humana.

controlarlos, mayores son los riesgos generados en otra parte del sistema *(*López y Luján *2000:13).*

De esta forma, el propio discurso tecnológico parece avanzar en medio de una conflictiva relación formulada en términos de afecto/rechazo: afecto, al avizorar la sociedad el amplio abanico de posibilidades inimaginables emergidas tras su vertiginoso avance, y al ofrecer ésta (la tecnología) soluciones temporales a calamidades expuestas. Y rechazo, al estimular la aparición de un conglomerado de situaciones confusas y amenazantes, y al suscitar peligros y situaciones no deseadas como parte de este mismo proceso.

Tal relación, es enunciada por el filósofo alemán Nicholas Rescher de la siguiente manera: por una parte, sólo ella [la tecnología] es capaz de proporcionarnos los requisitos para hacer posible la vida humana dentro de las condiciones del mundo moderno. Por otra parte, la tecnología misma hace que, de muchas maneras, la vida sea más complicada, menos agradable y más peligrosa *(Rescher, 1999:46).*

- Enfoque en riesgo financiero

Debido a lo extenso y variado que puede resultar el estudio de los riesgos, se requiere una presentación metódica con el propósito de facilitar su entendimiento. En el caso que ocupa, el ente regulador ha establecido y desarrollado dicha clasificación, de la siguiente manera: (JM-56-2011).

  - Riesgo de crédito: es la contingencia de que una institución incurra en pérdidas como consecuencia de que un deudor o contraparte incumpla sus obligaciones en los términos acordados.

- Riesgo de liquidez: es la contingencia de que una institución no tenga capacidad para fondear incrementos en sus activos o cumplir con sus obligaciones oportunamente, sin incurrir en costos financieros fuera de mercado.

- Riesgo operacional: es la contingencia de que una institución incurra en pérdidas, debido a la inadecuación o a fallas de procesos, personas, los sistemas internos o bien a causa de eventos externos. Incluye los riesgos tecnológicos y legales.

- Riesgo tecnológico: es la contingencia de que la interrupción, alteración o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, provoque pérdidas financieras a la institución.

- Riesgo de mercado: es la contingencia de que una institución incurra en pérdidas como consecuencia de movimientos adversos en precios en los mercados financieros. Incluye los riesgos de tasa de interés y cambiario.

- Riesgo país: es la contingencia de que una institución incurra en pérdidas, asociada con el ambiente económico, social y político del país donde el deudor o contraparte tiene su domicilio y/o sus operaciones. Incluye los riesgos soberano, político y de transferencia.

8.3. Definición de vulnerabilidades

- Tipos de vulnerabilidades

  - Análisis de vulnerabilidades

En esta etapa se analizan las fallas de seguridad en el entorno, según los estándares internacionales referenciados en la bibliografía de este trabajo. Se

considera una vulnerabilidad a toda diferencia entre los parámetros deseados recomendados por dichos estándares y las mejores prácticas profesionales en cuanto a Seguridad Informática. Los objetivos de control considerados, según [IRAM/ISO/IEC17799], [BS7799], [Cobit], [MRSA-ISACA], [AAW-ISI], [OSSTMM-ISECOM] y [AACF-ROBOTA] son los siguientes:

- Aspectos funcionales
  - Que exista una adecuada definición de funciones y estructura de comunicación en el área.
  - Que las tareas incompatibles sean adecuadamente segregadas.
- Que existan licencias de uso del producto para cada recurso / usuario.
- Que las aplicaciones activas en el entorno contribuyan a perseguir los objetivos del negocio.
- Que se haya definido y documentado un modelo de administración de la seguridad.
- Que existan estándares y procedimientos de trabajo definidos para todas las tareas del área.
- Que el circuito de trabajo responda a criterios de seguridad, eficiencia y productividad.

- Que los procedimientos adoptados estén de acuerdo con normas estándares en la materia.

- Que estén definidos y se encuentren documentados para cada puesto del organigrama, perfiles de usuario modelo a los cuales se les asocian las identificaciones individuales de cada persona.

- Que los equipos informáticos sean utilizados sólo con fines autorizados y siguiendo los procedimientos establecidos.

- Que todo procesamiento esté debidamente autorizado por los responsables correspondientes.

- Que existan procedimientos de control de los resultados que surgen del procesamiento en los equipos.

    - Que existan estándares definidos a seguirse para la realización de pruebas de los desarrollos y/o mantenimientos, que contemplen:

        - ✓ La realización de pruebas de detalle por parte de personal de sistemas, antes de ser probados por personal de las áreas usuarias.

        - ✓ La realización, por parte de personal de las áreas usuarias, de la definición de los casos, ejecución de las pruebas, análisis de los resultados, interfaces, corridas mensuales y anuales, etc. antes de la implantación.

- ✓ La forma de documentación de la participación y validación de los resultados de las pruebas.

- ✓ Los requerimientos en cuanto a niveles de autorización para su implantación en el ambiente productivo.

- El procedimiento de implantación de producción

  - Que el acceso a la documentación de los sistemas de aplicación de producción, sólo se permita a personal autorizado.

  - Que exista un encargado de soporte del mantenimiento para las aplicaciones analizadas.

  - Que existen adecuados procedimientos manuales o automatizados de control de cambios a los programas.

  - Que existen cláusulas de confidencialidad en los contratos con los proveedores de software y/o terceros que trabajen en las aplicaciones.

Este análisis permitirá visualizar el nivel de adhesión que tiene la estructura del proceso a los estándares metodológicos que se tengan establecidos para el desarrollo y mantenimiento, así como para la documentación de las etapas del proceso. Además se podrán establecer los criterios que fueron utilizados para definir y establecer las características de los controles internos y las validaciones. El análisis funcional permite visualizar las distintas etapas que se suceden en el proceso, así como también identificar etapas de alto, medio y bajo riesgo.

Para verificar estos puntos de control su equipo de trabajo puede realizar las siguientes tareas:

- Revisar la documentación del proceso de negocio de la empresa, objetivo con el fin de conocer su estructura y funcionamiento.

- Entrevistar a los analistas/programadores/técnicos responsables del mantenimiento de las aplicaciones y equipos y comparar el procedimiento que cada uno está aplicando.

- Entrevistar a los analistas/programadores responsables del desarrollo/mantenimiento, de las aplicaciones, así como al personal usuario, a efectos de obtener una visión global del mismo, tanto en su fase manual como automática.

- Entrevistar a los analistas/programadores/técnicos responsables del desarrollo/mantenimiento de las aplicaciones, y equipos para validar la adecuada concientización del personal a fin de cumplir con la documentación vigente.

Obtener de los usuarios y de los analistas, información adicional sobre el entorno a relevar, tal como:

- Satisfacción funcional de los requerimientos de información de los usuarios.

- Tiempos de procesamiento y de generación de salidas.

- Experiencias anteriores sobre procesamiento de errores.

- Confianza de los usuarios en la información que manejan estos equipos y aplicaciones.

- Para ello se pueden distribuir encuestas de evaluación del funcionamiento de las aplicaciones y equipos entre personal del área de sistemas y de sectores usuarios.

- Obtener información sobre trazas de auditoría, históricos de archivos generados por los sistemas y procedimientos de emergencia, de reenganche y de procesamiento alternativo disponible.

- Conocer los procesos y funciones de administración de las bases de datos y de back-up de archivos y programas (fuentes y ejecutables) de cada una de las aplicaciones.

Entrevistar a ciertos usuarios finales, elegidos al azar a efectos de verificar cuán involucrados están con las distintas fases de desarrollo/mantenimiento de sistemas (diseño, desarrollo, prueba y aceptación). Además, se obtendrá de los usuarios finales la siguiente información:

- Nivel de participación con relación a la calidad de los servicios.

- Problemas detectados durante el último año.

- Asignaciones incorrectas de acceso a los archivos de datos y a las transacciones de las aplicaciones *on-line.*

- Relevar y probar los procedimientos de administración, control de los cambios efectuados a las aplicaciones, e identificar a los responsables de llevar a cabo los mismos.

- Identificar y entrevistar al personal responsable de implantar cambios, de realizar controles sobre las incidencias que involucren las aplicaciones, para verificar que se cumpla con los procedimientos vigentes.

- Solicitar (en caso de existir) y analizar el *log* utilizado para priorizar y monitorizar la recepción y progreso de los cambios de sistemas.

Solicitar y analizar muestras de documentos relacionados con modificaciones de los programas:

- Documentos aprobados por los supervisores de desarrollo, autorizando la puesta en producción de los programas modificados.

- Documentos que demuestren que los usuarios finales han aprobado los desarrollos/modificaciones efectuados antes de migrar los nuevos programas al área de producción.

- Formularios o memorándums que formalmente comuniquen el orden de ejecución de los programas modificados (Job step) al área de operaciones.

- Identificar una muestra de requerimientos de cambios a las aplicaciones relevadas en el *log* requerido y verificar que para cada uno de ellos se haya complementado adecuadamente el procedimiento de modificación de programas y catalogación en producción, con su respectivo control.

8.4. Regulaciones internacionales

- Reglamentos y normas

En los años 70, el crecimiento de mercados financieros internacionales y el flujo de dinero entre países, realzaron la falta de una supervisión bancaria efectiva a un nivel internacional. Las autoridades de supervisión bancaria, básicamente regulaban bancos domésticos y las actividades domésticas de bancos internacionales, mientras que las actividades internacionales de estos bancos no eran siempre supervisadas de cerca. El colapso en 1974 del Bankhaus Herstatt en Alemania y del Franklin National Bank en Estados Unidos exhortó a los gobernantes de 10 bancos centrales a crear el Comité de Basilea para Supervisión Bancaria. (Coronel Hoyos, K. D. R. 2008).

El Banco de Pagos Internacionales (BIS por sus siglas en inglés: Bank for International Settlements), es la institución financiera internacional más antigua del mundo y sigue siendo el centro principal para la cooperación de bancos centrales internacionales y la búsqueda de la estabilidad financiera y monetaria. Además, da soporte al trabajo de los comités y organizaciones basados en Basilea, siendo un enlace de distribución de información estadística bancaria, de seguridades, tipos de cambio y mercados derivados.

En 1988 el Comité de Basilea, emitió el Acuerdo de Capital de Basilea, introduciendo un marco de trabajo que se convirtió en un estándar globalmente aceptado. La mayoría de países en el mundo, adoptaron las recomendaciones emitidas por el BIS en el acuerdo de 1988. Una revisión de este acuerdo de capital en el 2004, conocido como Basilea II, incluyó en sus estándares el riesgo operativo. Tales estándares, que se están implementando a nivel

mundial desde finales del 2006, apuntan a lograr una mejor y más transparente medición de varios riesgos a los que se enfrentan las instituciones financieras, limitando la posibilidad de contagio en caso de una crisis y fortaleciendo la infraestructura financiera global.

Internacionalmente, el marco de trabajo de COBIT y todos los productos y publicaciones relacionados que emitió el ITGI, guía a las organizaciones en la implementación de un adecuado gobierno de TI que garantice el cumplimiento de los objetivos del negocio por medio del valor agregado que debe brindar la tecnología de información, la administración de los riesgos y recursos y la medición del desempeño.

Además integra estándares internacionales generalmente aceptados como COSO, ITIL, ISO 9001, ISO 27002, AS/NZ 4360:8 2004, etc., que lo convierten en un marco de trabajo completo y alineado con las mejores prácticas relativas a la tecnología de información. El presente trabajo se orienta a buscar una solución, adoptando para ello las mejores prácticas que el marco de trabajo de COBIT 4.1 puede aportar en ese tema.

8.5. Regulaciones nacionales

- Reglamentos y normas

Artículo 55 de la Ley de Bancos y Grupos Financieros, Decreto No. 19-2002 del Congreso de la República. El referido artículo norma lo relacionado con la administración de riesgos y establece que los bancos y las empresas que integran grupos financieros, deberán contar con procesos integrales que incluyan, según el caso, la administración de riesgos de crédito, de mercado, de tasas de interés, de liquidez, cambiario, de transferencia, operacional y otros a

que estén expuestos, que contengan sistemas de información y un comité de gestión de riesgos, todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos.

Resolución JM-56-2011 Reglamento para la Administración Integral de Riesgos. Este reglamento tiene por objeto regular los aspectos mínimos que deben observar las entidades, con relación a la administración integral de riesgos.

Otras normativas relacionadas con riesgos:

- Resolución JM-93-2005 Reglamento para la Administración del Riesgo de Crédito.

- Resolución JM-117-2009 Reglamento para la Administración del Riesgo de Liquidez.

- Resolución JM-134-2009 Reglamento para la Administración del Riesgo Cambiario Crediticio.

- Resolución JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico.

8.6. Enfoque en instituciones bancarias

- Antecedentes

El riesgo en general está definido como la probabilidad de que una amenaza, peligro o incertidumbre, a que se ve enfrentada una institución, en este caso bancaria, por efecto o acción relacionada con sus líneas de negocio, operaciones y demás actividades, que pudieran afectar su situación financiera. La administración de riesgos, es el proceso mediante el cual se identifican, miden, monitorean, limitan, controlan, previenen, mitigan e informan los distintos tipos de riesgo a que se encuentran expuestas las entidades bancarias, teniendo como instrumento un conjunto de políticas, procedimientos y sistemas. (JM-102-2011)

El intento exhaustivo por minimizar el riesgo de cualquier tipo, es una tarea del día a día. Se prevé mantener una cultura de riesgo, buscando crear conciencia en torno al mismo, adoptando igualmente las prevenciones en los casos posibles por parte de todos sus colaboradores. Considerando que para el desarrollo normal de sus actividades, los bancos dependen en un alto grado del uso de tecnología de la información, lo que hace necesario gestionar adecuadamente el riesgo tecnológico para asegurar la integridad, disponibilidad, confidencialidad de la información, así como la continuidad de la prestación de sus servicios.

Se debe proponer un modelo para la medición del riesgo tecnológico, que se sustente en una visión sobre las amenazas tecnológicas, a que está expuesta la institución y en la necesidad de afianzar la cultura de evaluación de dichos riesgos en el banco y de minimizar el impacto de los mismos.

Derivado que en toda actividad financiera se deben administrar los riesgos, la Ley de Bancos y Grupos Financieros, en su artículo 55, establece que los bancos deberán contar con procesos integrales para la administración de los riesgos de crédito, mercado, tasas de interés, liquidez, cambiario, transferencia, operacional y otros a que estén expuestos. Por otra parte, la Resolución JM-102-2011 Reglamento para la Administración del Riesgo Tecnológico, emitida por Junta Monetaria, establece lineamientos generales para la adecuada gestión de riesgos tecnológicos.

- Administración integral de riesgos

La administración integral de riesgos, es el proceso de identificar, medir, monitorear, controlar, prevenir y mitigar los distintos riesgos, entre éstos, el riesgo de crédito, liquidez, mercado, operacional y otros inherentes al negocio, así como evaluar la exposición total a los mismos. (Minguillon Roy, A. 2010).

El proceso incluye lo siguiente:

- Supervisión activa por parte de la auditoría interna, cumplimiento, riesgo integral y por el consejo de administración.

- Desarrollo de políticas, procedimientos y sistemas para la administración integral de riesgos.

- Identificación, medición y monitoreo de los distintos riesgos y definición de sistemas de control.

- Auditorías y controles internos integrales, a efecto de prevenir y mitigar los diferentes riesgos.

Se deben identificar los factores externos que pueden motivar potencialmente cambios importantes en los riesgos, aún y cuando las políticas puedan definirse como conservadoras.

Dentro de estos factores están: macroeconómicos como la inflación, riesgo político, riesgo sectorial, riesgo de tasa de interés, riesgo de liquidez, etcétera. De este modo, todos los riesgos mencionados pueden tener un impacto sobre las operaciones que realice el banco.

La gestión de riesgos considera dos premisas claramente relacionadas:

Gestionar los riesgos, basados en el principio de la misión de transparencia y en los valores institucionales de honestidad y pasión por la excelencia; y según el objetivo de alto nivel del área de riesgo y entorno, de ejercer la gestión del riesgo integral del negocio con prudencia y calidad.

A través de lo anterior, la institución incorpora la gestión de riesgos como un elemento estratégico permanentemente relacionado con la gestión de negocios, y refleja la conciencia de la administración acerca del valor agregado en el tiempo, que representa el adecuado manejo de riesgos.

- Elementos del sistema de administración integral de riesgos

    - Políticas para la administración integral de riesgos

Se consideran políticas y estrategias, al conjunto de actividades y procedimientos o formas de dirección de los procesos que se crean con el fín de alcanzar los objetivos establecidos.

De manera general, las políticas para la gestión integral de riesgos son las siguientes:

- Debe contar con un Departamento de Riesgo Integral, que garantice la existencia de herramientas y metodologías para la adecuada administración de los diferentes riesgos a los que está expuesto.

- El análisis y evaluación de tendencias de riesgos, el planteamiento o modificación de políticas de riesgos, así como el resultado de la evaluación de políticas de riesgos, serán reportados por el Departamento de Riesgo Integral al Comité de Riesgo Integral. Dicho comité es un órgano técnico que tiene a su cargo la dirección de la administración integral de riesgos, y somete a aprobación del consejo de Administración del banco, las evaluaciones y documentación emanada por el Departamento de Riesgo Integral.

- En el desarrollo de nuevos productos y servicios del banco, y previo al lanzamiento de los mismos, se debe realizar la evaluación general de riesgos de dichos productos y servicios.

- Las políticas específicas de cada riesgo constan en los manuales individuales del riesgo que se trate; y, las mismas deben ser actualizadas periódicamente, como mínimo, cada año. Dichas políticas serán aprobadas por el Consejo de Administración del banco.

- La política de cada riesgo particular debe considerar diferentes niveles de autorización de operaciones y asegurar una adecuada segregación de funciones.

- Para el control de cada riesgo particular, debe llevarse un registro y seguimiento de excepciones, a fin de comunicarlas oportunamente y tomar las medidas correctivas que sean necesarias.

- Deben establecerse límites de tolerancia para cada riesgo, que el banco esté en capacidad de asumir. Dichos límites de tolerancia deben definirse en los manuales específicos de cada riesgo individual.

- El banco debe disponer de sistemas de información que proveen a la alta administración y a las áreas involucradas, de toda la información necesaria para tomar decisiones oportunas y adecuadas para el manejo de los diferentes riesgos.

- Metodologías para la gestión de riesgos

Las metodologías se refieren al conjunto de operaciones organizadas, con las que se pretende el logro de la medición de riesgos; y, tienen como propósito:

  - Identificar, medir, monitorear, controlar e informar los distintos tipos de riesgo a que se encuentra expuesta la entidad.

  - Determinar el impacto de los riesgos en distintos escenarios en función del riesgo que se trate.

- Límite de exposición o tolerancia al riesgo

Es el nivel máximo de exposición total a riesgos específicos, cuya exposición se define en términos cuantitativos, que pueden ocasionar pérdidas a la institución, que la misma está dispuesta y en capacidad de asumir, tomando en cuenta su plan estratégico, condición financiera y su rol en el sistema financiero.

Este límite de exposición no debe ser interpretado como un nivel de pérdida permisible, ya que el hecho de que una pérdida no agote el límite establecido, no exonera de responsabilidad a los funcionarios involucrados. Los límites constituyen una guía para la alta dirección que le permite una toma de decisiones oportuna, en relación a la ejecución de una actividad. La definición de los límites de tolerancia, se incluirá en los manuales específicos de cada riesgo particular, y su métrica puede establecerse en función del volumen de ingresos, resultados, capital del banco, posición patrimonial o bien, otro rubro representativo que guarde relación estrecha con el riesgo que se trate.

- Infraestructura y sistemas de información

Se refiere a las bases de funcionamiento del sistema de administración integral de riesgos, entendiéndose por ello a los recursos de orden humano, financiero y tecnológico que resulten necesarios para la adecuada gestión de riesgos, y establecer una organización de carácter funcional que permita el ejercicio de las diferentes actividades, a fin de garantizar el cumplimiento de los objetivos de la organización.

8.7. Enfoque en continuidad de negocio

- Descripción general

Continuidad del negocio – Recuperación de desastres (BCM – Business Continuity Management / DRM – Disaster Recovery Management):

El proceso de identificar, prevenirse y prepararse para los eventos que puedan interrumpir las actividades del negocio. Business Continuity Management (BCM) – Administración de la continuidad del negocio involucra a toda la organización y se enfoca en procesos de negocio, recurso humano, terceros y tecnología.

Incorporación de estándares y mejores prácticas reconocidos internacionalmente en relación con la continuidad y disponibilidad del negocio incluyendo el DRI – Disaster Recovery Institute, el BCI –Business Continuity Institute y el estándar BS25999.

- Diagnóstico – BCM Health Check

Analiza su estado actual en la definición, desarrollo, y gestión de la continuidad de los procesos críticos de negocio, así como de los servicios y la infraestructura tecnológica de la organización.

Estudia e identifica las brechas y oportunidades de mejora frente a los estándares y las mejores prácticas asociados a la continuidad y disponibilidad de los servicios de TI (DRI, NIST, ISO 27001, NFPA, BCMM).

A partir de los resultados obtenidos en el diagnóstico se definen los siguientes aspectos:

- Brechas identificadas.

- Definiciones o actividades a desarrollar o fortalecer dentro del Plan de Recuperación de Desastres – DRP.

- Planes de acción u oportunidades de mejora identificadas en relación a la continuidad de los servicios de TI y la disponibilidad de la infraestructura tecnológica.

- Evaluación de riesgos – continuidad y disponibilidad

Se identifican y evalúan los riesgos que afectan la continuidad y disponibilidad de los procesos críticos y de los servicios e infraestructura de TI.

En relación con los servicios e infraestructura tecnológica se consideran aspectos como:

- Problemas de desempeño, capacidad, disponibilidad de los servicios y recursos tecnológicos.

- Obsolescencia tecnológica e ineficacia de la plataforma tecnológica.

- Problemas o fallas en las actividades y procesos asociados a la operación de la plataforma tecnológica.

- Fallas en la plataforma tecnológica por accidentes, daños o siniestros.

- Fallas en servicios de comunicaciones.

- Pérdida de información o datos históricos de los sistemas de información.

- Fallas de hardware o software.

- Fallas por desastres naturales.

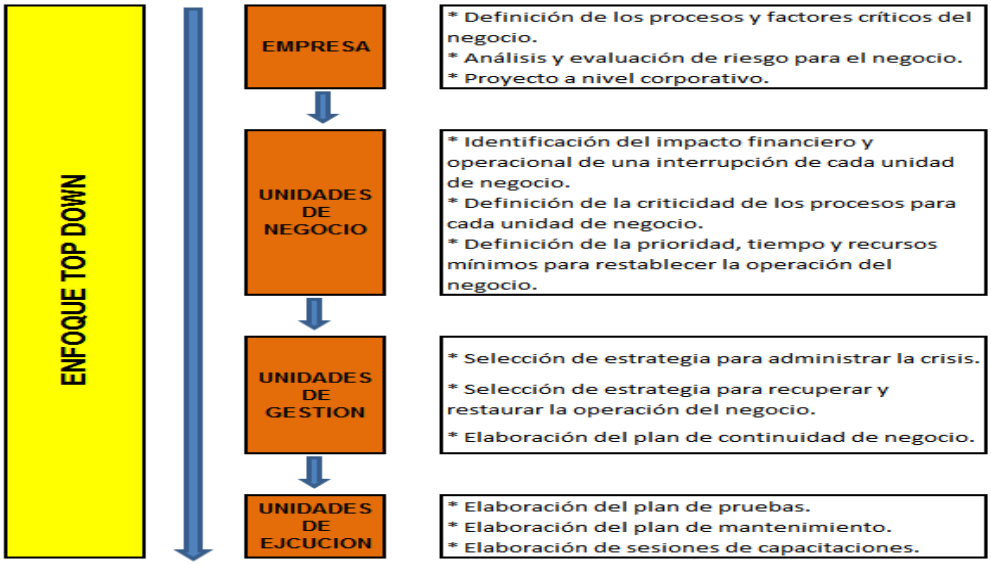
- Desarrollo BCM / BCP / DRP

Como respuesta al reto de responder a escenarios de falla, manteniendo la continuidad de las operaciones críticas y la disponibilidad de los servicios e infraestructura tecnológica hemos desarrollado un enfoque viable y práctico.

- Mantenimiento y sostenibilidad BCM / BCP / DRP – Outsourcing

Adicional al desarrollo de proyectos de continuidad de negocios y recuperación de desastres, se deben realizar actualizaciones, mantenimientos y mejora continua de las estrategias, equipos y procedimientos de recuperación definidos. Para la actualización y mantenimiento de los planes de continuidad de negocio, se pueden utilizar herramienta *BCM Expert*, que permite la gestión de los diferentes componentes por medio de la definición de flujos de trabajo que se integran con los equipos de recuperación definidos.

Figura 1. **Enfoque Top Down**



Fuente: Business Continuity Institute 2002.

8.8. Metodología para verificación del grado de madurez

- Modelo de madurez de dominio (rr)

  - 0 - No existente cuando

La organización no ha reconocido la necesidad de administrar las cuestiones de riesgos y las exposiciones al negocio y sus operaciones. No hay procesos de crisis de comunicación que estén en su lugar. Seguimiento de control interno no existe. No hay conciencia de los requisitos externos para implementar los controles, capacidades y recursos para limitar la frecuencia y el impacto (magnitud de la pérdida) de los acontecimientos relacionados con las TI. (Cobit5 2012).

- 1- Inicial cuando

El reconocimiento de la necesidad de una respuesta de riesgo, está surgiendo, pero es visto como limitado a evitar riesgos, para cumplir con los requisitos de cumplimiento y transferencia a través de seguros. Hay conciencia individual mínima de las amenazas y de qué hacer en caso de que se materialicen.

Existe una responsabilidad mínima para garantizar que las medidas razonables de respuesta de riesgos están en el lugar y reflejan el ambiente de amenaza y los valores de los activos. Eventos de TI relacionados y condiciones que podrían afectar el día a día las operaciones, en ocasiones se discuten en las reuniones de gestión, pero las respuestas de riesgo específicos no se consideran.

Los controles de TI existen, pero se basan en requisitos de cumplimiento, varían ampliamente en relación al riesgo y operar en silos aislados. La falta de habilidades y competencias para la respuesta de riesgo, puede obligar a la empresa a aceptar el riesgo más allá de los niveles de tolerancia, cuando las propuestas de valor son particularmente convincentes.

- 2 - Repetible cuando

Hay conciencia individual de las amenazas y los puntos de contacto para la dirección cuando se materialicen. La respuesta en cuestiones de riesgos de TI, son comunicadas por la gestión, pero las discusiones de respuesta de riesgo de TI pueden verse afectadas por la competencia, por un lenguaje de unidad de negocio de riesgo específico. Hay un líder emergente para la respuesta de

riesgo de TI, asume la responsabilidad para mitigar los riesgos y ayudar a gestionar el impacto de los acontecimientos.

Deficiencias de control pueden ser identificados, pero no se remedian en forma oportuna. Los procesos de reducción del riesgo están comenzando a ponerse en práctica cuando se detecten problemas de TI de riesgo. Requisitos de formación mínimos son identificados para las áreas críticas de la articulación de riesgos, mitigación y gestión de crisis. Existen enfoques comunes para el uso de herramientas de mitigación y respuesta de riesgos, pero se basan en las soluciones desarrolladas por los individuos clave.

- 3 - Definida cuando

A través de la organización hay comprensión individual del impacto de las amenazas de negocio y las acciones específicas a tomar en caso de que se materialicen las amenazas de negocio. Responsabilidad y rendición de cuentas para las prácticas de respuesta clave de riesgo, se definen y los dueños del proceso han sido identificados.

Las deficiencias de control son identificadas y remediadas de manera oportuna. Una empresa en toda la política de respuesta a los riesgos define cuándo y cómo responder a los riesgos. Las descripciones de trabajo incluyen las expectativas de respuesta a los riesgos.

Los empleados son capacitados periódicamente en amenazas relacionadas de TI, los escenarios de riesgo, y los controles pertinentes a sus funciones y responsabilidades. El plan se ha definido para su uso y normalización de las herramientas para automatizar las actividades de reducción del riesgo, como el aprovisionamiento de usuarios.

- 4 - Gestionado cuando

Hay ambos, comprensión individual y organizativa de todos los requisitos para responder a los riesgos. La alta dirección empresarial y la gestión de TI en conjunto, determinan si una condición de riesgo es superior a las tolerancias definidas de riesgo. Una cultura de la recompensa está en el lugar, motivando a la acción positiva. La eficiencia y la eficacia de la respuesta a los riesgos son medidos y comunicados, y vinculado a los objetivos de negocio y el plan estratégico de TI. Todos los aspectos del proceso de respuesta de los riesgos, se documentan y son cuantitativamente gestionados.

Los requisitos de habilidad son rutinariamente actualizados para todas las zonas de riesgo de respuesta, incluyendo la articulación de riesgos, mitigación de riesgos, reaccionando a los acontecimientos y aprovechando oportunidades. Las herramientas se utilizan en las principales zonas para permitir la gestión del riesgo de cartera de la empresa y supervisar los controles críticos, las capacidades y recursos.

- 5 - Optimizado cuando

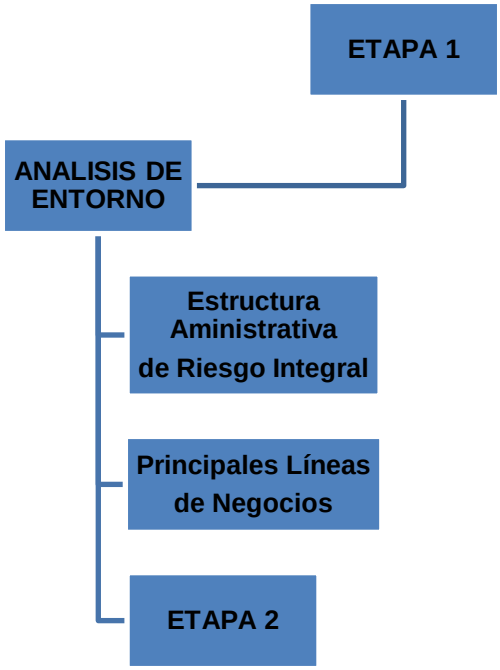
No es a la vez individuales y empresariales comprensión de todos los requisitos para hacer frente al riesgo. Las respuestas a los riesgos reales, a las operaciones reales se comunicarán vigorosamente en toda la empresa. La organización colabora en conjunto con entidades externas para responder a las cuestiones comunes y la pandemia de riesgo. La empresa mide la eficacia de los esfuerzos de respuesta a los riesgos, tanto a nivel interno y en colaboración con entidades externas. La gama completa de estrategias de respuesta de riesgo, es aplicado de manera integral y, cuando sea plenamente justificado, controles costo-eficacia mitigan la exposición al riesgo en forma continua.

La empresa exige formalmente la mejora continua de las capacidades de respuesta de riesgos (por ejemplo, la articulación de riesgo, la mitigación, la gestión de crisis) sobre la base de definir claramente los objetivos personales y de organización. La empresa emplea tecnologías avanzadas de respuesta de riesgos para inteligentemente asumir riesgos adicionales y aprovechar las oportunidades competitivas.

9. METODOLOGÍA

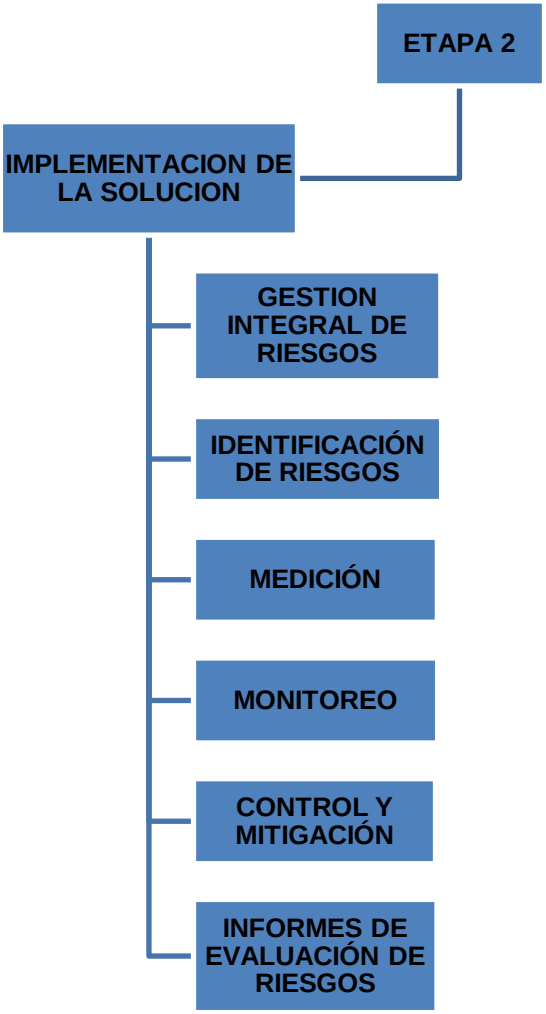
La metodología que a continuación se describe, consta de 2 etapas, la primera etapa es el estudio del entorno, que a su vez consta de 2 fases, las cuales comprenden la estructura administrativa de riesgo integral y las principales líneas de negocios y la segunda etapa, es la implantación de la solución, que consta de 6 fases, las cuales describen los pasos que se deben cumplir para poder obtener el grado de mitigación de impacto del riesgo tecnológico, lo cual se deberá verificar en las evaluaciones de las 3 fases de la continuidad.

Figura 2. **Etapa 1: análisis de entorno**



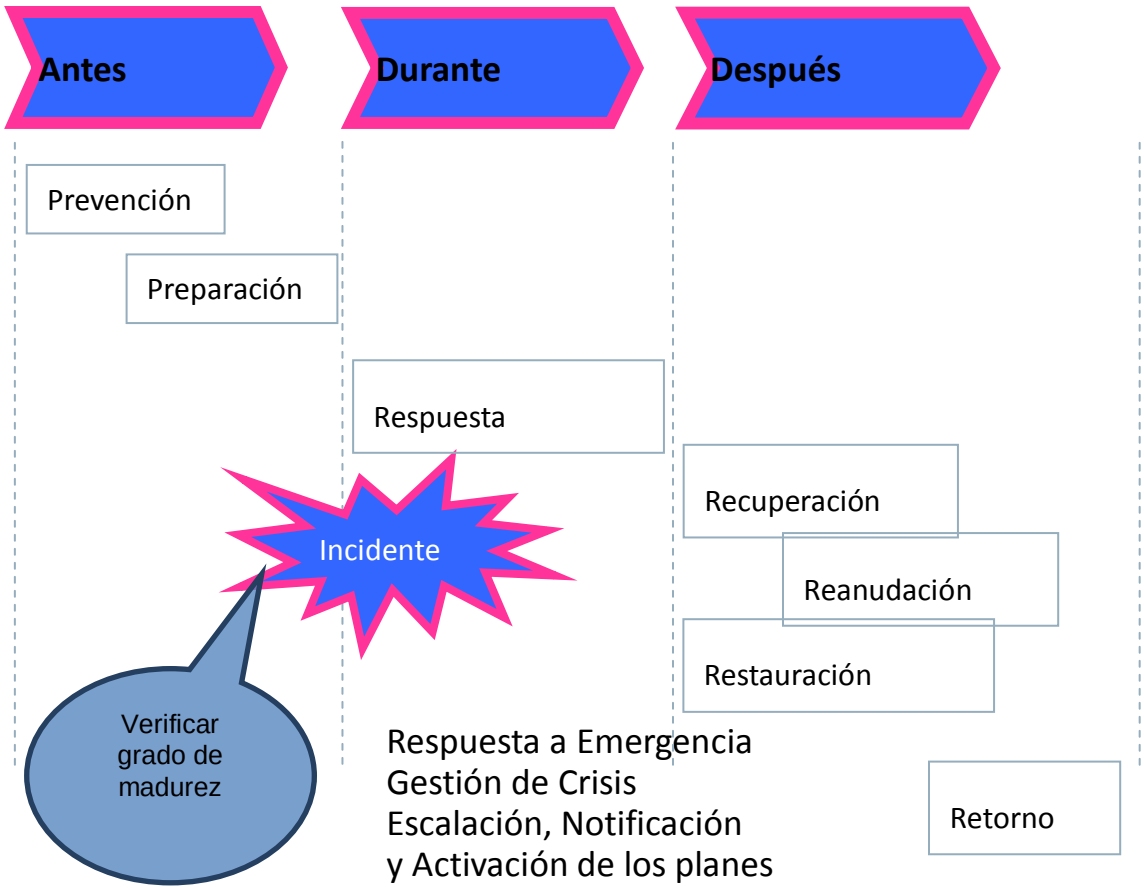
Fuente: elaboración propia.

Figura 3. **Etapa 2: implementación de la solución**



Fuente: elaboración propia.

Figura 4. **Fases de la continuidad**



Fuente: elaboración propia.

9.1. Análisis de entorno

- Organización para la administración del riesgo integral

Un aspecto fundamental para la puesta en marcha del sistema de administración de riesgos, es la separación de las unidades de negocio, áreas, departamentos, divisiones que generan los riesgos de aquellas áreas o unidades que monitorean su administración y control. La estructura organizacional de Banco Internacional, S. A. a cargo de la gestión integral de riesgos, se integran por el Consejo de Administración y la alta dirección, el Comité de Riesgo Integral, del cual el Departamento de Riesgo Integral es un integrante permanente, los que aseguran su independencia y capacidad para supervisar y gestionar los riesgos a que está expuesto el banco.

Asimismo, existen comités de riesgos especializados que se han creado con la finalidad de evaluar cada riesgo específico en particular, siendo éstos los Comités ALCO[6], de riesgo operativo y riesgo tecnológico, que representan las principales líneas de negocio y cuyas funciones son las de evaluar todos los riesgos asociados, según la línea de negocio que por sus funciones atiende. Toda la información que estos comités recopilen representara la población a estudiar.

6 Comité ALCO: es la instancia responsable de las políticas, procedimientos y límites respecto de los riesgos de mercado y del monitoreo del desempeño de éstos a la luz de los riesgos asumidos. Por recomendación de este comité, el área de Riesgos de Mercado y la Tesorería del Banco llevan un control diario de los riesgos, tanto transaccionales como no transaccionales.

Figura 5. **Estructura organizacional de riesgo**

Fuente: elaboración propia.

- Principales líneas de negocio

Banco Internacional, S. A. ofrece productos y servicios financieros a través de las diferentes unidades de negocios integradas en las siguientes bancas, las cuales serán la base de este estudio:

Banca de empresas: su principal actividad es otorgar financiamientos a empresas medianas y corporativas de diferentes sectores económicos, atendiendo necesidades financieras orientadas a actividades diversas, tales como, capital de trabajo, inversión en activos fijos (maquinaria y equipo), inversiones en inmuebles (adquisición de bodegas, oficinas, locales), así como financiar operaciones de comercio exterior a empresas que se dedican a la importación y exportación de distintos productos. Adicionalmente, la Banca de Empresas, dentro de sus actividades, se dedica a la captación y administración de los recursos de su clientela.

Banca Comercial: la principal función de ésta, es la de captar recursos financieros del público y otorgar créditos, para apoyar el desarrollo de las actividades económicas del país y el consumo, principalmente para medianas empresas, profesionales y clientes varios de perfil comercial; y, la venta de productos y servicios financieros.

Para el cumplimiento de sus fines, la banca comercial está distribuida a través de su red de agencias en 3 regiones geográficas: región nor-oriente, región central y región sur-occidente. Las solicitudes y gestiones de los clientes son canalizadas por gerentes de agencia, quienes están bajo la supervisión de un gerente regional para cada región, quienes, a su vez, reportan al gerente de banca comercial.

Banca Privada: la banca privada se dedica a gestionar el dinero de clientes privados, especializándose en clientes con grandes cuentas que desean que su dinero se invierta y gestione a corto o largo plazo, atendiéndolos de forma personalizada. Para el desarrollo de sus funciones, se cuenta con ejecutivos especializados en prestar un servicio profesional.

Las líneas de negocio involucran una serie de actividades y procesos que generan determinados productos o servicios, los cuales le aportan valor a la institución. De las bancas referidas previamente, se desprenden las líneas de negocio del banco, las cuales serán objeto de este estudio.

9.2. Implementación de la solución

- Gestión integral de riesgos

La gestión integral de riesgos involucra un conjunto de fases o etapas, cuyo objetivo es gestionar y controlar los riesgos a que está expuesto el banco. La metodología que ha dispuesto Banco Internacional, S. A. para la gestión integral de riesgos, se basa en 2 grandes aristas: gestión activa y gestión proactiva.

- Gestión activa de riesgos

Se entiende por gestión activa a las diversas actividades que se desarrollan de manera cotidiana en distintas áreas del banco, encaminadas a identificar los distintos riesgos que pueden presentarse por el mismo giro de la actividad diaria, y con mayor énfasis, en aquellas de alta exposición al riesgo. Entre las principales áreas involucradas en la gestión activa de riesgos, se mencionan soporte y control operacional, tecnología, Departamento de Riesgo Integral, Auditoría Interna.

El objetivo de dichas unidades y áreas, es identificar y monitorear, en el curso de las actividades diarias, los riesgos potenciales que afectan el desarrollo de actividades de la institución.

- Gestión proactiva de riesgos

La gestión proactiva de riesgos tiene como fin anticiparse a la materialización de riesgos importantes; y, se conforma por las etapas de identificar, medir, monitorear, controlar, prevenir y mitigar los distintos riesgos.

Es por ello que la segunda arista de gestión, se relaciona con la revisión constante de los principales procesos del banco a fin de identificar y evaluar los distintos riesgos.

- Identificación de riesgos

Previamente establecidas las líneas de negocio, así como los procesos más críticos, la primera fase de la gestión de riesgos, consiste en identificar los riesgos a que está expuesto el banco, es decir, determinar los eventos internos y externos que pueden tener un impacto negativo sobre los objetivos del banco. Esta etapa exige un análisis meticuloso del proceso, del cual deriva determinado riesgo, dentro del contexto en el que se desenvuelve la institución.

Entre los riesgos a identificar se puede citar la existencia de transacciones impropias o ficticias, fallas en los sistemas de información, que el volumen de las operaciones de los registros contables no esté completo o que las transacciones no se hayan registrado adecuadamente, entre otros. La identificación de riesgos es puntual a cada proceso particular, por lo cual es necesario el conocimiento pleno de cómo funciona dicho proceso. Dadas las principales líneas de negocio de Banco Internacional, S. A., se ha llevado a cabo la etapa de identificación de riesgos sobre las operaciones activas que contribuyen con el 80 por ciento de ingresos del banco.

- Medición

La medición involucra la ponderación o forma de cuantificar los riesgos, para ello se debe tipificar el efecto negativo o impacto que pueda repercutir en la institución. Para dicha medición, será necesario determinar para cada riesgo,

la frecuencia y la intensidad de ocurrencia o impacto, lo que se realiza por medio de una matriz.

- Frecuencia

Por frecuencia, se entiende la probabilidad de ocurrencia o el porcentaje de estimación de ocurrencia de un riesgo en un período de tiempo. La escala de frecuencia establecida para Banco Internacional, S. A. va desde el nivel 1 hasta el nivel 5 (en su orden, muy baja, baja, moderada, alta y muy alta).

- Impacto

Determinar el impacto previsible de los distintos riesgos, es necesario evaluar las consecuencias estimadas, sin tener en cuenta el impacto de los mecanismos de administración. El impacto se refiere a la trascendencia que tiene la materialización del riesgo para la entidad, ya sea porque tiene un efecto financiero importante o porque afecta la continuidad de operaciones de la institución.

La escala de impacto definida para Banco Internacional, S. A. va desde el nivel 1 hasta el nivel 5 (en su orden, muy bajo, bajo, moderado, alto y muy alto). Asimismo, la descripción de cada nivel de la escala de impacto será establecida en el manual específico de cada riesgo que se trate.

- Ponderación de factores (riesgo inherente)

Es el resultado de la multiplicación de la frecuencia por el impacto determinado para cada riesgo. Con ello, se persigue poder estratificar los distintos riesgos, a manera que se priorice el análisis de aquellos que presenten

un impacto y frecuencia alta, para cuya atención se concentrarán los mayores esfuerzos en recursos. De la ponderación de factores, se establece una matriz de riesgos, conformada en el eje vertical por la frecuencia y en el eje horizontal por el impacto, de la siguiente manera:

Tabla II. **Frecuencia impacto de riesgo**

FRECUENCIA						
	MUY ALTA	5	10	15	20	25
	ALTA	4	8	12	16	20
	MEDIA	3	6	9	12	15
	BAJA	2	4	6	8	10
	MUY BAJA	1	2	3	4	5
		MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
		IMPACTO				

Fuente: elaboración propia.

El proceso descrito, permite identificar los riesgos más críticos para la institución, a fin que se priorice la evaluación de los mismos y se identifiquen los mecanismos de control que coadyuven a su mitigación.

- Monitoreo

El monitoreo de los principales riesgos, es una forma de estar presente en todos los niveles de la organización, permitiendo que a través de controles se muestre el desarrollo de los procesos y los problemas que podrían ocurrir en el transcurso de las actividades.

Parte de la gestión de riesgos, involucra el monitoreo cotidiano de los distintos procesos del banco, lo cual es apoyado por el personal, desde los responsables de cada proceso hasta los órganos de verificación interna independiente como la auditoría interna.

- Control y mitigación

Conocidos los riesgos a los que se encuentra sometido el banco en función de las operaciones que realiza, la frecuencia e impacto que eventualmente pueden generar los mismos, así como determinar su importancia para la institución, es necesario definir los mecanismos de los que se dispone para su adecuada gestión.

El mecanismo de control se refiere a las políticas, procedimientos, actividades o herramientas tendientes a disminuir la frecuencia del riesgo o su impacto. Para ello, el personal debe tener pleno conocimiento del efecto que involucra la realización inadecuada de actividades, lo cual puede desencadenar en riesgos potenciales para la institución.

A fin de determinar el nivel de calidad de los controles establecidos, se ha dispuesto que la escala de control va desde el nivel 1 hasta el nivel 5 (en su orden, deficiente, insatisfactorio, bueno, muy bueno y excelente).

- Riesgo residual

Es el riesgo resultante luego de tomar en cuenta el efecto del control interno sobre la ponderación de frecuencia e impacto de cada riesgo. Este se calcula de la siguiente forma:

Riesgo residual = (frecuencia * impacto) /control

El riesgo residual es el riesgo resultante después de la aplicación de los distintos controles del banco. Esto permite orientar las labores de análisis y reforzar los controles de aquellos procesos que presenten riesgos residuales más altos.

- Grado de mitigación

El proceso de mitigación considera todas aquellas medidas correctivas que se toman debido a la presencia de elementos que incrementan el nivel de riesgo. La mitigación establece en qué proporción ha sido cubierto el riesgo, dado el control existente y se calcula como sigue:

Grado de mitigación: 1- riesgo residual

- Informes de evaluación de riesgos

El Departamento de Riesgo Integral elaborará, en conjunto con los responsables de cada riesgo específico, los informes de exposición al riesgo. El resultado de dicha evaluación debe hacerse del conocimiento del Comité de Riesgo Integral, quien debe analizar la exposición del banco y tomar las decisiones más acertadas para su adecuada gestión.

10. CRONOGRAMA

Tabla III. **Cronograma de actividades**

CRONOGRAMA DE ACTIVIDADES							
Id	Nombre	Duración	Comienzo	Fin	Trabajo	Variación de duración	Variación de trabajo
1	Definición de la estructura de la Administración del Riesgo Tecnológic	2 días	01/08/2011 08:00	02/08/2011 17:00	16 horas	2 días	16 horas
2	Integración del comité de Riesgo	2 días	19/09/2011 08:00	20/09/2011 17:00	16 horas	2 días	16 horas
3	Integración del Oficial de Seguridad Tecnológica	2 días	14/11/2011 08:00	15/11/2011 17:00	16 horas	2 días	16 horas
4	Identificación de los procesos prioritarios	45 días	19/09/2012 08:00	20/11/2012 17:00	360 horas	45 días	360 horas
5	Evaluacion de los factores de Riesgo	5 días	05/03/2012 08:00	09/03/2012 17:00	40 horas	5 días	40 horas
6	Definición de la Gestión de riesgo	2 días	02/04/2012 08:00	03/04/2012 17:00	16 horas	2 días	16 horas
7	Elaboración de planes de Recuperación de Desastres	30 días	03/05/2012 08:00	13/06/2012 17:00	240 horas	30 días	240 horas
8	Elaboración de planes de Continuidad de Negocio	60 días	22/05/2012 08:00	13/08/2012 17:00	480 horas	60 días	480 horas
9	Procesos de las Principales Líneas del Negocio del Banco	5 días	24/05/2012 08:00	30/05/2012 17:00	40 horas	5 días	40 horas
10	Esquema de la información del negocio	3 días	04/06/2012 08:00	06/06/2012 17:00	24 horas	3 días	24 horas
11	Listado de Riesgos Tecnológicos	20 días	01/10/2012 08:00	26/10/2012 17:00	160 horas	20 días	160 horas
12	Ponderación de Factores	5 días	04/10/2012 08:00	10/10/2012 17:00	40 horas	5 días	40 horas
13	Asignación de prioridad por Proceso	5 días	11/10/2012 08:00	17/10/2012 17:00	40 horas	5 días	40 horas
14	Análisis y diseño de herramienta para control estadístico del riesgo	5 días	10/12/2012 08:00	14/12/2012 17:00	40 horas	5 días	40 horas
15	Desarrollo de herramienta para control estadístico del riesgo	20 días	02/01/2013 08:00	29/01/2013 17:00	160 horas	20 días	160 horas
16	Puesta en producción de herramienta para control estadístico del riesg	10 días	30/01/2013 08:00	12/02/2013 17:00	80 horas	10 días	80 horas
17	Evaluacion de Riesgos	60 días	18/10/2012 08:00	09/01/2013 17:00	480 horas	60 días	480 horas
18	Informe de evaluación de riesgo	5 días	10/01/2013 08:00	16/01/2013 17:00	40 horas	5 días	40 horas
19	Revisión de informe de riesgos	5 días	17/01/2013 08:00	23/01/2013 17:00	40 horas	5 días	40 horas
20	Toma de decisiones sobre gestión de riesgos	2 días	24/01/2013 08:00	25/01/2013 17:00	16 horas	2 días	16 horas
21	Asignación de prioridades de gestión de riesgos	2 días	28/01/2013 08:00	29/01/2013 17:00	16 horas	2 días	16 horas

Fuente: elaboración propia.

11. PRESUPUESTO

Los recursos físicos, aplicaciones y personal para el análisis, desarrollo y evaluación de la metodología de mitigación del impacto del riesgo tecnológico, serán proporcionados por la División de Operaciones y Tecnología del Banco Internacional.

También se proporciona un presupuesto si este proyecto fuese contratado con soporte externo.

Tabla IV. **Propuesta de presupuesto**

PRESUPUESTO				
INVERSION				
No.	**DESCRIPCION**	**CANTIDAD**	**COSTO**	**TOTAL**
1	PC con Software de ofimática	4	Q 5,000.00	Q 20,000.00
2	Software para proyectos	4	Q 1,600.00	Q 6,400.00
3	Diseño software para mitigación de impacto	1	Q30,000.00	Q 30,000.00
4	Asesoría de tesis	1	Q 2,500.00	Q 2,500.00
		TOTAL INVERSION		**Q 58,900.00**
GASTO				
No.	**DESCRIPCION**	**CANTIDAD**	**COSTO**	**TOTAL**
1	Horas 2 programadores	160	Q 200.00	Q 32,000.00
2	Horas 1 analista	40	Q 350.00	Q 14,000.00
3	Horas 1 asesoría en Continuidad de Negocio	40	Q 400.00	Q 16,000.00
4	Horas revisión responsable de control de calidad producto	40	Q 350.00	Q 14,000.00
5	Horas implementador	80	Q 350.00	Q 28,000.00
6	Horas digitador	80	Q 100.00	Q 8,000.00
7	Horas responsable proyecto	160	Q 400.00	Q 64,000.00
		TOTAL GASTO		**Q 176,000.00**
		TOTAL GENERAL		**Q234,900.00**

Fuente: elaboración propia.

12. BIBLIOGRAFÍA

1. BECK, Ulrich (1998): La sociedad del riesgo. Hacia una nueva modernidad, Barcelona, Paidos.

2. BECK, Ulrich (2002): La sociedad del riesgo global, Madrid, Siglo XXI.

3. Bisogno, M. A., (2004). Metodología para el Aseguramiento de Entornos Informatizados. (Tesis Ingeniería en Informática). Universidad de Buenos Aires, Argentina.

4. Business Continuity Institute 2002. Understanding your business. Versión BCI DJS 1.0 01/11/02. Recuperado el 15/03/12, Disponible en: http://www.auckland.ac.nz/security/images/BCI%20GPG%2020Stage%201.pdf.

5. Business Continuity Institute 2007. A Management Guide to Implementing Global Good Practice in Business Continuity Management Section 4 Developing and implementing a BCM response. Versión 2007.3 Octubre 2007 disponible en http://www.thebci.org/GPG2008V1%20Section4.pdf

6. Cobit5 (2012), ISACA, recuperado de https://www.isaca.org/bookstore/Pages/default.aspx

7. Comité de Basilea sobre supervisión Bancaria, julio 2002, recuperado de http://www.sib.gob.gt/web/sib/leyesyreglamentos/reglamentos

8. Coronel Hoyos, K. D. R. (2008). Metodología de evaluación del riesgo tecnológico en las instituciones del sistema financiero ecuatoriano, utilizando COBIT 4.1.

9. DRI International. Developing business continuity strategies. 2004. disponible en: http://www.drii.org/DRII/ProfessionalPractices/Pro_04.aspx

10. Gartner, Disaster Recovery Plans and Systems Are Essential, by Roberta Witty, Donna Scott, 12 September 2001.

11. Introducción a la Fiabilidad, Última actualización el jueves, 16 de octubre de 2008, 15:43:34 por Jeff, Recuperado el 14/03/12 de : http://es.kioskea.net/contents/surete-fonctionnement/haute-disponibilite.php3

12. LÓPEZ, José; LUJAN José (2000): Ciencia y política del riesgo, Madrid, Alianza Editorial.

13. Marco de Riesgo de TI (2009). ISACA, Risk IT, recuperado de https://www.isaca.org/bookstore/Pages/default.aspx

14. Minguillon Roy, A. (2010). La auditoría de sistemas de información Integrada en la auditoría financiera. La perspectiva del sector público, Valencia, España: Sindicatura de Comptes de la Comunitat Valenciana

15. Ramírez, I. B., y Latorre, J. E. (2000). Estudio y Propuesta para Implantar una Unidad de Inteligencia Financiera en Venezuela, (Tesis Maestría en Ciencia). Universidad nueva Esparta, Caracas, Venezuela.

16. Ramírez, O. J. (2009): RIESGOS DE ORIGEN TECNOLÓGICO: APUNTES CONCEPTUALES PARA UNA DEFINICIÓN, CARACTERIZACIÓN Y RECONOCIMIENTO DE LAS PERSPECTIVAS DE ESTUDIO DEL RIESGO TECNOLÓGICO, Manizales, Colombia.

17. Reglamento para la Administración del Riesgo Tecnológico, Junta Monetaria JM-102-2011, 17/08/2011, Superintendencia de Bancos de Guatemala, recuperado de: http://www.sib.gob.gt/web/sib/leyesyreglamentos/reglamentos?p_p_id=110_INSTANCE_n1HH&p_p_action=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=column-3&p_p_col_pos=1&p_p_col_count=2&_110_INSTANCE_n1HH_struts_action=%2Fdocument_library_display%2Fview&_110_INSTANCE_n1HH_folderId=455681

18. Reglamento para la Administración Integral de Riesgos, Junta Monetaria JM-56-2011, 18/05/2011, Superintendencia de Bancos de Guatemala, recuperado de: http://www.sib.gob.gt/c/document_library/get_file%3FfolderId%3D455681%26name%3DDLFE-9147.pdf&q=JM-56-2011&ei=IypdUJ_fH42K8QSYh4HAAg&usg=AFQjCNGLpGtLULe7pcFhrHnbAutUfuXAZg

19. RESCHER, Nicholas (1999): Razón y valores en la Era científico-tecnológica, Barcelona, Paidos.

20. RODRÍGUEZ, J. (1999): “El riesgo como utopía negativa. Notas para una reflexión”, en Ramos, R; García Selgas, F. Globalización, Riesgo, Reflexividad. Tres temas de teoría social contemporánea, Madrid. Centro de Investigaciones Sociológicas (CIS), pp. 191-204.

21. Superintendencia de Bancos de Guatemala, http://www.sib.gob.gt