



**UNIVERSIDAD DE CHILE  
FACULTAD DE CIENCIAS FISICAS Y MATEMATICAS  
DEPARTAMENTO DE INGENIERIA INDUSTRIAL**

**“INNOVACIÓN ESTRATÉGICA EN LA GESTIÓN DEL RIESGO  
OPERACIONAL TECNOLÓGICO DE BANCO BCI”**

**TESIS PARA OPTAR AL GRADO DE MAGISTER EN GESTIÓN Y DIRECCIÓN  
DE EMPRESAS**

**GONZALO RODRIGO FLORES OPAZO**

**PROFESOR GUÍA:  
JORGE LARA BACCIGALUPPI**

**MIEMBROS DE LA COMISIÓN:  
ANTONIO HOLGADO SAN MARTIN  
RENATO BLASKOVIC ARAVENA**

**SANTIAGO DE CHILE  
Julio, 2012**

Esta tesis tiene como objetivo principal, el desarrollo de un modelo avanzado de medición y valorización del riesgo operacional tecnológico para el Banco Crédito e Inversiones (en adelante BCI), basado en los requerimientos de capital planteados en el acuerdo internacional de Basilea II.

Este modelo busca ajustar (disminuir) la provisión por riesgo operacional en un 20% de aquí a 3 años (5% el 1er año, 10% el 2do y 20% el 3er año), aumentar las utilidades, el valor de la empresa, potenciar el control interno y el Gobierno Corporativo de la organización.

El modelo propuesto se divide en tres etapas; la primera consiste, en el desarrollo de un marco conceptual basado en las mejores prácticas recomendadas por el estándar internacional Cobit, a objeto de identificar y evaluar los controles asociados a los procesos tecnológicos considerados como claves y que pueden generar riesgos en este ámbito.

En una segunda etapa, se establecen métricas idóneas y una metodología para medir cualitativamente el riesgo, la efectividad y cumplimiento de cada uno de los controles claves seleccionados, obteniéndose información valiosa para gestionar mejoras a dichos controles y de esta manera influir en la disminución continua de los niveles de riesgo tecnológico.

En una tercera etapa, se desarrolla un modelo estadístico de evaluación cuantitativa del riesgo operacional tecnológico, tomando como base metodológica un modelo conceptual desarrollado por PricewaterhouseCoopers y la metodología Value At Risk (VaR), realizando la gestión de toda la información proveniente de las entradas definidas en la primera etapa del Modelo. De acuerdo a lo anterior, se establece una manera de integrar toda la información de riesgos generada, transformándose en un panel de luces de los principales riesgos asociados a los procesos tecnológicos, niveles de cumplimiento, efectividad de los controles y la valorización asociada a estos riesgos.

Finalmente, se efectúa un ejercicio real de cálculo de provisiones utilizando el modelo avanzado de cálculo de Riesgo Operacional Tecnológico propuesto y se compara el resultado obtenido, con el resultado del cálculo efectuado por el Banco a finales del 2010, sin la aplicación de éste modelo, a objeto de comprobar si se cumplen los objetivos propuestos.

En conclusión, se demuestra en parte la tesis propuesta, ya que la disminución del requerimiento de capital para los riesgos tecnológicos del Banco disminuyó en MM\$328 (7,8%) para año 2011 (1er año), respecto de lo calculado en el ejercicio anterior durante el 2010, faltando el cálculo de los montos de provisión para el resto de los procesos y unidades de negocio cuyos riesgos operacionales también deben ser evaluados y que no eran parte del ámbito de este proyecto.

De acuerdo al resultado obtenido, el ahorro en provisiones puede seguir aumentando si se logra mejorar el nivel de madurez de los controles, lo que permitiría disminuir aun más las pérdidas reales, mejorar la calificación del riesgo y su posterior valorización, lo que transforma a este modelo en una herramienta poderosa para la gestión de dichos conceptos y un apoyo importante al Gobierno Corporativo del Banco.

## **AGRADECIMIENTOS**

Quiero expresar mi gratitud y dedicar este trabajo a mi Madre Rosita, por todo el amor, el apoyo, la fuerza y por todas las enseñanzas que me ha dado durante mi vida y que me han hecho lo que soy. A mi mujer Marcela y a su familia por estar siempre conmigo, apoyándome, escuchándome, comprendiéndome y por el amor y cariño que me han entregado incondicionalmente. A mis 4 hijos Catalina, Gonzalo, Antonia y Maximiliano, por darme una gran razón de vida, por comprender los momentos en que estuve ausente, y por la motivación que día a día me dan para superarme como padre, como profesional, pero sobre todo, como persona.

Gracias a ustedes familia por sembrar en mí el deseo de hacer de este mundo un mundo mejor y dedicar parte de sus vidas a eso. Ustedes son mis héroes y las personas que más amo en este mundo.

Me gustaría agradecer también a la comunidad académica de la Universidad de Chile por su apoyo en la realización de esta tesis, en especial a mi profesor Guía Sr. Jorge Lara, mi profesor auxiliar Sr. Héctor Umanzor y mi profesor invitado Sr. Renato Blaskovic, por encausar mi inspiración y aportar al desarrollo de mi trabajo con sus experiencias y sabias conversaciones, las cuales fueron muy perspicaces, entretenidas y de un gran valor para mí.

Quiero incluir dentro mis agradecimientos a las Srtas. Loreto Porte y Paula Guerrero y a los Sres. Aldo Verdugo y Marco Arenas, todos de la Gerencia de Riesgo Operacional de Banco BCI, por toda la ayuda y la buena disposición entregada para el desarrollo de este trabajo y a las dos Secretarias de la Gerencia de Contraloría, Oriana e Isabel por su apoyo y respaldo en este trabajo.

En forma especial quiero agradecer a la Sra. Graciela Duran – Gerente Contralor de Banco BCI, por confiar y creer en mí y ofrecerme la oportunidad de estudiar este Magister y a mis compañeros de trabajo por apoyarme en el día a día, especialmente en los momentos de mayor exigencia laboral y académica.

Destaco y agradezco a todos mis compañeros de generación del Magister por toda las experiencias, ayuda y colaboración entregada, en especial a los Sres. Alex Day y Enzo Nicolini, por su alegría, lealtad y sobre todo por ser tan buenos amigos.

Esta Tesis tiene un gran esfuerzo personal, pero sin duda el mayor esfuerzo lo realizó mi familia, a quienes amo y les agradezco infinitamente.

Gracias a todos.

Gracias a Dios.

## INDICE

<b>Capítulo 1. Introducción General.....</b>	<b>7</b>
1.1. Introducción.....	7
1.1.1. ¿Por qué un modelo de gestión de riesgo TI?.....	7
1.1.2. ¿Cuáles son las mejores prácticas en el mercado actual?.....	8
1.1.3. ¿Por qué BCI?.....	9
1.2. Descripción del Mercado y de la Organización.....	10
1.2.1. Mercado Financiero.....	10
1.2.2. Reseña histórica y evolución de BCI.....	12
1.2.3. Productos y Canales de servicio y distribución de BCI.....	14
1.2.4. Situación Económica y Participación de Mercado.....	16
1.2.5. Análisis Financiero y de Productos.....	20
1.2.6. Organización TI de BCI.....	24
1.2.7. Instalaciones e infraestructura de BCI.....	29
1.2.8. Tecnología e Innovación de BCI.....	30
1.2.9. Compromiso de Transparencia de BCI.....	33
1.2.10. Responsabilidad Social de BCI.....	35
1.3. Descripción del Riesgo en la Organización.....	35
1.3.1. Administración de Riesgo en BCI.....	35
1.3.2. Evolución del Riesgo Operacional en BCI.....	41
<b>Capítulo 2. Descripción del Modelo a desarrollar.....</b>	<b>42</b>
2.1. Objetivos de Modelo.....	43
2.2. Alcances del Proyecto.....	44
2.3. Resultados Esperados.....	45
2.4. Marco Conceptual.....	47
2.5. Análisis de FODA para el modelo propuesto.....	50
2.6. Preguntas Claves.....	53
2.7. Factores Críticos de éxito.....	54
<b>Capítulos 3. Análisis de los modelos de cálculo existentes.....</b>	<b>56</b>
3.1. Análisis de regulación existente para la gestión del riesgo operacional.....	56
3.1.1. Evolución hacia Basilea II de la Banca Chilena.....	56
3.1.2. Evolución hacia Basilea II de la Banca Internacional.....	57
3.2. Levantamiento del proceso de cálculo y medición actual de Riesgo Operacional de Banco BCI.....	60
3.2.1. Metodología de Cálculo de Riesgo Operacional.....	61
<b>Capítulos 4. Desarrollo del Modelo de Gestión de Riesgos TI.....</b>	<b>64</b>
4.1. Levantamiento y descripción de los principales procesos tecnológicos del Banco y sus controles asociados.....	64

4.1.1. Identificación de procesos críticos TI.....	64
4.1.2. Identificación de controles claves TI.....	66
4.2. Determinación de indicadores de riesgo tecnológico y de eficiencia para el Banco (Evaluación Cualitativa).....	68
4.2.1. Desarrollo de indicadores de riesgo (KRIs).....	68
4.2.2. Definición de escala de riesgo.....	73
4.2.3. Análisis de Riesgo (Impacto /Probabilidad de ocurrencia).....	79
4.3. Valorización de Riesgos TI (Evaluación Cuantitativa).....	81
4.3.1. Análisis de la Base de Datos de Pérdida.....	81
4.3.2. Desarrollo del modelo matemático de valorización (PE y VaR).....	82
4.3.3. Cálculo a través de Operational Risk Capital (ORC).....	88
<b>Capítulos 5. Resultados y Conclusiones del Modelo.....</b>	<b>91</b>
5.1. Cálculo de Riesgo Operacional bajo el modelo propuesto.....	91
5.2. Integración de la gestión cualitativa y cuantitativa.....	95
5.3. Proyección del riesgo TI en BCI a tres años.....	96
5.4. Evaluación de 3 proyectos asociados al logro de la proyección.....	97
5.5. Análisis de costo/beneficio del nuevo modelo.....	99
5.6. Análisis de sensibilidad financiero.....	100
5.7. Conclusiones del Modelo de Gestión de Riesgos TI. ....	102
<b>Referencias Bibliográficas.....</b>	<b>108</b>
<b>ANEXO A: Riesgo en la Banca.....</b>	<b>110</b>
A.1. Tipología de riesgos.....	110
A.2. Fuentes de Riesgo Operacional.....	114
A.3. Riesgo Operacional Tecnológico.....	116
A.4. Descripción de Normativa Chilena.....	116
A.5. Descripción de Normativa Internacional.....	118
A.6. Mejores prácticas Internacionales de Gestión de riesgo TI.....	120

## **CAPITULO 1: INTRODUCCIÓN GENERAL**

### **1.1. INTRODUCCIÓN**

Este trabajo abordará el desarrollo de un modelo de gestión de riesgos tecnológicos para el Banco de Crédito e Inversiones basado en las mejores prácticas de seguridad de la información y gestión de riesgos, que permita evaluarlos, cuantificarlos y entregar una herramienta potente para el gobierno corporativo de la organización.

#### **1.1.1. ¿Por qué un modelo de gestión de riesgo TI?**

La crisis financiera internacional ocurrida entre los años 2007 y 2009 ha dejado de manifiesto la necesidad de contar con un adecuado marco de gestión de riesgos a los cuales las instituciones financieras deben apuntar. Los distintos tipos de riesgos (de mercado, crédito, operacional y liquidez) son transversales y de naturaleza distinta, por lo que la definición de un modelo aplicable para abordar cada uno de ellos es de suma importancia.

Hoy día la Banca Chilena se mantiene en un proceso de transición hacia el nuevo Marco de Capital de Basilea II, el cual indica la necesidad de gestionar el riesgo operacional; fundamentalmente en su cuantificación y otros aspectos técnicos y cualitativos subyacentes a los distintos enfoques, para una adecuada gestión y medición, sin embargo, el riesgo tecnológico el cual es parte importante del riesgo operacional, no ha sido incorporado dentro de las metodologías de valorización de riesgo.

Es importante mencionar, que en las grandes industrias y en especial en el sector bancario, los procesos tecnológicos son de suma importancia para el desarrollo y mantención de productos y servicios en forma eficiente y a menores costos y todos estos procesos (operativos y tecnológicos) cuentan con una variable de

riesgo que los puede afectar fuertemente en cualquier momento, generándose, como consecuencia de esto, pérdidas importantes en términos de calidad, gastos por corrección errores, eventuales ilícitos, daño a la imagen corporativa y contingencias legales.

### **1.1.2. ¿Cuáles son las mejores prácticas en el mercado actual?**

En el mercado de las metodologías de administración de riesgos, existe una gran variedad de normas y procedimientos que intentan englobar la mayor cantidad de procesos críticos asociados a las tecnologías de información, dentro de las cuales destacan la Normas ISO 27001 (Seguridad de Información), ISO 31000 (Gestión de Riesgos), ISO 38500 (Gobierno de TI), el Modelo Cobit (Objetivos de Control para la información y las tecnologías asociadas), VAL IT (Gobierno de las inversiones TI), Value at Risk (VaR) entre otras. Estas Metodologías proponen mejores prácticas de controles asociados a las TI, sin embargo, ninguna de ellas propone un modelo explícito para implantar dichos controles, automatizarlos, y herramientas concretas (reportes o indicadores) para dimensionar el riesgo a que se exponen, valorizarlo y proporcionar herramientas de información para tomar adecuadas decisiones. Debido a que las normativas chilenas para los Bancos sólo exigen un modelo de cálculo de riesgo operacional estándar, es decir, calcular provisiones de acuerdo a un porcentaje del margen bruto (15%), los Bancos en general, no han desarrollado modelos avanzados que involucren la medición de riesgo tecnológico. Adicionalmente, BCI realizó, a finales de 2010, su primera prueba informal de cálculo, utilizando un modelo avanzado, sin embargo, este modelo no consideró la gestión de los riesgos tecnológicos.

Dicho lo anterior, se presenta una necesidad para el mercado de las grandes empresas, y en particular una oportunidad para el Banco BCI, empresa sujeta a muchas normativas y exigencias que lo obligan a medir su riesgo operacional (Normas SBIF, Basilea II, entre otras), para optimizar su proceso de gestión de riesgos y cálculo de provisiones, dentro de lo cual, el riesgo tecnológico, es parte importante.



El contar con adecuados controles e indicadores de efectividad de éstos, permite corregir errores, disminuir los tiempos de respuestas (eficiencia), disminuir el riesgo como tal (eventuales ilícitos) y finalmente, esto se traduce en una mejora oportuna en la operación del Banco, en la calidad de los servicios entregados a sus clientes y le permite contar con un mejor gobierno corporativo.

### **1.1.3. ¿Por qué BCI?**

Actualmente, BCI es el tercer Banco privado en términos de colocaciones y el cuarto Banco en número de clientes, detrás de los privados: Banco Santander Chile, Banco de Chile; y el Estatal Banco Estado.

BCI es uno de los Bancos más importantes del país, con numerosas sociedades filiales que complementan y apoyan su giro, con más de 350 puntos de contacto en el país, oficinas en el extranjero, miles de clientes provenientes de diferentes mercados, con alrededor de 10.000 colaboradores que responsablemente ayudan a mantener el Banco como uno de los principales actores del concierto bancario nacional y con el control accionario en manos de las mismas raíces familiares que han conducido la empresa desde su nacimiento.

El Banco cuenta con una gran variedad de tecnologías, con altos estándares de control, excelencia en la calidad y permanente innovación y como tal, está dispuesto a impulsar iniciativas que ayuden a mantenerlo posicionado como un Banco líder.

Desde el punto de vista del negocio, para el Banco BCI es muy atractivo desarrollar este modelo, debido a que el costo adicional al presupuesto que se debería invertir, está muy por debajo de los grandes ahorros que podrían producirse debido a las mejoras en la gestión de las TI.

Por último, este modelo podría ser aplicado a cualquier tipo de empresa con procesos tecnológicos estándares, para apoyar la gestión de riesgo y la mejora de sus servicios tecnológicos.

## **1.2. DESCRIPCIÓN DEL MERCADO Y DE LA ORGANIZACIÓN**

### **1.2.1. Mercado Financiero:**

En la actualidad existen 25 bancos establecidos y operando en el país. El último autorizado fue el DnB Nor Bank ASA en junio del 2008. Estos bancos atienden a un total aproximado de 3,7 millones de clientes, medido de acuerdo al número de personas que mantienen deudas en el sistema bancario.

De dichos bancos, hay 19 que se consideran de acuerdo a la SBIF, como "Bancos Establecidos en Chile", que son Banco de Chile, Banco Internacional, Banco Scotiabank Chile, Banco Crédito e Inversiones, Corpbanca, Banco Bice, HSBC Bank (Chile), Banco Santander Chile, Banco Itaú Chile, Banco Sudamericano, Banco Security, Banco Falabella, Deutsche Bank (Chile), Banco Ripley, Rabobank Chile, Banco Consorcio, Banco Penta, Banco Paris y Banco Bilbao Vizcaya Argentaria Chile (BBVA).

Además de los anteriores, hay 5 Sucursales de Bancos Extranjeros, que son: Banco Do Brasil S.A, JP Morgan Chase Bank, N. A., Banco de la Nación Argentina, The Bank of Tokyo-Mitsubishi LTD y DnB Nor Bank Asa.

Finalmente, existe un Banco Estatal, que corresponde al Banco de Estado de Chile.

#### **a) Situación de la Industria financiera:**

En los últimos meses, nuevamente se ha puesto en duda la interconexión del sector financiero europeo, y los efectos que un nuevo escenario de estrés sobre la deuda de los países periféricos europeos tendría sobre la banca de la zona. En particular al cierre de 2010 y comienzos de 2011, fueron Irlanda, Portugal y recientemente renovados temores sobre Grecia los que se mantuvieron como foco de preocupación de los agentes económicos, en atención a sus debilitadas finanzas públicas.

La industria bancaria chilena sigue ajena a dichos cuestionamientos. Desde mayo de 2009, las utilidades se han mantenido en un camino ascendente, sólo detenido en diciembre recién pasado, lo que no impidió una mejora en el retorno sobre el patrimonio frente al cierre del año anterior.

En lo que respecta a la utilidad, el sistema acumuló en el primer trimestre de 2011 un total de \$444.297 millones, un aumento porcentual de 44,75% con respecto a los resultados del trimestre anterior. La razón radica en el adelantamiento de provisiones de cara a nuevas regulaciones, lo que fue permitido por la SBIF al cierre de 2010, así como una recuperación en el margen de interés, gracias al alza de la UF y en la utilidad de operaciones financieras, entre otros.

A marzo de 2011 las colocaciones como sistema, llegaron a los \$78.832.272 millones, cifra mayor a la obtenida al cierre de 2010, mayormente explicado por la recuperación económica. En términos trimestrales, se observa una aceleración del crecimiento ya que el aumento de las colocaciones para el primer trimestre 2011 fue de 3,93%, superior al obtenido el trimestre anterior de 2,58%.

Al desglosar las colocaciones por componentes vemos alzas generalizadas y donde se destaca el mayor crecimiento en colocaciones comerciales en comparación al trimestre anterior (2.15%) proveniente de la recuperación económica.

Por otra parte, a diferencia del trimestre anterior, se observa un crecimiento importante de los depósitos a plazo en 6,33% que se han visto impulsados por el aumento de la tasa política monetaria y la recuperación económica.

**Tabla 1: Principales cifras del sistema financiero.**

<b>\$ Millones</b>	<b>1T'10</b>	<b>4T'10</b>	<b>1T'11</b>	<b>1T'11 / 4T'10</b>
<b>Colocaciones Totales</b>	<b>71.039.919</b>	<b>75.979.032</b>	<b>78.965.084</b>	<b>3,93%</b>
Adeudado por Bancos	1.721.453	1.025.051	1.221.709	19,19%
Colocaciones Clientes	69.318.466	74.953.981	77.743.375	3,72%
Comerciales	42.724.674	45.629.263	47.514.046	4,13%
Consumo	8.773.015	9.738.588	10.177.542	4,51%
Vivienda	17.820.777	19.586.130	20.051.787	2,38%
<b>Activos Totales</b>	<b>101.836.562</b>	<b>108.233.852</b>	<b>113.782.989</b>	<b>5,13%</b>
Saldos Vista	16.436.707	19.480.107	19.064.613	-2,13%
Dep. a Plazo	42.668.644	45.486.777	48.366.164	6,33%
Capital y Reservas	8.045.861	8.523.365	8.688.848	1,94%
<b>Utilidad</b>	<b>407.185</b>	<b>306.947</b>	<b>444.297</b>	<b>44,75%</b>

Fuente: www.sbf.cl.

### **1.2.2. Reseña histórica y evolución de BCI:**

El 10 de junio de 1937, luego de ser autorizado por el Decreto Supremo de Hacienda N°1683, BCI abrió sus puertas como una sociedad anónima de giro bancario. Desde su inicio el objetivo principal fue atender el sector productivo del país, enfocado principalmente a la pequeña y mediana empresa y a las personas. Desde sus orígenes, el BCI se ha caracterizado por su permanente calidad de servicio, espíritu innovador, y un decidido propósito de atender a los distintos segmentos de la economía.

BCI apunta a satisfacer y resolver las necesidades financieras de personas y empresas, ofreciendo una amplia gama de productos y servicios bancarios, buscando constantemente mejoras en sus operaciones, productos y servicios.

Después de la crisis de los años 80, BCI fue el primer Banco en prepagar su deuda con el Banco Central.

BCI, es miembro de la Confederación Internacional de Bancos Populares (CIBP), organización internacional con sede en Bruselas que reúne bancos cooperativos de todo el mundo.

### **Evolución de BCI:**

- **1956:** Abre sus puertas, la primera sucursal del Banco, en Valparaíso, primer puerto del país y plaza comercial por excelencia.
- **1978:** Se inicia el proyecto computacional más avanzado de la banca Chilena. BCI procesa las operaciones entre sucursales a velocidad electrónica, incluyendo el pago de los cheques en cualquier sucursal.
- **1989:** Como iniciativa única en el mercado, BCI ofrece el primer sistema de cuenta a la vista.
- **1992:** La comisión clasificadora de riesgo, autoriza a las administradoras de fondos de pensiones para invertir los recursos administrados, en acciones de BCI, primera y única institución bancaria que se hace acreedora de esta distinción.
- **1998:** BCI crea la novedosa modalidad de servicios bancarios a distancia que denomina TBANC.
- **2003:** Ingresa al Marketing Hall of Fame, distinción otorgada por la pontifica Universidad Católica de Chile.
- **2004:** El Banco destina el 54,4% de la utilidad obtenida el año 2003, es decir \$40.087,6 millones al fondo de reserva para futura capitalización.
- **2005:** BCI establece una oficina de Representación en Hong Kong, República Popular China.
- **2006:** BCI crea la nueva sociedad filial Administradora General de Fondos S.A., dirigida principalmente a administrar fondos de inversión de diferente naturaleza. El Instituto Chileno de Administración Racional de Empresas, ICARE, otorga a BCI, la distinción “Empresa Destacada 2006”, como reconocimiento por su gestión, la que promueve la innovación, calidad de servicio a sus clientes, así como la preocupación por sus colaboradores y la información que reciben sus accionistas. Es la primera vez que este reconocimiento lo recibe un Banco.
- **2007:** BCI cumple 70 años de vida, facilitando la vida a sus clientes e introduciendo singulares innovaciones que han trazado el andar del sistema financiero. Se destaca la implementación de “BCI 2010”, un ambicioso proyecto que cambia el modelo de negocios para competir mejor y transformar la forma de operar para sorprender al cliente. Comienza a operar la Banca Móvil BCI,

constituyéndose en una innovadora plataforma permite obtener productos bancarios mediante diversos medios, entre ellos, la telefonía celular. Se implementó el pago de cuentas mediante Cajeros Automáticos y se obtuvo por tercer año consecutivo, el premio al Concurso Anual de Memorias entregado por Revista Gestión y PriceWaterhouseCoopers.

- **2009:** Dentro de las innovaciones de BCI, este año destacan dos iniciativas únicas en el mundo: el chequemático; máquina que cambia cheques por dinero en forma automática y Magneprint; un sistema que evita la clonación de las tarjetas.

- **2010:** En la versión 2010 de la encuesta de empresas más admiradas, BCI sube desde el noveno puesto (2009) y por primera vez en los doce años de la encuesta, obtiene el gran premio, ganando en tres de las nueve categorías. Sus mejores notas son la "Capacidad de Innovación" (6,68), "Información al Exterior" (6,84) y "Gobierno de la Empresa" (6,41).

### **1.2.3. Productos y Canales de servicio y distribución de BCI:**

BCI cuenta con una serie de productos que son parte de la cartera de productos que ofrece la Banca en general, con pequeñas variaciones en su composición y precio, dentro de estos productos se encuentran las cuentas corrientes, cuentas primas, tarjetas de crédito y débito, líneas de sobregiro, líneas de emergencia, créditos de consumo, créditos comerciales, créditos hipotecarios, inversiones, depósitos a plazo y cuentas de ahorro, entre otros.

A fines del 2010, BCI contaba con una amplia red de 365 sucursales y puntos de contacto dentro de Chile, que le permiten estar siempre cerca de sus clientes y responder a sus necesidades con un servicio ágil y eficaz. Para mejorar la atención a los clientes, en el 2010, el Banco invirtió US\$ 57 millones en la remodelación, traslado y apertura de nuevas sucursales y puntos de atención.

Algunos de estos puntos son del tipo:

**a) Sucursales multiservicio:** entregan un servicio integral, con atención de ejecutivos y especialistas en inversiones, factoring, apoyo a empresarios, entre otros.

**b) Cajas auxiliares:** Puntos de contacto de formato pequeño, enfocado especialmente a los aspectos transaccionales y de tesorería. Cuentan con cajas, ATM y servicios básicos de consulta automatizados.

**c) Plataformas comerciales:** Son puntos de atención dirigidos a determinados segmentos de clientes, quienes reciben atención personalizada y exclusiva con ejecutivos especialistas que responden a sus necesidades.

**d) Sucursales premier:** Unidades exclusivas para clientes de la Banca Personas de BCI. Tienen un formato pequeño, entregan atención comercial y transaccional, aunque también se apoyan en los servicios automatizados.

**e) Banca privada y Banca preferencial:** Son oficinas enfocadas a servicios para clientes de alto patrimonio.

**f) Centro de atención a distancia (TBanc):** Banca que entrega servicios mediante teléfono e Internet, las 24 horas del día, todos los días de la semana.

**g) Puntos de venta:** Tienen un formato pequeño y atienden principalmente a la Banca de Personas. Cuentan con servicios de venta y postventa.

**h) Oficinas de servicios automáticos:** Cuentan con dispositivos electrónicos autosuficientes, que permiten realizar depósitos, giros, cambio y depósito de cheques, pago y solicitud de vales vista, y obtención de certificados.

**Tabla 2: Punto de Contactos.**

Puntos de Contacto	Bci	Bci Nova	Total
Sucursales multiservicio	198	78	276
Cajas auxiliares	11	1	12
Plataformas comerciales	37	-	37
Sucursales premier	16	-	16
Banca privada y banca preferencial	4	-	4
Centro de atención a distancia (TBanc)	1	-	1
Puntos de venta	18	-	18
Oficinas de servicios automáticos	1	0	1
<b>TOTAL</b>	<b>286</b>	<b>79</b>	<b>365</b>

Fuente: Memoria anual de BCI 2010.

#### 1.2.4. Situación Económica y Participación de Mercado:

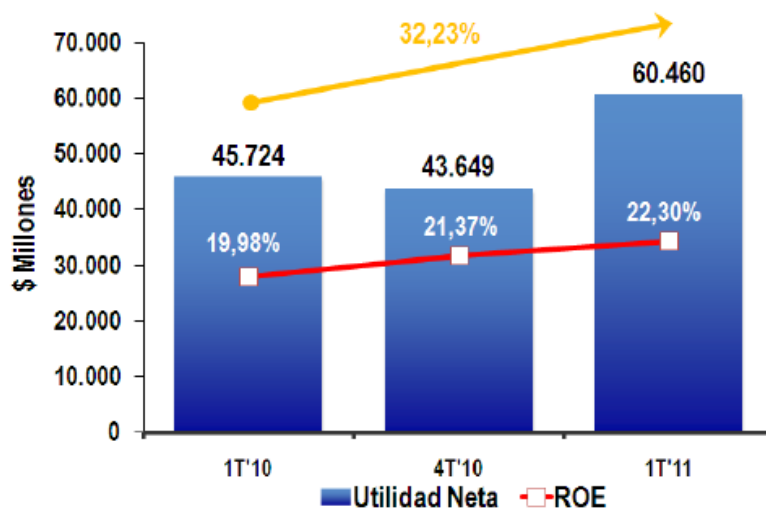
##### Utilidad Neta de BCI:

La Utilidad Neta de BCI durante el primer trimestre de 2011 totalizó en \$60.460 millones. Este resultado muestra, un aumento del 38,51% respecto al trimestre anterior y de 32,23% respecto al mismo trimestre del ejercicio 2010. Esto representa un resultado superior al acumulado en 2010, en \$14.736 millones, lo que muestra una recuperación con respecto a los resultados a comienzos de 2010, principalmente, explicados por un menor gasto en riesgo y un importante crecimiento del margen operacional.

El aumento de la utilidad trimestral respecto al mismo período del año anterior, se debe principalmente a un aumento en el Margen Bruto de \$18.770 millones y a la disminución del gasto en provisiones y castigos por \$8.972 contrarrestado por un aumento en gastos de apoyo por \$7.609 millones.

En términos de rentabilidad, el ROE anualizado al primer trimestre de 2011 fue de 22,30%, por sobre el 19,98% alcanzado en el mismo período del 2010. Esto, confirmando los buenos rendimientos mostrados por el Banco desde el segundo semestre del año 2009, cuando los efectos de la crisis financiera internacional comenzaron a ceder.

**Figura 1: Utilidad Neta**



Fuente: Memoria anual de BCI 2010.



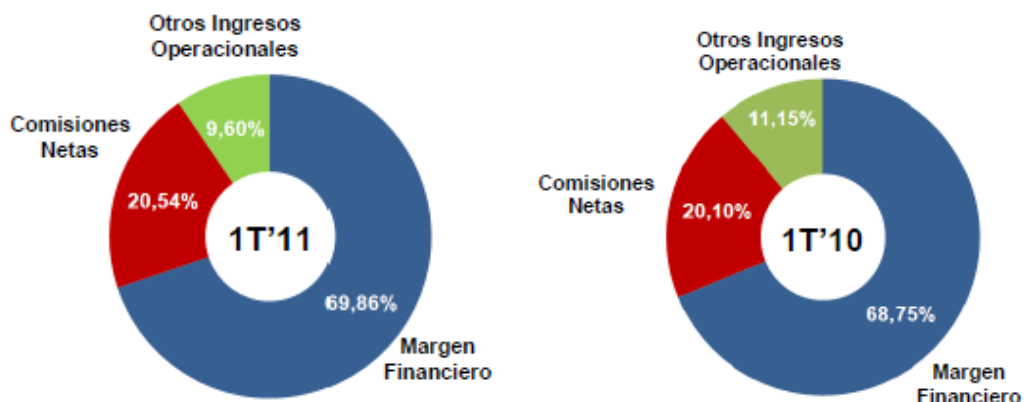
### **Margen Bruto:**

A nivel de Margen Bruto\*, BCI alcanzó \$188.137 millones durante el primer trimestre de 2011, lo que representa un incremento de 5,57% con respecto al trimestre anterior. Este aumento, se explica principalmente por incrementos en las operaciones de Banco Retail, y un eficiente manejo del gap de moneda, aprovechando el aumento de la inflación del primer trimestre comparado con el período anterior.

Con respecto al primer trimestre de 2010, los resultados del primer trimestre de 2011 fueron 11,08% mejor, debido principalmente a un aumento del Margen Financiero en \$14.994 millones.

Como se observa, BCI ha logrado mantener los niveles de generación de Margen Bruto, principalmente, mediante una buena estrategia de pricing de los distintos productos y un adecuado manejo de los descalces de moneda y tasas.

**Figura 2: Margen Bruto 1er Trimestre 2011 y Margen Bruto 1er Trimestre 2010**



Fuente: Memoria anual de BCI 2010.

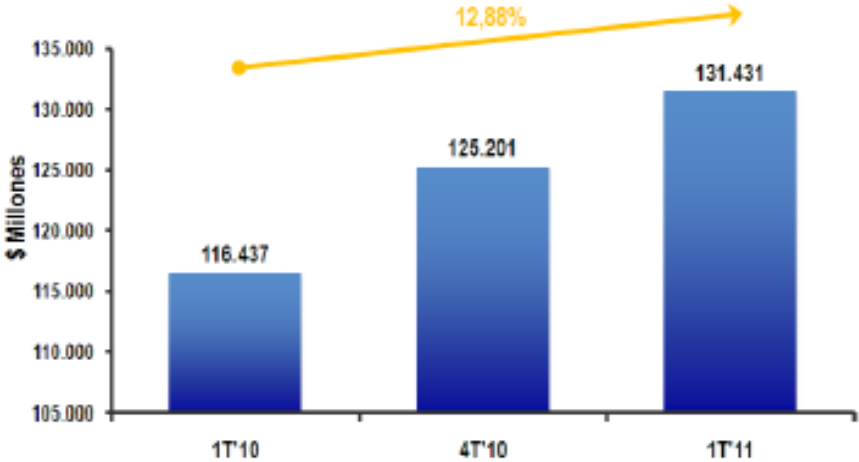
### **Margen Financiero:**

Durante el primer trimestre de este año, el Margen Financiero compuesto por intereses y reajustes, totalizó en \$131.431 millones, lo cual representa un aumento de 4,98% respecto al trimestre anterior explicado principalmente, por el aumento de inflación y la normalización de los spread de venta.

Ahora bien, comparado con el primer trimestre del año 2010, el Margen Financiero presenta un incremento de 12,88%, que se explica por la recuperación generalizada de las colocaciones comerciales de consumo y vivienda que se han visto impulsadas por el crecimiento y la recuperación económica, las bajas tasas en el mercado y los esfuerzos por la reconstrucción después del terremoto.

Por otra parte, el aumento del Margen Financiero con respecto al mismo período del año anterior, se explica por un eficiente manejo del descalce de tasas y por el impacto que tuvo la inflación en los activos denominados en UF, reflejado en los crecientes ajustes que tuvo durante el comienzo de este año.

**Figura 3: Margen Financiero**

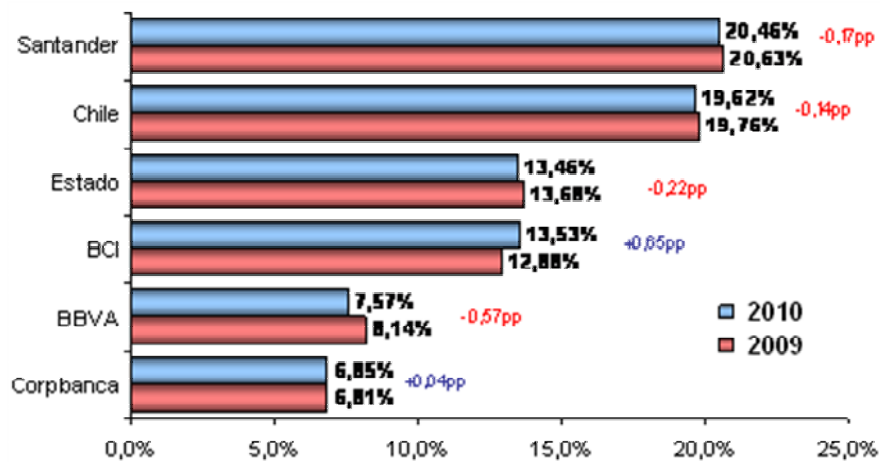


Fuente: Memoria anual de BCI 2010.

**Participación de Mercado:**

De acuerdo a la participación de mercado y los segmentos de clientes a los que apuntan, los principales competidores de BCI son Banco de Chile, Banco Santander Chile y el Banco Estado.

**Figura 4: Participación de Mercado 2009 - 2010**



Fuente: www.sbif.cl.

### **Principales competidores:**

**a) Banco de Chile:** Haciendo uso de los avances tecnológicos, el Banco de Chile ha transitado durante los últimos años hacia el mundo digital, con la finalidad principal de acercar cada vez más la información del Banco hacia los clientes. Ejemplo de esto, es la creación de “BanChile Inversiones”, en donde los clientes tienen acceso a información de distintos instrumentos, movimientos de mercado y en donde además pueden realizar operaciones en línea.

En definitiva la estrategia del Banco se enfoca en transmitir la entrega de servicios de calidad a través de procesos simples, controlables y medibles, los cuales han sido mejorados constantemente de acuerdo a estándares de servicios transparentes y diferenciados, según las necesidades del negocio. Todo lo anterior, de la mano de una infraestructura que soporte la estabilización, crecimiento y contingencia necesaria, junto con el desarrollo de metodologías de administración de ambientes tecnológicos.

**b) Banco Santander:** Cuenta con una fuerte presencia en mercados locales que combina políticas corporativas, capacidades globales y respaldo de su Casa Matriz en España. El cliente es el foco de la estrategia de esta institución financiera. Asimismo, aspira a mejorar de manera continua la captación, la satisfacción y la vinculación de los clientes a través de una amplia oferta de productos y servicios.

Santander Chile, ubica a sus clientes en diferentes tramos, donde todos son importantes, desde el cliente que cambia un cheque en la caja bancaria más cercana a su trabajo, hasta llegar al cliente con cuenta corriente y años de servicio en la empresa. Evalúan a sus clientes constantemente según sus estados de cuentas, prioridades, solicitudes de créditos, y vigilan desde cerca que sean personas confiables y durables en dicha identidad bancaria.

Por consiguiente, es dable concluir que el Banco Santander Chile ofrece productos y servicios financieros de valor agregado a todos los segmentos de clientes, con propuestas innovadoras que den respuesta a sus necesidades y a menor precio.

**c) Banco del Estado de Chile:** Pertenece en un 100% al Fisco de Chile y su patrimonio está conformado de capital único en pesos chilenos.

BancoEstado fomenta el ahorro en las personas, el endeudamiento responsable y el desarrollo de los micro y pequeños empresarios.

Para las personas, BancoEstado posee diversos instrumentos y sistemas seguros y fáciles de usar que implican importantes ahorros de tiempo y dinero, como Cuenta RUT y Caja Vecina.

Construye su estrategia sobre los cimientos de las declaraciones estratégicas fundamentales, contenidas en sus definiciones de visión y misión, así como en el posicionamiento que busca entre sus clientes.

El posicionamiento de BancoEstado se caracteriza por su cercanía y relación de largo plazo con sus clientes; por entregar un servicio de calidad competitiva; por su compromiso con el fomento del emprendimiento y la inclusión financiera; por su rol de banco estatal que promueve activamente la bancarización.

#### **1.2.5. Análisis Financiero y de Productos de BCI:**

##### **a) Análisis Financiero:**

El BCI determinó en mayo de 2010, una nueva estructura de segmentos con el fin de optimizar la atención a los clientes de acuerdo al producto y servicio, teniendo en cuenta las características comerciales más relevantes al respecto. Los nuevos segmentos son:

- Banca Comercial: Para personas jurídicas cuyas ventas superen las 12.000 UF anuales.
- Banco Retail: Para personas naturales y jurídicas con ventas inferiores a 12.000 UF anuales.
- Banco Finanzas e Inversión: Para operaciones de las áreas que administran posiciones propias (Trading), áreas de distribución, empresas corporativas, banca privada y áreas de balance.
- Filiales y otros: Incluye filiales como BCI Factoring; BCI Asset Management Administradora General de Fondos S.A.; BCI Corredores de Seguros S.A.; BCI Administrador General de Fondos S.A.; BCI Corredor de Bolsa S.A., BCI Asesoría Financiera S.A. y BCI Securitizadora S.A.

La asignación de gastos a los diferentes segmentos se desarrolla básicamente en 3 etapas:

- Gastos Directos: Sueldos, materiales, depreciaciones, etc.
- Gastos Indirectos: Telefonía, depreciación de bienes raíces en relación al número de metros cuadrados utilizados, etc.
- Gastos provenientes de Gerencias de apoyo: son asignados en función del tiempo y recursos que consuman.

Antiguamente, el Banco segmentaba en: Área Empresas, Área Personas, Área Finanzas y Filiales. El cambio más relevante, es el límite impuesto sobre la segmentación de Empresas y Personas, que eran 50.000 UF para ambas. Cambio relevante en ampliar la oferta, tanto en productos como acceso. Para las áreas de Finanzas y Filiales, el cambio fue marginal.

La estructura general del Activo versus Pasivo y Patrimonio es el siguiente:

**Tabla 3: Estructura general del Activo versus Pasivo y Patrimonio.**

ACUMULADO DICIEMBRE 2010	31 de diciembre de 2010				
	Empresas	Personas	Finanzas	Filiales y otros	Consolidado
	MM\$	MM\$	MM\$	MM\$	MM\$
ACTIVOS	6.019.548	4.123.928	2.809.537	251.161	13.204.174
PASIVOS Y PATRIMONIO	5.957.116	4.121.412	2.689.100	214.466	12.982.094
UTILIDAD	62.432	2.516	120.437	36.695	222.080

ACUMULADO DICIEMBRE 2009	31 de diciembre de 2009				
	Empresas	Personas	Finanzas	Filiales y otros	Consolidado
	MM\$	MM\$	MM\$	MM\$	MM\$
ACTIVOS	5.302.619	4.306.155	3.303.136	209.612	13.121.522
PASIVOS Y PATRIMONIO	5.234.299	4.290.277	3.265.593	170.579	12.960.748
UTILIDAD	68.320	15.878	37.543	39.033	160.774

Fuente: [www.bci.cl](http://www.bci.cl)

Respecto al resultado del ejercicio, tenemos para el 2010:

**Tabla 4: Resultado del ejercicio para el 2010.**

ACUMULADO DICIEMBRE 2010	31 de diciembre de 2010				
	Empresas	Personas	Finanzas	Filiales y otros	Consolidado
	MM\$	MM\$	MM\$	MM\$	MM\$
Ingresos netos por intereses y reajustes	125.161	226.039	141.673	22.851	515.724
Ingreso neto por comisiones	32.697	58.475	(1.932)	59.324	148.564
Otros ingresos operacionales	31.182	2.358	26.739	23.664	83.943
<b>Total ingresos operacionales</b>	<b>189.040</b>	<b>286.872</b>	<b>166.480</b>	<b>105.839</b>	<b>748.231</b>
Provisiones por riesgo de crédito	(45.603)	(66.578)	738	(4.804)	(116.247)
Ingreso operacional neto	143.437	220.294	167.218	101.035	631.984
<b>Total gastos operacionales</b>	<b>(68.218)</b>	<b>(217.263)</b>	<b>(22.113)</b>	<b>(70.157)</b>	<b>(377.751)</b>
Resultado operacional	75.219	3.031	145.105	30.878	254.233
Resultado por inversiones en sociedades	-	-	-	7.051	7.051
Resultado antes de impuesto a la renta	75.219	3.031	145.105	37.929	261.284
Impuesto renta	(12.787)	(515)	(24.668)	(1.234)	(39.204)
<b>UTILIDAD DEL EJERCICIO</b>	<b>62.432</b>	<b>2.516</b>	<b>120.437</b>	<b>36.695</b>	<b>222.080</b>

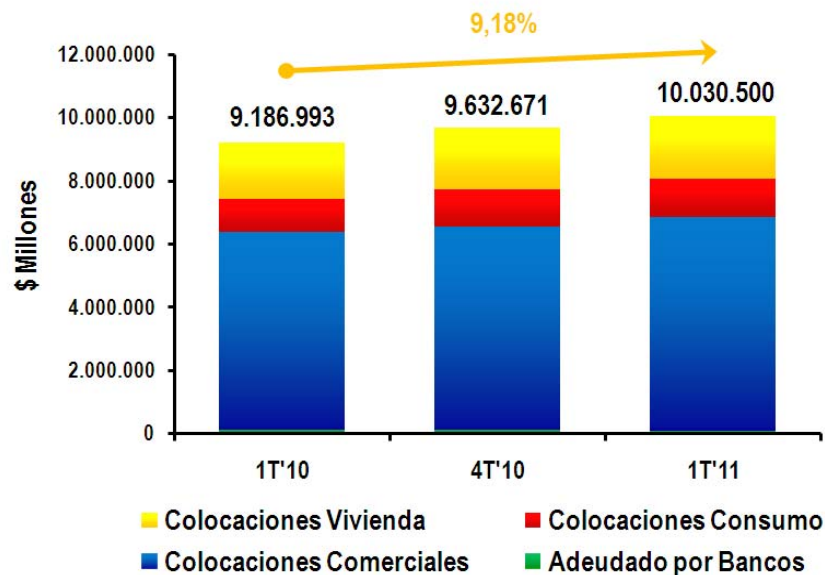
Fuente: [www.bci.cl](http://www.bci.cl)

Se generó un aumento del 38,1% para el 2010 respecto al 2009 en la utilidad del ejercicio. El canal de Finanzas (inversiones) aumentó considerablemente el 2010 en un 220%, compensando la baja en las de personas (-84%).

## b) Análisis de Productos:

BCI continúa ocupando el cuarto lugar en colocaciones (entendemos por Colocaciones a todos los Préstamos realizados por una institución financiera a una persona o empresa) en el sistema bancario, y en el tercer lugar entre los bancos privados.

**Figura 5: Total Colocaciones BCI Primer Trimestre 2011.**



Fuente: [www.bci.cl](http://www.bci.cl)

Importante es el Riesgo de la Cartera en este análisis y podemos exponerlo de la siguiente manera:

- La relación Provisión/Colocación alcanzó un 2,57% aumentando 27 puntos base respecto al 2010, esto principalmente, por el deterioro de algunos balances de clientes por la crisis subprime y la nueva normativa de IFRS de la SBIF.
- La política reservada del BCI le ha permitido tener una cobertura sobre el 100% en el ratio NPL (Relación de reservas para insolvencias de créditos morosos), salvo en el sector vivienda.
- El Gasto en provisiones y Castigos ha disminuido principalmente, por la mejora en la actividad económica y capacidad de pago de los deudores.

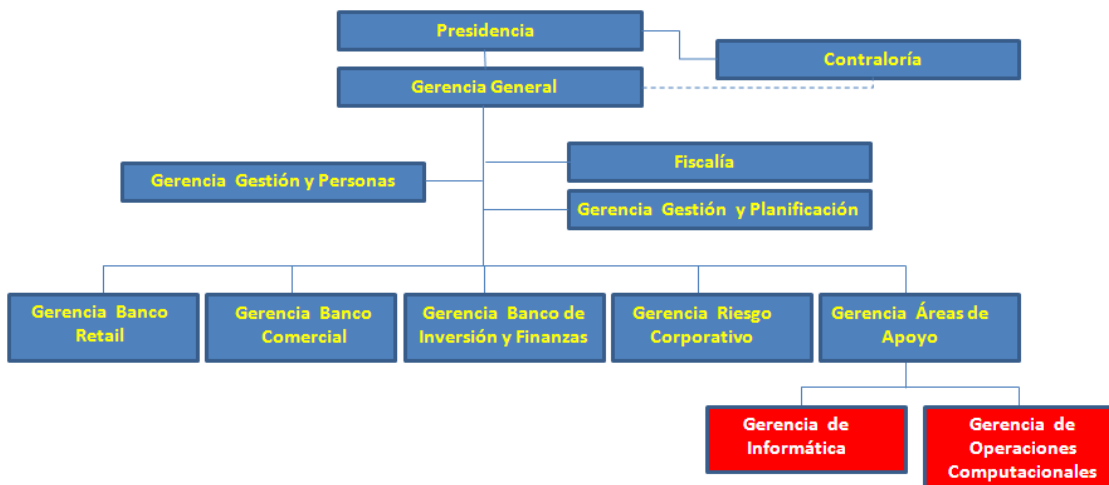
### c) Conclusiones del análisis:

El presente análisis financiero nos muestra que BCI tiene una solidez importante para sustentar confianza en sus clientes. La nueva forma de segmentar, le ha permitido ampliar y dar dinamismo a la cartera de clientes, así como contabilizar, de acuerdo a las necesidades de la empresa y pensando en cumplir con la normativa de la SBIF, sobre todo en el tema de IFRS. La distribución de gastos le da pie, a trabajar en el futuro con mayor eficiencia en los procesos. Ha sabido superar la crisis subprime y adaptarse a las debacles económicas, tanto nacional (terremoto) como internacionales (situación Europea), y así enfrentar de buena forma el repunte en la economía.

#### 1.2.6. Organización TI de BCI:

Para analizar la organización TI, es importante ubicar estratégicamente a las dos Gerencias que interactúan directamente con las tecnologías, estas son la Gerencia de Informática y la Gerencia de Operaciones Computacionales. En el siguiente organigrama del Banco se aprecia la dependencia de éstas:

**Figura 6: Organigrama BCI.**



Fuente: Desarrollado por Gonzalo Flores

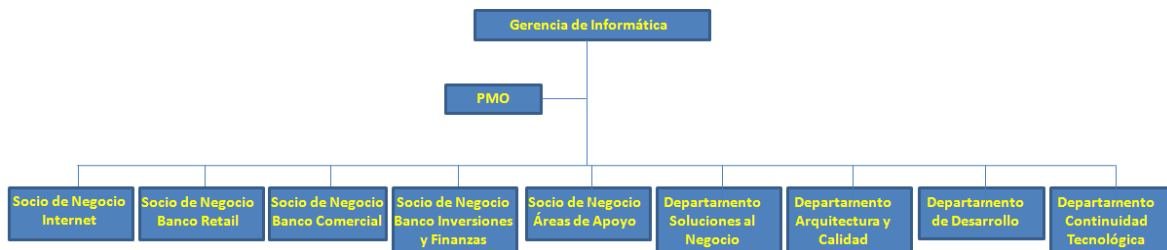


Como se puede apreciar en el Organigrama general del Banco, la Gerencia de Informática y la Gerencia de Operaciones Computacionales dependen de la Gerencia de Áreas de Apoyo, cuya función principal, es dar soporte a las necesidades internas del Banco para la entrega de servicios de calidad y efectivos.

Cada una de estas gerencias tiene las siguientes estructuras:

#### a) Gerencia de Informática:

**Figura 7: Organigrama Gerencia de Informática.**



Fuente: Desarrollado por Gonzalo Flores

Donde su misión principal es proveer y garantizar a BCI la infraestructura tecnológica, sistemas y modelamiento de información alineados con los procesos de negocio, apoyando la capacidad de diferenciarse a través de la tecnología, minimizando el riesgo tecnológico y agregando valor a los accionistas y clientes.

Las principales funciones de esta gerencia son:

- Maximizar el valor de la informática para BCI, asegurar su rentabilidad y apoyar la capacidad de diferenciarse de la institución, a través de la tecnología, con la finalidad de potenciar la competitividad de la institución en el mercado.
- Fomentar el uso adecuado de las tecnologías de información para el logro de ventajas competitivas de la corporación en el mercado, velando por el mejoramiento continuo de las prácticas, técnicas, herramientas y recursos asignados, maximizando la eficacia, eficiencia y seguridad de la gestión de informática.
- Proponer la planificación global de los proyectos informáticos de la Corporación, siendo responsable de la adecuada materialización de los

sistemas, aplicaciones y productos requeridos por la corporación, dirigiendo la gestión de desarrollo de las unidades de servicio bajo su responsabilidad, analizando los planes de trabajo, fijando prioridades, coordinando la asignación de recursos, orientando a través de instrucciones técnicas específicas y de normativa general, controlando los estados de avance de los proyectos y evaluando a su término el cumplimiento de los objetivos involucrados.

- Brindar un nivel de servicio informático óptimo a los clientes y a los usuarios internos de las aplicaciones y productos informáticos de la corporación, a través de una adecuada planificación, diseño, construcción e implantación de los sistemas de procesamiento de información, tanto centrales como distribuidos, garantizando en su diseño y construcción el aprovechamiento eficaz, eficiente y seguro de los recursos tecnológicos y el adecuado soporte a los usuarios de los servicios de la gerencia.

**Socios de Negocio:** La responsabilidad de los equipos de Socios de Negocios es estructurar y gestionar el desarrollo e implantación de productos y servicios de TI a través de un fuerte trabajo con los equipos de las áreas de negocio, en la definición y estructuración de sus portafolios de proyectos, con el fin de asegurar el cumplimiento estratégico de los mismos, mantener la continuidad operacional y asegurar la entrega de soluciones tecnológicas que apoyen la gestión y el logro de objetivos de las distintas líneas de negocio.

**Departamento de Arquitectura y Calidad:** Su principal responsabilidad, es definir la visión tecnológica de la Corporación y la arquitectura más adecuada para cada uno de los proyectos desarrollados por la Gerencia de Informática. Esta visión tecnológica incluye aplicaciones, plataformas de software, plataformas computacionales, redes, gestión de datos, seguridad y calidad de software.

**Departamento de Desarrollo:** Tiene como responsabilidad, la construcción de todas las soluciones tecnológicas de las distintas líneas de negocio, a través de la instrumentación de un conjunto de fábricas especializadas en diferentes tipos de

desarrollo. Adicionalmente, es garante de la certificación de las aplicaciones, el piloto, la puesta en producción y el cierre de los proyectos.

**Departamento de Continuidad Tecnológica:** Su responsabilidad, es dirigir y controlar la definición y mantención de las mejoras aplicativos y tecnológicas, a fin de asegurar el cumplimiento de estándares comprometidos y la continuidad operacional tecnológica y de aplicaciones que soportan productos y servicios del Banco. Este departamento debe velar por la adopción de las mejoras prácticas de la industria (ITIL), con el fin de asegurar la calidad de servicio que requiere la Corporación BCI, gestionando los incidentes que se produzcan y aplicando soluciones de fondo a los problemas que surjan. Además, es responsable de asegurar la actualización de las plataformas de hardware y software básico, tanto para las plataformas de sistemas computacionales, como para las redes y centrales telefónicas.

**Project Management Office (PMO):** Su responsabilidad principal, es dirigir y controlar el desarrollo del portafolio de proyectos de la Corporación, evaluando metodologías y definiciones y desarrollando un conjunto de indicadores que faciliten al Governance de TI, la evaluación de prioridades de inversión con bajos niveles de riesgo. En el desarrollo de sus funciones, debe facilitar la adopción de los procesos definidos entregando las facilidades de gestión del proceso y de los cambios que se estimen necesarios. Además, es responsable de la gestión de los presupuestos de proyectos y la correcta activación de los proyectos terminados.

## b) Gerencia de Operaciones Computacionales:

**Figura 8: Organigrama Gerencia de Operaciones Computacionales.**



Fuente: Desarrollado por Gonzalo Flores

Su función principal, es controlar el ambiente de producción tecnológico encargándose de funciones como la ejecución de procesos computacionales, monitoreo de procesos, administración de mallas automáticas de procesos, registro, gestión de cancelaciones de procesos, administración cambios de programas y su traspaso al ambiente de producción, administración de los centros de procesamientos principales del Banco, para los cual se definen protocolos formales.

**Área de Explotación:** Esta área, realiza funciones de explotación y soporte de sistemas (administración de espacio en disco y ejecución de proceso en producción), el ingreso de datos fijos a los sistemas (tablologos), administración de sistemas de cara al cliente para resolver pedidos, generación de cuadraturas, entre otras.

Realiza la administración de la producción (Mallas de procesos, Respaldos y plataformas de correo)

**Área de Operaciones:** Sus funciones principales, se concentran en proveer de continuidad operacional al Banco, a través del monitoreo 7x24 y control procesos, administración y mantención de los centros de procesamientos del Banco (Morandé y Longovilo).

**Área de Seguridad Operacional:** Esta área cuenta con cuatro subdivisiones que realizan diferente funciones:

- **Investigación y Monitoreo:** Responsable de prevenir fraudes internos y/o externos que afecten el patrimonio de BCI y clientes, de acuerdo a los requerimientos de la circular N° 3.400 de la SBIF, a través del continuo monitoreo y análisis de alertas sobre transacciones y comportamientos sospechosos.
- **Seguridad Operativa:** Responsable de la administración y monitoreo de la herramientas de software de seguridad tecnológica del Banco.
- **Usuarios Y Privilegios:** Responsable de la administración de cuentas de usuarios y privilegios de las distintas plataformas y sistemas computacionales de Banco.

- Mesa de Ayuda: Responsable de dar soporte a los usuarios internos del Banco ante problemas en los sistemas y equipos computacionales y telefónicos.

### 1.2.7. Instalaciones e Infraestructura:

El Banco para ofrecer sus servicios cuenta con una infraestructura compuesta por:

**a) Colaboradores:** BCI cuenta con aproximadamente 10.000 colaboradores distribuidos a través del País.

**b) Puntos de Contacto:** 365 puntos de contacto (sucursales) en todo el país incluyendo la Antártida.

**c) Infraestructura:** Cuenta con dos edificios Corporativos en los sectores de mayor movimiento comercial (Sector oriente y centro).

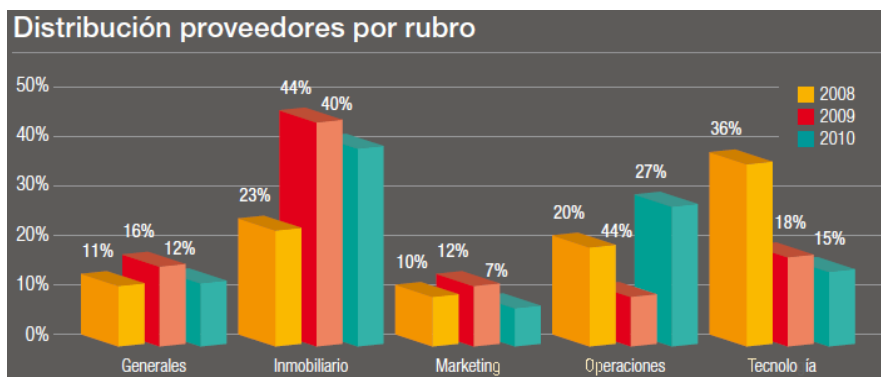
**d) Tecnología:** Cuenta con más de 800 sistemas de información y 30 plataformas tecnológicas distintas.

**f) Cajeros Automáticos:** 1.200 cajeros automáticos, repartido en distintos puntos del país.

**g) Centros de Procesamiento:** Dos centros de procesamiento a más de 100 Km de distancias con las más altas y sofisticadas medidas de seguridad (Santiago Centro - Longovilo).

**h) Proveedores:** Aproximadamente 800 proveedores de distinto tipo que se clasifican en:

**Figura 9: Distribución de Proveedores.**



Fuente: [www.bci.cl](http://www.bci.cl)

Adicionalmente, el Banco cuenta con una fuerza ventas externa, a través de la empresa Proservices. Esta empresa, utilizan los sistemas del Banco para ejecutar la campañas con clientes, a través de telefonía y visitas personalizadas.

Para el proceso de entrega de productos (Delivery), existen empresas externas como Messinger y Promobanc que se encarga de armar y sellar los productos y despacharlos.

### **1.2.8. Tecnología e Innovación BCI:**

BCI cuenta con una gran variedad de tecnologías para dar soporte a sus servicios y procesos.

#### **a) Tecnología:**

BCI se caracteriza por tener una gran variedad de tecnologías que integran la estabilidad y la innovación.

Para explicar las tecnologías utilizadas debemos separarlas en tecnologías de uso interno y de cara al cliente:

- **Tecnología de uso Interno:** En este aspecto el Banco cuenta con una mezcla de tecnologías de alta capacidad de procesamiento (Mainframe – IBM - Tandem) y tecnologías para la gestión de redes y archivos como Windows y Unix, con una serie de aplicaciones desarrolladas internamente y paquetes de software adquiridos con proveedores externos.

También el Banco ha optado por tecnologías ERP para algunos de sus procesos internos, como la administración de proveedores, para lo cual adquirió SAP.

- **Tecnología de cara al cliente:** Para la atención de clientes, el Banco utiliza plataformas amistosas, eficientes y seguras, principalmente, basada en internet, como WebLogic, WebSevices, Windows, Ephiphany (CRM), entre otros.

## **b) Innovación:**

Uno de los pilares de la estrategia de BCI es la innovación, lo cual ha permitido adicionar a los canales tradicionales, tales como:

- **Los cajeros automáticos 2.0:** Cobrar cheques, retirar transferencias y pagar cuentas, son algunas de las nuevas operaciones que se pueden hacer a través de los cajeros automáticos. Es que el sólo hecho de retirar dinero, dejó de ser la prioridad de estos instrumentos, además tienen que ser más humanos, sencillos y capaces de entregar mayor sensación de seguridad y privacidad. En los cajeros de mayor innovación, el cliente puede ver que está haciendo la plataforma en cada momento de la operación a través de la pantalla, asumiendo una virtualización de las transacciones, una mezcla de experiencia real con la virtual, dejando de lado la antigua pantalla en negro. Son capaces de realizar todo tipo de trámites y se puede acceder a un menú personalizado que reconoce las operaciones anteriores y los patrones de conducta del usuario (tecnología predictiva)

- **El Banco en el celular:** La banca móvil es una de las grandes innovaciones que están aplicando algunos bancos. Esta tendencia, responde a la importancia que está adquiriendo para los clientes la movilidad y poder hacer transacciones a cualquier hora, sin importar donde esté.

- **Maneje sus finanzas personales por el Banco:** Una de las principales líneas de desarrollo que está potenciando la banca, dice relación con ayudar al cliente a tener una visión más fácil de sus finanzas personales. En los próximos años, lo más probable es que los consumidores, logren incorporar y manejar el balance total de sus gastos a través del banco, aprovechando que este canal consolida gran parte de la información financiera del cliente, la cual además queda disponible en línea.

- **Seguridad – defina monto máximo de giros:** Evitar plagios y robos son parte de las estrategias que está intensificando el sistema financiero nacional para dar más seguridad a los usuarios. Por ejemplo, colocar límites personales a montos asociados a transacciones bancarias.

- **El portal de las inversiones:** La banca, en los últimos años ha ido ganando terreno como un canal que permita concretar las inversiones que desean realizar

sus clientes. En esta línea, las entidades financieras están derivando desde servicios puntuales que ofrecen para transacciones de fondos mutuos o acciones, a implementar portales que aporten contenidos que faciliten la decisión de los clientes.

- **Usuarios a la medida y solución de problemas:** Acelerar y optimizar el proceso de atención al cliente, es parte de la finalidad de la banca. Las instituciones financieras están o han implementado plataformas que permiten una mayor identificación del cliente cuando realizan llamadas por teléfono al banco. Rápidamente se analiza el segmento al que pertenece para derivar su llamado a equipos especializados. Con esto, se busca acelerar los trámites y reducir los tiempos de respuesta. Los énfasis de las sucursales físicas, que siguen siendo una parte importante de la relación con el cliente, también están sufriendo cambios. Se están complementando los modelos de atención con modelos de solución de problemas, donde la idea es que el cliente ahorre el mayor tiempo posible cuando visita la sucursal.

- **Sólo con la huella digital:** El uso de la huella digital para identificarse, es otra tendencia que se observa en el sistema financiero. Por ejemplo, en algunos casos ya no es una obligación para obtener una clave automática, acercarse al mesón, mandar una solicitud y esperar para obtenerla. Ahora, con la huella digital y el RUT existen cajeros que te entregan la clave de manera automática.

- **Educación financiera:** El objetivo es, explicar de manera sencilla y transparente los temas relacionados con los servicios y productos financieros.

- **TV Baking (Banco por televisión):** A través de operadores de cable que poseen la tecnología, se implementa un Menú interactivo a través del cual se pueden hacer compras y consultar por el estado de los productos de Cuentas Corrientes.

- **Redes Sociales:** A través de Twitter y Facebook se captura reclamos y sugerencias por parte de clientes y no clientes y se responden en el corto plazo.

- **Sucursales Lean:** Sucursales con atención personalizada, con una plataforma tecnológica sofisticada pero amistosa para los clientes, entre otros.



### **1.2.9. Compromiso de Transparencia BCI:**

El cliente es el elemento central de la visión y misión de BCI. Por ello, desde sus inicios, el Banco ha trabajado para construir relaciones de largo plazo con los distintos segmentos de clientes, generando lealtad y confianza. Para lograr este objetivo, la Corporación ha puesto especial atención en el tema de la transparencia.

En esa línea, se inserta el concepto de marca “Somos Diferentes”, que plasma uno de los objetivos que el Banco se ha propuesto: ser distinto del resto de la industria, no sólo por la innovación en los productos y servicios financieros, sino también por la transparencia con los clientes.

En los últimos cinco años, BCI ha realizado cambios importantes en el acceso de los clientes a la información. Para ello, actualmente cuenta con diversos canales de información que permiten contactarse con BCI las 24 horas al día y los siete días de la semana, sin importar el lugar donde se encuentren los clientes. Uno de ellos es “BCI Directo”, una plataforma telefónica que permite a sus clientes realizar diversas operaciones y transacciones bancarias, y comunicarse con un ejecutivo de lunes a domingo, a cualquier hora del día o de la noche.

En el año 2007, el Banco lanzó el documento “Nuestro compromiso con usted, BCI al servicio de sus clientes”, que regula la forma de relacionarse con ellos y de entregarles soluciones financieras.

Durante el año 2010, BCI siguió fortaleciendo la transparencia de cara a los clientes e implementó una serie de iniciativas concretas para alcanzar este objetivo.

Uno de los principales focos de BCI, fue fortalecer la comunicación con los clientes, para asegurarse que tuvieran claridad respecto a los productos y servicios que contratan y sus condiciones asociadas. Para que los clientes adopten las mejores decisiones en este sentido, el Banco amplió la información de su página web, con un lenguaje claro y fácil de entender, un formato atractivo y el apoyo de videos didácticos.

En la misma línea, con el fin de mantener a los clientes informados, el Banco envió más de cinco millones de emails con los estados de cuentas para los usuarios de cuentas corrientes, líneas de crédito y tarjetas de crédito. Estos correos detallaron las comisiones asociadas a los servicios contratados con el Banco y la tasa de interés de los productos de crédito. En los casos en que las condiciones fueron actualizadas, la información fue entregada en forma oportuna a través de cartas, según la normativa vigente.

BCI también realizó modificaciones relevantes a los contratos, para facilitar su lectura y que los clientes tuvieran absoluta claridad de sus condiciones, cuando se adquiere un nuevo producto.

En la red de sucursales, el Banco incorporó nuevos dispositivos que permiten mantener información actualizada y en línea para los clientes. El Banco cuenta con 50 sucursales que tienen soporte digital dual view, es decir, pantallas que refrescan permanentemente las condiciones de los productos de inversión.

Además, BCI se preocupó de enseñar a los clientes las distintas formas en que pueden hacer llegar sus inquietudes y solicitudes al Banco. Para facilitar el contacto, se abrieron distintos canales de comunicación en línea con los clientes, como; mail específico con la Gerencia General, mensajes de texto SMS y Twitter. Estas iniciativas tuvieron una muy buena acogida. En 27% de los casos los clientes felicitaron a BCI por la respuesta entregada.

El Programa de Educación Financiera realizado por BCI también apuntó a una mayor transparencia con los clientes, específicamente con el nivel socio económico C3-D, segmento que cuenta con un bajo nivel de bancarización. Este proyecto ayudó a promover el endeudamiento responsable y entregó herramientas para que las personas estuvieran mejor informadas al momento de contratar un determinado producto financiero. A través de BCI Nova, el Banco ha capacitado a más de 1.200 personas a través de charlas y clínicas bancarias gratuitas y abiertas a toda la comunidad.

### **1.2.10. Responsabilidad social BCI:**

Una de las iniciativas más destacadas en Responsabilidad Social Empresarial (RSE) fue la mitigación de los efectos de la huella de carbono producidos por los eventos corporativos de BCI, con el fin de hacer un aporte concreto al medio ambiente. El proyecto de mitigación consideró la forestación de áreas desprotegidas en la cuenca de Santiago, que se implementó a través de un programa de voluntariado. En éste, participaron más de 100 colaboradores de BCI y sus familias, quienes plantaron más de 500 árboles en la ribera del río Colina.

BCI suscribió una alianza con Fundación Enseña Chile y, de esta manera, renovó su compromiso y contribución con la educación chilena de los sectores más vulnerables del país. Esta alianza implica que el Banco participe en el Consejo Directivo de la Fundación, contribuyendo con ideas y experiencia, además de los aportes en materia de liderazgo, a través de la Academia Líder BCI.

## **1.3. DESCRIPCIÓN DEL RIESGO EN LA ORGANIZACIÓN**

### **1.3.1. Administración de Riesgo en BCI:**

El riesgo del negocio de BCI es administrado por la Gerencia de Riesgo Corporativo, que está encargada de evaluar y manejar el riesgo crediticio, de mercado, de liquidez y operacional.

En el ámbito de las empresas, la Gerencia de Riesgo Corporativo, junto a las áreas comerciales, evalúa en forma individual, bajo modelos propios, el financiamiento de proyectos o de empresas pertenecientes a distintos sectores económicos, como generación eléctrica, industria, minería e infraestructura, entre otros. Adicionalmente, esta área cuenta con una unidad de riesgo internacional, que evalúa también la situación económica, política y social de cada país en el cual BCI está presente, con el fin de acotar el riesgo de las operaciones de financiamiento externo, así como de clientes locales con operaciones en dichos países.

En lo que se refiere a la evaluación de riesgo de los créditos a personas, especialmente los créditos de consumo e hipotecario, se aplica un modelo de provisiones sustentado en la pérdida esperada. Esta última, se estima a partir del comportamiento estadístico de pago de los deudores y su probabilidad de incurrir en incumplimiento. Este programa, es continuamente revisado en su nivel de predicción y busca prevenir pérdidas futuras contempladas para un período de 12 meses.

La administración del Riesgo se divide en:

- Riesgo Financieros.
- Riesgo de Crédito.
- Riesgo de Liquidez.
- Riesgo Operacional.

Específicamente para el riesgo operacional existe un marco de gobernabilidad interno de BCI se compone de los siguientes participantes:

**Figura 10: Marco de Gobernabilidad del Riesgo Operacional en BCI**



Fuente: Gerencia de Riesgo Operacional BCI

Las provisiones por riesgo se componen de tres factores; el riesgo de crédito, el riesgo de mercado y el riesgo operacional, y se han calculado históricamente a través de las siguientes formulas normativas:

<b>Basilea I</b>	<b>Basilea II</b>
$\frac{\text{Capital Regulatorio}}{\text{RC} + \text{RM}} \geq 8.0\%$	$\frac{\text{Capital Regulatorio}}{\text{RC} + \text{RM} + \text{RO}} \geq 8.0\%$

A partir del 2004 (Basilea II) se comenzó a incorporar el Riesgo Operacional a la formula y en general, las provisiones no pueden ser inferiores a un 8% del Margen Bruto.

Existen tres modelos para calcular la provisión de capital, estos son:

**a) Modelo Básico:** Este modelo es el más simple de todos e indica que la provisión por riesgo operacional se calcula de la siguiente forma:

$$\text{Provisión de capital RO} = \text{Margen Bruto} * 15\%$$

Para BCI a diciembre de 2010 este valor representaba MM\$ 85.658 de provisiones de capital por concepto de Riesgo Operacional.

**b) Modelo Estándar Alternativo:** Este es el modelo utilizado actualmente por la Banca y exigido por la SBIF para el cálculo de provisiones y consiste en generar a través de paneles de expertos una sensibilización y medición del impacto del riesgo separado por Riesgo de Crédito, Riesgo de Mercado y Riesgo Operacional, de acuerdo a una base de datos histórica de pérdidas, con la cual se calcula el porcentaje de impacto en riesgo de cada una de estas áreas y ese porcentaje se multiplica por el margen bruto:

$$\text{Provisión de capital} = (\% \text{ R. Mercado} + \% \text{ R. Crédito} + \% \text{ R. Operacional}) * \text{Margen Bruto}$$

A diciembre de 2010 el Riesgo Operacional en BCI aportaba con un 13,6% del margen bruto a la provisiones, lo que se traduce a MM\$ 77.540 en provisiones de

capital solo por este concepto, donde no existe una clasificación o separación de lo que implica o aporta el riesgo tecnológico dentro de esta cifras.

**c) Modelo Avanzado:** Actualmente sólo es exigencia en países como Estados Unidos, España y Holanda, sin embargo, en Chile sólo se han realizado iniciativas por parte de algunas instituciones, dentro de las cuales se encuentra BCI, por comenzar a utilizar estos modelos.

Este modelo consiste en desarrollar 4 aspectos para medir cualitativa y cuantitativamente el riesgo, tal como los muestra el siguiente esquema:

**Figura 11: Modelo Avanzado de Cálculo de Provisiones.**



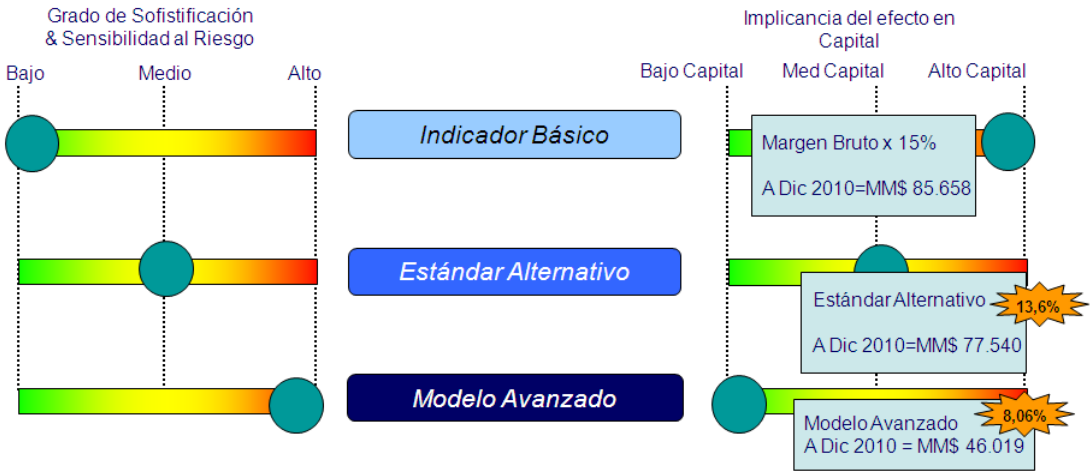
Fuente: Gerencia de Riesgo Operacional BCI

En diciembre de 2010 BCI realizó un primer ejercicio informal utilizando un modelo avanzado, desarrollado al interior del Banco, con el cual se demostró un importante ahorro en provisiones de capital logrando bajar el porcentaje de riesgo operacional al 8,06%, lo que representa MM\$ 46.019 en provisiones de capital por

riesgo operacional. No obstante, este modelo avanzado nuevamente no consideró, en específico, aspectos de riesgo tecnológicos, objetivo que es parte de esta tesis.

Comparativamente, la aplicación de los tres modelos de cálculo de provisiones por riesgo operacional se refleja en el siguiente diagrama:

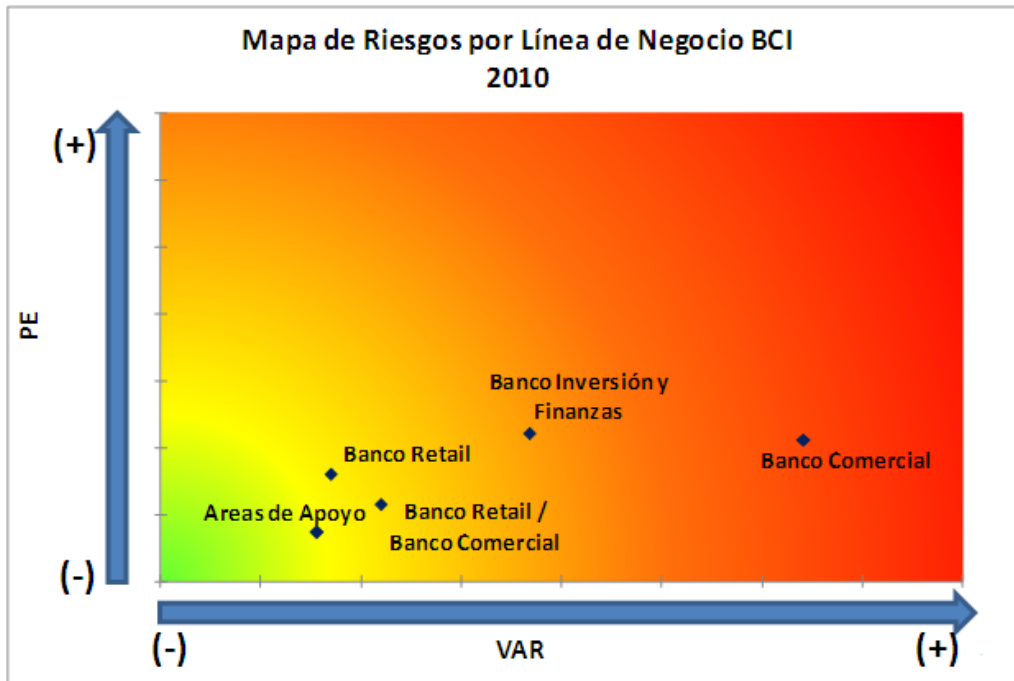
**Figura 12: Comparación entre Modelos de Cálculo.**



Fuente: Gerencia de Riesgo Operacional BCI

Por último, si analizamos el mapa de riesgos operacionales del Banco a diciembre de 2010, éste nos indica que las Área de Apoyo, donde se encuentra incluida Tecnología (no dimensionada), está evaluada como uno de los riesgos más bajos a nivel de pérdidas esperadas (PE) y por su valorización de riesgo (VaR):

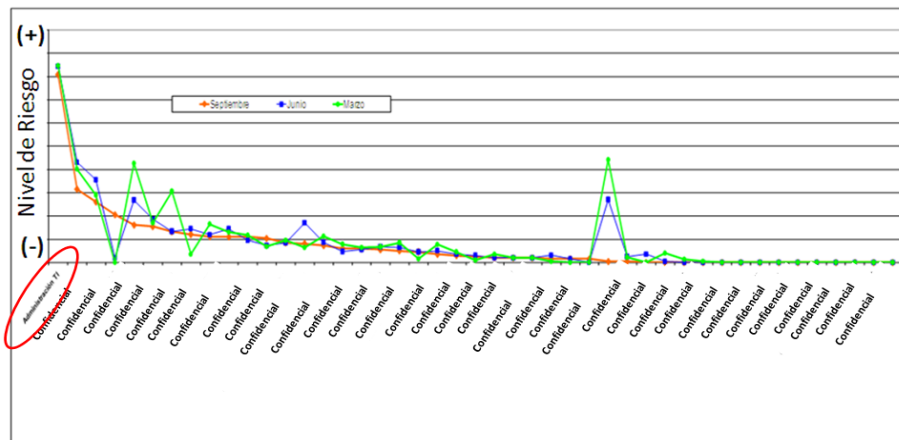
**Figura 13: Mapa de Riesgos Operacional por línea de negocio.**



Fuente: Gerencia de Riesgo Operacional BCI

Si comparamos esta gráfica con los riesgos levantados por la Contraloría durante el 2010, se aprecia una inconsistencia, ya que los principales riesgos del Banco se concentran en la administración TI:

**Figura 14: Mapa de Riesgos de Contraloría.**



Fuente: Gerencia de Contraloría BCI

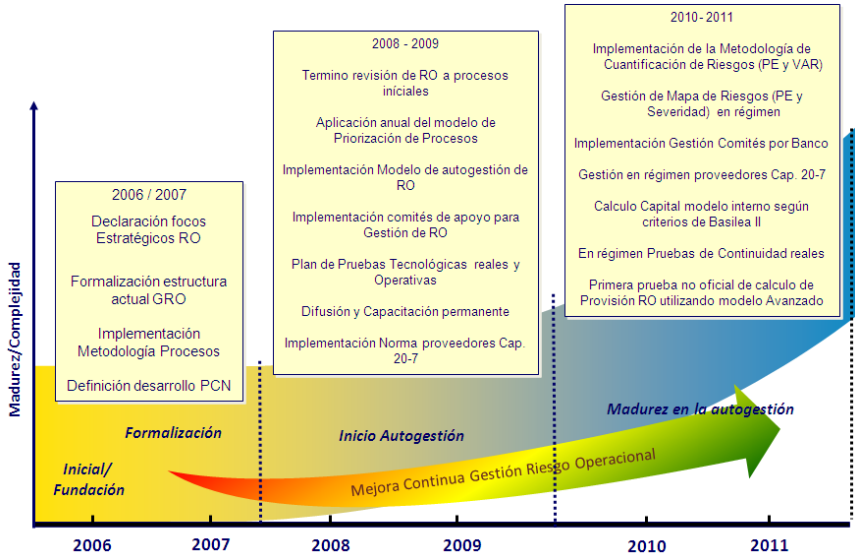
De esta manera, claramente se sustenta una mejora al modelo general, incorporando la gestión de riesgos tecnológicos, para disminuir los eventuales



eventos de pérdidas y a través de la adecuada gestión, aumentar el ahorro en provisiones por este tipo de riesgos.

**1.3.2. Evolución del Riesgo Operacional en BCI:**

**Figura 15: Evolución del riesgo Operacional.**



Fuente: Gerencia de Riesgo Operacional BCI

De acuerdo a evolución del Riesgo Operacional en BCI, si bien existe un área de Seguridad de Información, aún no se han desarrollado iniciativas para incorporar la gestión de Riesgos Tecnológicos, utilizando la metodología de perdida esperada y Value at Risk (VaR), parte del objetivo de este proyecto.

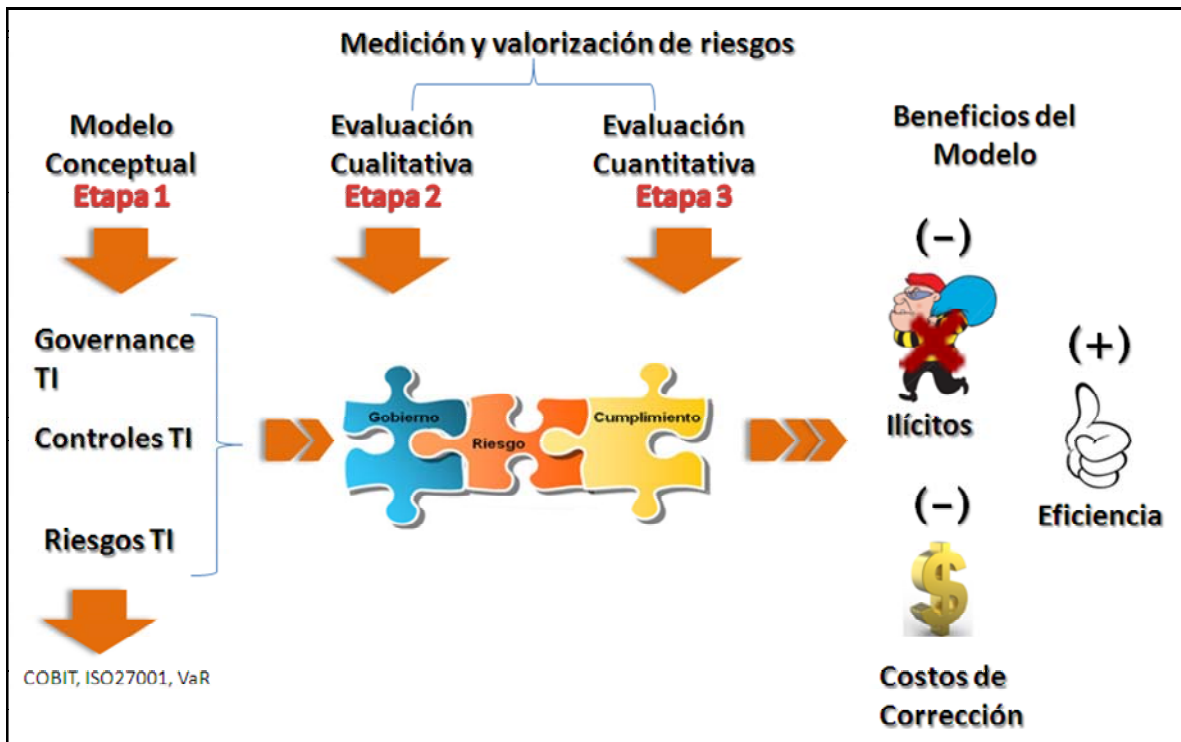
## **CAPITULO 2: DESCRIPCIÓN DEL MODELO A DESARROLLAR**

El modelo propuesto consiste, en una primera etapa, en el desarrollo de un marco conceptual que reúne a los procesos considerados como claves para el monitoreo de riesgos de tecnología, basado en las mejores prácticas recomendadas por el estándar Cobit, identificando los controles claves asociados a los procesos TI seleccionados.

En una segunda etapa, se establecerán métricas idóneas para medir el riesgo, efectividad y cumplimiento de cada uno de los controles claves seleccionados, información que puede ser utilizada para gestionar mejoras a los controles y de esta manera los niveles de riesgo podrán disminuir.

Finalmente, en una tercera etapa, se desarrolla un modelo estadístico de evaluación cuantitativa del riesgo operacional tecnológico, tomando como base metodológica un modelo conceptual desarrollado por PricewaterhouseCoopers, el acuerdo de Basilea II y la metodología Value At Risk (VaR), que permite realizar la gestión de toda la información proveniente de las entradas definidas en la primera etapa del Modelo, estableciéndose una manera de integrar toda la información de riesgos generada, transformándose en un panel de luces de los principales riesgos asociados a los procesos tecnológicos, niveles de cumplimiento, efectividad de los controles y la valorización asociada a estos riesgos. Tal como muestra el siguiente diagrama:

**Figura 16: Modelo Propuesto por esta Tesis.**



Fuente: Desarrollado por Gonzalo Flores

## 2.1. OJETIVOS DEL MODELO.

- Aportar, de aquí a tres años, con una disminución del 20% del porcentaje de provisiones por riesgo operacional calculado a través de modelos avanzados (8,06%), esperando llegar a un 6,44% del Margen Bruto en 3 años, es decir MM\$ 36.769, ahorrando al Banco MM\$ 9.250 en provisiones. Para diciembre de 2011, a través de esta tesis, se espera disminuir en un 5% el porcentaje de provisión por riesgo operacional (8,06%), es decir llegar a un 7,65% del margen bruto con un ahorro de MM\$ 2.340 en provisiones (bajar provisiones por RO, de MM\$ 46.019 a MM\$43.678).
- Mejorar el proceso de gestión de riesgos tecnológicos de BCI, mediante el desarrollo de un modelo potente, que conecte en forma natural indicadores asociados a los elementos tecnológico principales sujetos a riesgo del Banco, con un proceso de cálculo y valorización de estos riesgos, permitiendo mejorar

la efectividad de los controles, y permitiendo maximizar la calidad de los servicios tecnológicos entregados, aportando a la disminución de los gastos en corrección de errores y eventuales ilícitos.

- Mejorar la gestión del gobierno corporativo del Banco.
- Fomentar la gestión proactiva en lugar de la reactiva.
- Mejorar la identificación de oportunidades y amenazas para el Banco.
- Mejorar la confianza de los grupos de interés (Stakeholders).
- Establecer una base sólida y fiable para la toma de decisiones y planificación.
- Repartir y utilizar de forma efectiva los recursos para gestión de riesgos.
- Mejorar la prevención de incidentes.
- Minimizar las pérdidas.

## **2.2. ALCANCES DEL MODELO.**

En esta investigación, se pretenden identificar los aspectos fundamentales para evaluar y cuantificar el riesgo operacional tecnológico de BCI. Para el desarrollo de esta propuesta de investigación, se desarrollará un prototipo de modelo de evaluación y cuantificación del Riesgo Operacional Tecnológico, asociado a una muestra de los principales procesos del Banco, que permita determinar niveles y rangos de riesgos adecuados para cada uno.

El Modelo como propuesta, se enfocará en la evaluación cualitativa y cuantitativa de 4 controles claves TI, lo cual implica el desarrollo de indicadores, escalas de medición y formulas matemáticas de cuantificación, y de un proceso de clasificación de eventos de pérdida históricos asociados a los riesgos tecnológicos seleccionados y entrevistas con paneles de expertos. Luego, a través de un modelo de cálculo avanzado, se determinará un monto de provisión ajustado por concepto de Riesgo Operacional Tecnológico.

El modelo propuesto, no considera la gestión para corregir los problemas encontrados en la medición, ya que esto es parte del proceso normal de mejora continua del Banco.

El proceso clave asociado al Plan de Continuidad de Negocio no será abordado en esta tesis, ya que en el Banco este proceso, es administrado por un área independiente de la Gerencia de Informática y el proceso de valorización de riesgos de los distintos escenarios de contingencia es efectuado utilizando los Análisis de Riesgos (RIA) y Análisis de Impacto en el Negocio (BIA).

El modelo propuesto permitirá su complementación y ampliación de su alcance en nuevas etapas, lo que implica que a medida que transcurra el tiempo, se incorporarán nuevos controles claves y se ajustará aun más el resultado del cálculo.

También es parte de este modelo, efectuar un ejercicio de cálculo del Riesgo Operacional Tecnológico, a objeto de validar si efectivamente hay una reducción de las provisiones en el porcentaje planteado como objetivo para fin de año (5% menos).

### **2.3. RESULTADOS ESPERADOS**

A través del este modelo se pretende mejorar la efectividad de los controles en los distintos procesos y servicios de tecnología de BCI, estableciendo un proceso de medición y cuantificación que adicionalmente permitirá disminuir de manera importante (más de MM\$2000) los montos de provisiones por concepto de riesgo operacional, permitiendo al Banco contar con estos fondos para mejorar sus utilidades anuales.

Adicionalmente, a través de este modelo, se pretende alcanzar dentro del marco de mejoramiento continuo del Banco, los siguientes resultados:

- Calidad de servicio: Diminución de reclamos y de tiempos muertos por fallas tecnológicas.
- Disminución de errores: Bajar los costos asociados a mantenciones correctivas de sistemas y plataformas tecnológicas.

- Disminuir los riesgos de seguridad de la información asociados a la pérdida de confidencialidad, disponibilidad e integridad de la información de los clientes del Banco.
- Cuantificación del Riesgo Tecnológico para provisionar de forma más exacta el ítem de riesgo operacional.

El siguiente diagrama muestra el modelo de mejora continua, a través del cual se pretende mejorar el cálculo de provisiones:

**Figura 17: Modelo de mejora continua propuesto.**



Fuente: Desarrollado por Gonzalo Flores

A través de la revisión y evaluación constantes de los controles tecnológicos, los errores y fallas serán corregidos, disminuyendo las pérdidas reales y las

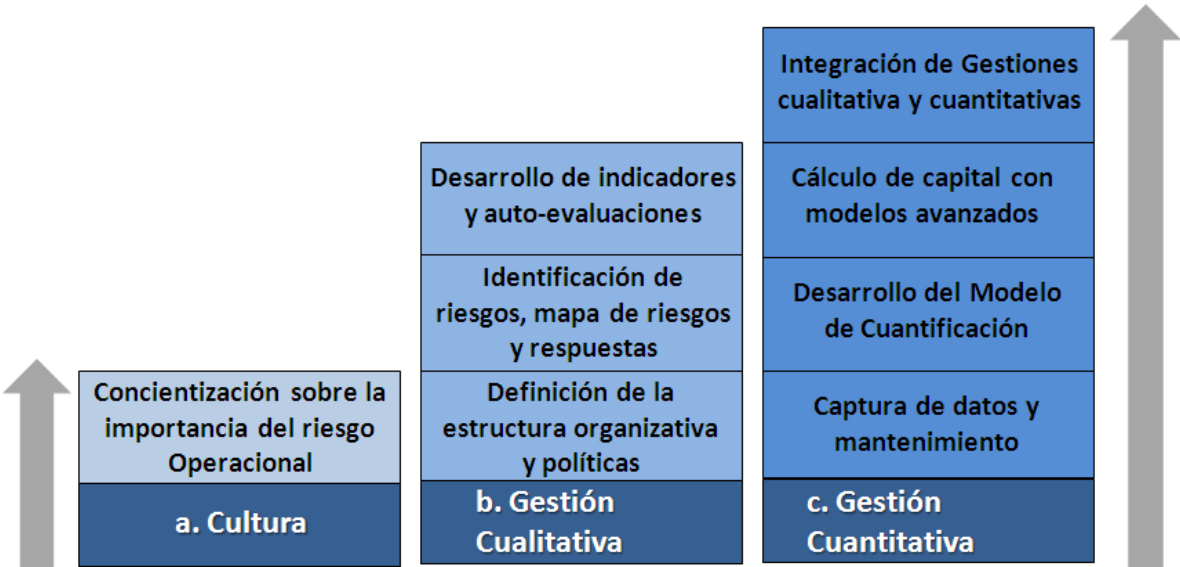
percepciones de riesgo, impactando positivamente en los procesos de votación y valorización de riesgos y en las provisiones por este concepto.

**2.4. MARCO CONCEPTUAL**

Para desarrollar el modelo, utilizaremos la definición de Riesgo Operacional Tecnológico que nos entrega la Superintendencia de Bancos e instituciones Financieras (SBIF) y que lo plantea como “la probabilidad de pérdidas ante fallas de los sistemas de información, así como a la probabilidad de fraudes internos y externos a través de los mismos”. Utilizaremos la definición de Enfoques de Medición Avanzados (EMA) que nos entrega el Acuerdo de Basilea II y que lo plantea como el “mecanismo que utiliza la estimación de distribuciones de probabilidad, para lograr una medición del capital requerido mucho más ajustado a la situación particular de cada entidad” y como conceptos claves utilizaremos las definiciones establecidas en el anexo A: Riesgo en la Banca.

En relación a las etapas de desarrollo requeridas para nuestro modelo, utilizaremos los conceptos y definiciones metodológicas efectuadas por la Consultora PricewaterhouseCoopers y que son las siguientes.

**Figura 18: Metodología de PricewaterhouseCoopers.**



Fuente: Metodología pública de PricewaterhouseCooper

**a) Cultura:** Este primer aspecto, ya está implantado en BCI e implicó el convencimiento de la alta dirección de los beneficios y de la necesidad de implantar un marco que administre el riesgo operacional. Dentro de las razones para dicha administración, es posible mencionar:

- Las exigencias regulatorias.
- La comprensión del impacto del riesgo operacional.
- La necesidad de obtener información de gestión sobre las causas y consecuencias del riesgo operacional.
- El poder asignar el capital según el riesgo asumido.
- La necesidad de obtener más información que permita mejorar las decisiones sobre la mitigación del riesgo operacional.

**b) Gestión Cualitativa:** Este paso, considerará tres aspectos claves: la identificación de riesgos tecnológicos, el modelo organizativo para administrarlos y las herramientas de gestión utilizadas. El primer paso, consiste en la elaboración de un mapa de procesos tecnológicos del Banco que sirva para detectar los riesgos y controles existentes basados en metodologías como Cobit e ISO 27001, así como también, para realizar una valoración en términos de severidad y frecuencia de los eventos de pérdidas.

A nivel organizativo, resulta vital la existencia de una unidad independiente, responsable por la gestión del riesgo operacional tecnológico y en BCI esta unidad es la Gerencia de Riesgo Operacional, sin embargo, el proyecto será impulsado por la Gerencia de Contraloría, dado que actualmente es la unidad de la organización con más conocimiento de los riesgos tecnológicos del Banco.

Por último, es necesario el desarrollo e implantación de herramientas para la gestión cualitativa del riesgo operacional como mapas de procesos y riesgos, indicadores de riesgo, alertas, bases de datos y, por sobre todo, auto-evaluaciones (auditorías internas de riesgo tecnológico).

**c) Gestión Cuantitativa:** Un aspecto fundamental del modelo, es poder pasar de un enfoque cualitativo a un marco de gestión cuantitativa del riesgo operacional



tecnológico, a través de la generación de una base de datos de pérdidas operacionales tecnológicas.

Una vez finalizada la construcción de la base de datos, se abordará el desarrollo del modelo de medición del riesgo operacional tecnológico.

Como el Banco debe regirse por el nuevo acuerdo de Basilea II, existe la intención de posicionarse en un enfoque avanzado, tanto por los beneficios de gestión, como por los potenciales ahorros de capital regulatorio.

Por último, se debe realizar la integración final de los aspectos cualitativos y cuantitativos. Esto implica el diseño y el establecimiento de las relaciones entre los datos recopilados, los indicadores, los mapas de riesgos y controles y las mediciones de capital. Este enfoque debe ser dinámico y confluir en el establecimiento de un plan de acciones correctivas para afrontar las debilidades detectadas.

Como referencia para este modelo de cuantificación de riesgos tecnológicos, se debe considerar las siguientes etapas propuestas por la Metodología VaR que es una metodología utilizada en la Banca Europea, la cual es la más avanzada en modelos de cuantificación:

**Figura 19: Metodología Value At Risk.**



Fuente: Metodología Value At Risk.

De estas etapas, las únicas con las que el Banco ya tiene avances son el Marco de Gestión (1) y la Base de Datos de Pérdidas (3), la que tiene una historia desde el 2004 en adelante, sin embargo, no se ha efectuado la identificación, clasificación y valorización de los riesgos tecnológicos. El resto de las etapas son parte del desarrollo de este proyecto.

## **2.5. ANÁLISIS FODA PARA EL MODELO PROPUESTO**

Un paso importante para establecer el modelo de gestión de riesgos tecnológicos, es la determinación de las ventajas y desventajas, así como, de oportunidades y amenazas de la implementación de éste en la organización, esto nos ayudará posteriormente a realizar mejores estimaciones, supuestos y detectar potenciales riesgos a los que se puede enfrentar el proyecto en el corto y mediano plazo.

#### **a) Fortalezas:**

- BCI es una empresa acostumbrada a cambios organizacionales y tecnológicos, debido a la cultura de innovación existente, lo que podría facilitar la implantación de nuevos controles o modelos.
- La Gerencia de Contraloría, donde se desarrollará el modelo, cuenta con una vasta experiencia e información de la organización, sus procesos y sus riesgos, incluyendo los tecnológicos (más de 40 años). Adicionalmente, cuenta con una gran reputación al interior de la organización, lo cual servirá al momento de determinar los riesgos principales y sustentar la implantación del modelo.
- Existen gran motivación en la alta administración del Banco, para desarrollar modelos de provisiones más exactos y que permitan mejorar el ambiente de control interno.
- 4 de los 9 objetivos estratégicos del Banco, están contenidos en los objetivos del modelo (objetivos estratégicos del Banco: aumentar la utilidad con riesgo acotado sobre el capital, aumentar la eficiencia, entregar servicios de calidad a los clientes e innovar para agregar valor), lo que permite contar con un proyecto muy alineado a los objetivos estratégicos de la organización.

#### **b) Oportunidades:**

- Existe una normativa de la Superintendencia de Bancos e Instituciones Financieras (SBIF) que propone el uso de modelos avanzados para el cálculo del Riesgo Operacional, propuesta que aún no tiene fecha límite de implantación obligatoria, sin embargo, en el corto y mediano plazo, los Bancos deberán contar con modelos avanzados, por lo que BCI podría estar preparado con anterioridad para cualquier exigencia normativa.

- Marcar un precedente en la Banca con un modelo inédito en Chile, para la medición y cuantificación del riesgo operacional tecnológico, que podría ser utilizado por otras empresas del rubro financiero y de otros rubros también.
- Los ahorros en provisiones pueden ser utilizados para potenciar la gestión y mejora continua del Banco, de modo de hacer sus procesos más eficientes y seguros.
- Aportar directamente a los objetivos de rentabilidad y eficiencia que posee el Banco BCI.
- El modelo a implantar es totalmente optimizable y complementable en el tiempo, con lo cual, los beneficios pueden aumentar a medida que éste madure en la organización.
- Establecer una imagen de líder en gestión de riesgos internos de cara a los stakeholders y al servicio que es entregado a los clientes.

**c) Debilidades:**

- En la gerencia de Informática no existe una cultura adecuada para administración del riesgo TI, lo que se refleja en los indicadores de riesgo del Banco generados por la Gerencia de Contraloría, en base a las auditorías realizadas.
- No existen referencias en el mercado chileno, respecto de la implantación de modelos avanzados de cálculo de riesgo operacional TI, para efecto de incorporar mejoras a estas experiencias, en el modelo propuesto.
- Insuficiente infraestructura (normativa interna, procedimientos y tecnologías) para medir en detalle el riesgo de los diferentes Procesos TI del Banco.

- Ausencia de interpretaciones adecuadas del riesgo TI e impacto de éste sobre los procesos de negocio del Banco.

**d) Amenazas:**

- La situación económica internacional, podría provocar eventuales recesiones o impactos negativos en la economía que afecten el comportamiento de pago de los clientes del Banco, afectando los índices de provisiones de éste.
- El nuevo acuerdo Basilea III, aun no presentado en Chile, propone nuevas exigencias para el resguardo de capitales que son mucho más exigentes que los propuestos por Basilea II, por lo que las eventuales rebajas en las provisiones que tiene como objetivo el modelo de gestión de riesgos TI propuesto, podrían verse afectadas producto del aumento de los porcentajes mínimos exigidos de provisión.
- El Banco es una empresa que se caracteriza por su gran potencial en innovación, especialmente en tecnología, sin embargo, el afán de implantar productos y procesos innovadores antes que la competencia, aumenta los riesgos operativos tecnológicos, debido a que muchos de los controles existentes podrían no ser efectuados correctamente, aumentando el nivel de riesgo y por ende las provisiones.
- De no existir un buen proceso de gestión del cambio incorporado al proceso de gestión de riesgos TI, el modelo podría fracasar y perder exactitud en el tiempo, ya que la medición y la mejora continua que deben efectuar las distintas personas y áreas involucradas, son parte esencial del modelo.

**2.6. PREGUNTAS CLAVES.**

A través de esta tesis se intentará responder las siguientes preguntas que se han definido como claves:

- ¿A los bancos les interesará implementar un modelo de este tipo para bajar sus provisiones?
- ¿Le agrega valor a los bancos?
- ¿Constituye una ventaja competitiva para los bancos implementarlo?
- ¿Se podrán generar en el futuro otras alternativas menos costosas para bajar las provisiones?
- ¿Por qué no hay bancos con modelos de gestión de riesgo TI implantados?
- ¿Se podría comercializar el modelo en otras industrias?
- ¿El dejar fuera del modelo algunos riesgos TI, afectará la precisión de este?
- ¿Se puede bajar el riesgo tecnológico al mínimo a través de este modelo?
- ¿Está preparada la organización para una medición de este tipo?

## 2.7. FACTORES CRÍTICOS DE ÉXITO.

- **Apoyo de la alta administración:** La alta administración del Banco debe estar de acuerdo y ser Sponsor de un modelo de estas características.
- **Cultura organizacional:** Se requiere en la organización de una cultura de riesgo y control fuerte, apoyado por adecuadas políticas y normativas claras.
- **Participación de expertos:** Se requiere de la participación de la mayor cantidad de expertos del Banco en el proceso de identificación y valorización de los riesgos TI.

- **Plan de implantación y comunicación:** Debe generarse un proceso paulatino de implantación del modelo de medición de controles, acompañado de un proceso de comunicación adecuado y apoyado ojalá por un proceso de Change Management, que permita evitar impactos negativos y de resistencia al cambio, por problemas culturales de la organización.
- **Tecnologías de apoyo:** Se debe contar con adecuadas herramientas tecnológicas para efectuar los procesos de levantamiento, evaluación, medición y valorización de riesgos TI, a objeto de abarcar la mayor cantidad de procesos y controles TI, de modo de hacer la medición mucho más exacta y cercana a la realidad.

## **CAPITULO 3: ANÁLISIS DE LOS MODELOS DE CÁLCULO EXISTENTES**

### **3.1. ANÁLISIS DE LA REGULACIÓN EXISTENTE PARA LA GESTIÓN DE RIESGO OPERACIONAL.**

Este capítulo, tiene por objetivo identificar los conceptos, lineamientos y exigencias existentes para la Banca, respecto de la medición del riesgo operacional, y que el modelo propuesto tenga aplicabilidad y sustentabilidad para ser replicado en cualquier tipo de empresa.

#### **3.1.1. Evolución hacia Basilea II de la Banca Chilena.**

La regulación local básicamente está determinada por la Superintendencia de Bancos e Instituciones Financieras de Chile (SBIF), la cual a su vez, regula la aplicación de modelos de cálculo para los requerimientos de capital (provisiones) por concepto de riesgo.

El riesgo operacional, es una de las áreas temáticas de la evaluación de gestión para las instituciones financieras, basadas en las mejores prácticas internacionales.

El capítulo 1-13 de la Recopilación Actualizada de Normas (RAN) disponible en [www.sbif.cl](http://www.sbif.cl), indica en términos generales la utilización de buenas prácticas en la gestión del riesgo operativo, destacándose entre otras la seguridad de la información, la continuidad del negocio y la calidad de la información, productos y servicios, materias que son evaluadas en función de estándares internacionales.

En enero del 2005, la SBIF emitió la “Hoja de Ruta” para la transición de la banca chilena hacia Basilea II, en la cual se señala el método de cuantificación de los riesgos operativos, considerando que para su medición se utilizará el método estándar alternativo.

Algunas acciones emprendidas por Chile, hacia Basilea II son:

- Evaluación externa del cumplimiento de los principios básicos de supervisión efectiva del Comité de Basilea.



- Perfeccionamiento del sistema de clasificación de cartera y construcción de provisiones.
- Aplicación de un nuevo modelo de supervisión orientado hacia la gestión de los riesgos.
- Convergencia de las normas contables a estándares internacionales.
- Cuantificación del impacto del nuevo acuerdo de capital para el sistema en su conjunto.

### **3.1.2. Evolución hacia Basilea II de la Banca Internacional.**

El espectacular colapso de Barings en 1995, el ataque terrorista al World Trade Center, los 691 millones de pérdidas por fraudes que reportó el Allied Irish Bank en 2002 y la gran falla eléctrica que afectó a 50 millones de personas en el noreste de los Estados Unidos y Canadá en agosto de 2003, son casos concretos, pero muy diferentes, de riesgo operativo.

Bancos y empresas están estableciendo posiciones de gerencia para manejar estos riesgos resultantes de inadecuados o fallidos procesos internos (ya sea de las personas o de los sistemas), o debido a eventos externos. Típicamente son errores en el procesamiento de transacciones, fallas en los sistemas informáticos, robo, fraude, juicios y actividades, de empleados o terceros, que lleven a pérdidas o daños en los activos.

Estos tres son los principales riesgos identificados por el Comité de Supervisión Bancaria de Basilea que representa a los Bancos Centrales de Alemania, Bélgica, Canadá, España, Estados Unidos, Francia, Gran Bretaña, Holanda, Italia, Japón, Luxemburgo, Suecia y Suiza. El comité fue establecido en 1974 y se reúne cuatro veces al año para desarrollar estándares de supervisión bancaria y guías de mejores prácticas para los sistemas bancarios nacionales.

En junio de 1999, el Comité lanzó una propuesta para un Nuevo Marco de Adecuación de Capital conocido como Basilea II. Los tres pilares del control bancario son, según Basilea II; la adecuación de capital por riesgo de mercado, de crédito y operativo; la supervisión bancaria por parte del Banco Central del país en

cuestión y la disciplina de mercado. Esto dio un impulso notable a la elaboración de modelos para medir riesgo operativo, los cuales están en constante desarrollo. De acuerdo a lo anterior, la evolución de la implementación de Basilea II en la región, la representaremos en 5 países:

**a) Brasil:** El Banco Central do Brasil, está planificando emitir una regulación cualitativa sobre riesgo operacional, no obstante, el riesgo operativo ha sido evaluado por la supervisión como un riesgo relevante que debe ser considerado por el directorio y la alta gerencia, de acuerdo a lo requerido por la regulación de control interno y las guías de supervisión. Dicha regulación, establece que todos los riesgos inherentes a las actividades de una institución financiera deben ser identificados, incluyendo: riesgo de crédito, riesgo de mercado (incluyendo riesgos de tasa de interés, tipo de cambio y precios), riesgo de liquidez, riesgos operativos, legales y reputacionales.

Los riesgos operativos, legales y reputacionales no son fáciles de adaptar a las técnicas cuantitativas de gestión de riesgo. Sin embargo, es responsabilidad de la alta gerencia la identificación y entendimiento de estos riesgos, así como el establecimiento de políticas de control interno y procedimientos para mitigar su potencial impacto negativo en la fortaleza y viabilidad económico-financiera.

**b) Colombia:** La Superintendencia Financiera de Colombia (SFC), a través de la Circular Externa 46, fijó las bases y los lineamientos mínimos que deben ser implementados para el desarrollo de un Sistema de Administración del Riesgo Operativo (SARO). Definen al Riesgo Operacional (RO) como la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en los recursos humanos, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y (a diferencia de Basilea II) también el riesgo reputacional.

La SFC establece que las entidades sometidas a su supervisión se exponen al RO y por lo tanto, deberán desarrollar, establecer, implementar y mantener un SARO, acorde con su estructura, tamaño, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente el RO.

**c) Guatemala:** Los artículos 55 y 56 de la Ley de Bancos y Grupos Financieros (LBGF), contemplan que los bancos y los grupos financieros deberán contar con procesos integrales, para la administración del riesgo operativo que incluyan sistemas de información y un comité de gestión de riesgos. Todo ello, con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos, además de contar con políticas escritas actualizadas, para una adecuada administración de los diversos riesgos a que están expuestas.

Por su parte, el oficio No. 1216-2003 de la Superintendencia de Bancos (SB), en materia de riesgo operativo, incluyó como requerimientos mínimos a los bancos del sistema, lo siguiente: a) sistema de control interno que incluya políticas y procedimientos para identificar, monitorear, controlar y mitigar las exposiciones al riesgo operativo en todos los productos, procesos y sistemas existentes o en proyecto; b) identificación de procesos críticos de las operaciones, incluyendo aquellos donde exista dependencia de proveedores externos; c) planes de sustitución o relevo cuando se identifiquen personas claves dentro de la organización; y d) planes de contingencia y continuidad de negocios.

Cabe mencionar que actualmente, la SB se encuentra trabajando en las normas de general aplicación y requisitos mínimos que los bancos deben de cumplir con relación a los diversos riesgos que asumen, incluyendo el riesgo operativo.

Guatemala experimenta dificultades al introducir prácticas internacionales, debido a que el país está todavía en proceso de implementar prácticas de gestión de riesgo y de obtener datos e información que posibilitará evaluar este tipo de riesgos. Es por ello que todavía no ha determinado el método más acorde ni ha establecido un cronograma de implementación de requerimientos de capital para riesgo operativo, en función de los lineamientos de Basilea II.

**d) Honduras:** El Artículo 30, Sección 4 de la LSF obliga al Directorio de las Entidades Financieras a asegurar que se implementen y mantengan apropiados sistemas de gestión y control de riesgos. Esto también es requerido por la regulación de gobierno corporativo. Las normas para auditores internos requieren el examen de la efectividad de los controles internos en la mitigación del riesgo operativo.

**f) Estados Unidos:** Las agencias de supervisión poseen una gran cantidad de orientación sobre gobierno corporativo, controles internos y seguimiento e información en sus respectivos procedimientos y políticas de inspección. Todas las agencias tienen normas para operaciones sanas y seguras y para la protección de la información sobre los clientes. Además, existen varias normativas interinstitucionales que cubren temas relacionados con la estructura de control interno. Entre ellas, por ejemplo, el manual sobre la planificación de la continuidad de la actividad de mayo de 2003 (Federal Financial Institutions Examination Council's (FFIEC's) Business Continuity Planning Booklet), el manual sobre la seguridad de la información, de enero de 2003 (FFIEC's Information Security Booklet), las declaraciones de política interinstitucionales sobre la tercerización del tratamiento de la información y de las transacciones (Outsourcing of Information and Transaction Processing) de febrero de 2000 y la orientación sobre la gestión de riesgos de la tecnología tercerizada (Guidance on the Risk Management of Outsourced Technology) de noviembre de 2000.

La política de inspecciones y procedimientos pueden ser encontrados en los sitios web siguientes:

- [www.ffiec.gov](http://www.ffiec.gov)
- [www.fdic.gov](http://www.fdic.gov)
- [www.frb.gov](http://www.frb.gov)

### **3.2. LEVANTAMIENTO DEL PROCESO DE CÁLCULO Y MEDICIÓN ACTUAL DE RIESGO OPERACIONAL EN BANCO BCI.**

Esta etapa tiene por objetivo, identificar los conceptos utilizados en la metodología actual de medición y valoración del riesgo operacional en BCI, a objeto de utilizar parámetros compatibles en el modelo a desarrollar, que puedan ser incluidos a la metodología actual y que permitan potenciar los indicadores actuales.

### **3.2.1. Metodología actual de Cálculo de Riesgo Operacional.**

El Banco actualmente, utiliza como metodología de cálculo de provisiones por Riesgo el modelo estándar alternativo, sin embargo, para explicar este método es necesario entender el modelo estándar, donde las actividades del Banco se dividen en 8 líneas de negocio:

1. Finanzas Corporativas, 2. Negociación y Ventas, 3. Banca Minoristas, 4. Banca Comercial, 5. Pagos y Liquidación, 6. Servicios de Agencia, 7. Administración de activos, 8. Intermediación minorista.

En ingreso bruto de cada línea de negocio, es un indicador amplio que permite aproximar el volumen de operaciones del Banco y con ello, el nivel de riesgo operativo que es probable que asuma en estas líneas de negocio. El requerimiento de capital de cada línea de negocio, se calcula multiplicando el ingreso bruto por un factor (denominado beta) que se asigna a cada una de las líneas. Beta se utiliza como una aproximación a la relación que existe, en el conjunto del sector bancario, entre el historial de pérdidas debido al riesgo operativo de cada línea de negocio, y el nivel agregado de ingresos brutos generados por esa misma línea de negocio. Es importante resaltar que, en el modelo estándar, se calcula el ingreso bruto de cada línea de negocio y no el obtenido por el Banco en su conjunto.

La exigencia de capital, se calcula como la media de 3 años de la suma simple de las exigencias de capital en cada una de las líneas de negocio en cada año.

Los rubros contables que definen el concepto de ingreso bruto en el Estado de Resultados Consolidado corresponden a la agregación de:

**5003:** Ingreso neto por intereses y reajustes.

**5004:** Ingreso neto por comisiones.

**4300:** Utilidad neta de operaciones financieras (excluyéndose el ítem 4300.3).

**4350:** Utilidad (pérdida) de cambio neta.

**4700:** Resultado por inversiones en sociedades.

Luego el requerimiento total de capital puede expresarse como:

$$KTSA = \frac{1}{3} \left\{ \sum_1^3 \text{Máx} \left[ \sum_1^8 \beta_i * GI_i; 0 \right] \right\}$$

Donde:

KTSA = exigencia de capital en el método de estándar.

GI<sub>i</sub> = ingresos brutos anuales para cada una de las 8 líneas de negocio.

β<sub>i</sub> = porcentaje fijo, establecido por el Comité de Basilea, que relaciona la cantidad de capital requerido, con el ingreso bruto de cada una de las 8 líneas de negocio. Los valores de beta se detallan en la siguiente tabla:

**Tabla 5: valores beta por Línea de negocio.**

Línea de Negocio	Factor Beta
Finanzas Corporativas	β <sub>1</sub> = 18%
Negociación y Ventas	β <sub>2</sub> = 18%
Banca Minoristas	β <sub>3</sub> = 12%
Banca Comercial	β <sub>4</sub> = 15%
Liquidación y Pagos	β <sub>5</sub> = 18%
Servicios de Agencias	β <sub>6</sub> = 15%
Administración de Activos	β <sub>7</sub> = 12%
Intermediación Minorista	β <sub>8</sub> = 12%

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

Para implantar un método alternativo estándar (Alternative Stándar Approach - ASA), el Banco debió demostrar mejoras, como por ejemplo: eliminar la doble contabilización de los riesgos y debió ser autorizado por la SBIF.

En el modelo ASA, la metodología es la misma utilizada para el modelo estándar, salvo en dos líneas de negocio; Banca Minorista y Banca Comercial. En el caso de estas líneas de negocio, los préstamos y anticipos, multiplicados por un factor fijo “m”, sustituyen a los ingresos brutos como indicador de riesgo. Los factores beta de la banca minorista y de la banca comercial, son los mismos que en el método estándar. El requerimiento de capital por riesgo operativo en el modelo ASA, en el caso de la banca minorista (la misma fórmula básica es aplicable a la banca comercial), es el siguiente:

$$KRB = m * \beta RB * LARB$$

Donde:

KRB = requerimiento de capital de la línea de negocio de banca minorista.

$\beta$ RB = factor beta de la línea de negocio de la banca minorista.

LARB = importe total pendiente de los préstamos y anticipos (no ponderados por riesgo y brutos de provisiones), promediado durante los 3 últimos años.

M = 0,035

Finalmente, el Banco debe multiplicar KRB por 12,5 para convertir el requisito de capital regulatorio por riesgo operacional en un equivalente al activo ponderado por riesgo. Lo anterior, bajo el supuesto que el requisito mínimo de suficiencia de capital es de 8 %.

## CAPITULO 4: DESARROLLO DEL MODELO DE GESTIÓN DE RIESGOS TI

### 4.1. LEVANTAMIENTO Y DESCRIPCIÓN DE LOS PRINCIPALES PROCESOS TECNOLÓGICOS DEL BANCO Y SUS CONTROLES ASOCIADOS.

Esta etapa, tiene por objetivo identificar los principales procesos tecnológicos y de gestión TI de acuerdo a los estándares y mejores prácticas internacionales y determinar los controles claves de cada uno, para que luego a través de una muestra de 4, éstos sean evaluados, medidos y valorizados a través del modelo.

#### 4.1.1. Identificación de procesos críticos TI.

Para determinar los procesos críticos TI, utilizaremos la Metodología Cobit, la cual cubre los siguientes aspectos de riesgos:

**Tabla 6: Controles basados en Cobit.**

<b>Proceso de Cobit</b>	<b>Procesos TI de BCI</b>	<b>Control Clave BCI</b>
Administración de la Calidad	Proceso de certificación (QA) de aplicaciones	Control de Incidentes en Producción
Adquirir y mantener software aplicativo	Proceso de Desarrollo y Mantenimiento de Sistemas	Control de Catalogación y vueltas atrás
Definir y administrar niveles de servicio	Proceso de Explotación y Monitoreo de Sistemas	<b>Fuera del Alcance</b>
Seguridad de Sistemas	Proceso de Control de Accesos	Control de Accesos y cambios en Bases de Datos en producción.
Administración de Capacidades	Proceso de Capacity Planning	<b>Fuera del Alcance</b>
Administración de Medios	Proceso de Soporte y Mesa de Ayuda	Control de Virus y securitización de equipos
Monitoreo de Control Interno y regulatorio	Proceso de Auditoría Interna y externa	<b>Fuera del Alcance</b>

Fuente: Metodología Cobit.



De acuerdo a los procesos que la metodología Cobit define como claves, se asociaron los procesos internos referentes y similares a los propuestos por el estándar:

**a) Administración de la Calidad:** En el Banco existe un proceso de desarrollo y mantención de aplicaciones, en el cual existen distintas etapas, siendo una de las más importantes el proceso de certificación de aplicaciones, en el cual destacan certificaciones de tipo full y las certificaciones fastrack, donde la primera consiste en aplicar el plan de pruebas en su totalidad, y el segundo esquema consiste en probar el cambio específico realizado. Este último esquema, se utiliza para implantaciones de programas cuya justificación es una contingencia.

**b) Adquirir y mantener software aplicativo:** El proceso de desarrollo del Banco exige documentación formal para los requerimientos, presupuestos, evaluación de factibilidad técnica y económica del proyecto, manuales técnico y de usuarios.

Existe un proceso llamado Catalogación, el cual consiste en la autorización para traspasar un nuevo programa desde el ambiente de desarrollo, al ambiente de producción, para lo cual, es necesario validar que se hayan cumplido todos los requerimientos de control que exige la metodología de desarrollo, más las etapas de la metodología de certificación de aplicaciones y las autorizaciones por parte de los Jefes de Proyecto de la Gerencia de Informática y los usuarios dueños del proceso de negocio afectado.

Por último, existe un proceso de llamado “control de cambio de programas” que implica llevar un registro de las versiones de programas en un sistema llamado Harvest, el cual cuenta con una biblioteca con las distintas versiones de los sistemas de información del Banco.

**c) Definir y administrar niveles de servicio:** En la Gerencia de Operaciones Computacionales del Banco, existe un proceso diario de explotación de sistemas y monitoreo del Up-Time, niveles de servicio y errores de las aplicaciones del Banco, información que queda reflejada en un reporte llamado “Informes de Novedad de Producción”. A través de este proceso, se controla el cumplimiento de los estándares de calidad de atención definidos por el Banco hacia los Clientes.

**d) Seguridad de Sistemas:** Existe una gran variedad de procesos asociados a la seguridad en los sistemas del Banco, sin embargo, destacan los procesos de Control de accesos y Gestión de Incidentes de Seguridad, con los cuales se regula a los usuarios que pueden acceder a los diferentes tipos de información y que pueden hacer con ésta y por otro lado; existen un equipo de personas encargadas de registrar, en una aplicación llamada ERI, cada incidente, informando a la Unidad de Seguridad de la Información, para poder hacer la gestión y resolución de éstos, de modo de investigar causas e implantar soluciones permanentes.

**e) Administración de Capacidades:** En el área de Plataformas Centrales y Bases de Datos, se efectúa un monitoreo, a través de la herramienta de software llamada Patrol, de las capacidades de los servidores que mantienen los sistemas y bases de datos del Banco, en aspectos como uso de CPU, espacio en disco, tiempos de respuesta, entre otros aspectos. Luego, los datos recabados son contrastados con los estándares comprometidos por la unidad y se entregan informes diarios de desempeños y capacidad de los equipos. Esta información es utilizada en forma posterior para generar los Capacity Planning del Banco.

**f) Administración de Medios:** La Gerencia de Operaciones Computacionales cuenta con un proceso formal de soporte y mesa de ayuda para usuarios el cual se encarga de la instalación y configuración de nuevos PCs, su mantención en el tiempo y resolución de problemas, a través de procedimientos formales establecidos.

**g) Monitoreo de control interno y regulatorio:** El Banco cuenta con una Gerencia de Contraloría que realiza procesos formales de auditoría, cuyo objetivo, es evaluar el cumplimiento de los controles, existiendo dos revisiones externas adicionales durante el año, las cuales son realizadas por los auditores externos y por la SBIF.

#### **4.1.2. Identificación de controles claves TI.**

De acuerdo a los procesos descritos en la sección 4.1.1., hemos seleccionado de acuerdo a su criticidad, 4 procesos y sus controles claves asociados, cuyos

objetivos son asegurar su correcto desarrollo y que para efectos de esta tesis, serán medidos y evaluados. Los procesos seleccionados son; Administración de la calidad, adquisición y mantención de software aplicativo, Seguridad de sistemas y Administración de medios; y los controles claves asociados a cada unos de estos son los siguientes:

**a) Administración de la Calidad:** Para administrar la calidad de servicio de las aplicaciones, el Banco cuenta con un control de monitoreo efectuado por el área de Operaciones Computacionales, el cual, a través de herramientas de software y operadores que trabajan en turnos 7x24, registran y solucionan incidentes que afectan la producción diaria.

**b) Adquisición y mantención de software aplicativo:** Un control clave para medir el proceso de desarrollo y mantenciones de aplicaciones es el control QA (Quality Assurance) efectuado por el área de Certificación del Banco, antes de implantarlas en el ambiente de producción, este control debe asegurar que las aplicaciones no tengan errores al momento de ser utilizadas por los clientes o colaboradores del Banco.

**c) Seguridad de Sistemas:** Para este proceso existen variados controles implantados en el Banco, sin embargo, se han seleccionado dos que se consideran claves para asegurar que las aplicaciones resguardan adecuadamente la información del Banco y de sus clientes, estos son:

- Control de Accesos a las bases de datos en ambiente de producción, función realizada por el área de Control de Accesos, la cual debe regular la creación de cuentas de usuarios en las aplicaciones y bases de datos, de modo de crear sólo cuentas con perfiles que permitan efectuar acciones al usuario, de acuerdo a la función que realiza, con las autorizaciones respectivas y según la normativa interna del Banco.
- Control para cambios efectuados directamente en el ambiente de producción, control que es realizado por la unidad de Control de Cambios de la Gerencia de Operaciones Computacionales del Banco y que consiste en regular que sólo en casos contingentes se realicen cambios a sistemas y bases de datos directamente en el ambiente de producción, con la debidas autorizaciones y pruebas.

**d) Administración de Medios:** La unidad de Mesa de Ayuda y Soporte, perteneciente a la Gerencia de Operaciones Computacionales efectúa la labor de instalar y mantener los equipos del Banco de acuerdo a los estándares de seguridad definidos en la Política de Seguridad de la Información de la Corporación.

Dentro de los aspectos que deben controlarse, está la instalación de software anti-virus y anti-spyware y de la actualización de las políticas y diccionarios de virus, a objeto de mantener resguardada la red computacional del Banco. Estas instalaciones y actualizaciones son monitoreadas a través del software EPO.

#### **4.2. DETERMINACIÓN DE INDICADORES DE RIESGO TI Y DE EFICIENCIA PARA EL BANCO (EVALUACIÓN CUALITATIVA).**

En esta etapa se identificarán y desarrollarán los indicadores de riesgo (KRIs – Key Risk Indicators) asociados a los procesos tecnológicos seleccionados para el Banco y a sus controles claves. Estos indicadores entregarán índices de medición del riesgo.

##### **4.2.1. Desarrollo de indicadores de riesgo.**

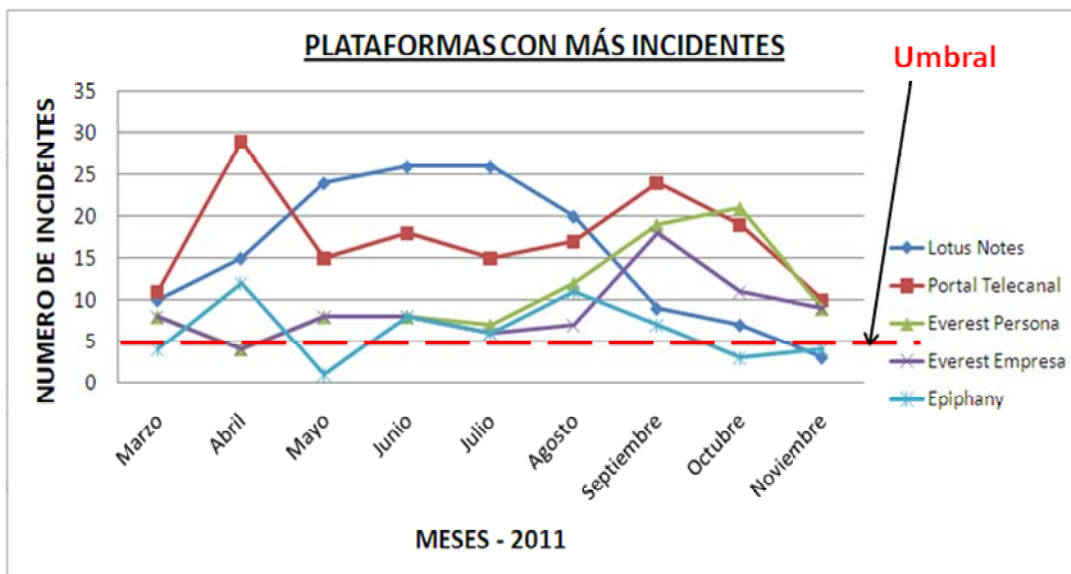
De acuerdo al alcance de esta tesis, seleccionamos 5 métricas (KRIs) asociadas a 4 controles claves existentes en el Banco, los cuales serán medidos de forma cualitativa y cuantitativa. Los controles seleccionados son:

**a) Administración de la Calidad:** Para este dominio de Cobit, se ha generado el KRI llamado “Incidentes de sistemas que afectan la operación interna y de cara a clientes”.

Esta métrica, está orientada a medir el riesgo de no contar con una adecuada calidad del servicio de los sistemas de información de acuerdo a un umbral, definido por un panel de expertos, de no más de 5 incidentes mensuales permitidos por sistema, a modo de no tener impacto económico significativo para

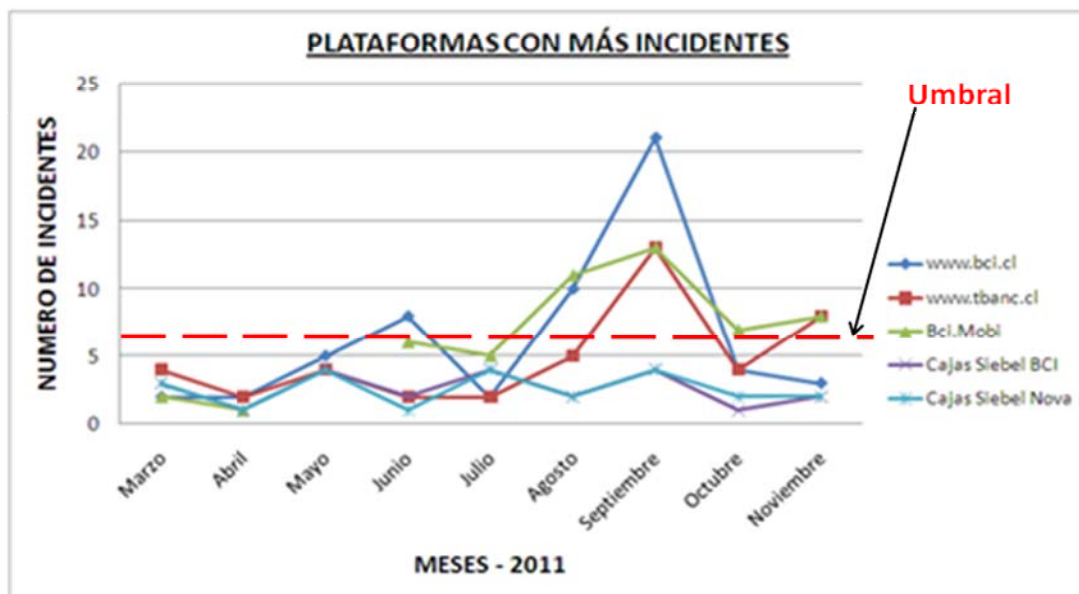
el Banco. La medición se ha efectuado desde del mes de marzo de 2011, información que es extraída del “Informe de Novedades de Producción”, emitido en forma diaria por la Gerencia de Operaciones Computacionales del Banco y se puede apreciar en el siguiente gráfico:

**Figura 20: Sistemas de Operación Interna.**



Fuente: Desarrollado por Gonzalo Flores.

**Figura 21: Sistemas Servicio a Clientes.**

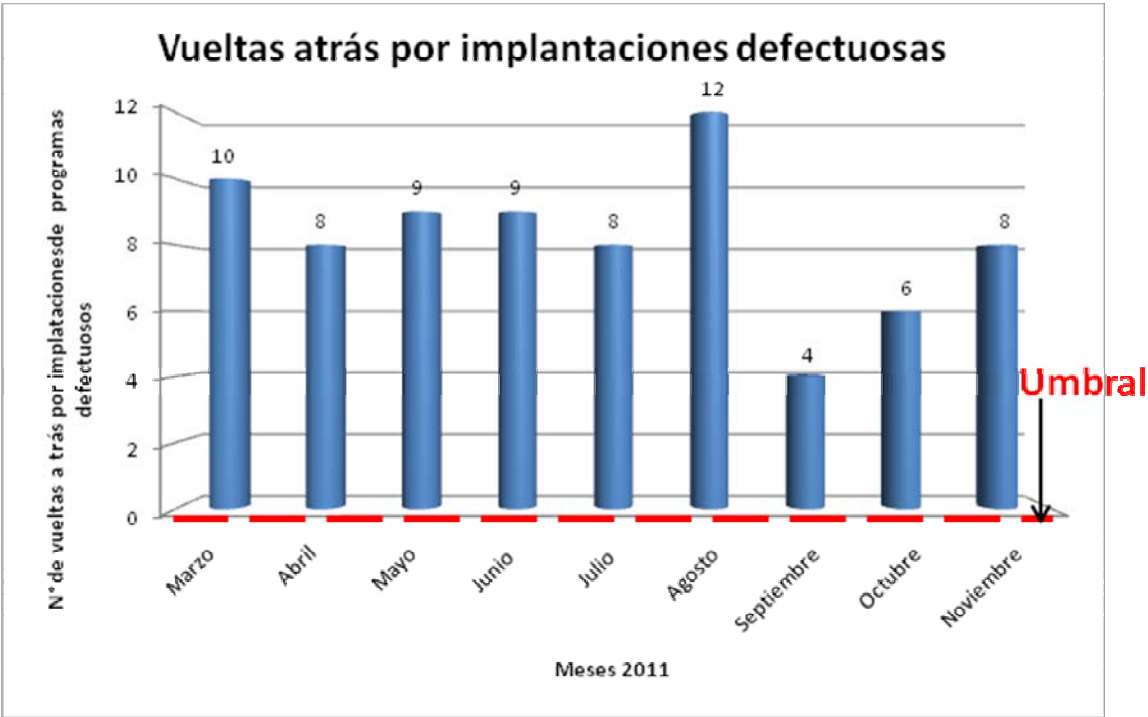


Fuente: Desarrollado por Gonzalo Flores.

**b) Adquisición y mantención de software aplicativo:** Para este dominio se utilizará el KRI llamado “Impacto en sistemas en ambiente de producción, por errores no detectados en implantación de programas defectuosos”.

Esta métrica está orientada a determinar el impacto en producción a través de las vueltas atrás de implantaciones de programas defectuosos en ambiente de producción, con un umbral definido por un panel de expertos de 0 implantaciones defectuosas permitidas. La medición ha sido realizada a partir del mes de marzo de 2011, información que es extraída del “Informes de Novedades de Producción” emitido en forma diaria por la Gerencia de Operaciones Computacionales del Banco y se puede apreciar en el siguiente gráfico:

**Figura 22: Vueltas atrás por implantaciones defectuosas**



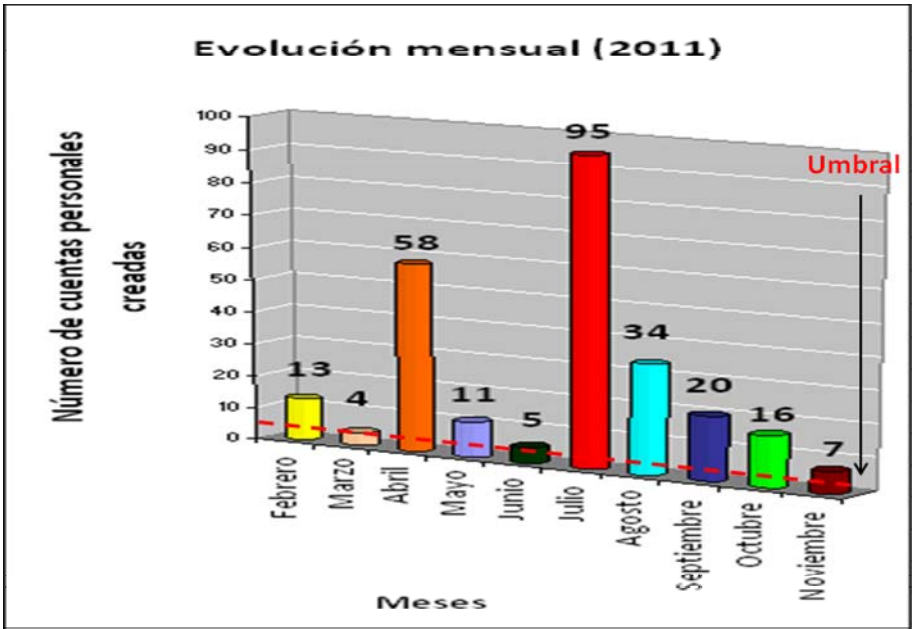
Fuente: Desarrollado por Gonzalo Flores.

**c) Seguridad de Sistemas:** Para este dominio se utilizarán los KRIs llamados “Cuentas creadas en bases de datos de producción” y “Creación de objetos en bases de datos utilizando cuentas no autorizadas”.

Estas métricas, están orientadas a medir el número cuentas de usuarios creadas en las bases de datos de producción (Sybase) en forma mensual, de acuerdo a un

umbral, definido por un panel de expertos, de no más de 5 cuentas mensuales permitidas, de modo de evitar accesos no autorizados a producción. Es importante aclarar que no deberían existir cuentas de usuarios finales en las bases de datos y sólo se debería utilizar para realizar labores de administración y soporte. La medición se ha efectuado desde del mes de febrero de 2011, información que es extraída de un procedimiento almacenado ejecutado mensualmente en el motor de base de datos Sybase de producción y que se puede apreciar en el siguiente gráfico:

**Figura 23: Evolución mensual de creación de cuentas personales.**

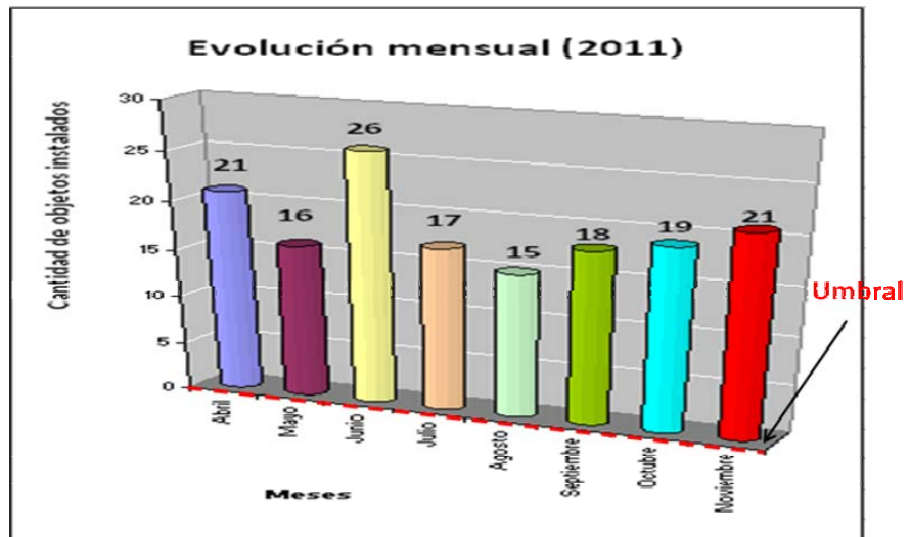


Fuente: Desarrollado por Gonzalo Flores.

Por otro lado, el KRI que mide la cantidad de objetos creados en producción utilizando cuentas no autorizadas, nos permite medir el riesgo de implantación de cambios en sistemas, sin adecuadas autorizaciones y que puedan poner en riesgo la integridad, disponibilidad y confidencialidad de la información y que de acuerdo a un umbral definido por un panel de expertos, no debería existir ninguna.

La medición se ha efectuado desde del mes de abril de 2011, información que es extraída de un procedimiento almacenado ejecutado mensualmente en el motor de base de datos Sybase de producción y que se puede apreciar en el siguiente gráfico:

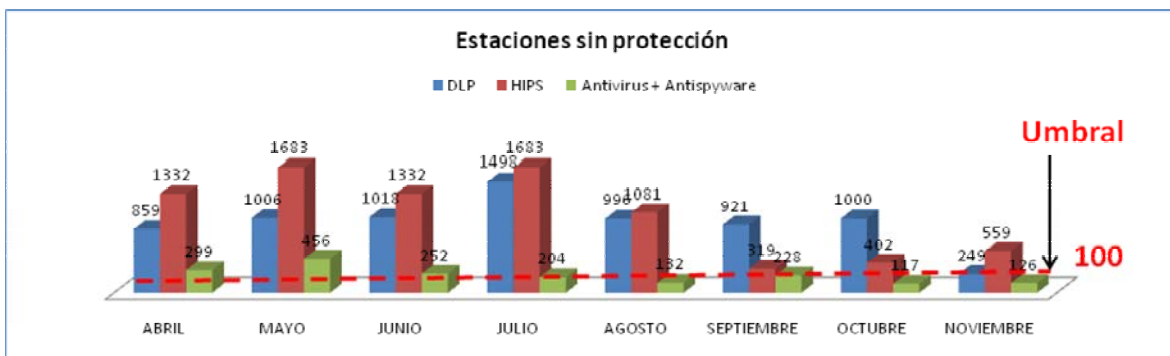
**Figura 24: Evolución mensual de implantación de objetos.**



Fuente: Desarrollado por Gonzalo Flores.

**d) Administración de Medios:** Para este dominio se utilizará el KRI llamado “Equipos no protegidos e inadecuadamente protegidos contra ataques externos e internos”. Esta métrica está orientada a determinar el nivel de protección de los equipos computacionales del Banco y cuantos equipos están expuestos a ataques de virus fallas, pérdida de información y de la continuidad operativa, con un umbral definido por un panel de expertos, de no más de 100 equipos sin protección mensual permitidos. La medición ha sido realizada a partir del mes de abril de 2011, información que es extraída de la consola de administración EPO (E- Policy Orchestrator), informe emitido en forma mensual por la Gerencia de Operaciones Computacionales del Banco y se puede apreciar en el siguiente gráfico:

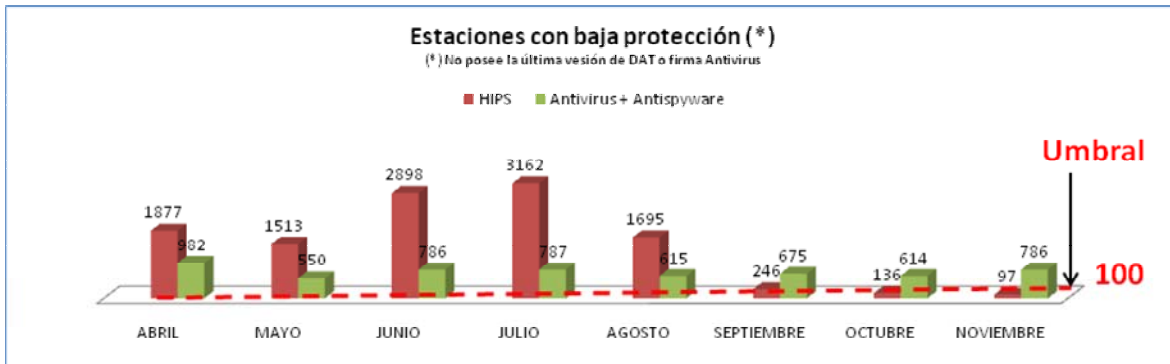
**Figura 25: Estaciones de trabajo sin protección.**



Fuente: Desarrollado por Gonzalo Flores.



**Figura 26: Estaciones de trabajo con baja protección.**



Fuente: Desarrollado por Gonzalo Flores.

#### 4.2.2. Definición de escala de riesgo.

Para determinar la nota de riesgo de cada uno de los indicadores, se calificó el riesgo residual (definido como el riesgo aún no cubierto por controles que permiten administrarlo), y sobre dicha amenaza o vulnerabilidad, aplicamos la fórmula que considera los factores de riesgo y la probabilidad de ocurrencia:

<b>Nota de riesgo</b> (sobre riesgo residual)	=	<b>Factores de riesgo</b> (Impacto)	x	<b>Probabilidad de ocurrencia</b>
--	---	--	---	-----------------------------------

Los factores de riesgo han sido segregados en 4 grupos, para cubrir de manera razonable el universo de situaciones evaluadas y cada factor pondera en 25% y su impacto se define en categorías Alto, Medio o Bajo, según las siguientes definiciones:

- Gestión, eficiencia y rentabilidad.
- Impacto financiero
- Calidad de servicio e imagen corporativa.
- Cumplimiento normativo y calidad de datos e información.

La probabilidad de ocurrencia se determina en función de alguna de las siguientes variables, las que podrán considerarse en forma independiente o combinada, según corresponda a cada caso, acorde a las siguientes definiciones:

- Impacto relativo en función del monto de las operaciones con reparos con respecto a la situación analizada.
- Porcentaje de casos con reparos sobre la situación analizada.
- Cantidad estimada de veces que podría ocurrir el evento en un período de 12 meses.

El impacto se calificará en las siguientes 5 categorías: Alto, Medio-alto, Medio, Medio-bajo y Bajo. Adicionalmente, para determinar y/o cuantificar la probabilidad de ocurrencia, consideraremos la información de los eventos registrados por la Gerencia de Riesgo Operacional (Base Histórica de Pérdidas), cuando ello corresponda.

En atención a que los riesgos evolucionan en forma permanente, las calificaciones asignadas a los indicadores serán sometidas a validación periódica de su nota, en función de nuevas evaluaciones que se hayan realizado y/o de nuevos eventos que potencien los riesgos, labor que se concretará en las respectivas evaluaciones.

A continuación se presenta la matriz de ponderación de riesgos, con las definiciones y circunstancias que inciden en los factores de riesgo a nivel de impacto y probabilidad de ocurrencia.

**Tabla 7: Matriz de Ponderación de Riesgos:**

FACTORES DE RIESGO	Ponderación	IMPACTO		
		Alto (3)	Medio (2)	Bajo (1)
<u>Impacto financiero</u> : medido sobre activos, pasivos, pérdidas, utilidades o patrimonio.	25%	<ul style="list-style-type: none"> <li>• Si la situación implica un efecto financiero y/o patrimonial mayor o igual al 5% del resultado anual.</li> </ul>	<ul style="list-style-type: none"> <li>• Si la situación implica un efecto financiero y/o patrimonial entre un 0,5% y un 4,9 % del resultado anual.</li> </ul>	<ul style="list-style-type: none"> <li>• Si la situación implica un efecto financiero y/o patrimonial inferior a 0,5 % del resultado anual.</li> </ul>
<u>Gestión, eficiencia y rentabilidad</u> : la calificación del impacto financiero (alto, medio, bajo) dependerá de la magnitud o severidad de la situación de acuerdo al juicio del evaluador, que deberá considerar, además del impacto en gestión, eficiencia y/o rentabilidad, el historial de la permanencia del riesgo sin resolver, la frecuencia y otros.	25%	<ul style="list-style-type: none"> <li>• Afecta directamente la calificación de gestión SBIF.</li> <li>• Impacto severo en la calidad, integridad, oportunidad y/o confidencialidad de la información.</li> <li>• Incumplimiento grave o trasgresión de límites y márgenes de gestión interna (Directorio, Comité AP, Comité de Créditos, otros).</li> <li>• Exposición a eventual hurto de bases de datos de clientes, negocios y/o información estratégica.</li> <li>• Servicios críticos externalizados y/o sin controles adecuados y sin resguardos legales u otros que protejan al Banco.</li> <li>• Control deficiente sobre proyectos con impacto en gastos, eficiencia operacional u otros.</li> </ul>	<ul style="list-style-type: none"> <li>• Incumplimiento o trasgresión de forma en cuanto a límites y márgenes de gestión interna (Directorio, Comité AP, Comité de Créditos, otros).</li> <li>• Exposición a eventual hurto de datos de clientes.</li> <li>• Servicios de mediana criticidad externalizados sin los controles ni resguardos establecidos en las políticas.</li> <li>• Impacto parcial en la calidad, integridad, oportunidad y/o confidencialidad de la información.</li> </ul>	<ul style="list-style-type: none"> <li>• Servicios de baja criticidad externalizados sin controles y/o resguardos establecidos en las políticas.</li> <li>• Impacto leve en la calidad, integridad, oportunidad y/o confidencialidad de la información.</li> </ul>
<u>Calidad de servicio e imagen corporativa</u> : la criticidad y nivel de impacto dependerá del universo de clientes afectados y del tipo de información.		<ul style="list-style-type: none"> <li>• Si el riesgo implica un impacto negativo importante en la calidad de información a clientes y/o imagen corporativa, en responsabilidad social empresarial y/o clima laboral.</li> <li>• Trasgresiones importantes de colabo-</li> </ul>	<ul style="list-style-type: none"> <li>• Si el riesgo implica un moderado impacto negativo en la calidad de información a clientes y/o imagen corporativa, en responsabilidad social empresarial y/o clima laboral.</li> </ul>	<ul style="list-style-type: none"> <li>• Si el riesgo implica una baja posibilidad de impacto en la calidad de información a clientes y/o imagen corporativa, en responsabilidad social empre-</li> </ul>

FACTORES DE RIESGO	Ponderación	IMPACTO		
		Alto (3)	Medio (2)	Bajo (1)
	25%	<ul style="list-style-type: none"> <li>• radores en temas éticos, calidad de servicio a clientes y/o reclamos de proveedores.</li> <li>• Impacto en servicio sobre el 5% del total de clientes afectados o por falla sobre el 30% del producto.</li> <li>• Reclamos masivos de clientes con posibilidad de pérdida de ellos.</li> <li>• Posibles fraudes con un impacto significativo y con divulgación en prensa.</li> <li>• Operaciones de lavado de activos no reportadas ni detectadas.</li> </ul>	<ul style="list-style-type: none"> <li>• Impacto en servicio entre un 2% y hasta 4,9% del total de clientes afectados o por falla del producto entre un 10% y hasta 30%.</li> <li>• Reclamos reiterados de clientes.</li> </ul>	<ul style="list-style-type: none"> <li>• sarial y/o clima laboral.</li> <li>• Impacto en servicio afecta a menos de un 2% del total de clientes o por falla menor a un 10% del producto.</li> <li>• Reclamos puntuales de clientes de fácil solución.</li> </ul>
<u>Cumplimiento normativo</u> (normas internas y externas) y calidad de datos e información.	25%	<ul style="list-style-type: none"> <li>• Incumplimiento de leyes o normas internas y/o externas vigentes con riesgo de juicios, eventuales multas o sanciones de organismos fiscalizadores (SBIF, SII, UAF, Banco Central, Inspección del Trabajo, SERNAC y otras) o que representan trasgresión y/o vulneración de facultades.</li> <li>• Errores, omisión y/o retrasos relevantes en información oficial financiera o de otra índole entregada a SBIF, SII, Banco Central, UAF, Directorio, etc.</li> <li>• Riesgo de eventuales multas por trasgresión de límites o márgenes.</li> <li>• Falta de segregación de funciones en procesos críticos o claves.</li> </ul>	<ul style="list-style-type: none"> <li>• Posibles reconvenciones o recomendaciones de organismos fiscalizadores.</li> <li>• Observaciones de auditores externos con riesgo medio.</li> <li>• Errores o retrasos en información entregada a SBIF, SII, Banco Central, UAF, Directorio, etc.</li> <li>• Falta de segregación de funciones en procesos de mediana criticidad.</li> </ul>	<ul style="list-style-type: none"> <li>• Sin impacto de sanciones normativas o regulatorias.</li> <li>• Posibles recomendaciones de auditores externos con riesgo menor.</li> <li>• Falta de formalización y/o actualización de normas y procedimientos internos vigentes.</li> <li>• Falta de segregación de funciones en procesos de baja criticidad.</li> </ul>

**Tabla 8: Probabilidad de ocurrencia:**

Se determina la probabilidad de ocurrencia aplicando el sano juicio independiente, objetivo y criterio que caracteriza al evaluador y podrá utilizarse cualquiera de los siguientes parámetros en forma independiente u otros que estime pertinentes o que procedan.

Para calificar la probabilidad de ocurrencia debe considerarse la importancia del problema en cuanto a efectos sobre los estados financieros y factibilidad de que exista error sistemático. Debe considerar lo confirmado en los indicadores de riesgo y los eventos de pérdida registrados por la Gerencia de Riesgo Operacional.

Error sistemático: existe cuando una norma o procedimiento no se cumple en gran parte de los elementos de la muestra analizada (desde un 70%)

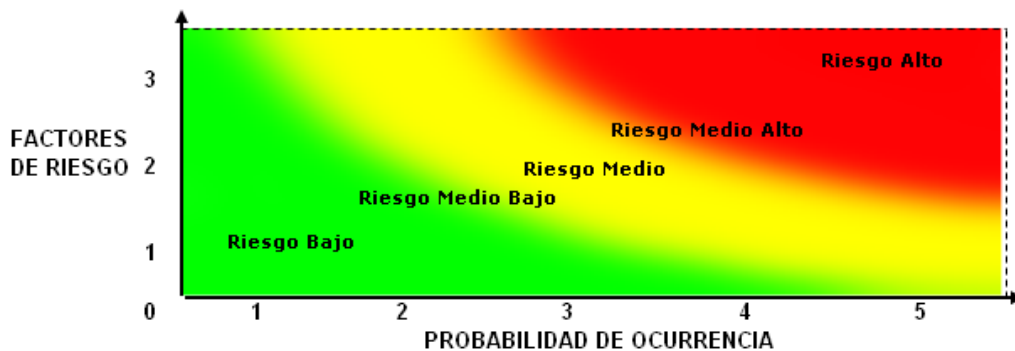
<b>ESCALA</b>				
<b>Alta (5)</b>	<b>Medio alto (4)</b>	<b>Media (3)</b>	<b>Medio bajo (2)</b>	<b>Baja (1)</b>
Impacto alto en función del monto de las operaciones con reparos en relación al total.	Impacto significativo o severo en función del monto de las operaciones con reparos, en relación al total.	Impacto moderado en función del monto de las operaciones con reparos en relación al total.	Impacto menor en función del monto de las operaciones con reparos, en relación al total.	Impacto marginal en función del monto de las operaciones con reparos en relación al total.
Sobre un 70% con reparos, lo que representaría un error sistemático.	Entre un 69% y un 45% con reparos.	Entre un 44% y un 20% con reparos.	Entre un 19% y hasta un 5% con reparos.	Inferior a un 5% con reparos.
Probabilidad que el evento pueda ocurrir 6 veces o más durante un período de 12 meses.	Probabilidad que el evento pueda ocurrir 5 veces o más en un período de 12 meses.	Probabilidad que el evento pueda ocurrir 4 veces en un período de 12 meses.	Probabilidad que el evento pueda ocurrir más de 2 veces en un período de 12 meses.	Baja probabilidad de ocurrencia del evento, menor a 2 veces en un período de 12 meses.

**Tabla 9: Sensibilización de los Factores de Riesgo:**

A continuación, se presenta la tabla completa con la sensibilización de riesgos y las notas a las que se llega en cada caso, de acuerdo a todo lo explicado anteriormente:

Factores de riesgo aplicados	Probabilidad de ocurrencia					Nota de riesgo
	1	2	3	4	5	
1	1	2	3	4	5	Nota de riesgo
1,1	1,1	2,2	3,3	4,4	5,5	
1,2	1,2	2,4	3,6	4,8	6	
1,3	1,3	2,6	3,9	5,2	6,5	
1,3	1,3	2,6	3,9	5,2	6,5	
1,4	1,4	2,8	4,2	5,6	7	
1,5	1,5	3	4,5	6	7,5	
1,6	1,6	3,2	4,8	6,4	8	
1,7	1,7	3,4	5,1	6,8	8,5	
1,8	1,8	3,6	5,4	7,2	9	
1,9	1,9	3,8	5,7	7,6	9,5	
2	2	4	6	8	10	
2,1	2,1	4,2	6,3	8,4	10,5	
2,2	2,2	4,4	6,6	8,8	11	
2,3	2,3	4,6	6,9	9,2	11,5	
2,4	2,4	4,8	7,2	9,6	12	
2,5	2,5	5	7,5	10	12,5	
2,6	2,6	5,2	7,8	10,4	13	
2,7	2,7	5,4	8,1	10,8	13,5	
2,8	2,8	5,6	8,4	11,2	14	
2,9	2,9	5,8	8,7	11,6	14,5	
3	3	6	9	12	15	

**Representación Gráfica del Riesgo**



Fuente: Desarrollado por Gonzalo Flores.

### 4.2.3. Análisis de Riesgo (Impacto /Probabilidad de ocurrencia).

Aplicando los resultados entregados por los 5 indicadores que permiten la medición de los controles claves TI que fueron seleccionados para el Banco, en la escala de riesgo definida para este modelo, tenemos los siguientes resultados:

**Tabla 10: Resumen de Evaluación de Riesgo de Indicadores (KRIs)**

#	Indicadores	Gestión, Eficiencia, Rentabilidad	Impacto Financiero	Calidad de servicio e Imagen Corporativa	Cumplimiento Normativo	Puntuación Factores de Riesgo	Probabilidad de ocurrencia (1 a 5)	Puntuación Riesgo	Riesgo
1	Incidentes de sistemas que afectan la operación interna y de cara a clientes	2	2	3	2	2,2	4	8,8	Medio Alto
2	Impacto en sistemas en ambiente de producción, por errores no detectados en implantación de programas defectuosos.	2	2	2	1	1,7	3	5,1	Medio
3	Cuentas creadas en bases de datos de producción.	2	2	2	3	2,2	4	8,8	Medio Alto
4	Creación de objetos en bases de datos utilizando cuentas no autorizadas.	1	2	1	2	1,5	3	4,5	Medio
5	Equipos no protegidos e inadecuadamente protegidos contra ataques externos e internos.	2	1	1	2	1,5	4	6	Medio

Fuente: Desarrollado por Gonzalo Flores.

Indicador 1): Incidentes de sistemas que afectan la operación Interna y de cara al cliente:

**Nota de Riesgo:**  $((2 * 0,25) + (2 * 0,25) + (3 * 0,25) + (2 * 0,25)) * 4 = 8,8$

**Evaluación Cualitativa:** Riesgo Medio Alto

Indicador 2): Impacto en sistemas en ambiente de producción, por errores no detectados en implantación de programas defectuosos:

**Nota de Riesgo:**  $((2 * 0,25) + (2 * 0,25) + (2 * 0,25) + (1 * 0,25)) * 3 = 5,1$

**Evaluación Cualitativa:** Riesgo Medio

Indicador 3): Cuentas creadas en bases de datos de producción:

**Nota de Riesgo:**  $((2 * 0,25) + (2 * 0,25) + (2 * 0,25) + (3 * 0,25)) * 4 = 8,8$

**Evaluación Cualitativa:** Riesgo Medio Alto

Indicador 4): Creación de objetos en bases de datos utilizando cuentas no autorizadas:

**Nota de Riesgo:**  $((1 * 0,25) + (2 * 0,25) + (1 * 0,25) + (2 * 0,25)) * 3 = 4,5$

**Evaluación Cualitativa:** Riesgo Medio

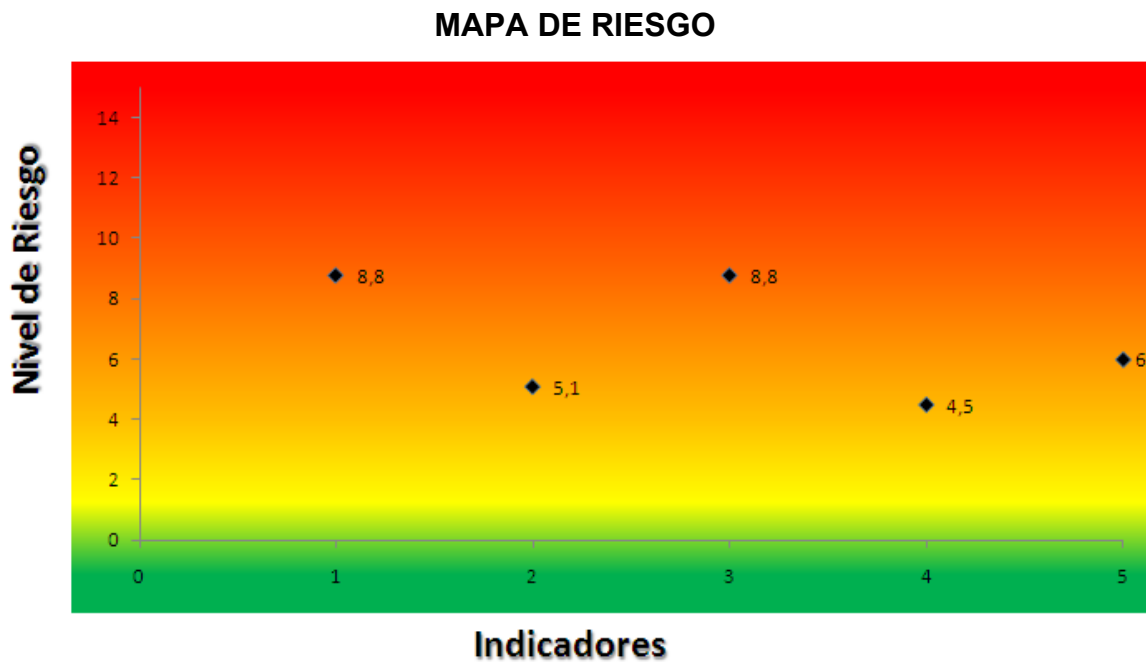
Indicador 5): Equipos no protegidos e inadecuadamente protegidos contra ataques externos e internos:

**Nota de Riesgo:**  $((2 * 0,25) + (1 * 0,25) + (1 * 0,25) + (2 * 0,25)) * 4 = 6$

**Evaluación Cualitativa:** Riesgo Medio

De acuerdo a los valores calculados a través de la escala de riesgo desarrollada, los diferentes indicadores (KRIs) se grafican de la siguiente forma:

**Figura 27: Mapa de Riesgo basado en indicadores**



Fuente: Desarrollado por Gonzalo Flores.

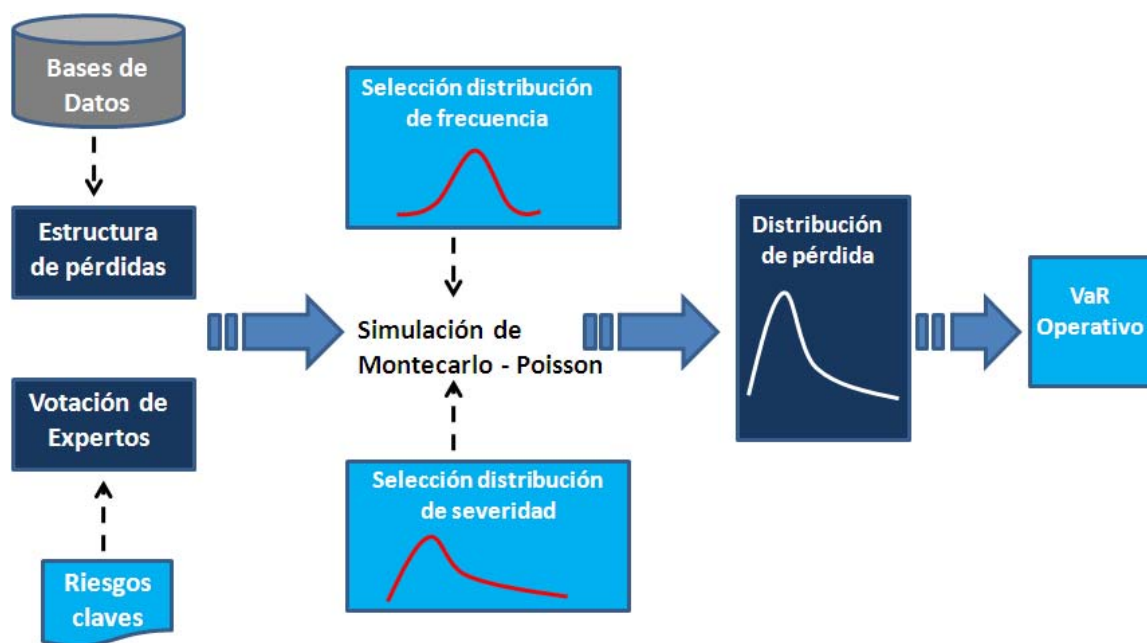


### 4.3. VALORIZACIÓN DE RIESGOS TI (EVALUACIÓN CUANTITATIVA).

En esta etapa se desarrollará el modelo de cálculo para la valorización del riesgo tecnológico, aplicando la metodología VaR para estimar los montos.

El diagrama general de la metodología de evaluación cuantitativa es el siguiente:

**Figura 28: Diagrama general de metodología Value At Risk.**



Fuente: Metodología Value At Risk (VaR).

#### 4.3.1. Análisis de la Base de Datos de Pérdida (Cuantificación TI).

La base de datos de pérdida, es un registro histórico contable de cuentas de castigos, la cuales fueron registradas en el Banco a partir del año 2004. Estas cuentas, fueron analizadas y clasificadas de acuerdo a los distintos tipos de riesgos que Basilea II exige.

Para realizar este análisis tomaremos una muestra acotada de las cuentas contables de castigos históricos entre los años 2009 y 2011 relacionados a eventos de sistemas y clasificaremos estos eventos en distintos tipos de riesgos

tecnológicos (se considerarán solo 3 años debido a la gran cantidad de registros que implica analizar y el reducido presupuesto de tiempo).

A través de esta clasificación obtendremos la pérdida real asociada al ámbito tecnología del Banco, con la cual podremos efectuar una comparación entre la provisión por concepto de riesgo operacional tecnológico (PE y VAR) y los montos de castigos reales por eventos de riesgos efectivos (base de datos de pérdida), lo cual nos permitirá validar si el modelo utilizado se ajusta a la realidad del Banco.

De acuerdo a lo anterior, las cuentas contables de castigo asociadas a eventos de pérdidas tecnológicas seleccionadas son las siguientes:

**Tabla 11: Resumen de Cuentas Históricas de Castigos.**

Monto		Año contable			
Cuenta Contable	Nombre cuenta	2009	2010	2011	Total general
590000959	OTROS GASTOS DE OPERACIÓN-CONOSUR	289.422	16.422	60.960	366.804
625503315	Otras Multas		666.656		666.656
631500012	Ajuste resultados ejercicios anteriores		19.963.405	-6.566.266	13.397.139
631501540	Castigos No Operacionales	6.457.337	4.317.466	2.174.896	12.949.699
631501541	Castigos No Operacionales comerciales	1.196.286	2.705.122	768.337	4.669.745
631501542	Castigos No Operacionales sistemas	154.151.758	291.789.585	1.769.940	447.711.283
631501543	Castigos No Operacionales fraudes			172.657.976	172.657.976
631501600	Sinistros No Cubiertos Por Compañías De Seguros			4.611.518	4.611.518
631501950	Castigo Pérdida De Caja-Conosur			5.737.479	5.737.479
<b>Total general</b>		<b>162.094.803</b>	<b>319.458.656</b>	<b>181.214.840</b>	<b>662.768.299</b>

Fuente: Desarrollado por Gonzalo Flores.

De acuerdo a los saldos por castigos asociados a problemas relacionados con tecnología, ha existido una pérdida histórica acumulada de MM\$ 662 pesos, lo cual, al menos debería ser aprovisionado de acuerdo a los criterios de Basilea II (acumulación de pérdida de los últimos 3 años).

#### 4.3.2. Desarrollo del modelo matemático de valorización (PE y VaR).

Para llevar a cabo el cálculo de Pérdida Esperada y VaR como una forma de evaluar escenarios de riesgos, se utilizará la siguiente metodología Value At Risk, la cual indica que se debe contar con la siguiente información:

**a) Periodicidad del Evento:** El responsable del proceso en la Unidad de Negocio/Apoyo debe indicar cuántas veces puede ocurrir la pérdida y el intervalo de tiempo asociado.

Por ejemplo: 5 veces al mes, 1 vez cada 3 meses, etc. Lo que posteriormente se anualiza.

**b) Pérdida Esperada por Evento (M\$) y Máxima Pérdida por Evento (M\$):** Para ambos casos, el responsable del proceso puede indicar los montos exactos de la pérdida que está estimando, o en su defecto, entregar un rango de valores (intervalos dados según tabla). Por ejemplo, puede indicar que por cada vez que ocurra un evento de riesgo, la pérdida media corresponde a M\$1.800 y la pérdida máxima alcanza los M\$5.700.

En caso que no tenga el valor exacto debe indicar los intervalos en que se encuentran los valores, de acuerdo a la tabla:

**Tabla 12: Intervalos de Pérdida Esperada.**

Intervalo 1	Intervalo en Miles de Pesos	Rango menor	Rango mayor	Marca Media
1	1. < M\$ 900	M\$ -	M\$ 900	M\$ 450
2	2. >= M\$ 900 < M\$ 5000	M\$ 900	M\$ 5.000	M\$ 2.950
3	3. >= M\$ 5000 < M\$ 10000	M\$ 5.000	M\$ 10.000	M\$ 7.500
4	4. >= M\$ 10000 < M\$ 16000	M\$ 10.000	M\$ 16.000	M\$ 13.000
5	5. >= M\$ 16000 < M\$ 23000	M\$ 16.000	M\$ 23.000	M\$ 19.500
6	6. >= M\$ 23000 < M\$ 30000	M\$ 23.000	M\$ 30.000	M\$ 26.500
7	7. >= M\$ 30000 < M\$ 38000	M\$ 30.000	M\$ 38.000	M\$ 34.000
8	8. >= M\$ 38000 < M\$ 48000	M\$ 38.000	M\$ 48.000	M\$ 43.000
9	9. >= M\$ 48000 < M\$ 60000	M\$ 48.000	M\$ 60.000	M\$ 54.000
10	10. >= M\$ 60000	M\$ 60.000		M\$ 66.000

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

De esta manera para el riesgo cuya Pérdida Esperada por Evento (M\$), se indica el rango 4 y su Máxima Pérdida por Evento (M\$) también pertenece al rango 4, se tiene el siguiente resultado:

Pérdida Esperada = M\$13.000 (Marca Media) y Pérdida Máxima = M\$16.000 (Rango mayor).

La pérdida esperada debe considerar el riesgo residual, es decir, se deben considerar todos los controles.

La Pérdida máxima para un evento de pérdida, para el riesgo evaluado, considera el peor escenario para el riesgo. Ej. Peor escenario robo cajero, es el total de efectivo en la caja.

**c) Determinación de parámetros, para determinar distribución de pérdida agregada:**

- Frecuencia:** La periodicidad entregada por el responsable del proceso al momento de evaluar los riesgos, es utilizada como input en la obtención de la distribución de frecuencia. Las funciones disponibles para llevar a cabo este proceso son Poisson y Binomial Negativa, siendo la primera la más recomendada, por requerir de un único parámetro  $\lambda$  (lambda), el que corresponde al promedio de eventos de pérdida (es decir, la periodicidad de ocurrencia de la pérdida anualizada).

**Tabla 13: Probabilidad de Ocurrencia con Pérdida.**

Probabilidad de ocurrencia con pérdida	
Número de veces que ocurre el evento	Periodicidad
Corresponde al número promedio de eventos de pérdida para el riesgo evaluado en un período determinado de tiempo.	Se refiere a la periodicidad de los eventos de pérdida promedio.
1	1 Diaria
2	2 Semanal
3	3 Mensual
4	4 Trimestral
5	5 Semestral
N	6 Anual

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

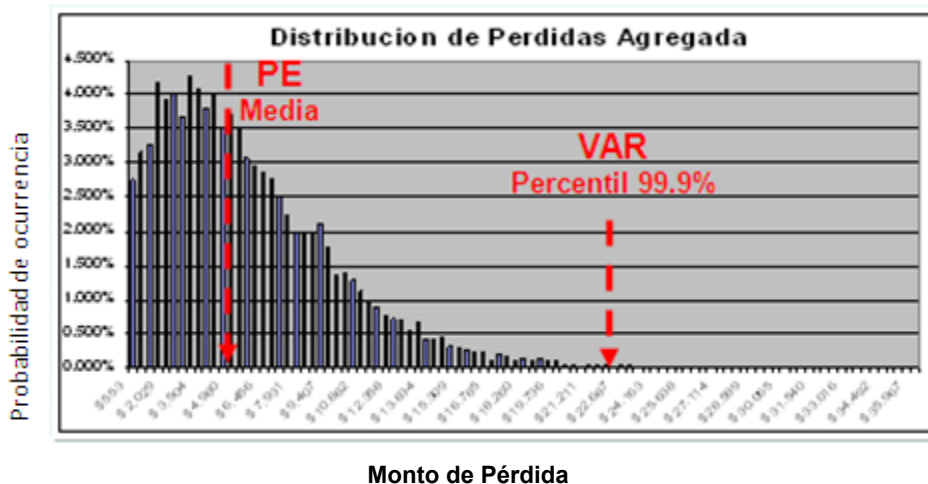
- Severidad:** Los montos de pérdida entregados por el responsable del proceso, son el input para obtener la severidad. Dentro de las funciones de distribución continua disponibles, la utilizada para estimar la severidad de los riesgos, es Weibull, la cual requiere solamente de 2 parámetros  $\alpha$  (alpha) y  $\beta$  (beta). Además esta distribución entrega buen ajuste a datos reales de pérdidas.

**d) Determinación de distribución de pérdida agregada:** Una vez identificados los parámetros de las distribuciones de frecuencia y severidad, es necesario generar una distribución de pérdida agregada (LDA). Esta distribución, representa la probabilidad de pérdidas operacionales en un determinado período de tiempo (anual), de acuerdo al escenario evaluado.

Las mejores prácticas de la industria, proponen realizar este proceso a través de una simulación Montecarlo (100.000 simulaciones), con el objeto de determinar la distribución de pérdida agregada. La metodología de simulación Montecarlo a utilizar cuenta de las siguientes etapas:

- Simulación de la distribución discreta de frecuencia Poisson con parámetro  $\lambda$  (lambda).
- Simulación de la distribución de severidad (Weibull) de acuerdo a la simulación de frecuencia y suma de estas.

**Figura 29: Simulación de Montecarlo.**



Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

**e) Resultado del Modelo:** Una vez determinada la distribución de pérdida agregada, se puede calcular el VaR y la Pérdida Media para un escenario determinado para el período de tiempo de un año.

Para obtener el VaR al 99.9% sólo basta calcular el percentil 99.9% de la distribución de pérdida, así mismo, para obtener la Pérdida Esperada sólo basta calcular la media de la distribución de pérdida.

**f) Determinación de los Riesgos Tecnológicos a valorizar:** Para aplicar esta metodología, se realizó un proceso de evaluación de los principales riesgos tecnológicos existentes en la organización y se le consultó a un panel de expertos por los montos de pérdidas asociados a estos, en caso que se hicieran efectivos y adicionalmente, se les consultó por el monto máximo de pérdida esperado por la ocurrencia del evento. Otro aspecto consultado, son las probabilidades de ocurrencia en un año.

Previo a este proceso, se les enseñó a los expertos el resultado de la evaluación cualitativa a través de los indicadores de riesgos (KRIs) desarrollados en el acápite 4.2.1., a modo de entregar datos concretos para la evaluación cuantitativa. Respecto a los principales riesgos tecnológicos, éstos fueron asignados a los controles claves de los procesos TI de BCI, que fueron seleccionados de acuerdo a la metodología Cobit, basándose en los riesgos TI más importantes reportados por la Gerencia de Contraloría, Gerencia de Riesgo Operacional, Auditores externos y la Superintendencia de Bancos e Instituciones Financieras. Es importante mencionar, que cada año los riesgos pueden cambiar de prioridad, por lo que siempre es necesario efectuar una nueva evaluación y adicionalmente, se pueden ir agregando más riesgos (De acuerdo a la norma Basilea II no es aconsejable evaluar más de 20 riesgos).

De acuerdo a lo anterior, los riesgos TI seleccionados para este proceso de evaluación fueron siete:

**a) Código de Riesgo BCTI2011-12-1:** Pérdida de operaciones por aplicaciones defectuosas o que fallan, con impacto en la operación diaria del Banco (servicio a clientes) y en la imagen Corporativa.

**b) Código de Riesgo BCTI2011-12-2:** Implantación de aplicaciones con errores que afecten la integridad y disponibilidad de la información de negocios y clientes.

**c) Código de Riesgo BCTI2011-12-3:** Pérdida de confidencialidad, integridad y disponibilidad de la información por ausencia de adecuados procesos de monitoreo de plataformas y sistemas.

**d) Código de Riesgo BCTI2011-12-4:** Fraude por fuga de información y pérdidas económicas por accesos e implantación de componentes de software sin autorización en ambiente de producción.

**e) Código de Riesgo BCTI2011-12-5:** Mala calidad de servicios de los sistemas de información, por mala estimación de requerimientos de procesamiento y espacio en disco, de acuerdo a los niveles de crecimiento del negocio.

**f) Código de Riesgo BCTI2011-12-6:** Daño de imagen Corporativa y pérdidas económicas por falla o indisponibilidad de servicio por activación de software malicioso (virus, malware, spyware, etc).

**g) Código de Riesgo BCTI2011-12-7:** Multas y daño a imagen Corporativa por incumplimiento de normas y resolución de riesgos informados por entidades externos e internas.

Estos riesgos se asocian a los controles claves de la siguiente manera:

**Tabla 14: Riesgo Claves TI.**

Procesos Cobit	Procesos TI de BCI	Control Clave BCI	Riesgos TI Claves
Administración de la calidad	Proceso de Certificación (QA) de aplicaciones	Control de incidentes en Producción	Pérdida de operaciones por aplicaciones defectuosas o que fallan con impacto en la operación diaria del Banco (servicio a clientes) y en la imagen Corporativa.
Adquirir y mantener software aplicativo	Proceso de desarrollo y Mantenición de aplicaciones	Control de Catalogación y vueltas atrás	Implantación de aplicaciones con errores que afecten la integridad y disponibilidad de la información de negocios y clientes.
Definir y Administrar niveles de servicio	Proceso de explotación y monitoreo de sistemas	<b>Fuera de Alcance</b>	Pérdida de confidencialidad, integridad y disponibilidad de la información por ausencia de adecuados proceso de monitoreo de plataformas y sistemas.
Seguridad de Sistemas	Proceso de Control de Acceso	Control de accesos y cambios en Bases de Datos en producción	Fraude por fuga de información y pérdidas económicas por accesos e implantación de componentes de software sin autorización en ambiente de producción.
Administración de capacidades	Proceso de Capacity Planning	<b>Fuera de Alcance</b>	Mala calidad de servicios de los sistemas de información, por mala estimación de requerimientos de procesamiento y espacio en disco, de acuerdo a los niveles de crecimiento del negocio.
Administración de medios	Proceso de Soporte y mesa de Ayuda	Control de virus y securitización de equipos	Daño de imagen Corporativa y pérdidas económica por falla o indisponibilidad de servicio por activación de software malicioso.
Monitoreo de control interno y regulatorio.	Proceso de Auditoría Interna y Externa	<b>Fuera de Alcance</b>	Multas y daño a imagen corporativa por incumplimiento de normas y resolución de riesgos informados por entidades externos e internas.

Fuente: Desarrollado por Gonzalo Flores.

El siguiente paso consiste en efectuar un proceso de votación de los riesgos, consultando a un panel de expertos dentro del Banco, respecto de los parámetros requeridos para el cálculo de la PE y el VaR, de acuerdo a la metodología descrita en este punto, proceso que será desarrollado en el capítulo 5, acápite 5.1.

#### **4.3.3. Cálculo a través de Operational Risk Capital (ORC).**

Antes de realizar la evaluación cuantitativa de los riesgos TI de BCI, es importante explicar cómo se calcula la provisión por Riesgo Operacional utilizando modelos avanzados, para lo cual utilizaremos la matriz ORC. Los Operational Risk Capital (ORC) se denominan a la matriz que agrupa las líneas de negocio de la organización, asociándolas con las tipologías de riesgo de acuerdo a las definiciones que entrega Basilea II.

Cada una de las intersecciones representan los montos calculados a través de Value At Risk (VaR), en relación a la valoración cualitativa de los riesgos operacionales, incluyendo el tecnológico.

Como ya lo hemos dicho en capítulos anteriores, el BCI, en el ejercicio para el cálculo de Provisión por Riesgo Operacional, utilizando modelos avanzados, considero un valor por riesgo para tecnología basado en una pérdida histórica ponderada, valor al cual se le calculó un VaR.

El cálculo de la provisión total por riesgo operacional, que llegó a un monto de MM\$ 46.019, tuvo una matriz ORC agrupando los riesgos y áreas de negocio de la siguiente manera:



**Tabla 15: Agrupación de ORC en BCI.**

Riesgos Basilea II \ Líneas de Negocios	Banco Comercial	Banco Retail	Banco Retail /Comercial	Banco Inversión y Finanzas	Áreas de Apoyo
Fraude Interno	ORC 3	ORC 3	ORC 3	–	ORC 3
Fraude Externo	ORC 10	ORC 11	ORC 11	ORC 9	ORC 11
Relaciones laborales y seguridad en el puesto de trabajo	–	ORC 13	ORC 13	ORC 13	ORC 13
Clientes, Productos y Prácticas empresariales	ORC 8	ORC 12	ORC 8	ORC 8	ORC 8
Daños a activos materiales	ORC 2	ORC 2	ORC 2	ORC 2	ORC 2
Incidencias en los negocios y fallos en los sistemas	ORC 5	ORC 7	ORC 6	ORC 1	ORC 4
Ejecución, entrega y gestión de procesos	ORC 5	ORC 7	ORC 6	ORC 1	ORC 4

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

Los VaR calculados para cada agrupación de ORC (por color), en el ejercicio a diciembre de 2010, retornó los siguientes valores:

**Tabla 16: Valorización de ORCs de BCI a diciembre de 2010.**

ORC	Datos Integrados (cualitativos)	
	PE	VaR
ORC 01	1.972.316.318	9.313.416.527
ORC 02	151.689.092	3.866.026.128
ORC 03	570.987.056	4.882.401.247
ORC 04	336.196.799	4.191.895.047
ORC 05	1.450.445.364	6.964.527.966
ORC 06	1.005.055.490	4.660.378.843
ORC 07	1.595.455.165	3.512.146.089
ORC 08	240.935.703	351.706.173
ORC 09	26.509.776	125.818.501
ORC 10	254.822.240	1.998.646.744
ORC 11	1.015.084.967	4.524.576.415
ORC 12	674.183.762	690.800.708
ORC 13	108.904.006	936.851.993
TOTAL	9.402.585.740	46.019.192.381

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

El ORC N° 4 corresponde a la valorización de los riesgos tecnológicos durante el 2010, con un monto provisionado de MM\$ 4.191, valor que a través del modelo propuesto, se pretende disminuir.

## CAPITULO 5: RESULTADOS Y CONCLUSIONES DEL MODELO

### 5.1. CÁLCULO DE RIESGO OPERACIONAL BAJO EL MODELO PROPUESTO.

Para realizar el cálculo de provisión por concepto de Riesgo Operacional Tecnológico se consideraron los 7 riesgos claves seleccionados en la sección 4.3.2., y se sometieron a votación con los expertos en temas tecnológicos y de negocio, de acuerdo a la metodología VaR. Los resultados obtenidos de la votación son los siguientes:

**Tabla 17: Votación de Riesgos TI 2011.**

Cod. Riesgo	Ámbito	Votante	Valores Votados			
			N° de eventos	Periodicidad	PE por evento (M\$)	Max. Pérdida por evento (M\$)
BCTI2011-12-1	Operaciones TI	Gerente de Informática	3,0	Anual (6)	20.000	400.000
BCTI2011-12-2	Desarrollo TI	Gerente de Informática	3,0	Anual (6)	5.000	500.000
BCTI2011-12-3	Operaciones TI	Gerente de Informática	2,0	Anual (6)	4.500	300.000
BCTI2011-12-4	Operaciones TI	Gerente de Informática	2,0	Anual (6)	2.000	400.000
BCTI2011-12-5	Continuidad TI	Gerente de Informática	0,5	Anual (6)	2.950	43.000
BCTI2011-12-6	Operaciones TI	Gerente de Informática	2,0	Anual (6)	20.000	300.000
BCTI2011-12-7	Riesgo Operacional TI	Gerente de Riesgo Operacional	2,0	Anual (6)	2.950	43.000

Fuente: Desarrollado por Gonzalo Flores.

Una vez obtenidos los parámetros exigidos por la metodología, se efectuó la proyección estadística a través de los modelos de Poisson y Weibull, a objeto de determinar la pérdida esperada (PE) y el valor del riesgo (VaR) de cada uno y de esta forma, contar con los saldos acumulados.

Es importante recordar que la PE representa la media de los montos de pérdida votados por los expertos (valor de pérdida esperada por evento y valor máximo de pérdida por evento) y el VaR representa el percentil del 99,9% de la distribución de pérdida.

Luego el cálculo de PE y VaR entregó los siguientes resultados:

**Tabla 18: Valorización de Riesgos TI 2011.**

<b>Cod. Riesgo</b>	<b>Poisson Lambda</b>	<b>Weibull ALFA</b>	<b>Weibull BETA</b>	<b>VaR (M\$)</b>	<b>PE (M\$)</b>
BCTI2011-12-1	3,0	0,39	5.702,8	1.361.653	80.597
BCTI2011-12-2	3,0	0,25	191,6	946.709	14.921
BCTI2011-12-3	2,0	0,31	532,6	439.620	8.970
BCTI2011-12-4	2,0	0,18	17,8	597.203	3.796
BCTI2011-12-5	0,5	0,65	2.150,2	38.432	1.456
BCTI2011-12-6	2,0	0,64	14.327,6	421.557	39.553
BCTI2011-12-7	2,0	0,65	2.150,2	58.579	6.000
<b>TOTALES</b>				<b>3.863.757</b>	<b>157.293</b>

Fuente: Cálculo desarrollado por Gerencia de Riesgo Operacional Bci.

Una vez calculados la PE y el VaR de cada uno de los 7 riesgos tecnológicos principales seleccionados, se puede calcular el VaR acumulado, el cual suma un total de MM\$ 3.863, monto que debería ser incorporado al total de provisiones por riesgo operacional y que si en forma particular, lo comparamos con el monto calculado a diciembre de 2010 de MM\$ 4.191, en el ámbito de Áreas de Apoyo (Tecnología), podemos apreciar una disminución de MM\$328 (7,8%) en el requerimiento de capital por este concepto (solo tecnología), situación que sustenta la tesis propuesta y si bien, para validarla es necesario efectuar el proceso de valorización de riesgo operacional en el resto de las áreas, se puede aspirar a que a medida que los controles mejoren su efectividad y la organización adquiera una mayor madurez en su cultura de riesgo, las pérdidas reales disminuirán, las evaluaciones cualitativas serán mejores y las votaciones por riesgo serán más exactas y menos conservadoras, disminuyendo año a año su valorización y por ende su provisión.

Por otro lado, al BCI definió una escala de prioridades para abordar proyectos asociados a la disminución de los riesgos principales, basado en los montos de sus PE y VaR, donde las prioridades fluctúan entre los valores 1 y 4, siendo 1 baja prioridad y 4 prioridad crítica. De acuerdo a lo anterior, la escala definida por el Banco es la siguiente:

**Tabla 19: Escala de prioridad de Riesgo por PE.**

Criticidad	PE	Prioridad Riesgo
CRI	>= \$ 100.000	4
ALT	>= \$ 40.000	3
MED	>= \$ 20.000	2
BAJ	< \$ 20.000	1

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

**Tabla 20: Escala de prioridad por Riesgo VaR.**

Criticidad	VAR	Prioridad Riesgo
CRI	>= \$ 3.000.000	4
ALT	>= \$ 1.000.000	3
MED	>= \$ 600.000	2
BAJ	< \$ 600.000	1

Fuente: Desarrollado por Gerencia de Riesgo Operacional Bci.

De acuerdo a las escalas anteriores, podemos priorizar los riesgos de la siguiente forma:

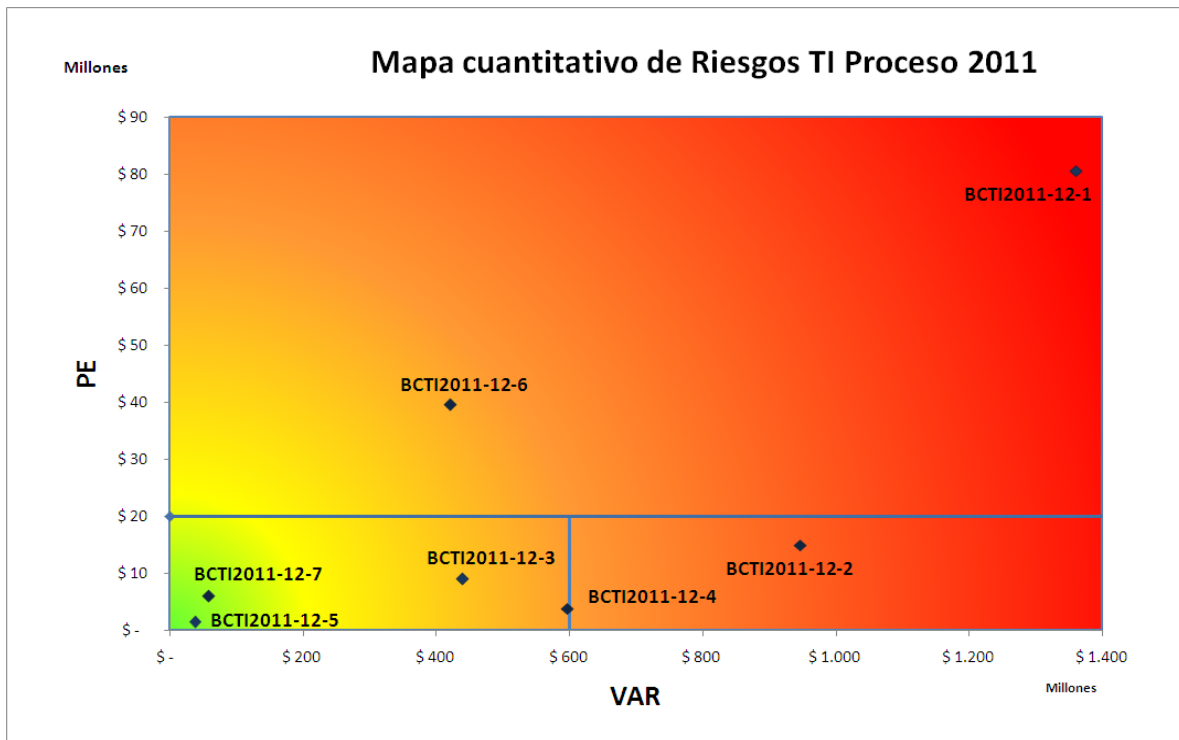
**Tabla 21: Totales de Var y PE con prioridades.**

Código Riesgo	VaR (M\$)	PE (M\$)	Prioridad VaR	Prioridad PE
BCTI2011-12-1	1.361.653	80.597	3	3
BCTI2011-12-2	946.709	14.921	2	1
BCTI2011-12-3	439.620	8.970	1	1
BCTI2011-12-4	597.203	3.796	1	1
BCTI2011-12-5	38.432	1.456	1	1
BCTI2011-12-6	421.557	39.553	1	2
BCTI2011-12-7	58.579	6.000	1	1
<b>TOTAL</b>	<b>3.863.757</b>	<b>155.297</b>		

Fuente: Desarrollado por Gonzalo Flores.

El siguiente gráfico muestra el mapa cuantitativo de riesgos TI con su distribución y prioridad para el proceso de toma de decisiones y mejora continua:

**Figura 30: Mapa cuantitativo de Riesgos TI**



Fuente: Desarrollado por Gonzalo Flores.

De acuerdo al gráfico y a la escala de prioridades de PE y VaR, los riesgos, cuyas soluciones de mitigación deberían ser abordados con prioridad son:

- a) **Código de Riesgo BCTI2011-12-1 - Pérdida de operaciones por aplicaciones defectuosas o que fallan con impacto en la operación diaria del Banco (servicio a clientes) y en la imagen Corporativa:** Este riesgo tiene una evaluación cuantitativa que lo presenta como el principal riesgo tecnológico que posee el Banco, ya que de acuerdo a su evaluación, tanto la pérdida promedio (PE), como la pérdida máxima (VaR), que puede generar, son muy altas, debiendo ser prioridad su mitigación.
- b) **Código de Riesgo BCTI2011-12-2 - Implantación de aplicaciones con errores que afecten la integridad y disponibilidad de la información de negocios y clientes:** Este riesgo debe ser trabajado debido a que su pérdida máxima (VaR) es muy alta en caso de hacerse efectivo.

**c) Código de Riesgo BCTI2011-12-6 - Daño de imagen Corporativa y pérdidas económicas por falla o indisponibilidad de servicio por activación de software malicioso:** Este riesgo tiene prioridad en su tratamiento, debido a que su pérdida promedio (PE) es alta, independientemente que su máxima pérdida, no se encuentra dentro de las más altas.

**d) Código de Riesgo BCTI2011-12-4 - Fraude por fuga de información y pérdidas económicas por accesos e implantación de componentes de software sin autorización en ambiente de producción:** Este riesgo está justo en el límite de las pérdidas máximas (VaR), aunque sus pérdidas promedio son bajas.

## 5.2. INTEGRACIÓN DE LA GESTIÓN CUALITATIVA Y CUANTITATIVA.

Para generar la integración de la gestión cualitativa y cuantitativa, es necesario establecer relaciones entre todas las herramientas que fueron generadas durante ésta tesis; mapas de riesgos, controles claves establecidos, indicadores de riesgos (KRIs), datos de pérdidas operacionales recopilados y clasificados, las mediciones de capital para los riesgos principales y los planes de acción para mejorar; de esta forma, se puede tener una visión general que permita apoyar el proceso de toma de decisiones orientadas a mejorar la gestión de riesgos. Esta integración, se transformará en una especie de panel de luces dinámico que confluya en el establecimiento de un plan estratégico, para mitigar el riesgo operacional tecnológico.

**Tabla 22: Propuesta de Panel de Luces dinámico.**

Control	Riesgo	Pérdida Real	Nota Cualitativa	Evaluación Cuantitativa	Plan de Acción	
Control 1	Riesgo 1	Pérdida 1	●	Nivel de riesgo 1 ●	VaR y PE 1 ●	Plan 1
Control 2	Riesgo 2	Pérdida 2	●	Nivel de riesgo 2 ●	VaR y PE 2 ●	Plan 2
Control n	Riesgo n	Pérdida n	●	Nivel de riesgo n ●	VaR y PE n ●	Plan n

Fuente: Desarrollado por Gonzalo Flores.

### 5.3. PROYECCIÓN DEL RIESGO TI EN BCI A TRES AÑOS.

De acuerdo a los objetivos planteados para esta tesis, a través de la gestión continua de los riesgos, se pretende disminuir los montos de provisión por riesgo operacional en un 20% en 3 años de funcionamiento, lo que implica lograr una provisión del 6,44% del Margen Bruto (MM\$ 36.769) en el último año.

Para los cálculos de proyección, se tomaron los datos calculados en el único ejercicio efectuado por el BCI utilizando un modelo avanzado, ejercicio realizado a diciembre de 2010.

**Tabla 23: Provisiones a diciembre 2010.**

	Valores
Margen Bruto 2010	570.957.721.849
Provisiones RO 2010	46.019.192.381
Porcentaje Margen Bruto 2010	8,06%

Fuente: Desarrollado por Gonzalo Flores.

De acuerdo a lo anterior, la proyección de provisiones en los próximos 3 años se distribuirá de la siguiente manera:

**Tabla 24: Proyección de provisiones RO a 3 años.**

	Provisión RO 2011	% del Margen Bruto 2011	Provisión RO 2012	% del Margen Bruto 2012	Provisión RO 2013	% del Margen Bruto 2013
Provisión por Riesgo	43.678.265.721	7,65%	41.394.434.834	7,25%	36.769.677.287	6,44%

Fuente: Desarrollado por Gonzalo Flores.

Los ahorros para el Banco deberían ser los siguientes:

**Tabla 25: Proyección de Ahorro/utilidades en 3 años.**

	Año 2011	% de Ahorro 2011	Año 2012	% de Ahorro año 2012	Año 2013	% de Ahorro año 2013
Ahorro en Provisiones	2.340.926.660	5%	4.624.757.547	10%	9.249.515.094	20%

Fuente: Desarrollado por Gonzalo Flores.



#### 5.4. EVALUACIÓN DE 3 PROYECTOS ASOCIADOS AL LOGRO DE LA PROYECCIÓN.

Para el desarrollo del modelo de gestión de riesgos TI, hemos planteado tres proyectos, que se consideran indispensables para el éxito de éste.

El detalle de los proyectos es el siguiente:

**a) Proyecto 1:** Adquisición de un software de clase mundial, para la gestión del riesgo operacional del Banco, con el cual se pueda almacenar una base de datos histórica de riesgos y pérdidas, generar y calcular regresiones estadísticas y estimar valores de acuerdo a modelos avanzados conocidos tales como el Value At Risk (VaR)

El costo de este proyecto incluye Hardware (4 servidores para ambientes de desarrollo, pruebas y producción), Software, capacitación, 5 licencias anuales, mantención, soporte e implantación (ajustes a BCI) tiene un costo de US\$ 2.250.000.

**Tabla 26: Desglose de Costos – Proyecto 1.**

<b>Proyecto 1 - Software</b>			
<b>Item de Costos</b>	<b>Costo en US\$</b>	<b>Tipo de cambio</b>	<b>Valor en \$</b>
Licencias (5)	250.000	500	125.000.000
Implantación	500.000	500	250.000.000
Capacitación	100.000	500	50.000.000
Soporte (1 año)	200.000	500	100.000.000
Hardware (4 servidores)	1.200.000	500	600.000.000
<b>COSTO TOTAL</b>	<b>2.250.000</b>	<b>500</b>	<b>1.125.000.000</b>

Fuente: Desarrollado por Gonzalo Flores.

**b) Proyecto 2:** Consultoría para efectuar un proceso detallado de valorización de riesgos tecnológicos, para complementar los 4 controles iniciales definidos para este modelo. Con esta asesoría se pretende optimizar también los modelos matemáticos para el cálculo y valorización del riesgo operacional tecnológico.

El costo de este proyecto está calculado a 2,5 UF la hora consultor (se requiere de al menos un consultor y un líder de proyecto) y se estima una duración de 10

meses, es decir 300 días hábiles. De acuerdo a lo anterior, el costo de este proyecto se estima en US\$ 567.600

**Tabla 27: Desglose de Costos – Proyecto 2.**

Proyecto 2 - Consultoría		HH / Consultor 2,5 UF	HH / Líder 5 UF				
Item de Costos	Días/Consultor	Días/Líder	Valor UF	Costo en US\$	Tipo de cambio	Valor en \$	
Levantamiento de Controles	180	120	21.500	361.200	500	180.600.000	
Desarrollo de Indicadores	90	30	21.500	129.000	500	64.500.000	
Capacitación	30	30	21.500	77.400	500	38.700.000	
<b>TOTALES</b>	300	180	21.500	567.600	500	283.800.000	

Fuente: Desarrollado por Gonzalo Flores.

**c) Proyecto 3:** Proyecto de Change Management para complementar el modelo y asegurar una correcta implantación. Este proyecto contaría con las siguientes etapas:

- Reingeniería del Proceso: Donde se aplicaría un cambio radical en la forma de medir los controles riesgos asociados a los procesos tecnológico del Banco.
- Administración de Ineficiencias: Donde se establecería nuevos procedimientos para mejorar la eficacia y eficiencia de los controles TI.
- Administración de la Calidad Total: Etapa en que los procesos serán mejorados de modo de aumentar la calidad de los servicio TI entregados.

La integración de este proyecto al Modelo de Gestión de Riesgo TI propuesto tiene un importante componente de comunicación el cual debe ser aplicado en la totalidad de la organización.

El proyecto tiene un costo total de US\$ 2.300.000.

**Tabla 28: Desglose de Costos – Proyecto 3.**

Proyecto 3 - Change Management			
Item de Costos	Costo en US\$	Tipo de cambio	Valor en \$
Etapa 1: Reingeniería	1.000.000	500	500.000.000
Etapa 2: Adm. de Ineficiencias	800.000	500	400.000.000
Etapa 3: Adm. Calidad Total	500.000	500	250.000.000
<b>TOTALES</b>	2.300.000	500	1.150.000.000

Fuente: Desarrollado por Gonzalo Flores.

Los 3 proyectos se estima serán desarrollados uno por año en el siguiente orden:

**Tabla 29: Costos / Proyectos**

Proyectos	Costo en US\$	Tipo de Cambio	Valor en \$
P1:Software	2.250.000	500	1.125.000.000
P2: Consultoría	567.600	500	283.800.000
P3: Change Management	2.300.000	500	1.150.000.000
<b>COSTO TOTAL</b>			<b>2.558.800.000</b>

Fuente: Desarrollado por Gonzalo Flores.

## 5.5. ANÁLISIS DE COSTO/BENEFICIO DEL NUEVO MODELO.

Para realizar el análisis de costo beneficio utilizaremos el método de Valor Actual Neto (VAN).

Para los flujos futuros utilizaremos los ahorros proyectados en el acápite 5.2., como ingresos esperados, la inversión inicial será el costo del proyecto asociado a la compra del software, el segundo año se efectuará el proyecto de consultoría para desarrollar el modelo con una evaluación detallada de todos los controles TI del Banco y el tercer año, se realizará el proyecto de Change Management para potenciar los aspectos culturales y operativos necesarios para disminuir los riesgos.

La tasa de descuento utilizada será la definida por el Banco, para proyectos tecnológicos y operativos y que es de un 15%.

De acuerdo a lo anterior, el VAN los calcularemos de la siguiente manera:

**Tabla 30: Flujos – VAN**

Conceptos	Año 0	Año 1	Año 2
<b>Ingresos (Ahorro en Provisión)</b>	2.340.926.660	4.624.757.547	9.249.515.094
<b>Costos de Proyectos</b>	1.125.000.000	283.800.000	1.150.000.000
<b>Flujos</b>	1.215.926.660	4.340.957.547	8.099.515.094
<b>Tasa de Descuento</b>	15%		
<b>VAN</b>	\$ 9.665.277.738		

Fuente: Desarrollado por Gonzalo Flores.

El Valor Actual Neto del Modelo propuesto es de MM\$ 9.665 positivo, lo cual nos permite contar con una cartera de proyectos rentables.

## 5.6. ANÁLISIS DE SENSIBILIDAD FINANCIERO.

No obstante la evaluación anterior, para tener una visión del grado de riesgo que puede tener la inversión en este proyecto, efectuaremos un análisis de sensibilidad tomando como base 2 factores que impactan fuertemente en el valor actual neto del proyecto; la tasa de descuento y los ahorros en provisión presupuestados (flujos de ingresos).

**a) Variación de la tasa de descuento:** Los supuestos tienen relación con la disminución de la liquidez en el mercado, aumento de las tasas de interés para los Bancos, tipos de cambio en alza y que impactan directamente en la tasa de retorno, los cuales aumenta de 15% a 25%. De acuerdo a lo anterior, el nuevo VAN de proyecto sería el siguiente:

**Tabla 31: Flujos – VAN con variación de tasa de descuento.**

Conceptos	Año 0	Año 1	Año 2
<b>Ingresos (Ahorro en Provisión)</b>	2.340.926.660	4.624.757.547	9.249.515.094
<b>Costos de Proyectos</b>	1.125.000.000	283.800.000	1.150.000.000
<b>Flujos</b>	1.215.926.660	4.340.957.547	8.099.515.094
<b>Tasa de Descuento</b>	25%		
<b>VAN</b>	\$ 7.897.905.886		

Fuente: Desarrollado por Gonzalo Flores.

El Valor Actual Neto del Modelo, incluyendo una variación en la tasa de descuento, es de MM\$ 7.897 positivo, y si bien, es más bajo que el valor calculado utilizando una tasa de 15%, podemos contar con un modelo con proyectos rentables.

**b) Variación de los porcentajes de ahorro en provisión (ingresos):** Los supuestos en este caso, tienen relación con el empeoramiento del comportamiento de pago de la cartera de clientes, aumento de los porcentajes de provisión por riesgo operacional por parte de la SBIF, aumentos de los castigos por problemas en los sistemas, aumento de los fraudes tecnológicos y que impactan en un aumento en las provisiones por riesgo operacional TI, disminuyendo los ahorros

anuales en un 30% de lo presupuestado. De acuerdo a lo anterior, el nuevo VAN de proyecto sería el siguiente:

**Tabla 32: Flujos – VAN con variación en los ingresos (ahorros de provisión).**

Conceptos	Año 0	Año 1	Año 2
<b>Ingresos (Ahorro en Provisión – 30%)</b>	1.638.648.662	3.237.330.283	6.474.660.566
<b>Costos de Proyectos</b>	1.125.000.000	283.800.000	1.150.000.000
<b>Flujos</b>	513.648.662	2.953.530.283	5.324.660.566
<b>Tasa de Descuento</b>	15%		
<b>VAN</b>	\$ 6.180.994.984		

Fuente: Desarrollado por Gonzalo Flores.

El Valor Actual Neto del Modelo, incluyendo una disminución del 30% en los ingresos anuales (ahorros en provisiones), es de MM\$ 6.180 positivo, siendo la situación más desfavorable para el modelo, sin embargo, a pesar de ésta, podemos contar una rentabilidad positiva.

Ambos resultados (a y b) nos permiten contar con un margen de error importante en la estimación inicial, sin que la factibilidad del proyecto se vea comprometida.

**b) Variación de los flujos para un VAN = 0:**

Adicionalmente, como parte de este análisis se han querido presentar las condiciones bajo las cuales el Valor Actual Neto del proyecto podría tener un valor de cero.

Las condiciones para que dicha situación se produzca, tienen relación con la variación negativa de los flujos de ingresos (ahorro) en cada período, bajo los siguientes supuestos:

- a) Los costos y la tasa de descuento no tendrán variaciones.
- b) Para el primer año no habrá disminución en el monto de provisiones por concepto de riesgo tecnológico, situación que podría ocurrir si la medición de la efectividad de los controles retornara resultados negativos, por lo que no existiría un ahorro del 5% para el Banco de acuerdo a lo proyectado.

c) El Ahorro estimado en provisiones para el segundo año sería de un 2% y no de un 10% de acuerdo a lo proyectado, situación que podría ocurrir bajo el mismo supuesto del punto b).

d) El ahorro estimado en provisiones para el tercer año sería de 4% y no de un 20% de acuerdo a lo proyectado, situación que podría ocurrir bajo el mismo supuesto del punto b).

De acuerdo a dichos supuesto, los valores deberían ser los siguientes:

**Tabla 33: Flujos – VAN = 0.**

Conceptos	Año 0	Año 1	Año 2
<b>Ingresos (Ahorro en provisión)</b>	0	1.113.000.000	1.684.232.500
<b>Costos de Proyectos</b>	1.125.000.000	283.800.000	1.150.000.000
<b>Flujos</b>	-1.125.000.000	829.200.000	534.232.500
<b>Tasa de Descuento</b>	15%		
<b>VAN</b>	\$ 0		

## 5.7. CONCLUSIONES DEL MODELO DE GESTIÓN DE RIESGO TI.

De la presente investigación se desprenden una serie de conclusiones relevantes, no sólo respecto del cumplimiento, o no, de la tesis propuesta, sino que también, respecto de los aportes al crecimiento personal, profesional y respecto de los aportes a la industria bancaria y sus modelos de Gobierno Corporativo.

### a) Resultado de la tesis propuesta.

- Repasando los objetivos planteados para este proyecto, principalmente se intentó demostrar que a través de una buena gestión de riesgos TI y la utilización de un modelo avanzado de valorización de estos riesgos, es posible disminuir las provisiones por concepto de Riesgo Operacional, tesis que pudo ser demostrada en parte, debido a la disminución del requerimiento de capital para los riesgos tecnológicos en MM\$328, respecto de lo calculado en el ejercicio anterior efectuado en diciembre de 2010, faltado la ejecución del cálculo de los montos de

provisión para el resto de los procesos y unidades de negocio cuyos riesgos operacionales son evaluados y que no fueron parte del ámbito de esta tesis.

- De acuerdo al resultado obtenido, el ahorro en provisiones puede aumentar si se logra aumentar el nivel de madurez de los controles, lo que disminuiría las pérdidas reales, mejorará la calificación de riesgo y su posterior valorización. Lo anterior, debe ser parte del proceso de mejora continua de cualquier organización que se proponga administrar adecuadamente sus riesgos.

- Este proyecto se alineó directamente con los objetivos estratégicos de la organización y que no sólo tienen que ver con los ámbitos financieros y de rentabilidad, sino que también con los objetivos relacionados a la mejora continua de los procesos internos para facilitar la vida a los clientes y a la innovación que es un pilar fundamental en BCI.

- Si bien, en la actualidad solo las instituciones financieras están obligadas a provisionar por concepto de Riesgo Operacional, este modelo es perfectamente aplicable a otro tipo de industrias que quieran mejorar su control interno en aspectos tecnológicos y contar con una herramienta potente de Gobierno Corporativo, como por ejemplo Compañías de Seguro, Mineras, empresas de Retail e Industrias en general.

- Un elemento que surge como conclusión de esta tesis, es que a través de las entrevistas realizadas a los expertos del negocio y tecnología, se pudo evidenciar que la sensibilización para estimar una valorización del riesgo por parte de éstos, es muy variada, y esta diversidad hace que los puntajes más extremos se encuentren muy dispersos, por lo tanto, se hace necesario un proceso de evaluación cualitativa de controles y riesgos, que permita direccionar de mejor manera este proceso, aspecto totalmente cubierto por el modelo propuesto en esta tesis.

- Producto del análisis y evaluación de controles TI, realizada a través de este trabajo, se puede concluir que los controles claves y riesgos principales TI pueden ir variando en el tiempo y deben ser evaluados y gestionados constantemente, de modo que el modelo no pierda su efectividad y cuente con niveles adecuados de exactitud.

- La metodología de evaluación cualitativa de controles TI, puede ser perfectamente utilizada como una herramienta potente de control de gestión para las Gerencias de Tecnología, Operaciones Computacionales y Riesgo Operacional, ya que permite medir la efectividad de los controles a través de los indicadores desarrollados (KRIs) y de aquellos que se puedan desarrollar como complemento al modelo propuesto, permitiendo establecer métricas de efectividad y eficiencia para estas Gerencias.
- A nivel estratégico un modelo de estas características, con una mejora continua de los controles TI, permite potenciar la cadena de valor del Banco, aumentando la disponibilidad, integridad y confidencialidad de los servicios entregados a los clientes, que en su mayoría interactúan con tecnología, algo muy valorado por ellos y por los stakeholders en general, lo que trae consigo como consecuencia, mejores evaluaciones por parte de entidades reguladoras y evaluadoras, desembocando finalmente en mejores indicadores de confianza que permiten aumentar el valor de la acción.
- Respecto a los temas relacionados con la regulación existente (Basilea II) y a una posible exigencia futura para la utilización de modelos avanzados en cálculo de provisiones por riesgo operacional, esta tesis entrega herramientas al Banco para avanzar desde ya en mejorar sus procesos y cultura de control, para disminuir los riesgos y de esta forma estar mucho más preparados para cuando ese momento llegue.

#### **b) Aspectos Culturales y de Gobierno Corporativo:**

- Un primer aspecto importante para que la administración del riesgo operacional verdaderamente funcione, es contar con bases concretas dentro de la estructura organizativa y de la alta dirección, allí las buenas prácticas de gobierno corporativo y la capacitación en temas de riesgo resultan ser fuertes mitigantes del riesgo, siempre que estén asumidas adecuadamente dentro de toda la organización. Luego, a través de este trabajo, se puede concluir que, independientemente que la organización ha instaurado y reforzado constantemente una cultura de



administración de riesgo, existe una gran falencia en la cultura de riesgo, especialmente en las áreas de tecnologías que generan diferencias importantes en los criterios de identificación y evaluación de éstos, que dificultan un adecuado control, lo que hace muy necesario que se generen procesos globales de apoyo tales como capacitación y Change Management, a objeto de homologar criterios y reforzar la cultura de riesgo.

- El segundo factor importante con impacto en el proceso de gestión de riesgos, es la contingencia diaria que afecta a las organizaciones en general y de la cual, el Banco no está exento. Estas situaciones sumadas a la constante necesidad de cumplir metas comerciales, merman la disponibilidad de los ejecutivos en el adecuado cumplimiento de los controles.
- El tercer aspecto observado, tiene relación con el nivel de madurez de los controles establecidos en la organización, ya que de acuerdo a las mejores prácticas internacionales, el Banco cuenta con controles específicos en cada uno de los aspectos declarados como importantes dentro de los estándares de seguridad, sin embargo, al momento de medirlos a través de los indicadores (KRIs) desarrollados en esta tesis, se puede deducir que estos controles no son lo suficientemente robustos para disminuir el riesgo, por lo que también, se hace necesario generar un proceso de levantamiento y mejoramiento de los controles TI existentes.
- El cuarto y último aspecto tiene que ver con la importancia de contar con buenas herramientas de gestión y de gobierno corporativo en las organizaciones y se espera haber generado un aporte en este sentido, tanto para el Banco como para cualquier organización que quiera utilizar un modelo de ésta naturaleza, el cual ayudará a contar con un mejor ambiente de control interno.

### **c) Aspectos a mejorar.**

Algunos aspectos que creo pueden potenciar el modelo propuesto son:

- Definir la totalidad de controles claves e indicadores (KRIs) que un estándar o mejor práctica internacional (Cobit, ISO 2700; entre otros) recomienda, de modo de abarcar la totalidad de áreas claves al momento de medir el riesgo.
- Complementar la valorización de riesgos con escenarios y datos externos para acercar más la visión de riesgo del Banco, respecto de lo que ocurre en la Banca local e internacional.
- Establecer procesos formales de votación de riesgo para los procesos Tecnológicos, que cuenten con la mayor cantidad de expertos posibles, de modo de obtener un visión más amplia. Para esta tesis, no fue posible reunirlos a todos.
- De acuerdo al análisis de la base de datos de pérdida pudimos comprobar que existen riesgos que no tienen representación en pérdidas de manera adecuada en la contabilidad, lo que implica que el Banco tiene que corregir la asignación de las cuentas de castigos, a los centros de costos que efectivamente son responsables de las pérdidas.

#### **d) Aspectos Personales:**

- En lo personal este trabajo, más que permitir desarrollar una innovación para la mejora de procesos de control de la institución en la cual trabajo, me permitió obtener un aprendizaje importante respecto de las cosas que se requieren para generar una innovación en una organización, pensando en que BCI tiene una cultura organizacional, donde el riesgo tecnológico siempre ha sido controlado gracias a la función de Contraloría y no, a los controles internos de la línea de producción, y con una función de Riesgo Operacional, que de acuerdo a lo relevado a través de este trabajo, se encuentra comenzando a explorar procesos un poco más sofisticados de medición, por lo que iniciativas de este tipo son muy necesarias, así como el apoyo de la alta dirección del Banco.
- Conocí en profundidad las distintas visiones respecto del riesgo operacional tecnológico en BCI y en la Banca en general, el nivel de sensibilidad respecto de éste en la organización, el nivel de madurez de los controles establecidos para

disminuir los riesgos existentes y me permitió potenciar la capacidad de desarrollar herramientas valiosas para la gestión.

#### **e) Aspectos Generales.**

Este modelo permitirá al Banco, pasar de un enfoque de riesgo por impresiones a un enfoque por demostraciones, lo cual es un valor agregado a la hora de justificar los proyectos para potenciar la seguridad y los controles, situación que es muy común en las organizaciones que no tienen cifras para justificar inversiones. No obstante lo anterior, es muy importante no perder el foco y tener claridad en que la medición del riesgo operacional no reemplaza su gestión.

Finalmente quisiera resumir las conclusiones de este proyecto en tres beneficios de su aplicación:

- El trabajar con esquemas de medición avanzada de riesgo operacional permite, en el mediano plazo, la reducción de las provisiones por riesgo.
- El segundo beneficio surge de la administración proactiva del riesgo operacional, que puede reducir las pérdidas operativas, por medio de su impacto directo en los ratios de eficiencia y como consecuencia de ello, en los resultados.

El racional de esto, es que cuanto mejores sean las herramientas para administrar el riesgo operacional, mayor será la habilidad para mitigar las pérdidas.

- El tercer beneficio esta dado por la integración de las mejoras surgidas a partir de la gestión del riesgo operacional, con aquellas que puedan surgir de los procesos de mejora de calidad y de atención al cliente.

## REFERENCIAS BIBLIOGRÁFICAS

- AROMÓS Antonio y TIPPELT Rudolf: Paper “Gestión del Cambio y la innovación, un reto de las organizaciones modernas”, Alemania, Abril 2005, [www.inwent.org](http://www.inwent.org).
- Banco Crédito e Inversiones: Memoria Anual y Estados Financieros 2010, Santiago, Chile, Marzo 2011. <http://www.bci.cl/medios/BCI2/accionistas/pdf/memoria/MemoriaBci2010.pdf>.
- Banco Crédito e Inversiones: Página Web Institucional, Chile, 2011, [www.bci.cl](http://www.bci.cl).
- DELFINER Miguel, MANGIALAVORI Ana y PAILHÉ Cristina: Paper “Buenas prácticas para la administración del riesgo operacional en entidades financieras”, Argentina, Enero 2007. <http://mpr.ub.uni-muenchen.de/1803/>.
- FIGUEROA María, INDRI Ana María, MARASCA Rubén y STEFANELLI Darío: Basilea II; Paper: “Hacia un nuevo esquema de medición de riesgos”, Argentina, 2003, [http://www.felaban.com/boletin\\_clain/basileall.pdf](http://www.felaban.com/boletin_clain/basileall.pdf).
- Information System Audit and Control Association (ISACA); Página Web Institucional, EEUU, 2011, [www.isaca.org](http://www.isaca.org).
- International Organization for Standardization: Estándar Internacional ISO/IEC 27001, Primera Edición – Sistema de Seguridad de la Información – Requerimientos, España, 2005.
- International Organization for Standardization: Estándar Internacional ISO/IEC 31000, Principios y Lineamientos para gestión de riesgos, EEUU, 2009.
- IT Governance Institute & ISACA Chapter : Cobit (Objetivos de Control para la información y tecnologías relacionadas), EEUU, 2007.
- IT Governance Institute & ISACA Chapter : Marco de Riesgos de TI - Risk IT, EEUU, 2009, ISBN 978-1-60420-111-6.
- IT Governance Institute & ISACA Chapter: Valor para la Empresa: Buen Gobierno de la inversiones en TI – El Marco de VAL IT, Cobit, EEUU, 2006. ISBN 1-933284-32-3.

- Superintendencia de Bancos e Instituciones Financieras (SBIF); Página Web Institucional, Chile, 2011, [www.sbif.cl](http://www.sbif.cl).
- Universidad de Chile, Facultad de Ciencias Físicas y Matemáticas, Departamento de Ingeniería Industrial, Lista de titulados de Magister, Chile, 2010.

## ANEXO A: RIESGO EN LA BANCA

### A.1. Tipología de riesgos:

El término Riesgo, se utiliza en general para situaciones que involucran incertidumbre, en el sentido de que el rango de posibles resultados para una determinada acción, es en cierta medida, significativo.

El riesgo es la posibilidad de que una acción o una actividad, dará lugar a una pérdida (un resultado no deseado). Las pérdidas potenciales pueden también ser llamados "riesgos".

En general existen infinitos tipos de riesgo, sin embargo, los que tienen relación con este proyecto, son los que indican la Normas de auditoría internacionales, la clasificación entregada por la SBIF y la que utiliza el BCI para medir sus riesgos.

#### a) Clasificación según Normas Internacionales de Auditoría:

La clasificación de riesgo de las Normas Internacionales de auditoría es la siguiente:

**Riesgo del Negocio:** Es cualquier cosa que pueda hacer que un objetivo del negocio no se cumpla. Los riesgos del negocio, sólo pueden ser identificados y definidos en base a los objetivos del negocio.

**Riesgo de Auditoría:** Es cualquier posible acción que pueda afectar la opinión en relación al control interno.

El riesgo de auditoría tiene 3 componentes:

- Riesgo Inherente: Es aquel riesgo que por su naturaleza no se puede separar de la situación donde existe. Es propio del trabajo a realizar. Es el riesgo propio de cada empresa de acuerdo a su actividad.
- Riesgo de Control: Es aquel que existe y que se propicia por falta de control de las actividades de la empresa y puede generar deficiencias del Sistema de Control Interno.

- Riesgo de Detección: Es aquel que se asume por parte de los auditores que en su revisión no detecten deficiencias en el Sistema de Control Interno.

#### **b) Clasificación según SBIF:**

La Superintendencia de Bancos e Instituciones Financieras (SBIF) en la RAN 1-13 entrega las clasificaciones de riesgos que deben considerar los Bancos y los aspectos que se deben controlar en cada una:

- **Riesgo de Crédito**: Es la posible pérdida que asume un Banco como consecuencia del incumplimiento de las obligaciones contractuales que incumben a las contrapartes con las que se relaciona (clientes).

Algunos de los controles, que en este sentido, la SBIF exige a los Bancos son:

- Gestión de riesgo de crédito y los factores de riesgo del proceso de crédito, desde la definición del mercado objetivo hasta la recuperación de los préstamos.
- Políticas y procedimientos acorde a las operaciones y estrategia (identificación, cuantificación, límite y controles para grandes exposiciones).
- Aprobaciones, supervisión, controles para el cumplimiento de las políticas y procedimientos.
- Segregación funcional, (comercial, riesgo, operaciones, contraloría).
- Detección, reconocimiento, medición, seguimiento oportuno de los riesgos (clasificación cartera).
- Contar con sistemas de información de gestión.
- Contar con auditoría interna.

- **Riesgo Financiero**: También conocido como riesgo de crédito o de insolvencia. Hace referencia a las incertidumbres en operaciones financieras derivadas de la volatilidad de los mercados financieros y de créditos.

Por ejemplo, la incertidumbre asociada al rendimiento de la inversión, debido a la posibilidad de que la empresa no pueda hacer frente a sus obligaciones financieras (pago de los intereses, amortización de las deudas); es decir, el riesgo financiero es debido a un único factor; las obligaciones financieras fijas en las que se incurre.

Algunos de los controles, que en este sentido, la SBIF exige a los Bancos son:

- Manejo del riesgo liquidez y precios (tasa de interés y tipo de cambio).
- Identificación, cuantificación, limitación y control de los riesgos.
- Segregación funcional, (comercial, riesgo, operaciones y contraloría).
- Políticas y procedimientos acorde a las operaciones y estrategia (identificación, cuantificación, límite y controles).
- Contar con sistemas de información de gestión.
- Contar Auditoría interna.

• **Riesgo Operacional:** Es el riesgo de pérdidas resultantes por la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas, o bien aquellas que sean producto de eventos externos.

En otras palabras, es el riesgo que incurre un banco por su operatoria, que no está ya clasificado como riesgo de crédito, de mercado u otros ya tradicionales, y que ha cobrado gran notoriedad dada la mayor externalización de procesos, sistemas tecnológicos complejos, productos derivados y estructurados, y una mayor diversidad de negocios financieros.

Algunos de los controles, que en este sentido la SBIF exige a los Bancos son:

- Controlar el riesgo de pérdida resultante de una falla de adecuación o de una falla de los procesos, del personal y de los sistemas internos o acontecimientos externos.
- Identificación, cuantificación, limitación y control de los riesgos operacionales.
- Políticas y procedimientos acorde a las operaciones y estrategia.
- Inversiones en tecnología, continuidad del negocio.
- Contar con sistemas de información de gestión.
- Contar con auditoría interna.

• **Riesgos de Exposición en el Exterior y Control sobre las Inversiones en Sociedades:** Riesgo que pueden afectar a sucursales en el exterior, filiales, y sociedades de apoyo al giro por falta de control de la Matriz.

Algunos de los controles, que en este sentido, la SBIF exige a los Bancos son:

- Control de sucursales en el exterior, filiales y sociedades de apoyo al giro; transacciones efectuadas en el extranjero.
- Controles de la matriz sobre sus sucursales en el exterior, filiales y SAG.



- Riesgo país (evaluación, límites, concentración).
- Contar con sistemas de información de gestión.
- Contar con auditoría interna.

• **Riesgos de Estrategia de Negocio y Gestión de Capital:** Riesgos del proceso de diseño, formulación y seguimiento de la estrategia de negocios como también de la elaboración y control de los planes desarrollados por el Banco.

Algunos de los controles, que en este sentido la SBIF exige a los Bancos son:

- Viabilidad de la estrategia (fundada, sostenible).
- Requerimientos de capital actuales y futuros (objetivos estratégicos).
- Contar con sistemas de información de gestión.
- Contar con auditoría interna.

• **Riesgo en la Calidad de Atención a los Usuarios y Transparencia de la Información:** Riesgos que afectan la buena calidad en la atención de los clientes, así como la calidad de la información que les es divulgada y deben ser parte de los aspectos importantes de imagen del Banco.

Algunos de los controles, que en este sentido, la SBIF exige a los Bancos son:

- Existencia de políticas y procedimientos para gestionar el servicio a clientes (controversias, entrega información de cobros, etc.).
- Contar con sistemas de información de gestión.
- Contar con auditoría interna.

• **Riesgo de Lavado de Activos y Financiamiento del Terrorismo:** Riesgo de operaciones de blanqueo de capitales con falta de controles adecuado e involucramiento del Directorio.

Algunos de los controles, que en este sentido la SBIF exige a los Bancos son:

- Existencia de políticas y procedimientos formales.
- Existencia de un oficial de cumplimiento, procedimiento de; “conozca a su cliente” y selección de personal, código de conducta.
- Contar con sistemas de información de gestión.
- Contar con auditoría interna.

### **c) Clasificación según BCI:**

En el Banco los riesgos se gestionan y clasifican en Riesgo Financieros, Riesgo de Crédito, Riesgo de Liquidez y Riesgo Operacional.

El nivel de severidad de los riesgos esta dado por:

- **Riesgo bajo:** Corresponde a aquella en que los procesos validados, no revelan riesgos importantes que pudieran afectar el patrimonio o resultados del Banco y/o Filiales y los eventuales incumplimientos de políticas o normas son puntuales, sin mayores riesgos asociados.
- **Riesgo medio:** Corresponde a aquella en que los procesos validados revelan algunos tipos de riesgos derivados de incumplimiento de políticas y/o normas o por otras causas que, de mantenerse, podrían afectar el patrimonio o resultados del Banco y/o Filiales pero que con medidas y acciones a implementar, es posible acotar.
- **Riesgo alto:** Esta calificación revela riesgos relevantes en los procesos validados que están o podrían estar afectando el patrimonio o resultados del Banco y/o Filiales, no existe una adecuada cultura de control.

### **A.2. Fuentes de Riesgo Operacional:**

**a) Procesos Internos:** Posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas, en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y presupuestos planeados.

**b) Personas:** Posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores. Se puede también, incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación.

**c) Tecnología de Información:** Posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Las instituciones pueden considerar incluir en ésta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas de información, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear las TI con los objetivos de negocio, entre otros aspectos. Otros riesgos incluyen la falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

**d) Eventos Externos:** Posibilidad de pérdidas, derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

### **A.3. Riesgo Operacional Tecnológico:**

El Riesgo Tecnológico, es uno de los componentes principales del Riesgo Operacional, e implica la probabilidad de pérdidas ante fallas de los sistemas de información, sumado a las fallas que se puedan dar a través de los canales de Banca Electrónica, así como a la probabilidad de fraudes internos y externos a través de los mismos, involucrando al riesgo legal y al riesgo reputacional que están presentes por fallas en la seguridad y distorsiones en la no disponibilidad de los sistemas de información, entre otros.

### **A.4. Descripción de Normativa Chilena:**

La normativa relacionada al Riesgo Operacional Tecnológico para el Banco, principalmente está dada por la SBIF, que es la institución que lo regula y se concentran en la Recopilación Actualizada de Normas (RAN) en su Capítulo 1-13 Clasificación de Gestión y Solvencia, y en una serie de circulares asociadas a la gestión del riesgo operacional y a requerimientos de capital por riesgo operacional para la implantación de Basilea II. En este sentido, algunos de los elementos exigidos son:

- El BCI tiene una definición de lo que entiende por riesgo operacional y lo ha reconocido como un riesgo gestionable. Especial importancia, tendrá la existencia de una función encargada de la administración de este tipo de riesgo.
- La entidad mantiene políticas para la administración de los riesgos operacionales, aprobadas por el directorio o la administración superior, que atienden la importancia relativa de los riesgos operacionales, considerando el volumen y complejidad de las operaciones.
- La estrategia de administración del riesgo operacional definida por BCI, es consistente con el volumen y complejidad de sus actividades y considera el nivel de tolerancia al riesgo del banco, incluyendo líneas específicas de responsabilidad. Esta estrategia, ha sido implementada a través de toda la

organización bancaria, y todos los niveles del personal asumen y comprenden sus responsabilidades respecto a la administración de este riesgo.

- La entidad administra los riesgos operacionales considerando los impactos que pudieran provocar en el banco (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.
- La entidad realiza evaluaciones del riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas. Asimismo, se asegura que antes de introducir nuevos productos, emprender nuevas actividades, o establecer nuevos procesos y sistemas, el riesgo operacional inherente a los mismos, esté sujeto a procedimientos de evaluación.
- El BCI ha integrado a sus actividades normales el monitoreo del riesgo operacional y ha identificado indicadores apropiados que entreguen alertas de un aumento del riesgo y de futuras pérdidas.
- El banco es capaz de cuantificar los impactos de las pérdidas asociadas al riesgo operacional y constituir prudencialmente los resguardos necesarios.
- Los sistemas de información, permiten hacer un monitoreo continuo de la exposición a los riesgos operacionales. Poseen la cobertura y profundidad necesarias para servir en forma eficiente al proceso de toma de decisiones de la alta administración y directorio.
- El BCI cuenta con políticas para administrar los riesgos asociados a las actividades entregadas a terceras partes y lleva a cabo verificaciones y monitoreos a las actividades de dichas partes.
- El BCI realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los riesgos operacionales y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.
- El BCI cuenta con una adecuada planificación a largo plazo para la infraestructura tecnológica y dispone de los recursos necesarios para el desarrollo normal de sus actividades y para que los nuevos proyectos previstos se concreten oportunamente.

- El BCI cuenta, con una estructura que permite administrar la seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad.
- El BCI considera, en sus planes de continuidad del negocio y contingencia, diversos escenarios y supuestos que pudieran impedir que cumpla toda o parte de sus obligaciones y en ese sentido ha desarrollado una metodología formal que considera en sus etapas, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación, así como pruebas periódicas de tales estrategias.
- El BCI ha implementado, un proceso para controlar permanentemente la incorporación de nuevas políticas, procesos y procedimientos, que permiten detectar y corregir sus eventuales deficiencias, de manera de reducir la frecuencia y severidad de los eventos de pérdida. Asimismo, la entidad emite reportes con la información pertinente a la alta administración y directores.
- La entidad bancaria ha adoptado una estrategia y sistema de gestión de calidad respecto de sus productos, servicios, e información que suministra a sus clientes, reguladores y a otros entes.
- La extensión y profundidad de las auditorías, es proporcional al nivel de riesgo y al volumen de actividad. La función de auditoría está en posición de evaluar en forma independiente el cumplimiento de las políticas, la eficacia de los procedimientos y los sistemas de información.

#### **A.5. Descripción de Normativa Internacional:**

**Basilea I:** Es el acuerdo que en 1988 publicó el Comité de Basilea, compuesto por los gobernadores de los Bancos Centrales de Alemania, Bélgica, Canadá, España, EE. UU., Francia, Italia, Japón, Luxemburgo, Holanda, el Reino Unido, Suecia y Suiza. Se trata de un conjunto de recomendaciones para establecer un capital mínimo que debía tener una entidad bancaria en función de los riesgos que afrontaba.

El acuerdo establecía una definición de "capital regulatorio" compuesto por elementos que se agrupan en 2 categorías; si cumplen ciertos requisitos de permanencia, de capacidad de absorción de pérdidas y de protección ante quiebra. Este capital debe ser suficiente para hacer frente a los riesgos de crédito, mercado y tipo de cambio.

Cada uno de estos riesgos, se medía con unos criterios aproximados y sencillos. El principal riesgo era el riesgo de crédito, y se calculaba agrupando las exposiciones de riesgo en 5 categorías según la contraparte y asignándole una "ponderación" diferente a cada categoría (0%, 10%, 20%, 50%, 100%), la suma de los riesgos ponderados formaba los activos de riesgo.

El acuerdo estableció que el capital mínimo de la entidad bancaria debía tener el 8% del total de los activos de riesgo (crédito, mercado y tipo de cambio sumados). Este acuerdo, era una recomendación y cada uno de los países participantes, así como cualquier otro país, quedaba libre de incorporarlo en su ordenamiento regulatorio con las modificaciones que considerase oportunas.

El primer acuerdo de capital de Basilea, ha jugado un papel muy importante en el fortalecimiento de los sistemas bancarios. La repercusión de ese acuerdo, en cuanto al grado de homogenización alcanzado en la regulación de los requerimientos de solvencia ha sido extraordinaria. Entró en vigor en más de 130 países.

Dado que el acuerdo contenía ciertas limitaciones en su definición, en junio del 2004 fue sustituido por el llamado acuerdo Basilea II.

**Basilea II:** El objetivo de Basilea II, es sustituir el anterior Acuerdo de Capital Basilea I. Ese capital denominado "regulatorio", busca garantizar la solvencia de las entidades frente a posibles pérdidas generadas por sus posiciones de riesgo de crédito, de mercado y operacional, no cubiertas mediante provisiones.

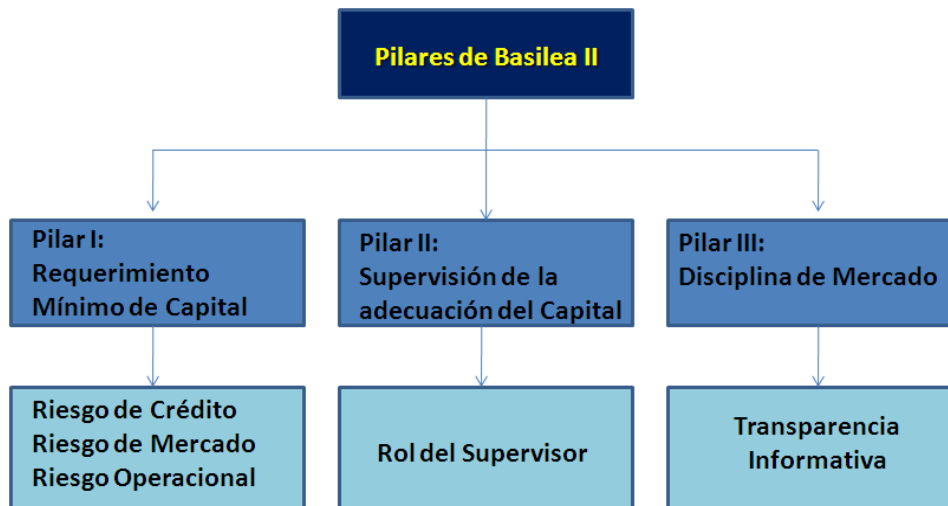
Basilea II, supone un importante salto cualitativo frente a la norma anterior, al permitir:

- Una cobertura completa de los riesgos actuales del negocio financiero.
- Incorporar nuevas modalidades de riesgos no contempladas por Basilea I.

- Establecer una metodología de cálculo de capital más sensible a los riesgos.
- Acercar los requerimientos de capital regulatorio al capital económico.

A través de sus tres pilares, Basilea II se convierte en una herramienta de mucho valor para mejorar los actuales modelos de gestión.

**Figura 31: Pilares de Basilea II.**



Fuente: [www.sbfci.cl](http://www.sbfci.cl)

#### A.6. Mejores prácticas Internacionales de Gestión de riesgo TI:

En el mercado, existe un sinfín de metodologías y mejores prácticas asociadas a la gestión de riesgos tecnológicos, sin embargo, para el proyecto describiremos a grandes rasgos, las que se ajustan de mejor manera al mercado financiero chileno, estas son:

**a) Norma ISO 27001:2005:** El estándar para la seguridad de la información ISO/IEC 27001 (Information technology - Security techniques - Information security management systems Requirements) fue aprobado y publicado como estándar internacional en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el



conocido Ciclo de Deming llamado PDCA, que es el acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar) y tiene su origen en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

Los 10 dominios para los cuales se exigen controles claves a incorporar son:

- Políticas de seguridad.
- Organización de la Seguridad.
- Control y Clasificación de Activos.
- Seguridad del Personal.
- Seguridad Física y Ambiental.
- Gestión de las Operaciones y Comunicaciones.
- Control de Acceso.
- Desarrollo y Mantenimiento de Sistemas.
- Gestión de la Continuidad del Negocio.
- Cumplimiento normativo y regulatorio.

**b) Norma ISO 31000:2009:** Es la nueva norma internacional ISO de gestión de riesgos, principios y directrices, que pretende ayudar a las organizaciones en contar con una gestión de riesgos efectiva. Establece los principios, el marco y un proceso para la gestión de cualquier tipo de riesgo en una forma transparente, sistemática y fiable en cualquier ámbito o contexto. Al mismo tiempo, la ISO publica la Guía ISO 73:2009, que es el vocabulario de gestión de riesgos, que complementa la norma ISO 31000, proporcionando una colección de términos y definiciones relativas a la gestión del riesgo.

El enfoque está estructurado en tres elementos claves para una efectiva gestión de riesgos:

1. Los principios para la gestión de riesgos.
2. La estructura de soporte.
3. El proceso de gestión de riesgos.

**c) Cobit 4.1 (Control Objectives for Information and related Technology):** Es un conjunto de mejores prácticas, para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto para el Gobierno de las Tecnologías de la Información (ITGI) en 1992.

En su cuarta edición, COBIT tiene 34 objetivos de alto nivel que cubren 210 objetivos de control clasificados en cuatro dominios:

- Planificación y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Supervisión y Evaluación.

**d) COSO (Committee Of Sponsoring Organizations):** El denominado Informe COSO, sobre control interno, publicado en EE.UU. en 1992, surgió como una respuesta a las inquietudes que planteaban la diversidad de conceptos, definiciones e interpretaciones existentes en torno a la temática referida.

Plasma los resultados de la tarea realizada durante más de cinco años por el grupo de trabajo que la Treadwat Commission, National Commission on Fraudulent Financial Reporting creó en Estados Unidos en 1985 bajo la sigla COSO.

El Informe COSO es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno. Debido a la gran aceptación de la que ha gozado, desde su publicación en 1992, el Informe COSO se ha convertido en el estándar de referencia en todo lo que concierne al Control Interno. El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control.
- Evaluación de riesgos.
- Actividades de control.
- Información y comunicación.
- Supervisión.

**g) Value at Risk (VaR):** El concepto de Value at Risk (VaR), o valoración del riesgo, proviene de la necesidad de cuantificar con determinado nivel de significancia o incertidumbre el monto o porcentaje de pérdida que un portafolio enfrentará en un período predefinido de tiempo

Su medición tiene fundamentos estadísticos y el estándar de la industria es calcular el VaR con un nivel de significancia del 5%. Esto significa que solamente el 5% de las veces, o 1 de 20 veces (es decir, una vez al mes con datos diarios, o una vez cada cinco meses con datos semanales), el retorno del portafolio caerá más de lo que señala el VaR, en relación con el retorno esperado.

La forma de medición de este concepto puede variar, y de hecho varía. Además de que el VaR puede referirse a un día o a una semana, o tener distintos intervalos de confianza, la forma en la que se calcula estadísticamente este dato varía.