

**UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA, MANAGUA**

**RECINTO UNIVERSITARIO CARLOS FONSECA AMADOR**

**FACULTAD DE CIENCIAS ECONÓMICAS**

**DEPARTAMENTO DE CONTADURÍA PÚBLICA Y FINANZAS**



**SEMINARIO DE GRADUACIÓN PARA OPTAR AL TÍTULO DE LICENCIADO EN  
BANCA Y FINANZAS.**

**TEMA:**

**ADMINISTRACIÓN DE RIESGO Y TEORÍA DE LA CARTERA**

**SUB TEMA:**

**TEMA: IMPORTANCIA DE UNA EFICIENTE GESTIÓN DE RIESGO OPERACIONAL  
EN EL BANCO DE FINANZAS S, A (BDF) NICARAGUA PARA EL AÑO 2015.**

**AUTORES.**

**BR. ALICIA DEL ROSARIO ROQUE ORTIZ.**

**BR. YASAIRA MERCEDES RAUDEZ RAMOS.**

**TUTORA:**

**Lic: JENNYFER ZELAYA MELENDEZ**

**2016**

## **Dedicatoria**

Primeramente a Dios por haberme permitido llegar hasta este punto, por darme la salud, ser el manantial de vida y proveerme de todo lo necesario para seguir adelante día a día; por darme la fuerza necesaria para lograr los objetivos propuestos, además de su infinita bondad, misericordia y amor.

A mis padres Juan Francisco Raudez Mendoza y Johana del Socorro Ramos Álvarez por haberme apoyado en todo momento, por sus consejos, sus valores, la motivación constante que me ha permitido ser una personas de bien, pero más que a nadie a mi madre, por su amor, por sus ejemplos de perseverancia y constancia de lucha, por ser el pilar fundamental en mi vida. Por todos esos valores que la caracterizan y que me ha transmitido siempre para salir adelante.

A nuestra maestra por su gran apoyo y motivación para la culminación de este proyecto de investigación, por su apoyo ofrecido en este trabajo, por habernos transmitidos los conocimientos obtenidos y habernos llevado pasó a paso en el aprendizaje.

Yasaira Raudez Ramos

## **Dedicatoria**

Quiero dedicar este trabajo a mi padre celestial, Dios que me ha dado la vida, la fortaleza y sabiduría necesaria, para terminar este proyecto de investigación.

A mis maestros, gracias por su tiempo, por su apoyo que me brindaron en el desarrollo de mi formación profesional, por guiarme en la elaboración de este trabajo y llegar a la culminación del mismo.

A mi padre José Ignacio Roque Martínez, que está en el cielo gracias por tu buena voluntad, en especial a mi madrecita Rosario Ortiz Salgado, a quien le debo toda mi vida, quien me fortaleció con buenos sentimientos, con su amor incondicional, hábitos y valores para salir adelante, gracias por ser mi inspiración.

Alicia del Rosario Roque Ortiz

## **Agradecimiento**

Principalmente al dador de vida, Dios todo poderoso, por su infinita misericordia y amor que nos muestra día con día, Por la sabiduría y entendimiento que me ha brindado para llegar hasta el día de hoy.

A mis padres Johana del Socorro Ramos Álvarez y Juan Francisco Raudez Mendoza, quienes a lo largo de toda la vida me han apoyado y motivado en mi formación académica, creyeron en mí en todo momento y no dudaron de mis capacidades. A mi esposo Avid Yonat Gutiérrez González por brindarme su apoyo incondicional en estos últimos años de formación académica.

A nuestros profesores a quienes les debemos gran parte de nuestros conocimientos, gracias a su paciencia y enseñanza, finalmente un eterno agradecimiento.

A esta prestigiosa universidad la cual abre sus puertas a jóvenes como nosotros, preparándonos para un futuro competitivo y formándonos como profesionales con sentido de seriedad, responsabilidad y rigor académico.

Yasaira Raudez Ramos.

## **Agradecimiento**

Primeramente a Dios, por estar con migo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente, y por haber puesto en mi camino a todas aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mis maestros gracias por su enseñanza, por la paciencia con que muchas veces me enseñaron a prepararme en este mundo de competencias.

A mis hnos. Ernesto, Frank y Johnny Roque, a mi hermanita Jeysell Altamirano gracias por su apoyo, alegría, por motivarme y darme las fuerzas necesaria para seguir adelante.

A esta prestigiosa universidad por darme la oportunidad de prepararme profesionalmente a los profesores, gracias por su colaboración, por la paciencia, apoyo y sobre todo el tiempo que dispusieron para con esta investigación.

A una amiga en especial Yadira Méndez Gutiérrez, que ha sido un pilar fuerte de apoyo y motivación en mis proyectos.

Alicia del Rosario Roque Ortiz

## Carta Aval del Tutor

Managua, 24 de Mayo del 2017

**MSc. Álvaro Guido Quiroz**

Director del Departamento de Contaduría Pública y Finanzas

Facultad de Ciencias Económicas

UNAN-Managua

Su despacho

Estimado Maestro Guido:

Por medio de la presente, remito a Usted los juegos resumen final de Seminario de Graduación correspondiente al II Semestre 2016, con tema general *“Administración de Riesgo y Teoría de cartera”* y subtema *«IMPORTANCIA DE UNA EFICIENTE GESTION DE RIESGO OPERACIONAL EN EL BANCO DE FINANZAS S,A (BDF) NICARAGUA PARA EL AÑO 2015»* presentado por los bachilleres **Yasaira Mercedes Raudez Ramos** con número de carné **11204908** y **Alicia del Rosario Roque Ortiz** con número de carné **11207724**, para optar al título de Licenciados en Banca y Finanzas.

Este trabajo reúne los requisitos establecidos para resumen final de Seminario de Graduación que especifica el Reglamento de la UNAN-Managua.

Esperando la fecha de defensa final, me suscribo deseándole éxito en sus labores cotidianas

Cordialmente,

**Lic. Jennyfer Patricia Zelaya Meléndez**

Docente del Departamento de Contaduría Pública y Finanzas

Tutor de Seminario de Graduación

UNAN-Managua

Cc.: Archivo

## **Resumen**

El presente trabajo investigativo tiene como objetivo demostrar la importancia que tiene una eficiente gestión de riesgo operativo en las entidades bancarias, con el propósito de hacerlo un procedimiento de continuidad dentro del banco e instituciones financieras y no meramente un concepto que se maneja a niveles de gobierno corporativo, sino que todos los miembros de la institución aporten y cumplan los controles operacionales establecidos. Su aplicación en las medidas y cuantificación de pérdidas por el tipo de riesgo operativo son un tema del que las instituciones no pueden obviar actualmente.

Este trabajo se elaboró mediante la elaboración de consultas y entrevistas a personal del Banco de Finanzas, S.A durante el periodo 2015 con el fin de conocer las políticas, normas y procedimientos para la medición del riesgo operativo y de esta manera realizar una evaluación del mismo y poder determinar las estrategias de contingencia ante este tipo de riesgo. Mediante el caso práctico se muestran los resultados obtenidos a partir de una supervisión in situ cabe destacar que los datos presentados son meramente para fines de ejemplo y para el cumplimiento de la explicación metodológica.

En conclusión para la institución financiera Banco de Finanzas, S.A, con certeza cumple con los procedimientos, políticas y seguimiento de mitigación de riesgo operativo. Se ha podido observar en el caso práctico que es posible la medición y cuantificación así como las estrategias del comité para su valoración y elaboración de políticas de Riesgo Operativo.

## Índice

Dedicatoria.....	
Dedicatoria.....	
Agradecimiento.....	
Agradecimiento.....	
Carta Aval del Tutor .....	
Resumen.....	
Índice.....	
I. Introducción.....	1
II. Justificación .....	4
III. Objetivos.....	5
3.1 Objetivo general .....	5
3.2 Objetivos específicos.....	5
IV. Desarrollo del subtema. ....	6
4.1 Generalidades de la administración de riesgo.....	6
Concepto de administración de riesgo.....	6
4.1.1 Principios básicos de administración de riesgo. ....	7
4.1.2 Entes reguladores del riesgo bancario en Nicaragua. ....	14
4.2 Tipos de riesgos bancarios .....	15
Concepto de riesgo bancario.....	15
4.2.1 Clasificación de los tipos de riesgo.....	15
4.2.1.1 Riego crediticio. ....	15
4.2.1.2 Riesgo de negocio. ....	16
4.2.1.3 Riesgo de liquidez .....	16
4.2.1.4 Riesgo cambiario.....	17
4.2.1.5 Riesgo de tasa de interés. ....	17

4.2.1.6	Riesgo de mercado. ....	17
4.2.1.7	Riesgo operativo.....	18
4.2.1.8	Riesgo Legal.....	19
4.2.1.9	Riesgo de tecnología. ....	19
4.2.1.10	Riesgo de reputación. ....	20
4.2.1.11	Riesgo de insolvencia. ....	20
4.3	Riesgo Operativo.....	21
	Definición de riesgo operativo. ....	21
4.3.1	Factores de riesgo operativo. ....	22
4.3.1.1	Procesos Internos.....	23
4.3.1.2	Personas.....	25
4.3.1.3	Eventos Externos.....	26
4.3.1.4	Tecnología De Información .....	26
4.3.2	Principios básicos de administración de riesgos operativos. ....	26
4.3.2.1	Principios básicos:.....	27
4.3.2.2	Administración de Riesgos: identificación, evaluación, monitoreo y mitigación /control. 28	
4.3.2.3	La función de los supervisores .....	30
4.3.2.4	La función de divulgación de información. ....	31
4.3.2.5	Otros puntos clave:.....	31
4.3.3	Métodos de medición, control y mitigación de riesgo operativo.....	31
4.3.3.1	Evaluación.....	31
4.3.3.2	Mediciones del Riesgo Operativo .....	32
4.3.3.3	Método del Indicador Básico .....	32
4.3.3.4	Método Estándar. ....	33
4.3.3.5	Metodo estandar alternativo. ....	38
4.3.3.6	Métodos de medición avanzada (AMA). ....	39
V.	Caso Práctico. ....	46
5.1	Perfil de la empresa. ....	46
5.1.1	Historia de la empresa.....	46
5.1.2	Visión.....	47
5.1.3	Objetivos estratégicos.....	47

5.1.4	Valores .....	49
5.1.5	Organización.....	49
5.2	Sistemas de identificación de riesgos y cuantificación de pérdidas.....	51
5.2.1	Identificación y evaluación de riesgos operativos: .....	54
5.2.2	Planes de Mitigación de Riesgos Principales.....	55
5.2.3	Registro de Incidentes.....	56
5.3	Estrategia Tecnológica .....	57
5.3.1	Canales de servicio alternos y Bancarización:.....	58
5.3.2	Estrategia de Tercerización.....	59
5.4	Continuidad de negocios y planes de contingencia.....	60
5.5	Seguridad de la Información .....	62
5.5.1	Documentación física: (Contratos, pagarés, certificados en garantías, pólizas, etc.) 65	
5.5.2	Auditoría Interna.....	66
5.5.2.1	Auditoría de Sistemas: .....	68
5.5.2.2	Auditorías de aplicaciones. ....	68
5.5.2.3	Auditorías de Procesos de TI. ....	69
VI.	Conclusión.....	71
VII.	Bibliografía.....	74
VIII.	Anexos .....	75

## **I. Introducción**

En los últimos años la banca nacional ha presentado un constante crecimiento a pesar de la profunda crisis del 2000 la cual se caracterizó por el cierre de varias entidades bancarias, fusiones y traslado de activos y pasivos de los bancos clausurados a los bancos más sólidos del país. Es con respectas suscitaciones que el circulo de la banca internacional, entes reguladores y otros organizaciones ha surgido la naciente preocupación por el riesgo operacional, mismo que ha estado presente desde los inicios del negocios de la banca, sin embargo en la actualidad este tiene más impacto a causa de la complejidad de la banca actual, la globalización y sistemas tecnológicos. Los fraudes y desfalco a este tipo de negocios son causados por una mala e ineficiente gestion de riesgo operacional, fallas en los sistemas, segregación de las funciones controles inadecuados o incluso la ausencia de estos, prácticas irregulares con los clientes es lo que provoca pérdidas a las instituciones bancarias

El presente trabajo de investigación pretende dar a conocer la importancia de una eficiente gestion del riesgo operativo en el Banco de Finanzas S, A (BDF) Nicaragua en el periodo 2015, para ello se debe determinar y entender los factores que implica el riesgo operacional en la administración de los riesgos que definen algunas circunstancias o eventos que pueden suscitarse en la institución y reducir o limitar el rendimiento y liquidez de los valores objeto de la oferta pública

Es de vital importancia establecer una política de seguridad en los parámetros que definan la tolerancia al riesgo del banco, para que se pueda limitar el riesgo de ataques internos

y externos en la banca, así como el riesgos reputación producida por rupturas de seguridad. Y también se lograra garantizar el cumplimiento de las medidas de seguridad y establecer procedimientos que evalúen la ejecución de la política, las medidas disciplinarias y la comunicación de posibles violaciones en la seguridad.

En la elaboración de este estudio encontramos que los tipos de riesgo bancario a lo cual están expuestas las instituciones bancarias que deben tener una correcta identificación y gestión, pues es capaz de reconocer dificultades que existen en la práctica de la actividad bancaria para definir y valorar dicho riesgo en la debida administración y lograr el éxito en el banco. Estos varían en gran parte por su capacidad semejanzas en la gestión de riesgos con el sistema bancario. Para la Gestión de riesgos en Nicaragua: Los bancos deben sopesar, por un lado, beneficios y riesgos reportados por la banca y, por otro, ser capaces de gestionar, organizar y controlar los riesgos, así como absorber cualquier pérdida derivada si fuera necesario. Abordaremos más ampliamente estas semejanzas en el trabajo que a continuación desarrollamos.

Para la realización del presente trabajo se utilizó el método de investigación documental, cónsula biográfica, recopilando la información disponible en materia de riesgo operacional, publicaciones de las normas institucionales del riesgo operativo en Nicaragua, tanto internacional, como nacional; así mismo con el fin de conocer sobre los avances en la gestión del riesgo operacional en Nicaragua, se efectuó la entrevista al personal y colaboradores de la institucion bancaria centrada en el estudio de la gestión del riesgo operacional que se realiza en el banco de finanzas S,A (BDF) Nicaragua.

La realización de este seminario se ha realizado en cuatro acápite, los cuales se pueden resumir en investigación y búsqueda de información, análisis de la misma y redacción.

El en el cuarto acápite encontraremos el desarrollo del subtema el cual está dividido en tres subtemas en el primer acápite del subtema se ha consistido en buscar información sobre los aspectos generales del riesgo definición de este. La investigación se ha basado principalmente en buscar información electrónica, mediante buscadores de internet, recursos de la biblioteca de la Universidad Nacional Autónoma de Nicaragua, y a partir del registro y búsqueda en páginas especializadas. Esta fase se ha realizado en dos sub-fases, donde se encontraran los principales principios de riesgo y los entes que regulan las actividades bancarias del país. En el segundo acápite del subtema ha consistido en analizar la información obtenida en el subtema anterior y estructurarla y organizarla para identificar los tipos de riesgos bancarios. En el tercer acápite del subtema ha consistido en la determinación del tema principal que es el Riesgo Operativo. Podemos identificar tres sub-temas. En el primero de ellos ha estado focalizada en determinar los factores del Riesgo Operativo. En él los principios básicos de administracion de Riesgos Operacionales, El tercero encontramos los métodos de medición en la aplicación al Riesgo Operativo. En un quinto acápite encontraremos la presentación del caso práctico el cual está basado en la prestación de una auditoria in-situ al Banco de Finanzas S.A para el periodo 2015.

## II. Justificación

La gestión de riesgo es un tema de mucha importancia en toda institución bancaria, el elevado importe de las operaciones significa que cualquier exposición al riesgo puede tener consecuencias financieras negativas para el banco y su balance. Pero los errores o las fallas también pueden ocasionar graves daños de reputación en muchas instituciones, la noción del riesgo operacional no es muy conocida o no tiene gran significancia y son muy pocas las instituciones que cuentan con un plan de continuidad de las operaciones.

La importancia de una eficiente gestión de riesgo operacional en el banco BDF, así como un efectivo análisis y prevención de este tipo de riesgo son de mucho interés ya que vivimos en un mundo de cambios que exige que la instituciones bancarias sean eficientes al momento de tomar decisiones es por ello que se debe realizar una revisión en cuanto a la administración del riesgo operativo.

En consecuencia, la presente investigación es de gran relevancia, ya que los resultados permitirán tener una pauta bibliográfica, que contribuirán a la toma de decisiones apropiadas que deben tomar en cuenta las entidades bancarias para mejorar e implementar estrategias eficiente en la gestión del riesgo operacional, minimizando las pérdida de capital y el seguir los procedimientos de evaluación de este tipo de riesgo.

### **III. Objetivos**

#### **3.1 Objetivo general**

Exponer la importancia de una eficiente gestión de riesgo operativo en el banco de finanzas S, A (BDF) para el año 2015.

#### **3.2 Objetivos específicos**

- Conocer Aspectos Generales sobre administración de riesgo en las instituciones financieras.
- Identificar los tipos de riesgos a los que están expuestas las instituciones bancarias.
- Subrayar la importancia de la aplicación, medición y control del Riesgo Operativo.
- Presentar un caso práctico de un diagnóstico de riesgo operacional en el banco de finanzas S, A (BDF), para el año de 2015.

## **IV. Desarrollo del subtema.**

### **4.1 Generalidades de la administración de riesgo**

#### **4.1.1 Concepto de administración de riesgo.**

La administración de riesgo es el proceso por el cual la dirección de una empresa u organización combina los recursos financieros, humanos, materiales y técnicos de una entidad, para identificar o evaluar el amplio espectro de los riesgos potenciales a los cuales está expuesto (tanto sean de mercado como operacionales) de acuerdo al nivel de riesgo al cual están dispuestos a exponerse según sus objetivos estratégicos y decidir cómo manejarlos en una combinación optima de costo - efectividad.

La administración de riesgos se puede definir como el proceso de identificación, medida y administración de los riesgos que amenazan la existencia, los activos, las ganancias o al personal de una organización, o los servicios que ésta provee.

Según la Norma Sobre La Administración Integral De Riesgos Resolución No. Cd-Siboif-423-1-May30-2006. Publicada en La Gaceta No. 124 del 27 de Junio del 2006 Artículo 3. Inciso a) Define el la administración de riesgo como el “Conjunto de objetivos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, limitar, controlar, informar y revelar los distintos tipos de riesgos a que se encuentran expuestas las instituciones.”

#### **4.1.2 Principios básicos de administración de riesgo.**

Los Principios Básicos conforman un marco de normas mínimas para la adecuada supervisión que se considera de aplicación universal. El Comité redactó los Principios Básicos y su Metodología con el fin de contribuir al fortalecimiento del sistema financiero mundial. Cualquier deficiencia en el sistema financiero de un país, ya sea desarrollado o en desarrollo, puede poner en peligro la estabilidad financiera tanto dentro como fuera de sus fronteras. El Comité considera que la aplicación de los Principios Básicos por todos los países supondría un avance considerable para la mejora de la estabilidad financiera nacional e internacional, al tiempo que sentaría las bases para un mayor desarrollo de sistemas de supervisión eficaces.

- Principio 1 – Objetivos, independencia, potestades, transparencia y cooperación: todo sistema eficaz de supervisión bancaria debe contar con atribuciones y objetivos claros para cada autoridad que participe en la supervisión de los bancos. Cada una de ellas deberá contar con independencia operativa, procesos transparentes, un buen gobierno corporativo y recursos adecuados, y deberá hacerse responsable del desempeño de sus funciones. También ha de existir un marco jurídico apropiado para la supervisión bancaria, con normas relativas a la autorización de las instituciones bancarias y a su supervisión continua, potestades para asegurar el cumplimiento de la ley así como la seguridad y solidez, y protección legal para los supervisores. Debe haber mecanismos para el intercambio de información entre los supervisores que permitan preservar el carácter confidencial de la misma.

- Principio 2 – Actividades permitidas: deben definirse claramente las actividades que pueden desarrollar las entidades autorizadas a operar como bancos y sujetas a supervisión, y debe controlarse en la medida de lo posible el uso de la palabra “banco” como razón social.
  
- Principio 3 – Criterios para la concesión de licencias: la autoridad encargada de conceder las licencias debe tener potestad para fijar criterios y rechazar las solicitudes que no cumplan con las normas establecidas. Como mínimo, el proceso de autorización debe evaluar la estructura de propiedad y el buen gobierno del banco y del grupo al que pertenece, incluyendo la adecuación e idoneidad de sus consejeros y altos directivos, su plan estratégico y operativo, sus controles internos y gestión del riesgo, así como la evolución prevista de su situación financiera, incluida su base de capital. Cuando el propietario u organismo matriz del banco propuesto sea extranjero, deberá obtenerse el consentimiento previo del supervisor del país de origen.
  
- Principio 4 – Cambio de titularidad de participaciones significativas: el supervisor tiene potestad para examinar y rechazar propuestas para transferir participaciones significativas o de control, tanto si se poseen de modo directo como indirecto, en bancos existentes.
  
- Principio 5 – Adquisiciones sustanciales: el supervisor tiene potestad para analizar, basándose en criterios prescritos, las adquisiciones o inversiones sustanciales que realice un banco, incluida la realización de operaciones transfronterizas, para

confirmar que la estructura del grupo o de la empresa no expone al banco a riesgos innecesarios ni obstaculiza la supervisión eficaz.

- Principio 6 – Suficiencia de capital: el supervisor debe imponer a los bancos requerimientos mínimos de capital que reflejen los riesgos que éstos asumen y debe definir los componentes del capital teniendo en cuenta la capacidad de éstos para absorber pérdidas. Al menos en el caso de bancos con actividad internacional, estos requerimientos no pueden ser inferiores a los que establece el Acuerdo de Basilea aplicable.
  
- Principio 7 – Proceso para la gestión del riesgo: los supervisores deben tener constancia de que los bancos y grupos bancarios cuentan con un proceso integral de gestión de riesgos (que incluya la vigilancia por el Consejo y la alta dirección) para identificar, evaluar, vigilar y controlar o mitigar todos los riesgos sustanciales y para evaluar su suficiencia de capital global con respecto a su perfil de riesgo. Estos procesos han de ser proporcionales a las dimensiones y complejidad de la institución.
  
- Principio 8 – Riesgo de crédito: los supervisores deben tener constancia de que los bancos cuentan con un proceso para la gestión del riesgo de crédito que incorpore el perfil de riesgo de la institución, con políticas y procesos prudenciales para identificar, calcular, vigilar y controlar el riesgo de crédito (incluido el riesgo de contraparte). Esto

incluiría la concesión de préstamos y la realización de inversiones, la evaluación de la calidad de todos ellos y la gestión continua de las carteras crediticia y de inversión.

- Principio 9 – Activos dudosos, provisiones y reservas: los supervisores deben tener constancia de que los bancos establecen y cumplen políticas, prácticas y procedimientos adecuados para gestionar activos dudosos y para evaluar la suficiencia de sus provisiones y reservas.
  
- Principio 10 – Límites de exposición a grandes riesgos: los supervisores deben tener constancia de que el banco cuenta con políticas y procesos que permitan a la dirección identificar y gestionar las concentraciones en el seno de la cartera, y también deben fijar límites prudenciales que restrinjan las posiciones del banco frente a una misma contraparte o grupo de contrapartes vinculadas.
  
- Principio 11 – Posiciones con partes vinculadas: a fin de evitar abusos al mantener posiciones (tanto dentro como fuera de balance) con partes vinculadas y para resolver cualquier conflicto de intereses, los supervisores deben establecer requisitos para que aquellos bancos que mantienen posiciones con personas físicas o jurídicas vinculadas lo hagan con total imparcialidad, que dichas posiciones puedan ser controladas eficazmente, que se adopten medidas para controlar o mitigar riesgos, y que el reconocimiento contable de pérdidas en dichas posiciones se realice con políticas y procesos estándar.

- Principio 12 – Riesgo país y riesgo de transferencia: los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos adecuados para identificar, cuantificar, vigilar y controlar el riesgo país y el riesgo de transferencia en sus préstamos e inversiones internacionales, y para mantener un nivel de reservas adecuado para dichos riesgos.
  
- Principio 13 – Riesgos de mercado: los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos para identificar, cuantificar, vigilar y controlar con precisión los riesgos de mercado; los supervisores deben tener potestad para imponer límites y/o exigencias de capital específicos para las exposiciones al riesgo de mercado, cuando esté justificado.
  
- Principio 14 – Riesgo de liquidez: los supervisores deben tener constancia de que los bancos cuentan con una estrategia para gestionar el riesgo de liquidez que incorpora el perfil de crédito de la institución, con políticas y procesos prudenciales para identificar, cuantificar, vigilar y controlar el riesgo de liquidez y para poder gestionar diariamente la liquidez. Los supervisores exigen que los bancos cuenten con planes de contingencia para afrontar problemas de liquidez.
  
- Principio 15 – Riesgo operacional: los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y controlar/mitigar el riesgo operacional. Estas políticas y procesos han de ser proporcionales a las dimensiones y complejidad del banco en cuestión.

- Principio 16 – Riesgo de tipos de interés en la cartera de inversión: los supervisores han de tener constancia de que el banco cuenta con sistemas eficaces para identificar, cuantificar, vigilar y controlar el riesgo de tipos de interés en la cartera bancaria, incluyendo una estrategia bien definida aprobada por el Consejo y puesta en práctica por la alta dirección, proporcional al tamaño y complejidad de dicho riesgo.
  
- Principio 17: Control y auditoría internos: los supervisores deben tener constancia de que los bancos cuentan con controles internos acordes al tamaño y complejidad de su actividad. Dichos controles deben incluir normas claras sobre delegación de autoridad y responsabilidades; segregación de las funciones que implican el compromiso del banco, el desembolso de sus fondos y la contabilidad de sus activos y pasivos; conciliación de estos procesos; protección de los activos del banco; y funciones independientes de auditoría interna y de cumplimiento para comprobar la observancia de estos controles, así como de la legislación y regulación aplicables.
  
- Principios 18: Utilización abusiva de servicios financieros: los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos adecuados, incluyendo normas estrictas sobre el conocimiento de la clientela (“know-your-customer” o KYC), que promuevan normas éticas y profesionales de alto nivel en el sector financiero e impidan que el banco sea utilizado, intencionalmente o no, con fines delictivos.
  
- Principio 19 – Enfoque supervisor: un sistema eficaz de supervisión bancaria exige que el supervisor desarrolle y mantenga un profundo conocimiento sobre las

operaciones de los bancos por separado y de los grupos bancarios, así como del sistema bancario en su conjunto, centrándose en la seguridad y solidez y en la estabilidad del sistema bancario.

➤ Principio 20 – Técnicas de supervisión: un sistema eficaz de supervisión bancaria debe incluir tanto supervisión in situ como a distancia, además de contactos periódicos con la gerencia del banco.

➤ Principio 21 – Informes de supervisión: los supervisores deben contar con los medios necesarios para obtener, revisar y analizar los informes prudenciales y estadísticos de los bancos, tanto a título individual como en base consolidada, con el fin de verificarlos independientemente, ya sea a través de inspecciones in situ o con la ayuda de expertos externos.

➤ Principio 22 – Contabilidad y divulgación: los supervisores deben tener constancia de que cada banco mantiene registros adecuados conforme a las políticas y prácticas contables ampliamente aceptadas internacionalmente y que publica con regularidad información que refleja razonablemente su situación financiera y su rentabilidad.

➤ Principio 23 – Potestades correctivas del supervisor: los supervisores deben contar con una gama adecuada de herramientas de supervisión que les permita aplicar

medidas correctivas oportunas. Esto incluye la capacidad de revocar, cuando sea necesario, licencias bancarias o recomendar su revocación.

- Principio 24 – Supervisión consolidada: para la supervisión bancaria resulta esencial que los supervisores lleven a cabo su labor en base consolidada para todo el grupo bancario, realizando un adecuado seguimiento y, cuando corresponda, aplicando normas prudenciales a todos los aspectos de las actividades que el grupo realiza a escala mundial.
  
- Principio 25 – Relación entre el supervisor de origen y el de destino: la supervisión transfronteriza consolidada exige la cooperación y el intercambio de información entre los supervisores del país de origen y aquellos otros con competencias dentro del grupo bancario, en especial las autoridades de supervisión del país de acogida. Los supervisores bancarios deben exigir que las operaciones locales de bancos extranjeros se lleven a cabo en virtud de las mismas normas que se aplican a las entidades locales.

#### **4.1.3 Entes reguladores del riesgo bancario en Nicaragua.**

La administración de riesgo y el riesgo operativo del sistema bancario está regulado por las Normas sobre la administración integral de riesgo, Ley General de Bancos Ley General de Bancos, Instituciones Financieras no Bancarias y Grupos Financieros (Ley 561) en conjunto con otras leyes importantes, sobresaliendo la Ley Creadora de la Superintendencia de Bancos y Otras Instituciones Financieras (Ley 316) y la Ley Orgánica del Banco Central de Nicaragua.

Asimismo, y en virtud de dichas leyes, el sistema está supervisado por la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF)

## **4.2 Tipos de riesgos bancarios**

### **Concepto de riesgo bancario.**

Lo riesgos bancarios deben tener una correcta identificación y gestión para que exista un éxito en el negocio bancario, pues es capaz de reconocer dificultades que existan en la práctica de la actividad bancaria para definir, valorar y gestionar dichos riesgos; en la debida administración del riesgo es donde está la clave del éxito.

### **4.1.4 Clasificación de los tipos de riesgo**

#### ***4.2.1.1 Riego crediticio.***

Éste se refiere a la posibilidad de tener grandes pérdidas por el motivo de que un cliente no cumpla con las obligaciones de crédito a las cuales se comprometió. El riesgo de crédito surge cuando las contra partes están indispuestas o son totalmente incapaces de cumplir sus obligaciones contractuales. El riesgo de crédito abarca tanto el riesgo de incumplimiento, que es la valuación objetiva de la probabilidad de que una contra parte incumpla, como el riesgo de mercado que mide la pérdida financiera que será experimentada si el cliente incumple.

#### ***4.2.1.2 Riesgo de negocio.***

Es la amenaza de que un hecho o acción afecte negativamente a la capacidad de la empresa de lograr sus objetivos de negocio y de maximizar su valor para sus grupos de interés. El riesgo de negocio implica tanto la posibilidad de que no se realicen oportunidades de negocio, como que se produzcan errores o se materialicen las amenazas. Es la posibilidad de quebrantos que se derivan de las pérdidas de la posición de mercado, la posición de negocio frente a los mercados en los que se operan. En cualquier negocio, si se pierden ventas y los costes se mantienen iguales, es casi inevitable caer en pérdidas. Lo mismo ocurre en la banca, si se vive sólo de la cartera generada, y se pierde demanda de crédito, probablemente habrá una pérdida en los ingresos que puede llegar en algunos casos a poner en peligro la continuidad de la entidad.

#### ***4.2.1.3 Riesgo de liquidez***

Es la Posibilidad de que una sociedad no sea capaz de atender a sus compromisos de pago a corto plazo. Las entidades financieras deben resolver diariamente la estimación de la cantidad de dinero que deben mantener en efectivo para atender todas sus obligaciones a tiempo. Entre estas obligaciones se pueden citar la recuperación de la cartera de sus proveedores de fondos, ya sea al final del término de un depósito a plazo, o cuando el cliente de cuenta de ahorro o corriente los requiera.

El Riesgo de liquidez se produce cuando una entidad a corto plazo no tiene liquidez suficiente para atender este tipo de pagos. Éste se refiere a la posibilidad de que se produzcan

pérdidas excesivas por causa de las decisiones tomadas en pro de disponer de recursos rápidamente para poder cumplir con los compromisos presentes y futuros.

#### ***4.2.1.4 Riesgo cambiario.***

Éste se refiere a la posibilidad de pérdidas por las variaciones en las tasas de cambio de las diferentes monedas con las cuales una institución financiera realiza operaciones o tiene recursos invertidos. El riesgo de cambio o riesgo cambiario es el fenómeno que implica el que un agente económico coloque parte de sus activos en una moneda, o instrumento financiero denominado en moneda diferente de la cual utiliza este agente como base para sus operaciones cotidianas.

#### ***4.2.1.5 Riesgo de tasa de interés.***

Éste se refiere a la disminución del valor de los activos o del patrimonio de una entidad debido a las variaciones en las tasas de interés, lo cual puede conducir a que la institución tenga graves pérdidas. Es la que resulta del impacto de movimientos en los precios o tipos de los activos (tipo de interés, tipo de cambio, cotizaciones bursátiles) sobre la cartera de inversión y de negocio de un banco. Este riesgo provoca un impacto en la misma dirección para todas las identidades, que se verán afectadas de manera distinta según el tamaño de su posición y según estén en posiciones cortas o largas respecto al activo y cuyo precio ha variado.

#### ***4.2.1.6 Riesgo de mercado.***

Ante una posición tomada en una serie de activos a un tipo de interés fijo o una determinada moneda pues cambia el tipo de cambio o del tipo de interés. “Es el que resulta del impacto de movimiento en los precios o tipos de activos (tipo de cambio o cotizaciones

bursátiles) sobre la cartera de inversiones y negocio de un banco. Además es la posibilidad de que los precios globales de las acciones o de los bonos declinen por períodos cortos o extendidos.

Los mercados de acciones y bonos tienden a moverse en ciclos, con períodos de subida de precios y de períodos de caída.

También conocido como riesgo sistemático, está asociado con la volatilidad del mercado tomado en forma general, envuelve en cierto grado las inversiones en acciones, bonos o fondos mutuales. Casi todas las acciones que poseas sufrirán pérdidas si el mercado se desploma. Los ciclos económicos, condiciones políticas y las tendencias del mercado son factores que afectan el movimiento del mercado acentuando el riesgo.

#### ***4.2.1.7 Riesgo operativo.***

El riesgo operativo resulta de “peligros escondidos” que pueden causar pérdidas debido a fallas en los procesos, en la tecnología, en la actuación de la gente, y también, debido a la ocurrencia de eventos externos. Las entidades financieras y las empresas del sector real están en una etapa de cambios que ha incrementado el riesgo operativo. Reestructuraciones internas, fusiones y adquisiciones, cambios en los sistemas tecnológicos y la complejidad en las transacciones, crean mayores exposiciones al riesgo operativo.

La forma en que se manejen estos riesgos está bajo creciente escrutinio tanto por los accionistas, como por los reguladores y por el mercado en general, que buscan por igual, mayor certidumbre en los resultados.

#### ***4.2.1.8 Riesgo Legal.***

Tradicionalmente se definía riesgo legal como “todo aquello que no se encuadra dentro del riesgo de crédito ni de mercado”. A partir del Nuevo Acuerdo de Capital surge una nueva definición más clara y precisa en relación con el riesgo operacional que queda definido como “... el riesgo de que deficiencias en los sistemas de información o controles internos produzcan pérdidas inesperadas. El riesgo operacional está asociado a errores humanos, a fallas en los sistemas y a la existencia de procedimientos y controles inadecuados”.

En el marco legal nicaragüense se define riesgo legal como: Pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la afectación por resoluciones administrativas o judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las instituciones llevan a cabo.

#### ***4.2.1.9 Riesgo de tecnología.***

Es uno de los componentes principales del Riesgo, definido como el “Riesgo de pérdidas debido a fallas o a inadecuados procesos, personal y sistemas internos o bien a causa de acontecimientos externos”. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación” El riesgo tecnológico 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.

#### **4.2.1.10 Riesgo de reputación.**

Es el daño que para el banco resulta de una publicidad negativa en relación con sus prácticas de negocio, sean ciertas o no y que pueden afectar a su base de clientes, a sus costos de litigación o a sus ingresos. En muchos casos, se trata de un riesgo que resulta de algunos de los riesgos anteriores.

Las entidades financieras creen que los riesgos derivados de la reputación son la principal amenaza a la que se enfrenta su valor de mercado, aunque el riesgo de crédito sigue siendo la mayor preocupación en relación con los beneficios; así lo desvela una encuesta a directivos elaborada por la consultora Price waterhouse Coopers, según la cual los riesgos cuantificables siguen acaparando "demasiada atención" en perjuicio de cuestiones como el gobierno corporativo.

#### **4.2.1.11 Riesgo de insolvencia.**

Se conoce también como riesgo de quiebra. Es un resultante conjunto de los anteriores riesgos. Es la probabilidad de la no posibilidad de la empresa de hacer frente a sus deudas y obligaciones al no tener la cantidad de efectivo necesaria en el momento del vencimiento de estas.

También podemos clasificar los tipos de riesgo de acuerdo con La norma sobre administración integral de riesgo, Resolución No CD-SIBOIF - 423- 2MAY30-2006, Publicada en la gaceta No 124 DEL 27 DE JUNIO DEL 2006, en su artículo 3 clasifica a los riesgos de la siguiente manera:

- **Riesgo de Crédito:** Pérdida potencial por la falta de pago de un deudor o contraparte en las operaciones que efectúan las instituciones.

- **Riesgo de Liquidez:** Pérdida potencial por la imposibilidad de renovar pasivos o de contratar otros en condiciones normales para la institución; por la venta anticipada o forzosa de activos a descuentos inusuales para hacer frente a sus obligaciones, o bien, por el hecho de que una posición no pueda ser oportunamente enajenada, adquirida o cubierta mediante el establecimiento de una posición contraria equivalente.
- **Riesgo de Mercado:** Pérdida potencial por cambios en los factores de riesgo que inciden sobre la valuación de las posiciones por operaciones activas, pasivas o causantes de pasivo contingente, tales como tasas de interés, tipo de cambio, índices de precio, entre otros.
- **Riesgo Operacional:** El riesgo de pérdida debido a la inadecuación o fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos y comprende, entre otros, los siguientes:
  - **El Riesgo Tecnológico:** Pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios financieros a los clientes de la institución.
  - **El Riesgo Legal:** Pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la afectación por resoluciones administrativas o judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las instituciones llevan a cabo.

### 4.3 Riesgo Operativo

#### **Definición de riesgo operativo.**

Existen diversas definiciones que se han dado al concepto de riesgo operativo.

El hecho de dar una definición es vital, porque supone un gran avance hacia el consenso y la homogeneización de términos. Basilea II ha venido a aportar, en este sentido, un punto de partida básico y un marco de referencia a la hora de tratar este riesgo. A continuación se menciona la emitida por el Comité de Basilea II, la cual señala que:

El riesgo operativo resulta de la posibilidad para la compañía de incurrir en pérdidas por deficiencias o fallas en recurso humano, procesos, tecnología, infraestructura y ocurrencia de eventos externos.

Por lo que se acaba de exponer, se infiere que el riesgo operativo puede definirse como:

“El riesgo de pérdida como resultado de fallas o sistemas inadecuados en los procesos internos, personas, eventos externos.”

#### **4.1.5 Factores de riesgo operativo.**

Según la Superintendencia de Bancos y Otras Instituciones Financieras (Resolución N° CD-SIBOIF-611-1-ENE22-2010 De fecha 22 de enero de 2010 NORMA SOBRE GESTION DE RIESGO OPERACIONAL) los factores de riesgos operacional “Se refiere a las fuentes generadoras de eventos en las que se originan las pérdidas por riesgo operacional a nivel de la actividad o líneas de negocios, entre los cuales se encuentran: procesos internos, personas, eventos externos y tecnología de información.”

Los factores de riesgo operacional a los que mayormente se ven expuestas las instituciones financieras son los siguientes:

- **Procesos internos;**
- **Personas**
- **Eventos externos; y**

➤ **Tecnología de información.**

Es determinante para un efectivo control de dichos factores, que las instituciones financieras cuenten con una definición apropiada de cada uno de estos, para lo cual deberán observar los criterios que se desarrollan en los capítulos que conforman el presente Título.

***4.3.1.1 Procesos Internos***

*4.3.1.1.1 Gestión de riesgos asociados a procesos internos.*

Las instituciones financieras deberán gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, de tal forma que se minimice la posibilidad de pérdidas relacionadas al diseño inapropiado de los procesos, o a 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 procesos y/o 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 costos planeados.

#### 4.3.1.1.2 *Desarrollo de políticas.*

Las instituciones financieras deberán contar con políticas escritas relativas al diseño, control, actualización y seguimiento de los procesos. Dichas políticas se referirán, al menos, a los aspectos siguientes:

- Diseño de los procesos, los cuales deben ser adaptables y dinámicos;
- Descripción en secuencia lógica y ordenada de las actividades, tareas, y controles;
- Identificación de las personas responsables de ejecutar los procesos para su correcto funcionamiento, a través de establecer medidas y fijar objetivos, garantizando que las metas globales del proceso se cumplan; definir los límites y alcance; mantener contacto con los clientes internos y externos del proceso para asegurar que se satisfagan y conozcan sus expectativas, entre otros;
- Difusión y comunicación de los procesos; y
- Actualización y mejora continua a través del seguimiento permanente en su aplicación.

#### 4.3.1.1.3 *Segregación de funciones.*

Las instituciones financieras deberán tener una adecuada segregación de funciones que eviten incompatibilidades, entendidas éstas como aquellas tareas cuya combinación en las competencias de una sola persona, eventualmente, podría permitir la realización o el ocultamiento de fraudes, errores, omisiones u otros eventos de riesgo operacional.

#### 4.3.1.1.4 *Inventarios.*

Las instituciones financieras deberán mantener inventarios actualizados de los procesos en funcionamiento, los cuales contarán, como mínimo, con la información siguiente: tipo de

proceso, nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, así como, deberá indicar si se trata de un proceso crítico.

#### **4.3.1.2 Personas**

##### *4.3.1.2.1 Gestión de riesgos asociados a personas.*

Las instituciones financieras deberán gestionar apropiadamente los riesgos asociados a las personas de la institución, de tal modo que se minimice la posibilidad de pérdidas asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Las instituciones deberán evaluar su organización con el objeto de determinar si se han definido las necesidades de recursos humanos con las competencias idóneas para el desempeño de cada puesto, considerando no sólo la experiencia profesional y la formación académica, sino también los valores, actitudes y habilidades personales que puedan servir como criterio para garantizar la excelencia institucional.

Asimismo, las instituciones deberán mantener información actualizada de los recursos humanos, que permita una adecuada toma de decisiones por parte de los niveles directivos y la realización de análisis cualitativos y cuantitativos de acuerdo con sus necesidades. Dicha información deberá referirse al personal existente en la institución; a la formación académica y experiencia; a la forma y fechas de selección, reclutamiento y contratación; a información histórica sobre los eventos de capacitación en los que han participado; a los cargos que han desempeñado en la entidad; a los resultados de evaluaciones realizadas; a las fechas y causas de

separación del personal que se ha desvinculado; y, a cualquier otra información que se considere pertinente.

#### ***4.3.1.3 Eventos Externos***

##### *4.3.1.3.1 Gestión de riesgos asociados a eventos externos.*

Las instituciones financieras deberán tomar en cuenta en la gestión del riesgo operacional la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la institución que pudiesen alterar el desarrollo de sus actividades, afectando los aspectos que dan origen al riesgo operacional referidos en los artículos precedentes. En tal sentido, entre otros eventos, se podrán tomar en consideración los siguientes:

- Las contingencias legales;
- Las fallas en los servicios públicos;
- La ocurrencia de desastres naturales, atentados y actos delictivos; y
- Las fallas en servicios críticos provistos por terceros.

#### ***4.3.1.4 Tecnología De Información***

##### *4.3.1.4.1 Gestión de riesgos asociados a tecnología de información.*

Las instituciones financieras deberán gestionar los riesgos asociados a TI, cumpliendo los requerimientos establecidos en la presente norma, en la normativa que regula la materia sobre administración integral de riesgos y en la normativa sobre gestión de riesgo tecnológico.

#### **4.1.6 Principios básicos de administración de riesgos operativos.**

El comité de Supervisión Bancaria de Basilea emitió un documento denominado “Prácticas sanas para Administración y Supervisión del Riesgo Operativo”, en Febrero del año 2003, en el cual ha emitido una serie de principios, de manera que las instituciones financieras

los consulten y realicen una gestión y supervisión eficaz del Riesgo Operativo, de modo que los bancos y autoridades supervisoras puedan utilizarlos al evaluar las políticas y prácticas destinadas a gestionar este tipo de riesgos.

El Comité de Basilea de Supervisión de Bancos reconoce que el enfoque exacto para la administración del riesgo operativo escogido por un banco individual dependerá de una serie de factores, incluyendo el tamaño, nivel de sofisticación, y la índole y complejidad de las actividades del banco.

#### ***4.3.1.5 Principios básicos:***

**Principio 1:** El directorio (consejo de administración) debería estar consciente de los principales aspectos de los riesgos operativos del banco como una categoría diferente de riesgo a ser administrado, y debería aprobar y revisar periódicamente el marco de administración del riesgo operativo del banco.

El marco debería proporcionar una definición a lo largo de la empresa del riesgo operativo y especificar los principios para la identificación, evaluación, monitoreo y control / mitigación del riesgo operativo.

**Principio 2:** El consejo de administración debería asegurar que el marco de Administración del riesgo operativo del banco sea sujeto a una auditoría interna efectiva e integral por personal competente, independiente desde el punto de vista operativo y con una adecuada capacitación. La función de auditoría interna no debería tener la responsabilidad directa por la administración del riesgo operativo.

**Principio 3:** Alta gerencia (consejo de administración) La gerencia debe traducir el marco de administración del riesgo operativo fijado por el directorio en políticas, procesos y procedimientos específicos que se pueden implementar y verificar en las diferentes unidades de

negocio. Mientras que cada nivel de la administración, es responsable por la conformidad y efectividad de las políticas, procesos, procedimientos y controles dentro de su ámbito de trabajo, la alta gerencia debe asignar la autoridad, responsabilidades y relaciones de presentación de informes para promover y mantener el sistema, y asegurar que se estén los recursos necesarios para administrar con efectividad el riesgo operativo.

La alta gerencia debe asegurar que las actividades del banco sean llevadas a cabo por personal calificado con la experiencia y capacidad técnica requerida y con acceso a recursos, y que el personal responsable por el monitoreo e imposición de la política de riesgo de la institución tenga autoridad independiente de las unidades bajo su supervisión.

La gerencia debe asegurar que la política de administración del riesgo operativo del banco se haya comunicado claramente al personal en todos los niveles en las unidades expuestas a Riesgos operativos importantes

#### ***4.3.1.6 Administración de Riesgos: identificación, evaluación, monitoreo y mitigación /control.***

**Principio 4:** Los bancos deberían identificar y evaluar el riesgo operativo inherente en todos los productos, actividades, procesos y sistemas importantes. Los bancos también deberían asegurar que, antes de introducir o emprender productos, actividades, procesos y sistemas nuevos, el riesgo operativo inherente en los mismos sea sujeto a procedimientos adecuados de evaluación.

La identificación de riesgos es esencial para el desarrollo posterior de un sistema viable de monitoreo y control del riesgo operativo. Una efectiva identificación de riesgos toma en cuenta tanto factores internos (como ser la estructura del banco, la índole de las actividades del banco, la calidad de los recursos humanos del banco, cambios organizativos y rotación del

personal) como factores externos (como ser cambios en el sector y avances tecnológicos) que pudieran tener un impacto negativo en el logro de los objetivos del Banco.

**Principio 5:** Los bancos deberían implementar un proceso para monitorear regularmente los perfiles del riesgo operativo y las exposiciones importantes a pérdidas. La información pertinente se debería presentar regularmente a la alta gerencia y el directorio (consejo de administración) que apoya la administración pro-activa del riesgo operativo.

Un proceso de monitoreo efectivo es esencial para poder administrar adecuadamente el riesgo operativo. El monitoreo regular puede tener la ventaja de la rápida detección y corrección de deficiencias en las políticas, procesos y procedimientos de administración del riesgo operativo. La rápida detección y solución de estas deficiencias puede reducir en gran medida la potencial frecuencia y/o seriedad de un evento de pérdida.

**Principio 6:** Los bancos deberían tener políticas, procesos y procedimientos para controlar y/o mitigar riesgos operativos importantes. Los bancos deberían hacer una revisión periódica de sus estrategias de limitación y control de riesgos y deberían ajustar su perfil de riesgo operativo de acuerdo con ello utilizando estrategias apropiadas, a la luz de su perfil y apetito general de riesgo. El propósito de las actividades de control es enfrentar los riesgos operativos identificados por el banco. Con respecto a todos los riesgos operativos importantes que fueron identificados, el banco debería decidir si quiere utilizar procedimientos adecuados para controlar y/o mitigar los riesgos, o si quiere asumir el riesgo. Para los riesgos que no se pueden controlar, el banco debería decidir si quiere aceptar esos riesgos, o si quiere reducir el nivel de las actividades que den lugar a ese riesgo o si quiere retirar esa actividad completamente. Se deben fijar procesos y procedimientos de control y los bancos deben tener un

sistema para asegurar el cumplimiento de un conjunto documentado de políticas internas relativas al sistema de administración de riesgos.

**Principio 7:** Los bancos deben tener planes de contingencia y de continuación de las actividades para asegurar su capacidad de operar de forma constante y limitar sus pérdidas en caso de una seria interrupción de las actividades. Por motivos fuera del control de un banco, un evento serio puede resultar en la incapacidad de dicho banco de cumplir con algunas o todas sus obligaciones, especialmente si está dañada o inaccesible la infraestructura física, de telecomunicaciones, o de tecnología de información del banco.

#### ***4.3.1.7 La función de los supervisores***

**Principio 8:** supervisores bancarios

Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes como parte de su aproximación general a la gestión de riesgos.

Deberán instar a los bancos a desarrollar y utilizar las mejores técnicas posibles para la gestión del riesgo operativo (las prácticas siguen evolucionando), especialmente en la medida que los riesgos operativos ponen en peligro la seguridad y solidez de los bancos.

Los marcos deberán estar acordes con la orientación de las buenas prácticas y el tamaño de complejidad y perfil del riesgo de los bancos.

**Principio 9:** los supervisores bancarios deberán:

Realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos relacionados con los riesgos operativos.

Verificar de que sean puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en una institución bancaria, como:

Exámenes en situ, análisis extra situ y esfuerzos de extensión.

#### ***4.3.1.8 La función de divulgación de información.***

**Principio 10:** información suficiente, los bancos deberán proporcionar;

Información pública suficiente para que los partícipes del mercado puedan evaluar sus estrategias de gestión de riesgo operativo.

#### ***4.3.1.9 Otros puntos clave:***

- La divulgación de información pública frecuente y oportuna mejora sustancialmente la disciplina de mercado y, por ende, se consideran controles más eficaces.
- La práctica de divulgación del riesgo operativo todavía no están bien asentadas los bancos están desarrollando sus técnicas de evaluación de riesgo operativo. Sin embargo. Los inversionistas y las contrapartes probablemente se beneficien de la divulgación de información.

### **4.1.7 Métodos de medición, control y mitigación de riesgo operativo.**

#### ***4.3.1.10 Evaluación***

Para evaluar el Riesgo Operativo generalmente se toma en cuenta dos variables:

- La frecuencia o probabilidad de suceso de un evento de riesgo, que consiste en el número de ocasiones en la que se detecta la presencia de eventos causales de riesgo.
- La severidad, o importancia del impacto de los eventos de riesgo sobre los resultados o el patrimonio de la empresa.

#### **4.3.1.11 Mediciones del Riesgo Operativo**

Se aplican cuatro metodologías en el cálculo del riesgo operativo como:

Riesgo operacional

- Método de indicador básico.
- El método estándar.
- Método de estándar alternativo.
- Métodos de medición avanzada (AMA).

#### **4.3.1.12 Método del Indicador Básico**

En el método de indicador básico, el cálculo de capital se basa en una proporción según Basilea II propone tres alternativas en el riesgo operativo: Básico, Estándar y de medición avanzada. Asimismo, permite modificar al método estándar, lo cual señala método estándar alternativo. Es el método más simple de los métodos propuesto por el nuevo acuerdo que implica a un requerimiento de capital donde se equivale al producto resultante de multiplicar de los ingresos brutos anuales en un promedio de los últimos tres años por  $0,15 = (15\%$ , factor fijo establecido por el comité).

El método de indicador básico que utilizan los bancos deberán cubrir el riesgo operativo en el promedio expuesto de un porcentaje fijo (denominado como alfa) de los ingresos anuales positivo. Al calcularlo, se excluirán tanto del numerador como del denominador los datos de cualquier año en que el ingreso bruto anual se haya encontrado negativo o equivalente a cero. La demanda de capital se expresa de la siguiente manera:

$$\mathbf{KBIA=GI \times \alpha}$$

Dónde:

KBIA = la exigencia de capital en el Método del Indicador Básico

GI = ingresos brutos anuales medios, cuando sean positivos, de los tres últimos años

N = número de años (entre los tres últimos) en los que los ingresos brutos fueron positivos

$\alpha = 15\%$ , parámetro establecido por el comité de Basilea, que relaciona el capital exigido al conjunto del sector con el nivel del indicador.

La definición del ingreso bruto a los ingresos netos por intereses más otros ingresos netos distintos de intereses. Esta determinación se refiere a que los ingresos sean brutos de diferente previsión (por ejemplo, intereses impagado) y que exceptúe los beneficios o las pérdidas provenientes de pérdidas de valores de la cartera de inversión o las partidas extraordinaria (ingreso provenientes de actividades del seguro, por ejemplo).

#### **4.3.1.13      *Método Estándar.***

Este método establece ocho líneas de negocio y determina exigencias de capital para cada una de ellas. En esta forma, el requerimiento de capital en riesgo operativo correspondería

a la sumatoria de las exigencias determinadas en cada línea lo cual respondería en la expresión siguiente:

$$RCop = \sum (LNi * \beta_i) \quad i = 1$$

Dónde:

**LNi** = ingreso Brutos medios de los tres últimos años para la i-esima línea de negocios.

**$\beta_i$**  = Multiplicador establecido por el comite de Basilea para la i-esima línea de negocio.

El 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 operacional que es probable que asuma el banco en estas líneas de negocio. El requerimiento de capital de cada línea se calcula multiplicando el ingreso bruto por un factor (denominado beta) asignada a cada una de ellas. Beta se utiliza como una aproximación a una relación que existe en el sector bancario entre el historial de pérdidas debido al riesgo operacional en cada línea de negocio y el nivel agregado de ingresos generadores por esa misma línea. Cabe destacar que en el método estándar, se calcula el ingreso bruto de cada línea de negocios y no por el que obtiene la institución en su conjunto.

En el siguiente recuadro se muestran las líneas de negocios y los respectivos ponderados impuestos por el comité.

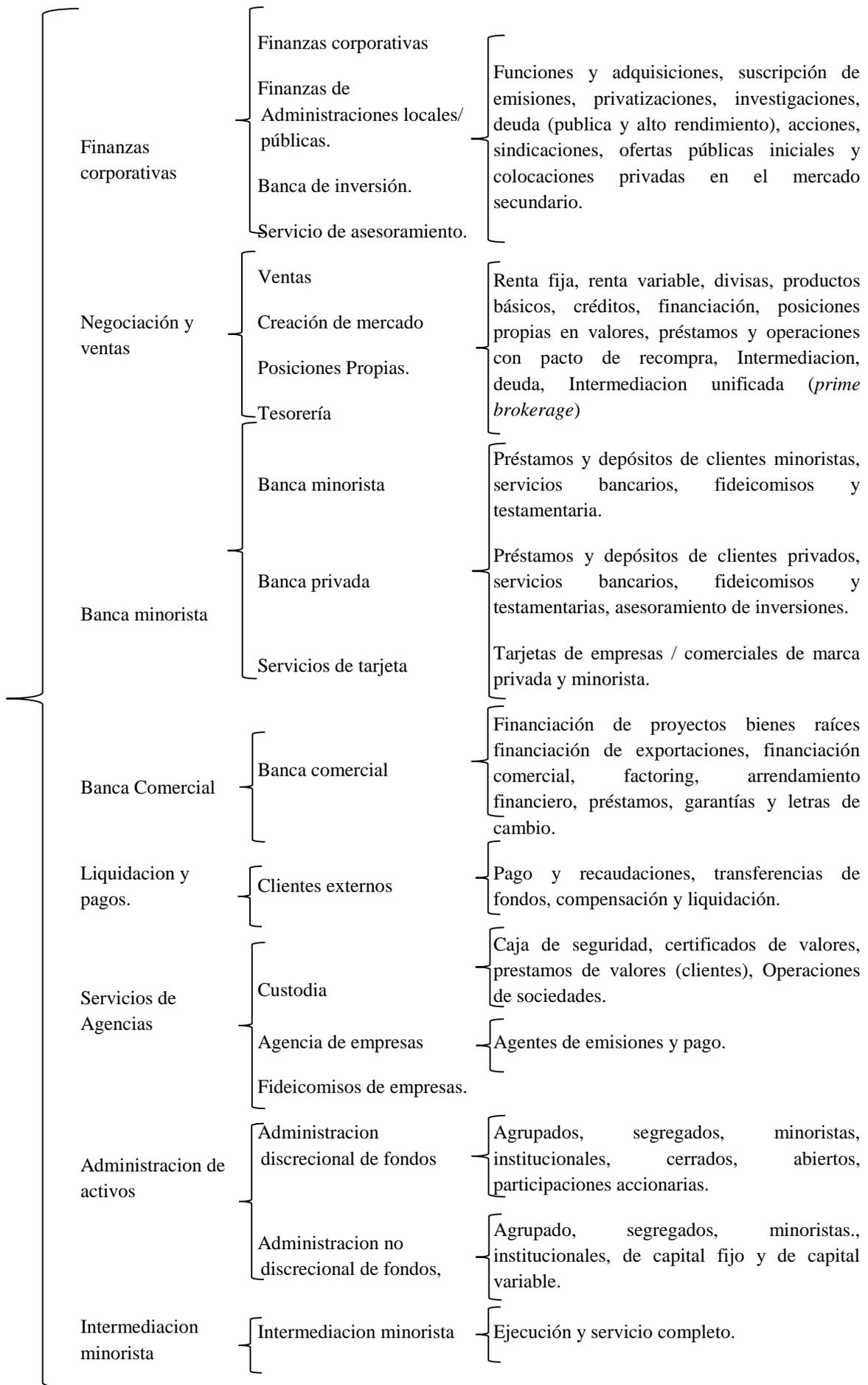
Tabla 1

Línea de negocio en el método estándar.

<b>Líneas de Negocio</b>	<b>Multiplicador (<math>\beta</math>)</b>
Finanzas corporativas	18%
Negociación y ventas	18%
Banca Minorista	12%
Banca comercial	15%
Liquidación y pagos	18%
Servicios de agencias	15%
Administración de activos	12%
Intermediación minorista	12%

Fuente: “Convergencia internacional de medidas y normas de capital” COMITÉ DE  
BASILEA, Versión integral junio 2006.

## Alcance y definiciones de las líneas de negocios



#### *4.3.1.13.1 Criterio admisión en el método estándar.*

Para poder utilizar el método estándar, el banco deberá demostrar a su supervisor que, como mínimo:

- su consejo de administración y su alta dirección, según corresponda, participan activamente en la vigencia del marco de gestión operacional.
- Posee un sistema de gestión del riesgo operacional prácticamente sólido que aplica con integridad, y
- cuenta con recursos suficientes para utilizar la metodología en las líneas de negocios principales, también en el ámbito de control y auditoría.

El supervisor tiene derecho a realizar un seguimiento inicial del método estándar de un banco antes que este pueda utilizarse en efecto de capital regulador. El banco deberá desarrollar políticas específicas y documentar criterios para insertar en el método estándar los ingresos brutos de las líneas de negocio y actividades existentes.

En algunos bancos internacionalmente activo deberán utilizar el método estándar, lo cual es importante mencionar que estos bancos cuenten con los sistemas adecuados para gestionar el riesgo operacional. Por consiguiente un banco con actividad internacional que utilice el método estándar deberá satisfacer otros criterios como:

- El banco deberá constar con un sistema de gestión de riesgo operacional que asigne responsabilidades claras a una unidad operativa que lo gestione. Esta unidad será la responsable del desarrollo de las estrategias para identificar, medir, evaluar y reducir el riesgo operativo; en modificar las políticas y procedimientos dirigida a la gestión y

control para la entidad. Aplicar y diseñar un sistema para una buena información en dicho riesgo.

- El riesgo operacional como parte importante en la integración del sistema de la evaluación interna del banco, lo cual deberá analizar la información de manera sistemática disponible de dicho riesgo, incluyendo las pérdidas relevantes en las líneas de negocio. El sistema de evaluación de riesgo deberá estar integrado en los procesos de control y seguimiento del perfil del riesgo operativo de la institución bancaria.
- El banco deberá contar con procedimientos que permitan adoptar acciones necesarias en tener la información completa para los informes de gestión.
- El sistema de riesgo operacional del banco deberá estar bien documentado para una buena gestión.
- Los sistemas de evaluación de riesgo operativo y los procesos de gestión con los que cuenta el banco deberán someterse a procedimiento de validación y aun examen independiente, que deberá incluir las operaciones de unidades de negocios como también las actividades de las unidades de gestión del riesgo operacional.
- El sistema de evaluación del riesgo operacional de la institución bancaria deberá someterse a exámenes periódicos realizados por auditores internos y por los supervisores (incluidos en la revisión los procesos de validación interna).

#### **4.3.1.14      *Metodo estandar alternativo.***

Este metodo, es una variante del anterior, prácticamente sea la que se aplique en Chile.

En el metodo estandar difiere en la práctica los siguientes aspectos:

Los ingresos brutos de la banca comercial y minorista se sustituyen por el 3,5% de los anticipos y préstamos, conservando el multiplicador  $\beta$  para las respectivas línea de negocio en la definición del método estándar. De esta manera, el requerimiento de capital en cada línea de negocios ( $R_{cln}$ ) se define en la siguiente forma:

$$R_{clni} = \beta_i * m * LA_i$$

*Dónde:*

$\beta_i$ : el factor beta de la línea de negocio correspondiente

$LA_i$ : promedio de los últimos tres años de los montos totales de los préstamos y anticipos (no ponderado por riesgos brutos y provisiones).

$m$ : 3,5%(0,035).

En la banca minorista y la banca comercial existe una posibilidad de que trabajen en conjunto; en este caso el ponderado beta asciende a 15% (factor más elevado entre ambos tipos de banca).

Comúnmente, los bancos que estén imposibilitados de desagregar los ingresos brutos de las seis líneas de negocio restante, podrán trabajar estas líneas en forma conjunta; en este caso el ponderado beta asciende a 18% (el mayor en todos los factores).

#### **4.3.1.15 Métodos de medición avanzada (AMA).**

En este método se presenta una flexibilidad grande la cual permite que sea cada institución bancaria la responsable de la creación de su metodología propia para la medición del riesgo operativo; la condición que exige el comité es que los sistemas y procedimientos utilizados sean suficientemente integrados

Se espera que los bancos adopten gradualmente este método con actividades internacionales y las que mantienen altas exposiciones al riesgo operacional.

El AMA en su desarrollo y su aplicación requiere de manejo de información de difícil acceso y exhaustiva, así como evidencias y verificaciones empíricas que permitan validar de forma confiable las metodologías y los procedimientos a utilizar para determinar el riesgo operativo y las exigencias de capital para tales efectos.

En los AMA, el requerimiento de capital regulador será igual a la media generada por el sistema interno del banco para el cálculo del riesgo operacional utilizando los criterios cuantitativos y cualitativos aplicables a los AMA que se analizan más adelante.

El banco que adopte los AMA, por previa aprobación de los supervisores del país de acogida y respaldo de su supervisión de origen, lo cual podrán utilizar un mecanismo de distribución para determinar el requerimiento de capital regulado para las filiales de bancos con actividad internacional que no se consideren significativa con respecto al grupo en su conjunto pero que estén sujeta al presente marco en virtud del primer pilar.

Al determinar si la metodología de asignación resulta adecuada, habrá que tener en cuenta el grado de desarrollo de las técnicas de distribución sensible al riesgo y hasta qué punto se refleja el nivel de riesgo operacional en las entidades legales y en el grupo bancario.

Estos bancos que adopten las AMA deberán calcular el requerimiento de capital utilizando esta metodología.

Lo cual son determinados por el sistema de medición del riesgo operacional interno de la institución. Para la utilización del método se requiere la aprobación del regulador local, misma que dependerá del cumplimiento de los siguientes requisitos:

- La administración debe estar plenamente involucrada con el marco de administración de riesgo operacional.
- Se debe constar con un buen sistema de administración de riesgo operacional integro.
- Se debe de constar con recursos suficientes en el uso del enfoque en las líneas de negocios más importantes así como en las áreas de control y auditoria.
- Estándares cualitativos y cuantitativos.

El AMA considera tres enfoques:

1. ***El enfoque de medición interna.*** Este regulado determina el índice de exposición y múltiplo, él lo cual se convierte la pérdida esperada (EL) y pérdida no esperada (UL) para todo el gremio en forma análoga y para cada entidad que obtiene, solamente, estimaciones de probabilidad de fallo y proporción de pérdida dado al fallo.

2. ***El enfoque de distribución de pérdida.*** Es un modelo de VaR (valué at Rick) en las líneas de negocios y tipos de eventos de perdidas, en donde el VaR total es la suma de los VaR de todas las combinaciones sin considerar correlaciones.

3. ***El enfoque de tarjeta de puntaje.*** Se calcula un nivel de riesgo considerando como base las estadísticas de todos los eventos de pérdida disponibles para la entidad (habida cuenta de que es estadísticamente significativa), y que se reorganiza por línea de negocio, en función de la tarjeta de puntaje diseñada aplicada y que contiene ciertas medidas de control.

El capital regulatorio del AMA está dado por la suma de pérdida esperada (EL) y la no esperada (UL). En el caso que la institución pueda demostrar que su registro es apropiado la pérdida esperada (EL), entonces podrá disminuir el monto de pérdida no esperada (UL).

#### *4.3.1.15.1 Criterios cualitativos*

Las instituciones bancarias deberán tener en cuenta los siguientes criterios cualitativos para emplear un AMA primeramente autorizados para calcular su requerimiento de capital por riesgo operacional:

- Los auditores internos y externos deberán llevar a cabo exámenes periódicos de los procesos de gestión y sistemas de medición de riesgo operacional. En estos exámenes deberán incluir las actividades de la unidad independiente de gestión de riesgo operativo como las operaciones de la unidad de negocio.
- La validación del sistema de medición del riesgo operativo que deben de llevar a cabo los auditores externos y/o las autoridades supervisoras deberán regirse a los siguientes aspectos:

Un buen funcionamiento en los procesos de validación interna,

Una buena accesibilidad y transparencia del flujo de los datos asociados al sistema de medición del riesgo y de su procedimiento. En general, es necesario que los auditores y las autoridades supervisoras puedan acceder fácilmente a las especificaciones y parámetros del sistema, siempre que se estimen necesarios y se realicen los procedimientos oportunos

#### *4.3.1.15.2 Criterios cuantitativos*

##### *Criterios sólidos de los AMA.*

El banco tiene la obligación de demostrar que su método identifica eventos situados en las “colas” de la distribución de las probabilidades, generadores de pérdidas trascendental, con

independencia del método utilizado, la institución bancaria deberá demostrar que la estimación del riesgo operacional retribuye u criterio sólido comparable al exigido en el método de tratamiento del riesgo de crédito basado en calificaciones internas ( es decir relacionado a un periodo de mantenimiento de 1 año y con un intervalo de confianza del 99,9%).

#### *Análisis del ambiente*

Junto con los datos externo, el banco deberá utilizar análisis del ambiente o eventualidades basadas en opiniones profesionales, al objeto de evaluar su exposición a eventos generadores de pérdidas trascendental. Este método se sirve del conocimiento de directivos experimentados y de expertos en gestión de riesgo para obtener una buena evaluación razonable de las pérdidas que posiblemente podría sufrir la entidad. Por ejemplo, las evaluaciones de estos expertos podrían expresarse en forma de parámetros de una distribución estadística supuesta de la pérdida. Asimismo, el análisis del ambiente deberá utilizarse para valorar el efecto de las desviaciones que se produzcan con respecto a los supuestos de corrección incorporados en el marco de medición del riesgo operacional del banco a fin de evaluar, en definido, las pérdidas procedentes de múltiples eventos simultáneos de pérdidas por dicho riesgo.

Factores relacionados con el entorno de la institución y con el control interno.

Además de utilizar los datos de pérdidas, ya sean reales o basados en escenarios, la metodología de evaluación de riesgo aplicada al conjunto de la entidad bancaria deberá de identificar aquellos factores básico de su entorno y de su control interno que pueden modificar su perfil de riesgo operacional. Estos factores permitirán que las evaluaciones del riesgo que realiza el banco estén más orientados hacia el futuro, que reflejen de forma más directa la

calidad de los entornos operativos y de control de la institución, a la contribución en la alineación de las evaluaciones de capital con los objetivos de la gestión de riesgo y del reconocimiento inmediato tanto de la mejora como el deterioro de los perfiles del riesgo operacional. La medición del riesgo de una entidad bancaria tendrá que satisfacer los criterios que a continuación se presentan:

- La selección de cada factor deberá justificarse por generar riesgo de forma significativa, a partir de la experiencia y de la opinión de los expertos del personal del área de negocio afectadas.
- Deberá exponer adecuadamente la sensibilidad de las estimaciones de riesgo del banco ante la variación de los factores, así como la ponderación relativa de los diversos factores. Por lo tanto la identificación de las variaciones de riesgo por mejoras en los controles de riesgo, la metodología también deberá señalar incrementos potenciales del riesgo atribuibles a una mayor complejidad de las actividades o aun volumen de negocios más elevado.
- La metodología y cada elemento de su aplicación, incluido el razonamiento a favor de ajustes potenciales en las estimaciones empíricas, deberán documentarse y someterse al examen independiente del propio banco y de sus supervisores.
- A lo largo del tiempo, el proceso y los resultados obtenidos tendrán que validarse, comparándolos con el historial interno de pérdidas efectivas y con datos externos relevantes y con los ajustes oportunos introducidos.

#### *4.3.1.15.3 Cobertura del riesgo*

Cuando el banco utiliza un AMA, está autorizado a reconocer el efecto reductor del riesgo que genera el seguro en las medidas del riesgo operacional utilizadas a calcular los

requerimientos mínimo de capital regulador. El reconocimiento de la cobertura de los que se tienen en consideración la totalidad de los riesgos operacionales existentes en el conjunto de las operaciones consolidadas del banco;

- Todas las operaciones del banco cubiertas por AMA satisfacen los criterios cualitativos exigidos para la utilización del mismo, en tanto que el resto de las operaciones que emplean algunos de los métodos más sencillos cumplen con los criterios de admisión de dicho método.
- En su fecha de aplicación, el AMA ya recoge una parte significativa de los riesgos operacionales de los bancos.
- El banco presenta a su supervisor un plan que especifica el calendario que pretende seguir para comenzar a desplegar el AMA en todas sus unidades de negocio significativas. El plan deberá regirse por lo práctico y factible que resulte adoptar el AMA con el paso del tiempo, y por ningún otro criterio.

Sujeto a la aprobación del supervisor, el banco que opte por la utilización parcial podrá determinar en qué parte de sus operaciones empleara el AMA, en base a las líneas de negocios, estructuras jurídicas, ubicaciones geográficas u otro criterio determinado internamente.

## V. Caso Práctico.

### 5.1 Perfil de la empresa.

#### 4.1.8 Historia de la empresa.

BDF es un banco de tamaño mediano dentro del sistema financiero nicaragüense fue fundado el 2 de junio de 1992 con la perspectiva de establecerse sólidamente en el mercado nicaragüense con visión de largo plazo.

Desde sus inicios, el BDF se definió como una banca orientada al consumo y a los pequeños negocios y se ha caracterizado por brindar oportunidades y acceso al sistema financiero a más de 200 mil nicaragüenses.

A finales del año 2006, el Grupo ASSA de Panamá adquirió una participación mayoritaria del BDF, fortaleciendo así su presencia en Nicaragua y expandiendo sus horizontes de crecimiento hacia Centro América. El banco pertenece a Grupo BDF, S.A. (Grupo BDF), entidad jurídica creada en 2008 por las leyes de la República de Panamá, cuya subsidiaria más importante es BDF y su accionista mayoritario es Grupo ASSA S.A. (Grupo ASSA) mientras que el resto de la participación accionaria se reparte entre empresas propiedad del Instituto de Previsión Social Militar y varios inversionistas.

Grupo ASSA, S.A. fue fundado en 1972 y las empresas que lo conforman manejan destacadas operaciones en el campo de los seguros y las finanzas en Panamá. El grupo ha iniciado una clara estrategia de expansión en Centroamérica. En Nicaragua, luego de la

adquisición accionaria del BDF en el 2006, el Grupo adquirió control también de Metropolitana Compañía de Seguros.

BDF tiene una orientación de banca minorista, con dos tercios de su cartera enfocados en el segmento de personas. El banco tiene definida su orientación de cartera en tres pilares: consumo, hipotecas y corporativo; para los cuales pretende mantener una distribución de cartera equitativa. La cartera de consumo es el principal generador de ingresos, incluso superando las contribuciones combinadas de los otros pilares. El banco prevé que se mantenga esta estructura de ingresos sin cambios significativos en el futuro. La orientación minorista y, en especial, la posición líder del banco en hipotecas representan una oportunidad para una venta cruzada mayor de productos y, especialmente, para el lado pasivo, en el que su franquicia es más débil.

#### **4.1.9 Visión**

Visión: Ser el banco preferido de los nicaragüenses por ofrecer el mejor servicio, contribuyendo al desarrollo de sus clientes y de la comunidad

#### **4.1.10 Objetivos estratégicos.**

Los objetivos estratégicos contemplan mantener el equilibrio actual de la cartera en los tres pilares, con la posibilidad de presentar pequeñas variaciones naturales año con año. No obstante, la administración prevé que el banco incremente gradualmente su participación de mercado en el sector comercial. La empresa también planea desarrollar más su oferta de medios de pago y apalancarse de sus nexos en el sector empresarial para poder ofrecer sus productos a empleados de las corporaciones que ya atiende. También espera que el establecimiento de una cámara de compensación (ACH por sus siglas en inglés) beneficie a bancos del tamaño de BDF

que no poseen la franquicia del lado pasivo, a diferencia de las entidades más grandes del sistema.

BDF ha logrado alcanzar sus objetivos a través de los últimos años. El desempeño en el sector financiero se ha beneficiado del entorno económico nicaragüense favorable y, en opinión de Fitch, este se mantendrá como el factor clave en el crecimiento de resultados del sistema bancario.

Los objetivos estratégicos de BDF se enfocan en crecer en los principales segmentos que atiende, como consumo, vivienda y empresas, de manera que su cartera se distribuya equitativamente entre dichos sectores. El banco proyecta un crecimiento en activos de 8.3% en 2016, derivado de un aumento de 10% en sus préstamos. Al mismo tiempo, planea diversificar productos y servicios de banca electrónica y ampliar sus canales de atención al cliente. En el lado pasivo, proyecta un crecimiento de 6% en depósitos, enfocándose en captaciones con plazos mayores, para asegurar estabilidad en sus calces. Asimismo, el banco buscará diversificar sus fuentes de fondeo mediante un aumento de USD15 millones en sus emisiones de bonos.

La administración cuenta con un buen historial de logro de sus objetivos estratégicos en los últimos años. Aunque el entorno económico ha sido favorable para la industria y ha facilitado el desempeño de las instituciones financieras, en opinión de la agencia, la administración de BDF posee la habilidad y capacidad para llevar a cabo una ejecución razonable de las estrategias de negocio de largo plazo. No obstante, el alcance de los objetivos siempre estará sujeto a un entorno mucho más retador que el resto de países en la región, una vez que se experimente un cambio en el ciclo económico.

#### 4.1.11 Valores.



#### 4.1.12 Organización.

##### Equipo Gerencial

➤ **Presidente Ejecutivo y Gerente**

##### **General**

Juan Carlos Argüello Robelo

➤ **Director de Operaciones**

Violeta del Carmen Pérez Orozco

➤ **Director de Banca de Empresas**

Jimena Zelaya Lacayo

➤ **Director de Tecnología**

Zurama Tatyana Corea López

➤ **Director de Banca de Personas**

Jaime Alberto Altamirano Ramírez

➤ **Director Financiero**

➤ **Gerente de Crédito**

##### **Corporativo**

Glenda del Carmen Aburto

Rodríguez

➤ **Gerente de Mesa de Cambio**

y **Comex**

Patricia Esperanza Diaz Solís

➤ **Gerente de Negocios**

##### **Institucionales**

María de los Ángeles García

➤ **Gerente de Préstamos**

##### **Personales**

Leonel José Quant Jarquín

➤ **Director Sucursales Y Canales  
Electrónicos**

Yvette Cecilia Fonseca

➤ **Director de Riesgo**

Marlon Jesús Pérez Bustos

Lucia Beatriz Alvarado Aragón

➤ **Gerente de Tarjetas de  
Crédito y Débito**

Carmen María Urtecho Espinoza

➤ **Gerente de Préstamos de  
Vivienda**

Carolina Pineda Zeledón

➤ **Gerente de Préstamos de  
Vehículo**

Lohanna Arguello Choiseul

➤ **Gerente Pyme**

Ricardo Antonio Zeas Marquez

➤ **Gerente de Excelencia en el  
Servicio**

Norma Guadalupe Maltéz Tapia

➤ **Gerente de Cumplimiento**

Mariela Lacayo

➤ **Gerente de Recursos  
Humanos**

Maritza Abdalah

## 5.2 Sistemas de identificación de riesgos y cuantificación de pérdidas

El riesgo operativo se define en BDF como el riesgo de pérdida debido a la inadecuación o a fallos de los **procesos, personas** y los **sistemas internos** o bien a causa de acontecimientos **externos**. Para BDF esta definición incluye el riesgo legal y el de reputación.

La gestión de riesgo operativo, incluye los procesos de ambiente de control, identificación, evaluación y mitigación de riesgos operativos, evaluación de controles y reporte de incidentes, los cuales deben ser realizados descentralizadamente en las áreas funcionales, siguiendo los estándares definidos por el área de riesgo operativo.

La política de riesgo operativo expresa que el diseño del marco general de administración de los riesgos operativos está diseñado en base a cuatro principios administrativos centrales:

- Propiedad descentralizada de los riesgos con responsabilidad de cada área funcional.
- Coordinación y seguimiento general por el Área de Riesgo Operativo.
- Supervisión independiente de la ejecución de parte del Comité de Riesgo y Tecnología y la Unidad de Administración Integral de Riesgo.
- Evaluación independiente de la Auditoría Interna, externa y del ente regulador.

La política determina que la condición principal para la administración de los riesgos operativos, se refiere a su enfoque hacia los procesos, por lo que es requisito indispensable disponer del Mapa de Procesos institucional, incluyendo las respectivas interrelaciones y objetivos.

La política busca asegurar los siguientes objetivos organizacionales:

- Salvaguardar los activos, evitando incidentes que puedan producir pérdidas monetarias (por causas deliberadas - fraude - o accidental).
- La eficiencia operativa, evitando incidentes que puedan producir reproceso (correcciones o repeticiones parciales o totales de un proceso que implican costo o tiempo de personal) debido a fallas en procesos, sistemas, gente o por eventos externos.
- La continuidad del negocio, evitando que puedan interrumpir las operaciones y prestación de servicios de la entidad.
- El cumplimiento regulatorio, evitando incidentes que puedan producir incumplimiento de cualquier regulación o ley nacional.
- De revelación financiera, evitando incidentes que puedan hacer que los registros contables sean inexactos.

El banco ha definido la siguiente estructura para la gestión del riesgo operacional



El rol de la Junta Directiva en la administración del riesgo operacional, es que como máxima autoridad, aprueba las políticas y manuales de RO. Son responsables por la

continuidad de las operaciones de la institución y de constituir e integrar el Comité de Riesgo y Tecnología para supervisar la administración integral de riesgos.

Este comité debe estar conformado por cuatro miembros de JD, Gerente General y Directores de área (Directora de Operaciones, Director de Banca de Empresas, Director Banca de Personas, Director de Riesgo Crediticio, Directora de Tecnología, Gerente de Seguridad y Control, Director UAIR y Auditor Interno) y son los encargados de proponer a la JD la política de GRO, aprobar metodologías para la GRO, conocer el monto de las estimaciones y las pérdidas efectivamente realizadas para mejora de los procesos y garantizar la adecuada implementación de la política y metodología de la GRO. Este Comité sesiona bimestralmente.

Como parte de la administración y control de riesgo operacional, en la política se incluye las responsabilidades de otras áreas de apoyo como son: Gerencia de Calidad, Gestión Humana, Auditoría Interna, Legal.

La metodología del banco define y determina los niveles de apetito de riesgo a que están dispuestos a asumir. Para cada uno de los objetivos organizacionales se establecieron los niveles de riesgo máximos aceptables (apetito de riesgo) ponderando los valores de los dos atributos con los que se realiza la evaluación de todos los riesgos operativos (Probabilidad e Impacto).

<b>N°</b>	<b>Objetivo</b>	<b>Límite de apetito</b>
1	Salv guarda de activos (pérdidas por	$P \times I < 3.5$
2	Eficiencia Operativa	$P \times I < 3.5$
3	Continuidad de Negocio	$I < 2$
4	Cumplimiento regulatorio	$I < 2$
5	Revelación financiera	$I < 2.5$

Estos límites fueron determinados en función de lo que definen las mejores prácticas, y de la experiencia propia que han tenido (guiándose por las pérdidas ya incurridas, aunque sin mucha precisión).

#### **4.1.13 Identificación y evaluación de riesgos operativos:**

En este proceso intervienen el área de riesgo operacional y las áreas funcionales, en éstas últimas el jefe del área se denomina dueño del proceso y este a su vez debe designar dentro de su estructura uno o más encargados de realizar actividades relacionadas con la administración de riesgo operativo, los cuales son denominados gestores de riesgo operativo. Estos están en línea con el Coordinador de Riesgo Operacional, para implementar una metodología estándar.

Los insumos para identificar riesgos son: Nuevos productos, operaciones o servicios, Reporte de Incidentes de RO, Informe de Auditoría Interna y Externa u otros.

Los riesgos operativos deben ser identificados en función de los objetivos de cada proceso y evaluados de acuerdo a la probabilidad de ocurrencia e impacto. En la etapa actual están reevaluando estos riesgos para los procesos críticos y los están llevando a una herramienta que les guía para este proceso y pondera el nivel de riesgo en base a unos criterios definidos, una vez que se ha realizado una sesión interna y se compara con las matrices de otras unidades de control y de operaciones.

La identificación y evaluación de riesgos está prevista realizarse en forma periódica de acuerdo a la madurez del proceso de gestión de riesgo operativo o cuando se den cambios importantes en los procesos.

#### 4.1.14 Planes de Mitigación de Riesgos Principales

Una vez que se haya realizado la evaluación de los riesgos, cualquier riesgo cuya evaluación esté por encima de los límites del apetito de riesgo, debe ser mitigado, para que quede dentro de esos límites. La mitigación de riesgos puede hacerse mediante el establecimiento de controles o la transferencia de los riesgos por mecanismos aceptados.

Cada área funcional debe definir e implementar los planes de mitigación correspondientes, utilizando alguna de las siguientes alternativas:

- 1) Revisar estrategias y políticas;
- 2) Actualizar o modificar procesos y procedimientos establecidos;
- 3) Implantar o modificar límites de riesgo;
- 4) Constituir, incrementar o modificar controles;
- 5) Implantar planes de contingencias y de continuidad del negocio;
- 6) Revisar términos de pólizas de seguro contratadas; y,
- 7) Contratar servicios provistos por terceros, u otros, según corresponda (mitigación a través de pólizas de terceros – Ejemplo: traslado de valores).
- 8) Proyecto de largo plazo (sistemas).

En lo que respecta a las pólizas de seguros, actualmente cuentan con las relacionadas a protección de todo daño físico en edificios e instalaciones, colectivo de vida y de accidentes, de daño a equipo electrónico, póliza bankers blanket bond (BBB) y de fidelidad comprensiva.

Una vez definidos y aprobados los planes de mitigación, éstos son ingresados al módulo por el gestor de riesgo operativo, quien a su vez incluye las tareas, plazos y responsables para el monitoreo del avance en su implementación.

Para la evaluación de controles, el banco utiliza una metodología que conlleva 5 etapas: identificación de controles, prueba de controles para verificar efectividad, análisis de resultados de pruebas, elaboración del reporte de prueba de controles e informe de resultados. Actualmente están en la fase del levantamiento de inventario de controles y algunos de ellos empiezan a realizar pruebas.

Dentro de éstos controles tenemos: Revisiones formales, Aprobaciones, Conciliaciones, Validaciones, Controles cruzados, otros.

#### **4.1.15 Registro de Incidentes**

En el ciclo de la gestión del riesgo operacional se incluye el reporte de incidentes que consiste en la obligación, que tiene cada una de las áreas funcionales, de reportar todos los incidentes que ocurren en sus áreas, derivados de inconsistencias en la ejecución de sus procesos.

Para incidentes que tengan un potencial bruto de pérdidas financieras, se deben reportar al Comité de Riesgos los casos por encima de US\$5,000, aunque se registran todos. Para los casos que tienen algún impacto reputacional, necesitarán ser reportados independientemente del tamaño de la pérdida potencial.

Estos incidentes deben ser registrados por los gestores de riesgo operativo en el módulo establecido en un período de 7 días laborables, una vez descubierto.

Mensualmente el equipo de RO realiza una consolidación de todos los incidentes reportados en una base de datos que contiene todos los incidentes y Riesgo Operacional

analiza todos los incidentes reportados con el fin de determinar comportamientos particulares, tendencias, debilidades en los procesos, oportunidades de capacitación a colaboradores, entre otros.

Para su control, los incidentes de riesgo operativo se clasifican en 4 categorías de factores de riesgos de Nivel I (Recursos humanos, procesos internos, eventos externos y sistemas), luego se dividen en 7 tipos de eventos (Nivel II), de igual forma se sub dividen en 25 categorías de sub tipos de eventos (Nivel III) y finalmente se dividen en 129 sub categorías (Categorías de Incidentes de Nivel IV), de acuerdo a la nomenclatura sugerida por Basilea. El Área de Riesgo Operativo clasifica los incidentes de riesgo operativo reportados por las áreas funcionales usando las categorías de incidentes de nivel IV.

A partir de marzo 2012 el banco cuenta con el aplicativo de riesgo operativo (Help Desk) cuya función esencial es la capacidad de proporcionar apoyo para el cálculo del capital regulatorio del banco mientras exista una base de datos de pérdidas que permita predecir mediante la utilización de métodos estadísticos el volumen de las pérdidas asociadas a estos errores.

### **5.3 Estrategia Tecnológica**

La institución cuenta con un proceso de planificación estratégica, el que tiene un horizonte no mayor de 3 años. Tecnología se inserta como parte de este plan como un área funcional de apoyo, para la consecución de los objetivos estratégicos.

Los proyectos de mejora a la plataforma tecnológica se definen al inicio de cada año y está conformado por proyectos en ejecución del año anterior, proyectos estratégicos

definidos anualmente y los proyectos de inversión. La prioridad de ejecución se basa en el siguiente orden de importancia: cumplimiento regulatorio, aumento de rentabilidad, mejora en procesos de impacto directo en atención al cliente y mejoras en el control interno y seguridad.

Los proyectos en dependencia del carácter del mismo son presentados en el comité de riesgos y sistemas, para ser finalmente llevados a Junta Directiva.

Los proyectos actuales cuentan con un presupuesto aprobado y están encaminados a la actualización de la plataforma tecnológica (servidores y componentes críticos), respaldo centralizado de equipos de puestos críticos, banca en línea y el fortalecimiento de la seguridad de la red BDF.

No obstante lo anterior y tomando como referencia que a nivel del mercado en Estados Unidos la mayor parte de las vulnerabilidades y ataques han sido focalizados en aplicaciones, el banco estableció como estrategia de modernización posible a un corto plazo, la migración de componentes críticos a nuevas tecnologías, como el remplazo del canal de banca electrónica por uno que cumpla con todos los requerimientos funcionales y de seguridad, integrable con el core-banking actual.

#### **4.1.16 Canales de servicio alternos y Bancarización:**

El banco actualmente cuenta con canales alternos establecidos, dentro de los cuales se tienen:

- Red de dispensadores de dinero (ATM).
- Pago electrónico de planillas
- Sucursal electrónica para productos de banca y de tarjeta de crédito.
- Servicio de charla en línea (WebChat) en el sitio web del banco.
- Centro de atención telefónica.

#### **4.1.17 Estrategia de Tercerización**

BDF cuenta con la política “Gestión de compras y proveedores”, que tiene como objetivo, garantizar que los proveedores cumplan con las políticas y requisitos contemplados en el contrato, así como los estándares de calidad establecidos, por medio de evaluaciones periódicas. Su alcance incluye desde la selección de proveedores hasta la compra y recepción del bien o servicio.

La gestión de compras y proveedores está a cargo de la gerencia administrativa, todo nuevo proveedor ya sea ocasional o no, debe ser autorizado previo a la compra de producto y/o servicio, por la Gerencia Administrativa y/o Jefe de compras y proveedores.

Se considera Proveedor Ocasional de Banco de Finanzas, a todas aquellas personas naturales o jurídicas a los cuales se les realicen menos de cinco pagos durante el año y el total de pagos realizados no exceda los treinta mil dólares.

Los responsables de los procesos (Directores/Gerentes/Jefes de áreas) deben garantizar que los proveedores de bienes y servicios se ajusten plenamente a los requisitos de identificación establecidos por las leyes, normas y procedimientos internos. Además deben garantizar que los expedientes de proveedores cumplan con los requisitos establecidos en la matriz de requisitos a proveedores, la actualización y mantenimiento de la Matriz de Proveedores, está a cargo de la Gerencia Administrativa.

Actualmente el banco cuenta con 132 servicios tercerizados, de los cuales 86 son de bajo riesgo, 41 medio y 5 son de alto riesgo (Transunion Nicaragua, S. A., ULTRAVAL, AMNET y ULTRANIC).

Las evaluaciones a los proveedores son realizadas anualmente por los responsables de los procesos.

En el caso de los proveedores de alto riesgo, estos deberán presentar los Estados Financieros que incluyan Balance General, Estado de Resultado – del último año – y/o anexos, debidamente firmados por el Gerente General y/o representante legal y Contador o Financiero, sean estos auditados o no. De igual forma debe solicitar referencia bancaria o comercial, sea esta nacional o extranjera. Aunque el requisito de Estados Financieros son proveídos, no hay un análisis o evaluación de los mismos, constituyendo solo un requisito sin alguna utilidad.

El contrato con los proveedores debe establecer e identificar todos los aspectos relevantes según la Matriz de contratos que está acorde lo establecido en Norma sobre la contratación de proveedores de servicios financieros para la realización de operaciones o servicios a favor de las instituciones financieras, Resolución No CD-SIBOIF- 421-1-MAY16- 2006.

#### **5.4 Continuidad de negocios y planes de contingencia**

El modelo de gestión de continuidad de negocio del banco considera las siguientes etapas:

- Hacer un análisis de impacto de negocio (BIA) y análisis de riesgos (AR)
- Selección de estrategias de recuperación.
- Desarrollar e implementar estrategias.
- Dar mantenimiento a planes y hacer pruebas.

Los análisis BIA y AR permiten identificar los servicios críticos y definir las prioridades de recuperación; Sin embargo, apunta más hacia un Plan de Recuperación ante desastres, que aunque sigue un procedimiento lógico, tampoco está actualizado.

Las bases de las estrategias de recuperación se realizaron estableciendo una priorización de procesos, las cuales son las siguientes:

1. Recuperación selectiva y en etapas (en la que la etapa 1 se normaliza en un máximo de 1 semana).
2. Basada en Tecnología
3. Reubicación de Colaboradores
4. Cierre de algunas Sucursales

Sin embargo, uno de los supuestos sobre los que se basa esta estrategia es la existencia de un Sitio Alterno, con infraestructura tecnológica suficiente para restaurar completamente la operatividad computacional de los procesos críticos y de los procesos de apoyo seleccionados y esta es una debilidad que presenta el banco al contar con un sitio secundario en la capital a una distancia muy cercana del centro principal y en una zona altamente sísmica.

El cronograma de actividades para el año próximo establece las siguientes actividades:

- la creación de la cultura de continuidad de negocios
- realización y/o actualización de BIA
- priorización de procesos
- ajuste de estrategias de recuperación
- actualización de documentos

- Pruebas y simulacros (prueba del árbol de llamadas y simulacros de evacuación)

En cuanto a las pruebas y simulacros, no existe un plan de pruebas aprobado por el comité de riesgos y tecnología. A la fecha no se ha realizado ninguna prueba.

## **5.5 Seguridad de la Información**

El banco cuenta con políticas de seguridad de la información de alto nivel que tienen como propósito ser el marco de control institucional que debe seguirse para garantizar los adecuados niveles de seguridad en el uso de la información mediante los sistemas de información que el banco provee a sus colaboradores.

Esta política abarca los siguientes temas:

- Control de acceso lógico y físico
- Seguridad Física en Cuartos de Cómputo y Redes
- Gestión de Incidentes
- Desarrollo y Mantenimiento de Sistemas
- Intercambio de información
- Uso adecuado de recursos y servicios tecnológicos

Esta política fue creada en el año 2005 con el fin de implementar un modelo de gestión de seguridad del banco basado en la mejor práctica ISO 17799:2005, desde su implementación ha sido actualizada principalmente con cambios menores, siendo su última modificación en abril de 2011.

Este estándar sugiere 12 áreas que deben ser cubiertas, para poder garantizar un nivel adecuado de seguridad.

1. Evaluación de riesgos
2. Políticas de Seguridad de la información
3. Organización y gobierno corporativo
4. Administración de Activos de Información
5. Recursos Humanos
6. Seguridad Física y Ambiental
7. Gestión de la Operación y las Comunicaciones
8. Control de Acceso a la Información
9. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
10. Gestión de Incidentes de Seguridad de Información
11. Gestión de Continuidad de Negocios
12. Cumplimiento regulatorio

A nivel organizativo, la institución tiene bien establecidas las instancias de gobierno corporativo, siendo el Comité de Riesgos y Tecnología quien se encarga de aprobar y resolver los temas de seguridad de la información. El banco cuenta además con 3 oficiales de seguridad.

El tema de seguridad del recurso humano se gestiona mediante diferentes controles establecidos, entre ellos:

- Capacitaciones de inducción al personal de nuevo ingreso en temas de seguridad de información.
- Firma de aceptación y entendimiento a la política de seguridad.

- Definiendo acuerdo de confidencialidad con proveedores y personal temporal.
- Firma de acta de responsabilidad en el uso de dispositivos móviles.
- Definición de Matriz de roles y accesos x puestos.
- Se coordinó con Gestión Humana la definición de sanciones por incumplimiento de políticas de seguridad.

La seguridad física de todo el negocio se encuentra a cargo de una gerencia especializada en el tema, esta gerencia tiene a cargo la gestión del personal de seguridad y el monitoreo de los sistemas CCTV.

Sobre los temas de control de acceso, a nivel de aplicativo se ha logrado contar con una matriz de control de acceso basado en los perfiles de puesto de cada usuario, esto es una actividad en constante cambios de acuerdo a las modificaciones organizacionales del banco, se hace un trabajo conjunto entre la gerencia de operaciones, tecnología y riesgo.

Se han desarrollado controles para establecer la seguridad en el proceso de desarrollo de sistemas, esta tarea se realiza en el área de tecnología con personal destinado a la certificación de las tareas de desarrollo interno, se hace uso de la fuerza laboral interna para el mantenimiento de los sistemas de misión crítica del banco, los nuevos productos son realizados por terceros o en conjunto con ellos.

En cuanto a la gestión de incidentes el banco cuenta con recursos destinados al monitoreo de la disponibilidad de los servicios tecnológicos, así como al monitoreo de amenazas o vulnerabilidades que puedan afectar al banco así como a su infraestructura.

A nivel de aplicación, la institución ha realizado la implementación de los siguientes controles:

- Autenticación Usuario y Clave.

- Validación de entradas de datos a nivel de aplicación Web
- Implementación de autenticación multifactorial en BDF

El comité de riesgos y tecnología es posible apreciar iniciativas de mejoras en cuanto a infraestructura tecnológica y lanzamiento de nuevos productos para mejorar la atención al cliente.

#### **4.1.18 Documentación física: (Contratos, pagarés, certificados en garantías, pólizas, etc.)**

El banco cuenta con la asesoría de dos despachos legales que emiten su opinión sobre la calidad de las garantías hipotecarias en lo que respecta a la capacidad de ser sujetas a gravamen y ser ejecutables. Esto se ha verificado en la revisión de las muestras de cartera realizadas. La opinión legal del despacho es un requisito para la aprobación del crédito.

También este despacho efectúa revisión de los términos de los contratos de operaciones activas y pasivas del banco (contratos de adhesión), en la procura de que cumplan las leyes aplicables a la industria, incluidos los convenios con organismos proveedores de fondos. Los contratos diseñados para la formalización de créditos al segmento de empresas fueron revisados en el marco de revisión completa dado hace aproximadamente 2 años para la ampliación de este segmento, dentro de su estrategia de negocios.

El banco está en un proceso de digitalización de los documentos legales de los expedientes de operaciones activas y pasivas, para evitar documentación duplicada y los originales resguardados en bóveda.

En cuanto a la seguridad física el banco cuenta con una política de seguridad que comprende la integridad física de los clientes, colaboradores, así como de salvaguardar el

patrimonio del Banco, mediante la prevención, control y minimización de los riesgos de seguridad en todas las áreas, protegiendo física y electrónicamente los bienes de la institución.

La Gerencia de seguridad debe procurar proveer los medios y determinar los procedimientos, en coordinación con otros sectores de la entidad, para proteger física y electrónicamente los bienes de la entidad financiera, el personal y los clientes, a fin de evitar hechos delictivos y siniestros o bien minimizar los daños en caso de ocurrencia, entendiendo como bienes el dinero, los cheques, los títulos, los bonos y, en general, la documentación, así como los bienes muebles e inmuebles.

Para la administración de la política, se designó al comité de seguridad interna que está conformado por el Gerente General, Director de Operaciones, Asesor Legal y Gerente de Seguridad. Este comité es el responsable del análisis de las medidas administrativas y legales que correspondan aplicarse de acuerdo al caso.

Las oficinas y Sucursales del banco que administren efectivo y documentos valores en general, deben cumplir con las normas de seguridad física, electrónica y de procedimientos establecidos.

En lo que respecta a Bóveda en Tesorería, Sucursales, Ventanillas y Sitio Alterno, cuentan con medios de detectores sísmicos controlados, reciben mantenimiento de forma periódica, con el fin de mantenerlos en óptimas condiciones.

Auditoría Interna verifica la aplicación de esta política en cuanto a accesos físicos y electrónicos y el cumplimiento y observación de las medidas de seguridad establecidas.

#### **4.1.19 Auditoría Interna**

La función de auditoría es realizada por la Dirección de Auditoría Interna del Banco, la que administrativa y funcionalmente depende del Comité de Auditoría.

El Director de Auditoría debe participar en los comités de auditoría, riesgo y tecnología y el comité administrador de contingencias.

Esta dirección apoya su gestión en un vice gerente de auditoría que tiene bajo su cargo tres auditores supervisores y auditores, para desarrollar las auditorías informáticas y apoyar las auditorías de procesos cuenta con un vice gerente de auditoría de sistemas con el apoyo de dos auditores de sistemas.

El marco para la labor de auditoría interna se basa en las Normas Internacionales para la Práctica Profesional de la Auditoría Interna (The IIA), las disposiciones de la Norma de Control y Auditoría Interna, emitida por la Superintendencia de Bancos y de Otras Instituciones Financieras (SIBOIF) y en su defecto, en lo que aplique, con las Normas Internacionales de Auditoría (NIAs). Además en las mejores prácticas como ITIL, COBIT, ISO 27001 y COSO.

El alcance de auditoría para el seguimiento del riesgo operacional incluye:

- Aprobación de Política de Gestión de Riesgo Operacional y su respectivo Manual de Procedimiento.
- Seguimiento a comunicaciones entre la Unidad responsable de la Gestión Integral de Riesgo y la Superintendencia de bancos en relación a la implementación de la Gestión de Riesgo Operacional.
- Envío de reportes trimestrales de avance concernientes a la implementación de la Norma de Gestión de Riesgo Operacional.

#### ***5.5.1.1 Auditoría de Sistemas:***

El enfoque de las auditorías de sistemas es el siguiente:

Los procesos de negocio reciben soporte o están estrechamente vinculados con aplicaciones de tecnología de información. Las aplicaciones de TI y la infraestructura tecnológica que utilizan para operar, son administradas por procesos informáticos. Por lo que se realizan dos tipos de auditorías: Auditorías de Aplicaciones y Auditorías de procesos de TI.

#### ***5.5.1.2 Auditorías de aplicaciones.***

Orientada a la revisión de las aplicaciones asociadas con los procesos de negocios críticos que impactan la información financiera (controles de aplicación) enfocada a tecnología de la información.

# Auditoría de procesos y sistemas

## Proceso de Identificación y pruebas de controles de Aplicación



### 5.5.1.3 Auditorías de Procesos de TI.

Orientada a la revisión de procesos de TI relevantes para las aplicaciones (controles generales) y los componentes de la infraestructura que podría comprometer la integridad y el procesamiento de los datos.

## Controles Generales de TI

Administración de Riesgos	<ul style="list-style-type: none"> <li>• Metodología, eventos de pérdida, matriz de riesgos y controles, Gobierno TI.</li> </ul>
Planeación y Organización de TI	<ul style="list-style-type: none"> <li>• Planificación, gestión de proyectos, metodología, cumplimiento y Gobierno TI.</li> <li>• Organigrama, descriptores, gestión de los recursos humanos.</li> </ul>
Controles Generales de TI	<ul style="list-style-type: none"> <li>• Políticas, planes y capacitación en seguridad.</li> <li>• Monitoreo, medios removibles, computación móvil, redes, seguridad física.</li> </ul>
Perfiles de Usuarios	<ul style="list-style-type: none"> <li>• Administración de usuarios, documentación de cambios, pistas de auditoría.</li> </ul>
Administración de Bases de Datos	<ul style="list-style-type: none"> <li>• Administración, seguridad, control de accesos, monitoreo, respaldos, pistas, cierres.</li> </ul>
Cambios a Sistemas	<ul style="list-style-type: none"> <li>• Análisis y desarrollo (procedimientos y documentación de cambios)</li> <li>• Pruebas, certificación y distribución.</li> </ul>
Administración de problemas e incidentes	<ul style="list-style-type: none"> <li>• Solicitud, asignación y atención de requerimientos (registro).</li> <li>• Monitoreo</li> </ul>
Plan de contingencia ante desastres	<ul style="list-style-type: none"> <li>• Continuidad del Negocio (Respaldos, ANS, Seguros)</li> <li>• Continuidad del Servicio (BCP, DRP, Gobierno)</li> </ul>

En los informes emitidos del último año, se destinó un 53% de tiempo al plan horas/hombres para las evaluaciones de riesgo operacional de las cuales, 8 auditorías de sistemas (perfiles de usuarios, administración de bases de datos, controles generales de seguridad de TI, organización y planeación de TI, administración de riesgo de TI, administración de cambios a los sistemas, administración de problemas e incidentes), 38 auditorías a sucursales, en estas se aplica la matriz de riesgo, controles y pruebas a controles de los procesos de caja, por medio del cual se identifica el subproceso, funcionario a cargo, procedimiento ¿qué se hace?, descripción del proceso ¿Cómo lo hacen?, porque o para que lo hacen, riesgo, consecuencia, riesgo inherente, control (tipo), pruebas de controles (manuales, automáticos), resultados de las pruebas y finalmente se determina el riesgo residual.

## **VI. Conclusión.**

Podemos concluir que las entidades bancaria que cuenta con la correcta implementación de las normas de la SIBOIF sobre gestión de Riesgo Operacional y los acuerdos de Basilea II, mediante la publicación de los principios sobre “prácticas sanas para la administración y supervisión del RO”, han aportado a que la institución maximice sus recursos: humanos, tecnológicos, de crédito, y de liquidez, debido a la interrelación que existe entre riesgo operacional con los demás riesgos.

Este caso práctico fue basado en un modelo de auditoría operativa, y adaptado al riesgo operativo del banco meramente para fines didáctico lo cual no representa la situación real del BDF.

BDF cuenta con políticas y procedimientos para la administración del riesgo operacional, estas incluyen la metodología de identificación y evaluación de procesos con sus respectivos controles claves y planes de mitigación, según sea el caso. En el presente año están reevaluando sus procesos e integrándolos en una herramienta de gestión que permite a cada área funcional ingresar los eventos e incidentes de pérdidas con la finalidad de realizar ejercicios de cuantificación para capital por riesgo operacional y mejora de procesos. Por la importancia que reviste en la institución, la medición del riesgo está valorándose incluirla en el desempeño de cada área. En general cuenta con una ruta definida. Por ser un tema en proceso, es necesario dar seguimiento para conocer de sus avances. Tiene un mapa de procesos, que lo actualizan continuamente, cuyo criterio de definición de criticidad está en función de su estrategia institucional.

La gerencia de calidad y el comité de calidad garantizan este procedimiento. Banco no con una estrategia tecnológica de largo plazo. La Dirección de tecnología se inserta como área de apoyo en la estrategia de negocios de la institución diseñada para un horizonte no mayor de 3 años.

La institución bancaria cuenta con una política de gestión de compras y proveedores que incluye desde la selección hasta la compra y recepción del bien o servicio. El control de esta política está a cargo de la gerencia administrativa a través de mecanismos de monitoreo y evaluación de los servicios tercerizados el que realizan en conjunto con las áreas funcionales.

Aunque no se observaron proveedores de servicios relacionados al banco, la política de proveedores de servicios no contiene una política para el tratamiento con relacionados, aunque la política define que los proveedores de alto riesgo deben presentar estados financieros actualizados, éstos no son analizados.

El banco cuenta con un marco de gestión para la seguridad de la información, además ha destinado los recursos (herramientas y personal) para su implementación. El marco de gestión de seguridad de la información ha sido implementado y es actualizado en base a mejores prácticas aplicables.

La Dirección de Auditoría cuenta con procedimientos para comprobar que el sistema de control interno del banco está funcionando adecuadamente, entre estos están la utilización de la matriz de riesgo y control, riesgo de fraude, calificaciones de riesgo de las sucursales, pruebas analíticas, pruebas de controles de aplicación, pruebas de recorrido y pruebas detalladas.

La Unidad de Auditoría Interna mantiene un porcentaje importante de su plan de trabajo para la evaluación de riesgo operacional del banco, emitiendo sus recomendaciones en cada caso.

Auditoría Interna ha recibido mucho apoyo de la Junta Directiva para la ejecución de su labor y realiza una labor independiente, con respaldo del Comité de Auditoría en cuanto a recursos, capacitación y ejecución de sus recomendaciones por parte de las áreas funcionales.

En Nicaragua las disposiciones normativas dictada por la SIBOIF, son de gran avance ya que propician la implementación de acciones de RO, la Norma de gestion del riesgo operacional estipula que las instituciones apliquen la metodología existente para medir el riesgo, conformando las base de datos en función de las líneas de negocios, así como la implementación de sistemas de gestion de riesgo. La asimilación, preparación e implementación de la gestion de riesgo operacional en la práctica por parte de las instituciones financieras es un proceso complejo, minucioso y costoso pero gestionable.

Para finalizar, se considera que una vez establecida la política, estrategia de administracion del RO, se evaluarán los riesgos a todo tipo de producto, actividades, procesos y sistemas, contribuyendo a una mejora de la eficiencia de los procesos, la rentabilidad de la solidez y solvencia de las entidades financieras, arrojando en consecuencia beneficios positivos para la estabilidad del banco.

## **VII. Bibliografía.**

**Comité de Supervisión Bancaria de Basilea, Principios Básicos para una supervisión bancaria eficaz; Octubre de 2006.**

**NORMA SOBRE LA ADMINISTRACIÓN INTEGRAL DE RIESGOS, RESOLUCIÓN No CD-SIBOIF-423-1-MAY30-2006, Publicada en La Gaceta No. 124 del 27 de Junio del 2006.**

**NORMA SOBRE GESTIÓN DE RIESGO OPERACIONAL, RESOLUCIÓN N° CD-SIBOIF-611-1-ENE22-2010, Aprobada el 22 de enero de 2010, Publicada en La Gaceta No. 64 del 08 de Abril del 2010.**

**Prospecto Banco de Finanzas, S.A. (BDF), PROGRAMA DE EMISION DE VALORES ESTANDARIZADOS DE RENTA FIJA OFERTA PÚBLICA, Acta de Junta Directiva No. 243 del 24 de septiembre de 2013, Inscripción No. 0379, Resolución No. 0382 del 20 de noviembre de 2013.**

**Superintendencia de Bancos y de Otras Instituciones Financieras, “Informe de Gestión, Año 2015”**

## VIII. Anexos

Ejemplo de método estándar de una supervisión bancaria en las líneas de negocio.

TABLA 1.

BIA	Ingreso Anual Bruto (GI)				Pri	Fa	Capit
	Lineas de negocios	2013	2014	2015			
Ingreso brutos anuales positivos	1	1	2	186	15	2797	
	5620	7977	2321	39	.00%		
Total	1	1	2	186		2797	
	5620	7977	2321	39			

Tabla 2

STDAOp	Ingreso Anual Bruto (GI)				P	F	Cap
	Lineas de negocio	2013	2014	2015			
Finanzas Corporativas	0	0	3	1	1	2	
			0	0	8		
Negociación y ventas	5	78	1	1	1	192	
	65	1	846	064	8		
Pagos y	7	91	1	9	1	164	

Liquidación	55	8	062	12	8	
Banca Comercial	4	50	6	5	1	790
	532	35	226	264	5	
Servicios de Agencias	-	-	-	-	1	0
					5	
Banca Minorista	9	11	1	1	1	134
	600	096	2994	1230	2	8
Administración de Activos	1	14	1	1	1	20
	69	7	83	66	2	
Intermediación Minorista	-	-	-	-	1	0
					2	
<b>Total</b>	<b>1</b>	<b>17</b>	<b>2</b>	<b>1</b>		<b>251</b>
	<b>5620</b>	<b>,977</b>	<b>2 341</b>	<b>8 639</b>		<b>5</b>

TABLA 1.

**RWA=Capital requerido x 12.5**

**2797 x 12.5= 34, 949.**

TABLA 2.

**RWA= Capital requerido x 12.5**

**2, 515 x 12.5=31, 438.**

**BDF**