AAQ1464

Universidad Católica Andrés Bello

TESIS
IF2004
P47

CARACAS UNIVERSIDAD CATÓLICA ANDRÉS BELLO
ESTUDIOS DE POSTGRADO
POSTGRADO EN INSTITUCIONES FINANCIERAS

Definición e Implantación de políticas y Cultura de Riesgo Operacional en el Banco de Venezuela/Grupo Santander.

PEDRO PABLO PERNÍA MADRID V. 10.110.230
PROFESOR GONZALO BELLO

TRABAJO ESPECIAL DE GRADO
PRESENTADO COMO REQUISITO PARA
OPTAR AL TÍTULO DE
ESPECIALISTA EN INSTITUCIONES FINANCIERAS.
MENCION FINANZAS INTERNACIONALES
JULIO 2004

Contenido

Introducción 1
CAPÍTULO I: ASPECTOS INTRODUCTORIOS 4
1. Planteamiento del problema 4
2. Objetivos 5
2.1. Objetivo General 5
2.2. Objetivos Específicos 5
3. Marco metodológico 5
CAPÍTULO II: MARCO TEÓRICO 6
1. Resolución No. 136.03 de la Superintendencia de Bancos y otras Instituciones Financieras 6
2. Retos Frente a la Administración Integral de Riesgos 7
3. Como las instituciones financieras afrontan exitosamente la administración integral de riesgos 9
4. Definición de Riesgo Operacional 10
5. Categorías BIS II de Riesgo Operacional 11
6. Categorías Internas de Riesgo Operacional del Grupo Santander 17
CAPÍTULO III: DESARROLLO 22
1. Políticas de Riesgo Operacional 22
2. Creación e Implementación de Estructura Organizativa y Funcional 26
3. Niveles de Control 36
3.1. Control a Nivel Individual 37
3.2. Control de la Dirección 37
3.3. Control de Unidades Especializadas 38
3.4. Control de Entidades Externas 39
4. Controles Generales de Riesgo Operacional 39
5 Herramientas para la Implementación de Cultura del Riesgo Operacional 51
5.1. Herramientas Cualitativas 52
5.1.1. Mapas de Riesgo Operacional 52
5.1.2. Cuestionarios de Autoevaluación 53
5.1.3. Indicadores de Riesgo Operacional 54
5.1.4. Matrices de Riesgo Operacional 57
5.1.5. Diagramas de Flujo (procesos y controles) 58
5.1.6. Organigramas Funcionales 58
5.2. Herramientas Cuantitativas 59
5.2.1. Estadísticas de Actividad 59
5.2.2. Base de Datos de Errores e Incidencias 60
Conclusión y Recomendación 63
Bibliografía 67

Introducción:

El Comité de Supervisión Bancaria de Basilea es uno de los diversos comités que forman parte del Banco de Pagos Internacionales, Organización que fue fundada en 1930, tratándose de la organización financiera internacional más antigua del mundo, tiene su sede en Basilea, y se define así misma como "una organización internacional que fomenta la cooperación monetaria y financiera a escala internacional y realiza la función de banco para bancos centrales.

Este Comité es un foro de debate sobre la supervisión bancaria cuyo fin es "garantizar una supervisión eficaz de las actividades bancarias en todo el mundo".

El Nuevo Acuerdo de Capital (Basilea II) es una regulación bancaria que propone a las entidades financieras afinar al máximo en medición y gestión de riesgos y cuya aplicación está prevista para el año 2006.

La reciente propuesta del Comité de Supervisión Bancaria de Basilea, tiene como objetivo adecuar los niveles de requerimientos mínimos de capital de

las entidades financieras a la creciente sofisticación de las operaciones bancarias y de los mercados financieros. Tiene tres pilares:

Requerimientos mínimos de capital: define nuevas reglas para el tratamiento del riesgo de crédito, definiendo tres opciones distintas para el cálculo del Riesgo de crédito y fija, por primera vez, requisitos de capital por Riesgo Operacional. El riesgo de mercado no sufre cambios significativos en relación con la enmienda al Acuerdo de Capital de 1996 (Basilea I).

Examen supervisor de la suficiencia de capital: apunta a la necesidad de los bancos de evaluar sus posiciones de suficiencia de capital con respecto a sus riesgos globales, así como la de los supervisores para examinar y adoptar las medidas adecuadas como respuesta a dichas evaluaciones.

Disciplina de mercado/Divulgación pública: establece la obligación de la transparencia informativa sobre el perfil de riesgo de las instituciones financieras y sobre su nivel de capitalización.

La Superintendencia de Bancos en Venezuela emitió una Resolución en la que exige identificar, medir y controlar estos riesgos. Existe poca experiencia en el tratamiento y medición de los riesgos operacionales

Las Instituciones Financieras están instalando sus departamentos de Riesgos Operacionales en el entendido que la identificación y medición de éstos, puede mejorar su control y mitigación, generando un efecto positivo en los resultados y en el valor del negocio

El Riesgo Operacional se define de acuerdo al BIS como "la pérdida resultante de deficiencias o fallos de los procesos internos, recursos humanos o sistemas, o aquellas derivadas de circunstancias externas" y está incluido como una nueva modalidad de riesgo dentro del nuevo acuerdo de capital de Basilea (Basilea II).

En el presente trabajo se exponen los conceptos básicos para la implantación de políticas y cultura de Riesgo Operacional en una institución financiera, específicamente en el Banco de Venezuela Grupo Santander. Así como la estructura organizativa y funcional. Adicionalmente, se plantean los nivel de control necesarios y las herramientas para la evaluación de dicho riesgo.

Pese que al Comité de Supervisión Bancaria de Basilea no Incluye el riesgo estratégico y reputacional en esta definición, el Grupo Santander ha determinado que la gestión y control del riesgo reputacional será responsabilidad de la Unidad de Riesgo Operacional.

CAPÍTULO I: ASPECTOS INTRODUCTORIOS

1. Planteamiento del problema.

El Comité de Supervisión Bancaria de Basilea ha establecido un nuevo marco de gestión y control de los riesgos, así como de capital exigible a los Bancos, que se recoge dentro del documento consultivo para el Nuevo Acuerdo de Capital (BIS II). En él se señala al Riesgo Operacional como el tercer riesgo a tener en cuenta dentro de los tres pilares definidos: requerimientos mínimos de capital, revisión de los Supervisores, y disciplina de mercado. Esto supone un cambio importante, ya que los Bancos tendrán que incluir el Riesgo Operacional dentro de su estructura de control y gestión de los riesgos, y el mismo tendrá una incidencia importante en el cálculo de los requerimientos mínimos de capital.

En el Banco de Venezuela/Grupo Santander se requiere del establecimiento de cultura de riesgo operacional debido a la imperante necesidad del cumplimiento de la Resolución SUDEBAN No. 136.03 del 29/05/2003 "Normas Para una adecuada Administración de Riesgo".

2. Objetivos.

2.1. Objetivo General:

Definir e implementar las políticas y una cultura de Riesgo Operacional en el Banco de Venezuela/Grupo Santander para el conocimiento de las medidas de control general que los mitigan y eliminen.

2.2. Objetivos Específicos:

2.2.1. Definir los controles, asignación de funciones y responsabilidades a todos los niveles de la estructura organizacional.

2.2.2. La obtención veraz y consistente de la información entre todas las Divisiones y Áreas del Banco.

3. Marco metodológico.

La metodología a utilizar será la realización de un estudio teórico del tema a través de libros, revistas, artículos de prensa, y la normativa de la Superintendencia de Bancos y otras instituciones Financieras sobre la adecuada administración integral de riesgos. Adicionalmente, se recurrirá a las publicaciones de Internet, trabajos de investigación que manejan empresas consultoras, informes y presentaciones del Banco de Venezuela y del Grupo Santander a nivel Mundial, sobre riesgo operacional.

CAPÍTULO II: MARCO TEÓRICO

1. Resolución No. 136.03 de la Superintendencia de Bancos y otras Instituciones Financieras.

En Venezuela, la Superintendencia de Bancos y Otras Instituciones Financieras emitió la Resolución Bancaria 136.03 "Normas para una Adecuada Administración Integral de Riesgos" publicada el 3 de junio de 2003 en la Gaceta Oficial No. 37.703, la cual tiene por objeto, establecer los lineamientos básicos, que deben observar las instituciones financieras venezolanas en la implantación de un proceso de administración integral de riesgos en el sector bancario. El ámbito de los riesgos que contempla la resolución se presenta en la figura "Diferentes Riesgos en el Sector Bancario":

Bajo este nuevo entorno, las entidades financieras venezolanas se han visto en la necesidad de desarrollar estructuras funcionales para la administración integral de riesgos, así como políticas, procedimientos,

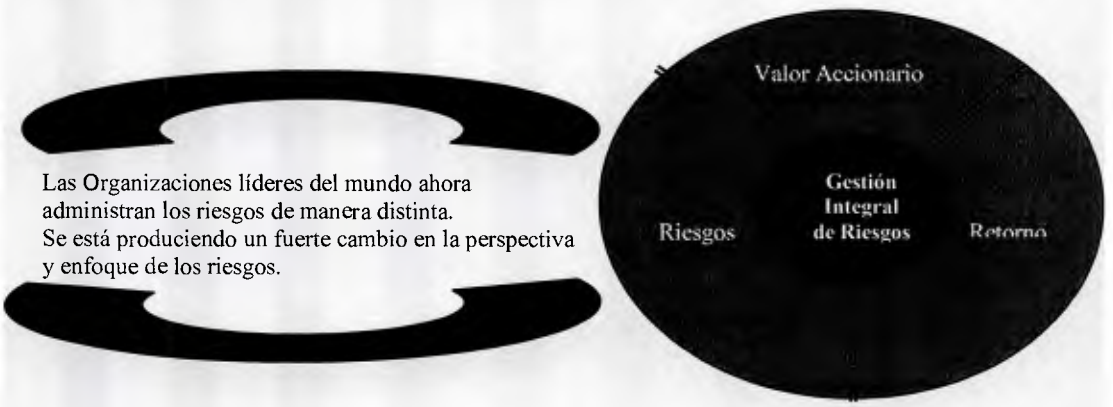
metodologías y herramientas (cualitativas y cuantitativas) que permitan identificar, medir, monitoriar, controlar, informar y revelar claramente los diferentes tipos de riesgos a los cuales están expuestas las instituciones financieras y, por ende, velar por el patrimonio que ellas representan.

Cada institución financiera seleccionará y desarrollará los métodos de gestión de riesgos que consideren más adecuados al grado de crecimiento de las operaciones del negocio, a la infraestructura del banco y al mercado financiero. Lo importante es determinar de manera consistente el impacto de los distintos riesgos en la cuenta de resultados de la entidad, aprovechando la base de conocimientos, lineamientos y técnicas de medición de riesgos propuestos por las mejores prácticas, tal como Basilea II, con una óptica global de integración y convergencia entre capital económico y regulatorio.

2. Retos Frente a la Administración Integral de Riesgos.

Los retos para la implantación de un enfoque integral de riesgos evolucionan a medida que las entidades y las regulaciones avanzan en la integración de los riesgos. Sin embargo, existen dos (2) principales a considerar:

El primer reto de las instituciones financieras es que la administración integral de riesgos sea un centro de beneficio y no de costos, capaz de incrementar el valor accionario, tal como se indica en la figura "Retos en la Administración Integral de Riesgos" a continuación:



El Segundo reto que deben afrontar las instituciones financieras venezolanas está relacionado con el cumplimiento de la Resolución Bancaria 136.96, por lo que es imperante disponer de estructuras adecuadas y avanzar en la implantación de modelos cuantitativos, mediante herramientas de apoyo a la toma de decisiones (ratings, scorings, entre otros) o en nuevos sistemas corporativos de medición de riesgo.

A estos dos grandes retos se les adiciona, el sostenimiento de la infraestructura de riesgo y la creación de una cultura de riesgo y control en todos los niveles de la institución, a fin que se establezcan criterios

consistentes y homogéneos de gestión de riesgos y claros roles y responsabilidades.

3. **Como las instituciones financieras afrontan exitosamente la administración integral de riesgos.**

Las organizaciones exitosas enfrentan los retos y aprovechan las oportunidades que ellos representan. En este sentido, para administrar efectivamente los riesgos las instituciones financieras necesitan de un marco de gestión que provea una manera de engranar la gestión del riesgo, los objetivos del negocio, las diferentes maneras de visualizar el riesgo, cómo éste debería ser controlado de acuerdo a las mejores prácticas y cómo los diferentes elementos deberían estar alineados con todos los niveles de la institución.

Modelo Organizativo y estrategia de gestión integral de riesgos

1

Desarrollo de un modelo Organizativo y estrategia que garantice la independencia de la unidad de riesgos, promueva el involucramiento de la Alta Dirección y establezca claras funciones y responsabilidades en los procesos de gestión de riesgos de la entidad. Además, implica la creación de una cultura de riesgo como elemento clave.

Políticas y procedimientos de gestión integral de riesgos

2

Definición de políticas y procedimientos de gestión integral de los riesgos, incluyendo establecimiento de límites, controles periódicos, informes de gestión y modelos de asignación de capital y evaluación de rentabilidad ajustada al riesgo.

Identificación, evaluación, medición y seguimientos de riesgos	3	La identificación, evaluación, medición de los riesgos incluye que se cuantifiquen los mismos, utilizando medidas estadísticas consistentes que permitan unir la medición del riesgo con los requerimientos de capital. Asimismo, involucra la supervisión de las áreas de negocios con mayor exposición a la materialización de los riesgos.
Implantación y mantenimiento del sistema.	4	La fase final incluye el desarrollo de una infraestructura tecnológica adecuada que promueva la integración de las distintas aplicaciones, centralización de las fuentes de datos, integridad de la información y herramientas de reportes integrales.

4. Definición de Riesgo Operacional.

La definición generalmente aceptada de Riesgo Operacional, tal y como se contempla en los últimos documentos elaborados por el Comité de Basilea, es la siguiente:

"Es el riesgo de incurrir en pérdidas como consecuencia de deficiencias o fallos de los procesos internos, recursos humanos o sistemas, o bien derivado de circunstancias externas".

Incluye el Riesgo Legal, el cual consiste en la posibles perdidas a consecuencia de incumplir con el aspecto legal o regulatorio, pero no el

Riesgo Estratégico ya que éste se encuentra inmerso en la planificación estratégica y toma de decisión, vinculados con la visión y misión. No

obstante, la propia definición del Grupo Santander también incluiría el Riesgo Reputacional, el cual se basa en las relaciones de compañías que se interrelacionan directamente con la operación, por lo que se considera como parte integrante del Riesgo Operacional.

Al tratarse de una definición muy amplia, es conveniente que señalemos las diferentes clases de Riesgo Operacional de forma que podamos conocer con más detalle los riesgos que engloba.

5. Categorías BIS II de Riesgo Operacional.

Basilea establece una clasificación general en 7 grandes tipos de sucesos de Riesgo Operacional (primer nivel) :

Fraude Interno: Actos que de forma intencionada buscan defraudar, apropiarse indebidamente de activos propiedad del Banco, soslayar regulaciones, las leyes o políticas de la entidad, excluyendo los sucesos de discriminación o diversidad laboral, y que implican al menos a una persona del Banco. Algunos ejemplos serían la falta de reporting de posiciones de forma intencionada, el robo por parte de personal, y la negociación indebida por cuenta del propio empleado.

Fraude Externo: Actos cometidos por personas ajenas al Banco, que intentan defraudar, apropiarse indebidamente de activos propiedad del Banco y soslayar las leyes. Algunos ejemplos serían el robo, falsificaciones, y los daños por violación de la seguridad de los sistemas.

Prácticas de Empleo, Salud y Seguridad en el Trabajo: Actos inconsistentes con las leyes o acuerdos de seguridad y salud en el trabajo, los cuales resultan en reclamaciones por daños personales o reclamaciones relacionadas con la discriminación o falta de diversidad laboral. Algunos ejemplos incluyen compensaciones o indemnizaciones a trabajadores, violaciones de las reglas de salud y seguridad en el puesto de trabajo, actividades sindicales, reclamaciones por discriminación y acondicionamiento general de las instalaciones (por ejemplo, al resbalar un cliente y caer en una oficina).

Prácticas con Clientes, Productos, y de Negocio: Fallos inintencionados o negligentes que impiden satisfacer una obligación profesional con los clientes (incluidos los requerimientos fiduciarios y de adecuación), o por la naturaleza o diseño de los productos. Algunos ejemplos incluyen errores de tipo fiduciario, uso de información privilegiada, negociación inadecuada por cuenta del Banco, blanqueo de dinero y venta de productos no autorizados.

Daños en Activos Físicos: Pérdidas o daños en activos físicos debido a desastres naturales u otros sucesos. Algunos ejemplos incluyen terrorismo, vandalismo, terremotos, incendios e inundaciones.

Interrupción del Negocio y Fallos en los Sistemas: Son todas las interrupciones que se producen en el negocio por motivos tecnológicos y fallos en los sistemas. Algunos ejemplos incluyen fallos de software y hardware, problemas de telecomunicaciones y faltas o caídas de suministros.

Ejecución, Entrega y Gestión de los Procesos: Fallos en el procesamiento de las transacciones o en la gestión de los procesos, así como en las relaciones con contrapartes financieras y vendedores. Algunos ejemplos incluyen errores de imputación de datos, fallos en la gestión de colaterales, documentación legal incompleta, acceso no autorizado a cuentas de clientes, gestión incorrecta con contrapartes financieras y disputas con vendedores.

Para facilitar la identificación de los sucesos, BIS II subdivide las 7 categorías iniciales (nivel 1) en subcategorías (nivel 2) y ejemplos concretos de los sucesos que pueden terminar produciendo pérdidas por Riesgo Operacional, se presenta el siguiente cuadro:

Categorías (Nivel 1)	Subcategorías (Nivel 2)	Ejemplos Actividad (Nivel 3)
Fraude Interno	Actividad No Autorizada	• Transacciones no informadas (intencionalmente) • Transacciones no autorizadas (intencionalmente) • Falseamiento de posiciones (intencionalmente)
	Robo y Fraude Interno	• Fraude, Fraudes de crédito, Depósitos sin valor, Robo, Extorsión, Malversaciones, • Apropiación indebida de activos, Destrucción intencionada de activos, • Falsificaciones, Contrabando, Apropiación de cuentas, Suplantación de personalidad, Incumplimientos fiscales, Evasión fiscal, • Sobornos, Actividades de trading realizadas por cuenta del operador
Fraude Externo	Robo y Fraude Externo	Robo, Fraude, Falsificaciones, Rueda de cheques, Papel colusión, etc.
	Seguridad de Sistemas	Piratería informática, Robo de información
Prácticas de Empleo y Seguridad en el Trabajo	Relaciones Laborales	Compensación, Beneficios, Indemnizaciones, Finalización de la relación laboral, Actividades sindicales
	Seguridad del Ambiente Laboral	Responsabilidades generales (caídas, resbalones, heridos,...), Normas de seguridad y salud laboral, indemnizaciones

Categorías (Nivel 1)	Subcategorías (Nivel 2)	Ejemplos Actividad (Nivel 3)
	Diversidad y Discriminación	Todo tipo de discriminación laboral
Prácticas con Clientes, Productos, y de Negocio	Adecuación, Confidencialidad, Fiduciario	Incumplimientos fiduciarios, Violación de instrucciones del cliente, Adecuación, Violación de confidencialidad de los clientes, Privacidad, Ventas agresivas, Manipulación de cuentas, Utilización de información privilegiada
	Prácticas Inadecuadas de Negocio o Mercado	Leyes antitrust, Prácticas inadecuadas de contratación o de mercado, Manipulación de los mercados, Actividades de Trading realizadas por cuenta de la empresa, Actividades sin licencia, Blanqueo de dinero
	Productos Defectuosos	Productos y Modelos con defectos (no autorizados, etc.)
	Selección, Patrocinio y Exposición	Fallos de detección de las instrucciones del cliente, Excesos en los límites del cliente
	Actividades de Asesoramiento	Disputas derivadas de las actividades de asesoramiento
Daños en Activos Físicos	Desastres y Otros Sucesos	Pérdidas por desastres naturales, Pérdidas humanas por sucesos externos (terrorismo, vandalismo, ...)

Categorías (Nivel 1)	Subcategorías (Nivel 2)	Ejemplos Actividad (Nivel 3)
Interrupción del Negocio y Fallos en los Sistemas	Sistemas	Equipos informáticos (hardware), Programas informáticos (software), Telecomunicaciones, Caídas o interrupciones de electricidad
Ejecución, Entrega y Gestión de los Procesos	Captura de Transacciones, Ejecución y Mantenimiento	Errores en la comunicación de operaciones, Errores de carga, Entrada y mantenimiento de los datos, Incumplimiento de plazos y responsabilidades, Mal funcionamiento de los sistemas o modelos, Errores contables, Errónea asignación a entidad, Otros errores operativos, Fallos de entrega, Fallos en la gestión de colaterales, Mantenimiento de datos estáticos
	Seguimiento e Información	Incumplimiento de las obligaciones de información, Informes externos inexactos
	Incorporación de Clientes y Documentación	Permisos de clientes, Falta de cláusulas de no responsabilidad, Falta de documentación legal o datos incompletos
	Clientes, Gestión de Cuentas de Clientes	Accesos inapropiados a cuentas, Información incorrecta de clientes, Pérdidas por negligencia o daños a activos de clientes
	Contrapartidas Financieras	Errores con contrapartidas financieras, Disputas con contrapartidas financieras
	Vendedores y Proveedores	Externalización de servicios, Disputas de vendedores

6. Categorías Internas de Riesgo Operacional del Grupo Santander.

Desde otra perspectiva más didáctica, y sin perjuicio de la clasificación y definiciones formales citadas anteriormente, podemos clasificar el Riesgo Operacional atendiendo a las causas concretas que lo generan, y que constituyen las categorías internas de Riesgo Operacional establecidas por el Grupo. De este modo, partiendo de las 7 categorías iniciales definidas por Basilea, se han incorporado 4 categorías adicionales:

Fraude Interno: fraude interno es todo acto cometido por el personal, de forma consciente, en el que incurre en prácticas o procesos que no son legales o no están autorizados, anteponiendo sus intereses personales a los de la Organización. Aquí se incluirían, por ejemplo, todo tipo de actividades u operaciones realizadas por el personal que no están autorizadas o informadas, falsificaciones, el robo y la malversación de fondos, sobornos, fraudes con tarjetas, violaciones en la seguridad de los sistemas informáticos, e incumplimientos y evasiones de tipo fiscal, legal o falseamientos contables.

Fraude Externo: por fraude externo entendemos todo acto cometido por personas ajenas a la Organización. Aquí se incluirían, por ejemplo, todo tipo de falsificaciones (firmas, importes, billetes,...), robos, ruedas de

cheques o papel colusión, fraudes con tarjetas, destrucción de activos o sabotajes, y violaciones de la seguridad de los sistemas.

Prácticas de Empleo, Salud y Seguridad en el Trabajo: aquí se incluirían todos aquellos sucesos que tienen su origen en los incumplimientos de las relaciones laborales por parte de la Organización (relativas a acuerdos de compensación y beneficios, convenios colectivos, etc.), de las normas de seguridad y salud en el puesto de trabajo, y todo tipo de discriminación laboral por motivo de raza, sexo, religión, aspectos políticos, culturales o socio-económicos.

Prácticas con Clientes, Productos, y de Negocio: en esta categoría, por ejemplo, se incluirían todos los sucesos originados por las actividades de selección de clientes, negociación y comercialización, y que comprenderían la contratación con clientes o proveedores no autorizados, la comercialización de productos erróneos, actividades de asesoramiento y comunicación, uso de modelos erróneos, realización de prácticas incorrectas de mercado, manipulación de mercados, contratación de operaciones en términos o límites incorrectos beneficiosas para la Organización, violaciones de la confidencialidad o privacidad, utilización de información privilegiada, así como incumplimientos administrativos y

de normativa, códigos de conducta internos, blanqueo de dinero, y cuestiones de cumplimiento en general.

Daños en Activos Físicos: en esta categoría se incluirían todos los sucesos que tienen su origen en daños producidos a los Activos Físicos de la Organización (edificios, instalaciones,...) por catástrofes naturales, accidentes, terrorismo y actos vandálicos.

Interrupción del Negocio y Fallos en los Sistemas: aquí se incluirían todas las interrupciones que se producen en el negocio por motivos tecnológicos y fallos en los sistemas. Son sucesos relacionados con la tecnología y con la gestión de la información en los sistemas. Los riesgos tecnológicos son de varios tipos, pero siempre se originan por una estrategia y arquitectura tecnológica inadecuada, el suministro de soluciones informáticas poco probadas, y una gestión incorrecta de los sistemas de explotación y apoyo. Los riesgos de la información se producen por la falta de integridad y calidad de la información por fallos en los sistemas, el incorrecto suministro de la información o su falta de disponibilidad. Entre ellos podemos señalar la interrupción en el ciclo de procesamiento de la información o de las transacciones debido a fallos o caídas en los sistemas informáticos y de comunicaciones (hardware, software, telecomunicaciones). Estos riesgos se minimizan con la

existencia de Planes de Contingencia Informáticos (programas y sistemas alternativos, copias de seguridad, etc.).

Ejecución, Entrega y Gestión de los Procesos: son los sucesos originados por deficiencias o fallos en los procesos internos o bien en el procesamiento de las transacciones y su control. Normalmente se deben a una falta de procesamiento, procesamiento incorrecto o tardío, a una información incorrecta, o insuficiente soporte legal. Estos riesgos dependerán de las características del Área, en función de que se trate de un Área de negocio o de apoyo, pero siempre aparecen como consecuencia de fallos en los controles o bien porque éstos son insuficientes a lo largo de las fases del ciclo Operacional. Como ejemplo, podemos señalar las siguientes fuentes: la ejecución errónea en el mercado; el inadecuado registro, imputación y mantenimiento de datos estáticos; las demoras en operaciones o servicios; los fallos en la verificación de datos; la falta de cuadres y conciliaciones; en la liquidación y contabilización de operaciones; el seguimiento e información de gestión; los errores en la documentación y soporte legal, en la gestión de cuentas de clientes, las disputas con contrapartes financieras y vendedores, la externalización de servicios y, en general, todos los fallos de ejecución de los procesos que no tienen una causa informática.

Cambios en el Entorno Económico - Jurídico: son los sucesos originados por cambios inesperados en la normativa legal, fiscal o contable, que provocan una necesidad de adaptación por parte de la Organización y que pueden afectar directamente al negocio y sus resultados atribuidos.

Gestión del Cambio, Nuevas Actividades y Productos: son los sucesos motivados por la falta de control y seguimiento de los proyectos de cambio en la organización, la inexistencia de estructura y sistemas suficientes para llevar a cabo las nuevas actividades y gestionar los nuevos productos, y la falta de conocimiento, valoración o aprobación de esas nuevas actividades o productos.

Estructura Organizativa: son los sucesos que tienen su origen en la existencia de una inadecuada estructura organizativa, bien por una incorrecta segregación de funciones, duplicidad o por una falta de transparencia y flujo de la información entre todas las partes o Áreas de la Organización.

Adecuación de Recursos Humanos: son los sucesos que tienen su causa en una inadecuada gestión de los Recursos Humanos de la Organización, ya sea en la selección del personal, en la existencia de un número insuficiente de personas para la realización de las tareas y actividades,

una excesiva rotación que perjudica los procesos, o bien porque el personal esté insuficientemente formado, desconozca la operativa, o exista una asignación ineficiente de tareas y responsabilidades.

CAPÍTULO III: DESARROLLO

1. Políticas de Riesgo Operacional.

1.1 Políticas Generales de Riesgo Operacional

La gestión del riesgo deberá formar parte integral de las responsabilidades de la Dirección, lo que se traducirá en una cultura de control, el conocimiento de los riesgos y el propio estilo de dirección.

Los gestores de cada una de las Áreas y Unidades son los que tendrán un mayor conocimiento de los procesos en sus actividades, así como de los puntos vulnerables que puedan ocasionar exposiciones importantes al Riesgo Operacional.

La Dirección, a todos los niveles, será la unidad responsable de gestionar, controlar, y mitigar los Riesgos Operacionales en sus Áreas de responsabilidad. En tal sentido, deberá existir un elevado nivel de participación de la Alta Dirección.

El Riesgo Operacional deberá ser gestionado directamente y de forma activa por cada una de las Divisiones o Áreas del Banco de Venezuela, Grupo Santander y para la totalidad de las fases del ciclo operacional, mediante la aplicación de los procesos y controles necesarios para eliminar las causas que generan los riesgos, y así minimizar las pérdidas que pudieran derivarse de los mismos.

El control del Riesgo Operacional, de forma independiente a la propia gestión, tendrá por objeto facilitar la identificación, evaluación, el seguimiento del grado de gestión, la mitigación, y en su caso la medición de los Riesgos Operacionales, para ello deberán usar las herramientas cualitativas y cuantitativas de diferente naturaleza.

Todos los empleados en cualquiera de los niveles de jerarquía deberán conocer los Riesgos Operacionales de su responsabilidad y asumir la responsabilidad que de acuerdo a sus niveles le corresponda, al atender o solucionar situaciones no previstas en las Políticas, su eficacia en la gestión y control de estos riesgos deberá formar parte de su evaluación anual. En tal sentido, las condiciones no previstas que pasen a ser recurrentes deberán ser reportadas a la consultadas con la Unidad de Riesgo Operacional y aprobadas por la Comité Integral de Riesgos para la incorporación respectiva.

1.2 Políticas Específicos de Riesgo Operacional

Las funciones y responsabilidades que se relacionan con la gestión y control del Riesgo Operacional deberán ser entendidas por la Dirección a todos los niveles, e incluirse dentro de los objetivos personales que forman parte de la evaluación anual de desempeño.

En todas las Áreas del Banco de Venezuela, Grupo Santander deberá existir un Coordinador Responsable de Riesgo Operacional o una Unidad específica responsable de controlar este riesgo.

LA VPA Gestión de Riesgo Operacional y Sistemas, es el Área encargada de coordinar la implantación de Políticas y Procesos de Riesgo Operacional en el banco y de supervisar la gestión y el control de este riesgo en el mismo.

El desarrollo e implantación de políticas y procesos para la gestión y control del Riesgo Operacional, que se basen en las mejoras prácticas, y que sean aplicadas a las características particulares de cada División o Área, es un aspecto fundamental dentro del marco establecido. Siempre que esté justificado, deberán elaborarse Manuales de Políticas y Procesos Operacionales que contemplen los Riesgos Operacionales y que sean conocidos por todo el personal.

El establecimiento de procesos y controles que garanticen la efectividad en el desarrollo de las tareas, la integridad de la información, y el cumplimiento de los requerimientos regulatorios, es básico con el fin de alcanzar los objetivos del Área y de la Organización.

La implantación de Planes de Contingencia es imprescindible, de forma que se puedan llevar a cabo todos los procesos operacionales en caso de situaciones extremas.

Existen herramientas cualitativas y cuantitativas que permitirán identificar los Riesgos Operacionales, controlarlos y reportarlos, y que facilitarán una asignación de capital por estos riesgos. Estas herramientas deberán ser utilizadas por todo el Banco de Venezuela, Grupo Santander, con base a los estándares fijados por la VPA Gestión de Riesgo Operacional y Sistemas

Todos los eventos e incidencias operativas del Grupo deberán reportarse a la VPA Gestión de Riesgo Operacional y Sistemas, mediante su incorporación en una Base de Datos de eventos e incidencias de riesgo en cada una de las áreas del Banco.

La Dirección debe optimizar las inversiones destinadas a la gestión y control del Riesgo Operacional, mediante un análisis de utilidad en donde se comparen los costes con los beneficios de dichas inversiones, su incidencia en el perfil de riesgo y en la asignación de capital correspondiente.

2. **Creación e Implementación de Estructura Organizativa y Funcional.**

   Este apartado define las funciones y responsabilidades con respecto a la gestión y control del Riesgo Operacional.

   Estas pueden agruparse en tres categorías:

   - Establecimiento de políticas.
   - Ejecución.
   - Verificación.

La Dirección ya sea a nivel del Banco o en cada una de las Áreas, será la unidad responsable de la gestión y control del Riesgo Operacional y, por tanto, será la responsable de estas tres categorías de funciones. Aunque la Dirección pueda delegar estas funciones, seguirá siendo responsable de su cumplimiento.

La estructura Organizativa y Funcional está conformada por:

Comité de Dirección del Banco.

En los documentos de trabajo, previos a la normativa definitiva de BIS II, así como en la Resolución 37.703 emitida por la Superintendencia de Bancos y Otras Instituciones Financieras relacionada con la adecuada administración del riesgo integral establecen que el Comité de Dirección del Banco (u órgano delegado) y la Alta Dirección deben estar activamente implicados en el proceso de gestión del Riesgo Operacional.

Por tanto, el Comité de Dirección precisa conocer las medidas que se toman por parte de la Alta Dirección para establecer las correspondientes políticas de riesgo, su ejecución y verificación, de forma que se alcancen los objetivos de la Organización. El Comité de Dirección deberá asegurarse que la Alta Dirección identifique, evalúe, realice el seguimiento, controle/ mitigue, y en su caso mida, todos los Riesgos Operacionales afrontados por el Grupo.

Para llevar a cabo esta supervisión, el Comité de Dirección deberá estar informado periódicamente sobre el grado de exposición y nivel de pérdidas del Banco por Riesgo Operacional.

Comité Integral de Riesgos.

En el actual esquema organizativo del Banco de Venezuela/Grupo Santander, la VPE Gestión de Riesgo, a través de la VPA Gestión de Riesgo Operacional y Sistemas, tiene la función de proporcionar periódicamente al Comité Integral de Riesgos un informe con la situación de la gestión y el control del Riesgo Operacional en el Banco.

Auditoria Interna.

El Área de Auditoría tendrá como responsabilidad, la emisión de opiniones independientes con respecto a la corrección de las políticas y los procesos, y los controles de riesgos llevados a cabo por el Banco. Así, la revisión interna suministrará a la Dirección en general todas las opiniones, análisis, y recomendaciones relativas a las actividades y el control de riesgos de las Unidades auditadas.

Sus principales funciones serán:

- Revisión del funcionamiento y adecuación de todos los procesos y sistemas utilizados en la operativa.
- Suministrar a la Dirección las recomendaciones de Auditoría para informarla de la inadecuación de los procesos, los riesgos

incurridos, y el calendario de implantación de las medidas necesarias para su corrección.

- Determinar si la información generada por los sistemas de información y los informes correspondientes satisfacen los requerimientos necesarios.

Auditoria Interna será la unidad responsable de verificar que la estructura de gestión sea adecuada y que las políticas y procesos de Riesgo Operacional se cumplan en todas las Áreas del Banco, pero no debería tener una responsabilidad directa en la gestión de este riesgo.

Por esta razón, la Auditoría Interna lleva a cabo un papel fundamental en la supervisión de la gestión de los Riesgos Operacionales, debiendo suministrar a la VPA Gestión de Riesgo Operacional y Sistemas, la información necesaria para el control de estos riesgos, incluyendo un reporte mensual de las recomendaciones realizadas y su estado de implantación.

Divisiones y Áreas.

Las respectivas Divisiones o Áreas del Banco son responsables de la gestión y control de los Riesgos Operacionales. Entre otras, tendrán las siguientes responsabilidades:

- Conocer y cumplir las políticas y procesos correspondientes a su operativa, y concretamente las relativas a la gestión y control del Riesgo Operacional.
- Nombrar a un Coordinador Responsable de Riesgo Operacional del Área.
- Identificar todos los Riesgos Operacionales.
- Facilitar toda la información que sea necesaria al Coordinador Responsable de Riesgo Operacional, de manera que pueda controlar los distintos riesgos.
- Proponer al Coordinador Responsable de Riesgo Operacional la conveniencia o necesidad de modificar los procesos y controles o bien la implantación de otros nuevos, con el fin de mejorar la operativa y el nivel de control de los riesgos.
- Colaborar con el Coordinador Responsable de Riesgo Operacional en la implantación de medidas correctoras para mitigar o eliminar los Riesgos Operacionales.
- Recibir la información periódica elaborada por el Coordinador Responsable de Riesgo Operacional para su seguimiento, análisis, y toma de decisiones.

El Comité de Basilea ha establecido, a efectos de "reporting" obligado al Supervisor, las siguientes 8 líneas de negocio:

- Banca Corporativa

- Tesorería
- Banca Minorista
- Banca Comercial
- Operaciones Bancarias
- Agency Services (Servicios de Agente de Pagos y Custodia)
- Asset Management (Gestion de Activos)
- Retail Brokerage (Intermediación Minorista)

Sin embargo, existirán otras áreas en el Banco cuya información de soporte será especialmente importante desde el punto de vista del Riesgo Operacional:

- Auditoría Interna
- Recursos Humanos, Inmuebles, Seguridad, Tecnología, Soporte Red Comercial, Operaciones de Tesorería
- División Financiera (Control de Gestión, Intervención General,...)
- División Secretaria General (Asesoría Jurídica del Negocio, Asesoría Fiscal, Atención al Cliente, Cumplimiento,...)
- Organización, Calidad y Proyectos Especiales
- División Riesgos (Riesgos de Crédito, Riesgos de Mercado, etc.)

Todas estas áreas de soporte, además de las distintas áreas de Negocios y Operaciones, deberán colaborar y proporcionar información a la Unidad de Riesgo Operacional, para el seguimiento de los Riesgos Operacionales.

Coordinadores Responsables de Riesgo Operacional.

Aunque la Dirección de la División o Área delegue sus responsabilidades al Coordinador Responsable de Riesgo Operacional, ésta sigue siendo responsable última de la gestión y el control de este riesgo. Este Coordinador Responsable, que se convierte en la figura clave dentro del marco establecido, tiene las siguientes responsabilidades:

- Seguimiento y control de la gestión del Riesgo Operacional en el Área de su competencia, a través de un contacto permanente con los responsables del Área y de sus Unidades, así como la supervisión directa de los indicadores de riesgo.
- Proporcionar apoyo y asesoramiento en materia de Riesgo Operacional a todas las Unidades del Área que gestionen directamente el riesgo.
- Implantación de una metodología homogénea que será utilizada para controlar el Riesgo Operacional en todas las Unidades de su Área respectiva. Esta metodología, que será consensuada con la

Unidad de Riesgo Operacional, incluirá la implantación de las herramientas cualitativas y cuantitativas necesarias.

- Recibir información periódica de los responsables del Área para poder consolidarla y realizar informes globales del Área.
- Enviar periódicamente a la Dirección del Área correspondiente y a la Unidad de Riesgo Operacional toda la información necesaria sobre el Riesgo Operacional asumido por el Área, así como los informes consolidados. La información reportada a la Unidad de Riesgo Operacional deberá ser consensuada con la misma.
- Establecimiento, en coordinación con la Unidad de Riesgo Operacional, de las medidas preventivas y acciones correctoras más convenientes para controlar el Riesgo Operacional y conseguir el nivel objetivo de riesgo que el Grupo está dispuesto a asumir.
- Proponer nuevas políticas y procesos, o mejoras de las ya existentes, que permitan una gestión y control adecuados del Riesgo Operacional en las distintas Unidades, incorporando las prácticas que se vayan desarrollando en el sector y que sean recomendadas por los Supervisores.
- Seguimiento y control del grado de implantación de las Recomendaciones de Auditoría Interna.

- Participación en el desarrollo de los proyectos del Área que impliquen Riesgo Operacional.
- Participación, en caso necesario, en los Comités de Nuevos Productos.

Cada Coordinador Responsable establecerá, en su ámbito de competencia, los procesos más adecuados para gestionar y controlar el Riesgo Operacional de su Área, pero siempre dentro del marco general de políticas y procesos determinados por la Unidad de Riesgo Operacional. Por tanto, se requiere una alineación máxima con las políticas y procesos del Grupo, por lo que las desviaciones sobre estas políticas deberán ser consultadas con la Unidad de Riesgo Operacional y aprobadas por la Comité Integral de Riesgos.

VPA Gestión de Riesgo Operacional y Sistemas.

La VPA Gestión de Riesgo Operacional y Sistemas, tendrá entre otras funciones las siguientes:

- Realizar un seguimiento de las fuentes de Riesgo Operacional en el Banco de Venezuela, Grupo Santander.
- Proponer a los Coordinadores Responsables de Riesgo Operacional la implantación de medidas preventivas, acciones correctoras, y controles que permitan reducir el nivel de Riesgo

Operacional y alcanzar el objetivo de riesgo asumido por la Dirección de la Entidad.

- Desarrollar y comunicar las políticas y procesos de Riesgo Operacional y proporcionar apoyo en relación con las mismas. Proponer los cambios necesarios en dichas políticas y procesos en función de las mejores prácticas y recomendaciones realizadas por los reguladores, de forma que se realice una mejor gestión y control del Riesgo Operacional de las distintas Áreas.
- Coordinar y apoyar a los Coordinadores Responsables de Riesgo Operacional en los procesos de implantación de una metodología de Riesgo Operacional homogénea para todo el Banco, así como de las herramientas cualitativas y cuantitativas necesarias (cuestionarios de autoevaluación, bases de datos de errores e incidencias, indicadores de riesgo, etc.).
- Desarrollar una Base de Datos de Errores e Incidencias a nivel Banco.
- Recibir información periódica e indicadores de riesgo de los Coordinadores Responsables, para poder realizar su seguimiento, consolidación y elaboración de informes globales para todo el Banco de Venezuela, Grupo Santander.
- Entregar al responsable de la VPE Gestión de Riesgos la información consolidada sobre el Riesgo Operacional que asume el

Banco, el nivel de pérdidas y provisiones, así como la dotación de capital correspondiente por este concepto.

- Coordinación con Auditoría Interna.
- Participación en los correspondientes Comités (Nuevos Productos, Irregularidades, Seguridad Bancaria, etc.).

3. **Niveles de Control.**

La gestión y el control del Riesgo Operacional debe ser parte integrante de las actividades diarias del Banco. Por tanto, las medidas para controlar este riesgo deben introducirse a lo largo de toda la Organización, y se concretarán en diferentes niveles:

- Control a nivel individual.
- Control de la Dirección.
- Control y recomendaciones de Áreas Especializadas, como Auditoría Interna y Coordinadores de Riesgo Operacional, así como los responsables de las diferentes Áreas Especializadas del Banco.
- Control y recomendaciones realizadas por entidades externas, como auditores externos y Supervisores.

Todos estos niveles formarán el Marco de Control del Riesgo Operacional.

3.1. Control a Nivel Individual.

Todo el personal será responsable de gestionar y controlar los Riesgos Operacionales de su competencia. En este sentido los valores corporativos (integridad personal, trabajo en equipo y profesionalidad), así como el conocimiento y comunicación de los posibles riesgos, son requisitos indispensables para la gestión y el control del Riesgo Operacional.

La calidad del control individual podrá estar influida por:

- Definición clara de los procesos de contratación, retención y finalización de contratos, así como existencia de modelos de competencia y evaluaciones anuales basadas en la eficiencia individual en la gestión y control del Riesgo Operacional.
- Apropiados procesos de selección, incorporación, promoción y formación.
- Adecuada comunicación de las políticas y procesos, cultura de control del riesgo, valores corporativos, y objetivos en el puesto de trabajo.
- Formación adecuada en el conocimiento de los riesgos.
- Asegurar el establecimiento de medidas disciplinarias.

3.2. Control de la Dirección.

Normalmente la Dirección tendrá que delegar tareas y establecer niveles de autoridad dado el tamaño de la Organización y la

especialización necesaria en las distintas tareas. Sin embargo, la Dirección seguirá siendo la responsable de las tareas delegadas. Por ello, será necesario que la misma establezca las adecuadas medidas de control en los procesos y sistemas de su competencia.

La Dirección será también responsable de supervisar la estructura de esos controles y realizar un seguimiento de su correcto funcionamiento.

3.3. Control de Unidades Especializadas

Muchas veces la Dirección podrá decidir que no se realicen directamente ciertas tareas de control, debido a la necesaria segregación de funciones y a la especialización que se requiere para ejecutarlas. En estos casos, la Dirección delegará dichas funciones a Unidades Especializadas.

La razón de ser de estas Unidades será la de suministrar a la Dirección opiniones expertas e independientes sobre el grado de gestión y control de los riesgos en un área concreta de la Organización o en un proceso concreto. Estas Unidades podrán estar especializadas en algunas Áreas o tipos de riesgo.

Sin embargo, esta transferencia de funciones no implicará que la Dirección no siga siendo responsable de la gestión y control de los riesgos.

3.4. Control de Entidades Externas.

Es el control y las recomendaciones realizadas por entidades externas, como Auditores Externos, Supervisores, etc., con ocasión de las revisiones o consultas periódicas llevadas a cabo en la Organización.

4. Controles Generales de Riesgo Operacional.

La Dirección y los responsables de las distintas Unidades deberán considerar si cuentan con las suficientes medidas de control para gestionar y mitigar estos riesgos.

En este apartado se recogen algunas medidas generales de control o requerimientos básicos para cada una de estas categorías de sucesos.

Fraude Interno y Fraude Externo.

Recogemos de forma conjunta estas dos categorías por ser los controles a realizar de naturaleza muy similar.

El establecimiento de medidas de seguridad será una parte fundamental en la gestión del Riesgo Operacional. Los actos ilegales y criminales podrán producirse en todos los terrenos de la Organización y es necesario implantar medidas que eviten su aparición, tales como:

- Implantación de medidas de seguridad contra cualquier tipo de fraude, falsificación y robo por parte de terceras personas ajenas a la Organización (fraude con tarjetas, robo de efectivo, billetes falsos, etc.).
- Implantación de medidas contra el fraude y criminalidad internos, como puede ser una adecuada segregación de funciones y la eliminación del riesgo de que una persona o pocas personas conozcan de forma exclusiva ciertas tareas y funciones a realizar, así como determinado tipo de información (relativa a clientes, procesos, sistemas, etc.).
- Realización de controles por parte de varias Áreas o personas cuando se trate de tareas o funciones susceptibles de provocar fraudes (efectivo, pagos, etc.). Por ello es importante identificar las tareas que precisan este doble control a lo largo de todo el ciclo de procesamiento.
- Acceso controlado a los edificios y lugares físicos (tornos, tarjetas de entrada, etc.).
- Acceso controlado a los sistemas informáticos (claves de acceso y passwords).
- Formación al personal en materias de seguridad.

- Establecimiento de medidas de seguridad en la incorporación y salida del personal de la Organización.
- Realización de auditorías y encuestas de seguridad de forma periódica.
- Comunicar todos los incidentes relativos a la seguridad a una Unidad Especializada.

Prácticas de Empleo, Salud y Seguridad en el Trabajo.

Entre las medidas que pueden tomarse para evitar las demandas, multas o sanciones a la Organización por motivo de incumplimientos en las relaciones laborales, las leyes de salud y seguridad en el puesto de trabajo o por discriminación laboral, estarían las siguientes:

- Implantar adecuadas relaciones laborales, relativas a la compensación y los beneficios, procesos de terminación de la relación laboral, etc.
- Cumplir con los acuerdos laborales y los convenios colectivos.
- Acondicionar las instalaciones para que se cumpla con las leyes de salud y seguridad en el puesto de trabajo.
- Evitar todo tipo de discriminación laboral en el trabajo por motivo de raza, sexo, religión, aspectos culturales o socio - económicos.
- Crear ambientes de trabajo agradables y saludables, donde existan relaciones adecuadas con jefes y compañeros, y en donde el personal esté suficientemente motivado y satisfecho en su puesto de trabajo.

Prácticas con Clientes, Productos, y de Negocio.

En la contratación, negociación, y comercialización se dan importantes focos de Riesgo Operacional. Al menos, se deberían controlar los siguientes aspectos:

- Relación de contrapartidas, clientes y proveedores autorizados.
- Relación de productos y operaciones autorizados.
- Límites establecidos a las operaciones.
- Revisión y validación de modelos de cálculo y valoración.
- Prácticas inadecuadas de contratación o negocio: operaciones a precio fuera de mercado, posiciones falseadas que benefician a la Entidad, concesión de exclusivas, prácticas restrictivas de la competencia, manipulación de mercados, realización de ventas agresivas, etc.
- Selección de los clientes y patrocinios.
- Actividades de asesoramiento, comunicación y motivos comerciales.
- Utilización de información privilegiada o violaciones de la confidencialidad.
- Incumplimientos administrativos o de normativa.
- Blanqueo de dinero.
- Cumplir con los códigos de conducta internos y normativa afín.
- Cumplir con la normativa vigente en nuestro país u otros países.
- Regular las operaciones de Gestión de Activos y Banca Privada.

Daños en Activos Físicos.

Las medidas generales a tomar para prevenir y reducir el impacto por daños en los Activos Físicos de la Organización son de dos tipos:

- Implantar medidas de seguridad que limiten el acceso a los edificios y lugares físicos (tornos, tarjetas de entrada, etc.), la contratación de empresas de seguridad, etc.
- Establecimiento de Planes de Contingencia de Activos Físicos, para el caso de catástrofes naturales, accidentes o actos terroristas.

Interrupción del Negocio y Fallos en los Sistemas.

Existen dos tipos generales de riesgos de sistemas: tecnológicos y de información. Los primeros tienen que ver con la estrategia y arquitectura de la tecnología, con el suministro de soluciones informáticas, y con los sistemas de explotación y apoyo. Los segundos hacen referencia más a la integridad, calidad y suministro de la información, así como a la disponibilidad de la misma. La interrupción en el ciclo de procesamiento de la información o de las transacciones debido a fallos o caídas en los sistemas informáticos y de comunicaciones puede originar importantes quebrantos para la Organización.

En este sentido, las medidas generales para evitar Riesgos Operacionales serían las siguientes:

- Establecimiento de estrategias tecnológicas adecuadas, así como mantenimiento de una estrecha colaboración entre las Áreas de Negocio y el Área de Tecnología, de forma que ambas conozcan las necesidades y limitaciones existentes.
- Desarrollo de unas Políticas y Procesos estándar que permitan llevar a cabo una gestión adecuada de los proyectos y peticiones realizadas por los usuarios.
- Medidas relacionadas con el suministro de soluciones informáticas, tales como la gestión de proyectos, realización de pruebas, aceptación por parte de los usuarios y documentación.
- Integración de los sistemas informáticos y de comunicaciones.
- Implantación de Planes de Contingencia Informáticos, de recuperación y sistemas alternativos para casos de emergencia, que permitan recuperar los procesos y la información cuando se producen interrupciones en el ciclo de procesamiento. Existencia también de Back Up diarios de la información.
- Incorporación de controles que permitan asegurar que la información procesada es correcta, completa y se suministra en los tiempos adecuados.
- Asegurar que la información confidencial no puede ser utilizada por personas no autorizadas.

Ejecución, Entrega y Gestión de los Procesos.

Al ser una fuente importante de Riesgo Operacional, es uno de los pilares básicos para la gestión y control de este riesgo. La Dirección debe introducir las medidas necesarias para realizar un control adecuado sobre todos los procesos y transacciones.

Entre las medidas preventivas podemos señalar:

- Los procesos deben estar plenamente documentados y la responsabilidad de actualización de los respectivos manuales y documentos debe estar claramente asignada.
- Es necesario informar por escrito de los niveles de autorización a todo el personal. Dichas autorizaciones deben estar en relación con el nivel de categoría profesional, y deben ser establecidas con cautela por la Dirección, sobre todo cuando se trata de autorizar pagos y aprobar exposiciones de riesgo de crédito o mercado.
- Otras medidas serían las relacionadas con el grado de criterio y competencia profesional, la capacidad, y el mantenimiento de la confidencialidad.

Aparte de estas medidas preventivas, deben realizarse controles periódicos de los procesos y de las transacciones. Estos controles internos deben

realizarse con frecuencia por personal independiente. De forma general, podemos indicar los siguientes:

- Controles y verificaciones sobre la imputación, registro y mantenimiento de datos, como por ejemplo, sobre los datos de las operaciones (precios, importes, etc.), datos estáticos, etc.
- Seguimiento de las demoras en los servicios prestados y de los fallos en la ejecución de los procesos.
- Controles en la liquidación de operaciones (abonos o adeudos incorrectos en cuentas de clientes, contrapartes, etc.) y la contabilización de las mismas.
- Cuadres y conciliaciones entre las Áreas de negocio y las de procesamiento, entre estas y las de control, o bien con entidades externas. Aquí podemos destacar los cuadres de actividad, posiciones y resultados entre las distintas Áreas, la reconciliación diaria de los saldos y títulos en balance entre los diferentes sistemas, la conciliación diaria de los saldos en cuentas y custodia, confirmaciones y liquidaciones de operaciones, cuadres contables, etc.
- Controles sobre los métodos de valoración de las operaciones, los modelos y los criterios de cálculo.
- Chequeo periódico de las cuentas usadas para contabilizar errores, así como análisis y gestión de las reclamaciones e incidencias pendientes.
- Verificaciones sobre la documentación y los contratos.

- Revisión de la adecuación de los informes de gestión internos y para entidades externas (calidad, adecuación y flujo de la información).
- Asegurar, mediante acuerdos contractuales u otras fórmulas, la continuidad de los servicios proporcionados por los proveedores de productos y servicios en caso de imposibilidad por parte de éstos de llevar a cabo sus actividades y compromisos por motivos extraordinarios (cámaras de compensación, corresponsales, etc.).

Cambios en el Entorno Económico – Jurídico.

El Banco puede verse afectado por cambios que se produzcan en el entorno económico y jurídico, como por ejemplo los producidos en la normativa contable, fiscal, y legal que afecten al negocio y sus resultados. Las medidas de prevención y anticipación generales para protegerse del efecto negativo de estos sucesos incluyen las siguientes:

- Seguimiento de las fuentes de información necesarias para poder anticiparse a la normativa legal, fiscal y contable que vaya apareciendo.
- Comunicación de la nueva normativa a todas las Áreas de la Organización que pudieran verse afectadas.

Gestión del Cambio, Nuevas Actividades y Productos.

Una Organización competitiva tiene que ser dinámica, lo que implica riesgos derivados de los procesos de cambio y nuevas actividades. Para llevar a cabo un control adecuado de estos riesgos es necesario:

- Realizar una coordinación, seguimiento, y reporting adecuado de los proyectos en la organización, utilizando equipos especializados destinados al efecto.
- Tener un conocimiento correcto de los riesgos implícitos en los procesos de cambio y hacer una valoración objetiva de las nuevas actividades o productos.
- Someter los proyectos y actividades a la aprobación de todas las Áreas implicadas, a través de Comités de Nuevos Productos o Actividades.
- Asegurar la existencia de una estructura y sistemas suficientes para llevar a cabo las actividades y gestionar los nuevos productos.

Estructura Organizativa.

La gestión del Riesgo Operacional comienza con una adecuada estructura organizativa. Las medidas a tomar para evitar riesgos derivados de esta estructura son los siguientes:

- Adecuada segregación de funciones entre las distintas áreas y entre las diferentes funciones en una misma área. Al menos debe existir segregación entre las siguientes grandes categorías de funciones:

- Autorización y Ejecución.
- Ejecución y Procesamiento.
- Procesamiento y Custodia.
- Procesamiento y Verificación.

- Transparencia de la información a todos los niveles, así como un claro entendimiento y asignación de las tareas y los objetivos, las responsabilidades y los riesgos. Debe existir un continuo flujo de información y las líneas de "reporting" tienen que estar bien definidas hasta llegar al Comité de Dirección (u órgano delegado). Más aún, las tareas, los niveles de autorización, y las responsabilidades del personal deben ser claras y estar bien documentadas. Este debería recibir información sobre sus tareas y objetivos, firmando su conformidad con las mismas y siendo anualmente evaluado por su grado de consecución.
- Controles realizados por varias Áreas o personas cuando se trata de tareas de riesgo grande o mediano, dígase aquellos que con probabilidad alta o mediana pueden desencadenar pérdidas importantes o daños serios a la reputación. Estos controles "dobles" deben ser de obligado cumplimiento en estos casos. Así, por ejemplo, deben realizarse cuando se trata de datos estáticos de clientes, datos contractuales, información para pagos, etc. Es importante identificar las tareas que precisan este doble control a lo largo de todo el ciclo de procesamiento.

Adecuación de Recursos Humanos.

Uno de los factores más importantes en el Riesgo Operacional es el propio factor humano. Las personas pueden cometer errores de forma involuntaria. Existen una serie de medidas que pueden ponerse en práctica para reducir estos riesgos:

- Llevar a cabo una adecuada selección del personal que tenga en cuenta, además de criterios profesionales, valores corporativos y humanos en su sentido más amplio.
- Potenciar algunos valores corporativos como la integridad, responsabilidad, competencia y posibilidades de desarrollo profesional.
- Realizar una gestión adecuada del personal, que suponga la existencia de un número suficiente de personas asignadas a las tareas en función de la evolución del negocio, fomentar la preparación del personal desde el punto de vista de formación y experiencia, y evitar la excesiva rotación.
- Facilitar el conocimiento del puesto de trabajo, las tareas y las responsabilidades, así como la influencia del mismo en otros puestos o Áreas de trabajo.
- Todo el personal debe recibir una clara descripción de sus funciones y objetivos. El grado de consecución de dichos objetivos debe formar parte de la evaluación anual del empleado.

- Establecer una adecuada delegación de funciones y responsabilidades, niveles de autorización, etc., en función de la categoría profesional, experiencia, formación, criterio y valores del personal.
- Evitar que una persona o pocas personas conozcan de forma exclusiva las tareas y funciones a realizar, así como determinado tipo de información (relativa a clientes, procesos, sistemas, etc.). Este riesgo se soluciona mediante una cultura que implique la transparencia de la información y la existencia de procesos documentados.

5 Herramientas para la Implementación de Cultura del Riesgo Operacional.

Las herramientas para el control del Riesgo Operacional son de dos tipos: cualitativas y cuantitativas. Ambas herramientas se combinan para realizar un diagnóstico y obtener un perfil de riesgo del Área. Una vez esto, se identifican las acciones correctoras a implantar y se realiza un análisis de utilidad para saber si los costes asociados a las acciones correctoras compensan las mejoras en el nivel de cobertura del Riesgo Operacional y, en consecuencia, en el nivel de provisiones y en la dotación de capital por dicho riesgo. Finalmente, tras la implantación de las acciones correctoras elegidas, se lleva a cabo un seguimiento cualitativo y cuantitativo de los resultados obtenidos a partir de dichas herramientas, incrementándoce una vez más el modelo.

5.1. Herramientas Cualitativas.

Dentro de las herramientas cualitativas podemos señalar las siguientes:

- Mapas de Riesgo Operacional
- Cuestionarios de Autoevaluación
- Indicadores de Riesgo Operacional
- Matrices de Riesgo Operacional
- Diagramas de Flujo (procesos o controles)
- Organigramas Funcionales

5.1.1. Mapas de Riesgo Operacional.

Con estos mapas se busca identificar, para cada proceso, subproceso y tarea, cada uno de los riesgos existentes, asignando una probabilidad de ocurrencia a cada uno de ellos (Frecuente, Probable, Ocasional, etc.) y clasificando dichos riesgos en grandes categorías (como por ejemplo, en Practicas de Empleo y Seguridad en el Trabajo, Fraude Interno, etc.). A su vez, se valora el impacto económico probable que tendrían estos riesgos en caso de materializarse (Insignificante, Moderado, Crítico, etc.). Todo ello permite realizar un mapping final de la probabilidad-impacto de los riesgos.

Esta herramienta es útil para identificar los distintos riesgos y obtener un perfil inicial de riesgo potencial de un Área, aunque no sirve para cuantificar el riesgo en términos de probabilidad y severidad.

5.1.2. Cuestionarios de Autoevaluación.

Es una de las principales herramientas del análisis cualitativo, que combinada con otras herramientas (la Base de Datos de Errores e Incidencias y los Indicadores de Riesgo), nos permite la obtención del perfil de riesgo del Área o Unidad.

Se busca identificar para cada Área o Unidad, y en cada uno de los procesos y tareas realizados, los riesgos a los que se expone el proceso en cada una de esas tareas y los factores que mitigan o cubren dichos riesgos. Las preguntas permiten realizar una ponderación de los riesgos y una evaluación de la cobertura del Riesgo Operacional con base al cumplimiento de los factores mitigantes.

Normalmente, se realizan entrevistas a las principales personas implicadas en todas las fases del proceso, redactando actas y consensuando los resultados con las mismas. Las preguntas

contestadas de manera insatisfactoria permiten identificar acciones correctoras.

El objetivo último es obtener un nivel de impacto y de cobertura del Riesgo Operacional en función de las respuestas del cuestionario. El modelo permite obtener resultados por riesgo y categoría de riesgo (Fraude Interno; Prácticas de Empleo, Salud y Seguridad en el Trabajo, etc.).

Por tanto el cuestionario es una herramienta de suma importancia para la medición del Riesgo Operacional ya que:

- Está basado en la asignación de pesos en términos de probabilidad y severidad.
- Nos proporciona niveles de cobertura con base en riesgos.
- Se pueden analizar los resultados bajo distintas perspectivas.
- Permite identificar acciones correctoras.
- Es un medio para realizar una gestión del Riesgo Operacional o nivel de exposición que el Área está dispuesta a asumir.

5.1.3. Indicadores de Riesgo Operacional.

Los indicadores de Riesgo Operacional son otra de las herramientas cualitativas básicas, que entre otras cosas permiten:

- Un seguimiento periódico de la evolución del nivel de riesgo.
- Alertar de situaciones graves de riesgo.
- Verificar el impacto en el nivel de riesgo de las acciones correctoras implantadas.

Los indicadores pueden ser de diferente naturaleza, en función de las características del Área, pero de forma general podemos señalar los siguientes:

- Estadísticas de Actividad, que permitan tener un conocimiento del nivel de actividad, procesos y operaciones realizadas en el Área (p.e., nº de operaciones realizadas en el mes y nº de operaciones vivas a fin de mes por productos/servicios, estadísticas de procesos, estadísticas de personal, etc.). De esta manera se puede hacer un seguimiento periódico de la actividad del Área, identificando situaciones de riesgo derivadas del aumento en el nivel de actividad con un nivel de recursos determinado. Además, las estadísticas de actividad nos permiten cuantificar el Riesgo Operacional, como luego veremos en el capítulo dedicado a la Metodología.
- Base de Datos de Errores e Incidencias, que nos proporciona información del número y coste real de los errores e incidencias que se producen en el Área, para cada una de las Unidades y por procesos, permitiendo un seguimiento de la evolución de los mismos y

del efecto de las acciones correctoras establecidas. Este indicador se comentará más en detalle cuando veamos las herramientas cuantitativas.

- Cuadres y Conciliaciones, realizados a lo largo del ciclo de procesamiento, para identificar situaciones de riesgo derivadas de descuadres o falta de conciliación de la información entre las diferentes Áreas de negocio y de soporte, o entre éstas y entidades externas. Para ello, se definirán los cuadres o conciliaciones más importantes de la operativa y se realizará un seguimiento periódico de los mismos.
- Grado de Implantación de las Recomendaciones de Auditoría Interna, para detectar situaciones de riesgo identificadas por la Auditoría en sus revisiones periódicas así como el grado de implantación mensual de sus recomendaciones.
- Eficiencia Operativa, para la elaboración de diferentes Benchmarking entre Áreas o Unidades, en función de las operaciones y procesos realizados y los recursos asociados a los mismos. Para ello, se realizan análisis de Dedicación de Actividades que permiten obtener los tiempos de dedicación en cada una de las tareas y procesos realizados, y así poder homogeneizar a una base común la diferente complejidad de los mismos y llegar a cifras de eficiencia y productividad comparables.

El área o Unidad deberá identificar las estadísticas, tipos de incidencias, cuadres y conciliaciones, o bien aquellos otros controles que sean más relevantes en su operativa, procediendo a establecer un sistema de reporte de la información que permita su control y seguimiento periódico.

5.1.4. Matrices de Riesgo Operacional.

Esta herramienta se basa en una tabla de tareas y controles, de forma que cada uno de ellos tenga asociada una Unidad y persona responsable. Para ello se identificarán:

- Todas las tareas y procesos de la Unidad.
- Todos los riesgos asociados a dichas tareas.
- Cada uno de los controles asociados a los riesgos.
- Las personas responsables de realizar los controles y elaborar los indicadores de riesgo.

Esta matriz, que deberá ser actualizada periódicamente, permite asignar tareas y responsabilidades a las personas encargadas de realizar los controles.

5.1.5. Diagramas de Flujo (procesos y controles)

Es una de las herramientas gráficas usadas para definir los procesos y controles operativos que se llevan a cabo en un Área determinada, así como sus riesgos asociados. En definitiva, es una herramienta complementaria a las Matrices de Riesgo Operacional, aunque más orientada a las tareas, riesgos y controles, en lugar de a las personas que las llevan a cabo.

5.1.6. Organigramas Funcionales

Los Organigramas Funcionales se utilizan principalmente para asegurar la segregación de funciones en el Área, así como la correcta estructura organizativa. En ellos, se asignan personas a las distintas funciones realizadas, identificándose concretamente a cada una de ellas. El objetivo es evitar que una misma persona, Unidad o Área realice funciones que no respetan la adecuada segregación de funciones, generando conflictos de intereses o Riesgos Operacionales que pueden ser evitados fácilmente.

El Coordinador Responsable de Riesgo Operacional del Área correspondiente deberá informar sobre éstas herramientas cualitativas a la Unidad de Riesgo Operacional.

5.2. Herramientas Cuantitativas.

Las herramientas cuantitativas más importantes para el Control del Riesgo Operacional son las siguientes:

- Estadísticas de Actividad
- Base de Datos de Errores e Incidencias

Ambas herramientas forman parte también de los Indicadores de Riesgo Operacional.

5.2.1. Estadísticas de Actividad.

Como hemos señalado, las estadísticas de actividad nos permitirán realizar un seguimiento de la evolución de la actividad en el Área, así como cuantificar el Riesgo Operacional asociado.

Serán las propias áreas las que determinen qué estadísticas son más significativas dentro de su actividad, así como los elementos más relevantes de las mismas. De forma general podemos señalar las siguientes:

- Estadísticas de Operaciones: operaciones contratadas en un periodo y vivas a fin de periodo. Lo mejor es disponer de archivos de operaciones, de manera que el Área disponga de todos los

datos principales de las mismas (importes, tipos de interés, plazos, etc.).

- Estadísticas de procesos: por ejemplo, número y volumen de confirmaciones realizadas, liquidaciones, contabilizaciones, etc.
- Estadísticas de Personal: número de personas por Unidad o Área, ausencias de personal, rotación del personal, apoyos externos, etc.

Las estadísticas nos valdrán para:

- Identificar riesgos y hallar frecuencias de errores por operación o proceso.
- Obtener estadísticos para los principales parámetros de las operaciones o de los procesos, así como para cuantificar el Riesgo Operacional.
- Conocer el nivel de actividad en operaciones o procesos.
- Conocer el nivel de recursos humanos asociados a los procesos y al procesamiento de operaciones.
- Obtener cifras de Eficiencia Operativa.

5.2.2. Base de Datos de Errores e Incidencias.

Esta base de datos nos va a permitir realizar un seguimiento de los errores e incidencias que se producen en el Área, conocer el nivel de

pérdidas y cuantificar el Riesgo Operacional derivado de dichos errores.

Las áreas respectivas deben conocer cuales son los tipos de errores e incidencias que se producen en su ciclo operacional, así como los datos más relevantes asociados a esas incidencias que permiten cuantificar el riesgo.

La base de datos deberá contener no sólo incidencias que se han materializado en pérdidas, sino también todas aquellos errores que se producen en la operativa y que no acaban por materializarse en P y G. Por otro lado, cualquier base de datos para el control operacional debe contemplar incidencias o riesgos tanto internos como externos.

Las base de datos nos valdrá para:

- Identificar los riesgos del Área.
- Realizar estadísticas de los errores e incidencias y sus costes (frecuencias, importes,...), así como conocer la evolución de las mismas durante el tiempo.
- Obtener desviaciones y estadísticos de errores, así como distribuciones de probabilidad que nos permitan modelar el comportamiento del Área (frecuencia, desviación, detección,...) y

que podrán ser posteriormente utilizadas en los cálculos para cuantificar el Riesgo Operacional.

- El Coordinador Responsable de Riesgo Operacional del Área correspondiente deberá informar sobre estas herramientas cuantitativas a la Unidad de Riesgo Operacional.

Conclusión y Recomendación

Al contar con un adecuado marco de gestión integral de riesgos alineados a las mejores prácticas, las instituciones financieras podrán aprovechar las oportunidades convirtiéndolas en beneficios presentes y futuros, entre las cuales se describen:

- Prevenir pérdidas e incrementar el valor de los accionistas.
- Reducción de costos y ahorro de capita, lo que se traduce en un centro de beneficio y no de costo.
- Crear una cultura de riesgo y compromiso en todos los niveles de la organización concerniente a la gestión "día a día" del riesgo.
- Lograr efectiva relación entre los riesgos y los objetivos estratégicos de la institución.
- Optimizar la efectividad y eficiencia de las operaciones del negocio.
- Mejorar la toma de decisiones, incluyendo la precisa inversión de recursos y foco de gestión.
- Cumplir con los requerimientos regulatorios tanto a nivel nacional como internacional.
- Responder rápidamente ante nuevas amenazas y oportunidades de mercado, ganando así ventaja competitiva.

La administración integral de riesgo plantea nuevos retos y desafíos , no sólo a las instituciones financieras, sino también a los organismos supervisores. Sin embargo, tales cambios deben verse, más que amenazas, como oportunidades, que permiten a las entidades una nueva forma de ver la gestión de riesgo y desarrollar métodos cualitativos y cuantitativos que combinados con las mejores prácticas mundiales y nuevos estándares de transparencia y calidad, pueden tener un impacto positivo en el valor accionario y en la posición competitiva de la Institución en los mercados financieros de capital.

Cada Institución financiera venezolana debe considerar las implicaciones relevantes del enfoque de gestión integral de riesgos y cómo enlazan las estrategias, políticas y procedimientos de riesgos con la cultura de riesgo y la operación de las actividades del negocio, además de determinar la mejor manera de valerse y aprovechar herramientas y lineamientos mundiales, tal como Basilea II, a fin de cumplir los requerimientos de la Resolución bancarias 136.03.

El Riesgo Operacional siempre ha existido, aunque era considerado como extremadamente remoto y no atrajo la atención de quienes se veían afectados, hasta la década de los noventa. Pérdidas importantes están ocurriendo de manera demasiado frecuente como para seguir ignorando el

problema. Instituciones admiradas y respetadas, especialmente Instituciones Financieras han sufrido pérdidas importantes debidas al Riesgo Operacional, lo cual explica el interés tan grande de los reguladores de ésta industria como lo son el comité de Basilea y la Superintendencia de Bancos.

La desregulación y la globalización de los servicios financieros, el crecimiento y sofisticación de la tecnología financiera están haciendo que los negocios de los Bancos sean cada vez más diversos y complejos. Riesgos debido a la alta dependencia de sistemas y tecnologías integradas y de alcance global. Riesgos nuevos asociados al comercio electrónico. Los cada vez más elevados volúmenes de transacciones obligan a tener políticas de mejoras continuas en los controles internos y adecuados sistemas de respaldo. Para cubrir los riesgos de nuevos instrumentos financieros, los Bancos están introduciendo técnicas nuevas como los son colaterales, derivados de crédito, bursatilización de Activos, que están generando nuevos riesgos.

Por último, para obtener el mayor beneficio de la implementación de las Políticas de Control de Riesgos, es imperante el apoyo de la Alta Directiva del Banco de Venezuela/Grupo Santander, a través de charlas de refuerzo, control y seguimiento al cumplimiento de las mismas, así como la motivación a todos los niveles jerárquicos, a que se cumplan a cabalidad cada una de las normas y procedimientos destinados a tal fin. Para ello se pudiese

implementar la comunicación vía intranet para suministrar tips que hagan referencia a dichas Políticas, así como suministrar detalle sobre determinados casos tales como: “Barings” ,“Parmalat”, donde de existir Políticas Definidas para Riesgo Operacional se hubiesen evitado. Así como establecer periódicamente talleres que permitan aclarar dudas o inquietudes relacionadas con el tema que permitirán de acuerdo a la experiencia tomar decisiones actuales.

Bibliografía

- Banco de Venezuela/Grupo Santander. Inducción a Coordinadores de Riesgos Operacionales. Diciembre 2003.
- Bank of International Settlements. Management and Supervision of Cross-Border Electronic Banking Activities, Julio 2003.
- Espiñeira, Sheldon y Asociados Boletín GRMS. Enero 2004.
- KPMG. Risk Advisory Services. Manual del Curso de Riesgo Operacional enfoque del Comité de Basilea. Febrero 2004.
- Superintendencia de Bancos y Otras Instituciones Financieras. Resolución 136.03 de 25 de mayo de 2003