UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Técnica Particular de Loja

ESCUELA DE CIENCIAS CONTABLES Y AUDITORÍA

MODALIDAD ABIERTA Y A DISTANCIA

"Beneficios de la implementación de la Norma de Riesgo Operacional en el Sector Bancario Ecuatoriano"

TESIS DE GRADO PREVIA A LA OBTENCIÓN DEL TÍTULO DE DOCTORAS EN CONTABILIDAD Y AUDITORÍA

AUTORAS: Martha Ximena Luna Unda
Verónica Patricia Maldonado Ávila

DIRECTOR: Dr. Lenín Paladines Salvador

CENTRO UNIVERSITARIO QUITO

2009

Doctor Lenín Paladines Salvador
DOCENTE DE LA ESCUELA DE CIENCIAS CONTABLES Y AUDITORÍA

C E R T I F I C A

Que el presente trabajo de tesis realizado por las estudiantes Martha Ximena Luna Unda y Verónica Patricia Maldonado Ávila, ha sido orientado y revisado durante su ejecución, por lo tanto autorizo su presentación.

Loja, septiembre del 2009

f) . . . . . .

DECLARACIÓN Y CESIÓN DE DERECHOS

"Nosotras, Martha Ximena Luna Unda y Verónica Patricia Maldonado Ávila declaramos ser autoras del presente trabajo y eximimos expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaramos conocer y aceptar la disposición del Art.67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que en su parte pertinente textualmente dice "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad"

. . . . . .
Martha Ximena Luna Unda

. . . . . .
Verónica Patricia Maldonado Ávila

AUTORÍA

Las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo, son de exclusiva responsabilidad de las autoras.

. . . . . .
Martha Ximena Luna Unda

. . . . . .
Verónica Patricia Maldonado Ávila

DEDICATORIA

A mi esposo, mis padres y a mis hijos.

Martha Ximena Luna Unda

A mis padres y hermanos.

Verónica Patricia Maldonado Ávila

AGRADECIMIENTO

A la Universidad Técnica Particular de Loja por permitirnos realizar nuestros estudios profesionales, a través de la Educación a Distancia.

Al Banco de la Producción Produbanco S.A, por permitirnos ser parte de su desarrollo y crecimiento durante este tiempo de permanencia en la Institución, contribuyendo al progreso de su gente y del país.

De manera especial, nuestro sincero agradecimiento al Doctor Lenín Paladines Salvador, por haber guiado y orientado nuestro trabajo de tesis.

. . . . . .
Martha Ximena Luna Unda

. . . . . .
Verónica Patricia Maldonado Ávila

ÍNDICE DE CONTENIDOS

RESUMEN EJECUTIVO

En el marco legal y normativo vigente a nivel mundial, el Riesgo Operacional es uno de los principales protagonistas de la Industria Financiera considerando sobre todo la crisis que se está viviendo en el sector.

En Latinoamérica en general, y en Ecuador específicamente se han dado importantes avances en los organismos reguladores de la actividad financiera, basándose en preceptos y mejores

prácticas que entidades como el Comité de Basilea ha dispuesto. La Superintendencia de Bancos y Seguros alineada a esta realidad en el año 2005 expidió la Resolución de Junta Bancaria JB-2005-834, que contiene las disposiciones que deben ser adoptadas por las Instituciones controladas, con la finalidad de lograr una adecuada administración de los riesgos de manera integral, incluyendo de esta manera al riesgo operacional como parte de todos los riesgos adicionales normados hasta ese momento.

A partir de esta fecha consideramos que en el Sector Financiero ecuatoriano se produjeron importantes cambios, no precisamente porque no existía la necesidad de administrar los riesgos derivados de la operatividad de los procesos, sino más bien porque el marco normativo delineaba de manera clara el alcance y objetivos que hasta cierto momento fueron en el caso de algunas Instituciones consideradas como un mito o algo prescindible frente a otras actividades, principalmente por la falta internalización de estos conceptos a todos los niveles de la organización.

En el desarrollo del presente trabajo, en el Capítulo I hemos incorporado los conceptos de Basilea I y II, partiendo desde sus orígenes, entendiendo sus objetivos, conformación del Comité, principios y pilares sobre los que sustenta los conceptos de control y eficiencia que son los que han amparado esta tendencia a nivel mundial, así como los procesos que las Instituciones están llevando a cabo para su aplicación.
También hemos desarrollado aspectos relacionados con normativas o estándares internacionales que apalancan o complementan la aplicación de medidas para minimizar los riesgos en las Instituciones Financieras como las NIIF'S (Normas Internacionales de Información Financiera), 25 Criterios de GAFI (Grupo de Acción Financiera Internacional), Recomendaciones especiales sobre la financiación del terrorismo, Acta Patriota o Ley Patriota, Reportes de Responsabilidad Social Corporativa.

Sobre el Sistema Financiero Ecuatoriano hemos dado un recorrido sobre la evolución de la normativa de control, considerando la identificación de riesgos que son ajenos a crédito, mercado y liquidez, y reputacional, entendiendo la problemática cada vez más creciente de controlar la operación de la Institución regulada. Incluimos conceptos que también están cobrando vigencia, a pesar de haberlos identificado hace algún tiempo atrás, como el Gobierno

Corporativo y el apoyo que debe otorgar a la implementación de las normas emitidas sobre administración de riesgos.

Otro aspecto importante que se incluye en este proceso, la seguridad de la información, incluimos conceptos de qué es, qué alcance tiene dentro de la Institución, cuáles son las mejores prácticas que se deben adoptar, el nivel de importancia dentro de la organización, así como sus principales aristas y prioridades.

Hemos dado un breve recorrido en Latinoamérica sobre la emisión y aplicación de la normativa generada por las Entidades Reguladoras y su evolución.

Dentro del Capítulo II nos adentramos en el Riesgo Operacional y la norma emitida por la Superintendencia de Bancos y Seguros, su definición, alcance y contenido de la misma. Adicionalmente incorporamos el glosario de términos que se forman parte de la Resolución y que permiten que todas las Instituciones del Sistema Financiero manejemos conceptos de manera estándar, lo cual favorece la comunicación y entendimiento a todo nivel.

Entendiendo que el propósito fundamental de lograr una apropiada administración de los riesgos operacionales de las Instituciones del Sistema Financiero, a través del cumplimiento de la normativa establecida es la reducción de pérdidas financieras atribuibles al riesgo operativo, detallamos la definición y alcance de los factores que se identifican como la causa primaria o el origen de un evento de riesgo operativo, así como los principales riesgos que se derivan de los mismos:

- Procesos,
- Personas,
- Tecnología de información, y;
- Eventos externos.

Dentro del factor procesos identificamos los riesgos más relevantes como: diseño inapropiado de los procesos críticos, o 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; así como también los aspectos más importantes a considerar para miminizarlos,

desde su clasificación en función de los objetivos estratégicos de la Institución, misión y visión, hasta el tratamiento y mejoras que deben ser aplicados para minimizar los riesgos y lograr mayor eficiencia.

Acerca del factor personas establecimos los principales aspectos que se incluyen en la norma desde el proceso de reclutamiento y selección, permanencia y desvinculación de los funcionarios con la premisa que contribuirán a minimizar riesgos relacionados con el factor humano como por ejemplo: negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, entre otros.

Sobre el factor tecnología, podemos indicar que siendo la base de la mayoría de operaciones que las entidades otorgan a los clientes, es uno de los factores más relevantes y por tanto la norma fija una serie de disposiciones alrededor de los procesos de tecnología y seguridad de la información, contemplando el ciclo completo de vida de los sistemas, adquisición, desarrollo, implementación y mantenimiento de las aplicaciones las instituciones y la protección que los datos deben tener basados en los conceptos de integridad, disponibilidad y confidencialidad de la información, pasando por el soporte y monitoreo de transacciones, acuerdos de servicio con los principales proveedores, esquemas de mesa de ayuda, así como niveles de autorización y segregación de funciones. Adicionalmente se incluye la necesidad de disponer de una adecuada administración de la infraestructura tecnológica.

Otro aspecto fundamental considerado en la norma se refiere a disponer de planes de contingencia y continuidad debidamente estructurados que permitan mantener la operación de la Institución Financiera cuando se haya producido un evento de contingencia mayor.

Los eventos externos que pueden afectar a las Instituciones del Sistema Financiero se consideran parte de los factores de riesgo operacional y tienen que ver principalmente con fallas en los servicios públicos, ocurrencia de desastres naturales, atentados, y actos delictivos. Para minimizar el impacto que pueden producir estos aspectos, es muy importante que las Instituciones controladas cuenten con planes de contingencia y de continuidad debidamente establecidos.

Finalizamos el segundo capítulo con un análisis sobre el impacto de la aplicación de la norma en una Institución Financiera y las consideraciones a tomar en cuenta para determinar la metodología a implementar para la administración de riesgos. Acerca del primer aspecto, si bien la Superintendencia de Bancos ha manifestado que la norma no está orientada a exigir que las Instituciones hagan grandes inversiones para su cumplimiento, sino más bien promueve un ambiente de control adecuado del riesgo operativo, las Instituciones deberán analizar la conveniencia de contar con un sistema que les facilite la administración de los riesgos, así como su correcta evaluación y gestión conforme a lo estipulado, así como la preparación del personal que esté a cargo del proceso.

Consideramos que se trata de una inversión, toda vez que la Institución Financiera desarrolla junto con la aplicación de la norma una ventaja competitiva importante frente a aquellas Instituciones, esto se revierte en la medida que a través de esta administración se eviten eventos de pérdida financiera importantes que pudieran afectar a las Instituciones.
Con relación al establecimiento de la metodología, no existe la fórmula perfecta sino que más bien creemos que se puede aplicar una propia que se ajuste a la realidad de la Institución partiendo de un diagnóstico de brechas que se deben establecer, y comprometer desde la Alta Gerencia, esta evaluación puede ser efectuada previa la capacitación respectiva con personal interno del Banco o con la asesoría de un tercero. Un tema crucial a tomar en cuenta es la medición y valoración de los riesgos, mientras más compleja sea la metodología escogida, más compleja será su implementación.

El Capítulo III contiene a detalle los principales aspectos que deben considerarse en la Administración del Riesgo Operacional, desde las funciones y responsabilidades del Directorio, Comité de Administración Integral de Riesgos, Unidad de Riesgos y Dueños de los procesos.

Adicionalmente se detallan los principales temas a ser considerados para clasificar los procesos, eventos de riesgo: identificación, registro, valoración, adopción de medidas; así como también los indicadores de gestión que sirven de apoyo a la gestión de riesgos operacionales

Es imprescindible recordar que la administración del riesgo operacional es una tarea conjunta que involucra a la Organización en sus diferentes instancias, y debe ser desarrollada progresivamente generándose una cultura de administración de riesgos, en tal sentido la

aplicación de la norma es un valor agregado para la Institución que mejora el control interno de la misma.

Se incluye en este capítulo además el código de ética que consigna valores fundamentales que forman parte de la tarea del Buen Gobierno Corporativo que busca lograr sus objetivos y los objetivos de sus funcionarios, a través de promover una cultura ética, honestidad, equidad, solidaridad y justicia.

El Capítulo IV está dedicado a los procesos de contingencia y continuidad del negocio, abarca todo el ciclo desde el establecimiento de la estrategia que debe seguir la Institución para asegurar que las principales operaciones sigan funcionando frente a un evento de fuerza mayor, hasta la metodología de implementación, pruebas y mantenimiento de los planes.

Al igual que la administración integral de riesgos es una ventaja competitiva para la Institución, lo es también contar con planes debidamente estructurados y probados para contingencia y continuidad, y la responsabilidad también es institucional.

Si se delinean apropiadamente las metodologías a seguir para los análisis de criticidad de procesos, la implementación si bien no resulta muy fácil, al menos permitirá mantener en todo momento una visión clara de los objetivos que se persiguen y el alcance que la Administración haya fijado al respecto. El análisis de impacto es vital a la hora de analizar las mejores estrategias que se deben adoptar frente a los eventos o fallas. Lo es también la capacitación al personal.

Ya para el Capítulo V hacemos un breve análisis sobre la interrelación que mantiene el riesgo operativo frente a los demás riesgos, crediticio, de mercado y liquidez y reputacional. En este análisis resaltan los temas relacionados con la crisis mundial que está afectando a todo el sistema financiero, así como las oportunidades de mejora que deben ser adoptadas por las Instituciones con el fin de minimizar los efectos y riesgos que pueden presentarse en el camino.

Concluimos el presente trabajo con el Capítulo VI en el cual hemos recopilamos aspectos adicionales que las Instituciones pueden tomar en cuenta con el fin de facilitar la implementación de la normativa vigente, y que están relacionadas principalmente con los

beneficios que tendrán frente a la competencia, las metodologías que implementarán contribuyendo al mejor desenvolvimiento de los procesos de administración de riesgos, desarrollo de planes de contingencia, administración de recursos tecnológicos, etc.

Algo importante que también mencionamos son algunos temas que en lo posible se deben evitar dentro de este proceso, por ejemplo creer que sin la ayuda de toda la organización se puede implementar la norma, no contar con la asesoría y preparación sobre el tema, bien sea a través de una asesoría o consultoría o programas de capacitación. El exceso de asesorías también puede ser riesgoso toda vez que el personal interno es el que mejor conoce el proceso.

Para terminar incluimos algunas conclusiones y recomendaciones que van en el mismo sentido de sacarle el mayor provecho a esta oportunidad que tiene la Institución, y en especial los Auditores Internos, de promover el mejoramiento del control interno, capacitarse en temas actuales y contribuir a brindar mayores y mejores servicios a nuestros clientes y público en general.

CAPÍTULO I INTRODUCCIÓN

1.3. El marco normativo de Basilea

1.3.1. El Comité de Basilea y sus principios básicos.

A raíz de la crisis que generó en el sistema financiero internacional por el cierre del Bankhaus Herstatt en Alemania en 1974, se creó el Comité de Basilea. La falta de cumplimiento a las órdenes de pago y cheques por parte del Chase Manhattan Bank en Nueva York contra la cuenta del Bankhaus Herstatt generó un caos en el sistema financiero internacional y en el sistema de pagos norteamericano, motivo por el cual, en febrero de 1975, se reunieron representantes de los Bancos Centrales del Grupo de los Diez (G-10), y formaron el Comité de Basilea, establecido como el Comité de Regulación Bancaria y Prácticas Supervisoras.

Los países miembros del Comité son, Bélgica Canadá, Estados Unidos, Francia, Alemania, Italia, Japón, Luxemburgo, Holanda, Suecia, Suiza, Reino Unido, y desde 2001, España.

El objetivo principal del Comité de Basilea fue mejorar la comprensión y control de calidad de la supervisión bancaria en todo el mundo, a través del intercambio de información, mejora de la eficacia de técnicas de supervisión internacional del negocio bancario, y el establecimiento mínimo de normas de control en las zonas donde se considere conveniente.

El Comité no posee autoridad de control supranacional. Emite normas, directrices, y declaraciones de las mejores prácticas para que sean adoptados y adaptados a la realidad nacional de cada país a través de normativa de cada uno de ellos.

En septiembre de 1997, el Comité de Supervisión Bancaria de Basilea publicó por primera vez los ***Principios Básicos para una Supervisión Bancaria Eficaz***. Como complemento, se emitió una metodología. En base a esos principios y metodología, los supervisores de los diferentes países han identificado medidas para aplicar prácticas de supervisión y evaluar la calidad de los sistemas de supervisión. El FMI y el Banco Mundial también aplican los principios básicos en su Programa para la Evaluación del

Sector Financiero (PESF) con el cual evalúan los sistemas y prácticas para supervisión bancaria en los distintos países.

Los Principios Básicos constituyen un marco de las mínimas normas que deben adaptarse para una adecuada supervisión, para fortalecer el sistema financiero mundial, ya que una deficiencia en el sistema financiero de cualquier país pone en peligro la estabilidad financiera del país e incluso de otros países. Más aún en el momento actual, que se encuentra totalmente globalizado. El Comité considera que la aplicación de los Principios Básicos por todos los países supondría un avance considerable para mejorar la estabilidad financiera nacional e internacional, y sentaría las bases para un mayor desarrollo de sistemas de supervisión eficaces.

El acuerdo de Basilea era una recomendación. Cada país signatario, así como cualquier otro país, quedaba libre de incorporarlo en sus normas y regulaciones con modificando los aspectos que considerase necesario. Fue adoptado por más de cien países.

Los Principios Básicos tienen 25 preceptos para la eficacia del sistema financiero. Los principios se agrupan en siete categorías. Debido a la importancia que tienen los Principios Básicos, a continuación transcribimos los mismos. Estos han sido tomados del Documento “Principios Básicos para una supervisión bancaria eficaz”, emitidos en octubre de 2006 por el Banco de Pagos Internacionales con sede en Basilea, Suiza:

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 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 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.

PRINCIPIO 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.

1.3.2. Los pilares de Basilea.

La principal limitación del acuerdo de Basilea I estaba relacionado con la exposición de crédito, por cuanto no tomaba en cuenta la calidad del crédito, y la probabilidad de incumplimiento de los deudores. En el año 2004 se propusieron nuevas recomendaciones, haciendo referencia a tres pilares:

Fuente: Presentación de Banco Agromercantil, Guatemala, oct 2003

- **PILAR I: LOS REQUISITOS MÍNIMOS DE CAPITAL**

Este pilar es fundamental en el Nuevo Acuerdo de Capital, ya que considera la calidad crediticia de los prestatarios así como el riesgo de mercado y operacional. Esto es, define el capital regulador y el cálculo de los requerimientos de capital por riesgo crediticio, de mercado y operacional (que no consideraba Basilea I).

La mayoría de países del mundo exigen que los bancos mantengan un nivel mínimo de capital, ya que es la base para el crecimiento futuro de la institución y proporciona un colchón de seguridad que se puede utilizar para eventos inesperados que generen pérdidas.

Un nivel adecuado de capital promueve la confianza del público en el sistema bancario, ya que si los bancos están bien capitalizados y administrados, pueden proveer crédito a sus clientes, tanto empresas como personas naturales, aún en fases críticas.

Técnicamente, es un desafío determinar el nivel de capital adecuado que proteja al banco contra pérdidas inesperadas, ya que si el nivel de capital es muy bajo, puede ser que no esté en capacidad de asumir pérdidas elevadas, incrementando el riesgo de quiebras bancarias y por tanto los depósitos de los clientes. Por otro lado, si el nivel es muy alto, se puede impedir la utilización eficiente de los recursos y limitar los niveles de crédito que se otorguen.

La fórmula aplicada es la siguiente:

$$\textbf{RMC} = \frac{\textbf{Capital}}{\textbf{Riesgo Crédito + Riesgo Mercado + Riesgo Operacional}} = \textbf{8\%}$$

El Capital Regulador es el capital básico o accionario. Esto es, acciones comunes y preferentes, debiendo sumar al menos el 50% del total. El capital adicional o secundario son las reservas y deudas a un plazo mayor a 5 años.

Requerimiento de capital por riesgo de crédito: Para cuantificar este riesgo, Basilea II presenta dos opciones, mientras Basilea I tenía una sola:

a) **Enfoque estándar:** Además de lo normado por Basilea I, incluye elementos para medir el riesgo crediticio, como la utilización de calificadoras de riesgo para establecer las ponderaciones de riesgo de los acreditados.

b) **Enfoque basado en calificaciones internas (IRB):** Faculta la calificación de los acreditados mediante modelos de medición y gestión de riesgos, desarrollados internamente por los bancos. Para ello los bancos agrupan la exposición de cartera en seis categorías de activos con distintas características de riesgo de crédito, esto es: **comercial, soberana, sistema financiero, consumo, valores y cuentas por cobrar elegibles.**

El Nuevo Acuerdo de Capital (NAC) propone fórmulas para calcular el requerimiento patrimonial para cada categoría de activos, mediante análisis teóricos y pruebas empíricas, que utilizan cuatro parámetros: probabilidad de incumplimiento, pérdida dado el incumplimiento, exposición al momento de incumplimiento y madurez.

Para requerimiento patrimonial, el NAC propone dos esquemas de medición interna del requerimiento patrimonial:

Enfoque IRB Básico: La entidad bancaria debe calcular internamente las probabilidades de incumplimiento de cada tipo de préstamos y aplicar los valores fijados por el supervisor para el cálculo de los requerimientos de capital en caso de pérdida por incumplimiento, exposición de riesgo crediticio y vencimiento o madurez.

Enfoque IRB Avanzado: Los bancos deben determinar y calcular internamente la totalidad de los parámetros de la fórmula de cálculo de requerimientos de capital.

Basilea II mejora la sensibilidad del marco de capital al riesgo de pérdidas por crédito en general, exigiendo un nivel más alto de capital para los prestatarios que considere que tienen mayor riesgo, y viceversa.

Los bancos y supervisores pueden escoger qué opción aplicar, adaptándola según la complejidad de las actividades y el grado de control interno del banco.

Los préstamos de menor riesgo tienen ponderación inferior, es decir, tienen requerimientos de capital menores frente a los que tienen mayor nivel de riesgo.

Basilea II presenta una exigencia de capital para las exposiciones de riesgo de pérdidas causadas por fallas en los sistemas, procesos o personas, o por causas externas, como desastres naturales.

Riesgo operacional: es el riesgo de pérdida causada por inadecuación o fallas en los procesos bancarios, personas, sistemas internos o causas externas. En Basilea II se calcula bajo diferentes alternativas, de acuerdo al grado de complejidad que implique, como:

a) **Método del Indicador Básico:** El requerimiento de capital es igual al 15% del promedio de los ingresos brutos del banco en los últimos tres años.
b) **Método Estándar:** Para este método existen ocho líneas de negocio: finanzas corporativas, negociación y ventas, banca minorista, banca comercial, pagos y liquidación, servicios de agencia, administración de activos e intermediación minorista.

   El requerimiento de capital se calcula por cada línea de negocio. Se multiplican los ingresos brutos de cada línea de negocio por unos factores que el Comité establece, y se suman los resultados de cada línea de negocio.

c) **Método Avanzado:** Los bancos pueden aplicar sus propios métodos, aprobados con anterioridad por los supervisores de la institución financiera.

Como vemos, las pautas del I Acuerdo de Basilea, (Basilea I), de adecuación de capital para la banca, ha demostrado su valor. En base a ello, los bancos deben

mantener un volumen de capital mínimo del 8% del valor total de sus activos, ponderado por su nivel de riesgo.

- **PILAR II: EL PROCESO DE REVISIÓN DEL SUPERVISOR**

El objetivo de este pilar es asegurar que cada banco cuente con procesos internos confiables para evaluar la suficiencia de su capital, en base a cálculos meticulosos de sus riesgos.

Este pilar está enfocado a fortalecer la labor del supervisor bancario, para que conozca efectivamente el grado de riesgo de las instituciones que supervisa y que éstas cuenten con el capital suficiente de acuerdo a su perfil de riesgo.

Los supervisores deben evaluar las actividades de riesgo de los bancos y las cuantificaciones que realicen de sus requerimientos de capital, y poder determinar cuándo una institución necesita un capital más elevado y las medidas correctivas que deben aplicarse, inclusive requerir a las instituciones que lo necesiten, un capital superior al mínimo normativo así como poder llevar a cabo una intervención temprana de los bancos que lo requieran.

El Comité de Basilea promueve un diálogo más activo entre los bancos y sus supervisores para poder actuar con rapidez y decisión, reducir el riesgo o restaurar el capital cuando se identifiquen deficiencias.

Otro aspecto que debe cubrir este proceso son los factores externos, tales como influencia de comportamientos cíclicos, y áreas de riesgo no consideradas total o parcialmente en el cálculo de requerimientos de capital, tales como riesgo de tipo de interés en libretas de ahorro o incertidumbre en la medición de los diferentes riesgos operacionales.

Los principios que establece este pilar son:

Principio 1. Los bancos deberán contar con un proceso de evaluación de la suficiencia de capital total en función a su perfil de riesgo y con una estrategia para mantener sus niveles de capital.

Principio 2. Los supervisores deberán examinar y evaluar las estrategias y valoraciones internas de la suficiencia del capital de los bancos, así como asegurar la aplicación de los coeficientes de capital de supervisión.

Principio 3. Los supervisores deberán asegurar que los bancos operen por encima de los coeficientes mínimos de capital regulador y tener la habilidad de exigir a las entidades que mantengan capital en exceso del mínimo.

Principio 4. Los supervisores deben procurar intervenir prontamente para evitar que el capital descienda por debajo de los niveles mínimos necesarios para cubrir las características de riesgo de un banco particular y exigir una acción correctiva inmediata cuando el capital no está en el nivel requerido.

En este pilar se analizan los riesgos que han sido tratados parcialmente en el pilar 1, como el riesgo de concentración del crédito; aquellos que no han recibido ningún tratamiento, como el riesgo de liquidez o de interés; y, los efectos externos al banco, como el ciclo económico.

- **PILAR III: LA DISCIPLINA DE MERCADO**

El Comité de Basilea insta a fomentar una disciplina de mercado a las instituciones bancarias a través de divulgar información financiera veraz y completa, es decir, a través de la transparencia de la información.

Un mercado bien informado premia a las instituciones, ya que los clientes se sienten protegidos, al poder identificar su nivel de riesgo. A menor riesgo, mayor confianza. Esto proporciona confianza en el sistema.

El cliente selectivo escoge un banco que brinde una imagen de seriedad, control interno adecuado, administración adecuada del riesgo. En esto juega un papel importante el Buen Gobierno Corporativo. Es por eso que el Comité de Basilea busca, a través de este pilar, transparentar la información a fin de que los depositantes estén adecuadamente informados sobre las características y

peculiaridades de cada banco, y por tanto puedan tomar decisiones en base a la valoración de riesgo. Los bancos establecen sus tasas en base a estos riesgos, y a través de ello demuestran su eficiencia. A mayor riesgo, la tasa de interés es más elevada, y viceversa.

1.3.3. Aspectos previstos para su implantación.

Entre los principales motivos para el Nuevo Marco de Capital, los sistemas de cálculo del capital mínimo exigible deben ser sensibles al riesgo, es decir, que para diferentes riesgos se calcule de diferente manera. Obviamente, esto general complejidad y por tanto necesidad de generar enfoques más avanzados, y que los entes de supervisión deban autorizar los enfoques que cada institución establezca.

Esto premia a las instituciones que administren con mayor profesionalismo sus riesgos, ya que a menor riesgo se necesitan menores recursos, y por tanto incentivando a sus administradores para que realicen una gestión eficiente de los riesgos. Por tal motivo, se incentiva el uso de técnicas modernas de gestión y medición de riesgos, con el uso de modelos avanzados.

Una entidad eficiente cuenta con sistemas que permitan mitigar razonablemente sus riesgos, generando una menor necesidad de capital y por tanto mejorando su rentabilidad. Por tanto el objetivo de las instituciones debe ser controlar los riesgos para reducir el nivel de recursos propios que requiere, en lugar de incrementar el nivel de capital para cubrir cualquier nivel de riesgo. De esta manera, los excedentes se dedican a nuevas actividades, productos o servicios, generando valor agregado a sus accionistas. La rentabilidad sobre el capital ajustado al riesgo, que debe calcularse a través de metodologías apropiadas, son un aspecto clave que deben considerar tanto los entes de control como el mercado, y por tanto se convierte en un aspecto estratégico a tratar y gestionar a su interior.

La responsabilidad de gestionar los riesgos y asegurar que el nivel de capital es adecuado al perfil de riesgo de la institución es de sus órganos de gobierno y dirección, esto es, la Alta Administración. Por tanto, es su responsabilidad conocer su perfil de

riesgo actual y determinar a qué nivel de riesgo llegará, es decir, establecer el nivel de apetito de riesgo que desea asumir. Esto implica que, de acuerdo a la estrategia de negocio que se escoja, debe establecer políticas, procedimientos y sistemas adecuados para medir y controlar, y proporcionar a la entidad de la organización y recursos necesarios. También debe establecer las fuentes y mecanismos para obtener y mantener el nivel de capital apropiado, determinando su composición y distribución.

Otro objetivo de Basilea II es incrementar la seguridad y sanidad del sistema financiero, manteniendo n nivel de capitalización adecuado a nivel de todas las entidades del sistema financiero.

Finalmente, otro objetivo es apoyar la igualdad competitiva entre entidades y países, aplicando criterios estandarizados para carteras con perfil de riesgo similar.

Todo lo anterior hace que se vea como muy compleja su implementación, y de hecho lo es, pues implica especializar al personal de la institución en evaluación de los diferentes riesgos, conocer sobre metodologías de medición y control, invertir en modelos automáticos que faciliten la administración del riesgo, etc. Es decir, que cada institución debe analizar a fondo sus procesos, evaluando las distintas opciones que ofrece Basilea II, encontrando puntos de equilibrio entre la sofisticación de los modelos que se utilicen, el perfil de riesgo institucional, y el costo de la implementación y mantenimiento de las metodologías avanzadas. Todo esto debe realizarse paulatinamente, incrementando progresivamente técnicas para gestionar el riesgo, determinando los recursos que se requieren y gestionando la autorización por parte de los organismos de supervisión y control.

Cada país debe normar, a través de los organismos de supervisión bancaria, adaptando a su realidad. Entonces es necesario empezar con el proceso de implantación. Este proceso es delicado, costoso y puede dar lugar a procesos largos y engorrosos si no se conducen adecuadamente. El Organismo de Control debe dar libertad a las instituciones de implementar la normativa de acuerdo a su realidad cultural, económica y de sus procesos. Pero también es necesario que el ente supervisor monitoree la implantación de la norma.

Para el caso de instituciones o grupos financieros internacionales, es necesario que los entes supervisores de los países donde operan bancos de un mismo grupo, coordinen y realicen convenios entre sí a fin de llevar un estricto control de la implantación, y considerando a la vez la diferencia en la normativa, plazos de implantación, prácticas bancarias diferentes, etc.

El proceso de normativa es complejo y largo, pues se va dando una complejidad incremental que debe ser adaptada por las instituciones paso a paso. En este proceso, es necesario un nivel de comunicación y retroalimentación permanente a fin de estandarizar dentro de lo posible los avances, hasta llegar a un nivel adecuado. A futuro, se podrán medir en forma equiparable, bancos de diferentes países del mundo.

1.3.4. Estándares internacionales.

Complementariamente a las normas de Basilea, existen una serie de normativas internacionales tendientes a estandarizar los controles, a fin de poder mitigar riesgos y a la vez medir en forma “estándar” a instituciones financieras alrededor del mundo. Entre ellos citamos:

- NIIFs, Normas Internacionales de Información Financiera, se encuentran en proceso de implementación en ciertos países, mientras que en otros ya han sido implementadas y paulatinamente sufren cambios o ajustes. Toda empresa que cotiza en bolsa debe utilizar estas normas para preparar las cuentas consolidadas, en la Unión Europea se aplica desde el 2005.

- 25 Criterios de GAFI (Grupo de Acción Financiera Internacional), en base a lo cual se norma la Prevención del Lavado de Activos y Financiamiento del Terrorismo. Toda entidad financiera debe tener políticas expresas sobre conocimiento del cliente, manual de políticas y procedimientos, una Unidad o al menos un Oficial de Cumplimiento, un Comité de Ética o de Prevención de Lavado de Activos y Financiamiento del Terrorismo, Herramientas y Metodologías para detección, monitoreo y reporte de operaciones inusuales,

selección de personal, programas de capacitación y código de conducta interno, Auditoría Interna, entre otros.

- Recomendaciones especiales sobre la financiación del terrorismo.

- Acta Patriota o Ley Patriota, ley estadounidense promulgado el 26 de octubre de 2001, se aprobó mayoritariamente luego de los atentados del 11 de septiembre de 2001. Su objetivo es ampliar la capacidad de control del Estado en aras de combatir el terrorismo, mejorando la capacidad de las agencias de seguridad americanas, dotándolas de poder de vigilancia contra el terrorismo. Estableció nuevos delitos y endureció las penas por delitos de terrorismo. Es criticada por organismos de derechos humanos por la restricción de libertades y garantías constitucionales.

- Implementación de Common Reporting, esquema europeo de estandarización de reportes de solvencia de instituciones de crédito, firmas de inversión bajo los requerimientos de capital de la UE. A estandarizarse a nivel mundial.

- Reportes de Responsabilidad Social Corporativa.

1.2 El Sistema Financiero Ecuatoriano

1.2.1 Evolución de la normativa de control.

La Banca y el Comité para la Supervisión Bancaria de Basilea han transitado en las últimas dos décadas hacia una gestión y supervisión basada en riesgos. Este proceso se inició con la reforma a la Ley General de Bancos en 1986, una vez que se superó la crisis financiera de comienzos de los ochenta. Dicho proceso se fortaleció con las modificaciones a esta ley en 1997 incorporando recomendaciones del Primer Acuerdo de Capital del Comité de Supervisión Bancaria de Basilea de 1988, o Basilea I, y con diversas medidas en años recientes. Estas incluyen la complementación de Basilea I con el enfoque sobre riesgo de mercado, la recolección de datos y estimación de

provisiones por riesgo de crédito, la identificación y control de factores de riesgo operacional por parte de los bancos, y la participación de sus Directorios y Altas Gerencias en la definición de políticas y procedimientos de seguimiento y control de riesgos.

El Comité ha orientado su supervisión hacia el riesgo que asumen los bancos en el desarrollo de sus negocios, enfatizando la evaluación de su gestión y solvencia.

Las resoluciones sobre las prácticas sanas para la gestión y supervisión del RO emitidas por el Comité para la Supervisión Bancaria de Basilea, tomaron como referencia algunos aspectos como: que la falta de regulación y globalización de los servicios financieros a nivel nacional, la creciente sofisticación de la tecnología financiera que hace que los perfiles de riesgo de las actividades de los bancos, sean más diversos y complejos. Algunos de los riesgos, distintos de los riesgos de crédito y liquidez, que se identifican como sustanciales tenemos:

- El uso de tecnología altamente automatizada tiene el potencial de transformar los riesgos de errores de procesamiento manual a riesgos de fallas de los sistemas.

- El crecimiento del e-commerce trae con él riesgos potenciales (ej: fraudes externos y aspectos de seguridad de los sistemas) que no son aún totalmente comprendidos.

- Las fusiones en gran escala, separaciones y consolidaciones prueban la viabilidad de los sistemas nuevos o recientemente integrados y han resultado en algunos problemas notables.

- El surgimiento de bancos actuando como proveedores de servicios de gran volumen crea la necesidad de mantenimiento continuo de controles internos de alto grado y de sistemas de respaldo.

- Los bancos pueden involucrarse en técnicas de mitigación de para optimizar su exposición al riesgo de mercado y riesgo de crédito, pero lo que a su vez pueden producir otras formas de riesgos.

- El uso creciente de arreglos de tercerización y la participación en sistemas ejecutados por terceras partes pueden mitigar algunos riesgos pero también pueden representar para los bancos otros riesgos significativos.

El Grupo de Administración de Riesgos del Comité demarca su pensamiento actual sobre la estructura para un cargo de riesgo operativo en su "Working Paper on the Regulatory Treatment of Operating RIsk", publicado en Septiembre 2001. En la elaboración de sus propuestas actuales para un cargo de capital regulatorio mínimo para el riesgo operativo, el Comité ha adoptado una definición común en la industria, denominada: 'el riesgo de pérdida resultante de procesos internos, gente y sistemas inadecuados o fallidos o de eventos externos'. La definición incluye riesgo legal pero excluye los riesgos estratégicos, de reputación y sistémicos.

Esta definición se enfoca sobre las causas del riesgo operacional y el Comité cree que esto es apropiado para administración del riesgo incluyendo, últimamente, la medición. El comité reconoce que por propósitos internos los bancos pueden optar por adoptar sus propias definiciones. Es importante que, cualesquiera sea la definición que se utilice, se considere el rango completo de riesgos operativos que enfrenta el banco.

Este documento se enfoca en el riesgo operativo, un subconjunto de 'otros riesgos'. "Otros riesgos" fue definido por el Comité sobre una base de exclusión, como todos los riesgos distintos de los riesgos de crédito, mercado y tasa de interés. El Comité reconoce que el riesgo operativo es un elemento sustancial de 'otros riesgos', y es un área donde los bancos por si mismos están dedicando una atención y recursos considerables. El riesgo operativo se presta en si mismo más fácilmente a la cuantificación, y por tanto a una efectiva administración, que algunos otros elementos de otros riesgos. No obstante, los bancos deberían buscar administrar todos los riesgos bancarios significativos, y los supervisores los revisarán como parte del Proceso de Revisión Supervisor (Pilar 2) del Nuevo Acuerdo de Capital de Basilea.

En su trabajo sobre la supervisión de riesgos operativos, el Comité ha intentado desarrollar una mayor comprensión sobre las tendencias y prácticas actuales de la industria para administrar el riesgo operativo. Estos esfuerzos involucraron numerosas

reuniones con organizaciones bancarias, encuestas sobre prácticas de la industria y análisis de los resultados. En base a estas fuentes de información, el Comité cree que tiene una buena comprensión tanto del rango actual de prácticas de la industria bancaria, como también de los esfuerzos de la industria para desarrollar métodos para administrar los riesgos operativos.

Anteriormente los bancos utilizaban mecanismos de control interno con el apoyo de Auditoría para administrar el riesgo operativo, aunque estos elementos mantienen su nivel de importancia, actualmente existen estructuras, herramientas y procesos específicos orientados a administrar el riesgo operativo de manera eficaz.

Una adecuada administración de riesgos, de acuerdo con una cantidad creciente de organizaciones representa un valor agregado que aporta seguridad y solidez al banco, protegiendo y acrecentando el valor para los accionistas.

Los enfoques para administrar el riesgo operacional están evolucionando rápidamente, en este sentido el Comité reconoce que aún hay mucho camino que recorrer, sobre todo en el tema de cuantificación de los riesgos para obtener índices que contribuyan al mejoramiento continuo de los procesos y por ende de la Institución.

Entre otras normas emitidas por el Comité se encuentran:

- 2003: “Sanas practicas para la gestión y supervisión del RO”.

- 2004: “Basilea II”.

- 2006: “Principios Básicos para una Supervisión Eficaz” (versión actualizada)

Estos documentos orientan a los bancos sobre los elementos cruciales para la administración de RO para bancos de cualquier tamaño y alcance, que se detallan a continuación:

- Estrategias definidas y su seguimiento por parte del Directorio y la alta gerencia.

- Sólida cultura de gestión del RO y de control interno.

- Herramientas eficaces para la transmisión interna de información y planes de contingencia.

Basilea II establece tres pilares fundamentales del nuevo marco de capitales:

Fuente: Grupo Implementación Riesgo Operacional Banco X

Basilea II establece una exigencia de capital por Riesgo Operativo, pero además se requiere que como precondición, las entidades tengan que aplicar las buenas prácticas y principios de gestión emitidos en 2003.

Los criterios para calificar para la aplicación de los distintos enfoques de medición, son proporcionales a la complejidad del enfoque elegido.

Así, cuanto más complejo sea el enfoque de medición elegido, mejor tendrá que ser el marco de gestión de Riesgo Operativo. Por ejemplo, para el enfoque más sencillo (de "Indicador Básico") se recomienda que las entidades apliquen las buenas prácticas del 2003.

La Regulación sobre Riesgo Operacional a nivel de Latinoamérica arranca desde el 2002 en Perú, el inicio de los países en la administración de riesgo operativo tiene como base que las entidades entiendan y cumplan con las mejores prácticas emitidas por el Comité, y luego con la ayuda de las entidades supervisoras o Superintendencias que han sabido agrupar en las diferentes normativas emitidas los aspectos más relevantes a ser considerados. En el 2005 al igual que Ecuador, siguen el proceso Chile y México, en el 2006 Brasil, Colombia y Argentina, en el 2007 Uruguay.

De acuerdo a lo indicado por Basilea es importante que cada país fije su Hoja de Ruta hacia la implementación de las practicas y normas emitidas, de tal manera que se pueda claramente organizar el proceso y llevarlo cabo sin mayores inconvenientes.

1.2.2 Principios de Buen Gobierno Corporativo en Ecuador.

El Buen Gobierno Corporativo consiste en una serie de principios y pautas de conducta para los accionistas, administradores y empleados. Están constituidos con el fin de transparentar las actividades de la empresa, diligenciar su gestión, y fomentar cultura de honestidad, lealtad, imparcialidad y buena fe en las organizaciones.

Estos principios fueron adoptados en la Ley Sarbanes Oxley en Estados Unidos, a raíz de los grandes escándalos financieros como Enron o Parmalat, y proporcionan un marco de referencia respecto a la forma en que la Junta Directiva y la administración ejecutiva gobiernan la entidad. El caso de Enron, por ejemplo, en esencia consistió en la creación de una empresa que a través de operaciones ficticias y mucha propaganda infló significativamente el valor de sus acciones, aparentando jugosas ganancias que no tenían sustento alguno. Esto se complicó aún más a través de la creación de empresas fantasmas en paraísos fiscales. En definitiva, los problemas se centraron en proceder con absoluta falta de ética y transparencia. Para la realización de este fraude, los ejecutivos de Enron emprendieron en cabildeos intensos con políticos norteamericanos, de manera que cuando se produjo el escándalo lo minimizaron y no dejaron que avancen las investigaciones debido a que algunos políticos estuvieron incluso aparentemente involucrados en las transacciones. Es decir, la corrupción contagió al sistema político, lo cual facilitó hasta la impunidad.

Basilea II insta a los bancos a mejorar su gobernabilidad, ya que su enfoque requiere mejorar el manejo de riesgo, considerando la relación entre la administración del riesgo y los objetivos corporativos. Basilea II emitió el documento "Enhancing Corporate Governance for Banking Institutions" ("Mejorar el Gobierno Corporativo par Instituciones Financieras") en Septiembre de 1999. En dicho documento, lo define de la siguiente manera:

"*El Gobierno Corporativo trata sobre la manera mediante la cual las instituciones y sus operaciones de negocios son supervisadas y dirigidas por la Junta Directiva y la Administración Ejecutiva, afectando cómo los Bancos:*

1- *Fijan sus metas corporativas, incluyendo la generación de beneficios económicos a sus dueños.*
2- *Rigen las operaciones del día a día de la institución.*
3- *Evalúan los intereses de los accionistas.*
4- *Establecen una cultura corporativa con el objetivo de operar de una manera segura y satisfactoria, y en cumplimiento con las leyes y normas vigentes.*
5- *Resguardan los intereses de los depositantes.*

El Acuerdo de Basilea II influye significativamente en la forma cómo los Bancos actúan dentro de estos cinco criterios.

Adicionalmente, el rol de supervisión, administración y control de las actividades de la organización por parte de la junta directiva y la administración ejecutiva ha sido enfatizado a través de los Documentos de Consulta de Basilea II y en otras publicaciones del BIS. Estos documentos existen como resultado de la importancia que da Basilea II al concepto de Mejoramiento de los Procesos de Manejo de Riesgo de las instituciones financieras".

La implementación de un buen gobierno corporativo contribuye a que las entidades emisoras atraigan inversión, crezcan y compitan con éxito, a fin de proteger la confianza de los inversionistas mediante la identificación, fortalecimiento y suficiencia de la información a la que pueden tener acceso. Contribuye significativamente al logro de los

objetivos de estabilidad, seguridad y confianza, promoción y desarrollo del mercado de valores y protección de los inversionistas, ahorradores y asegurados. Además ayuda a incrementar la productividad y es un factor determinante en los niveles de riesgo a los que están expuestas las entidades financieras.

Las prácticas de buen gobierno corporativo mitigan la existencia de conflictos entre partes interesadas, los riesgos asociados a la administración de la entidad controlada, incrementan la capacidad de toma de decisiones, reducen la necesidad de supervisión estatal y mejoran la calificación de riesgo de las instituciones financieras. Todo esto coadyuva a mitigar el riesgo de que se presente una crisis financiera y sus consecuencias, tanto en lo referente a los costos económicos como las consecuencias sociales de las cuales el Ecuador ha sido ya víctima.

Las normas de Buen Gobierno Corporativo proporcionan mecanismos para la existencia y puesta en marcha de procesos que equilibren la gestión de cada unidad y su gestión de control mediante pesos y contrapesos, permitiendo que las decisiones que se adopten se realicen según el mejor interés de la entidad, sus accionistas y acreedores y guardando respeto a los derechos de los consumidores financieros y otros grupos de interés. Estos grupos de interés están compuestos por los consumidores financieros, los acreedores, competidores, empleados, la comunidad en general y el supervisor. Todos ellos tienen intereses legítimos en el correcto funcionamiento de la entidad.

En Ecuador, gracias a la gestión realizada por la Cámara de Industrias, se ha promovido la implementación de prácticas de Buen Gobierno Corporativo en empresas que no son parte del sistema financiero, a fin de que estas empresas actúen en forma transparente y ética al interior de sus organizaciones, creando culturas de cumplimiento y respeto a las normas. Esto es un muy buen paso inicial, pero toma tiempo y un gran esfuerzo lograr su implementación, especialmente en el medio actual, en el que a diario se observan escándalos de corrupción a diferentes niveles. El Gobierno debería ser el primero en implementar estas políticas, de manera que se creen precedentes y una cultura de respeto y cumplimiento.

Pautas del Buen Gobierno Corporativo según Felaban:

- Autodisciplina.
- El ordenamiento de la empresa es voluntario, no por orden externa.
- El empresario, el accionista y el administrador son responsables de sacar adelante ala empresa sin lesionar los derechos de accionistas, ejecutivos, empleados, clientes y la comunidad.
- Imparcialidad.
- Diligencia.
- Lealtad.
- Buena Fe.
- Transparencia.
- Honestidad.

Un adecuado gobierno corporativo contribuye de forma crucial al logro de los objetivos de estabilidad, seguridad y confianza; promoción y desarrollo del mercado de valores, protección de los inversionistas, ahorradores y asegurados. El gobierno corporativo de las entidades financieras no es solamente un elemento importante para incrementar la productividad del sector, sino que es importante en la determinación del nivel de riesgo al que está expuesta la entidad financiera. También provee mecanismos para equilibrar la gestión y el control mediante sistemas de pesos y contrapesos para que se adopten decisiones que protejan los intereses de la entidad, sus accionistas y acreedores respetando los derechos de los clientes financieros y otros grupos de interés.

Los grupos de interés tienen intereses legítimos en el funcionamiento de las entidades. Estos grupos están constituidos por: consumidores, acreedores, competidores, empleados, el público, Organismos de Control.

La dispersión que existe de la propiedad, es decir, la falta de concentración del capital en pocas manos, genera tensiones básicas, esto es, accionistas respecto a los administradores, accionistas mayoritarios frente a los minoritarios, etc. Esto afecta también al funcionamiento de la Junta Directiva o Directorio, a quien se define como el máximo responsable del desempeño de una entidad. El Directorio es un órgano de supervisión que orienta la política general de la entidad, controla a los representantes

legales y sirve de enlace con los accionistas. Debe buscar el mejor interés de la sociedad y de sus accionistas.

Es necesario enfatizar que cuando las normas éticas voluntarias y autónomas que guían la conducta de la institución y sus funcionarios forma parte del funcionamiento de los bancos o instituciones que las adopten, pasan a ser estándares de conducta, normas implícitas, que finalmente terminan contagiando al mercado y fortalecen a la institución porque su buen prestigio es públicamente reconocido y valorado.

Tiene similitud con las normas antiguas del Buen Hombre de Negocios, que era reconocido y admirado en el mundo empresarial. Obliga a que tanto la Alta Dirección como la Junta Directiva actúen siempre de buena fe, y que se preparen para actuar con destreza y diligencia profesional. Los obligan a mantenerse informados, vigilar la marcha de la empresa e incluso investigar cuando consideren necesario.

PRINCIPIOS DEL BUEN GOBIERNO CORPORATIVO

La Organización para Cooperación y Desarrollo Económico OCDE, por sus siglas en inglés, emitió en el año 2004 los “Principios de Gobierno Corporativo”, que mencionamos a continuación:

Asegurar la base de un marco de referencia efectivo para el Gobierno Corporativo. Este marco de referencia debería promover mercados transparentes y eficientes, ser consistente con las reglas legales y articular claramente la división de responsabilidades entre diferentes autoridades supervisoras, reguladoras y de refuerzo.

Los derechos de los accionistas y las funciones de los propietarios clave. El marco de referencia del gobierno corporativo debería proteger y facilitar el ejercicio de los derechos de los accionistas.

1. El tratamiento equitativo de los accionistas. El marco de referencia del gobierno corporativo debería asegurar el tratamiento equitativo de todos los accionistas,

incluyendo los minoritarios y extranjeros. Todos los accionistas deberían tener la oportunidad de obtener compensación por la violación de sus derechos.

2. El rol de los accionistas en el Gobierno Corporativo. El marco de referencia del gobierno corporativo debería re conocer los derechos de los accionistas establecidos por ley o a través de acuerdos mutuos y fomentar la cooperación activa entre las corporaciones y los accionistas parar crear bienestar, trabajo y sostenibilidad de las empresas con reputación financiera sólida (Financially sound enterprises).

3. Revelación y Transparencia. El marco de referencia del Gobierno Corporativo debería asegurar la revelación oportuna y precisa en todos los aspectos materiales relacionados con la corporación, incluyendo la situación financiera, rendimiento, propiedad y gobierno de la compañía.

4. Las responsabilidades de la Junta. El marco de referencia del gobierno corporativo debería asegurar la guía estratégica de la compañía, el monitoreo efectivo de la gerencia y la trazabilidad de de la compañía para los accionistas.

SEGURIDAD DE LA INFORMACIÓN: COMPONENTE CLAVE DE UN BUEN GOBIERNO CORPORATIVO

La privacidad y protección de los datos personales de clientes y consumidores es un elemento clave en las empresas. La seguridad de la información es un elemento indispensable del buen Gobierno Corporativo.

El crecimiento y el riesgo están sumamente relacionados, especialmente debido a la globalización. El éxito en la ejecución de las estrategias de negocio está íntimamente relacionado con una adecuada administración de riesgos.

Las empresas se expanden a nuevos mercados, lanzan operaciones en economías emergentes a gran velocidad, que dependientes del uso de tecnologías de la información. Esto implica tomar mayores riesgos empresariales, incluyendo el riesgo

relacionado con la administración de la información crítica, tanto propia como de sus clientes.

Las nuevas oportunidades de negocio pueden ser un alto riesgo en el futuro cercano, especialmente si genera pérdidas o daño de la información, fuga de secretos del negocio, exposición no autorizada de la información del cliente o acceso a los sistemas.

Es por ello que la seguridad de la información es clave para el Gobierno Corporativo. Esto se evidencia porque cada vez las empresas invierten más en seguridad de la información. La alta gerencia se involucra en las políticas relacionadas con el tema. Las regulaciones, especialmente de los bancos, influyen en que se tomen medidas de este tipo. Todo esto implica que la seguridad de la información vaya tomando liderazgo.

La Novena Encuesta Global de Seguridad de la Información de Ernst & Young, reúne las perspectivas de profesionales en seguridad de la información de 1.200 organizaciones de 48 países, y confirma que ésta nunca ha sido más importante que hoy. Muestra que muchas compañías están progresando significativamente en mitigar sus riesgos fortaleciendo los mecanismos de control relacionados con la seguridad de información.

Si bien las empresas están realizando progresos significativos para implantar este sistema, deben dar pasos aún más contundentes para conseguirlo.

Cinco prioridades

Como consecuencia, se detectan cinco prioridades generales de seguridad de la información que tendrán un impacto importante en la habilidad de las organizaciones para administrar sus riesgos.

Integrar la seguridad de la información con la organización: La administración de riesgos relacionados con la información es parte integral del proceso general de administración de riesgos. La Seguridad de la Información está ahora más integrada en la cultura de las compañías. La función de Seguridad de Información está empezando a ser considerada dentro del portafolio de tercerización de funciones.

Extender el impacto de cumplimiento: El impacto que genera el cumplimiento continuará creciendo (Sarbanes Oxley, Basilea II, European Union's 8th Directive).
El cumplimiento promueve la integración entre el grupo a cargo de seguridad de la información y otros grupos funcionales del negocio. El cumplimiento mejora los mecanismos de control relacionados con la seguridad de la información.

Manejo del riesgo de relaciones con terceros: Las compañías reconocen los retos, hechos y acciones necesarias para manejar los riesgos con los proveedores globales y socios tercerizados. Los terceros están empezando a administrar sus propios riesgos relacionados.

Enfocarse en la protección de la privacidad y datos personales: Existe un enfoque creciente a la protección proactiva de la privacidad y datos personales. Las prácticas relacionadas con la protección de la privacidad y datos personales están formalizándose.

Diseñar y construir seguridad de la información: La seguridad de la información es más proactiva en el apoyo al cumplimiento de los objetivos del negocio. Las compañías están adoptando cada vez más estándares reconocidos.

1.2.3 Consideraciones prácticas para la implementación de Basilea II.

Dentro de los factores que consideramos críticos para una exitosa implementación de las normas de Basilea II, mencionamos algunos que proporcionan una guía adecuada a las entidades financieras, entre ellos:

- La implementación de Gobierno Corporativo debe incluir una clara definición de roles y responsabilidades, partiendo desde la Junta Directiva y la Alta Gerencia. Sin un apoyo y convicción de estos niveles, es sumamente difícil, por no decir imposible, la implementación de la normativa.

- El proceso de información debe también estar claramente establecido. Deben definirse esquemas tanto para la correcta definición como para la divulgación y

retroalimentación. El proceso de implementación de las normas de Basilea implican un cambio del enfoque y un fortalecimiento de la cultura empresarial.

- La cultura de riesgo debe ser explícita. Deben establecerse los parámetros de la administración: nivel de apetito del riesgo, estrategias para mitigarlo o eliminarlo, etc. Esta cultura de riesgo es específica para cada organización.

- La implementación de estas normas debe ir acompañada de esquemas de entrenamiento al personal, difusión de las responsabilidades de cada uno dentro de la organización y realización de talleres, cursos, folletos, etc., que permitan una difusión permanente y actualización continua.

- La administración de riesgos es un proceso continuo, una vez adoptado, va fortaleciéndose, modificándose, adaptándose y complementándose. Este principio debe estar asumido y entendido por la alta gerencia, los líderes de riesgos, el staff a cargo de los diferentes procesos (los dueños de los procesos), las unidades de control, etc.

El Nuevo Marco de Capital comprende tres Pilares los cuales tienen los siguientes objetivos en relación con la estabilidad financiera y solvencia de los bancos:

- El Pilar I se refiere a los requisitos de capital mínimo teniendo en cuenta los principales riesgos que asumen los bancos, y que son los de crédito, de mercado y operacional.

- El Pilar II aborda la suficiencia de capital en los bancos, por encima de los requisitos mínimos, principalmente con el objeto de que dispongan de capital para cubrir pérdidas por otros riesgos y para enfrentar pérdidas ante choques en el entorno económico y financiero.

- El Pilar III persigue la transparencia de la situación financiera de los bancos en vista del importante papel de disciplina de mercado que se atribuye a los depositantes e inversionistas.

La industria bancaria y el comité enfrentan importantes desafíos en la implantación de Basilea II.

El nuevo marco es una convocatoria para perfeccionar la gestión y supervisión de los sistemas bancarios. Su objetivo, en última instancia, es promover la estabilidad financiera.
Dentro de las principales novedades de Basilea II constan:

- Requerimientos de capital más ajustados a los riesgos.
- Gama de opciones metodológicas.
- Reconocimiento explícito del riesgo operacional.
- Reducción de los requerimientos de capital por riesgo de crédito para varios tipos de exposiciones.
- Uso de modelos internos en los enfoques avanzados.

Basilea II exige el cumplimiento de pre-condiciones, ellas se refieren al estado de la regulación, supervisión y gestión de los bancos. En gran medida están contenidas en los Principios Básicos de Supervisión Bancaria Efectiva del Comité de Basilea.

Existen varios beneficios importantes en la implementación de Basilea II, el cumplimiento de estándares internacionales constituye una ventaja competitiva a nivel mundial, una administración efectiva de los riesgos de operación de los bancos permitirá reducir pérdidas significativas dentro de la organización y por tanto agrega valor a los inversionistas.

Si bien es cierto la implementación no es una tarea fácil y de corto plazo, los pasos que se están dando a través de los organismos reguladores o supervisores de cada país es

fundamental. Es importante elaborar una hoja de ruta que contenga el cronograma de implementación incluyendo planes individuales y colectivos que deben cumplirse.

El nuevo acuerdo de Basilea II ambiciona adaptar y unificar los criterios de solvencia a un nuevo contexto marcado por la responsabilidad, la globalización, el entorno competitivo, nuevas técnicas de medición, diversificación de riesgos. Más aun considerando la crisis mundial actual, resulta vital para las empresas disponer de estándares internacionales implementados apropiadamente.

Basilea II contempla también la tendencia generalizada en el aumento de la transparencia e información facilitada al inversor. Según el acuerdo, las entidades financieras deben hacer público su compromiso con los inversionistas, accionistas, clientes, etc., tanto en el aseguramiento de capital como en la optimización de la gestión de riesgos. Este aspecto se considera indispensable en un mundo cada vez más diversificado e inestable y algunas entidades lo están incorporando ya a su política de responsabilidad social. Con estas medidas se pretende, en definitiva, mejorar la confianza en los mercados, aumentar la seguridad e incentivar la inversión.

LOS TRES PILARES FUNDAMENTALES

1. NIVELES MÍNIMOS DE CAPITAL Y GESTIÓN DEL RIESGO

Basilea II incrementa los requisitos en el cálculo de los niveles mínimos de capital, basados en una estimación más adecuada del riesgo para hacer frente a hipotéticas situaciones críticas. Incluye además un nuevo cargo de capital por riesgo operacional. El Fondo Estadístico de insolvencias establece las provisiones por pérdida esperada y Basilea II pretende efectuar el cálculo para las pérdidas inesperadas. Esta unión de cálculos supone mayor discriminación del riesgo y mayor certeza.

Basilea II insiste en que la evaluación de riesgos del banco debe ser conservadora, sobre todo en las áreas donde existan más dudas, incluso evaluando factores de riesgo del horizonte futuro. En el marco del nuevo acuerdo, el aumento del control de los distintos tipos de riesgos y de su supervisión deberá tratarse desde un enfoque integral, lo que conlleva la inclusión de nuevos riesgos.

Los riesgos medioambientales han sido tradicionalmente excluidos del proceso de evaluación a la hora de conceder créditos o participar en operaciones financieras, sin embargo, cobran gran importancia con un enfoque integral y bajo una perspectiva de futuro. La actual normativa ambiental, la introducción del concepto de responsabilidad social corporativa y sobre todo, la obligatoriedad de incluir los aspectos medioambientales en las cuentas anuales de la empresa, justifica su evaluación. Sin embargo, es muy importante que la nueva gestión se adapte al funcionamiento interno de cada entidad y que se desarrollen herramientas específicas de medición del riesgo.

Herramientas de medición del riesgo crediticio

La utilización de modelos internos avanzados en la medición del riesgo crediticio requiere la utilización de nuevas herramientas de rentabilidad, denominadas scorings y ratings, y como acción urgente, la recolección de datos internos de pérdidas es uno de los elementos básicos que debe implementarse en la organización.

Por un lado, estas herramientas establecen una clasificación de las distintas operaciones y clientes de la entidad en función de su calidad crediticia, y por otro, estiman la probabilidad de impago o pérdida de capital de las mismas. En último término, es necesario poder contar con sistemas orientados a estimar la recuperación que podría llegar a alcanzar una entidad financiera en el caso en que se incumpliesen las operaciones de pago o fracasase una operación de inversión.

El Comité de Basilea ha elaborado un método avanzado, en el que los bancos pueden utilizar estimaciones internas de tres componentes del riesgo adicionales al carácter básico del método de calificación interna: pérdida dado el incumplimiento (LGD), exposición en el momento del incumplimiento (EAD) y el tratamiento de garantías/derivados crediticios.

La selección de factores de riesgo y criterios específicos de gestión tendrá que apoyarse en un análisis interno confiable realizado por el banco. Los criterios deben ser consecuentes con las normas internas de concesión de préstamos del banco y deben

reflejar la opinión del banco sobre cuáles son los principales impulsores de las pérdidas a través de las exposiciones. Un banco debe utilizar factores de riesgo que incorporen características claves del prestatario y del tipo de producto o transacción.

Asimismo, debe considerar también algunos factores globales, incluso algunas características jurisdiccionales (especialmente el régimen de insolvencia) y otros factores adicionales, que podrían afectar a las probables recuperaciones, todo ello con el objetivo de perfeccionar y ampliar su análisis interno.

Control del riesgo operativo

En lo referente al control del riesgo operativo el nuevo acuerdo de Basilea pretende reforzar los esfuerzos de evaluación exhortando a la industria financiera para que utilice un método avanzado de gestión interna y recopile datos históricos.

Si bien la medición de los riesgos de operación continúa aún en una fase de desarrollo, el Comité de Basilea considera que un programa de gestión de los riesgos de operación facilita la seguridad y solidez bancaria, y protege y aumenta el valor del accionista, por lo que propone incluir el tratamiento de estos riesgos con una importancia similar a la que tienen los riesgos crediticios y de mercado. Por tanto, los bancos de inversión, los bancos internacionalmente activos y en general, los bancos con una exposición importante al riesgo operativo, deben establecer un proceso independiente de gestión y control que cubra el diseño, ejecución y revisión de su metodología de medición. Las responsabilidades incluyen establecer el marco para la medición del riesgo operativo y el control sobre la elaboración de la metodología.

Los bancos deben llevar a cabo pruebas de debida diligencia y monitorear las actividades de los proveedores. Para actividades críticas, el banco puede necesitar considerar planes de contingencia, incluyendo la disponibilidad de proveedores alternativos, y los costos y recursos necesarios para cambiar de proveedores, potencialmente con muy corto aviso previo. Es importante también que haya una revisión crítica de los supuestos en que se basan los parámetros claves de estas metodologías de medición de los riesgos operativos. Con el fin de validar la

razonabilidad de las metodologías, un banco debe demostrar que sus procesos de medición del riesgo son estructurados adecuadamente y que los cálculos de riesgo resultantes incluyen adecuadamente los riesgos a los que está expuesto. Los resultados de cualquier metodología de medición de los riesgos operativos deben formar parte integral de las actividades diarias de gestión de riesgos del banco.

Por otra parte, el procedimiento para determinar la exigencia de capital por riesgo operativo implica la definición de un conjunto amplio de tipos de riesgos y su combinación con las diferentes líneas comerciales. Dentro de cada combinación línea comercial/tipo de riesgo, el supervisor determina un indicador de exposición (EI).
Adicionalmente, se mide, sobre la base de sus datos internos de pérdida, un parámetro que representa la probabilidad de una situación de pérdida (PE) y un parámetro que representa la pérdida dada esa situación (LGE). El producto de EI, PE y LGE se utiliza para calcular la pérdida prevista (EL).

En un futuro cercano, con la implantación definitiva de la gestión avanzada del riesgo propuesta por Basilea II, las entidades financieras medirán y controlarán de forma sistemática sus exposiciones a todo tipo de riesgos, incluidos los medioambientales, e incorporarán un análisis detallado de rentabilidad a todas sus inversiones.

Control de riesgos medioambientales

Rainforest Action Network, grupo ecologista estadounidense, inició hace unos tres años una campaña contra el gigante de la banca norteamericana Citigroup. La compañía era acusada de ser culpable de la destrucción de los bosques tropicales, del cambio climático y de la perturbación de la vida de los indígenas a causa de sus inversiones en infraestructuras. Debido a ello, los seguidores de esta ONG (cuantiosos en número) cancelaron sus tarjetas de crédito con Citigroup y las enviaron de vuelta al banco. Pero este no es el único caso en que el ecologismo se ha impuesto al sector bancario. El banco alemán WestLab entró en disputa con los ecologistas debido a un oleoducto financiado por ellos en Ecuador, al que acusaron de causar graves impactos ambientales.

Podríamos definir estos conflictos como riesgos medioambientales que afectan a la imagen de la entidad, pero existen otros tipos, asociados al crédito (menor solvencia del prestatario por inversiones imprevistas por acontecimientos medioambientales adversos), a aspectos legales (multas y cierre de actividad por actuaciones negligentes) o asociados a proyectos (pérdida de valor de la propiedad ofrecida como garantía).

Todos ellos afectan en última instancia a la reputación de la entidad y por ende a sus resultados económico financieros.

Las primeras instituciones financieras en aplicar los métodos de gestión de riesgos medioambientales se localizan en EEUU durante la década de los ochenta, como respuesta a las leyes Superfund. Hoy en día, la mayoría de las instituciones financieras consideran que la valoración del proceso productivo, de las contingencias medioambientales asociadas a la actividad y de la capacidad de la empresa para subsanarlas, determinada por el análisis de riesgos, constituye un factor clave en la definición de las condiciones crediticias.
Los riesgos medioambientales están asociados tanto a operaciones de inversión como de crédito.

2. REVISIÓN DEL ORGANISMO SUPERVISOR

El papel de los supervisores es vigilar la eficiencia con que los bancos evalúan sus necesidades de capital en función de sus riesgos, e intervenir cuando corresponda.

En España, la responsabilidad supervisora recae sobre el Banco de España. El regulador español es actualmente uno de los más exigentes y estrictos a nivel mundial. Con la Circular 9/99, el banco ya impuso la exigencia de gestionar los riesgos apoyándose en el Fondo Estadístico de Insolvencias, por lo que las entidades españolas ya cuentan con una base firme para adaptarse a los nuevos requerimientos de Basilea II. El banco deberá tener también procesos y criterios definidos para asignar una exposición a un grado de prestatario. Estos criterios deberán ser lo suficientemente específicos como para permitir una evaluación de la exposición por terceros.

Adicionalmente, los supervisores deben esperar que los bancos operen por encima de los coeficientes mínimos de capital regulador y tener la habilidad de exigirles que mantengan capital en exceso del mínimo si consideran que el perfil de las entidades así lo requiere.

3. DISCIPLINA DEL MERCADO (TRANSPARENCIA)

El cambio de escenario en la economía mundial exige a las empresas un aumento de la responsabilidad y mayores exigencias de transparencia y de información, lo que aumenta la seguridad del inversor. La política de publicación de información de la entidad ofrece a los inversores mejores criterios de valoración de su solidez financiera.
Con la aplicación de Basilea II, los bancos deberán divulgar sus objetivos y políticas de gestión de cada tipo de riesgo (de crédito, mercado, operativo, estructural.).

Será información periódica, estandarizada y orientada al mercado, comprensible, relevante, veraz y comparable. Además, los bancos deben hacer efectivo un proceso para evaluar la propiedad de su divulgación, incluyendo la frecuencia de ésta.

Todas las instituciones tendrán que informar entre otros datos: el monto de reservas para incobrables, los índices de incumplimiento promedio para créditos clasificados en cada categoría, la estructura, gestión y organización de su procedimiento de control de riesgos y sus estrategias, objetivos y prácticas de mejora de esta gestión. Para poder llevar a cabo la divulgación, es necesario capturar y almacenar información actual e histórica sobre el riesgo de operaciones, las herramientas de calificación de riesgos o las acciones mitigadoras. La utilización de esta información permitirá por un lado realizar el cálculo de las pérdidas esperadas y del nivel mínimo de capital requerido, y por otro, informar a la entidad supervisora y a los inversores.

INVERSIONES Y BENEFICIOS DERIVADOS DE LA APLICACIÓN DE BASILEA II

Las principales inversiones se destinarán a la formación del personal y la adaptación de los sistemas principalmente para: confección de bases de datos, cálculos de capital por

categorías o tipos de riesgo, adicionalmente integración de herramientas, supervisión y comunicación.

Los beneficios derivados de la aplicación de los modelos internos avanzados vendrán condicionados por la incorporación de nuevos procesos y herramientas en el control del riesgo, que implicarán importantes ahorros de capital. Adicionalmente, proporcionará la información suficiente para permitir que el mercado evalúe su exposición al riesgo operativo y la calidad de su gestión, otorgándoles una gran ventaja competitiva.

A los accionistas les ofrece la posibilidad de mejorar el perfil riesgo/rentabilidad de las carteras de crédito y como consecuencia el retorno sobre capital.

A los acreedores les ofrece unas carteras de crédito más equilibradas que reducen la posibilidad de que eventos adversos puedan poner en peligro el cobro de sus deudas.

A los clientes la reducción de concentraciones y la existencia de nuevos productos para cubrir sus necesidades y una política más personalizada y ajustada a las características crediticias de cada uno de ellos que se podrá traducir en mejores precios en las financiaciones solicitadas.

En los últimos meses afloran las críticas hacia Basilea II, principalmente debido al elevado coste de implantación (entre 5.000 y 10.000 millones de euros en la Unión Europea según la European Private Equity & Venture Capital Association –EVCA-) y la complejidad del modelo avanzado de estimación del riesgo. La Federación Europea de Bancos, la Asociación de Banqueros Británicos (BBA), el Instituto de Finanzas Internacionales y la Asociación Española de Banca (AEB) son algunas de las entidades que reclaman mayor flexibilidad y plazos más amplios para la aplicación de Basilea II.

Sin embargo, es altamente probable que las entidades menos predispuestas a la aplicación de Basilea tengan dificultad en un futuro para acceder a las fuentes de financiación y vean intensificados sus problemas competitivos, las entidades más avanzadas serán las que más evolucionen y se diferencien del resto.

La incorporación del método avanzado propuesto por Basilea II supone finalmente un incentivo competitivo que pueden tener las entidades para implantar nuevas prevenciones y controles de pérdidas operativas, tener una menor carga de recursos propios y poder ser más agresivos comercialmente.
En definitiva, Basilea II supondrá no aumentar las pérdidas por fallidos y prevenir las pérdidas inesperadas por el mayor control de riesgos, liberando recursos por la optimización en el cálculo de provisiones. Básicamente, frente a la cultura tradicional de prevención, Basilea II presenta un nuevo horizonte de cuantificación y gestión activa del riesgo donde tiene cabida el control de nuevos aspectos, como los medioambientales.

1.2.4 Situación actual de la regulación y supervisión del riesgo operacional en algunos sistemas financieros de la región.

No existe mucha información comparativa sobre el avance de la implementación de riesgo operacional en Latinoamérica, sin embargo, en un análisis realizado por Everis, una consultora española, sobre el riesgo operacional en las entidades financieras en Latinoamérica, se mencionan hechos significativos como:

- Un alto porcentaje de las entidades considera que la implantación de las normas de Basilea II, en relación al riesgo operacional, es una oportunidad de gestionar adecuadamente el riesgo, generando una ventaja competitiva, y mitigando el riesgo, con lo cual se pueden evitar pérdidas millonarias.

- El estudio tomó una muestra de las principales entidades financieras de Brasil, Chile y México. En esto encuentran parecido con las entidades españolas, bastante preocupadas de le medición del riesgo operacional.

- El análisis realizado se fundamenta en dos áreas: dónde se producen las pérdidas operacionales y cómo medir y vigilar su evolución.

- Las entidades financieras latinoamericanas están desarrollando sistemas acoplados a sus realidades, pues están conscientes de que las pérdidas operacionales pueden ser sumamente significativas.

- El estudio permitió determinar que las entidades perciben como críticos los riesgos de:
  - gestión de procesos,
  - fraude externo,
  - interrupciones en el negocio
  - y fallas en los sistemas.

La concentración de Riesgo Operacional por Línea de Negocio concentra más el riesgo según el estudio en la Banca Empresarial, representando el 18% del total.

Dicho estudio también determina que las entidades más grandes concentran más riesgo operacional, sin embargo, tienen mayor madurez en su percepción del mapa de riesgo operacional.

Para medir el riesgo, las entidades están utilizando herramientas como:

- Autoevaluaciones (33%)
- Mapas de Procesos (23%), ya que estas mejoran el conocimiento de la organización.
- Indicadores y Alarmas (31%)
- Bases de Datos de Pérdidas Operacionales (33%).

Entre los impactos logrados con el modelo de gestión, figuran principalmente: la concienciación sobre la relevancia e impacto del riesgo operacional, la implementación de objetivos de control de riesgo por áreas, aspectos que han fortalecido significativamente el control y mitigado el riesgo.

Por otro lado, en análisis efectuados por otras consultoras, como DP&A, estarían a la cabeza México y Perú. Este último coincide con la evaluación realizada por el FMI, que evaluó muy positivamente el estado de avance de aplicación de la norma en este país.

Por otro lado, existen países como Costa Rica donde, a pesar de tener implementadas ciertas normas, aquéllas relacionadas con el riesgo operacional serán implementadas.

A continuación indicamos información referencial sobre las diferentes normativas emitidas en cada país:

Perú (enero de 2002):

La SBS aprobó el Reglamento para la Administración de los Riesgos de Operación. Definición de RO. Responsabilidades del Directorio, gerencia general, unidad de riesgos. Estructura adecuada, independencia entre la unidad de riesgos y otras unidades de negocio. Gestión del RO, etc.

Ecuador (octubre 2005):

Ley General de Instituciones Financieras (1994)
Ley de Comercio Electrónico
Ley de Transparencia
Resolución No. JB-2005-834 emitida por la Superintendencia de Bancos y Seguros del Ecuador. Regula la administración de riesgo operativo considerando sus cuatro factores: procesos, personas, tecnología, eventos externos. Adicional administración de riesgo operacional y planes de contingencia y continuidad.

Chile (agosto 2005):

La SBIF toma como marco de referencia la definición del BCBS. La SBIF evalúa el rol del directorio y la alta gerencia y la aprobación que han dado a la estrategia para administrar el RO. Se numeran los aspectos que revelan una "buena gestión del RO" (que existan definiciones, una función encargada de la gestión, estrategia apropiada, etc.)

México (diciembre 2005):

Los bancos deben observar los lineamientos mínimos sobre la Administración Integral de Riesgos (AIR), que incluye al Riesgo Operacional.

Riesgos: No cuantificables / Cuantificables: Discrecionales y no discrecionales => Riesgo Operacional.

Definir objetivos sobre exposición al riesgo. Desarrollar políticas y procedimientos para gestión. Delimitar funciones y responsabilidades, etc.

Brasil (junio 2006):

El BCB estableció que los bancos deben implementar una estructura de gestión del Riesgo Operacional, definiendo a ese riesgo y a una clasificación de eventos operativos de acuerdo con Basilea. Define las responsabilidades del Directorio y de una unidad específica. En línea con las buenas prácticas del BCBS (2003)

Colombia (diciembre 2006):

La SFC fijó los requisitos mínimos para la implementación del Sistema de Administración del RO (SARO). Normativa muy detallada y taxativa.
Requiere: estructura organizacional, Unidad de RO distinta de auditoría, mantener un registro de eventos de RO, medición cuantitativa y cualitativa (“evaluación”), etc

Uruguay (julio 2007):

Estándares de gestión de riesgos. Definición de RO. Responsabilidades del directorio. Gerencia responsable. Registro de eventos de pérdida. Disposiciones en línea con BCBS 2003.

Argentina (diciembre 2006):

En Diciembre 2006 el BCRA aprobó su “Hoja de ruta” para la implementación de Basilea II.

Respecto del Riesgo Operacional: está en estudio el enfoque específico a adoptar para la medición del capital por Riesgo Operacional (Pilar I).

No obstante hay que avanzar en los requerimientos de buenas prácticas de gestión del Riesgo Operacional.

Avanzar en el diseño de estándares mínimos para la recolección y reporte de datos.

CAPÍTULO II EL RIESGO OPERACIONAL

2.1 Concepto de Riesgo Operacional, Alcance de la aplicación de la norma y Glosario de Términos relacionados.

2.1.1 Definición de Riesgo Operacional

El riesgo operacional de acuerdo al marco de Basilea II se define como el riesgo de pérdida debido a la inadecuación o a fallos en los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos.

Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación. Sus objetivos se basan en identificar los riesgos, monitorear que los mismos se mitigan a niveles aceptables y cuantificar su consumo de capital.

De acuerdo a lo establecido en la resolución JB-2005-834, el riesgo operativo es la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.

El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

El riesgo operativo incluye el riesgo legal, definido como la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una institución del sistema financiero, derivadas de error, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones. El riesgo legal surge también de incumplimientos de las leyes o normas aplicables.

Fuente1: Buenas prácticas para la gestión y supervisión del riesgo operativo (Basilea II)
Fuente2: Superintendencia de Bancos y Seguros del Ecuador

COMENTARIO:

El conocimiento del riesgo operativo en las Instituciones Financieras no es nuevo, con la emisión de los principios de Basilea y ahora con la norma de la Superintendencia de Bancos ha cobrado mucho protagonismo, lo cual favorece a las entidades controladas ya que recoge en un documento específico las mejores prácticas que se pueden aplicar para administrarlo de manera eficiente, lo cual permite minimizar el riesgo de pérdida que puede tener una institución.

Por ejemplo: en una operación simple como un depósito en el banco pueden existir riesgos operativos que pueden ir desde fallas del sistema, errores al ingresar o validar los datos del cliente, fallas eléctricas, etc. si bien es cierto los sistemas bancarios cuentan con un sinnúmero de controles, existen factores de riesgo como el factor de personas, eventos externos o procedimientos que no son claros o no se han difundido de manera óptima y que ocasionan estas fallas.

El riesgo de las operaciones que muchas veces son evaluadas únicamente desde la perspectiva de negocio, o que en muchos casos no son considerados para evaluar el costo real de un servicio, gracias a la implementación de la norma pueden ser clasificados, valorados y por tanto también minimizados a través de controles efectivos. Es una forma de concientizar a la organización de la importancia que tienen en la prestación de servicios.

Otra ventaja derivada de la emisión de la normativa constituye la interiorización que se puede lograr en todos los niveles de la organización, ya sea a través de capacitación, talleres, etc. contribuyendo a mejorar el control interno.

Para el caso específico de los auditores internos también es una ventaja contar con la norma, siendo un marco de referencia y para hacer el respectivo seguimiento de su implementación.

2.1.2 Alcance de la aplicación de la norma

Haciendo un breve resumen de lo indicado en la norma podemos mencionar que las disposiciones de la norma de Riesgo Operacional emitida por la Junta Bancaria, son aplicables a las Instituciones Financieras públicas y privadas, al Banco Central del Ecuador, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros, a las cuales, dentro de la normativa se las denomina como instituciones controladas.

La resolución establece que antes de determinar cargos de capital por riesgo operativo, las Instituciones Financieras deberán desarrollar un ambiente apropiado de gestión de riesgo operativo. Esto implica asegurar una gestión efectiva de los procesos institucionales, recursos humanos y tecnología de la información, estableciendo y validando planes de contingencia y de continuidad de negocio.

Se estableció como parte de la norma que las instituciones supervisadas presenten su evaluación y un plan para poner en práctica las nuevas provisiones de gestión de riesgo operativo a la Superintendencia de Bancos y Seguros, dentro de seis meses después de la fecha de emisión de la resolución. El plan de puesta en práctica, debía estar aprobado por la junta directiva de la institución, e incluir el detalle de actividades y responsables de su ejecución.

Para el caso de las cooperativas de ahorro y crédito el plazo para la presentación del diagnóstico y proyecto de implementación es de un año contado a partir de la fecha de emisión.

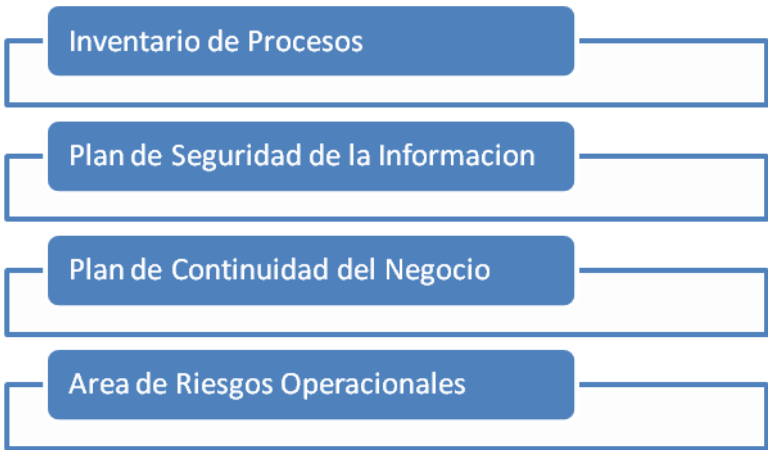
La implementación de la norma para las Instituciones Financieras, de acuerdo a la última notificación de la Superintendencia tiene como plazo máximo hasta agosto del 2009.

Para las cooperativas de ahorro y crédito que realizan intermediación con el público y las asociaciones mutualistas de ahorro y crédito para la vivienda, hasta cuatro años de plazo a partir de la presentación de su evaluación y plan de implementación.

Fuente: Superintendencia de Bancos y Seguros

COMENTARIO:

Considerando el alcance expuesto en la normativa entendemos que el proceso de gestión de riesgos operativos puede estar contenido en las siguientes actividades a desarrollar por parte de la Organización y sobre las que existe participación de todos los factores de riesgo:



Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

En primer lugar se encuentra el inventario de procesos, resulta imprescindible que exista este documento para determinar el nivel de criticidad que tienen frente al negocio, clasificados según lo dispone la norma. Esta es una tarea compartida por algunas áreas y lideradas por el o los responsables del proyecto de implementación.

Los criterios para determinar su nivel de criticidad pueden variar en cada Institución, entre los temas a considerar pueden estar: nivel de participación del proceso en los ingresos de la organización, porcentaje que representa en el balance general, es un

proceso al cual no podemos dejar de dar servicio, es decir debemos asegurar su continuidad en el tiempo, etc.

Una vez clasificados los procesos podemos otorgarles una prioridad para el levantamiento de todos los subprocesos inmersos llegando al nivel de detalle que se haya decidido en concenso.

Existen algunas técnicas que pueden servir para llevar a cabo esta tarea como: obtener de los responsables de los procesos un detalle de actividades, organizar grupos de trabajo para elaborar el mapa del proceso, obtener los procesos del área de Auditoría Interna, que normalmente en sus evaluaciones incluye flujogramas, etc.
El nivel de actualización de esta documentación marcará el gap o brecha frente a lo indicado por la norma con respecto a procesos, si bien es cierto puede ser considerado como un proceso permanente de actualización, es importante hacer un corte y establecer el estatus y posterior el plan de acción o cronograma con el fin de dar cumplimiento a la norma en los plazos establecidos.

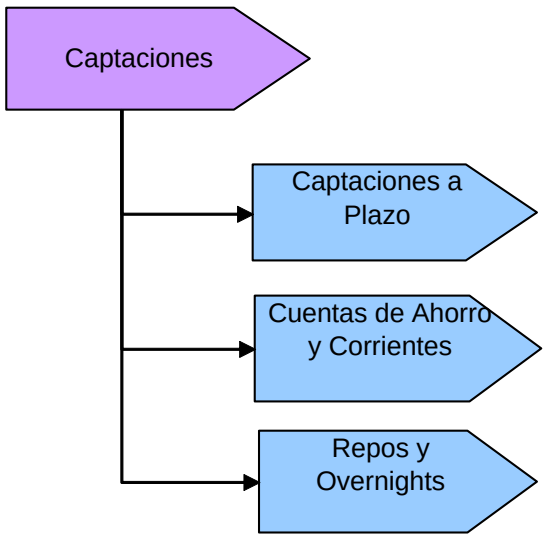
A manera de ejemplo de la clasificación de los procesos podemos indicar algunos que son parte de las Instituciones controladas y que no deben faltar en este inventario:

Clasificación	Macro Proceso	Total Procesos	Procesos Críticos
Estratégicos	Dirección del Negocio	3	1
	Administración Integral de Riesgos y Control Interno	8	1
Productivos	Diseño y Desarrollo de productos y servicios	9	2
	Captaciones	6	4
	Colocaciones	5	3
	Cobranzas y Recuperaciones	4	3
	Servicios Bancarios	10	8
De Apoyo	Administración de Canales	4	2
	Desarrollo y Gestión del Capital Humano	8	4

	Administración de Recursos de Tecnología de Información	7	3
	Gestión Contable	5	2
	Seguridad Corporativa	4	2

Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

Es fundamental que el relevamiento de los procesos se realice con un estándar para toda la organización, mejor si se puede contar con alguna herramienta que facilite esta tarea. La persona encargada del proceso debe ser quien facilite la información correspondiente para que el personal asignado modele y detalle al nivel que la organización estime, se puede llegar a nivel de tareas inclusive, todos los pasos o sub procesos que lo conforman. Adjuntamos un ejemplo del macro proceso de Captaciones con sus sub procesos definidos, luego se desarolla cada uno de ellos a nivel de detalle:



Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

Con respecto a la Seguridad de la Información, primero que nada debe existir el nivel de entendimiento de cómo establecer un plan que permita a las Instituciones contar con controles eficientes considerando que Tecnología es un factor preponderante en este proceso.

Aquí identificamos cuatro etapas para lograr el objetivo:

- Conocer y entender la Infraestructura de Tecnología.
- Identificar y evaluar los riesgos de Tecnología.
- Establecer el plan de seguridad de la información.
- Implementar el plan de seguridad de la información.

Conocer y entender la infraestructura de tecnología que apalanca los principales negocios del Banco o los procesos críticos, es uno de los principales objetivos que se debe plantear la organización.

Esta actividad debería al menos cubrir la documentación que dispone Tecnología, según lo indicado en la norma, identificar los sistemas de mision crítica, las aplicaciones principales del Banco, revisar procesos como control de cambios de aplicaciones, analizar la información según el nivel de sensitividad en base a los conceptos de cofidencialidad, integridad y disponibilidad de la misma, entre los más importantes.

Una vez que conocemos lo que la Insitución tiene, podemos establecer prioridades según el nivel de criticidad frente al negocio del Banco, así tambien se debe realizar la evaluación de los riesgos de tecnología, y si hubieran brechas que cumplir deben identificarse incluyendo los responsables y fechas de cumplimiento.

En este tipo de análisis se debe mantener presente que la información es el principal activo de la organización, pero también el exceso de controles puede generar descontrol.

Entre algunos de los principales riesgos informáticos podemos mencionar los siguientes:

RIESGOS INFORMATICOS
Fraudes informáticos
Interrupción de servicios
Accesos indebidos
Procedimientos incompletos o no existentes
Virus
Software ilegal
Agujeros de seguridad en redes
Intercepción de comunicaciones
Fallas en los equipos centrales
Falta de esquemas de recuperación
Empleados deshonestos
Denegación de servicios
Incumplimiento de leyes y regulaciones
Violación a correos electrónicos
Falta de segregación de funciones
Falta de administración de permisos en los servidores
Planes de contingencia errados o no existentes
Uso de claves default para administración
Errores en configuraciones de equipos

Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

El plan de seguridad así como su implementación dependen del resultado de este diagnóstico. Ojo que también en este análisis puede derivarse inversión en herramientas o recursos que deben ser tomados en cuenta para incluir en las fechas de cumplimiento.

Siempre es mejor acompañarse de metodologías que ya existen en el mercado para la evaluación de riesgos de Tecnología, principalmente Cobit, ISO27001, ISO 27005, ITIL, PSI, etc. Estas metodologías si bien no son de aplicación obligatoria brindan el marco teórico ideal para este tipo de evaluaciones, en la mayoría de casos son de libre distribución lo cual siempre es ventajoso.

En relación al Plan de Continuidad del Negocio existen de igual manera innumerables metodologías que se podrían aplicar sin problema, sin embargo es ideal que tomando en cuenta la realidad del negocio y los procesos críticos levantados, contar con una metodología hecha a medida.

Este es un proceso en el que es importante nombrar un coordinador general que gestione la elaboración de toda la documentación, pruebas, actualizaciones, análisis, etc. que se debe gestionar como parte de este análisis.

Hemos destinado un capítulo completo sobre este tema, por lo que no nos detendremos mayormente en esta instancia.

Con respecto a la estructura organizacional del Área de Riesgos, la norma apoya en el sentido de distinguir las principales responsabilidades que tienen todos los funcionarios desde el Directorio del Banco. Esto a nuestro criterio favorece la implementación de la norma toda vez que con el auspicio de la Alta Gerencia muchas veces tiene mayor importancia frente a otras actividades propias de la gestión bancaria.

Los niveles de reporte de los coordinadores o responsables de este proyecto también deben estar debidamente identificados para evitar malos entendidos.

En mayo de este año la Superintendencia de Bancos destinó un equipo de trabajo que tuvo a cargo la evaluación del cumplimiento a esa fecha, con miras a establecer si el nivel de avance justifica que se mantenga la fecha tope del 31 de agosto del 2009.

De lo que hemos podido conocer si bien el avance es importante hay temas como el mismo Plan de continuidad que demandan recursos para contar con sitios alternos, de operación o tecnológicos que no estamos seguras se cumplirán hasta la fecha estipulada, no obstante el haber participado en el diagnóstico de la Superintendencia nos ha permitido conocer si se esta por buen camino o hay que hacer ajustes de alcance o fechas de cumplimiento.

2.1.3 Glosario de Términos relacionados

Para efectos de la aplicación de las disposiciones se considerarán las siguientes definiciones:

Alta gerencia.- La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

Evento de riesgo operativo.- Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

Factor de riesgo operativo.- Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos;

Proceso.- Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

Insumo.- Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

Proceso crítico.- Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

Actividad.- Es el conjunto de tareas;

Tarea.- Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y mesurable;

Procedimiento.- Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad;

Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones;

Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

Tecnología de información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones;

Instalaciones.- Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información;

Responsable de la información.- Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones;

Seguridad de la información.- Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

Seguridades lógicas.- Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

Confidencialidad.- Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

Integridad.- Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

Disponibilidad.- Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

Cumplimiento.- Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

Pista de auditoría.- Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

Medios electrónicos.- Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

Transferencia electrónica de información.- Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

Encriptación.- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino;

Plan de continuidad.- Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación;

Plan de contingencia.- Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento;

Plan de reanudación.- Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema;

Plan de recuperación.- Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución;

Eficacia.- Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

Eficiencia.- Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores; y,

Riesgo Legal.- Es la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una institución del sistema financiero, derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones.
El riesgo legal surge también de incumplimientos de las leyes o normas aplicables.

Fuente: Superintendencia de Bancos y Seguros

COMENTARIO:

Es ventajoso manejar los mismos términos y conceptos dentro de todo el sistema financiero, esto permitirá una mayor compresión del alcance y aplicabilidad de lo establecido en toda la organización.

2.2 Factores del riesgo operacional.

Con el propósito de minimizar la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, la norma define a los siguientes factores como la causa primaria o el origen de un evento de riesgo operativo:

- Procesos,
- Personas,
- Tecnología de información, y;
- Eventos externos.

PROCESOS:
La norma ha establecido los siguientes grupos de procesos, considerando que es importante estructurar y organizar a los mismos en función de la misión, visión y objetivos estratégicos:

- Gobernantes o estratégicos;
- Fundamentales, productivos, de negocio u operativos; y,

- Habilitantes, de soporte o de apoyo

Procesos gobernantes o estratégicos: Son aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

Procesos productivos, fundamentales u operativos: Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

Procesos habilitantes, de soporte o apoyo: Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Adicionalmente la norma dispone que las entidades identifiquen, aún en los servicios provistos por terceros, sus procesos críticos, es decir, aquellos que en caso de una interrupción pondrían en peligro la continuidad de las operaciones; por lo cual, se justifica plenamente establecer planes de contingencia y de continuidad del negocio.

Estos procesos identificados y controlados deben ser sometidos a una mejora continua, a través de políticas que permitan identificar, diseñar, medir, analizar, actualizar y controlar los procesos.

Una vez que se hayan identificado todos los procesos críticos es necesario que se implementen mecanismos que minimicen los riesgos en cada uno de ellos. Para ello, las instituciones deben contar con políticas que incluyan:

- diseño claro de los procesos, los cuales deben ser adaptables y dinámicos;

- descripción en secuencia lógica y ordenada de las actividades, tareas, y controles;
- determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros;
- difusión y comunicación de los procesos buscando garantizar su total aplicación; y,
- actualización y mejora continua a través del seguimiento permanente en su aplicación.

Otro aspecto importante es la separación de funciones que debe existir en la Institución, lo cual contribuye a minimizar riesgos de fraude, errores, omisiones, y cualquier otro evento que pudiera darse.

Es importante que exista una actualización permanente del inventario de procesos que contemple información del tipo de proceso, nombre del proceso, responsable, productos y servicios que genera el proceso, clientes, fecha de actualización, nivel de criticidad del proceso.

PERSONAS:

Con la finalidad de que se promueva una cultura laboral y se alcance un trabajo eficiente y eficaz es necesario que las entidades definan políticas y procedimientos para la administración del recurso humano en los procesos de: selección o incorporación, permanencia y desvinculación de personal.

Estos procedimientos deben incluir: reclutamiento, selección, determinación de competencias, contratación, planes de carreras, evaluaciones de desempeño, criterios de remuneración, motivación, clima organizacional, higiene y seguridad, condiciones físicas y ambientales, rotación, finalización de la relación laboral, entre otros.

Los procesos de incorporación, incluyen:

- planificación de necesidades,
- reclutamiento,
- selección,
- contratación e inducción de nuevo personal.

Los procesos de permanencia, contemplan:

- condiciones laborales idóneas;
- promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos,
- competencias y destrezas;
- la existencia de un sistema de evaluación del desempeño;
- desarrollo de carrera;
- rendición de cuentas;
- incentivos que motiven la adhesión a los valores y controles institucionales

Los procesos de desvinculación, comprenden:

- planificación de la salida del personal por causas regulares,
- preparación de aspectos jurídicos para llegar al finiquito
- finalización de la relación laboral.

Estos procesos deben ser soportados técnicamente, de acuerdo con las disposiciones legales y deben incluir entre otras cosas con una evaluación sobre el personal, tomando en cuenta las competencias idóneas, formación académica, valores, actitudes y habilidades personales que puedan contribuir a minimizar los riesgos anteriormente descritos relacionados con el factor personas, así como también al crecimiento económico de las Instituciones a través de la adecuada administración de los riesgos.

Para lograr estos objetivos es imprescindible contar con información actualizada del capital humano, incluyendo toda la información propia del personal así como un historial de capacitación recibida, historial de cargos, evaluaciones, fechas y causas de separación, y demás información que la Institución considere necesaria.

TECNOLOGÍA DE INFORMACIÓN

En relación a la tecnología, la expectativa es que las Instituciones cuenten con una tecnología de información que soporte adecuadamente las operaciones y procesos de las entidades. Para esto, es necesario que las entidades planifiquen ordenadamente sus requerimientos actuales y futuros de tecnología; que establezcan toda una serie de requisitos y condiciones de seguridad y de continuidad del negocio, de manera que, puedan contar en todo momento con información íntegra, disponible y confidencial.

Con la finalidad de minimizar estos riesgos la normativa considera necesario que las Instituciones adopten o implementen políticas, procesos y procedimientos formalmente definidos que aseguren una adecuada planificación y administración de la tecnología de información, relacionadas a:

1. Con el fin de otorgar un soporte adecuado de los requerimientos de operación actuales y futuros de la entidad a través de una apropiada gestión de tecnología de información, deberán contar con un plan funcional de tecnología alineado con el plan estratégico, además un plan operativo que contenga todas las actividades que se realizaran durante un año, apoyo del directorio u organismo que haga sus veces y de la alta gerencia.

   Adicional la tecnología de información debe estar alineada a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada de acuerdo con las necesidades de la Institución.
   Es importante contar con un responsable de la información encargado de la definición y autorización de manera formal de los accesos y cambios funcionales a las aplicaciones y monitoreo del cumplimiento de los controles establecidos.

   En cuanto a las políticas, procesos y procedimientos de tecnología, deben ser elaboradas tomando como referencia estándares de general aceptación que permitirán asegurar la eficiencia, eficacia y cumplimiento de los criterios de control aplicados, avalados por las principales autoridades de la Institución.

Para que estas políticas y procedimientos sean efectivas es necesario que exista un esquema apropiado de difusión y comunicación a todo el personal. De igual manera la capacitación es importante no solo en temas relacionados con el negocio y operaciones sino también en temas relacionados a la tecnología de la información.

2. Para garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar con manuales o reglamentos internos, que establezcan responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento y respuesta a incidentes de tecnología.

   Adicionalmente es importante contar con un procedimiento de clasificación y control de activos de tecnología de información, considerando su registro, identificación, responsables de su uso y mantenimiento.

3. En relación a los servicios provistos por terceros la norma determina que estos deben ser administrados basándose en responsabilidades claramente definidas y sometidas a monitoreo en su eficiencia y efectividad, para lo cual deben tomar en cuenta dentro de los requerimientos contractuales la definición de la propiedad de la información y aplicaciones, la responsabilidad de la empresa proveedora sobre vulnerabilidades en sus sistemas con el fin de salvaguardar la integridad, disponibilidad y confidencialidad de la información.

   Adicionalmente deben considerar la inclusión de convenios que definan que las aplicaciones sean parametrizables, la transferencia de conocimiento de las mismas, así como la documentación técnica y de usuario que reduzca la dependencia del proveedor con los riesgos que esto implica.

4. Con respecto a la seguridad de la información que debe manejar la Institución la norma considera que para minimizar riesgos de uso, revelación y modificación no autorizados, las Instituciones tienen que contar con:
   - Políticas y procedimientos de seguridad de la información,

- Identificación de los requerimientos de seguridad de la información relacionados con la tecnología de información,
- Controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información,
- Un sistema de administración de las seguridades de acceso a la información,
- Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones,
- Sistemas de control y autenticación adecuados para evitar accesos no autorizados,
- Apropiados controles para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia,
- Controles formales para proteger la información contenida en documentos, medios de almacenamiento u otros dispositivos externos,
- Instalaciones de procesamiento de información critica en áreas protegidas con los suficientes controles de acceso,
- Condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento de la infraestructura de tecnología,
- Planes para evaluación del desempeño del sistema de administración de la seguridad de la información que permita tomar acciones para mejorarlo,
- Políticas y procedimientos de seguridad de la información que aseguren las transferencias y transacciones electrónicas.

5. En relación a la continuidad de las operaciones, las instituciones deberán contar con controles para minimizar riesgos potenciales de sus equipos ante fallas, daños o insuficiencia; así como con políticas y procedimientos de respaldos de información periódicos y en una ubicación remota, además de sistemas de comunicaciones y redundancia de los mismos.

6. En lo que se refiere al proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones las instituciones controladas deben disponer de una metodología apropiada para la administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones. Adicionalmente deben tener la documentación técnica y de usuario, y controles que

permitan administrar las versiones de las aplicaciones puestas en producción, de tal manera que se asegure la calidad de la información cumpliendo las características de integridad, disponibilidad y confidencialidad de la misma.

7. De igual manera es importante que exista adecuada administración de la infraestructura tecnológica que soporta las operaciones, monitoreo y documentación apropiada.

EVENTOS EXTERNOS

Otro factor importante dentro del riesgo operacional lo constituyen los eventos externos, principalmente relacionados con amenazas externas a los que las Instituciones están expuestas como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados, y actos delictivos. Para minimizar el impacto que pueden producir estos aspectos, es muy importante que las Instituciones controladas cuenten con planes de contingencia y de continuidad del negocio debidamente estructurados.

Fuente: Superintendencia de Bancos y Seguros

COMENTARIO:

Un apropiado ambiente de gestión de riesgo operativo, se construye basándose en el diagnóstico correcto de los riesgos que tiene la Institución considerando cada uno de los factores definidos, y la ejecución de planes que deriven en el cumplimiento de los aspectos incluidos en la norma.

De manera que sea más ilustrativa el contenido de esta parte de la norma y a modo de ejemplo presentamos el siguiente grafico sobre el que comentaremos mas adelante:

Factor de Riesgo	Tipo de Evento
Procesos	Deficiencias en la administración de procesos: falta de gestión permanente
Personas	Fraude Interno Fallas en procesos de negocio
Tecnología	Interrupción en el servicio por fallas en la tecnología
Eventos externos	Fraude externo Daños físicos

Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

Los factores o protagonistas del riesgo operacional deben ser analizados desde un contexto más amplio, tomando en cuenta que por ejemplo por más que la organización tenga la mejor tecnología del mercado está expuesta a fallas humanas, eventos externos, cambios en los procesos de manera desordenada, etc.

A cada factor se le asocian además varios riesgos específicos que deben ser evaluados y mitigados en la medida de lo posible.

La administración del recurso humano que es el proceso mediante el cual las instituciones planifican y gestionan el recurso humano para promover su desempeño eficiente y alcanzar los objetivos individuales de las personas y los objetivos institucionales, debe ser tomado como uno de los puntales mas importantes de la Institución.

Por otro lado considerando el índice de fraudes externos, violencia, situación política y social a nivel mundial no debemos desconocer que los eventos de tipo externo son cada vez más numerosos por ejemplo: fraudes electrónicos, asaltos express, violencia en cajeros automáticos, etc. por lo que la Institución debe dedicar especial atención al análisis y valoración de estos riesgos para poder aplicar soluciones concretas que optimicen las transacciones y aseguren su funcionalidad de manera permanente.

El mundo está cambiando y los riesgos también, aquellas medidas que en algún momento fueron adoptadas pueden ya no contribuir a minimizar el riesgo, la evaluación por lo tanto deberá efectuarse de manera permanente.

2.3 Contenido de la Resolución No. JB-2005-834 emitida por la Superintendencia de Bancos y Seguros del Ecuador.

RESOLUCIÓN No. JB-2005-834

LA JUNTA BANCARIA

CONSIDERANDO:

Que en el subtítulo VI “De la gestión y administración de riesgos”, del título VII “De los activos y de los límites de crédito” de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, consta el capítulo I “De la gestión integral y control de riesgos”;

Que en el artículo 1, de la sección I “Alcance y definiciones”, del citado capítulo I, se establece que las instituciones del sistema financiero controladas por la Superintendencia de Bancos y Seguros deberán establecer esquemas eficientes y efectivos de administración y control de todos los riesgos a los que se encuentran expuestas en el desarrollo del negocio, conforme con su objeto social, sin perjuicio del cumplimiento de las obligaciones que sobre la materia establezcan otras normas especiales o particulares;

Que la Superintendencia de Bancos y Seguros debe propender a que las instituciones del sistema financiero cuenten con un sistema de administración del riesgo operativo que les permita identificar, medir, controlar / mitigar y monitorear los riesgos de manera que se fortalezca su seguridad y solidez, en orden a proteger los intereses del público, de acuerdo a lo señalado en el artículo 1 de la Ley General de Instituciones del Sistema Financiero;

Que entre los riesgos frecuentes a las que están expuestas las instituciones del sistema financiero en el desarrollo de sus actividades se encuentra el riesgo operativo;

Que las instituciones del sistema financiero deben gestionar el riesgo operativo, como elemento fundamental de una administración preventiva que reduzca la posibilidad de pérdidas e incremente su eficiencia, para lo cual deberán implantar mecanismos, procesos y contar con recursos humanos calificados y experimentados a fin de mitigar este riesgo;

Que el Comité de Supervisión Bancaria de Basilea ha definido principios que recomienda sean aplicados por las instituciones del sistema financiero para la conformación de un adecuado ambiente para la administración cualitativa del riesgo operativo y que deben ser considerados por los supervisores al evaluar la gestión realizada por las instituciones controladas;

Que es necesario establecer estándares mínimos prudenciales para que las instituciones del sistema financiero administren el riesgo operativo en un ambiente favorable, previo a la medición del mismo para posteriores requerimientos de capital;

Que el control por parte del supervisor no consiste únicamente en garantizar que las instituciones del sistema financiero posean el capital necesario para cubrir los riesgos de sus actividades, sino también en alentarlas a que desarrollen y utilicen mejores técnicas de gestión de sus riesgos que les permita ser más eficientes y competitivas en el entorno de globalización de los negocios bancarios;

Que la Superintendencia de Bancos y Seguros, como parte de su política de comunicación y transparencia, puso en conocimiento previo el tema materia de esta norma, a los gremios y asociaciones de las instituciones controladas que tendrán que aplicarla;

Que el Comité Normativo y de Políticas de Supervisión y de Administración Interna de la Superintendencia de Bancos y Seguros, en sesión celebrada el 11 de octubre del 2005,

conoció y luego del análisis y discusión de su contenido recomendó a la Junta Bancaria la aprobación de la norma de riesgo operativo; y,

En ejercicio de la atribución legal que le otorga la letra b) del artículo 175 de la Ley General de Instituciones del Sistema Financiero,

RESUELVE:

ARTÍCULO 1.- En el subtítulo VI "De la gestión y administración de riesgos", del título VII "De los activos y de los límites de crédito" de la Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria, incorporar como capítulo V el siguiente y renumerar los restantes:

"CAPÍTULO V.- DE LA GESTIÓN DEL RIESGO OPERATIVO

SECCIÓN I.- ÁMBITO, DEFINICIONES Y ALCANCE

ARTÍCULO 1.- Las disposiciones de la presente norma son aplicables a las instituciones financieras públicas y privadas, al Banco Central del Ecuador, a las compañías de arrendamiento mercantil, a las compañías emisoras y administradoras de tarjetas de crédito y a las corporaciones de desarrollo de mercado secundario de hipotecas, cuyo control compete a la Superintendencia de Bancos y Seguros, a las cuales, en el texto de este capítulo se las denominará como instituciones controladas.

Para efecto de administrar adecuadamente el riesgo operativo, además de las disposiciones contenidas en el capítulo I "De la gestión integral y control de riesgos", de este subtítulo, las instituciones controladas observarán las disposiciones del presente capítulo.

ARTÍCULO 2.- Para efectos de la aplicación de las disposiciones del presente capítulo, se considerarán las siguientes definiciones:

1.1 **Alta gerencia.-** La integran los presidentes y vicepresidentes ejecutivos, gerentes generales, vicepresidentes o gerentes departamentales, entre otros, responsables de ejecutar las disposiciones del directorio u organismo que haga sus veces, quienes toman decisiones de alto nivel, de acuerdo con las funciones asignadas y la estructura organizacional definida en cada institución controlada;

1.2 **Evento de riesgo operativo.-** Es el hecho que puede derivar en pérdidas financieras para la institución controlada;

1.3 **Factor de riesgo operativo.-** Es la causa primaria o el origen de un evento de riesgo operativo. Los factores son los procesos, personas, tecnología de información y eventos externos;

1.4 **Proceso.-** Es el conjunto de actividades que transforman insumos en productos o servicios con valor para el cliente, sea interno o externo;

1.5 **Insumo.-** Es el conjunto de materiales, datos o información que sirven como entrada a un proceso;

1.6 **Proceso crítico.-** Es el indispensable para la continuidad del negocio y las operaciones de la institución controlada, y cuya falta de identificación o aplicación deficiente puede generarle un impacto financiero negativo;

1.7 **Actividad.-** Es el conjunto de tareas;

1.8 **Tarea.-** Es el conjunto de pasos o procedimientos que conducen a un resultado final visible y mesurable;

1.9 **Procedimiento.-** Es el método que especifica los pasos a seguir para cumplir un propósito determinado;

1.10 Línea de negocio.- Es una especialización del negocio que agrupa procesos encaminados a generar productos y servicios especializados para atender un segmento del mercado objetivo definido en la planificación estratégica de la entidad;

1.11 Datos.- Es cualquier forma de registro electrónico, óptico, magnético, impreso o en otros medios, susceptible de ser capturado, almacenado, procesado y distribuido;

1.12 Información.- Es cualquier forma de registro electrónico, óptico, magnético o en otros medios, previamente procesado a partir de datos, que puede ser almacenado, distribuido y sirve para análisis, estudios y toma de decisiones;

1.13 Información crítica.- Es la información considerada esencial para la continuidad del negocio y para la adecuada toma de decisiones;

1.14 Administración de la información.- Es el proceso mediante el cual se captura, procesa, almacena y transmite información, independientemente del medio que se utilice; ya sea impreso, escrito en papel, almacenado electrónicamente, transmitido por correo o por medios electrónicos o presentado en imágenes;

1.15 Tecnología de información.- Es el conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros;

1.16 Aplicación.- Se refiere a los procedimientos programados a través de alguna herramienta tecnológica, que permiten la administración de la información y la oportuna toma de decisiones;

1.17 **Instalaciones.-** Es la infraestructura que permite alojar los recursos físicos relacionados con la tecnología de información;

1.18 **Responsable de la información.-** Es la persona encargada de identificar y definir claramente los diversos recursos y procesos de seguridad lógica relacionados con las aplicaciones;

1.19 **Seguridad de la información.-** Son los mecanismos implantados que garantizan la confidencialidad, integridad y disponibilidad de la información y los recursos relacionados con ella;

1.20 **Seguridades lógicas.-** Se refieren a la seguridad en el uso del software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información;

1.21 **Confidencialidad.-** Es la garantía de que sólo el personal autorizado accede a la información preestablecida;

1.22 **Integridad.-** Es la garantía de mantener la totalidad y exactitud de la información y de los métodos de procesamiento;

1.23 **Disponibilidad.-** Es la garantía de que los usuarios autorizados tienen acceso a la información cada vez que lo requieran a través de los medios adecuados que satisfagan sus necesidades;

1.24 **Cumplimiento.-** Se refiere a la observancia de las leyes, regulaciones y acuerdos contractuales a los que los procesos de las instituciones controladas están sujetos;

1.25 **Pista de auditoría.-** Es el registro de datos lógicos de las acciones o sucesos ocurridos en los sistemas aplicativos u operativos, con el propósito de mantener información histórica para fines de control, supervisión y auditoría;

1.26 **Medios electrónicos.-** Son los elementos de la tecnología que tienen características digitales, magnéticas, inalámbricas, ópticas, electromagnéticas u otras similares;

1.27 **Transferencia electrónica de información.-** Es la forma de enviar, recibir o transferir en forma electrónica datos, información, archivos, mensajes, entre otros;

1.28 **Encriptación.**- Es el proceso mediante el cual la información o archivos son alterados en forma lógica, con el objetivo de evitar que alguien no autorizado pueda interpretarlos al verlos o copiarlos, por lo que se utiliza una clave en el origen y en el destino;

1.29 **Plan de continuidad.-** Está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos tanto en la información como en la operación. Un plan de continuidad incluye un plan de contingencia, un plan de reanudación y un plan de recuperación;

1.30 **Plan de contingencia.-** Es el conjunto de procedimientos alternativos a la operatividad normal de la entidad cuya finalidad es la de permitir su funcionamiento, buscando minimizar el impacto financiero que pueda ocasionar cualquier evento inesperado específico. El plan de contingencia se ejecuta el momento en que se produce dicho evento;

1.31 **Plan de reanudación.-** Especifica los procesos y recursos para mantener la continuidad de las operaciones en la misma ubicación del problema;

1.32 **Plan de recuperación.-** Especifica los procesos y recursos para recuperar las funciones del negocio en una ubicación alterna dentro o fuera de la institución;

1.33 **Eficacia.-** Es la capacidad para contribuir al logro de los objetivos institucionales de conformidad con los parámetros establecidos;

1.34 **Eficiencia.-** Es la capacidad para aprovechar racionalmente los recursos disponibles en pro del logro de los objetivos institucionales, procurando la optimización de aquellos y evitando dispendios y errores; y,

1.35 **Riesgo Legal.-** Es la posibilidad de que se presenten pérdidas o contingencias negativas como consecuencia de fallas en contratos y transacciones que pueden afectar el funcionamiento o la condición de una institución del sistema financiero, derivadas de error, dolo, negligencia o imprudencia en la concertación, instrumentación, formalización o ejecución de contratos y transacciones.

El riesgo legal surge también de incumplimientos de las leyes o normas aplicables.

ARTÍCULO 3.- Para efectos del presente capítulo, el riesgo operativo se entenderá como la posibilidad de que se ocasionen pérdidas financieras por eventos derivados de fallas o insuficiencias en los procesos, personas, tecnología de información y por eventos externos.

El riesgo operativo incluye el riesgo legal en los términos establecidos en el numeral 2.35 del artículo 2 de la Sección I de este capítulo.

El riesgo operativo no trata sobre la posibilidad de pérdidas originadas en cambios inesperados en el entorno político, económico y social.

SECCIÓN II.- FACTORES DEL RIESGO OPERATIVO

ARTÍCULO 1.- Con el propósito de que se minimice la probabilidad de incurrir en pérdidas financieras atribuibles al riesgo operativo, deben ser adecuadamente administrados los siguientes aspectos, los cuales se interrelacionan entre sí,:

1.1 Procesos.- Con el objeto de garantizar la optimización de los recursos y la estandarización de las actividades, las instituciones controladas deben contar con procesos definidos de conformidad con la estrategia y las políticas adoptadas, que deberán ser agrupados de la siguiente manera:

1.1.1 Procesos gobernantes o estratégicos.- Se considerarán a aquellos que proporcionan directrices a los demás procesos y son realizados por el directorio u organismo que haga sus veces y por la alta gerencia para poder cumplir con los objetivos y políticas institucionales. Se refieren a la planificación estratégica, los lineamientos de acción básicos, la estructura organizacional, la administración integral de riesgos, entre otros;

1.1.2 Procesos productivos, fundamentales u operativos.- Son los procesos esenciales de la entidad destinados a llevar a cabo las actividades que permitan ejecutar efectivamente las políticas y estrategias relacionadas con la calidad de los productos o servicios que ofrecen a sus clientes; y,

1.1.3 Procesos habilitantes, de soporte o apoyo.- Son aquellos que apoyan a los procesos gobernantes y productivos, se encargan de proporcionar personal competente, reducir los riesgos del trabajo, preservar la calidad de los materiales, equipos y herramientas, mantener las condiciones de operatividad y funcionamiento, coordinar y controlar la eficacia del desempeño administrativo y la optimización de los recursos.

Identificados los procesos críticos, se implantarán mecanismos o alternativas que ayuden a la entidad a evitar incurrir en pérdidas o poner en riesgo la continuidad del negocio y sus operaciones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas para un adecuado diseño, control, actualización y seguimiento de los procesos.

Las políticas deben referirse por lo menos a: (i) diseño claro de los procesos, los cuales deben ser adaptables y dinámicos; (ii) descripción en secuencia lógica y ordenada de las actividades, tareas, y controles; (iii) determinación de los responsables de los procesos, que serán aquellas personas encargadas de su correcto funcionamiento, a través de establecer medidas y fijar objetivos para gestionarlos y mejorarlos, garantizar que las metas globales se cumplan, definir los límites y alcance, mantener contacto con los clientes internos y externos del proceso para garantizar que se satisfagan y se conozcan sus expectativas, entre otros; (iv) difusión y comunicación de los procesos buscando garantizar su total aplicación; y, (v) actualización y mejora continua a través del seguimiento permanente en su aplicación.

Deberá existir una adecuada separación de funciones que evite concentraciones de carácter incompatible, 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 operativo.

Las instituciones controladas deberán mantener inventarios actualizados de los procesos existentes, que cuenten, como mínimo con la siguiente información: tipo de proceso (gobernante, productivo y de apoyo), nombre del proceso, responsable, productos y servicios que genera el proceso, clientes internos y externos, fecha de aprobación, fecha de actualización, además de señalar si se trata de un proceso crítico.

1.2 **Personas.-** Las instituciones controladas deben administrar el capital humano de forma adecuada, e identificar apropiadamente las fallas o insuficiencias asociadas al factor “personas”, tales como: falta de personal adecuado, negligencia, error humano, nepotismo de conformidad con las disposiciones legales vigentes,

inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una apropiada planificación y administración del capital humano, los cuales considerarán los procesos de incorporación, permanencia y desvinculación del personal al servicio de la institución.

Dichos procesos corresponden a:

1.2.1 Los procesos de incorporación.- Que comprenden la planificación de necesidades, el reclutamiento, la selección, la contratación e inducción de nuevo personal;

1.2.2 Los procesos de permanencia.- Que cubren la creación de condiciones laborales idóneas; la promoción de actividades de capacitación y formación que permitan al personal aumentar y perfeccionar sus conocimientos, competencias y destrezas; la existencia de un sistema de evaluación del desempeño; desarrollo de carrera; rendición de cuentas; e incentivos que motiven la adhesión a los valores y controles institucionales; y,

1.2.3 Los procesos de desvinculación.- Que comprenden la planificación de la salida del personal por causas regulares, preparación de aspectos jurídicos para llegar al finiquito y la finalización de la relación laboral.

Los procesos de incorporación, permanencia y desvinculación antes indicados deberán ser soportados técnicamente, ajustados a las disposiciones legales y transparentes para garantizar condiciones laborales idóneas.

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

Las instituciones controladas mantendrán información actualizada del capital humano, 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; información histórica sobre los eventos de capacitación en los que han participado; cargos que han desempeñado en la institución; resultados de evaluaciones realizadas; fechas y causas de separación del personal que se ha desvinculado de la institución; y, otra información que la institución controlada considere pertinente.

1.3 Tecnología de información.- Las instituciones controladas deben contar con la tecnología de información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones.

Para considerar la existencia de un apropiado ambiente de gestión de riesgo operativo, las instituciones controladas deberán definir formalmente políticas, procesos y procedimientos que aseguren una adecuada planificación y administración de la tecnología de información.

Dichas políticas, procesos y procedimientos se referirán a:

1.3.1 Con el objeto de garantizar que la administración de la tecnología de información soporte adecuadamente los requerimientos de operación

actuales y futuros de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

1.3.1.1 El apoyo y compromiso formal del directorio u organismo que haga sus veces y la alta gerencia;

1.3.1.2 Un plan funcional de tecnología de información alineado con el plan estratégico institucional; y, un plan operativo que establezca las actividades a ejecutar en el corto plazo (un año), de manera que se asegure el logro de los objetivos institucionales propuestos;

1.3.1.3 Tecnología de información acorde a las operaciones del negocio y al volumen de transacciones, monitoreada y proyectada según las necesidades y crecimiento de la institución;

1.3.1.4 Un responsable de la información que se encargue principalmente de definir y autorizar de manera formal los accesos y cambios funcionales a las aplicaciones y monitorear el cumplimiento de los controles establecidos;

1.3.1.5 Políticas, procesos y procedimientos de tecnología de información definidos bajo estándares de general aceptación que garanticen la ejecución de los criterios de control interno de eficacia, eficiencia y cumplimiento, debidamente aprobados por el directorio u organismo que haga sus veces, alineados a los objetivos y actividades de la institución;

1.3.1.6 Difusión y comunicación a todo el personal involucrado de las mencionadas políticas, procesos y procedimientos, de tal forma que se asegure su implementación; y,

1.3.1.7 Capacitación y entrenamiento técnico al personal del área de tecnología de información y de los usuarios de la misma.

1.3.2 Con el objeto de garantizar que las operaciones de tecnología de información satisfagan los requerimientos de la entidad, las instituciones controladas deben contar al menos con lo siguiente:

1.3.2.1 Manuales o reglamentos internos, debidamente aprobados por el directorio u organismo que haga sus veces, que establezcan como mínimo las responsabilidades y procedimientos para la operación, el uso de las instalaciones de procesamiento de información y respuestas a incidentes de tecnología de información;

1.3.2.2 Un procedimiento de clasificación y control de activos de tecnología de información, que considere por lo menos, su registro e identificación, así como los responsables de su uso y mantenimiento, especialmente de los más importantes;

1.3.3 Con el objeto de garantizar que los recursos y servicios provistos por terceros, se administren con base en responsabilidades claramente definidas y estén sometidas a un monitoreo de su eficiencia y efectividad, las instituciones controladas deben contar al menos con lo siguiente:

1.3.3.1 Requerimientos contractuales convenidos que definan la propiedad de la información y de las aplicaciones; y, la responsabilidad de la empresa proveedora de la tecnología en caso de ser vulnerables sus sistemas, a fin de mantener la integridad, disponibilidad y confidencialidad de la información; y,

1.3.3.2 Requerimientos contractuales convenidos que establezcan que las aplicaciones sean parametrizables, que exista una transferencia del conocimiento y que se entregue documentación

técnica y de usuario, a fin de reducir la dependencia de las instituciones controladas con proveedores externos y los eventos de riesgo operativo que esto origina.

1.3.4 Con el objeto de garantizar que el sistema de administración de seguridad satisfaga las necesidades de la entidad para salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben contar al menos con lo siguiente:

1.3.4.1 Políticas y procedimientos de seguridad de la información que establezcan sus objetivos, importancia, normas, principios, requisitos de cumplimiento, responsabilidades y comunicación de los incidentes relativos a la seguridad; considerando los aspectos legales, así como las consecuencias de violación de estas políticas;

1.3.4.2 La identificación de los requerimientos de seguridad relacionados con la tecnología de información, considerando principalmente: la evaluación de los riesgos que enfrenta la institución; los requisitos legales, normativos, reglamentarios y contractuales; y, el conjunto específico de principios, objetivos y condiciones para el procesamiento de la información que respalda sus operaciones;

1.3.4.3 Los controles necesarios para asegurar la integridad, disponibilidad y confidencialidad de la información administrada;

1.3.4.4 Un sistema de administración de las seguridades de acceso a la información, que defina las facultades y atributos de los usuarios, desde el registro, eliminación y modificación, pistas de auditoría; además de los controles necesarios que permitan verificar su cumplimiento en todos los ambientes de procesamiento;

1.3.4.5 Niveles de autorización de accesos y ejecución de las funciones de procesamiento de las aplicaciones, formalmente establecidos, que garanticen una adecuada segregación de funciones y reduzcan el riesgo de error o fraude;

1.3.4.6 Adecuados sistemas de control y autenticación para evitar accesos no autorizados, inclusive de terceros; y, ataques externos especialmente a la información crítica y a las instalaciones de procesamiento;

1.3.4.7 Controles adecuados para detectar y evitar la instalación de software no autorizado o sin la respectiva licencia, así como instalar y actualizar periódicamente aplicaciones de detección y desinfección de virus informáticos y demás software maliciosos;

1.3.4.8 Controles formales para proteger la información contenida en documentos; medios de almacenamiento u otros dispositivos externos; el uso e intercambio electrónico de datos contra daño, robo, accesos, utilización o divulgación no autorizada de información para fines contrarios a los intereses de la entidad, por parte de todo su personal y de sus proveedores;

1.3.4.9 Instalaciones de procesamiento de información crítica en áreas protegidas con los suficientes controles que eviten el acceso de personal no autorizado y daños a los equipos de computación y a la información en ellos procesada, almacenada o distribuida;

1.3.4.10 Las condiciones físicas y ambientales necesarias para garantizar el correcto funcionamiento del entorno de la infraestructura de tecnología de información;

1.3.4.11 Un plan para evaluar el desempeño del sistema de administración de la seguridad de la información, que permita tomar acciones orientadas a mejorarlo; y,

1.3.4.12 Las instituciones controladas que ofrezcan los servicios de transferencias y transacciones electrónicas deberán contar con políticas y procedimientos de seguridad de la información que garanticen que las operaciones sólo pueden ser realizadas por personas debidamente autorizadas; que el canal de comunicaciones utilizado sea seguro, mediante técnicas de encriptación de información; que existan mecanismos alternos que garanticen la continuidad del servicio ofrecido; y, que aseguren la existencia de pistas de auditoría.

1.3.5 Con el objeto de garantizar la continuidad de las operaciones, las instituciones controladas deben contar al menos con lo siguiente:

1.3.5.1 Controles para minimizar riesgos potenciales de sus equipos de computación ante eventos imprevistos, tales como: fallas, daños o insuficiencia de los recursos de tecnología de información; robo; incendio; humo; inundaciones; polvo; interrupciones en el fluido eléctrico, desastres naturales; entre otros;

1.3.5.2 Políticas y procedimientos de respaldo de información periódicos, que aseguren al menos que la información crítica pueda ser recuperada en caso de falla de la tecnología de información o con posterioridad a un evento inesperado;

1.3.5.3 Mantener los sistemas de comunicación y redundancia de los mismos que permitan garantizar la continuidad de sus servicios; y,

1.3.5.4 Información de respaldo y procedimientos de restauración en una ubicación remota, a una distancia adecuada que garantice su disponibilidad ante eventos de desastre en el centro principal de procesamiento.

1.3.6 Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente:

1.3.6.1 Una metodología que permita la adecuada administración y control del proceso de compra de software y del ciclo de vida de desarrollo y mantenimiento de aplicaciones, con la aceptación de los usuarios involucrados;

1.3.6.2 Documentación técnica y de usuario permanentemente actualizada de las aplicaciones de la institución;

1.3.6.3 Controles que permitan asegurar la adecuada administración de versiones de las aplicaciones puestas en producción; y,

1.3.6.4 Controles que permitan asegurar que la calidad de la información sometida a migración, cumple con las características de integridad, disponibilidad y confidencialidad.

1.3.7 Con el objeto de garantizar que la infraestructura tecnológica que soporta las operaciones, sea administrada, monitoreada y documentada de forma adecuada, las instituciones controladas deberán contar con políticas y procedimientos que permitan la adecuada administración, monitoreo y documentación de las bases de datos, redes de datos, software de base y hardware.

1.4 Eventos externos.- En la administración del riesgo operativo, las instituciones controladas deben considerar la posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos a su control, tales como: fallas en los servicios públicos, ocurrencia de desastres naturales, atentados y otros actos delictivos, los cuales pudieran alterar el desarrollo normal de sus actividades. Para el efecto, deben contar con planes de contingencia y de continuidad del negocio.

SECCIÓN III.- ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 1.- En el marco de la administración integral de riesgos, establecido en la sección II "Administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", de este subtítulo, las instituciones controladas incluirán el proceso para administrar el riesgo operativo como un riesgo específico, el cual, si no es administrado adecuadamente puede afectar el logro de los objetivos de estabilidad a largo plazo y la continuidad del negocio.

El diseño del proceso de administración de riesgo operativo deberá permitir a las instituciones controladas identificar, medir, controlar/mitigar y monitorear sus exposiciones a este riesgo al que se encuentran expuestas en el desarrollo de sus negocios y operaciones. Cada institución desarrollará sus propias técnicas o esquemas de administración, considerando su objeto social, tamaño, naturaleza, complejidad y demás características propias.

ARTÍCULO 2.- Para una adecuada administración del riesgo operativo las instituciones controladas deberán cumplir las disposiciones del artículo 1, de la sección II del presente capítulo y adicionalmente, deberán contar con códigos de ética y de conducta formalmente establecidos; con la supervisión del directorio u organismo que haga sus veces y de la alta gerencia; con una sólida cultura de control interno; con planes de contingencias y de continuidad del negocio debidamente probados; y, con la tecnología de información adecuada.

ARTÍCULO 3.- Con la finalidad de que las instituciones controladas administren adecuadamente el riesgo operativo es necesario que agrupen sus procesos por líneas

de negocio, de acuerdo con una metodología establecida de manera formal y por escrito, para lo cual deberán observar los siguientes lineamientos:

3.1 Los procesos productivos deberán asignarse a las líneas de negocio de acuerdo con los productos y servicios que generan, de forma que a cada uno de los procesos le corresponda una sola línea de negocio y que ningún proceso permanezca sin asignar; y,

3.2 Las líneas de negocio también deberán agrupar los procesos gobernantes y los procesos habilitantes que intervienen en las mismas. Si algún proceso gobernante o proceso habilitante interviene en más de una línea de negocio, la entidad deberá utilizar un criterio de asignación objetivo.

ARTÍCULO 4.- Las instituciones controladas deberán identificar, por línea de negocio, los eventos de riesgo operativo, agrupados por tipo de evento, y, las fallas o insuficiencias en los procesos, las personas, la tecnología de información y los eventos externos.

Los tipos de eventos son los siguientes:

4.1 Fraude interno;

4.2 Fraude externo;

4.3 Prácticas laborales y seguridad del ambiente de trabajo;

4.4 Prácticas relacionadas con los clientes, los productos y el negocio;

4.5 Daños a los activos físicos;

4.6 Interrupción del negocio por fallas en la tecnología de información; y,

4.7 Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

En el anexo No. 1 se incluyen algunos casos de eventos de riesgo operativo, agrupados por tipo de evento, fallas o insuficiencias que podrían presentarse en las instituciones controladas y su relación con los factores de riesgo operativo.

Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

ARTÍCULO 5.- Una vez identificados los eventos de riesgo operativo y las fallas o insuficiencias en relación con los factores de este riesgo y su incidencia para la institución, los niveles directivos están en capacidad de decidir si el riesgo se debe asumir, compartirlo, evitarlo o transferirlo, reduciendo sus consecuencias y efectos.

La identificación antes indicada permitirá al directorio u organismo que haga sus veces y a la alta gerencia de la entidad contar con una visión clara de la importancia relativa de los diferentes tipos de exposición al riesgo operativo y su prioridad, con el objeto de alertarlos en la toma de decisiones y acciones, que entre otras, pueden ser: revisar estrategias y políticas; actualizar o modificar procesos y procedimientos establecidos; implantar o modificar límites de riesgo; constituir, incrementar o modificar controles; implantar planes de contingencias y de continuidad del negocio; revisar términos de pólizas de seguro contratadas; contratar servicios provistos por terceros; u otros, según corresponda.

ARTÍCULO 6.- En razón de que la administración del riesgo operativo constituye un proceso continuo y permanente, será necesario que adicionalmente las instituciones controladas conformen bases de datos centralizadas, suficientes y de calidad, que permitan registrar, ordenar, clasificar y disponer de información sobre los eventos de

riesgo operativo; fallas o insuficiencias; y, factores de riesgo operativo clasificados por línea de negocio, determinando la frecuencia con que se repite cada evento y el efecto cuantitativo de pérdida producida y otra información que las instituciones controladas consideren necesaria y oportuna, para que a futuro se pueda estimar las pérdidas esperadas e inesperadas atribuibles a este riesgo.

ARTÍCULO 7.- Aspecto importante de la administración del riesgo operativo es el control, el cual requerirá que las instituciones controladas cuenten con sistemas de control interno adecuados, esto es, políticas, procesos, procedimientos y niveles de control formalmente establecidos y validados periódicamente. Los controles deben formar parte integral de las actividades regulares de la entidad para generar respuestas oportunas ante diversos eventos de riesgo operativo y las fallas o insuficiencias que los ocasionaron.

ARTÍCULO 8.- El esquema de administración del riesgo operativo de las instituciones controladas debe estar sujeto a una auditoría interna efectiva e integral, por parte de personal competente, debidamente capacitado y operativamente independiente.

La función de auditoría interna coadyuva al mejoramiento de la efectividad de la administración de riesgos a través de una evaluación periódica, pero no es directamente responsable de la gestión del riesgo operativo.

ARTÍCULO 9.- Las instituciones controladas deben contar permanentemente con un esquema organizado de reportes que permitan disponer de información suficiente y adecuada para gestionar el riesgo operativo en forma continua y oportuna.

Los reportes deberán contener al menos lo siguiente:

9.1 Detalle de los eventos de riesgo operativo, agrupados por tipo de evento; las fallas o insuficiencias que los originaron relacionados con los factores de riesgo operativo y clasificados por líneas de negocio;

9.2 Informes de evaluación del grado de cumplimiento de las políticas relacionadas con los factores de riesgo operativo y los procesos y procedimientos establecidos por la institución; y,

9.3 Indicadores de gestión que permitan evaluar la eficiencia y eficacia de las políticas, procesos y procedimientos aplicados.

Estos informes deben ser dirigidos a los niveles adecuados de la institución de manera que puedan ser analizados con una perspectiva de mejora constante del desempeño en la administración del riesgo operativo; así como para establecer o modificar políticas, procesos, procedimientos, entre otros.

SECCIÓN IV.- CONTINUIDAD DEL NEGOCIO

ARTÍCULO 1.- Las instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio.

Para el efecto, deberán efectuar adecuados estudios de riesgos y balancear el costo de la implementación de un plan de continuidad con el riesgo de no tenerlo, esto dependerá de la criticidad de cada proceso de la entidad; para aquellos de muy alta criticidad se deberá implementar un plan de continuidad, para otros, bastará con un plan de contingencia.

Las instituciones controladas deberán establecer un proceso de administración de la continuidad de los negocios, que comprenda los siguientes aspectos claves:

1.1 Definición de una estrategia de continuidad de los negocios en línea con los objetivos institucionales;

1.2 Identificación de los procesos críticos del negocio, aún en los provistos por terceros;

1.3 Identificación de los riesgos por fallas en la tecnología de información;

1.4 Análisis que identifique los principales escenarios de contingencia tomando en cuenta el impacto y la probabilidad de que sucedan;

1.5 Evaluación de los riesgos para determinar el impacto en términos de magnitud de daños, el período de recuperación y tiempos máximos de interrupción que puedan ocasionar los siniestros;

1.6 Elaboración del plan de continuidad del negocio para someterlo a la aprobación del directorio u organismo que haga sus veces;

1.7 Realización de pruebas periódicas del plan y los procesos implantados que permitan comprobar su aplicabilidad y realizar los ajustes necesarios; y,

1.8 Incorporación del proceso de administración del plan de continuidad del negocio al proceso de administración integral de riesgos.

ARTÍCULO 2.- Los planes de contingencia y de continuidad de los negocios deben comprender las previsiones para la reanudación y recuperación de las operaciones.

Los planes de contingencia y de continuidad deberán incluir, al menos, lo siguiente:

2.1 Las personas responsables de ejecutar cada actividad y la información (direcciones, teléfonos, correos electrónicos, entre otros) necesaria para contactarlos oportunamente;

2.2 Acciones a ejecutar antes, durante y una vez ocurrido el incidente que ponga en peligro la operatividad de la institución;

2.3 Acciones a realizar para trasladar las actividades de la institución a ubicaciones transitorias alternativas y para el restablecimiento de los negocios de manera urgente;

2.4 Cronograma y procedimientos de prueba y mantenimiento del plan; y,

2.5 Procedimientos de difusión, comunicación y concienciación del plan y su cumplimiento.

SECCIÓN V.- RESPONSABILIDADES EN LA ADMINISTRACIÓN DEL RIESGO OPERATIVO

ARTÍCULO 1.- Las responsabilidades del directorio u organismo que haga sus veces, en cuanto a la administración del riesgo operativo, se regirán por lo dispuesto en la sección III "Responsabilidad en la administración de riesgos", del capítulo I "De la gestión integral y control de riesgos", de este subtítulo.

Adicionalmente, el directorio u organismo que haga sus veces tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

1.1 Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operativo;

1.2 Aprobar las disposiciones relativas a los procesos establecidos en el numeral 1.1 del artículo 1, de la sección II de este capítulo;

1.3 Aprobar las políticas, procesos y procedimientos para la administración del capital humano conforme con los lineamientos establecidos en el numeral 1.2 del artículo 1, de la sección II de este capítulo;

1.4 Aprobar las políticas y procedimientos de tecnología de información establecidos en el numeral 1.3 del artículo 1, de la sección II de este capítulo; y,

1.5 Aprobar los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV de este capítulo.

ARTÍCULO 2.- Las funciones y responsabilidades del comité de administración integral de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos", de este subtítulo.

Adicionalmente, el comité de administración integral de riesgos tendrá las siguientes responsabilidades en relación con la administración del riesgo operativo:

2.1 Evaluar y proponer al directorio u organismo que haga sus veces las políticas y el proceso de administración del riesgo operativo y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación al riesgo operativo;

2.2 Evaluar las políticas y procedimientos de procesos, personas y tecnología de información y someterlas a aprobación del directorio u organismo que haga sus veces;

2.3 Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos;

2.4 Evaluar y someter a aprobación del directorio u organismo que haga sus veces los planes de contingencia y de continuidad del negocio a los que se refiere la sección IV del este capítulo; asegurar la aplicabilidad; y, cumplimiento de los mismos; y,

2.5 Analizar y aprobar la designación de líderes encargados de llevar a cabo las actividades previstas en el plan de contingencia y de continuidad del negocio.

ARTICULO 3.- Las funciones y responsabilidades de la unidad de riesgos se regirán por lo dispuesto en la sección III "Responsabilidad en la administración del riesgos", del capítulo I "De la gestión integral y control de riesgos", de este subtítulo.

Adicionalmente, la unidad de riesgos tendrán las siguientes responsabilidades en relación con la administración del riesgo operativo:

3.1 Diseñar las políticas y el proceso de administración del riesgo operativo;

3.2 Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, las personas, la tecnología de información y los eventos externos;

3.3 Analizar las políticas y procedimientos de tecnología de información, propuestas por el área respectiva, especialmente aquellas relacionadas con la seguridad de la información; y,

3.4 Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y de continuidad del negocio, al que se refiere la sección IV de este capítulo; así como proponer los líderes de las áreas que deban cubrir el plan de contingencias y de continuidad del negocio.

SECCIÓN VI.- DISPOSICIONES GENERALES

ARTÍCULO 1.- Para mantener un adecuado control de los servicios provistos por terceros, incluidas las integrantes de un grupo financiero, las instituciones controladas deberán observar lo siguiente:

1.1 Contar con políticas, procesos y procedimientos efectivos que aseguren una adecuada selección y calificación de los proveedores, tales como:

1.1.1 Evaluación de la experiencia pertinente;

1.1.2 Desempeño de los proveedores en relación con los competidores;

1.1.3 Evaluación financiera para asegurar la viabilidad del proveedor durante todo el período de suministro y cooperación previsto;

1.1.4 Respuesta del proveedor a consultas, solicitudes de presupuesto y de ofertas;

1.1.5 Capacidad del servicio, instalación y apoyo e historial del desempeño en base a los requisitos;

1.1.6 Capacidad logística del proveedor incluyendo las instalaciones y recursos; y,

1.1.7 La reputación comercial del proveedor en la sociedad.

1.2 Contratos debidamente suscritos y legalizados que contengan cláusulas que detallen, entre otros, los niveles mínimos de servicio acordado; las penalizaciones por incumplimiento; y, que prevean facilidades para la revisión y seguimiento del servicio prestado, ya sea, por la unidad de auditoría interna u otra área que la entidad designe, así como, por parte de los auditores externos o de la Superintendencia de Bancos y Seguros; y,

1.3 Contar con proveedores alternos que tengan la capacidad de prestar el servicio.

ARTÍCULO 2.- El manual que contempla el esquema de administración integral de riesgos, de que trata el artículo 1, de la sección IV “Disposiciones generales”, del capítulo I "De la gestión integral y control de riesgos, de este subtítulo, incluirá la administración del riesgo operativo.

ARTÍCULO 3.- La Superintendencia de Bancos y Seguros podrá disponer la adopción de medidas adicionales a las previstas en el presente capítulo, con el propósito de atenuar la exposición al riesgo operativo que enfrenten las instituciones controladas.

Adicionalmente, la Superintendencia de Bancos y Seguros podrá requerir a las instituciones controladas, la información que considere necesaria para una adecuada supervisión del riesgo operativo.

ARTÍCULO 4.- En caso de incumplimiento de las disposiciones contenidas en este capítulo, la Superintendencia de Bancos y Seguros aplicará las sanciones correspondientes de conformidad con lo establecido en el capítulo II “Normas para la

aplicación de sanciones pecuniarias", del subtítulo II "De las sanciones", del título X "De las limitaciones, prohibiciones y sanciones" de esta Codificación.

SECCIÓN VII.- DISPOSICIONES TRANSITORIAS

PRIMERA.- Las instituciones controladas presentarán a la Superintendencia de Bancos y Seguros, hasta el 30 de abril del 2006, su diagnóstico y el proyecto de implementación de las disposiciones contenidas en este capítulo, para una administración adecuada del riesgo operativo. El proyecto, debidamente aprobado por el directorio u organismo que haga sus veces, incluirá un cronograma detallado de las actividades que las instituciones controladas realizarán para su cumplimiento, señalando el responsable de cada una de ellas.

Para el caso de las cooperativas de ahorro y crédito que realizan intermediación financiera con el público, el plazo para la presentación del diagnóstico y proyecto de implementación será hasta el 31 de octubre del 2006.

SEGUNDA.- La implementación de las disposiciones previstas en este capítulo no podrá exceder de los siguientes plazos:

1.1 Para grupos financieros; y, para los bancos o sociedades financieras que no forman parte de un grupo financiero, las compañías de arrendamiento mercantil, las compañías emisoras y administradoras de tarjetas de crédito, las corporaciones de desarrollo de mercado secundario de hipotecas, las instituciones financieras públicas, hasta el 31 de octubre del 2008; y,

1.2 Para las cooperativas de ahorro y crédito que realizan intermediación con el público y las asociaciones mutualistas de ahorro y crédito para la vivienda, hasta el 31 de octubre del 2009. Esta fecha podrá ser modificada por el Superintendente de Bancos y Seguros, considerando el tamaño de la institución, la estructura organizacional, la cobertura geográfica y la complejidad de sus operaciones.

TERCERA.- Con el objeto de que la Superintendencia de Bancos y Seguros mantenga un adecuado conocimiento sobre el avance de la implantación de las disposiciones contenidas en el presente capítulo, las instituciones controladas deberán:

1.1 Hasta el 31 de diciembre del 2005, remitir a la Superintendencia de Bancos y Seguros, copia certificada del acta de la sesión en que el directorio u organismo que haga sus veces conoció el contenido del presente capítulo y de las disposiciones emitidas. También informarán el funcionario o área encargada de realizar el diagnóstico, así como de liderar el proyecto de implantación de la administración del riesgo operativo; y,

1.2 Hasta el 1 de marzo del 2006, deberán informar sobre el avance en la elaboración del proyecto y su cronograma."

ARTICULO 2.- La presente resolución entrará en vigencia a partir su publicación en el Registro Oficial.

COMUNÍQUESE Y PUBLÍQUESE EN EL REGISTRO OFICIAL.- Dada en la Superintendencia de Bancos y Seguros, en Guayaquil, el veinte de octubre del dos mil cinco.

Ing. Alejandro Maldonado García
PRESIDENTE DE LA JUNTA BANCARIA

LO CERTIFICO.- Guayaquil, veinte de octubre del dos mil cinco

Lcdo. Pablo Cobo Luna
SECRETARIO DE LA JUNTA BANCARIA

ANEXO No.1

IDENTIFICACIÓN DE EVENTOS, FALLAS O INSUFICIENCIAS Y FACTORES DEL RIESGO OPERATIVO

LINEAS DE NEGOCIO:

TIPOS DE EVENTOS	FALLAS O INSUFICIENCIAS	FACTORES DE RIESGO DE OPERATIVO	NUMERO DE VECES (FRECUENCIA)	EFECTO CUANTITATIVO PERDIDA PRODUCIDA
FRAUDE INTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Operaciones no reveladas adecuadamente	Mal diseño de proceso	Procesos		
Operaciones no registradas intencionalmente	Inadecuada selección de personal	Personas		
Inadecuada utilización de información confidencial	Ausencia de control en los perfiles de usuario	Tecnología de Información		
Apropiación indebida de activos	Inadecuada segregación de funciones	Personas		
Falsificación	Inexistencia de controles	Procesos		
Destrucción maliciosa de activos	Inadecuadas medidas de seguridad	Procesos		
Evasión de impuestos	Falta de ética	Personas		
Robo	Inadecuada segregación de funciones	Personas		
FRAUDE EXTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Robo	Falta de seguridades físicas	Procesos		
Emisión de cheques sin fondos	Inadecuada capacitación del Personal	Personas		
Perjuicios por intrusión o ataque de terceros	Falta de seguridades en la teconología de información para prevenir ataques de terceros	Tecnología de Información		
Falsificación	Falta de seguridades de la tecnología de información	Tecnología de Información		
PRACTICAS DE EMPLEO Y SEGURIDAD DEL AMBIENTE DE TRABAJO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Reclamos por compensación e indemnización al personal	Inadecuada contratación del personal	Procesos		
Violación de las normas de salud o seguridad	Falta de difusión y comunicación de políticas	Personas		
Todo tipo de discriminación	Inadecuada política de administración de personal	Personas		
PRACTICAS RELACIONADAS CON CLIENTES, LOS PRODUCTOS Y EL NEGOCIO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Mal manejo de la información confidencial de clientes	Falta de defininición de políticas y procedimientos	Procesos		
Prácticas contrarias a la competencia, prácticas inadecuadas de negociación	Falta de defininición de políticas	Personas		
Actividades no autorizadas	Incursión en nuevas actividades sin considerar riesgos	Procesos		
Abuso de información privilegiada a favor de la institución	Falta de ética	Personas		
DAÑOS A LOS ACTIVOS FÍSICOS PROVOCADOS POR				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Terrorismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Vandalismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Pérdidas por desastres naturales	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
INTERRUPCIÓN DEL NEGOCIO Y FALLAS EN LOS SISTEMAS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Fallas en el software	Deficiencia en el proceso de desarrollo y/o implantación	Tecnología de Información		
Fallas en el hadware	Falta de previsión de la capacidad de los recursos para el volumen de operaciones. Falta de mantenimiento preventivo de los servidores centrales	Tecnología de Información		
Problemas de telecomunicación	Caída en los enlaces de telecomunicaciones	Tecnología de Información		
Cortes en los servicios públicos	Falta de planes de contingencia	Eventos externos		
DEFICIENCIAS EN LA EJECUCIÓN DE PROCESOS, EN EL PROCESAMIENTO DE OPERACIONES Y EN LAS RELACIONES CON PROVEEDORES Y OTROS EXTERNOS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Errores en el ingreso de los datos	Falta de controles de ingreso de datos en las aplicaciones	Tecnología de Información		
Falla en la administración de colaterales	Inadecuada segregación de funciones	Procesos		
Documentación legal incompleta	Falta de verificación del área legal	Procesos		
Acceso no aprobado a las cuentas de clientes	Proceso no definido	Procesos		
Disputa con los proveedores	Deficiencias en la contratación	Procesos		
Incumplimiento en la entrega de la información hacia terceros	Falta de controles en el proceso de envio de información	Procesos		

NOTAS:

1.- En el presente Anexo constan ejemplos de eventos agrupados por tipo, los cuales consideran los lineamientos establecidos por el Comité de Basilea

2.- Los eventos que se produjeren que no esté alineados a los tipos de eventos especificados en este Anexo, deberán constar bajo la denominación "información no alineada, concepto bajo el cual constarán únicamente por excepción.

3.- Frecuencia, se refiere al número de veces que se repite cada evento

Fuente: Superintendencia de Bancos y Seguros del Ecuador

2.4 Evaluación del impacto de la aplicación de la norma en una institución financiera. Determinación de brechas que se deben cubrir.

COMENTARIO:

En general consideramos que todos los bancos están de acuerdo en que la responsabilidad primaria para la administración del riesgo operacional la tiene toda la Institución comenzando por sus Directivos. Esta responsabilidad se traslada a la unidad de riesgos, unidades de negocios o, en algunos bancos, la administración de productos, áreas de soporte o apoyo y funcionarios en general. Desde este punto de vista, se espera determinar si se dispone de sistemas apropiados de control del riesgo operacional. Muchos bancos refuerzan esta atribución de riesgos y responsabilidad a través de cargarle las pérdidas operacionales a los negocios relacionados o áreas de productos.

Aunque esto es algo que precisamente se quiere evitar con la implementación de la norma, en la práctica dependiendo del presupuesto que se disponga no siempre es posible erradicar por completo, en este sentido es preciso que se analice el impacto que representa para el negocio.

Dependiendo del caso, y tomando en cuenta que no existe una formula perfecta o receta de la mejor alternativa, si es una opción muy válida contratar una asesoría externa o capacitar al personal coordinador o responsable del proyecto para que se lleve a cabo el diagnóstico que determine el margen o brechas que existen en la organización frente a la norma.

Normalmente se deben establecer como parte del diagnóstico las necesidades de recursos ya sean de personal, tecnológicos, capacitación, etc.

Esto debe formar parte de un presupuesto aprobado por los niveles correspondientes.

Esto quiere decir que si bien es cierto vamos a tener una visión clara de la situación actual de la organización y las brechas a cubrir, también se consigue costear o presupuestar lo que significa el impacto de la implementación.

Desde el año 2005 que se emitió la resolución, a nivel de todos los bancos se han efectuado inversiones importantes, sobre todo en recursos de tecnología como adquisición de software para la administración de riesgos, equipamiento de centros de cómputo alternos como parte de los planes de contingencia, herramientas para levantamiento y administración de procesos, entre los más relevantes.

A pesar de la ventaja que representa lograr el nivel de exigencia de la norma, para algunos Bancos este impacto no ha sido muy fácilmente asumido por la Administración, sobre todo considerando la crisis actual del país y mundial, y la situación misma de las organizaciones.

La venta hacia el interior de la organización es otro aspecto que demanda un impacto elevado de recursos y tiempo, pero por sobretodo genera la necesidad de crear estrategias que permitan una interiorización y capacitación a todo el personal, en el caso de las Instituciones que tienen un importante número de personal a nivel de todo el país, ha resultado mas fácil construir o adquirir herramientas tipo e-learning que permitan cubrir esta necesidad.

Otro tema de mucho impacto para la vida de las Instituciones lo constituyen los centros de procesamiento alterno, de tipo operativo o de tecnología. Son importantes inversiones a nivel económico que pueden llegar a afectar a la organización si no parten de un análisis adecuado.

En todo caso siempre es bueno tener presente que los objetivos de la norma están enmarcados en lograr mayor eficiencia de los procesos de las Instituciones, así como evitar pérdidas derivadas de los riesgos de operación, y que por tanto en algún instante deberán ser reconocidos como ganancias o valor agregado de las operaciones.

En relación con establecer el gap (brecha) de cumplimiento, en el Ecuador se han incorporado en los últimos dos años algunas empresas locales e internacionales, dedicadas a brindar soporte y asesoramiento en materia de riesgo operacional, adicionalmente se pueden obtener varios cursos y seminarios relacionados que contribuyen al mejor entendimiento de la norma, así como refuerzan los lineamientos y mejores prácticas que de acuerdo con la realidad de cada Institución se pueden aplicar.

Si la decisión es asesoría externa, lo importante es asegurarse que el personal responsable del proyecto esté directamente relacionado con el personal externo, de tal manera que exista un traspaso de conocimiento que dará continuidad a la evaluación en el caso de servicios o productos nuevos. Considerar además que la Empresa seleccionada cuente con referencias de casos de éxito similares, y por supuesto que esté dentro del marco legal ofreciendo garantías de cumplimiento así como acuerdos de confidencialidad de la información.

Mas allá del diagnóstico siempre es bueno reflexionar en algunos interrogantes relacionados con el tema, pueden hacerse como una auto-evaluación sobre todo para comprobar que los diagnósticos presentados son coherentes en función de nuestro propio conocimiento, esto también puede verse como un punto de control para el asesor. Unos ejemplos de algunas preguntas o reflexiones podrían ser:

¿La Institución cuenta con políticas y procedimientos formalmente establecidos y debidamente aprobados?

¿Existe conciencia de los riesgos en la Institución?

¿La Institución cuenta con procesos definidos y controles apropiados?

¿Existen definidos procedimientos para mitigación de riesgos?

¿En la Institución se han definido planes de contingencia y continuidad para las principales operaciones?

¿La tecnología que soporta los procesos de la Institución tiene un nivel de seguridad razonable?

¿La estrategia de seguridad soporta la implementación de la norma?

¿Existe un apropiado cumplimiento del Banco con respecto a la regulación vigente?

¿Cuáles son las principales funciones y alcance de Auditoría Interna?

¿Se han establecido o al menos entendido dentro de la Institución las regulaciones o tendencias relacionadas con Basilea II?

¿Cuáles son los principales desafíos en la implementación de este proceso?

2.5 Consideraciones a tomar en cuenta para determinar la metodología a implantar para aplicar la norma de Riesgo Operacional.

Recopilando algunos conceptos que se incluyen en varios artículos del Internet relacionados con la gestión de riesgo operacional y su metodología, podemos mencionar lo siguiente:

En la actualidad existe una necesidad inminente de todas las Empresas de gestionar sus riesgos, no solamente por la normativa emitida sino por la ventaja competitiva que se deriva de una adecuada administración de riesgos.

Entre las principales razones que se deben considerar para implementar la gestión de riesgos en una Empresa podemos mencionar:

- Mantener estabilidad en las operaciones de la Institución, evitando incidentes inesperados que pueden resultar costosos.

- Concientizar en cada uno de los funcionarios una cultura de riesgo que contribuya a la consecución de los objetivos que la Institución se ha planteado.

- Implementar las mejores prácticas para el manejo del Gobierno Corporativo que promueva y auspicie una apropiada gestión de riesgos en la Institución.

- Cumplir con las normas establecidas por las Entidades de Control.

- Desarrollar la capacidad de crecimiento con niveles de adaptabilidad eficientes que signifiquen una ventaja competitiva frente al resto de Instituciones.

El éxito o fracaso de las organizaciones depende de cómo implementen la cultura de gestión de sus riesgos.

Entre los aspectos más importantes que contribuyen a este éxito están:

- Contar con el convencimiento y soporte de la Gerencia sobre la administración del riesgo operacional,

- Establecer un lenguaje común,

- Determinar el concepto de dueño del proceso o producto y difundirlo,

- Crear una cultura que permita la identificación, evaluación, mitigación y monitoreo o control del riesgo,

- Mantener una visión de la administración de riesgo operacional,

- Establecer roles en esta administración,

- Establecer un proceso de información y generación de reportes derivados de la administración de riesgo operacional,

- Determinar un coordinador de riesgo operacional y perfiles en las áreas de negocio de la Institución,

- Lograr la aceptación y consenso de todas las partes o áreas de la Institución,

- De preferencia iniciar el proceso de gestión de riesgos con un piloto, evaluando si la metodología es apropiada y determinando las mejoras necesarias,

- Asegurarse de contar con los recursos humanos y materiales apropiados para el proceso de gestión de riesgo operacional,

- Establecer el método para registrar y mantener la información de los eventos de riesgo en bases de datos apropiadas,

- Identificar y de ser el caso adquirir soluciones de software que contribuyan a la eficiencia de la administración,

- Establecer los requerimientos para el cálculo de capital por riesgo operativo.

COMENTARIO:

De la experiencia de haber trabajado en este proceso podemos rescatar algunos tips importantes que permitirán a las organizaciones tener una visión de cómo conseguir una metodología que siendo de fácil aplicación contribuya con los objetivos y factores de éxito citados anteriormente.

El proceso de implementación consta de tres etapas para lograr los objetivos planteados:

Etapa1: Concientización, importancia del riesgo operacional

Beneficios: Todos los niveles del negocio estarán conscientes de la importancia y la necesidad de la administración del riesgo operacional como forma de asegurar el cumplimiento de los objetivos.

Etapa 2: Definición de la Estructura organizacional, políticas y lineamientos.
Identificación de riesgos, mapas de riesgos, controles.
Desarrollo de incidentes, autoevaluaciones.

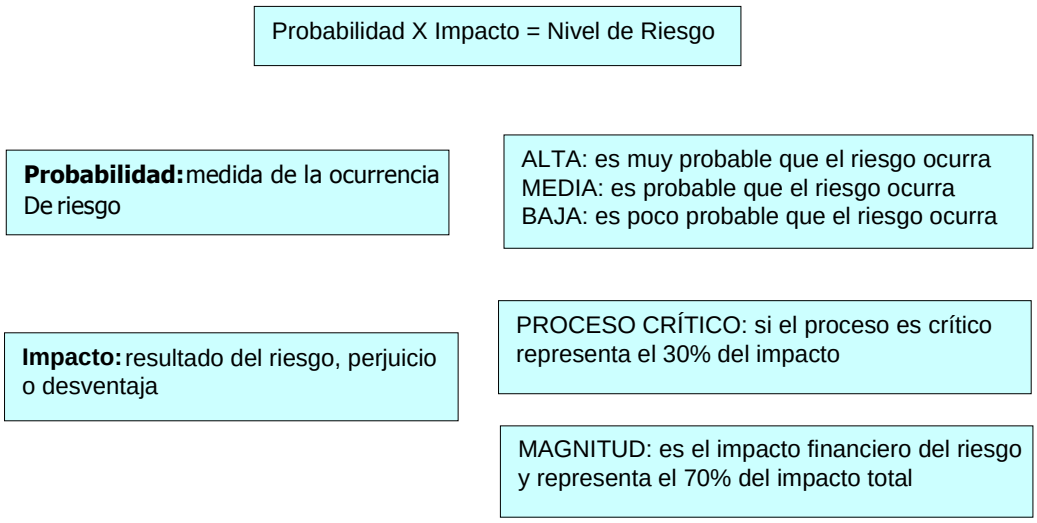
Beneficios: Definición formal de la estructura organizacional, políticas y procedimientos de la gestión de riesgo operacional.
Alineamiento de los objetivos del negocio, riesgos y controles.
Identificación y medición de los riesgos.
Evaluación de la efectividad de los controles.
Plan de respuesta al riesgo.
Evaluación continua de los riesgos.

Etapa 3: Captura de datos, mantenimiento
Desarrollo del modelo de cuantificación.
Calculo del capital con modelos.
Mapeo de riesgos.

Beneficios: Definición de las variables de eventos de riesgo para el registro en una base de datos.
Definición de los proceso de registro y mantenimiento de datos de pérdidas operacionales.

Otro aspecto importante a tomar en cuenta como parte de la metodología que se quiera implantar en la Institución, se refiere a los criterios para calificar o medir los riesgos, así, cuanto más complejo sea el enfoque escogido, mejor tendrá que ser el marco de gestión de Riesgo Operativo.

Se puede adoptar por ejemplo un tipo de valoración de riesgo que incluya los siguientes componentes o escala en la probabilidad e impacto:



Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

Acerca de contratar a terceros para que se hagan cargo de la gestión de riesgos operacionales, no necesariamente es la respuesta correcta, ya que el conocimiento de los procesos internos no siempre es transmitido de manera clara y precisa a los terceros, sin contar que puede presentarse falta de dirección y capacidad de proveer un sentido práctico y adaptable a los riesgos propios de la Institución. Si es recomendable, no obstante recurrir a una apropiada preparación del personal que estará a cargo de la administración de la gestión de riesgos, con el fin de mantener conocimiento y claridad en el momento de coordinar con todas las áreas de negocios, los objetivos y planes a seguir.

El desafío diario de vencer la resistencia al cambio y a comprender el valor agregado que tiene este tipo de enfoque para el negocio, superar la fuerte dependencia hacia los lineamientos basados en riesgo de crédito y de mercado, son algunos de los logros que a diario se pueden experimentar en el proceso de implementar la gestión de riesgos operacionales en una Institución.

EJEMPLO PRÁCTICO

Con fines didácticos a continuación se muestra el análisis efectuado al proceso de generación de respaldos de información en una Institución Bancaria, adoptando la

metodología que incluye la valoración del riesgo en una escala de alto, medio y bajo. Los pasos que se dieron fueron básicamente:

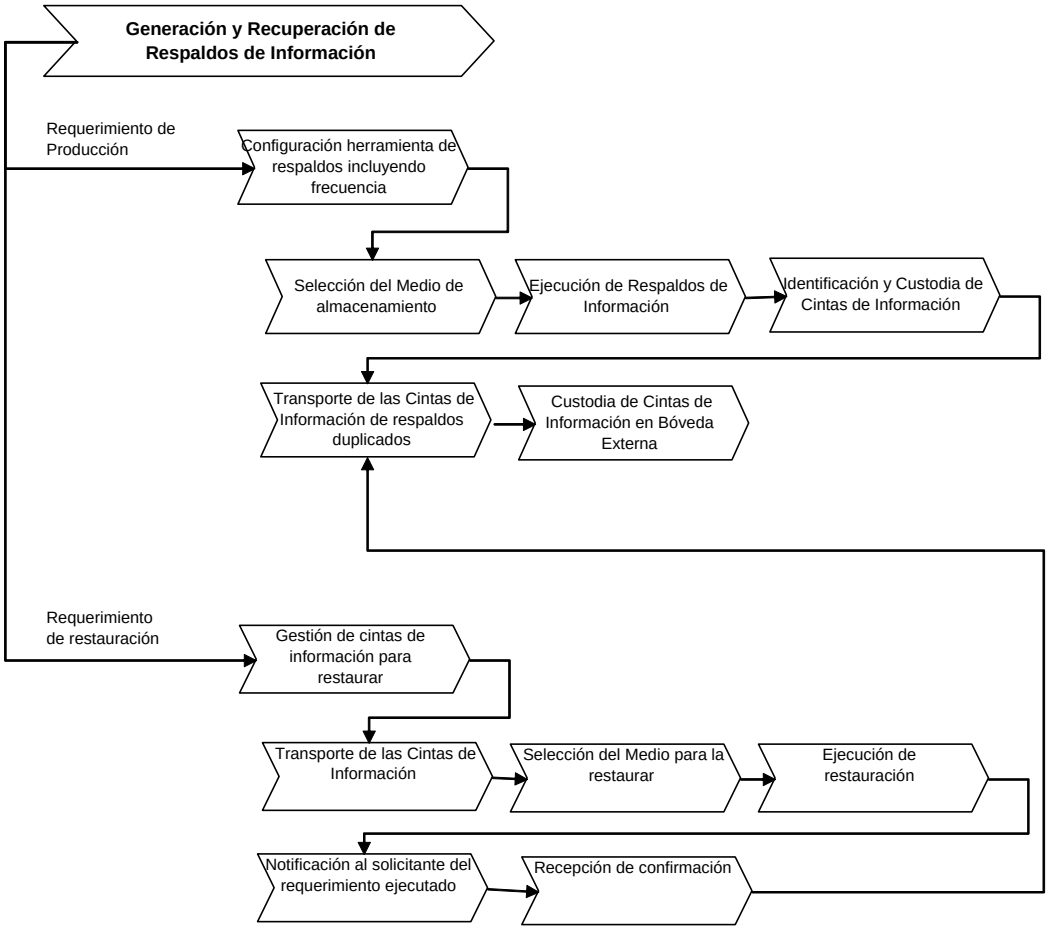
1. Levantamiento del flujo del proceso.
2. Análisis de riesgos de cada subproceso o tarea relevante del proceso definido para evaluación.
3. Elaboración de la matriz de riesgos incluyendo observaciones o recomendaciones.
4. Obtención del Riesgo Final del proceso (Alto, Medio o Bajo)

Levantamiento del flujo del proceso

La mejor manera de hacer este levantamiento es reuniéndose con el personal que está a cargo del mismo, es importante utilizar un lenguaje claro y conciso para que se entienda claramente el proceso, se deben considerar los sub procesos o tareas más importantes del mismo.

A continuación se muestra un ejemplo del proceso levantado en el Banco X:

PROCESO DE GENERACIÓN Y RECUPERACIÓN DE RESPALDOS DE INFORMACIÓN



Fuente: Grupo Implementación Riesgo Operacional Banco X

Como se puede apreciar en el gráfico, el proceso tiene dos sub procesos principales: el proceso de respaldo y el proceso de restauración.

En el primer caso, (respaldos), se deben establecer la frecuencia y alcance de los respaldos de la información más importante de la organización, esta tarea debe estar coordinada con los responsables o dueños de la información.

Siguiendo con el proceso está la ejecución del respaldo o copia, dependiendo de la herramienta que disponga la Institución se puede realizar de manera automática o manual,

lo recomendable es tener dos copias preferiblemente en cintas para almacenar una en el sitio principal y la otra en un sitio diferente a la matriz. Las cintas deben estar etiquetadas de manera clara para evitar confusiones al momento de archivarlas.

En el segundo caso, (restauraciones), se inicia el proceso cuando existe un requerimiento de algún usuario que necesita la información, se procede a realizar la solicitud y transporte de la cinta que guarda la información solicitada, y si se dispone de la tecnología necesaria se restaura la información de manera automática o manualmente. Lo importante es definir claramente en donde se restaura la información y el periodo de vigencia para que posterior a su uso se la borre, así evitamos que se formen grandes archivos de información que llegado el momento ya no se utilizan. Luego de entregar la información solicitada se devuelve la cinta para su custodia.

Análisis de riesgos de cada subproceso o tarea relevante del proceso definido para evaluación

El análisis de riesgos del Banco X para este proceso clasificado como crítico tiene como objetivo identificar aquellos aspectos que representan riesgo para la Institución, para que se facilite este análisis se pueden tomar como base algunas metodologías o estándares internacionales relacionados con Tecnología y Seguridad de la Información como Cobit, ISO 27005, etc. Este análisis forma parte del diagnóstico que mencionamos en varias partes del presente trabajo.

Entre los riesgos más comunes relacionados están: pérdida de información, fuga o mal uso de información crítica para el negocio, desperdicio de recursos si no existe un adecuado proceso de respaldos de información, pérdida de tiempo por fallas en la ejecución del proceso, etc.

El mayor activo de la Institución es la información por lo que resulta indispensable que este proceso tenga controles destinados a asegurar que la misma se mantenga en el tiempo, para ello una buena práctica es efectuar pruebas de restauración periódicas para revisar su integridad.

A continuación se muestra una parte de este análisis:

Matriz de Identificación de Riesgos y Controles de Tecnología de Información para el Proceso de Generación y Recuperación de Respaldos de Información del Banco X

Dominio COBIT	Problema detectado	Evento de riesgo	Evaluación sin control	Actividad de control	Evaluación luego del control
Planear y Organizar	No se respalda la información de los usuarios que puede ser considerada crítica para el negocio, pudiendo existir pérdida de información.	Pérdida o fuga de la informaciòn que puede ser critica para el negocio, ya sea por falta de normas o procesos de eliminación inadecuados.	A	Seguridad de la Informaciòn debe establecer la normativa para la informaciòn critica de usuarios del Banco y la normativa para una eliminaciòn segura de cintas de almacenamiento de informaciòn, a fin de evitar la pérdida o robo de la información por falta de definición de políticas.	M
	La formación académica de algunos recursos no cumple con los perfiles establecidos para el cargo.	Error en la ejecución de procesos por falta de conocimientos.	M	Actualización de files y funciones de los empleados para el cumplimiento de perfiles requeridos.	B
	Divulgación de información confidencial, cuando los empleados han salido de la organización	Robo o salida de información	A	Revisar los niveles de seguridad de la contratación de los empleados con respecto a los términos para la no divulgación de la información, una vez que el empleado ha salido de la empresa.	M
	Competencia, iniciativa de proyectos institucionales en otras empresas	La información confidencial del sea pública	A	Revisar los niveles de seguridad de la contratación de los empleados con respecto a los términos para la no divulgación de la información, una vez que el empleado ha salido de la empresa.	M
	No se respalda la información considerada crítica o se respalda información no requerida.	Pérdida de información	A	Mantener un esquema de clasificación de información que cataloge a la misma a fin de verificar si requiere o no respaldos.	M
Adquirir e Implantar	No se puede diferenciar los registros de accesos exitosos y fallidos del sistema de Gentec	Pérdida de tiempo en la generación de datos.	A	Optimizar el log del sitema de accesos de manera que diferencie los registros exitosos y fallidos, por parte de Gentec.	B
	No se mantiene la trazabilidad de los responsables de entregar y recibir las cintas de información, hora, ruta, novedades, etc.	Información incompleta	M	Optimizar el registro que realiza el Pool de Mensajeros en el envío recepción de información del Centro de Cómputo hacia el sitio externo.	B

Fuente: Grupo Implementación Riesgo Operacional Banco X

En este ejemplo se identifican algunos eventos de riesgo derivados de problemas detectados, para explicar vamos a revisar el primero: no respaldar la información crítica que pudiera ser objeto de pérdida o fuga, en este caso consta la actividad de control que se refiere a la normativa que Seguridad de la Información debe emitir para precautelar información crítica, que va desde la definición de las responsabilidades y el proceso en sí.

En la matriz se distinguen dos evaluaciones, una antes de la actividad de control y otra después de la misma. El riesgo que se mantiene al final se denomina riesgo residual, y es aquel que dependiendo de su nivel debe ser parte de las actividades o planes que se deben proponer para mitigarlo, ya que a pesar de mantener actividades de control puede ser elevado.

Elaborar la matriz de riesgos incluyendo observaciones o recomendaciones.

La matriz de riesgos es el documento en el cual se resumen los riesgos más relevantes del proceso y permite incluir observaciones como incumplimientos, mejoras y también recomendaciones que se efectúan con el fin de optimizar los controles para mitigar los riesgos.

MATRIZ DE RIESGOS-CONTROLES

Proceso: **Generación y Recuperación de Respaldos de Información**
Nivel de riesgo: Medio
Calificación: 3/4

			VALORACIÓN DEL RIESGO								
Aspectos más importantes inmersos en el proceso	**Controles existentes**	**Observaciones /Recomendaciones**	**Probabilidad de ocurrencia**			**Impacto/materialidad**			**Nivel de riesgo del proceso**		
			Alto	**Medio**	**Bajo**	**Alto**	**Medio**	**Bajo**	**Alto**	**Medio**	**Bajo**
Falta de procedimientos relacionados con el respaldo de la información que pueden facilitar la pérdida o fuga de la informaciòn que puede ser critica para el negocio.	Se cuenta con procedimientos de seguridad que incluye la normativa general sobre respaldos de información.	Seguridad de la Informaciòn debe establecer la normativa para la informaciòn critica de usuarios del Banco y la normativa para una eliminaciòn segura de cintas de almacenamiento de informaciòn, a fin de evitar la pérdida o robo de la información por falta de definición de políticas.	x			x			x		
La formación académica de algunos recursos no cumple con los perfiles establecidos para el cargo, lo que puede ocasionar errores en la ejecución de los procesos por falta de conocimientos.	Se mantiene un proceso adecuado de actualización de files y funciones de los empleados para el cumplimiento de perfiles requeridos.				x		x				x
Divulgación de información confidencial del GFP, cuando los empleados han salido de la organización que deriva en fuga o salida de información.	Existe un documento que firman los funcionarios cuando se desvinculan, no obstante no contienen disposiciones sobre el manejo de la seguridad de la información,	Revisar los niveles de seguridad de la desvinculación de los empleados con respecto a los términos para la no divulgación de la información, una vez que el empleado ha salido de la empresa.		x		x				x	

Fuente: Grupo Implementación Riesgo Operacional Banco X

En el ejemplo se esquematizan los riesgos más relevantes del proceso, sus controles y recomendaciones si aplican, en cuanto a las columnas destinadas a la valoración del riesgo se consideran los dos componentes: probabilidad de ocurrencia e impacto. La probabilidad se refiere a la frecuencia de ocurrencia y está directamente relacionada con la existencia de controles efectivos, ya que si no existen la probabilidad será mayor. En cuanto al impacto es alto en cuanto la Institución se ve más afectada frente a la pérdida fuga o mal uso de la información.

En algunas ocasiones la valoración de los riesgos puede resultar un análisis subjetivo, no obstante mientras más claras sean las especificaciones que se definan en la Institución más fácil será este análisis.

Obtención del Riesgo Final del proceso (Alto, Medio o Bajo)

Con la matriz de riesgos levantada, dependiendo de la escala, en este caso para el ejemplo se definió Alto (2), Medio (3), Bajo (4), entendiendo que Riesgo Alto puede resultar crítico para la Institución, se promedian los resultados parciales obteniendo el riesgo final. Para el ejemplo sería:
2+4+3= 9 / 3 = 3 (Riesgo Medio)

Existen otras escalas que se pueden emplear en la organización, por ejemplo:

Impacto 1=No significativo, 2=Menor, 3=Moderado, 4=Mayor, 5=Extremo	**Probabilidad** 1=Raro, 2=Improbable, 3=Posible, 4=Probable, 5=Alta Posibilidad

Otro aspecto importante a considerar es que los riesgos deben ser discutidos con los responsables de los procesos, puesto que los planes de mitigación los deben ejecutar ellos por lo que debe obtenerse la aceptación formal previa su publicación.

Los planes deben ser formalizados en cronogramas de implementación, que deberán dar seguimiento la Unidad de Riesgos y/o Auditoría Interna, no nos olvidemos que por norma esta última Unidad tiene la responsabilidad de informar a la Superintendencia de Bancos el avance de su cumplimiento.

Esperamos que este ejemplo sea de utilidad al momento de decidir cuál es la metodología más apropiada para la Institución.

CAPÍTULO III ADMINISTRACIÓN DEL RIESGO OPERACIONAL

3.1 Definición de responsabilidades en la administración del riesgo operacional.

La administración del riesgo operacional es una tarea conjunta que involucra a la Organización en sus diferentes instancias, y debe ser desarrollada progresivamente generándose una cultura de administración de riesgos.

Para ello debe crearse un ambiente adecuado, partiendo desde el Directorio y la Alta Dirección en general. A continuación comentamos las funciones y responsabilidades que tienen cada uno de los principales gestores del riesgo operacional.

En el caso de instituciones financieras ecuatorianas, las responsabilidades respecto a los riesgos integrales se encuentran consignadas en la Resolución No. JB-2004-631 emitida por la Superintendencia de Bancos y Seguros del Ecuador, mientras que las referentes al riesgo operacional están establecidas en la Resolución No. JB-2005-834 emitida por la misma Superintendencia.

El Directorio: tiene entre sus responsabilidades:

Respecto a la administración Integral de Riesgos:

- Conocer y comprender los riesgos de sus estrategias de negocio.

- Determinar y actualizar las estrategias, políticas, procesos y procedimientos que permitan una eficiente administración integral de riesgos, asegurando que Auditoría Interna audite este esquema, aprobando la incursión en nuevos negocios, operaciones y actividades, estableciendo límites prudenciales, implantando medidas correctivas si estos no se cumplen, asegurando que se establezca un sistema de medición de riesgos, que se cuente con recursos humanos, materiales y equipos que permitan la eficiente administración integral de riesgos y designando los miembros del comité integral de riesgos.

Respecto al Riesgo Operacional:

- Crear una cultura organizacional con principios y valores de comportamiento ético que priorice la gestión eficaz del riesgo operacional.

- Aprobar las disposiciones relativas a los procesos, las políticas, procesos y procedimientos para la administración del capital humano, tecnología de información, planes de contingencia y continuidad del negocio.

El Comité de Administración Integral de Riesgos:

Sobre la Administración Integral de Riesgos:

- Diseñar y proponer estrategias, políticas, procesos y procedimientos de administración integral de riesgos y someterlos a la aprobación del directorio.

- Asegurarse de la correcta ejecución de la estrategia e implantación de políticas, metodologías, procesos y procedimientos.

- Proponer al Directorio los límites específicos apropiados para cada riesgo.

- Conocer al detalle las exposiciones de los riesgos asumidos en términos de afectación al patrimonio técnico y con relación a los límites establecidos.

- Proponer al directorio las metodologías, procesos, manuales de funciones y procedimientos.

- Aprobar los sistemas de información gerencial, conocer los reportes de posición por cada riesgo, y el cumplimiento de límites fijados.

- Analizar y aprobar los planes de contingencia.

Sobre la administración de Riesgo Operacional:

- Evaluar y proponer al directorio las políticas y el proceso de gestión de riesgo operacional y asegurarse que sean implementados en toda la institución y que todos los niveles del personal entiendan sus responsabilidades con relación a este riesgo.

- Evaluar las políticas y procedimientos de procesos, personas, tecnología de información, y someterlas a aprobación del directorio.

- Definir los mecanismos para monitorear y evaluar los cambios significativos y la exposición a riesgos.

- Evaluar y someter a aprobación del directorio los planes de contingencia y de continuidad del negocio y asegurar su cumplimiento.

- Analizar y aprobar la designación de líderes encargados de realizar las actividades previstas en el plan de contingencia y de continuidad del negocio.

Unidad de Riesgos

Sobre la Administración Integral de Riesgos (AIR)

- Proponer al Comité de AIR políticas de Riesgos, de acuerdo con los lineamientos del directorio.

- Elaborar y someter a aprobación del Comité de AIR la metodología de AIR.

- Velar por el cumplimiento de los límites de exposición y los niveles de autorización.

- Revisar las exposiciones por tipo de riesgo: clientes, sectores, área geográfica, etc.

- Diseñar un sistema de información e informar periódicamente al Comité de Administración Integral de Riesgos.

- Preparar las estrategias alternativas para AIR y proponer al Comité los planes de contingencia.

- Calcular las posiciones de riesgo y su afectación al patrimonio técnico.

- Analizar nuevos negocios, operaciones y actividades.

- Analizar el entorno económico.

Respecto al Riesgo Operacional:

- Monitorear y evaluar los cambios significativos y la exposición a riesgos provenientes de los procesos, personas, tecnología de información y eventos externos.

- Analizar las políticas y procedimientos de TI, especialmente aquellas relacionadas con la seguridad de la información.

- Liderar el desarrollo, la aplicabilidad y cumplimiento de los planes de contingencia y continuidad.

- Proponer los líderes de las áreas que deban cubrir el plan de contingencias y continuidad.

Responsabilidades de los dueños de los procesos

- La responsabilidad directa de la apropiada gestión de los riesgos inherentes a las líneas de negocios, procesos, productos y áreas funcionales está en los ejecutivos y personal a cargo de ellos.

- Son responsables de identificar, evaluar, mitigar los riesgos.

- La Unidad de Riesgos les asiste para cumplir estas responsabilidades.

COMENTARIO:

Como se puede observar, el Riesgo Operacional forma parte de la administración de Riesgos Integrales. En el caso ecuatoriano la Superintendencia de Bancos ha venido emitiendo diferentes resoluciones a través de la Junta Bancaria, entre ellas: la norma sobre riesgos integrales, riesgo operacional, y los demás riesgos (crédito, que fue normado con anterioridad, especialmente basado en Basilea I, mercado, liquidez, etc.). Esto ha permitido que las Instituciones Financieras vayan paulatinamente implementando una infraestructura adecuada que comprende: recurso humano, es decir, las personas que se encargan de identificar, medir, normar, controlar, etc.; recursos físicos: oficinas, computadores, muebles y equipos de oficina; herramientas: software, registros, procedimientos, etc.

Las normas emitidas definen claramente las responsabilidades en la administración de los riesgos, partiendo del Directorio y la Alta Gerencia, como responsables de establecer "la cancha", es decir, el marco de referencia que genere una cultura de control adecuada, a través de la concientización de los riesgos que existen y la generación de políticas claras y la aprobación de las políticas complementarias, procedimientos y procesos que permitan un adecuado manejo de los mismos. Como complemento, tiene una Unidad de Auditoría Interna cuya responsabilidad es evaluar el riesgo, evaluar el control interno y determinar la suficiencia de las medidas establecidas y su cumplimiento. Auditoría Interna viene a ser "los ojos" del Directorio, pues debe reportar periódicamente el resultado de sus evaluaciones. Una frecuencia adecuada para dicho reporte es mensual, pues de esa manera el Directorio está permanentemente informado sobre los resultados obtenidos, los compromisos para solucionar los hallazgos y el seguimiento respectivo.

En la práctica, el Directorio establece las directrices generales, el Comité de Riesgos pone sobre la cancha trazada los parámetros y normas, propone al Directorio las reglas

complementarias del juego, esto es por ejemplo: establecer cupos de aprobación de crédito, límites de endeudamiento, niveles de aprobación de excepciones, calificar emisores y asignar cupos para operaciones como compra de papeles, establecer mercados objetivos, evaluar la evolución de cada mercado objetivo, considerando el riesgo del sector, riesgo país, etc.

El Comité de Riesgos Integrales debería estar constituido por:

- El Gerente General
- La cabeza de la unidad de riesgos (puede ser por ejemplo el Vicepresidente del área).
- La cabeza o representante del Departamento Legal.
- La cabeza o representante de la Unidad de Finanzas.
- La cabeza o representante de la Unidad de Tecnología
- La cabeza de las unidades que tienen relación con el tipo de riesgo que se trata:
    - Unidades de Crédito Corporativo o de Consumo, en el caso de crédito.
    - Unidad de Tesorería en el caso de Liquidez.

En algunos casos interviene algún miembro del Directorio. Los representantes de las áreas relacionadas o “afectadas” por las decisiones del Comité deben asistir con voz pero sin voto.

En el caso específico del subcomité de riesgo operacional, las áreas involucradas normalmente son más, por la naturaleza de dicho riesgo. Es decir, deberían asistir, a más de la Gerencia General, Unidad de Riesgos, el Departamento Legal, los representantes máximos de las siguientes áreas:

- Unidad de Recursos Humanos.

- Unidad de Tecnología.
- Unidad de Operaciones.
- Unidad a cargo de normar los procesos (organización y métodos/desarrollo organizacional/ productividad, etc.)
- La cabeza (vicepresidente) de Seguridad.
- Auditoría.

Este Comité debería entre otros aspectos:

- Conocer los riesgos identificados.
- Informarse de las medidas tomadas para administrar estos riesgos.
- El resultado de la evaluación de los procesos que realiza Auditoría, es decir, todo informe emitido por Auditoría debería ser remitido a este Comité.
- Los resultados que se obtengan de la autoevaluación de riesgos que resulten de los talleres realizados con los diferentes responsables de los procesos, para lo cual el administrador de riesgo operacional transmite una metodología a los responsables de cada proceso, y forma equipos interdisciplinarios que identifican, miden, evalúan y establecen el nivel de riesgo del proceso y luego proponen un plan de acción para mitigarlo. Este plan de acción debe ser conocido y aprobado por el Comité de Riesgo Operacional en base a una priorización previamente establecida.
- Presentar al Directorio el resultado de las evaluaciones realizadas y proponer políticas para mitigar los riesgos identificados. En caso de ser necesario, debe solicitar la aprobación del presupuesto y de las políticas y procedimientos que se establezcan como producto de la evaluación.

La Unidad de Riesgos es la encargada de proponer al Comité las políticas que considere, definir metodologías de control y monitoreo, informarle permanentemente el estado en que se encuentra cada riesgo, identificando nuevos riesgos a los que se encuentra expuesta la institución, sea por variación en la economía, por determinación de problemas con sectores o clientes específicos, desarrollo de nuevas modalidades de estafas a nivel nacional o internacional, apertura de nuevos “huecos” por cambios tecnológicos, normativos, etc. Es decir, viene a ser el “árbitro” del partido.

Así por ejemplo, la Unidad de Riesgos propone una política de control de información y documentación para guardar el sigilo bancario y prever posible fuga de información.

La Unidad de Riesgos plantea la política que diga: para preservar el sigilo bancario y la seguridad de la información, todo documento debe ser adecuadamente guardado en las carpetas y archivadores destinados para ello. La información del sistema bancario no puede ser almacenada fuera de él. Ningún funcionario podrá obtener en forma masiva la información, ni guardarla en dispositivos o transmitirla por ningún medio escrito o electrónico.

Una vez establecida la política coordina con las áreas de infraestructura física y de Tecnología a fin de asegurar que existan los mecanismos y capacidad instalada que permita dar cumplimiento a la norma. Estas áreas coordinan con todos los departamentos involucrados, una vez confirmado, se procede a dotar de lockers de seguridad o bóvedas de doble custodia para los departamentos que requieran este tipo de seguridad, o verificar que los archivadores proporcionen las facilidades para cumplir lo requerido.

El área de Tecnología procede a través de políticas del Active Directory o de las facilidades con que cuente su sistema operativo, a bloquear los dispositivos de salida de información. Se establece que en caso de que un funcionario requiera habilitar sus dispositivos de salida de información por motivos de trabajo, la Vicepresidencia del área deberá requerir a la Unidad de Riesgos su aprobación y solamente con las dos autorizaciones se habilitarán dichas salidas.

Adicionalmente, el funcionario cuyo computador tenga estos dispositivos activos, debe firmar un documento de compromiso de utilizarlo únicamente para los fines indicados.

Se establece un control trimestral que lo ejecuta Auditoría, cuyos resultados son informados a la Alta Gerencia, Comité de Auditoría, todas las Vicepresidencias. La Unidad de Riesgos informa al Comité de Riesgos Integrales. Si los resultados presentan incumplimientos frecuentes, se analizan las medidas que deben tomar para solventar el problema.

El siguiente gráfico pretende representar la estructura organizacional para la administración del Riesgo Operacional:

Fuente: Grupo Implementación Riesgo Operacional Banco X

3.2 Código de Ética y Conducta.

El Código de Ética es un documento que suscriben las empresas donde consignan los valores fundamentales que la guían, y que deben marcar el camino de la conducta de sus miembros. Entre los principios del Buen Gobierno Corporativo, se encuentra la definición y publicación de un código de ética institucional, que sea el marco de referencia de la actuación de sus directivos, empleados, funcionarios y en general todos quienes presten sus servicios. En este contexto, también dicta los principios y valores que guían sus relaciones con los clientes, proveedores, organismos de control, leyes y normas, y con la Sociedad en general.

El código de ética busca promover una cultura ética, basado en la confianza, evitar los conflictos de interés, de manera que cualquier relación que vaya o parezca ir contra el mejor interés de la organización se evite, ya que puede menoscabar la capacidad de una persona para desempeñar sus obligaciones y responsabilidades objetivamente.

COMENTARIO:

El Buen Gobierno Corporativo se basa en principios como la equidad, honestidad, solidaridad, justicia, tanto hacia los grupos de interés como para la sociedad en general, que puede verse afectada por actuaciones sin escrúpulos de ejecutivos llamados delincuentes de cuello blanco. Por ello, Basilea II insta a las instituciones financieras a establecer sus propios códigos de buen gobierno corporativo, en donde se definan, entre otros:

- Una estructura organizacional que desconcentrar funciones, limitar el poder, establecer comités para decisiones y eficiencia en la comunicación intradepartamental.
- Políticas claras con segregación de funciones, delimitando el alcance de las funciones. También debe establecer claramente cómo actuar en caso de conflictos de intereses, reglas de conducta para los diferentes niveles de la empresa.
- Deben establecerse claramente los métodos de transmisión de información a través de los diferentes niveles, y la comunicación de visión-misión, metas, objetivos, estrategias, estableciendo los valores corporativos como columna vertebral de la organización.
- Es necesario establecer un comité de análisis y control de riesgos, a fin de generar una cultura de prevención. Como complemento, deben establecerse comités para diferentes aspectos fundamentales, como: gestión de activos, pasivos y tesorería, comités de auditoría, evaluación del impacto de los diferentes tipos de riesgo y establecer medidas para administrarlos. Deben asegurarse el cumplimiento del objeto social, confiabilidad de los procesos, razonabilidad de la información y no movilización de activos provenientes de actividades ilícitas.
- Deben establecerse esquemas para el manejo de información y reportes, a fin de garantizar la calidad, confiabilidad, transparencia y oportunidad de la información financiera y no financiera.
- Debe tomar en cuenta el impacto de los avances tecnológicos, implementando sistemas eficientes de administración de los sistemas de información, los canales presenciales y

tecnológicos, establecer esquemas de control de la información, detección oportuna de fraudes, implementación de controles y registros auditables.

La consecuencia de la implantación de los códigos de buen gobierno corporativo, complementado con los códigos de ética y conducta, finalmente se reflejan en el prestigio, seguridad, eficiencia, credibilidad, imagen que la empresa genera hacia los entes relacionados interesados en la correcta marcha de la empresa, como sus clientes, proveedores, competencia, accionistas, empleados, etc.

A fin de dar transparencia y fortalecer la imagen institucional, los Bancos suelen presentar en sus páginas web sus códigos de ética para que el público pueda conocer las normas que los rigen. A continuación presentamos los códigos de ética de dos bancos ecuatorianos que adjuntamos como anexos. Estos códigos se encuentran disponibles en las páginas web de los bancos indicados:

- Código de ética de Produbanco (Anexo 1)
- Código de ética de Banco Internacional (Anexo 2)
- Código de ética de Banco de Crédito Agrícola de Cartago (Costa Rica) (Anexo 3)

3.3 Clasificación de los procesos. Consideraciones para su clasificación

En la actualidad, el enfoque de gestión por procesos tiene una gran importancia. Tanto así que las normas ISO 9000-2000 basan su filosofía en enfoque moderno de gestión de la calidad o gestión por procesos, tendientes a buscar organizaciones más exitosas y competitivas. De igual manera enfoca la filosofía de Calidad Total.

Según este enfoque, podemos señalar que un proceso se puede ejecutar en diferentes áreas, y por tanto puede utilizar recursos de diferentes subsistemas dentro de una institución, Este elemento es fundamental dentro de la Gestión por Procesos.

A continuación proporcionamos dos definiciones sencillas de procesos:

Según Evans y Lindsay, “proceso es una secuencia de actividades que tienen la finalidad de lograr algún resultado, generalmente crear un valor agregado para el cliente”.
Otra definición interesante de proceso, proporcionada por Krajewski y Ritzman, es la siguiente: “un proceso implica el uso de los recursos de una organización, para obtener algo de valor. Así, ningún producto puede fabricarse y ningún servicio puede suministrarse sin un proceso, y ningún proceso puede existir sin un producto o servicio”.

En definitiva, “un proceso es un conjunto de actividades interrelacionadas, que persiguen la creación de valor y que su salida final es la conformación de un bien o servicio para un cliente, ya sea interno o externo a la organización”. (Dr. José Manuel Pozo Rodríguez, “Consideraciones teóricas acerca de la Gestión por Procesos”).

Magáz define los procesos como una cadena de valor, por medio de su contribución a la creación de un producto o la entrega de un servicio. Cada paso de un proceso añade valor al paso anterior y así hasta el último paso del mismo, en el que el cliente externo o interno recibe el producto o servicio solicitado.

Para clasificar a los procesos, existe una diversidad de criterios que pueden ser utilizados de acuerdo a la utilidad que requiera la organización. Así pueden clasificarse por:

- El alcance en la organización.
- El impacto sobre el cliente final.

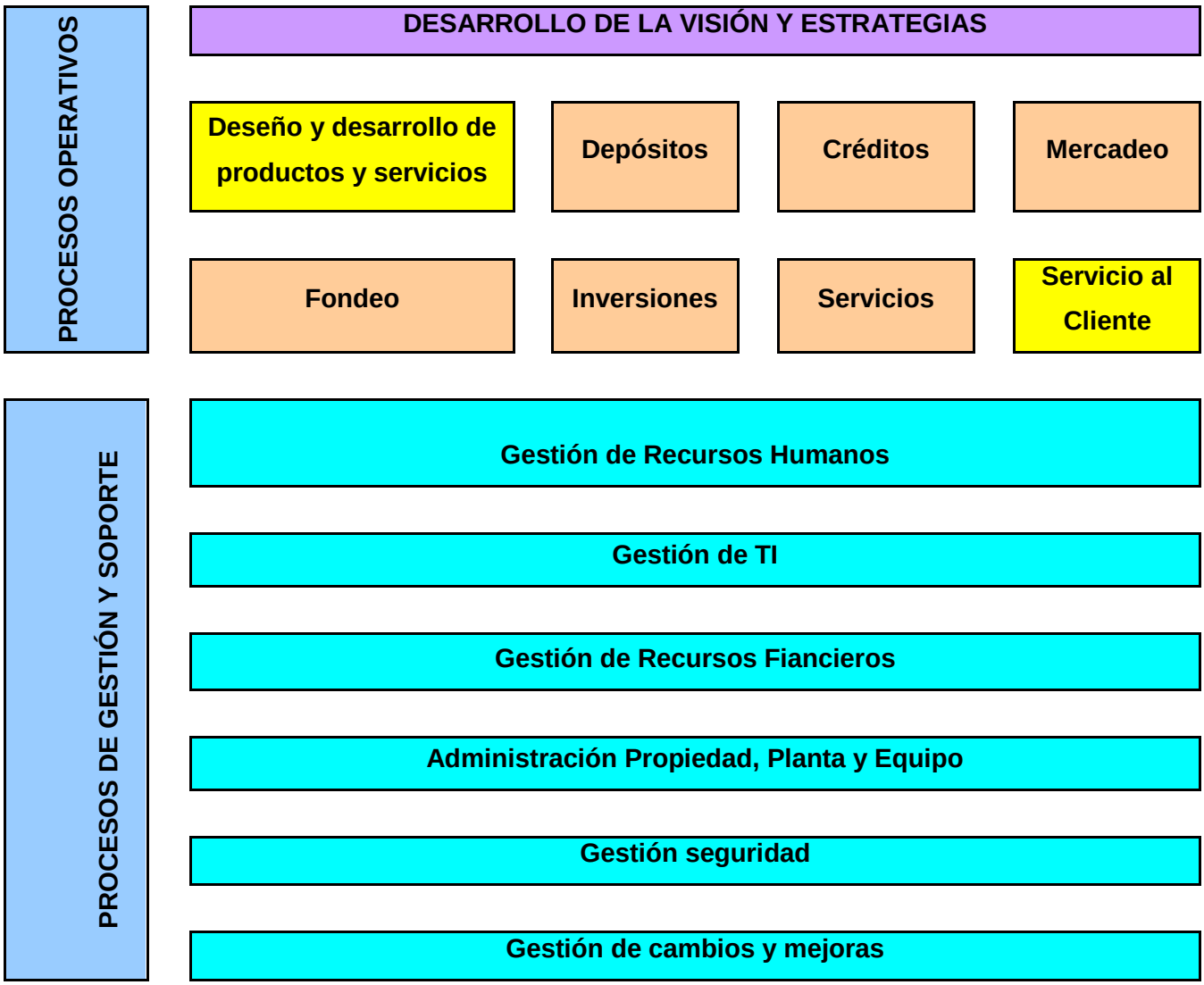
Vamos a revisar la clasificación por el impacto sobre el cliente final. De acuerdo a este punto de vista, los procesos pueden ser:

Procesos Claves o Fundamentales. Es decir, son los que se relacionan con la razón de ser de la organización. Implican a varias áreas de la empresa y tienen impacto directo sobre el cliente externo, creando valor para él. Contribuyen a realizar el producto o brindar el servicio. A partir de ellos el cliente percibe y valora la calidad de lo ofrecido.

De Soporte o Apoyo: Son los encargados de proveer a la organización de todos los recursos (materiales, humanos y financieros) y crear las condiciones para garantizar el exitoso desempeño de los procesos claves o fundamentales de la entidad.

Procesos críticos: son aquellos que siendo relevantes para la organización, es decir que son claves, muestran un pobre desempeño con relación a la calidad con que se brindan a los clientes.

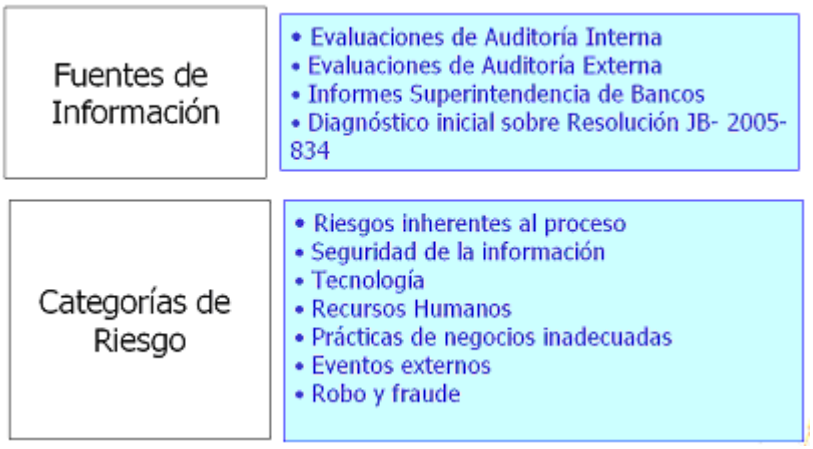
Clasificación de los procesos (un enfoque)



Fuente: Grupo Implementación Riesgo Operacional Banco X

Para poder clasificar los procesos, es necesario contar con un inventario de procesos. A partir de ello, se debe diagnosticar si los mismos cuentan con diseños estándar. De no ser así, es necesario estandarizarlos. Esto es, partir de diagramas que utilicen estructuras similares, procedimentarlos y conceptualizarlos igualmente bajo descripciones estandarizadas, de manera que sirva toda esta documentación de base para el análisis inicial.

Entre las fuentes de información para realizar un levantamiento inicial de los riesgos asociados a los procesos, tenemos información con que la entidad ha contado desde mucho tiempo atrás, y que toma relevancia a efectos de levantar un mapeo de procesos general. Este sería un punto de partida, luego del cual se complementa con mecanismos de auto evaluación y otros. A continuación graficamos las fuentes de información y las categorías de riesgos con que puede iniciarse la evaluación:



Fuente: Grupo Implementación Riesgo Operacional Banco X

El siguiente ejemplo permite ver un resumen de los procesos clasificados, identificando cuántos de ellos son considerados críticos:

CLASIFICACION	MACRO PROCESO	PROCESOS	P. CRITICO
ESTRATÉGICOS	DIRECCION DE NEGOCIO	4	1
	ADMINISTRACION INTEGRAL DE RIESGOS Y CONTROL INTERNO	9	
PRODUCTIVOS	DISEÑO Y DESARROLLO DE PRODUCTOS Y/O SERVICIOS	3	
	MARKETING Y VENTA DE PRODUCTOS Y SERVICIOS	2	
	CAPTACIONES	4	4
	COLOCACIONES	8	4
	COBRANZAS Y RECUPERACIONES	3	
	SERVICIOS BANCARIOS	7	4
	INVERSIONES Y FONDEO	8	6
	ADMINITRACION DEL SERVICIO AL CLIENTE	3	
DE APOYO	ADMINISTRACION DE CANALES	7	7
	DESARROLLO Y GESTION DEL CAPITAL HUMANO	6	2
	GESTION DE LOS RECURSOS DE TECNOLOGIA DE INFORMACIÓN	7	2
	GESTION CONTABLE	7	3
	ADMINISTRACION DE ACTIVOS Y LOGÍSTICA	10	8
	GESTION DE CAMBIOS Y MEJORAS	4	
	ADMINISTRACION DE LA SEGURIDAD CORPORATIVA	5	2
	GESTION LEGAL	8	5
	TOTAL	105	48

Fuente: Grupo Implementación Riesgo Operacional Banco X

Como se puede ver en el cuadro, con este resumen la institución cuenta con un inventario de sus procesos, de los cuales tiene identificados aquéllos que los ha catalogado como críticos. Cada institución define a qué procesos se los identifica como tales. Un criterio puede ser por ejemplo, los que tienen que ver con la atención al público que requieran atención inmediata. Así, los procesos de captaciones son considerados como críticos puesto que si el cliente se acerca a la Institución y no se lo atiende de inmediato, puede sentir que está en riesgo su dinero, generando algún tipo de reacción que de contagiarse con otros clientes podría generar pánico. Por tal motivo, todos los procesos de captaciones deberían considerarse como críticos. Otra explicación quizás más clara, es que para decidir si un proceso es crítico o no, se considere el tiempo que la institución puede dejar de atender en caso de una contingencia sin que esto genere una consecuencia grave. En este escenario, nuevamente diríamos que los procesos de captaciones son considerados críticos porque el cliente no espera en caso de tal contingencia, pues cualquier demora en la atención haría que tenga una percepción negativa respecto a la solvencia de la institución. Si nos fijamos en el macro proceso “Captaciones” del cuadro anterior, este se obtuvo de una gran matriz que indica en la institución X todos sus procesos de acuerdo a la clasificación indicada, con una columna

que permite clasificarlo como crítico o no. Así, el desglose del macro proceso "Captaciones" señalamos a continuación.

CLASIFICACIÓN	MACRO PROCESO	PROCESO	CRÍTICO (S/N)
PRODUCTIVOS	CAPTACIONES	CUENTAS CORRIENTES	S
		CUENTAS DE AHORRO	S
		DEPÓSITOS A PLAZO FIJO	S
		CUENTAS DE INTEGRACIÓN DE CAPITAL	S
	TOTAL	NÚMERO DE PROCESOS 4	CRÍTICOS 4

Fuente: Grupo Implementación Riesgo Operacional Banco X

El complemento de esto es que la Organización cuente con un manual de organización y funciones, que identifique las posiciones claves y detalle la segregación de funciones.

La Organización debe realizar un Mapa de Procesos institucional para que pueda aplicarse una metodología de identificación de riesgos a nivel de procesos del negocio.

COMENTARIO:

A continuación indicamos la forma de generar un mapa de riesgos:

Cálculo del nivel de riesgo:

Probabilidad X Impacto = Nivel de Riesgo	
Probabilidad: medida de la ocurrencia del riesgo	**ALTA**: es muy probable que ocurra **MEDIA**: es probable que el riesgo ocurra **BAJA**: es poco probable que el riesgo ocurra
Impacto: resultado del riesgo, perjuicio o desventaja	**PROCESO CRÍTICO**: representa el 30% del impacto. **MAGNITUD**: es el impacto financiero del riesgo y representa el 70% del impacto total.

Fuente: Grupo Implementación Riesgo Operacional Banco X

El mapa de riesgos es un reflejo de los diferentes procesos y su riesgo específico. Para poder levantar este mapa, es necesario que por cada uno de los procesos se identifiquen los riesgos asociados. Inicialmente se deben identificar absolutamente todos los riesgos, independientemente de si tienen o no controles, y a ello asignar un nivel de riesgo (alto, medio o bajo). Con esto tenemos la identificación de los riesgos inherentes. Una vez hecho esto, se evalúa por cada uno de los riesgos, el nivel de control que existe y su confiabilidad, con lo que se obtiene el riesgo residual, es decir, el riesgo que tiene el proceso con los controles que actualmente tiene.

Para cuantificar el nivel de riesgo, aplicamos la probabilidad de ocurrencia, es decir, asignamos una medida a la probabilidad de que ocurra un riesgo.

El impacto sería el efecto que causaría en caso de que ocurra el riesgo. Puede ser un perjuicio económico o una consecuencia que afecte a la institución, como por ejemplo

deterioro de su imagen. Aquí se considera si es proceso crítico, en cuyo caso tiene un 30% del valor, y la magnitud, que evaluaría el impacto financiero del riesgo, y representa el 70% del total.

Este es un proceso continuo, es decir, que una vez evaluado, no quiere decir que queda fijo, sino por el contrario, los cambios tecnológicos, normativos, la situación de la delincuencia, etc., hacen que los riesgos sean cambiantes y por tanto las matrices de riesgos deben ser constantemente actualizadas.

Así por ejemplo, hace años, el proceso de pago de cheques tenía un nivel de riesgo bajo, pues los bancos controlaban que los cheques que se pagaban correspondieran a la secuencia asignada a la cuenta, fueran emitidos en papel de seguridad, se verificaban las firmas, condiciones de giro, etc. Sin embargo, hubo una banda que consiguió papel de seguridad y empezó a emitir cheques, para lo cual identificaban en qué secuencia se encontraba girando el cliente, y emitían con numeraciones similares, con firmas correctas (seguramente su modus operandi incluía que consiguieran previamente de dichas empresas cheques similares para poder realizar la falsificación). Obviamente, esto subió el nivel de riesgo, por lo que ciertas instituciones generaron un “PIN” para los cheques, que consistía en un código de seguridad adicional que se asignaba a cada cheque en base a un algoritmo, para que se digitara al momento de pagarlo. Con esto se eliminó el riesgo, puesto que la banda no puede conocer el número que le corresponde a cada cheque. Este número se guarda encriptado, y nadie puede conocer cómo obtenerlo. Esta medida dio tan buen resultado, que otras instituciones hicieron lo mismo. Finalmente, ahora es un requisito que la Superintendencia de Bancos ha puesto como parte de la seguridad de los cheques.

De haber sido un riesgo bajo, pasó a un riesgo medio, pues mientras operaba esa banda la probabilidad de que ocurriera era media, y el impacto en caso de ocurrencia podía ser alto. Mientras se desarrollaba la opción indicada, las instituciones tomaron medidas como confirmar la emisión de cheques con el girador. Esto nos permite ejemplificar cómo debe ser un tema sumamente dinámico, que no puede esperar a que crezca el riesgo por no tomar medidas oportunas.

Aplicando a la práctica sobre un proceso específico, ejemplificamos la forma de evaluar con esta metodología, en base al ejemplo anterior de los cheques clonados, suponiendo que esta evaluación se realizó cuando se presentaban los casos mencionados:

Macro Proceso:	**Captaciones**						
Proceso:	**Cuentas Corrientes**						
Subproceso:	**Pago de cheques**						
Categoría de riesgo	**Tipo**	**Evento**	**Probabilidad**	**IMPACTO**			**FUENTES DE AUTOEVALUACIÓN**
				Proceso crítico 0.3	**Magnitud 0.7**	**Total 1**	
Eventos externos	Robo y Fraude	Clonación de cheques	2	1	0.3	1	Eventos suscitados en el último año han generado pérdidas por pago de cheques clonados. Los cheques cuentan con papel de seguridad, se encuentran dentro del número de secuencia de chequera del cliente y han sido pagados cumpliendo las normas establecidas.

Fuente: Grupo Implementación Riesgo Operacional Banco X

A continuación presentamos un cuadro de resumen cómo quedaría la evaluación global de riesgos de un proceso. Como vimos en el ejemplo anterior, esa es la manera de evaluar el riesgo de un proceso. El ejemplo a continuación presenta el formato de resumen de los riesgos evaluados para un proceso específico. Lo presentamos solamente para fines didácticos, y como se puede observar, los riesgos a los que se debe dar importancia son aquellos pintados con rojo, pues en este caso, 3 significa riesgo alto. Una vez que se mitiguen los riesgos identificados con rojo, se daría paso a los que tienen riesgo medio.

De esta manera se va construyendo la matriz de riesgos de la institución, en donde siempre se trabaja con los riesgos altos. Cada entidad puede definir el rango de riesgos que considere, por ejemplo: Riesgo Alto, Medio Alto, Medio, Medio Bajo, Bajo. Lo importante es que se lo mida adecuadamente y existan políticas para tomar medidas

inmediatas frente a lo que la administración considera un riesgo alto. Esto depende del apetito por el riesgo que asuma la Institución**.**

Procesos Revisados	Riesgos inherentes		Seguridad de la información		Tecnología		RRHH		Prácticas de negocios inadecuados		Eventos externos		Robo y fraude		Score Probab	Score impacto	Total Riesgo	Nivel de riesgo
	P	I	P	I	P	I	P	I	P	I	P	I	P	I				
Peso	16		15		15		7		14		15		18					
Proceso: Cuentas corrientes																		
Sobproceso: Chequeras	3	2	1	3	0	0	0	0	0	0	3	2	3	3	162	161	323	MEDIO

Fuente: Grupo Implementación Riesgo Operacional Banco X

La mayoría de organizaciones actualmente tiene un alto nivel de dependencia y desarrollo tecnológico, especialmente en el caso de Instituciones Financieras. Es por ello que, sobre este tema, debe evaluarse que la organización cuente con manuales adecuadamente documentados para evidenciar la robustez de la infraestructura tecnológica. Estos manuales deben incluir al menos:

- Estructura y administración de TI.
- Operaciones de TI.
- Servicios de Terceros en TI.
- Seguridad de TI.
- Continuidad de operaciones de TI y planes de contingencia y continuidad para eventos externos.
- Desarrollo de Aplicaciones.
- Documentación de Políticas y Procedimientos.

3.4 Eventos de riesgo operacional:

Dentro del ciclo de la gestión del riesgo operativo, tenemos las siguientes etapas:

1. Establecer un marco Adecuado.
2. Identificar los riesgos.
3. Valorar los riesgos.
4. Priorizarlos.

5. Gestionarlos.
6. Realizar seguimiento.

El flujo se encuentra graficado a continuación:

Fuente: Grupo Implementación Riesgo Operacional Banco X

Una de las novedades de Basilea II fue la introducción de requerimientos de recursos propios por riesgo operacional. Este no es un riesgo nuevo, sino que es un riesgo inherente a cualquier negocio. Sin embargo, es un riesgo al que se da mayor importancia, tanto por la complejidad y sensibilidad de las aplicaciones tecnológicas que soportan la operación bancaria, como por las pérdidas que han ocasionado a los bancos los diferentes riesgos, entre los que se encuentran el fraude, las fallas de control, los eventos externos, etc. Es así como en los noventas, existieron casos como el Banco Barinas, Bank of Credit and Commerce y Bankers Trust, que permitieron ver cómo las entidades financieras sufrieron pérdidas muy significativas que no provenían de los riesgos de crédito ni de mercado, poniendo en peligro su solvencia. Es por este motivo que se categorizó por separado al riesgo operacional. A este riesgo se suma la dependencia de los procesos automatizados, el desarrollo del comercio electrónico y las nuevas técnicas de mitigación de riesgos. En resumen, el sistema financiero es cada vez más complejo, que hacen que el riesgo operacional se más probable y genere un impacto más significativo.

Esto comprende la gestión general del riesgo, una herramienta que nos permite tener una fuente confiable y actualizada es el registro de eventos de riesgo operacional, que es uno de los elementos que la Unidad de Riesgos utiliza para llevar el correcto registro histórico que permita tomar medidas, evaluar su resultado, etc.

A continuación vamos a tratar sobre los eventos de riesgo operacional como herramienta básica que nos permite ubicar los hechos ocurridos que pueden tener como consecuencia pérdidas reales, pérdidas potenciales, deterioro de servicio, deterioro de imagen, etc., y es un parámetro más a considerar en la evaluación de riesgos.

3.4.1 Identificación

El primer paso que hay que dar para poder administrar los eventos de riesgo operacional es identificarlos. El Nuevo Acuerdo de Basilea clasifica los eventos de riesgo operacional en tres niveles. El primer nivel enumera siete tipos de eventos que tienen la consideración de pérdida por riesgo operacional y proporciona una definición de los mismos. Las entidades deben asignar sus datos de pérdidas a cada una de las siguientes categorías:

1. Fraude Interno,
2. Fraude Externo,
3. Relaciones laborales y seguridad en el puesto de trabajo,
4. Prácticas con clientes, productos y negocios,
5. Daños a activos materiales,
6. Incidencias en el negocio y fallos en los sistemas,
7. Ejecución, entrega y gestión de procesos.

En el segundo nivel se desglosa con mayor detalle el anterior, y en el tercero se anexan ejemplos de actividades de cada categoría de nivel 2. Esto se encuentra detallado en el anexo 7 del Nuevo Acuerdo.

Esta categorización es la base para que las instituciones financieras cataloguen en forma homogénea sus pérdidas por riesgo operacional y puedan obtener información comparable en el sector.

Una vez definido esto, Basilea II propone 3 métodos de cálculo, el básico, el estándar y los modelos avanzados. Son tres enfoques de complejidad creciente, cuyo propósito es proporcionar incentivos para que las entidades se desplacen a entornos más precisos y sofisticados de medición y gestión del riesgo operacional.

3.4.2 Registro

El segundo paso de esta metodología consiste en que cada entidad construya su base de datos de los eventos de riesgo operacional que ocurran. En la medida en que transcurra el tiempo, se puede tener una base de datos más sólida y completa. Las instituciones que cuentan con esta información tienen la posibilidad de generar provisiones más aproximadas, por tanto la base datos no solamente permite generar provisiones de mejor manera sino que dan la posibilidad de administrar más eficientemente los eventos, ya que al registrarlos se toman medidas, pues la idea es identificar las fallas que permiten que se presenten los eventos, evaluarlas y tomar medidas. Esto implica un estrecho seguimiento de cada evento, generando responsables de su regularización.

La información que se registra sobre los diferentes eventos, debería incluir un detalle de las incidencias presentadas, indicando al menos: fecha de la ocurrencia, clasificación del tipo de evento, descripción del evento, identificación de la causa probable, medidas tomadas, área responsable de la solución, consecuencias del evento (por ejemplo: pérdida monetaria, fallas en el servicio, daño de equipo, etc), cuantificación del daño incurrido, detalle de cómo se regularizó y cómo se solucionó, estado de implementación de la solución. Esto es importante detallar, ya que existen ciertos eventos que pueden ser generados por fallas cuya solución no es posible implementar inmediatamente. Por ejemplo, si es necesario realizar un desarrollo en el sistema, este puede tomar algún tiempo, pero mientras tanto, es necesario corregir los problemas que se presenten. En este caso, la solución definitiva es la

corrección del programa, mientras que la regularización son los pasos que deben seguirse para corregir los problemas que se presentan hasta que se implemente la solución definitiva. Para un manejo efectivo de esta información, lo ideal es desarrollar un aplicativo interno que permita realizar el registro, actualización y seguimiento, para lo cual deben generarse diferentes tipos de consultas y reportes para monitoreo.

Un buen diseño de la base de datos que permita identificar los eventos presentados, cuantificarlos, establecer sus reincidencias, evaluar la efectividad de las medidas tomadas, monitorear la evolución de las incidencias, etc., es una buena base que soporta la administración del riesgo operacional, permite mitigarlo y evaluarlo. Una buena base interna de eventos operativos contribuye a reducir su incidencia y las pérdidas generadas por los mismos, y especialmente a mejorar la calidad del servicio y de los productos. Esto requiere que se establezcan políticas y procesos para garantizar la consistencia e integridad de los procesos, y que se establezcan en forma consistente y clara, con una identificación adecuada del riesgo.

Los beneficios que genera una adecuada base de datos de eventos de riesgo permite tener una mayor conciencia de que las exposiciones al riesgo operacional pueden ser negativas para la entidad; al cuantificar el nivel de exposición, se focalizan los recursos para mitigarlo, y al analizar el origen o causa de los eventos repetitivos, se identifican oportunidades de mejoramiento de áreas o procesos.

3.4.3 Valoración

Para poder administrar el riesgo, es necesario conocerlo. El registro de eventos de riesgo nos proporciona elementos para identificar y administrar cada evento, de manera que se pueda identificar su impacto en la empresa. La valoración del impacto de cada evento no es fácil de hacer, pues no siempre el impacto es económico, o aún cuando lo fuera, no siempre se puede cuantificar con exactitud su alcance. Para ello es necesario que cada entidad identifique los riesgos y los modele, para poder aplicar con una metodología clara y específica.

Uno de los aspectos que debe considerarse en el modelaje es el umbral que debe aplicarse, ya que si este es muy bajo la institución entra en demasiado detalle, lo cual genera excesiva carga operativa que no es muy útil. Así mismo, si el umbral definido es muy alto, se pierde información y no se aplica el modelo de una manera óptima. Por tanto es sumamente importante definir un umbral razonable, que además debe ser monitoreado y ajustado continuamente.

Con los umbrales definidos, se estima la distribución de severidad teórica, para estimar la pérdida esperada. Es decisión de cada institución definir un solo umbral para todos los eventos o establecer umbrales según el producto o la línea de negocio. A nuestro criterio, es mejor hacerlo por producto o línea de negocio, pues en función de la rentabilidad y costo del producto deberían aceptarse los diferentes umbrales.

3.4.4 Adopción de medidas

Una vez identificados los eventos de riesgo operacional, la institución los evalúa y toma medidas, es decir, define si el riesgo se lo va a mitigar a través de la implementación de controles, se lo va a transferir a través de la contratación de seguros, entre otros. Lo importante es que la entidad debe establecer procesos y procedimientos de control y contar con un sistema que permita asegurar el cumplimiento de políticas internas, evaluar periódicamente las estrategias de control y reducción de riesgos y tomar las medidas correctivas que se requieran.

La Alta Gerencia y el Directorio deben generar una cultura sólida de control interno y cumplimiento y mantener un compromiso para fortalecer el ambiente de control de la entidad, designando un área responsable de la Gestión Integral de Riesgos y de preferencia con un funcionario a cargo de la Gestión de Riesgo Operacional, que será quien identifique y desarrolle las políticas y procedimientos para la gestión de este riesgo, establezca junto con la Administración planes de mitigación de riesgos y monitoree el avance. Debe tener un alto nivel de coordinación con Auditoría Interna, quien es la encargada de evaluar el riesgo. Así se complementan las funciones de

las diferentes áreas para mitigar el riesgo operacional, como se explica en el numeral 6 de este capítulo.

COMENTARIO:

Los eventos de riesgo operacional deben ser administrados de manera que se pueda efectuar un adecuado seguimiento y control. Para ello, las instituciones pueden desarrollar un aplicativo que facilite su clasificación adecuada y los respectivos seguimientos. En el caso que el volumen de transacciones no amerite el desarrollo de un aplicativo, deberían al menos llevarse registros en Excel, que igualmente faciliten un registro de control. A continuación indicamos los datos que deberían considerarse para el efecto, considerando que si se trata de un aplicativo más complejo, este debe contar con la posibilidad de emitir reportes, consultas de distinto tipo, considerando parámetros que faciliten su clasificación.
El registro debería contar con información como:

DATOS GENERALES					
Fecha evento	**Oficina**	**Ciudad**	**Tipo de Proceso**	**Proceso**	**Subproceso**
12/01/2008	Matriz	Quito	Apoyo	Administración Agencias	Pago Cheques
DATOS DEL EVENTO					
Tipo de evento	**Subtipo de evento**	**Evento específico**		**Causa del evento**	
Eventos externos	Falsificación firmas	Pago cheque con firma falsificada		No hay evidentes diferencias con original	
Descripción del evento:		El cheque No. 1234 de la cuenta 222999 del cliente Pedro Pérez se presentó al cobro. Cliente indica que no giró. Estudio grafológico determina que la firma no le corresponde.			
Pérdida generada	**Recuperado**	**Pérdida Neta**			
US$ 100.00	US$ 0.00	US$ 100.00			
Responsable del seguimiento:		Departamento de Seguridad debe ubicar a la persona que falsificó.			
Fecha de solución:		Pendiente.			
Proceso aplicado		Banco asume la pérdida. Cuando se determine el responsable se realizará el proceso legal correspondiente			
Estado del evento:		En proceso de investigación			
Fecha próximo seguimiento:		12/03/2008			
Comentarios		Ninguno			

Fuente: Grupo Implementación Riesgo Operacional Banco X

En este cuadro podemos observar la información que se registra para cada evento de riesgo. El registro adecuado de esta información nos permite contar con información histórica sobre los eventos ocurridos, identificando aquéllos que ocurren con mayor frecuencia, los que han generado mayor pérdida, los que han generado una alta exposición pese a que la pérdida no se haya concretado, las áreas que tienen mayor riesgo, etc. De acuerdo a las políticas que establezca la institución, pueden registrarse solamente los eventos que se han concretado. Sin embargo, a nuestro criterio, también es necesario incluir los intentos o los eventos que no han producido efectos nocivos, ya que cuando estos son recurrentes nos permiten identificar riesgos potenciales que a futuro pueden concretarse en eventos sumamente más fuertes. Por ejemplo, si se identifican intentos de transacciones con tarjeta de crédito en el exterior por montos insignificantes (por ejemplo, un dólar), hay que evaluar si existió lectura de la banda magnética, pues esto puede implicar un posible fraude con tarjeta clonada o fuga de información que permitiría intentos de fraude masivos. Si no se evalúa con esa perspectiva, se dejan pasar por alto indicios de potenciales fraudes que no son considerados adecuadamente.

El registro de eventos también es una herramienta de seguimiento que permite identificar los responsables de dar solución al riesgo, con fechas establecidas, y documentar las soluciones implementadas.

Este registro de eventos puede ser paulatinamente implementado. Es variable en cada entidad, y de acuerdo a la utilización que se le proporcione, suele ser sumamente útil. La evaluación periódica de su contenido, permite presentar estadísticas al Comité de Riesgos Integrales, tanto del período como comparada con períodos anteriores, con lo cual su seguimiento es efectivo, pues en caso de que el índice de eventos se eleve, o que persistan ciertos eventos por un tiempo sin encontrar soluciones adecuadas, se toman decisiones para mitigar de otra manera los eventos que ocurren.

Como habíamos indicado, si bien en instituciones pequeñas se puede llevar un registro manual, lo ideal es contar con un aplicativo que permita clasificar, evaluar, consultar, actualizar, asignar responsabilidades, hacer seguimientos, etc., a fin de que sea una

herramienta administrativa que permita tomar decisiones oportunas y conocer el estado y la evolución de los eventos presentados.

3.5 Indicadores de gestión como apoyo en la administración del Riesgo Operacional.

En general los bancos e instituciones financieras ya operan su modelo de gestión. También han venido administrando el riesgo operacional, quizás a veces en forma empírica, o en ocasiones intuitivamente.

Por tanto es necesario partir de la evaluación del estado de la aplicación de la norma de riesgo operacional. Para ello se parte como punto de referencia de una evaluación de riesgo, a fin de valorar la gestión de riesgo.

Dado que no existe un modelo único de gestión del riesgo operacional, en este proceso se integran todas las variables que nos permitan asegurar que el modelo de gestión cumple los requerimientos normativos, internos y externos, así como que se apega a las mejores prácticas establecidas para este proceso. Al final las entidades financieras tendrán un modelo seguro, eficiente y adecuado a sus necesidades particulares.

El modelo de gestión tiene dos grandes procesos:

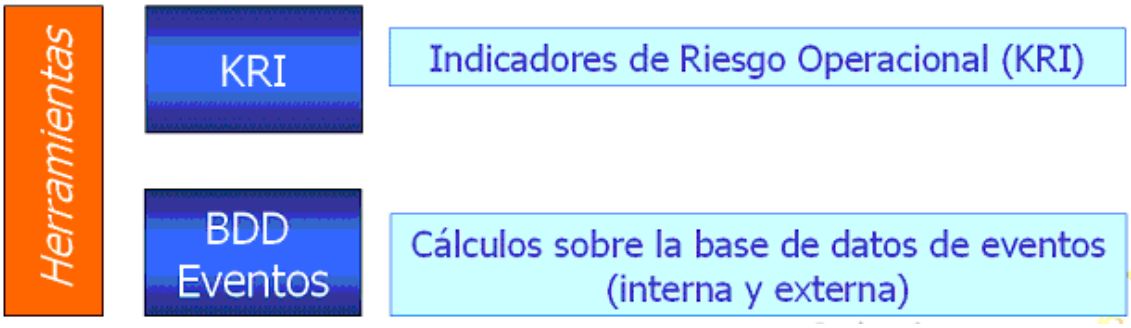
- Gestión Cualitativa
- Gestión Cuantitativa

En la Gestión Cualitativa se definen los métodos y procedimientos encaminados a identificar, monitorear y prevenir los riesgos operacionales, tales como:

- Identificación y clasificación de Riesgos y Controles,

- Auto evaluación de Riesgos y Controles,

- Indicadores Clave de Riesgos (KRI's), entre otros;



Fuente: Grupo Implementación Riesgo Operacional Banco X

En la Gestión Cuantitativa el desarrollo de los procedimientos y modelos tiene como objetivo identificar, registrar y modelar las pérdidas generadas por la materialización de los riesgos, para poder realizar el cálculo de las reservas de capital requeridas por Basilea II para afrontar este riesgo. Vamos a referirnos a los indicadores clave de riesgos (Key Risk Indicators, KRI por sus siglas en inglés).

El trabajo en este tipo de proyectos, se orienta básicamente a hacer efectivos las políticas y procedimientos establecidos en el modelo de gestión, mediante una planeación detallada que incluye, desde el análisis para identificar la criticidad y el orden de las áreas en las que será implementado, de ahí derivarán las labores de campo sobre la capacitación y la propia ejecución de los procedimientos, hasta la obtención de los reportes y análisis de los indicadores de gestión del riesgo operacional.

Debe definirse una metodología que permita mapear el riesgo operacional a fin de identificar los riesgos inherentes de las diferentes etapas del proceso de negocios, seleccionando un conjunto de variables que proporcionen un estimado de la severidad del riesgo operacional. Para ello deben establecerse los indicadores clave de riesgos, a los cuales hay que consolidar y resumir para proporcionar una mirada comprensiva de los riesgos por línea de negocio. Es un equivalente a un “tablero de comando de riesgos”.

Cada entidad debe por tanto, preparar su sistema de indicadores ajustado a sus características, a fin de reducir el número de normas y acciones de control, concentrando y combinando las mediciones para mejorar la efectividad del sistema de control interno. Así, podría prepararse un cuadro como el siguiente:

RIESGOS RELEVANTES	NORMAS Y ACCIONES DE CONTROL	INDICADORES DE CONTROL
Inadecuada preparación del personal.	Adecuar el programa de capacitación a las necesidades reales.	Puntos promedio en evaluación desempeño Número de cursos y cursistas Por ciento de aprovechamiento medio de la capacitación
Incumplimiento de los estándares el servicio.	Establecer un sistema de encuestas y entrevistas	Por ciento de satisfacción Por ciento de cumplimiento estándares Número de no conformidades Monto ($) de reclamaciones
Incumplimiento de las cifras presupuestadas.	Chequeo de planes y presupuestos	Costo por peso de Ingreso Productividad Variación precios promedio Rotación de inventarios Nivel de mermas Consumo electricidad Consumo de agua Por ciento ejecución del presupuesto Índices de solvencia, liquidez y otros financieros, convencionales o propios

*** Fuente: Publicación de Iralda Morales Alvarez y Onelio Díaz Martínez

Los indicadores que se definan deben ajustarse a las características de la entidad, enfocado a las líneas clave del negocio, y los servicios que sustentan estas líneas. Para ello es importante establecer parámetros que permitan identificar los aspectos a medir, como:

- Cuáles son los procesos clave? Este aspecto es parte del levantamiento de la norma de riesgo operacional, por tanto la entidad debe trabajar en base a dichos procesos.

- Para cada uno, es necesario identificar qué aspectos medir, y cómo hacerlo. Es decir, identificar cuáles son los aspectos que permitirán conocer si el proceso está bien gestionado, si se conocen oportunamente los eventos de riesgo que ocurran, si se toman medidas oportunas para mitigarlos, si éstas son efectivas, si se realiza seguimiento sobre ellas, etc. Para esto pueden aplicarse las normas ISO 9001-2000, que requieren llevar registros sobre las conformidades e inconformidades. Sobre estos registros, se pueden establecer metas de cumplimiento, por ejemplo: permitir un error máximo del 1% en algún caso específico.

- Complementariamente al establecimiento de cada índice, se establece la frecuencia, forma de medición, utilización del índice, a quién va dirigido, etc.

- Es necesario que se defina también una frecuencia y forma de evaluación de la variación de los índices, a fin de que la dirección pueda conocer estas tendencias y tome decisiones estratégicas sobre su eficiencia y eficacia.

- Como en todos los procesos de riesgo operacional, esta debe ser una tarea continua, que permita reconfirmar que los índices establecidos están enfocados a las prioridades del negocio y se ajustan permanentemente para ir de la mano con la dinámica de la empresa.

- Esta tarea de diseño, difusión, implantación y monitoreo implica que se aplique considerables esfuerzos y tiempo, por lo que la Unidad de Riesgos debe igualmente contar esta entre sus tareas importantes, y por tanto ser evaluados por ello.

- Identificar el conjunto ideal de indicadores claves requiere una aplicación de equilibrio cuantitativo y cualitativo, y es un proceso que se va complementando y perfeccionando con el tiempo. Pero sobre todo, debe estar alineado al establecimiento de objetivos estratégicos de control interno y permitir evaluar la calidad del control interno.

- Como todo objetivo, los indicadores deben ser medibles o cuantificables, calculables, comprensibles, relevantes y útiles. En su definición deben establecerse claramente las fuentes de información y asegurar que sean confiables y actualizadas, por tanto deberán establecerse las fechas de corte, muestras a tomar o universo que interviene, etc. Su cálculo debe ser realizado en forma automatizada, de preferencia evitando intervención humana para evitar errores.

A continuación detallamos algunos indicadores que permiten evaluar diferentes elementos de la gestión de riesgo operacional:

- Número de fraudes evitados en tarjeta de crédito en un mes. Este índice permite evaluar la eficiencia del monitoreo transaccional de tarjetas de crédito. Es complementario con el indicador del monto que "ahorra" (es decir, desde que se produjo la alerta en el sistema hasta que se bloqueó la tarjeta una vez confirmado que la transacción fue fraudulenta, cuánto se pudo haber consumido respecto al total del cupo disponible de la tarjeta). Este indicador es fundamental para evaluar la capacidad de respuesta frente a intentos fraudulentos, ya que la amenaza es a nivel mundial.

  Este indicador parte de la necesidad de evaluar la eficacia del monitoreo de tarjetas de crédito. La delincuencia a nivel mundial tiene alcances cada vez mayores, por lo que las franquicias mundiales establecen requisitos exigibles a los bancos para que detengan los fraudes a fin de mitigar las pérdidas. En tal sentido, establecen estándares para las instituciones, y comparan dichos indicadores contra los fraudes locales (país), regionales (Latinoamérica y el Caribe), y mundiales. En caso de que una institución tenga índices cuyo fraude está notoriamente fuera de los de la región, de inmediato reciben una auditoría por parte de la marca internacional para determinar el motivo o

motivos y recibe una fuerte sanción. En caso de no poner correctivos inmediatos o no presentar un plan de mitigación de dichos riesgos, es sancionada por fuertes sumas de dinero o se le retira la franquicia.

Ejemplo: La administración establece un índice de pérdidas por consumos del mes. El área de monitoreo de consumos de tarjeta de crédito establece entre sus objetivos uno que evalúe este resultado. El índice de pérdidas por mes es de 0.3%, y se calcula de la siguiente manera:

Índice de pérdidas en consumos de tarjeta de crédito = monto de pérdidas / total de consumos del mes.

Este objetivo tiene un valor de 20 puntos sobre 100 del total de la evaluación mensual del área. Cualquier exceso se penaliza con el 50% de la evaluación, siempre y cuando no exceda del 0.4%

Suponiendo que en el mes xx se realizaron un total de consumos por US$ 10'000.000, Si en dicho mes existieron pérdidas por fraude por 30.000 dólares, estaríamos dentro del margen permitido. Por tanto, el área tendría 20 puntos en la evaluación de este objetivo.

Pero si la pérdida por fraude fue de US$ 50.000, el índice sería del 0.5%. En este caso, el puntaje obtenido sería 0 puntos.

- Número de liquidaciones de operaciones de cartera con error, sobre el total de operaciones liquidadas en un mes. Se establece un rango máximo admisible, por ejemplo el 1%. El resultado debe ser parte de la evaluación del departamento a cargo de este indicador. En caso de que el índice supere este límite se notifica a la Unidad de Riesgo Operacional para identificar las causas y determinar el motivo que generó este resultado. En base a ello, se determina el camino a seguir.

  En este ejemplo, se ha determinado un indicador que permita poner índices de calidad del proceso de cartera, para ello se determina cuántas operaciones de tal naturaleza se realizan. En este caso, se obtendría un detalle del sistema en donde indique por sucursal el número de transacciones

de liquidación de cartera que se han efectuado en el mes. El mismo sistema indica si alguna transacción fue reliquidada y el motivo, para lo cual se escoge de un catálogo el motivo de reliquidación. Estos datos son incluidos en el reporte de sistemas y se calcula automáticamente el índice de eficiencia de las operaciones de cartera.

Índice de errores de liquidación de cartera = total errores/total liquidaciones procesadas en un mes.

Supongamos que el total de operaciones de cartera procesadas en el mes que se evalúa fue de 300, de las cuales se registraron 15 errores. Eso significa un error del 1.67%, es decir, tuvo un desempeño deficiente, pues sobrepasó el 1% establecido como meta, esta evaluación afecta al departamento de la sucursal que tuvo el error, y a la o las personas que sobrepasaron dicho indicador. La idea es que se cumpla el objetivo, que cada cierto tiempo es evaluado y si es necesario se ajusta a fin de mejorar la calidad del servicio paulatinamente. Como esto se transforma en parte de la evaluación de objetivos, si las áreas cumplen los funcionarios se ven compensados en su remuneración variable. Caso contrario, esta se ve también afectada.

- Número de reclamos por pagos erróneos de cajeros automáticos sobre el total de pagos realizados por cada cajero automático en una semana. Este indicador permite identificar fallas en la operación de cajeros y sirve para medir la oportunidad en la reparación de daños (operativos o técnicos) de los cajeros. Sin embargo, el control no se basa en el indicador, sino que existe un monitoreo automático que emite alertas directas al personal a cargo de la red de cajeros, proporcionando soluciones oportunas. Este indicador se utiliza también para evaluar la efectividad del servicio a clientes propios y de otras redes como por ejemplo Banred (local), Cirrus (MasterCard), electrón (Visa), ya que la entidad es evaluada en su uptime de servicio y no puede tener índices inferiores al 98% de servicio.

  Como se indica en el detalle, el indicador permite medir la eficiencia del servicio, por lo que su evaluación es parte de los objetivos del personal a

cargo de este proceso, incluyendo el área de tecnología. La información para esta evaluación se obtiene de un reporte que indica el número total de transacciones procesadas en cada canal tecnológico, por tipo de transacción, por cada tipo de tarjeta y emisor, en qué red se procesó, etc. Con lo cual el reporte indica el nivel de eficiencia, transacciones procesadas versus transacciones con error, para efectos de la evaluación.

Índice de reclamos por pagos erróneos en cajeros automáticos = número de pagos erróneos / total de pagos realizadas en el cajero automático.

Si el número de pagos realizados es de 500, y se presentaron 4 reclamos por pagos erróneos, el índice es 0.8%. Si la meta es una efectividad del 99%, el desempeño fue exitoso.

- Monto de faltantes de caja en un mes, sobre el total de efectivo asignado a la oficina. Permite medir la eficiencia de la oficina en el manejo de efectivo con los clientes y la aplicación correcta de las medidas establecidas para el efecto. Este índice es parte de los objetivos de la supervisión de la agencia y de los coordinadores.

  Índice de faltantes de caja = monto acumulado de faltantes en el mes / monto total de efectivo de la oficina.

  Este indicador permite evaluar los resultados de cada oficina y su incidencia en la efectividad del manejo de efectivo, lo cual se traslada a los objetivos del personal a cargo de la misma.

  Si en el mes de agosto se produjeron faltantes por 500 dólares, frente a un monto de efectivo manejado de US$ 2,000,000, el índice es de 0.03%. Si el objetivo planteado es de 0.01%, quiere decir que la gestión del manejo de efectivo en esa agencia es deficiente.

- Oportunidad en la atención de reclamos de clientes. La norma de la Superintendencia de Bancos permite un tiempo máximo de respuesta de 15 días ante reclamos de transacciones locales, y 60 cuando son transacciones internacionales. La Institución debe contar con infraestructura y

procedimientos que permitan atender los reclamos dentro del tiempo establecido, para lo cual debe mantener sistema de seguimiento. En este caso, el índice de cumplimiento debería ser del 100%, Esta evaluación afecta no solamente al área de atención al cliente sino que en caso de desfase, se traslada a las áreas responsables del desfase, pues tiene prioridad uno.

Este indicador es básico para la atención a clientes, pues su cumplimiento debe ser al 100% por tratarse de un requerimiento normativo. Para facilitar su evaluación, la entidad debe contar con un aplicativo donde se registren los reclamos que debe proporcionar información suficiente para evaluar el cumplimiento oportuno.

Índice de oportunidad de atención de reclamos a clientes = número de reclamos atendidos dentro del tiempo establecido por el Organismo de Control / Número total de reclamos presentados.

En este caso, cualquier valor diferente al 100% es considerado como deficiente, afectando a la evaluación de las áreas involucradas.

- Índice de fraudes en tarjeta de crédito, comparativo de la Institución versus los índices de la región (Latinoamérica) y del país. Se establece un porcentaje inferior en menos del 25% del índice del país.

  Índice de fraudes en tarjeta de crédito (comparativo vs país) = Monto de fraudes presentados en el mes / Monto de transacciones del mes (similar al primer índice presentado). Una vez obtenido este indicador, se compara con el índice de fraudes en tarjeta de crédito del país para el mes analizado.

  Índice de fraudes presentados en la institución financiera respecto al índice del país = índice de fraudes en banco x / índice de fraudes del país.

  Así, si el índice de fraudes en el país fue de 0,4% y el del Banco evaluado fue del 0.2%, el indicador que relaciona estos dos parámetros es 0.50%, por lo que la gestión es deficiente.

Complementariamente, en caso de dispararse los índices, también las franquicias establecen posibles causas y determinan nuevas normas de cumplimiento estricto tanto para los emisores de tarjetas de crédito como para las instituciones que realizan la Adquirencia de los establecimientos.

3.6 Rol de Auditoría

Responsabilidades de Auditoría Interna en la administración del Riesgo Operacional

De acuerdo a Basilea II, la implementación requiere esfuerzos e inversiones relevantes, por cuanto el proyecto implica el desarrollo de modelos, la revisión de procesos, evaluación de tecnología de la información, debe generar cambios culturales fuertes.

En este contexto, el Auditor Interno debe tener una activa participación en su desarrollo e implementación, manteniendo su independencia y cumpliendo sus funciones intrínsecas. Es necesario que el Auditor comprenda las definiciones y conceptos que utiliza. Sin embargo, como ya ha venido evaluando estos aspectos, generalmente para el auditor estas funciones las desarrolla de manera natural.

La implementación de metodologías y modelos implican que la organización se capacite y los desarrolle. Por tanto el Auditor debe avanzar en la capacitación a un ritmo igual o aún mayor que el resto de la organización, pues en temas de evaluación de riesgos hasta la presente fecha había sido quien lideraba.

Una vez adoptado un modelo o sistema, el auditor debe conocerlo y dominarlo a fin de poder evaluarlo.

Para el riesgo operacional, una vez implementadas las fases iniciales, Basilea II establece que se utilicen métodos avanzados AMA para el cálculo de capital por este riesgo, lo cual implica el empleo de modelos e información interna y externa sobre

pérdidas. El auditor debe entender las definiciones que se utilizan, algoritmos de estimación de los parámetros de riesgo, etc., y conocer el sistema de riesgo.

Basilea II norma que tanto los auditores externos como los internos deben llevar a cabo exámenes periódicos de los procesos de gestión y sistemas de medición del riesgo operativo.

También indica que las auditorías deben incluir las operaciones de las unidades de negocio y las actividades de la unidad de gestión del riesgo operativo, comprobar el buen funcionamiento de los procesos de validación interna y la transparencia y accesibilidad del flujo de datos asociados al sistema de medición del riesgo y de su procesamiento, así como la accesibilidad a las especificaciones y a los parámetros del sistema.

Entre las principales responsabilidades se encuentran:

- Evaluar la gestión de los riesgos significativos.
- Evaluar el reporte de los riesgos clave.
- Evaluar los procesos de gestión de riesgos.
- Asegurar que los riesgos son correctamente evaluados.
- Asegurar los procesos de gestión de riesgos.

Existen también ciertos roles considerados como legítimos para Auditoría, pero que deben ser ejecutados con salvaguardas, es decir, no son responsables directos del tema, pero pueden apoyar en ellos:

- Reporte consolidado de riesgos.
- Coordinación de actividades de administración de riesgos.

- Entrenar a la gerencia para responder a los riesgos.
- Facilitar la identificación y evaluación de los riesgos.
- Mantener y desarrollar el esquema de administración de riesgos.
- Patrocinar el establecimiento de administración de riesgos.
- Desarrollar la estrategia de gestión de riesgos para la aprobación del directorio.

Están claramente identificados los roles que Auditoría Interna **no** debe asumir, y que son:

- Establecer el apetito por el riesgo.
- Implementar los procesos de gestión de riesgos.
- Tomar decisiones basados en la respuesta al riesgo.
- Implementar respuestas de riesgo a nombre de la Gerencia.
- Responsabilidad de dar cuenta de la gestión de riesgos.

Finalmente, en conclusión, el Auditor asume también el rol de consultor, generando valor agregado a la empresa. Adicionalmente, deben examinar todos los elementos esenciales del sistema de gestión de riesgo, cálculo del indicador de Basilea, provisión por pérdidas esperadas.

Para cumplir a cabalidad su rol, el auditor debe conocer la organización, los procedimientos, los sistemas, las políticas, los modelos adoptados, así como entender correctamente las definiciones realizadas y los algoritmos de estimación de los parámetros.

CAPÍTULO IV CONTINGENCIA Y CONTINUIDAD DEL NEGOCIO

4.1 El proceso de administración de la continuidad del negocio

4.1.1 Establecer la estrategia y metodología.

Un plan de continuidad de negocios es el conjunto de acciones a ser llevadas a cabo ante distintos escenarios de desastres que pudieran afectar la correcta marcha de los negocios.

Determinar la estrategia de continuidad del negocio permite proporcionar una respuesta adecuada para cada producto o servicio, de tal manera que la organización pueda continuar proveyendo dichos productos y servicios a un nivel aceptable de operación y dentro de un período de tiempo apropiado durante y después de una interrupción.

La elección que se haga deberá tomar en cuenta la fortaleza y las opciones de contramedida que ya se encuentren presentes dentro de la organización.

Se deben estudiar las alternativas posibles, ventajas, inconvenientes y costos así como las medidas de reducción de riesgos como parte de la estrategia de recuperación.

El análisis o estudio de las diferentes estrategias a seguir se puede establecer con la ayuda de consultores externos o hacerlo con personal propio de la organización, lo cual agrega la ventaja del conocimiento y experiencia en los procesos, pero demanda preparación o capacitación para efectuar el levantamiento de los procesos así como el análisis de impacto.

Independientemente de la decisión que se adopte es necesario apalancar este proyecto en mejores prácticas y metodologías ampliamente conocidas y probadas. El estándar británico publicado en noviembre del 2006 denominado “Gestión de la continuidad del negocio”, fue preparado por el

Comité Técnico BCM/1; este documento fue desarrollado por profesionales de todos los ámbitos de la comunidad de continuidad del negocio, aprovechando su experiencia académica, técnica y práctica en el tema de la gestión de continuidad del negocio.

Es un documento que recopila las mejores prácticas, que sirve de referencia para la mayoría de situaciones en las que se puede ver avocada una Institución ya sea pequeña, mediana y grande, independiente del sector comercial, público o de beneficencia.

Las disposiciones de este estándar son recomendaciones o sugerencias que servirán de base para implementar una cultura de gestión de la continuidad que brindará un nivel de aseguramiento para las operaciones más importantes de la Institución frente a situaciones normales y en caso de contingencias.

Dentro de los beneficios de contar con un programa eficaz de gestión de continuidad del negocio podemos mencionar:

- Disponer de la capacidad de identificar de manera proactiva los impactos de una interrupción operativa.
- Tener en marcha un proceso de respuesta eficaz a interrupciones, que se minimiza el impacto de las mismas sobre la organización.
- Alentar el trabajo de equipo entre sus diferentes áreas.
- Contar con la capacidad de demostrar una respuesta verosímil por medio de procesos llevados a la práctica.
- Mejorar la reputación e imagen de la Institución.
- Obtener una ventaja competitiva, gracias a la capacidad de mantener la provisión de productos y servicios aún en situaciones de crisis.

Fuente1: Superintendencia de Bancos y Seguros

Fuente2: Artículos del Internet página www.isec-global.com

Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría.

COMENTARIO:

La elaboración de un plan de continuidad del negocio es un proyecto global que abarca a la totalidad de la organización no se trata de un proyecto de una área específica.

Primero se debe tener claro que los procesos críticos están soportados muy probablemente por sistemas informáticos, y éstos en algún momento o debido a determinadas circunstancias o eventos pueden fallar, pero la Institución no únicamente está compuesta por componentes tecnológicos, también existen procesos operativos, y por supuesto personas a cargo de ellos, de hecho los procesos de tecnología son dirigidos por funcionarios, sin olvidarnos de nuestros clientes. Todos los elementos de una organización se ven afectados cuando existen catástrofes o riesgos de tipo masivo o desastroso, lo importante de esto es contar con planes que permitan el mantenimiento de los servicios, equipos, personas, clientes, etc. durante este tiempo de emergencia, así como también se debe establecer el camino para regresar a la operación normal de la organización.

Disponer de un sitio alterno de procesamiento para asegurar que ciertos procesos no se detengan debe ser parte de los objetivos estratégicos de la Institución Financiera, por lo cual es importante contar con el apoyo del Directorio del Banco.

Para entender de mejor manera cómo se construye un plan o qué metodología se debe emplear, creemos importante que el personal a cargo tenga la suficiente preparación y de ser necesario buscar asesoría en los temas básicos o acompañamientos que confirmen el avance o determinación del proyecto.

Existen diversas metodologías que están disponibles en el mercado, pueden estar o no acompañadas de diagnósticos o acompañamiento, la mejor de ellas debe considerar la realidad de la organización.

Como ejemplo y con el fin de explicar de mejor manera los pasos a seguir para construir este plan resumimos de forma macro los siguientes pasos:

1. Contar con el apoyo de la Alta Gerencia

   A partir de la designación del coordinador o encargado de gestionar la realización de los planes, es importante que exista el compromiso formal de apoyo de la Directiva de la Institución, puesto que los recursos económicos que demandan este tipo de proyectos tienen que ser autorizados.

   De igual forma el compromiso de toda la organización para el logro de este objetivo debe ser transmitido desde la cabeza de la organización.

2. Determinar el sitio de procesamiento alterno

   Con la premisa que este tipo de planes se activa cuando el sitio principal de procesamiento se ha visto comprometido por algún evento catastrófico, es necesario encontrar el lugar en donde se podrá continuar con el servicio.
   En este momento es cuando se hace efectivo el apoyo de la Alta Gerencia porque se requiere financiamiento.

3. Elaboración del plan

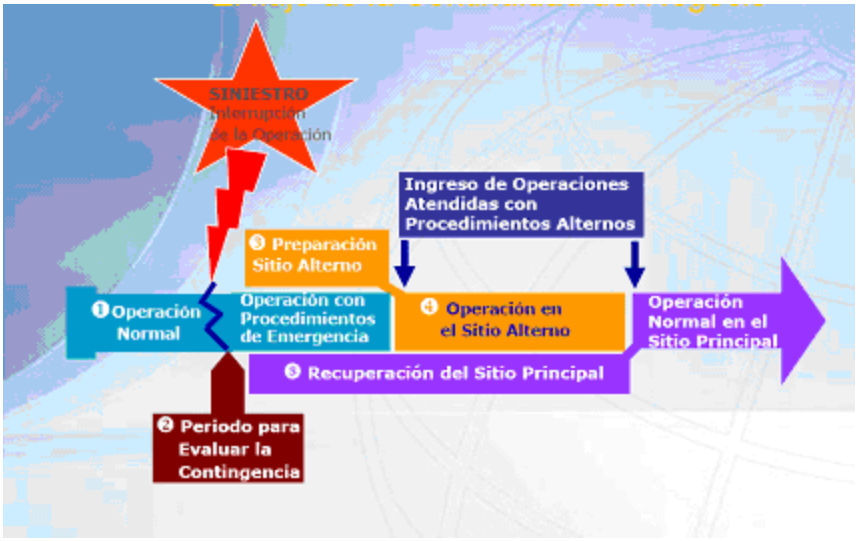
   En esta etapa o fase se deben desarrollar los planes de contingencia de los procesos que la Institución tenga interés que se mantengan funcionando en caso de contingencias, es decir no todo es sujeto a ser replicado o que siga funcionando siempre, todo va a depender de los objetivos de la organización y de la inversión que pueden efectuar, ya que mientras más rápido sea conectarse del sitio principal al alterno implica mayor costo por toda la tecnología y logística que debe mantener la Institución.

   El o los planes de continuidad deben incluir además los pasos o procesos para regresar a la operación del Banco, dependiendo de su realidad, habrá

procesos que dejen de ser atendidos, otros con soluciones temporales manuales. En todo caso entendiendo que en algún momento se tiene que restaurar la situación inicial de procesamiento, es indispensable saber el camino a seguir para regularizar todo aquello que no se pudo efectuar en su momento.

Por ejemplo, cuando el sistema falla en ventanillas, el procedimiento de contingencias mientras se restablece el sistema puede ser recibir depósitos, pagar cheques hasta cierto monto, etc. Una vez que el sistema se haya restablecido los cajeros deberán ingresar las transacciones que efectuaron manualmente en el tiempo que duró el evento y de esta manera evitar descuadres en su operación.

En la siguiente imagen mostramos el flujo de la continuidad del negocio que muestra gráficamente lo que hemos mencionado:



Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría.

En la operación normal que puede estar viviendo una Institución se presenta un siniestro que interrumpe el servicio que origina se adopten procedimientos de emergencia que incluyen preparación y activación de un

sitio alterno de procesamiento, el tiempo que dura la emergencia así como el regreso a la operación normal una vez superado el evento.

Es más fácil verlo gráficamente y parecería ser una tarea sencilla, no obstante es un proceso a mediano o largo plazo porque estamos hablando de una serie de planes que deben engranar en todas las operaciones de todas las unidades del Banco, lo cual nos lleva a pensar que en la práctica es real que sin la participación de todo el personal no se puede llevar a cabo un proyecto de esta magnitud.

Más adelante se explica en detalle todos los pasos que deben seguirse para establecer los planes.

4. Probar el plan

Todos los planes desarrollados deben ser sometidos a pruebas periódicas que contribuyen a validar su vigencia. Esto debe ser parte de la política establecida, sin importar el grado de dificultad se deben plantear pruebas periódicas que deben ser debidamente documentadas ya que son el insumo necesario para actualizar o ajustar los planes.

5. Mantener el plan

Producto de las pruebas y cambios propios de las organizaciones los planes son documentos que deben ser actualizados permanentemente, no cabría la posibilidad de establecer un plan y archivarlo. En la práctica si no se cumple esto, el riesgo de que el plan no sea de utilidad es muy alto.

4.1.2 Identificar los procesos críticos.

Los procesos críticos de la Institución deben ser debidamente identificados partiendo de un inventario inicial de todos los procesos y luego deberán ser sometidos a un análisis a fin de determinar su nivel de criticidad, mismo que

puede basarse en diversos criterios como por ejemplo su nivel de participación frente a todos los servicios que ofrece la organización, la rentabilidad que ofrecen con respecto a la totalidad de la utilidad o a los activos de la organización. Para el caso específico de la continuidad el criterio que debe primar está relacionado con los procesos que apalancan aquellos servicios que la organización está dispuesta a no dejar de otorgar a pesar de producirse un evento de contingencia menor o uno mayor que derive en la ejecución de los planes de continuidad planteados.

Estos procesos están directamente relacionados con los objetivos y metas que la organización se haya planteado, mediante sus planes estratégicos ya sean estos de mediano o largo plazo. Es muy importante que la gestión de continuidad del negocio tenga por tanto un nivel de comprensión y auspicio elevado para que se aseguren que estas metas y que los objetivos no se vean comprometidos por interrupciones inesperadas.

Las consecuencias de un incidente pueden variar en su impacto dependiendo del proceso que se vea afectado, siendo los más críticos aquellos a los que se debe dar prioridad de aseguramiento, a través de planes de contingencia y continuidad que contribuyan a disminuir el riesgo de que sean interrumpidos.

Se pueden identificar a los procesos críticos de una organización a través de varios mecanismos, entre ellos con cuestionarios de análisis de impacto, considerando su importancia y nivel de participación en la consecución de las metas establecidas por la Institución.

Fuente1: Superintendencia de Bancos y Seguros

Fuente2: Artículos del Internet página www.isec-global.com

Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría

COMENTARIO:

Es importante que los procesos críticos que constituyen el insumo para establecer el plan, se evalúen desde el punto de vista de la continuidad del

negocio con la contribución de los diferentes responsables de las unidades de negocio, además considerar el análisis de los recursos mínimos para mantener operativo un proceso, identificando cuáles son los más idóneos, no únicamente recursos humanos sino materiales, técnicos, de mantenimiento, etc.

Otro aspecto fundamental al momento de analizar los procesos es el tiempo o umbral permitido para no contar con el servicio o proceso y de ser posible cuantificar el valor que correspondería en función de este tiempo, la interrupción del servicio.

Una vez que se encuentren debidamente especificados los procesos críticos es necesario que sean aprobados por la administración y se priorice su análisis de riesgos e impacto para poder implementar las diferentes estrategias de continuidad.

4.1.3 Identificación de los riesgos y su impacto.

1. Análisis de Riesgos

Considerando que un plan de continuidad del negocio contiene las medidas o estrategias y aportación de recursos para hacer frente a situaciones creadas como consecuencia de la materialización de un riesgo, es básico antes de plantear las medidas a adoptar, analizar las amenazas más probables.

El análisis de riesgos que elabore la Institución deberá considerar entre sus objetivos:

- Analizar los riesgos a los que se ve expuesta la organización incluyendo los riesgos potenciales
- Incluir en el análisis la probabilidad y consecuencias o impacto de los riesgos identificados

- Determinar cuáles son los niveles de riesgo que la Institución está dispuesta a aceptar.

En 1974 el National Bureau of Standards de los Estados Unidos, nombrada en la actualidad como National Institute of Standards and Technology, publicó su Automated Data Processing Physical Security and Risk Management (FIPS-31), en el cual se incluía brevemente la idea del análisis de riesgos, pero no se establecía ninguna forma de metodología formal.

Posteriormente, en la publicación Guidelines for Automated Data Processing Risk Analysis, (FIPS-65), publicado en 1979 incluyó la primera metodología de análisis de riesgos que contenía un algoritmo muy simple para la cuantificación del riesgo.

A partir de este inicio se han diseñado innumerables metodologías con más o menos variaciones, pero tomando en cuenta la misma base de razonamiento, tomando en cuenta seis elementos que forman parte del riesgo, que son:

- Valor de los activos: el valor económico de los bienes o propiedades de la Institución.
- Frecuencia de la amenaza: cuántas veces es probable que ocurra un evento generalmente tomando el rango de un año como referencia.
- Impacto de la amenaza: el costo expresado en porcentaje del valor del activo dañado, producto de la ocurrencia de un suceso.
- Eficacia de las medidas de seguridad adoptadas.
- Costo de las medidas adoptadas: el costo no solo de la implantación, sino también el mantenimiento, reposición y adaptación en caso de cambios.
- Incertidumbre: Grada de confianza en las cantidades aplicadas a los elementos anteriores.

Al ser la incertidumbre el elemento determinante de riesgos, ya que el resto de elementos dependen de él, se concluye que si bien algunos de ellos se pueden cuantificar fácilmente, existe la necesidad de basarse en las estadísticas de eventos producidos e impacto sufrido. El inconveniente es que no existe en el país ni en varios países la cultura del análisis de riesgos que permitan mantener información histórica de costos incurridos derivados de incidentes de seguridad, ni tampoco datos sobre los costos de implementar sistemas de seguridad o soluciones puntuales a inconvenientes, que puedan ser utilizados en la valuación por lo que esta se vuelve netamente subjetiva.

Identificación de amenazas y vulnerabilidades

Dentro del análisis de riesgos es muy importante hacer un levantamiento de los tipos de amenazas a los que nuestros sistemas pueden estar expuestos, no se debe descartar ninguno, no obstante deben ser amenazas reales que verdaderamente apliquen a la Institución, ya que si los esfuerzos se centran en amenazas que jamás van a pasar o su probabilidad es poco menos que remota se estarían desperdiciando recursos. Hay que tener presente que la actitud de querer estar protegido contra todo cuando en muchos casos no existen las más elementales medidas de seguridad, resulta poco práctica y en muchas ocasiones conduce a la parálisis.

De acuerdo con algunas metodologías definidas se pueden elaborar catálogos de amenazas posibles, tomando como referencia grupos definidos que contienen: accidentes, errores, amenazas intencionales y amenazas internacionales.

Grupo A de Accidentes

- Accidentes físicos de origen industrial: incendio, explosión, inundación por roturas, daños por industrias cercanas o emisiones radioeléctricas.

- Averías: de origen físico o lógico, debido a defectos de origen o sobrevenidas durante el funcionamiento del sistema.
- Accidentes físicos de origen natural: fenómenos sísmicos o volcánicos, meteoro, rayo, desplazamientos de tierra, avalancha, derrumbe, etc.
- Interrupción de servicios o de suministros esenciales: energía, agua, telecomunicación, fluidos y suministros diversos. (vulnerabilidades en servicios provistos por terceros).
- Accidentes mecánicos o electromagnéticos: choque, caída, cuerpo extraño, radiación, perturbación electrostática.

Grupo E de Errores

- Errores de utilización ocurridos durante la recolección y transmisión de datos o en su explotación por el sistema.
- Errores de diseño existentes desde los procesos de desarrollo del software.
- Errores de ruta, secuencia o entrega de información en tránsito.
- Inadecuado monitoreo de la trazabilidad, registro de la información enviada y recibida.

Grupo P de Amenazas Intencionales Presenciales

- Acceso físico no autorizado con inutilización por destrucción o sustracción (de equipos, accesorios o infraestructura).
- Acceso lógico no autorizado con intercepción pasiva simple de la información.
- Acceso lógico no autorizado con alteración o sustracción de la información en tránsito o de configuración, es decir, reducción de la confidencialidad del sistema para obtener bienes o servicios aprovechables (programas, datos, etc.).
- Acceso lógico no autorizado con corrupción o destrucción de información en tránsito o de configuración.

- Indisponibilidad de recursos, sean humanos (huelgas, abandono, rotación) o técnicos (desvío del uso del sistema, bloqueo). Sabotaje interno.

Grupo T de Amenazas Intencionales de Origen Remoto

- Acceso lógico no autorizado con intercepción pasiva (para análisis de trafico de información)
- Acceso lógico no autorizado con corrupción o destrucción de información de información en tránsito o de configuración, es decir, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje inmaterial, infección vírica, etc.).
- Acceso lógico no autorizado con modificación de información durante la transmisión.
- Suplantación de origen del emisor o reemisor o de Identidad.
- Repudio del origen o de la recepción de información en el proceso de transmisión de datos.

Identificación de riesgos potenciales, probabilidades y consecuencias

Independientemente del método que la Institución adopte para su sistema de seguridad, es importante que se establezcan políticas y procedimientos que sean aplicables y de conocimiento general.

El análisis de riesgos debe incluir la detección de las vulnerabilidades de la organización ante las amenazas a que está expuesta, el análisis deberá hacerse de manera detallada para que el nivel de certeza sea mayor, y por tanto sean más eficaces las medidas que se implementen para la protección de la información.

Con el fin de que las medidas puedan afectar a los aspectos más importantes de la Institución, es importante priorizar los riesgos y ordenarlos de acuerdo a su criticidad.

Cuando ya se disponga de este levantamiento de los riesgos se debe armar la matriz de riesgos que incluye la probabilidad y el impacto del riesgo identificado, así como también los controles establecidos para su mitigación y las recomendaciones que correspondan.

El objetivo final del análisis de riesgos debe ser mantener un mapa de riesgos Institucional que permita tomar decisiones y adoptar medidas de seguridad en función de la realidad de los riesgos y su evolución permanente.

Las decisiones que puede adoptar la Institución frente a los riesgos identificados pueden ser:

- Transferir el riesgo mediante la contratación de pólizas de seguros.
- Eliminar el riesgo (en los casos en que sea factible) mediante la adopción de las acciones recomendadas en el informe.
- Reducir el riesgo en los casos en que su eliminación no sea posible.
- Aceptar el riesgo cuando la probabilidad de ocurrencia sea muy baja, o el coste de las medidas para eliminarlo o reducirlo no sea aplicable para la Institución.
- Una combinación de todas ellas.

2. Análisis de Impacto

Considerando que dentro de la Institución algunos procesos pueden ser más críticos que otros y que esto depende inclusive de la época por la que estén atravesando, es importante a través del análisis de impacto, otorgar a la alta gerencia elementos para que puedan tomar decisiones sobre las estrategias de recuperación que más le convengan.

Para conseguir este propósito es importante contar con un análisis de riesgos detallado, que permita obtener el grado de criticidad de los procesos

y el tiempo máximo a partir del cual, la interrupción de cada uno de ellos es inaceptable.

Planteado de esta manera se pueden incluir como objetivos de este análisis a los siguientes enunciados:

- Definir los tipos de impacto que se deberían considerar, ya sean de tipo económico, jurídico, comercial, operacional, reputacional, etc.
- Establecer el nivel de criticidad de los procesos de la Institución, en función de lo que representa la interrupción de cada uno de ellos.
- Informar al Directorio u organismo que haga sus veces el resultado del análisis anterior, de tal manera que puedan definir que procesos son considerados prioritarios y establecer el umbral máximo de recuperación para cada uno de ellos.
- Identificar los recursos mínimos necesarios para una recuperación satisfactoria de los procesos identificados como críticos.

Tipos de Impacto y Criterios de Valoración

El impacto se puede definir como las consecuencias negativas que puede sufrir la Institución producto de algún tipo de interrupción en uno o varios de sus procesos críticos.

Los impactos están directamente relacionados a un período de tiempo y pueden ser catalogados de diversos tipos de impactos como por ejemplo:

- Aumento de costos o gastos: se pueden generar pérdidas en los ingresos de las Instituciones o generar incremento en los costos o gastos derivados de la falta de productividad, multas, defectos o faltas de control en los diferentes procesos críticos de la organización.
- Peligro para el personal: si no se adoptan medidas de seguridad apropiadas en determinadas funciones y procesos de una

organización, pueden provocar incidentes o situaciones de riesgo para el personal. La valoración se debe basar en criterios lo más objetivos posible y calificando con escalas que pueden ir desde bajo, medio, alto, o en escala desde leve, medio, grave, catastrófico; dependiendo de la decisión de la organización, lo importante es tratar de ser lo más explícito posible.

- Impacto operacional: se refiere al mal funcionamiento o fallas en los procesos críticos de la Institución, que en principio se podrían valorar de manera cualitativa, aunque en muchos casos se podrá cuantificar por repercusión de un proceso con respecto a otro u otros.
- Impacto de tipo comercial: este tipo de impacto se refiere a la interrupción o errores en la relación con los clientes, los mismos que pueden interpretar la interrupción o falla como un incidente grave y mantenerse en espera o dependiendo de su criterio pueden hasta cambiar a la Institución por otra que le ofrezca mayor continuidad o efectividad en su servicio.
- Fallas o pérdida de calidad: se incluyen en este tipo de impacto las funciones o procesos cuya interrupción afecta al control de calidad de los servicios o productos que otorga la Institución a sus clientes.
- Impacto en la imagen de la organización: las fallas o interrupciones de determinados procesos pueden o no causar pérdidas de manera inmediata pero si un deterioro de la imagen de la Institución frente a sus clientes. Su criterio de valoración solamente puede ser cualitativo en el corto plazo.
- Impacto por incumplimiento de obligaciones legales: una función que si queda interrumpida, genere problemas de incumplimiento de obligaciones expone a la Institución a sanciones económicas o administrativas por parte de los organismos de control. Este tipo de impacto se puede valorar de manera cuantitativa, aunque deficiencias de este tipo también tienen repercusiones de la imagen de la Institución.

- Impacto ambiental: se refiere a los tipos de impactos sobre la salud de la población o impacto en el medio ambiente, derivados de procesos cuya interrupción o fallas ocasionen estos daños. El criterio de evaluación puede ser cuantitativo en el caso de sanciones o multas, así también puede resultar en impacto sobre la imagen de la Institución.

Fuente1: Superintendencia de Bancos y Seguros

Fuente2: Artículos del Internet página www.isec-global.com

Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría

COMENTARIO:

El análisis de riesgos e impacto de estar enfocado en el inventario de los procesos críticos definidos en la Institución, el nivel de criticidad está directamente relacionado con la contribución o aporte de los mismos, así como los recursos mínimos necesarios que se requerirán frente a las diferentes contingencias o fallas que pudieran presentarse.

Como todo proceso en el tiempo puede variar y por tanto algún proceso que originalmente no fue catalogado como crítico ahora si lo es y al revés.

La Institución podrá establecer las prioridades asignadas en los procedimientos dependiendo de su nivel de criticidad, en función del análisis de riesgos así como de todas las etapas mencionadas anteriormente. Es importante considerar no únicamente el impacto individual, sino las interrelaciones existentes entre todos los procesos.

La relación de los procesos se puede clasificar de períodos más cortos a más largos y de impacto más grave a más leve, así los procesos cuya interrupción dé cómo consecuencia un impacto más grave a corto plazo, deben ser considerados más críticos, pero también podría ocurrir que un proceso cuyo impacto es leve en un primer momento, llegue a convertirse en más critico que el resto con el transcurrir del tiempo. Todas estas

circunstancias particulares de cada proceso se deberán considerar a la hora de establecer los objetivos y los umbrales de recuperación. A continuación se muestra un ejemplo:

UN DIA					
PROCESO	**IMPACTO**	**LEVE**	**MEDIO**	**GRAVE**	**CATASTROFICO**
A	Económico		x		
B	Operacional	x			
D	Comercial	x			
C	Ambiental	x			

DOS DIAS					
PROCESO	**IMPACTO**	**LEVE**	**MEDIO**	**GRAVE**	**CATASTROFICO**
A	Económico		x		
B	Operacional	x			
D	Comercial		x		
C	Ambiental	x			

UNA SEMANA					
PROCESO	**IMPACTO**	**LEVE**	**MEDIO**	**GRAVE**	**CATASTROFICO**
A	Económico			x	
B	Operacional			x	
D	Comercial				x
C	Ambiental		x		

UN MES					
PROCESO	**IMPACTO**	**LEVE**	**MEDIO**	**GRAVE**	**CATASTROFICO**
A	Económico				x
B	Operacional				x
D	Comercial				x
C	Ambiental			x	

Fuente: Libro PLANES DE CONTINGENCIA, Juan Gaspar Martínez

Analizando este ejemplo, supongamos que se trata del daño de un servidor que provee de servicios de roles de pago a varios clientes corporativos del Banco, en el día uno el impacto por la falla puede ser medio en el tema económico porque el Banco dejaría de percibir los ingresos de las Empresas que han cargado sus órdenes.

Ya para el día dos, suponiendo que no se logra restaurar, ya no solo existe el impacto económico sino comercialmente se ven afectados los clientes al no poder ejecutar sus transacciones previamente establecidas.

En una semana las cosas empeoran toda vez que los clientes comerciales pueden perder oportunidades de negocios, y el mismo Banco puede verse afectado por el cierre de cuentas o pérdida de clientes al no restaurar las operaciones, también vemos que existe un impacto ambiental que puede estar derivado de una serie de medidas que van desde incluir equipos adicionales en la Institución de manera emergente y desordenada por la contingencia, sin medir el impacto en consumo de energía eléctrica, aire acondicionado, etc. que comienzan a perjudicar los niveles de control ambiental que se manejan.

En un mes resulta catastrófico, puesto que para esta fecha lo más probable es que las pérdidas sean enormes tanto para la Institución Financiera que pudiera en estas circunstancias dejar de otorgar el servicio, como para los clientes que perdieron un sin número de oportunidades de negocios.

En línea con lo explicado en este ejemplo resulta muy importante establecer tiempos máximos de espera para cada proceso crítico, llegar a determinar de manera concensuada con todas las Unidades del negocio el límite de pérdida que se puede asumir por dejar de operar o de dar un servicio.

Esto es similar a situaciones que nos pasan a diario, por ejemplo cuando una persona se levanta con el tiempo justo en la mañana, tiene todo calculado para llegar al trabajo y sale al garaje encontrando una llanta baja en su auto. Su contingencia es la llanta de emergencia que tiene lista para ser utilizada en casos así, y con esto en un tiempo determinado consigue transportarse y llegar a su destino. La persona debe asumir las consecuencias de esta decisión.

Otra alternativa o plan sería en función del tiempo que tiene tomar un taxi dejar el auto para reponer la llanta luego de solventar algunos pendientes

en su trabajo. De igual manera las consecuencias son asumidas por la persona.

Objetivos de recuperación, tiempos máximos y pérdidas asumidas

COMENTARIO:

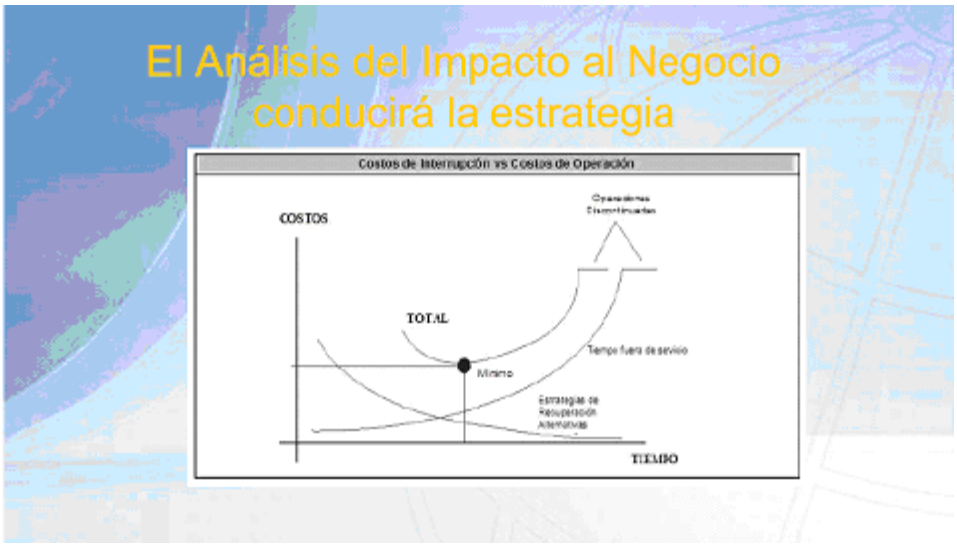
Resumiendo un poco lo que hemos comentado, la Institución debe establecer el orden de recuperación de los procesos, pensando obviamente en sus objetivos y el impacto sufrido cuando se produjo la interrupción.

Por otro lado debe analizar el impacto económico que significa adquirir recursos que hagan posible esta recuperación, no siempre es posible mantener un site alterno de igual magnitud que el principal, al menos en las actuales circunstancias del país y específicamente de la banca ecuatoriana.

En tal virtud existe un margen de pérdida que debe asumir la Institución y que debe estar claramente aceptada por la Alta Gerencia, esto no es una utopía si nos detenemos a pensar que quiénes son los que finalmente aprueban los recursos son ellos, entonces es posible.

Aunque no se puede negar el avance tecnológico que existe en la actualidad, la pretensión de recuperar todo inmediatamente con sólo apretar un botón, sigue siendo una ficción que inclusive puede provocar una parálisis, lo cual sería más perjudicial para una Institución.

En este gráfico se ilustra la importancia que tiene para la organización el análisis de impacto.



Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría.

En el gráfico se muestra la relación de tiempo frente a los costos que puede incurrir la Institución, la conjunción ideal para que se pueda establecer un tiempo mínimo en el que exista un equilibrio entre el costo de tiempo fuera de servicio y el costo de las estrategias de recuperación, se marca con un punto negro. Si esta variable pasa de este punto, los costos tanto de implementación de estrategias así como el tiempo fuera de servicio representan pérdida para las Instituciones, puesto que estaría saliendo de los límites fijados o establecidos previamente.

Es muy importante contar con un análisis previo del impacto que puede causar un evento, resultando más valioso aún el análisis posterior de un evento ya que permite ajustarse a la realidad y poder proyectar con mayor certeza aquellos eventos que no se han producido todavía. No olvidemos que los procesos cambian y por tanto sus riesgos también por lo que los planes de contingencias también deben ser actualizados.

4.1.4 Elaboración del plan de contingencias y continuidad.

Implementar un plan de contingencias y continuidad como parte del plan estratégico de la Institución, incluyendo a todos los departamentos y áreas,

es un proceso diseñado para reducir el riesgo operacional de negocio de una organización.

Su desarrollo, implementación y mantenimiento proporcionan a la organización una serie de beneficios frente a posibles fallas o interrupciones como:

- Minimizar potenciales pérdidas económicas.
- Reducir riesgos potenciales.
- Reducir las probabilidades de que ocurran interrupciones.
- Reducir interrupciones en las operaciones.
- Asegurar la estabilidad de la organización.
- Facilitar una recuperación ordenada.
- Minimizar las primas de seguros.
- Reducir la dependencia de ciertos elementos clave.
- Proteger los activos de la organización.
- Ampliar la seguridad del personal y de los clientes.
- Minimizar la necesidad de toma decisiones durante un incidente.
- Minimizar las responsabilidades legales.

Dependiendo de la metodología que se adopte el plan se formará considerando el desarrollo de algunas etapas o fases que pueden variar según la necesidad y estructura de la Institución, no obstante si tomamos como referencia las mejores prácticas se podrían considerar como partes del plan a las siguientes etapas:

- Creación de una política de continuidad del negocio y recuperación de desastres.
- Evaluación de riesgos.
- Análisis de impacto.
- Clasificación de los procesos y análisis de su criticidad.
- Desarrollo de la estrategia
- Respuesta a emergencias y operaciones

- Desarrollo de un plan de continuidad del negocio y procedimientos de recuperación de desastre.
- Programa de entrenamiento y concientización.
- Plan de pruebas y mantenimiento del plan.
- Comunicación de crisis y coordinación con externos.

Política de continuidad del negocio

Es importante que la Institución establezca la necesidad de disponer de una gestión de la continuidad de las operaciones mediante la elaboración y gestión de un Plan de Continuidad del Negocio, incluyendo el apoyo del Directorio de tal manera que el proyecto sea gestionado apropiadamente procurando que se cumplan los plazos y costos previamente establecidos.

Es importante conocer muy bien las necesidades propias de la Institución, también las limitaciones y definir claramente desde el principio para qué se está planificando y para que no se está planificando, mediante la definición de los llamados supuestos de partida. Es la única manera de definir un proyecto a la medida de las necesidades, aunque nos se puedan cumplir todas a la vez, pero teniendo en cuenta los recursos disponibles.

A través de una política de continuidad del negocio se pueden consolidar todos estos conceptos y definiciones, normando los lineamientos que la organización adoptará y con respecto a la continuidad de sus operaciones. Además con este respaldo se consigue el auspicio y respaldo de toda la Institución, por tanto el apoyo y contribución de todos sus funcionarios.

La política de la continuidad del negocio deberá incluir el alcance de la gestión y los términos en que se establecerán las diferentes estrategias.

Evaluación de riesgos

En el marco de la gestión de continuidad del negocio, el nivel de riesgo debe ser comprendido de manera específica con respecto a las actividades o procesos críticos de la organización, y el riesgo de una interrupción de los mismos.

Los procesos críticos son soportados por recursos como personas, tecnología, información, suministros, infraestructura física, etc. La organización debe entender las amenazas existentes para todos estos recursos y el impacto producido si una amenaza se convierte en incidente y provoca una interrupción.

El enfoque que la Institución le dé a la evaluación de riesgos, depende en gran medida de la conveniencia y necesidades que tenga, existen de acuerdo con las mejores prácticas, lineamientos que permiten elegir el enfoque apropiado. Los elementos más comunes que se pueden incluir en el mismo son:

- Determinación de los criterios para la aceptación de riesgos, éstos describen las circunstancias en las cuales la organización está dispuesta a aceptar los riesgos.
- Identificación de los niveles aceptables de riesgos, no importa que enfoque de evaluación se adopte.
- Considerar dentro del análisis de riesgos las amenazas específicas que pueden en algún momento causar un tipo de impacto sobre los recursos. Además identificar las vulnerabilidades en los diferentes procesos y recursos que pueden ocasionar algún tipo de interrupción en el proceso.

Posterior a esta evaluación, es importante identificar las medidas que reduzcan la probabilidad de interrupciones, reduzcan el tiempo de la

interrupción y limiten el impacto de una interrupción sobre los procesos críticos de la organización.

Estas medidas se conocen como reducción de pérdidas y tratamiento del riesgo y deben considerar que no todos los riesgos pueden ser prevenidos o reducidos a un nivel aceptable, depende de las estrategias, controles y hasta costo de las soluciones o medidas.

La organización puede aplicar una o varias de las estrategias de reducción de pérdidas frente a los riesgos identificados, dependiendo de su respuesta al riesgo. Las estrategias pueden ser:

- Continuidad del proceso: estas estrategias buscan mejorar la fortaleza de la organización frente a una interrupción asegurando los procesos críticos, para que sigan funcionando o sean reanudadas a un nivel mínimo aceptable y en los plazos estipulados por el plan.
- Aceptación del riesgo: se puede aceptar un nivel de riesgo sin tomar acciones adicionales, la capacidad de hacer algo sobre ciertos riesgos podría ser limitada, o el costo de adoptarlas puede ser elevado. La respuesta podría ser tolerar un nivel de riesgo siempre y cuando la dirección de la organización la acepte expresamente.
- Transferencia del riesgo: en otros casos se puede transferir el riesgo, puede ser por medio de pólizas de seguros, arreglos contractuales, o contratando un tercero que se ocupe del riesgo de una manera distinta. Es importante determinar que existen algunos riesgos no son totalmente transferibles.
- Cambio, suspensión o terminación: en algunos casos resulta adecuado hacer cambios a los procesos, suspenderlos o terminarlos en función del análisis de riesgos e impacto resultante, siempre y cuando no afecte a los objetivos estratégicos de la organización.

Análisis de impacto

La organización debe determinar y documentar el impacto que puede tener una interrupción sobre las actividades que respaldan sus procesos o productos claves o críticos.

Para cada proceso crítico se debe evaluar el tiempo que se puede dejar de contar con el mismo, así como su relación con las metas y objetivos del negocio.

Todo este proceso que se encuentra detallado más adelante, debe ser documentado y mantenido a través del tiempo.

Es importante recordar que durante una interrupción, los impactos por lo general aumentan conforme pasa el tiempo y afectan de manera diferente a cada actividad. Los impactos también podrían variar dependiendo del día, mes o punto dentro del ciclo de vida del negocio en que ocurran.

El periodo máximo tolerable de interrupción influirá en el objetivo de tiempo de recuperación de cada actividad cuando se determinen las estrategias del proceso de continuidad.

Clasificación de los procesos y análisis de su criticidad.

Para el proceso de continuidad, es ideal que las organizaciones clasifiquen sus procesos en función de cuan prioritaria es su recuperación, aquellas actividades cuya pérdida sea de mayor impacto y que requieren ser recuperadas o repuestas más rápidamente que las demás, pueden ser catalogadas como criticas.

Este análisis debe partir de un inventario total de procesos, puesto que hay que considerar aquellos que en un principio pueden no ser los más

importantes, pero en función del tiempo transcurrido llegan a ser críticos para la disponibilidad del servicio de la Institución.

Se debe considerar que el periodo máximo de tiempo para la reanudación de las operaciones puede variar entre segundos y varios meses, dependiendo de las estrategias de recuperación adoptadas por la Institución, en base a sus necesidades y recursos disponibles.

Desarrollo de la estrategia

La Institución debe establecer las estrategias de continuidad para sus procesos críticos considerando el riesgo e impacto frente a los objetivos de la organización, así como también el período máximo tolerable de interrupción del proceso, los costos de implementar las estrategias y las consecuencias de la inacción.

De acuerdo con las mejores prácticas se podría requerir estrategias para los recursos: personas, lugar físico de operaciones, tecnología, información, suministros, partes interesadas.

Personas: es importante identificar estrategias adecuadas para proteger al personal clave previamente seleccionado, ya sea por sus destrezas como por sus conocimientos. Una estrategia puede ser contar con personal backup o de respaldo para evitar concentrar funciones criticas en una sola persona, otra puede basarse en programas de capacitación, sistemas de rotación del personal en áreas críticas, etc.

Sitio físico de operación: la organización debe contar con estrategias para cuando las instalaciones normales de operación no puedan ser utilizadas por diferentes incidentes. Ya sea con un centro de procesamiento alterno u oficinas alternativas provistos con insumos básicos, alquiler de centros de operación de otras organizaciones afines que se puedan utilizar a través de

contratos de arrendamiento, o en su defecto contratando a terceros para que realicen las operaciones que están interrumpidas.

Tecnología: las estrategias de tecnología dependerán de la infraestructura empleada y de su relación con los procesos críticos, pero de manera general deberán considerar una combinación de los siguientes aspectos:

- Planes de contingencia que permitan minimizar las interrupciones prolongadas de los servicios, que deben estar operativos.
- Contratos de mantenimiento vigentes de la infraestructura principal que soporta los procesos críticos de la organización.
- Conservar equipos antiguos como reemplazos de emergencia o repuesto.
- Mantener piezas y partes como repuestos.

En lo que a servicios de tecnología se refiere, pueden requerir complejas estrategias de continuidad, en las cuales se puede considerar lo siguiente:

- Implementación de un sitio alterno tecnológico de procesamiento.
- Definición de los tiempos de recuperación para sistemas y aplicaciones que respaldan los procesos críticos de la organización.
- Contar con estrategias para contar con la conectividad de telecomunicaciones apropiada para el sitio alterno.
- Establecer contratos con proveedores de software y hardware, así como acuerdos de servicio.
- Determinar al personal backup o de respaldo que pueda operar los servicios de tecnología desde el sitio alterno sin inconvenientes.
- Contar con un plan de retorno al sitio principal de procesamiento.

Información: resulta imprescindible que la información más importante para las operaciones de la organización debe estar debidamente protegida y que pueda ser recuperable dentro los plazos establecidos.

Se pueden utilizar diversos métodos para proteger la información, como copias electrónicas o en cintas, microfichas, fotocopias, copias dobles, etc.

Recordemos que toda información requerida para desarrollar los procesos críticos de la organización, debe cumplir con los principios de confidencialidad, integridad, disponibilidad y aceptación.

Los procesos de recuperación de la información respaldada deberán incluir pruebas periódicas que aseguren la validez del método empleado y que la información cumpla con los principios indicados.

Suministros: debe existir un inventario de los suministros esenciales que se utilizan en los procesos críticos, las estrategias para asegurar su provisión podrían incluir: almacenamiento de suministros adicionales en un lugar alterno, acuerdos con terceros para la provisión de existencias solicitadas con poca antelación, identificación de suministros alternativos o sustitutos, etc.

Partes interesadas: La organización debería identificar estrategias adecuadas para gestionar sus relaciones con partes interesadas, negocios, asociados de servicios y contratistas clave.

Respuesta a emergencias y operaciones

La Institución debe conseguir desarrollar e implantar procedimientos para responder frente a los incidentes o contingencias que pudieran presentarse, para lo cual debe considerar al menos lo siguiente:

- Identificar emergencias potenciales y los tipos de respuesta para cada uno de ellos.
- Evaluar los procedimientos creados para atender emergencias.
- Estos procedimientos deben estar alineados con los desarrollados para continuidad, considerando que en muchas ocasiones un plan

de continuidad se activa posterior a tener algún tipo de emergencia o contingencia en la organización.

- Identificar las necesidades de la organización para hacer frente a la emergencia presentada.
- Determinar líneas de mando y procedimientos de actuación durante la emergencia, incluyendo responsabilidades.
- Revisar los procedimientos desarrollados asegurando que están enmarcados en las leyes vigentes.

Desarrollo de un plan de continuidad del negocio y procedimientos de recuperación de desastre

Para llevar a cabo el desarrollo e implantación de los planes de continuidad de la organización deberán considerar los siguientes pasos:

- Identificar los componentes del proceso de planificación: metodología de planificación, organización del plan, necesidades de personal, recursos requeridos, etc.
- Controlar el proceso de planificación y elaboración del Plan.
- Planificar el regreso a la normalidad de las operaciones.
- Proceso implementación del Plan.

Identificar componentes del proceso de planificación: dentro de este proceso es necesario establecer la metodología a emplear, los responsables de realizarlo, necesidades de personal y recursos a fin de cumplir con los objetivos planteados, en función de los procesos críticos.

Si bien existen varias metodologías disponibles, todas buscan cubrir los mismos objetivos: determinar procesos críticos, definir las necesidades para la recuperación de los procesos críticos, definir estrategias para la recuperación, establecer los recursos necesarios, elaborar pruebas y mantener actualizados los planes.

Es importante considerar que el responsable o coordinador debe contar con el soporte de todas las áreas de la Institución de tal manera que el apoyo durante todo el proceso sea uno de los pilares para que los planes resulten apropiados.

Controlar el proceso de planificación y elaboración del Plan: Es importante contar con el auspicio de la Gerencia General de la organización, en todas las fases de la planificación y elaboración del plan, esto facilita contar con el soporte y las opiniones del proceso en todo momento, así se asegura que los objetivos planteados se vayan cumpliendo, caso contrario podría pasar que a pesar de contar con un plan debidamente elaborado no sea aplicable puesto que está alejado de los objetivos estratégicos de la organización.

Es importante llevar a cabo un proceso ordenado, los planes y procedimientos deben estar elaborados en formatos estándar que todos conozcan y entiendan y que brinden facilidades para su mantenimiento.

Todos los planes deben contener los pasos a seguir antes, durante y después de la interrupción del servicio, hay que tener presente que no se pueden completar si antes no se han fijado las estrategias que aplicarán frente a los casos o escenarios de desastre planteados.

Es necesario estructurar cronogramas que permitan efectuar seguimientos oportunos del avance. El Plan debe estructurarse con la ayuda de equipos de recuperación, asignando responsabilidades específicas a cada uno.

Deberá existir un Comité o Gabinete de crisis cuyas funciones principales son: evaluar el incidente, activar el plan de recuperación y coordinar con el resto de equipos.

También contribuye a la supervisión del desarrollo del plan, de la documentación y coordinación del proceso de recuperación. Sus miembros

son responsables finales de tomar las decisiones, fijar las prioridades y las políticas a seguir en materia de continuidad del negocio.

Otro aspecto muy importante a considerar es la definición del centro de control o de operaciones de emergencia, es decir desde donde se dirigirán las operaciones durante una contingencia.

Planificar el regreso a la normalidad de las operaciones: esta planificación es tan importante como aquella realizada para activar el plan y procesar las operaciones desde el sitio alterno.

Es importante contar con procedimientos formales que incluyan algunas actividades importantes como:

- Establecer una reunión con el Comité de crisis o de gestión de incidentes con el propósito de estudiar las estrategias que se implementarán para el retorno a las operaciones normales de la Institución.
- Llevar a cabo reuniones de planificación con los equipos de recuperación para revisar los procedimientos a seguir, principalmente aquellos que controlan el manejo de la información critica, que buscan asegurar de mantener la integridad de la misma.
- Revisar las estrategias y procedimientos a seguir, y comunicar a toda la organización para que contribuyan en los aspectos que puedan según su ubicación en la organización.
- Evaluación de los resultados de la aplicación de los planes de retorno y ajuste de los planes en lo que aplique.

Implementación del Plan: las actividades para la implementación del plan van encaminadas al establecimiento de: implementar el centro de operaciones alterno, el centro de procesamiento o site alterno y centro de almacenamiento o respaldo externo. Así también incluye la identificación de

las acciones y recursos necesarios para poner en práctica las estrategias definidas.

Estas actividades van desde generar la documentación respectiva hasta adquirir los insumos o recursos necesarios, así como organizar al personal que interviene en el desarrollo de los planes y capacitar a todo el personal de la organización.

Al igual que los planes, es importante probar las instalaciones una vez que se encuentren listas, ajustar procedimientos, elaborar simulacros con los equipos que intervienen, comprobar equipos, líneas telefónicas y demás implementos necesarios para la operación desde los sitios alternos, asegurando su funcionamiento.

Programa de entrenamiento y concientización

Como parte del desarrollo de los planes de contingencia y continuidad, resulta básico que todo el personal de la organización tenga plena conciencia de la importancia de los mismos. La única forma de lograr que funcionen los planes es con la contribución y ayuda de todos los funcionarios.

Los planes de capacitación deben estar debidamente organizados y coordinados con Recursos Humanos. Es importante hacer seguimiento del cumplimiento y dejar documentados los resultados.

En este tipo de proyectos al recibir el auspicio directo de la Gerencia de la organización es más fácil lograr que el resto de la organización apoye no sólo asistiendo a las capacitaciones sino aportando con ideas que pueden optimizar los planes y estrategias planteadas.

Es fundamental que el personal comprenda que estos procesos son continuos y una vez implementados son parte integrante de la vida de la

organización, por tanto es ilimitado, ya que al desarrollarse un nuevo servicio o producto ingresa al esquema de continuidad si es categorizado como crítico y por tanto contará con un plan que deberá ser informado y capacitado al personal que corresponda.

En la actualidad los métodos de capacitación son diversos, gracias a los recursos tecnológicos ya no es indispensable reunir en un solo sitio a todo el personal a ser capacitado, sino que se pueden enviar documentos, generar herramientas como e-learning, aprovechar el uso del correo electrónico para capacitar al personal.

Plan de pruebas y mantenimiento del plan

Es parte integrante del desarrollo de un plan de continuidad la ejecución de pruebas, y existen algunos tipos que van desde la revisión de escritorio o lectura de los planes hasta la ejecución misma de las operaciones desde los sitios alternos de procesamiento.

Es importante y base fundamental para conseguir éxito en las pruebas a realizar contar con una planificación adecuada, hay que considerar todos los elementos que participan, desde los recursos humanos, insumos, tecnología, proveedores, etc.

Por otro lado se deben documentar los resultados de las pruebas, así como hacer los ajustes que correspondan en los planes dependiendo de la ejecución de las pruebas.

Tanto la ejecución de las pruebas como el mantenimiento del plan deben formar parte de las políticas y procedimientos de continuidad fijados por la organización, de tal manera que se pueda dar seguimiento a su cumplimiento.

Comunicación de crisis y coordinación con externos

Es parte integrante del plan de continuidad contar con un procedimiento de comunicación que incluye listas de contactos internos y externos.
Adicionalmente es básico establecer los canales regulares de comunicación en caso de un incidente, las que deben ser conocidas por todo el personal con el fin de evitar confusiones antes, durante y después de presentarse un evento de contingencia.

Estas listas deberán ser verificadas permanentemente puesto que en el tiempo se dan cambios de personal, pueden ser parte de las pruebas periódicas que se realizan sobre el plan. Deben existir responsables de actualizarlas dentro de cada grupo de trabajo y deben estar disponibles.

Con relación a externos sean clientes o proveedores también debe ser desarrollada una estrategia de comunicación que permita informar apropiadamente o coordinar acciones para no causar confusiones ni malos entendidos que pudieran afectar la imagen de la organización.

Estos procedimientos deben estar formalmente establecidos y acordados sobre todo con los terceros, es importante mantener comunicación activa para que las listas de contactos se mantengan debidamente actualizadas.

Fuente1: Superintendencia de Bancos y Seguros
Fuente2: Artículos del Internet página www.isec-global.com
Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría

COMENTARIO:

Los planes o el plan de continuidad del negocio tienen como objetivo principal reducir el riesgo de operación o riesgo operacional de una Institución, en este sentido fue incorporado como parte de la norma emitida por la Superintendencia de Bancos.

En los párrafos anteriores se muestran los principales componentes del plan así como el alcance de cada uno de ellos, no obstante haciendo un resumen de los aspectos más relevantes que deben considerar en este proceso podemos mencionar:

- El Plan de Continuidad del Negocio no está limitado a las operaciones que tienen soporte en la tecnología, sino que abarcan todos aquellos que la organización quiere mantener funcionando en tiempo de interrupciones. Por ejemplo: la seguridad física de sus funcionarios, seguridad de las instalaciones.

- Se identifican las amenazas potenciales de la Institución y sus impactos en la operatividad del Banco, por eso es tan importante y estratégica.

- Establece diferentes estrategias para sostener o recuperar aquellos procesos catalogados como críticos para el negocio.

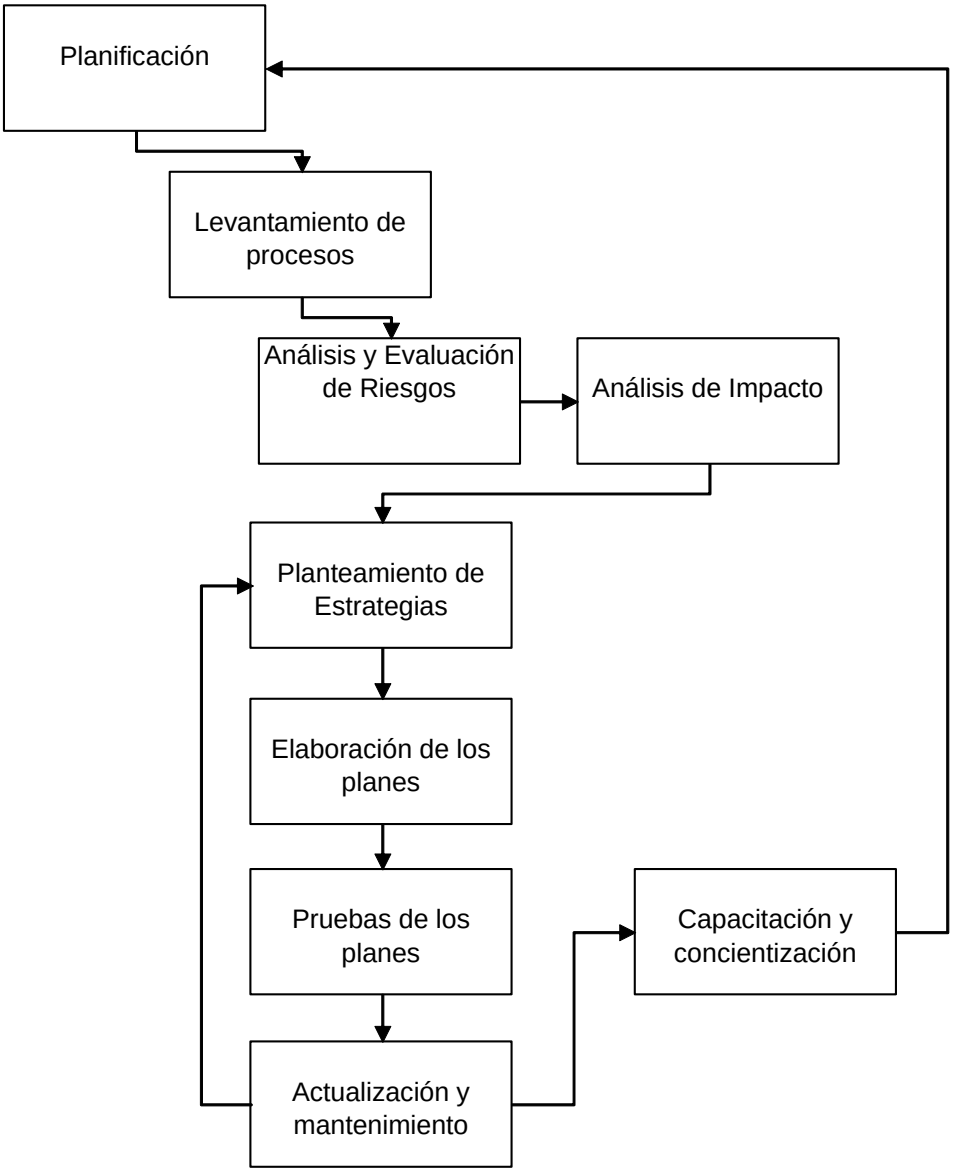
- La base para construir un buen plan radica en la organización apropiada de las diferentes etapas del plan, contar con recursos capacitados o asesoría que facilite su comprensión y aplicación es vital.

- Los componentes básicos que deben ser parte del plan se refieren principalmente a cuatro etapas: planear, hacer, monitorear y mejorar, siendo lo más importante la etapa de planificación puesto que en ella se crea la política de continuidad del negocio, se determinan los procesos críticos para la continuidad es decir aquellos que no deben dejar de operar en caso de eventos de contingencia, se efectúa el análisis de riesgos e impacto, se establecen las estrategias que se adoptarán en cada caso, se establece la metodología para documentar el plan, se elabora el plan

de capacitación y concientización del personal así como el de comunicación.

Si se puede resumir todo lo mencionado en un solo gráfico sería como el que se muestra a continuación:

CONTINUIDAD DEL NEGOCIO



Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

Partiendo de una apropiada planificación se establecen el resto de fases para construir el plan en el siguiente orden: levantamiento de procesos, su evaluación de riesgos e impacto para el negocio, planteamiento de estrategias y documentación de planes, pruebas, capacitación, ajustes y mantenimiento.

4.1.5 Pruebas del plan.

Entendiendo que el plan de continuidad es un proyecto institucional es preciso establecer una compañía de sensibilización a los responsables de las diferentes áreas, e implantar mecanismos de seguimiento para informar los resultados conseguidos, cuando el plan haya sido desarrollado e implementado y posteriormente, cada vez que se hagan pruebas.

Adicional a esta campaña de informar, también se debe incluir el entrenamiento de los equipos de recuperación de cada área y mantener el manual actualizado para que refleje la realidad de la Institución a lo largo del tiempo y las circunstancias que la rodean.

Las mejores prácticas y experiencia de algunos organismos muestran que los programas de entrenamiento y pruebas periódicas son muy valiosos para conseguir el éxito en la recuperación eficaz. Los programas de pruebas y entrenamiento son también la forma más sencilla de mantener actualizados los planes en un nivel apropiado.

Se pueden fijar algunos objetivos en esta fase del plan de continuidad como los siguientes:

- Planificar como será actualizado el plan, y como conseguir que el personal este preparado en todo momento para poder aplicarlo de forma correcta.

- Establecer un programa de mantenimiento del plan que debe contar con tres elementos: Revisiones periódicas, Ejercicios de entrenamiento y Pruebas.
- Instituir una programación anual para la ejecución de los elementos citados en el punto anterior.
- Determinar responsables de actualizar el plan, dependiendo de los resultados de las pruebas.

Revisiones periódicas

Las revisiones periódicas tienen como objetivo cubrir algunos aspectos sobre el plan, entre los que podemos mencionar los siguientes:

- Comprobar si se encuentran disponibles los recursos que se emplearán en el plan de recuperación, incluyendo las copias de información que se mantienen por seguridad en el sitio de almacenamiento externo.
- Evaluar si procesos críticos definidos como tal, incluyendo los umbrales de tiempo son todavía los apropiados para la Institución.
- Determinar si la criticidad sobre la información se mantiene vigente e incluir aquella que pudo haber sufrido cambios y que actualmente es esencial para la operación de la Institución.

Ejercicios de entrenamiento

Es recomendable efectuar un ejercicio anualmente, con la participación de todo el personal que compone cada equipo de recuperación incluyendo a los backups o suplentes. El objetivo principal es que se familiaricen con las estrategias y procedimientos que forman parte del plan.

El programa de entrenamiento deberá contar con los siguientes componentes:

- Detalle de objetivos y componentes del programa de entrenamiento.

- Identificación de las necesidades o alcance del entrenamiento.
- Metodología clara que se empleará en el entrenamiento para que sea de fácil comprensión y aplicación.
- Componentes o insumos que servirán para efectuar el entrenamiento.
- Identificación de las oportunidades de entrenamiento externo.
- Realización de ejercicios de manera periódica.

Pruebas

El buen funcionamiento del plan depende en gran medida del buen funcionamiento de la tecnología, se recomienda aplicar una prueba anual de los componentes tecnológicos y logísticos, que permitan asegurar la aplicación del plan definido, y hacer ajustes de acuerdo a los resultados de las pruebas.

El plan de pruebas deberá contar con los siguientes elementos:

- Planificación de la prueba a realizar.
- Definición del alcance que tendrá la prueba.
- Coordinación de la prueba con todas las áreas involucradas en la misma.
- Ejecución de la prueba.
- Evaluación de los resultados.
- Documentación de los resultados.
- Actualización del plan en función de los resultados.
- Generación del informe o informes para entregar a la alta gerencia.

Se espera que conforme se lleven a cabo las pruebas vayan creciendo en su alcance, para que se cubran la mayoría o todos los aspectos o procesos críticos de la organización.

En el proceso de pruebas cobra vital importancia la planificación del esquema a seguir, por ello es importante considerar algunas actividades recomendadas:

- **Establecer un programa de pruebas:** se debe determinar un esquema que tenga un enfoque lógico y estructurado, desarrollando una estrategia que no ponga en peligro la operación normal de la organización, que sea práctica, asegurando que existan los recursos apropiados, sin exceder el costo previsto y que brinde confianza en los resultados para que se pueda considerar como valor agregado.

- **Determinar las necesidades de las pruebas**: es importante fijar los objetivos y niveles de éxito esperados, identificar los tipos de pruebas incluyendo sus ventajas y desventajas: simulaciones y ejercicios, pruebas modulares, pruebas funcionales, pruebas anunciadas, pruebas sorpresa. Además es fundamental establecer y documentar el alcance, periodicidad y logística necesarios para efectuar las pruebas.

- **Desarrollar escenarios reales:** es importante crear escenarios similares a los incidentes más probables y a los problemas asociados con ellos. Entrenar a los equipos que intervienen en las pruebas.

- **Establecer criterios de evaluación y de las pruebas y documentación de los resultados:** se deben establecer los tipos de criterios para las pruebas como: observación, documentación, evaluación de resultados obtenidos frente a resultados esperados, necesidad de actualización del plan.

- **Definir un plan de controles e informes:** es importante especificar un plan de controles de las pruebas así como un método para informar los resultados a la Gerencia.

- **Evaluar los resultados de la prueba y actualizar el plan en función de los mismos:** se deben documentar los resultados así como los ajustes que deberán ser aplicados en el plan, con el fin de mantenerlo para que se ajuste a la realidad del negocio frente a los escenarios de fallo planteados como alcance de la prueba.

- **Auditar la estructura y contenido del plan:** un aspecto de apoyo fundamental para la alta Gerencia es contar con un plan definido para efectuar auditorias a los planes y estrategias implementadas. Es un valor agregado que permitirá rectificar o ratificar algunas decisiones.

Fuente1: Superintendencia de Bancos y Seguros
Fuente2: Artículos del Internet página www.isec-global.com
Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría

COMENTARIO:

Las pruebas constituyen el termómetro ideal para validar la aplicabilidad de los planes y permiten mejorar permanentemente su calidad.

Existen varios tipos de pruebas que se pueden aplicar y que van desde su revisión en la documentación (prueba de escritorio), hasta simulacros de operaciones u oficinas completas. Todo dependerá de los objetivos que se planteen, el alcance que se les quiera dar.

Un factor fundamental para que una prueba sea exitosa es su planificación, si no existe una buena planeación es casi seguro que la prueba será un fracaso.

Por esto es importante tomarse el tiempo necesario que cubra un gran porcentaje de aspectos que muchas veces pueden resultar desapercibidos, pero que en el momento de la prueba pueden generar problemas.

Se debe prever: el personal que intervendrá, logística, movilización, contactos actualizados, refrigerio, tareas con tiempos establecidos, charlas previas explicando el alcance de la prueba, responsabilidades de los participantes, hora planificada de término de la prueba, entre otras cosas.

En el caso de pruebas de transacciones o procesos automatizados no olvidarse de coordinar con los proveedores externos como: comunicaciones, cajeros automáticos, etc. dependiendo del alcance de la prueba pudiera ser necesario que asistan o que estén en stand by.

De preferencia se deben ejecutar pruebas parciales, sobre todo cuando se trata de los sitios alternos de procesamiento, analizar los riesgos que implica el alcance definido para la prueba.

Se puede tomar como base la prueba anterior y procurar ampliar el objetivo para que en un momento determinado se haya cubierto el cien por ciento de procesos críticos.

La documentación de las pruebas es otro aspecto muy importante para la organización, debe estar estructurada y respaldada para evitar que se pierda.

Otro tema que muchas veces es descuidado en este proceso es la comunicación interna y el plan de contactos. Es fundamental que se encuentren actualizados todo el tiempo. Siempre hay que recordar que los protagonistas o responsables de la ejecución de las pruebas son los funcionarios por lo que los riesgos asociados al factor personas pueden influir en el éxito o fracaso de las pruebas.

En todo momento el Comité de Continuidad y el Comité de Riesgos Integrales deben estar informados y deben autorizar la ejecución del plan de pruebas presentado, recordemos que este proceso debe formar parte de las

estrategias que tiene el Banco, no limitarse únicamente a cumplir con la norma.

4.1.6 El proceso de contingencias y la administración integral de riesgos.

COMENTARIO:

La gestión de continuidad del negocio constituye el complemento del marco de gestión de riesgos instituido en la organización.

La administración integral de riesgos y planes de contingencia y continuidad, busca administrar todos los riesgos en los procesos identificados como críticos para la Institución, y establecer niveles de eficacia de los planes de contingencia establecidos. El proceso de continuidad precisamente busca medir que tan efectivas son las estrategias adoptadas, que tipo de ajustes se deben hacer a los planes y por supuesto la concienciación de toda la Institución sobre las consecuencias que resultan de los riesgos administrados.

Al centrarse en el impacto de la interrupción o fallas, la gestión de la continuidad permite identificar los servicios o procesos críticos, es decir aquellos con los que la organización no podría seguir funcionando, contribuyendo con el diagnóstico de necesidades y estrategias que deben aplicarse con el fin de evitar que algunas amenazas se conviertan en hechos.

Hay que considerar las innumerables oportunidades y ventajas que tiene una Institución al contar con planes que complementen la administración de riesgos integrales, y proporcionen a la alta Gerencia una visión completa de la realidad por la que está atravesando la organización, así como le permite tomar decisiones con mayores elementos frente a asumir, minimizar, trasladar o evitar los riesgos.

4.2 La función de contingencias y continuidad como una tarea continua que retroalimenta a otras funciones relacionadas con el riesgo operacional

La Gestión de la continuidad es un elemento muy importante para el buen manejo de la organización, la administración tiene responsabilidad sobre los servicios y productos que provee a sus clientes, así como para el cumplimiento de obligaciones contractuales con proveedores, terceros, funcionarios, etc.

Considerando que todos los procesos de negocio están sujetos a fallos o interrupciones, disponer de planes debidamente estructurados para reaccionar frente a las contingencias operativas, protegiendo el bienestar y la seguridad.

En la actualidad y dada la normativa vigente, la gestión de la continuidad del negocio no debe ser vista como un gasto sino como una inversión que agrega muchas ventajas para la organización.

Las personas encargadas de la implementación y el mantenimiento del programa de continuidad del negocio pueden pertenecer a diversas áreas de la organización, dependiendo del tamaño y complejidad de sus procesos.

Dentro del proyecto existen actividades que deben llevarse a cabo tanto en el inicio como de manera continua, entre las que mencionamos las siguientes:

- Definición de alcance, funciones y responsabilidades de la gestión de continuidad del negocio.
- Designar a un responsable o equipo de gestión de la continuidad del negocio.
- Mantener vigente el programa de continuidad del negocio a través de la práctica más adecuada.
- Concientizar, promover, difundir los planes de continuidad del negocio en todos los ámbitos de la organización y más allá.
- Efectuar y documentar debidamente los resultados de pruebas y simulacros de los planes de continuidad del negocio.

- Coordinar la evaluación y actualización regular de las evaluaciones de riesgo y análisis de impacto del negocio.
- Monitorear el desempeño de la capacidad de la continuidad del negocio a través del registro histórico de los incidentes, así como de los resultados de las pruebas de los planes.
- Administrar los costos asociados con la capacidad de la continuidad del negocio.

Como hemos mencionado, las personas asignadas al mantenimiento de la continuidad del negocio deberán crear y mantener la documentación relacionada que debería incluir al menos lo siguiente:

- Políticas de continuidad del negocio.
- Análisis de impacto del negocio.
- Evaluación de riesgos.
- Análisis de impacto del negocio.
- Estrategias de continuidad.
- Programa de capacitación y concientización.
- Planes de gestión de incidentes.
- Planes de continuidad.
- Planes de recuperación.
- Acuerdos y contratos de niveles de servicio.
- Cronogramas e informes de pruebas.

El mantenimiento del proceso de continuidad del negocio debe ser distribuido al personal clave, en el momento en que se haya corregido o actualizado algún documento dentro de un proceso formal de control de cambios que asegure disponer de información actualizada en todo momento.

Al ser un proceso continuo, es importante efectuar auto evaluaciones de los planes y estrategias y someter a los nuevos servicios o productos a un análisis de riesgos e impacto que permita establecer si se trata de un proceso crítico que debe ser incluido como parte de los planes.

Las evaluaciones pueden tomar la forma de auditorías internas, externas o autoevaluaciones. Su frecuencia puede estar incluida en la política de continuidad, así como puede ser influida por leyes o reglamentos emitidos por organismos de control, también pueden estar basadas en las necesidades propias de la organización.

Como parte de los aspectos que deben considerarse dentro de estas evaluaciones están:

- Revisar el proceso de identificación de procesos críticos, productos y servicios clave, estableciendo si están acorde con los objetivos estratégicos de la Institución.
- Evaluar las políticas, estrategias, estructura y planes de continuidad del negocio, estableciendo si son suficientes y reflejan las prioridades y necesidades de la organización.
- Revisar la competencia y capacidad de la gestión de continuidad estableciendo su eficacia.
- Establecer si los programas de prácticas y mantenimiento de la gestión de continuidad del negocio han sido implementados de manera eficaz.
- Determinar si se aplican los programas de capacitación al personal de manera continua.
- Evaluar el nivel de conocimiento y concientización que tiene el personal sobre sus funciones y responsabilidades frente a la gestión de la continuidad del negocio.
- Determinar si existe y es eficiente el programa de control de cambios que asegura el mantenimiento de la documentación y planes actualizado.

Si la decisión es realizar una auditoría independiente, debe ser realizada por personas calificadas, que identifiquen puntos débiles reales y potenciales, aspectos de mejora en las diferentes fases del proyecto.

Si se trata de un proceso de autoevaluación, debe buscarse la verificación cualitativa de la capacidad de la organización para recuperarse de un incidente. Este proceso debería realizarse tomando como marco de referencia los objetivos

de la organización, buenas prácticas y estándares de internacionales así como el marco legal vigente.

En cualquier caso se deberá contar con el apoyo de la alta gerencia y la colaboración de todo el personal involucrado en el proceso, de tal manera que esta revisión contribuya con mejoras que permitan tener mayor eficiencia en la gestión de la continuidad del negocio, y efectuar los ajustes que sean necesarios a los planes vigentes.

Fuente1: Superintendencia de Bancos y Seguros
Fuente2: Artículos del Internet página www.isec-global.com
Fuente3: Presentaciones entregadas en cd en el 3er Congreso Nacional de Auditoría

COMENTARIO:

Como hemos mencionado en todo este capítulo y en anteriores, contar con planes de continuidad del negocio y una adecuada administración de los mismos es un proceso de carácter permanente, al existir cambios en los procesos, cambian los riesgos asociados y aquellos procesos que no fueron catalogados como críticos cambian y se vuelven imprescindibles para la organización.

El personal encargado de dar mantenimiento a los planes debería incorporar dentro de sus funciones estas tareas ya que debe existir la responsabilidad aceptada de manera expresa.

Preferible si se cuenta con un sitio de almacenamiento de los planes que tenga seguridades suficientes que permitan disponer de la información en el momento oportuno, estén protegidos los documentos y que se controlen las actualizaciones que se realizan para un control más efectivo.

Auditoría Interna tiene dentro de sus responsabilidades dar seguimiento a la documentación apropiada de los planes, su custodia y administración.

Otro aspecto importante que debe ser de carácter permanente es la capacitación al personal de toda la organización.

CAPÍTULO V INTERRELACIÓN DEL RIESGO OPERACIONAL CON LOS DEMÁS RIESGOS

Las normas de Basilea II están claramente enfocadas hacia los tres pilares. El primero abarca los requerimientos mínimos de capital, donde las instituciones deben hacer el gran esfuerzo por implementar modelos que permitan identificar adecuadamente sus riesgos y ponderarlos para establecer sus requerimientos mínimos de capital.

A continuación un breve análisis de estos riesgos.

5.1 Riesgo de crédito

Tal como se indica en el acuerdo de Basilea II, uno de los principales objetivos es alinear los requerimientos de carácter regulatorio con aquellos principios económico/financieros de gestión de riesgos.

El nuevo acuerdo no sólo perfecciona aspectos considerados en Basilea I, sino que también incorpora nuevos elementos a ser tomados en cuenta, basándose en tres pilares que se refuerzan mutuamente: requerimientos de capital, acción de los organismos supervisores y disciplina del mercado.

En lo que respecta al riesgo de crédito, el acuerdo propone tres alternativas para su determinación. El primero de ellos, en su mecánica, es similar a lo establecido en Basilea I (ponderación preestablecida según riesgo para los distintos tipos de activos), pero presenta mejoras que lo hace más sensible al riesgo e incorpora el uso de clasificaciones externas efectuadas por agencias especializadas. Los otros dos métodos (no consideradas en Basilea I) se basan en mediciones internas realizadas por los propios bancos.
La medición del riesgo de crédito, se pueden adoptar diferentes sistemas de evaluación, inclusive aplicando métodos propios de la Institución. La aprobación de los modelos internos por parte de las Entidades Reguladores se basa en la evaluación del enfoque de la Institución, de su cultura, estructura e implementación del gobierno corporativo.

Los reguladores además, deben analizar el rol de supervisión y control que ejerce la Junta Directiva, Presidencia Ejecutiva y demás personal administrativo dentro del proceso operativo de crédito.

Por su parte, el riesgo operativo está relacionado con las necesidades de capital como consecuencia de las eventuales pérdidas derivadas de deficiencias en los procesos o sistemas de las instituciones.

Conforme avanza la tecnología y los procesos mundiales globalizados, el riesgo de procesamiento manual o automático también va generalizándose, el crecimiento de los canales empleados para efectuar las transacciones bancarias, incremento en e-commerce, fusiones, nuevos servicios, etc. son circunstancias que demandan la implementación de niveles de control apropiados, basados en una evaluación de riesgos que se combinan entre los diferentes tipos: de crédito, mercado y liquidez, reputacional.

Cada proceso analizado de manera integral, combina en algún momento alguno de los riesgos o todos, es importante contar con procedimientos de actualización permanente, que permitan asegurar periódicamente la efectividad de los controles aplicados en todas las instancias, así como también contar con el mapa de riesgos actualizado. Este es un valor agregado para la administración de la Empresa, que le permitirá tomar decisiones oportunas sobre cambios o innovaciones en los negocios.

Otro aspecto importante para el éxito de la administración de riesgos, es fomentar la cultura de riesgo en la Institución, que se conozcan las políticas para el manejo de riesgos de crédito, se profundicen aquellos conceptos básicos que permitan que cada funcionario independiente del área en donde trabaje contribuya a mantener un entorno adecuado de control interno, esta es una responsabilidad de todos los integrantes de la Institución.

Frente a todo esto sigue latente la gran pregunta si Basilea II y sus conceptos serán capaces de prevenir la crisis o de empeorarla?

Esta es la interrogante que un sinnúmero de analistas económicos y financieros tratan de explicar desde diferentes perspectivas, más aún considerando que la principal fuente de fallas en controles se registró en el sector hipotecario.

Algunos analistas o administradores en general creen necesario endurecer las medidas de control, considerando que fue evidente que no se registraron los debidos controles ni supervisión por parte de los Entes Reguladores. Otros ven la implementación de Basilea II como un factor determinante que mejorará el control y sobre todo precautelará de mejor manera el capital de los clientes en sus diversas modalidades, y de las propias Instituciones Financieras.

Dentro del comportamiento de la economía, cuando se registra estabilidad, se puede distinguir un incremento del negocio aún en aquellos bancos mal administrados que tienen niveles inadecuados de capital y provisiones, pero cuando la economía empeora, esos bancos tienen que modificar sus políticas crediticias para evitar la quiebra.

Durante esta época de crisis se pueden dar situaciones que beneficien a algunas Instituciones así como otras que vayan en su contra, dependerá de otro sector de la economía relacionado con la productividad y crecimiento de la industria. Por ejemplo en tiempos favorables el riesgo crediticio medido según la probabilidad de incumplimiento sería bajo, así como lo serían los requisitos de capital; a la inversa, en tiempos difíciles los bancos enfrentarían necesidades de capitalización mucho mayores, lo que podría tener un efecto no deseado en la economía si los bancos sufrieran limitaciones de capital y se vieran forzados a reducir sus préstamos cuando más se los necesita.

Es una realidad que mientras exista una caída de la economía o una recesión, a los bancos se les hace más difícil aumentar su capital porque sus utilidades y, por ende, su capacidad de acumular reservas disminuyen. También pueden tener más dificultad para aumentar el capital y emitir deuda subordinada debido a la mayor incertidumbre. La combinación de requisitos de capital más elevados (debido al mayor riesgo) y la dificultad de captar capital nuevo podrían llevar a las instituciones a reducir el crédito a las empresas y a los hogares, agravando la recesión o impidiendo la recuperación económica.

En cualquier modo, muchos analistas coinciden en que no existe la certeza absoluta que Basilea II pueda solucionar estos inconvenientes por los que están siendo afectados los bancos y la economía en general, pero sin duda alguna contribuirá a mejorar el nivel de control en las Instituciones Financieras y fomentará la precaución ante posibles niveles de crisis a través de las reservas que se requieren.

COMENTARIO:

El riesgo de crédito ha sido tradicionalmente considerado el más importante de los riesgos bancarios, ya que una parte muy significativa de los ingresos de las instituciones financieras se basa en la gestión crediticia. En tal sentido, las normas que rigen este riesgo han sido permanentemente fortalecidas con modelos cada vez más sofisticados. Actualmente este riesgo ya no se lo ve únicamente enfocado a un cliente específico, sino que intervienen evaluaciones permanentes del sector o industria, situación macro y macroeconómica del país, evaluación de la concentración de crédito, entre otros. Actualmente ya ni siquiera existe posibilidad de créditos vinculados, que en el pasado fueron causa de la crisis de algunos bancos, por cuanto se abusó de ellos y no se dieron garantías adecuadas.

En el Ecuador a raíz del cambio de la Ley de Bancos por la Ley de Instituciones Financieras, se desregularizó el control a la Banca, con el fundamento del “autocontrol”. Esto llevó a una grave crisis que fue totalmente evidente a fines del año 1998 y que en marzo de 1999 concluyó con el famoso feriado bancario que afectó al país entero, pues no tuvo precedentes. El gobierno decretó que durante una semana no se atendiera al público y durante ese tiempo se congelaron las cuentas. Luego vino como consecuencia la dolarización, se emitieron decretos para desagiar los créditos (establecer nuevas tasas dolarizadas para los créditos que habían sido emitidos en otras monedas y a tasas sumamente elevadas), hubo posteriormente un redesagio.

Finalmente, en una economía dolarizada que sin ser una panacea, se logró una estabilidad y las tasas fueron bajando. Obviamente, debido al riesgo país que tenemos, nuestras tasas nunca van a acercarse a las tasas que el país emisor del dólar, Estados Unidos, maneja. Esto se debe a un sinnúmero de causas que no son objeto de este estudio.

Una vez dolarizados, tanto la legislación ecuatoriana, a través de la emisión de las leyes Trole I y II como la Superintendencia de Bancos, a través de diferentes resoluciones, ha venido implementando normas de control que van en línea con las directrices de Basilea II.

El sistema financiero ha tenido una fuerte evolución en las últimas décadas. Por un lado, los márgenes se reducen cada vez más. Por otro lado, el cliente cuenta con nuevas opciones de financiamiento a través de los Mercados de Capital, donde a través de titularizaciones, emisiones de obligaciones, y otros mecanismos, puede obtener financiamiento a tasas inferiores. Obviamente quienes se ven más favorecidos, son las grandes empresas, que pueden recurrir a este tipo de financiamiento.

En el Ecuador, hasta el año 2006 también existía el financiamiento externo, a tasas sumamente más bajas, puesto que los bancos del exterior tenían costos inferiores y no tenían los impuestos que aquí se manejaban. Esto cambió radicalmente a raíz del 2007, ya que se generaron una serie de impuestos como el Impuesto a la Salida de Divisas (ISD), y otras limitaciones como que las empresas no puedan deducir los gastos de financiamiento si provienen de países catalogados como paraísos fiscales.

Por otro lado, el control de tasas que realiza el Banco Central, no permite a los bancos fijarlas libremente, sino que este organismo establece un techo que con cierta frecuencia es evaluado y ajustado.

Finalmente, entre otros de los aspectos que influyen fuertemente en este tema, está la crisis mundial, que tiene incidencia en nuestra economía, entre otros aspectos, debido a que los productores nacionales disminuyen su producción por la demanda decreciente en los mercados mundiales y locales.

Todos estos cambios que hemos comentado brevemente, han marcado entornos diferentes en la situación de la Banca ecuatoriana.

Por tanto el riesgo crediticio es uno de los que más preocupan a las instituciones, ya que una deficiente gestión del mismo puede provocar graves problemas a la entidad, generando

incluso problemas a nivel del país. De existir estas condiciones, hay la posibilidad de un riesgo sistémico, es decir, que se vea afectado el sistema financiero del país.

Por tal motivo, las instituciones financieras han desarrollado modelos para gestionar el riesgo crediticio, dotando de un capital que asegure la continuidad del negocio. El Acuerdo de Basilea da mucha importancia a los modelos que cada entidad desarrolle, basado en técnicas estadísticas que permiten identificar la probabilidad de no pago como variable fundamental.

Las instituciones financieras están enfocadas también al riesgo de liquidez, lo que ha generado que se produzcan titularizaciones de sus carteras, con lo cual se traslada el riesgo.

No pretendemos profundizar en este análisis, sin embargo anotamos que existen dos tipos de riesgos:

- Diversificable: que por ser específico, se puede mitigar mediante la desconcentración, es decir, los bancos deben establecer mercados objetivos que permitan que sus créditos vayan a diferentes sectores, diferentes clientes, diferentes regiones, etc. La diversificación de la cartera permite mitigar este riesgo.

- Sistémico: este riesgo no permite la diversificación, pues depende de las tendencias del mercado. Es cuando por ejemplo un país, una región, o el mundo entero tiene una crisis, que inevitablemente afecta a todo el sistema. La tasa que se establezca debe cubrir el rendimiento libre de riesgo más una prima que cubra los riesgos sistémicos.

Para cubrir los dos riesgos, existen modelos, como el de Sharpe, que considera el riesgo de la cartera, el coeficiente de volatilidad, el riesgo total de mercado y el riesgo específico del activo. Como este hay otros modelos, como el CAPM que permiten medir el riesgo, Cada banco debe establecer la metodología que más le convenga y monitorear permanentemente su evolución para tomar las medidas adecuadas.

En definitiva, el riesgo crediticio debe reflejarse en provisiones y patrimonio técnico de la institución para preservar el dinero de los depositantes.

5.2 Riesgo de Mercado y Liquidez

La crisis económica y financiera mundial, que inició a mediados del 2007 y se acentuó o se hizo más explícita en el 2008 a nivel mundial, especialmente en Estados Unidos y en la Unión Europea, ha generado importantes pérdidas a los bancos, especialmente aquellos con presencia internacional, así como una crisis de liquidez en los mercados interbancarios. Esto se evidencia en caídas bursátiles repentinas, alta volatilidad y desaceleración del crecimiento de la economía.

El origen de esta crisis está en la falta de control, regulación y supervisión financiera, especialmente en Estados Unidos, donde los grandes bancos abusaron de las figuras de transmisión del riesgo de crédito a terceros mediante la contratación de seguros y la titularización de la cartera, colocando crédito hipotecario otorgado a clientes sin un análisis de capacidad de pago, generando la famosa “burbuja financiera”, que para evitar que los organismos de control pudieran impedirlo, se manejaron en bancos off shore ubicados en los famosos paraísos fiscales. De esta manera, podían recontratar seguros en varios niveles, generando liquidez que en realidad no estaba respaldada por garantías reales.

Esto generó también riesgo de mercado, por lo que como podemos ver, la situación se complicó y abarcó realmente riesgo de crédito, de mercado y liquidez.

En definitiva, el origen de esta crisis se resume en lo siguiente:

- Otorgar crédito a clientes sin cumplir las normas mínimas de: tener fuente de pago para financiar la compra, con miras a que las propiedades cada vez subían de precio y era suficiente con tenerlas hipotecadas. Esto a la final no resultó, en primer lugar por la falta de una fuente de ingresos del deudor, y en segundo lugar, por la titularización “en cadena”, que hizo que las propiedades no fueran suficientes para cubrir los “hedge funds” que los garantizaban, sumados a la gran caída del precio de los bienes hipotecarios.

- Se incrementaron las facilidades de financiamiento, con cuotas iniciales bajas o inclusive nulas, incluyendo flexibilidades como pagar solamente intereses durante un período, inclusive ajustando periódicamente de acuerdo a la capacidad del deudor.

- Financiamiento de casi el 100% del bien que se adquiría.

- Utilización laxa del modelo de credit score (modelo que realiza una evaluación de la capacidad crediticia del cliente en base a parámetros preestablecidos), a fin de facilitar la concesión de préstamos.

A todo esto hay que sumar que las calificadoras de riesgo calificaron como AAA los productos estructurados que se generaron de esta manera, lo cual ha generado desconfianza de las calificadoras de riesgo.

Todos estos hechos han levantado cuestionamientos respecto al planteamiento teórico del Nuevo Acuerdo de Capital, es decir Basilea II. Es necesario aceptar que existe una nueva ingeniería financiera, que debe ser analizada con mayor profundidad.

Por tanto al momento resulta sumamente difícil analizar y determinar si los métodos de validación son suficientes para prevenir este tipo de riesgos.

La calificación que otorgan las calificadoras de riesgo a un banco o a una empresa se obtiene como resultado de un complejo proceso que cuenta con diferentes herramientas, entre las que se encuentran reuniones con el personal directivo del Banco, análisis de los estados financieros, información interna, evaluación del Gobierno Corporativo, comunicación remitida y recibida del Organismo de Control (Superintendencia de Bancos), y aplica mucho criterio por parte del evaluador, por lo que existen elementos subjetivos. Basilea busca sustituir estos elementos por métodos y modelos objetivos en base a estadística.

Todavía falta mucho camino por recorrer, pero los modelos y métodos están en constante evolución. Deben considerarse estimaciones externas e internas,

probabilidades de incumplimiento, lo cual complica el modelo porque no son medidas fáciles de obtener. En definitiva, debe establecerse un modelo “predictivo”.

Como complemento, la supervisión bancaria debe realizarse comparando las tasas de incumplimiento reales con las probabilidades de incumplimiento estimados para el sistema. El Ente de Control tiene una gran tarea para tecnificar sus métodos, su personal y sus sistemas para poder realizar un adecuado control.

Sin embargo, queda mucho por decir. Esta grave crisis ha provocado estudios de diferentes entidades, y el BIC no se queda atrás.

COMENTARIO:

El riesgo de mercado se mide en el riesgo del tipo de interés, precio, inflación, tipo de cambio.

El tipo de interés está directamente afectado por la sensibilidad del precio de mercado ante los cambios en el tipo de interés. Existen diferentes formas de evaluar este riesgo, entre ellos la duración, la duración modificada.

El riesgo de precio: que refleja la variación en los precios de los activos financieros.

Riesgo de inflación: incertidumbre que la existencia de la inflación provoca sobre la tasa de rendimiento real de la inversión.

Tipo de cambio: el riesgo de que variaciones en el tipo de cambio de divisas afecten al rendimiento de la inversión.

Por su parte, el riesgo de liquidez es la incapacidad de una entidad para cumplir cabalmente y de manera oportuna las obligaciones de pago, ya sea por insuficiencia de recursos líquidos o necesidad de asumir costos excesivos de fondeo. El efecto de esto es que el mercado lo perciba como inestable y genere pánico que provoque corrida de depósitos. En nuestro país, debido a la crisis de los años 1998 y 1999, este es un tema sumamente

sensible, que puede generar un pánico generalizado, por lo que este riesgo hay que manejarlo en forma muy delicada.

Las instituciones financieras tienen entre sus activos las inversiones, que son locales y en el exterior, a fin de diversificar el riesgo y poder contar en un momento dado con recursos locales o del exterior que pueden ser traídos en cuestión de horas para poder atender demandas inusuales y atender oportunamente las necesidades de los clientes.

La Superintendencia de Bancos ha emitido durante estos dos últimos años, y especialmente en el presente, regulaciones tendientes a que los bancos traigan sus inversiones al Ecuador para dinamizar la economía ecuatoriana. Para ello ha generado impuestos que deben ser pagados en caso de mantener estas inversiones fuera del país, y ha establecido porcentajes que debían repatriarse dentro de un cronograma. Esto sumado a la tasa de ISD que inició con un 0.5%, luego subió al 1% y en la actualidad hay un proyecto de ley para duplicarlo.

Complementariamente, ha creado un fondo de liquidez para atender las necesidades de las instituciones en caso de requerirlo.

En todo caso, el riesgo de liquidez debe ser controlado a través de un manejo técnico que permita a la institución tener una relación entre los plazos o maduración de las posiciones activas y pasivas de acuerdo a los vencimientos esperados, a fin de poder cubrir sus necesidades de liquidez adecuadamente.

Dentro de las normas de gestión y administración de riesgos, existen algunas específicas para el riesgo de liquidez, según la cual “se entiende por riesgo de liquidez, cuando la institución enfrenta una escasez de fondos para cumplir sus obligaciones, y que por ello, tiene la necesidad de conseguir recursos alternativos o vender activos en condiciones desfavorables, esto es, asumiendo un alto costo financiero o una elevada tasa de descuento, incurriendo en pérdidas de valorización”. Para prevenir este riesgo, la norma indica que la administración de la institución controlada debe asegurar razonables niveles de liquidez para atender eficientemente y bajo distintos escenarios alternativos, las obligaciones con el público y los otros pasivos de naturaleza financiera que contraiga, dentro del giro de su negocio. Responsabiliza al directorio emitir e implementar políticas y

procedimientos idóneos para administrar la liquidez, en base a la complejidad y volumen de las operaciones, considerando escenarios en que se responderá si las alternativas se convierten en realidad. También establece responsabilidades del Comité de Administración Integral de Riesgos, quien debe monitorear, establecer planes de contingencia para este riesgo, reportar al directorio y recomendar el ajuste a políticas, estrategias y procedimientos, establecer sistemas de control y medición de riesgo de liquidez, tanto en negocios individuales como consolidados. Todo esto debe ser formalizado a través de manuales de políticas y procedimientos que son periódicamente enviados a la Superintendencia de Bancos.

La norma indica que las instituciones deben contar con sistemas informáticos que permitan tener la información necesaria para tomar decisiones oportunas.

Establece una metodología para determinar la exposición al riesgo de liquidez, para lo cual indica que se debe realizar un análisis de maduración de los activos y pasivos, distribuyendo los saldos registrados en los estados financieros con cierre a la fecha de evaluación, de acuerdo a sus vencimientos, de acuerdo a los siguientes criterios:

1. Situación contractual corriente, donde se clasifican activos y pasivos por bandas según el plazo de vencimiento, ya sea total, parcial, o fechas de reprecio.

2. Recuperación esperada: vencimientos esperados de las cuentas que no tienen vencimiento contractual o a fecha cierta. Si las cuentas tienen vencimiento incierto, se realiza un análisis de tendencia y estacionalidad usan métodos estadísticos apropiados, como el de regresión múltiple, incorporando como variable explicativa al PIB y todas las variables que la institución considere pertinente, de acuerdo al mercado, con un nivel de confianza de al menos 99%. Para los pasivos sin fecha contractual de vencimiento, como depósitos a la vista, se realizan análisis técnicos que permitan estimar los retiros máximos probables que se puedan presentar por período, y la porción permanente. El Organismo de control puede fijar límites mínimos al porcentaje de retiros que se estimen en cada banda de tiempo.

3. Se utilizan bandas por mes, siendo las del primer mes más específicas, pues detalla a nivel de semanas.

4. Se incluyen los intereses y dividendos de las operaciones activas y pasivas registradas en el balance.

5. Se determinan las brechas de liquidez, en base a la diferencia entre el total de operaciones activas más el movimiento neto de cuentas patrimoniales respecto al total de operaciones pasivas, de acuerdo al formulario que analizaremos más adelante.

6. En el reporte de cuentas de activo y pasivo se consideran movimientos de efectivo que se esperan por el cumplimiento de obligaciones contingentes y movimiento de fondos por cumplimiento de productos derivados.

7. La brecha se calcula dentro de cada banda, a la vez que se calcula la brecha acumulada existente, dentro de cada período, de la siguiente manera:

   - Brecha de liquidez (n)= ACT (n) + PATR (n) – PAS (n)

   - Brecha acumulada de liquidez (n) = brecha de liquidez (n) + brecha acumulada de liquidez (n-1)

     Donde

     Brecha de liquidez (n) = Exceso o deficiencia de liquidez para la banda n

     ACA (n) = Activos que vencen en la banda

     PAS (n) = Pasivos que vencen en la banda n

     PATR (n) = Movimiento neto de patrimonio

N = n-ésima banda de tiempo y n=1,2,3,..,q;
donde q es el número de bandas

Si la brecha acumulada es negativa, debe calcularse la diferencia de su valor absoluto respecto a los activos líquidos netos. Si el monto resultante es positivo se denomina “liquidez en riesgo”.

Los activos líquidos netos (ALN) se definen como la sumatoria de

- Fondos disponibles.

- Fondos interbancarios netos y pactos de reventa menos pactos de recompra.

- Inversiones de libre disposición y que cumplan con los siguientes requisitos: en las sociedades constituidas en el Ecuador que tengan una calificación de riesgo no menor a “A”, emitida por una calificadora de riesgo calificada por la Superintendencia de Bancos y Seguros, en bancos operativos del ext3erior o sociedades constituidas en el exterior que tengan una calificación de riesgo dentro de la categoría de grado de invesión otorgada por FITCH IBCA – Duff & Phelps Credit Rating Co. Moody’s Investor Services o Standard & Poors Corporation.

Entonces:

Liq R = ([brecha acumulada de liquidez (n) < 0] – ALN) > 0

Donde:

Liq.R = liquidez en riesgo

[] = valor absoluto

ALN = fondos disponibles + fondos interbancarios netos + pactos de reventa – pactos de recompra + inversiones negociables

N = n-ésima banda de tiempo y n=1,2,3…,q donde q es número de bandas

Se determinan límites de riesgo:

1. No podrá presentar una posición de “liquidez en riesgo” a 7 o 15 días. Si ocurre, se somete a supervisión in situ, para determinar conveniencia de someterse a programa de regularización.

2. Si mantiene posición de “liquidez en riesgo” para la banda de 90 días, en el siguiente mes no puede incurrir en dicha posición de riesgo a 90 días o menos.

3. Si mantiene posición de “liquidez en riesgo” para la banda de 60 días, en el siguiente mes no podrá incurrir en posición de “liquidez en riesgo” a 60 días o menos.

4. Si mantiene una posición de “liquidez en riesgo” para la banda de 30 días, en el siguiente mes no podrá volver a incurrir en posición de “liquidez en riesgo” a dicho plazo.

5. No podrá presentar una posición de “liquidez en riesgo” a 90 días en cuatro meses, consecutivos o no, durante un mismo ejercicio económico.

6. No podrá presentar posición de “liquidez en riesgo” a 60 días en tres meses, consecutivos o no, durante un mismo ejercicio económico, y

7. No podrá presentar una posición de “liquidez en riesgo” a 30 días en dos meses, consecutivos o no, durante un mismo ejercicio económico.

Si se incumplen las disposiciones, la institución entra al proceso de supervisión in situ para determinar la consecuencia de someterse a un programa de regularización.

Si mantiene una posición de “liquidez en riesgo” mayor a 90 días, la Superintendencia podrá someter a la institución controlada a un programa de regularización u otro de vigilancia preventiva de acuerdo a los criterios que se establezcan en la “Guía de supervisión extra-situ”, así como en los manuales de inspección.

Si la institución mantiene una posición de “liquidez en riesgo” en cualquiera de las bandas temporales, debe presentar a la Superintendencia de Bancos dentro del plazo que ésta establezca, un plan de contingencia que contemple medidas concretas y factibles de ser puestas en práctica que le permitan superar tal situación.

En los anexos 4 y 5 se muestran reportes del índice estructural de liquidez de un banco y de una cooperativa, que ejemplifican lo expuesto referente al riesgo de liquidez.

Como podemos observar, la norma establecida por la Superintendencia de Bancos permite controlar en forma técnica que la liquidez de una institución se maneje adecuadamente, detectando posibles brechas en forma oportuna. Esta norma establece claras responsabilidades a nivel del Directorio y Unidad de Riesgos para que establezcan normas y políticas claras, monitoreen en forma efectiva, determinen escenarios diferentes y realicen pruebas al menos con cierta frecuencia, con lo cual las instituciones deben tomar las medidas oportunas para prevenir este riesgo.

La norma establece claramente las cuentas que se aplican para el cálculo de liquidez, que en definitiva consiste en determinar que las necesidades de liquidez en x período de tiempo no tengan inconveniente en ejecutarse, asegurando que lo que tengo que cubrir (pasivos, patrimonio) tenga una fuente de recuperación adecuada en períodos similares. Esto es en términos comunes lo que pretende controlar la norma.

Las instituciones que aplican esta y otras normas de prudencia en el manejo de los recursos de los depositantes, permiten que sea el mismo público quien catalogue a las mismas y les brinde su confianza. Sin embargo, en nuestro país, pese a las graves consecuencias de lo ocurrido en la crisis de fines de los 90, así como las dolorosas escenas que miramos cuando la gente “invierte” con personas o empresas que captan dinero en forma ilegal, el nivel de conciencia sobre el tema de liquidez en el público en general es todavía bajo.

Esta norma es una herramienta poderosa para que el Organismo de Control determine en forma temprana indicios de posible riesgo de liquidez de las Instituciones, ya que cuentan en forma permanente con información que puede ser verificada en cualquier momento, por lo que no deberían en teoría presentarse nuevos casos, ya que si este organismo interviene en forma oportuna y toma medidas adecuadas, se previene que las instituciones caigan.

Los bancos deben desarrollar pruebas de stress que permitan identificar posibles problemas que podrían presentarse en caso de períodos de fuerte demanda de liquidez y cómo se cubriría esa situación.

Es por eso que los bancos nacionales muchas veces no pueden ofrecer créditos a largo plazo, pues normalmente las inversiones de los clientes son a corto y en ocasiones a mediano plazo, pero no existe casi la inversión de clientes a largo plazo.

El riesgo de mercado y liquidez, por su naturaleza, son sumamente sensitivos. Si bien existen normas que los rigen, es necesario todavía establecer de mejor manera un mecanismo que permita evaluar integralmente los riesgos.

Basta el ejemplo que hemos tratado en este capítulo, de lo ocurrido en el escenario internacional, cuyo origen se da en créditos mal concedidos otorgado a clientes cuya capacidad de pago no tenía respaldo, con garantías sobrevaloradas que cuando se produjo la crisis deterioraron su valor en porcentajes sumamente elevados. Esto produjo una crisis tan grande (riesgo sistémico) que las casas, aunque bajaron de precio tan significativamente, no pueden ser comercializados. Por otro lado, las instituciones que garantizaban a través de los hedge funds las carteras que fueron titularizadas por los bancos no pudieron cubrir dichas garantías, generando una crisis de liquidez y de crédito por falta de recuperación que casi acaba con instituciones tan grandes como AIG (compañía de seguros más grande a nivel mundial), Citibank, Morgan Stanley, Bear Sterns, Lehman Brothers, Cerril Lynch, Goldman Sachs, J.P. Morgan, entre otras.

Si observamos estas grandes instituciones, podemos determinar que fueron: aseguradoras y bancos tradicionales y bancos de inversión. Pero la crisis no quedó allí, ya que los bancos europeos tenían también parte en esto y fueron severamente afectados.

Los gobiernos americano y europeos han tenido que inyectar sumas de dinero (a través de la máquina de hacer dinero llamada emisión) para salvar estas instituciones, lo cual se ve directamente reflejado en tasas de inflación. Aún no se sabe las consecuencias exactas de esta crisis, todavía no se sabe si se tocó fondo o vienen más sorpresas. Pero definitivamente, la nueva normativa debe ser a nivel extraterritorial, a fin de controlar más allá de sus fronteras.

Las nuevas normas requerirán acuerdos entre países para cubrir estos riesgos, y eso significa lograr consensos, que en la época actual se ven todavía difíciles. Pero para evitar nuevas crisis de alcances tan grandes, es necesario tener frentes comunes, de lo contrario estas crisis se repetirán.

5.3 Riesgo Reputacional

Basilea proporciona una importancia especial al tema de prevención de lavado de dinero y financiamiento del terrorismo, estableciendo estándares a nivel mundial, de manera que los negocios en cualquier lugar del mundo se sujeten a las mismas reglas. Para ello se basa en las convenciones y resoluciones de las Naciones Unidas.

Para ello norma que los bancos establezcan una metodología interna de medición y administración de riesgos, con criterios uniformes y estándares, y que las autoridades de supervisión establezcan una mayor vigilancia respecto a los sistemas de medición y administración de los riesgos que implementen los bancos. Respecto a la Disciplina de Mercado, sostiene que debe existir una mayor transparencia en las operaciones bancarias, teniendo mucho cuidado con la responsabilidad al suministrar información equivocada al mercado.

Basilea II proporciona orientaciones para la apertura de cuentas y la identificación del cliente, solicitando la debida diligencia con los clientes bancarios. Para ello proporciona

pautas que faciliten la identificación de los clientes, ya que no solamente es un elemento esencial para contar con un programa eficaz, sino que se transforma en una poderosa herramienta para protegerse contra los riesgos de reputación, operativos, legales y de concentración. También facilita el cumplimiento de los requisitos legales que permiten evitar el blanqueo de dinero y el financiamiento del terrorismo. Esto se complementa con pautas generales de buenas prácticas basadas en los principios que estipula en su documento base. En resumen, indica la información mínima que debe requerirse a un cliente para establecer la relación comercial, y la manera de comprobar la información para asegurar que el cliente sea quien dice ser. En estas pautas, diferencia la información y mecanismos de validación tanto de personas naturales como para personas jurídicas.

Basilea insta al Ente de Control a establecer normas claras de prevención de lavado de dinero y a controlar a las instituciones bancarias, propugnando que cada una establezca su metodología y sistema de control automatizado que facilite su labor.

Por otro lado, en Ecuador existe una Ley que tipifica y sanciona el lavado de activos y financiamiento de terrorismo, elaborada en base a experiencias de otros países, y de acuerdo a convenios internacionales.

Tanto la Superintendencia de Bancos como la Unidad de Inteligencia Financiera y el CONSEP son los entes encargados del control de prevención de lavado en las instituciones financieras.

Para ello, como parte de las normas internacionales, cada institución financiera debe normar, aplicar y controlar las políticas de “Conozca a su cliente”, “Conozca a su empleado”, “Conozca a su mercado”, “Conozca a su proveedor”. Estas políticas están encaminadas a que los funcionarios bancarios y de instituciones financieras apliquen normas y procedimientos tendientes a conocer:

- La identidad del cliente, es decir, asegurarse por los medios disponibles, que el cliente sea quien dice ser.

- El origen de los fondos, es decir, que estos provengan de fuentes lícitas.

- La actividad del cliente, y que ésta tenga relación con sus ingresos.

- El movimiento transaccional, de acuerdo a un perfil que debe identificarse desde el inicio de la relación comercial.

Estos mismos principios y políticas deben cumplirse para los empleados, de quienes debe realizarse un análisis previo a su contratación a fin de determinar de la mejor manera posible sus antecedentes, experiencia, situación financiera y económica, etc. Es obligación de las entidades sujetas a control de la Superintendencia de Bancos monitorear el comportamiento de sus empleados, establecer controles que permitan identificar posibles comportamientos inusuales, establecer políticas respecto al comportamiento que deben observar los funcionarios, respecto a detectar y notificar las transacciones inusuales, no aceptar propuestas de terceros respecto a dichas transacciones, reportar todo comportamiento que vaya en contra de los principios establecidos en el código de ética de la institución.

Respecto a proveedores, la institución debe también tener políticas claras que permitan conocer a los mismos de la mejor manera posible. Esto se puede lograr implementando normas como:

- Requerir referencias previas de otras instituciones en donde han prestado sus servicios.

- Requerir estados financieros para evaluar la capacidad económica de la empresa.

- Solicitar planillas de pagos al IESS para asegurar que está al día en sus obligaciones patronales.

- Llevar un registro de proveedores incumplidos, morosos, de mala reputación, etc.

- Llevar un monitoreo permanente de la relación con el proveedor.

En lo que respecta a la política “Conozca a su mercado”, partiendo de la identificación de los mercados objetivos, debe existir un permanente monitoreo de su evolución, lo cual le permite conocer su situación económica, proyecciones, metas, situación respecto a la evolución del país, relaciones con el exterior, etc., con lo cual se facilita la identificación de riesgos potenciales respecto a un mercado específico, y se complementa el análisis de la situación de los clientes corporativos, o de pequeñas y medianas empresas, inclusive de las microempresas.

Para efectos de establecer controles, las instituciones financieras deben consolidar los movimientos de los clientes, y reportar al Organismo de Control y a la UIF (Unidad de Inteligencia Financiera), los movimientos que sumados o en forma individual excedan los 10.000 dólares en un mes, y reportar las transacciones que la institución considere como inusual.

Complementariamente, las instituciones deben contar con software adecuado que le permita:

- Llevar un detalle del perfil del cliente y las desviaciones que se puedan detectar.

- Identificar oportunamente las transacciones inusuales, que salen de dicho perfil.

- Determinar si estas transacciones están de acuerdo a su actividad.

- En caso de que la desviación se produzca por transacciones específicas, solicitar al cliente el respaldo de tales transacciones (por ejemplo, si indica que recibió cien mil dólares por la venta de su casa, el cliente tendrá el respaldo documental que lo ratifique, además esta transacción no será repetitiva ni continua, y no debería alterar su perfil transaccional).

- Solicitar al cliente que llene el formulario del Consep para todas las transacciones de depósito en efectivo superiores a los 10.000 dólares.

COMENTARIO:

El lavado de activos y financiamiento de terrorismo es una realidad que se encuentra alrededor nuestro. Basta ver las consecuencias de su existencia en nuestro país vecino: muerte, secuestro, una sociedad altamente deteriorada en sus valores. En nuestro país el índice delictivo y la violencia con que se actúa ha crecido sustancialmente, en parte debido a la presencia que paulatinamente ha venido incrementándose desde Colombia y Perú de bandas organizadas.

Por tanto, las instituciones financieras deben mantener sus normas de prevención de lavado y estar alertas a posibles filtraciones de dinero proveniente de actividades ilícitas.

Este riesgo ha sido identificado por algunas instituciones desde mucho tiempo atrás, pero debido a la cantidad de clientes, a la variedad de servicios, a la complejidad de las transacciones financieras, a la multiplicidad de canales presenciales y tecnológicos, se requiere también de sistemas más complejos y constante capacitación al personal y fortalecimiento de valores institucionales.

Para efectos de llevar el monitoreo, las normas exigen que cada Institución nombre un Oficial de Cumplimiento, quien tiene nivel de reporte al Comité de Ética y Cumplimiento y al Directorio. El Oficial es el responsable de identificar políticas y procedimientos tendientes a prevenir el lavado de activos, solicitar al Comité de Ética su revisión, implementar los controles que considere pertinentes para prevenir el lavado de activos, monitorear el cumplimiento de los mismos, capacitar al personal en las normas de prevención de lavados.

Para esto debe contar con software especializado, llevar registros específicos por cliente, que le permita documentar el origen de los fondos. No hay que olvidar que la prevención es responsabilidad de todos, pero es el Oficial de Cumplimiento quien debe velar porque se guarden los respaldos respectivos de las transacciones, las explicaciones dadas por los clientes en los casos que consideró requerirlo, y dejar constancia expresa de lo actuado.

El Oficial de Cumplimiento reporta al Comité de Ética, que está constituido por un Director, el Representante Legal de la Institución, el Auditor Interno, un representante del

Departamento Legal, y representantes de las áreas de negocios, tecnología, operaciones y de las empresas subsidiarias. Para que sean más efectivas, es recomendable que las normas de prevención de lavado se establezcan y sean de cumplimiento obligatorio para todas las empresas que formen el grupo financiero, a fin de estandarizar los procesos y el control.

El Comité de Ética es el encargado de solicitar al Directorio la aprobación de políticas y procedimientos que fortalezcan el control de lavado, velar porque se doten de los recursos suficientes para el control, conocer los casos que el Oficial de Cumplimiento u otros presenten para su conocimiento y decidir qué hacer en tales casos (por ejemplo, si se presentan clientes con transacciones inusuales, el Comité puede solicitar cierres de cuentas, poner límites a las transacciones que se realicen, condicionar el cumplimiento de ciertos requisitos para aceptar una relación, etc.

Lo importante en esta materia es realizar la Debida Diligencia, que consiste en realizar todos los esfuerzos posibles para cumplir a cabalidad, y dejar documentada esta actuación.

El incumplimiento de estas normas implica graves consecuencias de orden inclusive penal para el Gerente General, el Auditor, el Oficial de Cumplimiento.
El lavado de activos es una actividad que se ha difundido a nivel mundial, especialmente en nuestra región, por la cercanía con Colombia. Solamente un esfuerzo conjunto, y el conocimiento claro del personal y el compromiso de evitar el lavado pueden ayudar a evitar este mal. Una institución que tiene fuerte compromiso moral, normas claras, ejemplo de cumplimiento de sus obligaciones, puede tener un programa de prevención efectivo para este riesgo, que en un momento dado podría ser fatal para la Institución.

CAPÍTULO VI: ASPECTOS ADICIONALES A CONSIDERAR EN LA IMPLEMENTACIÓN DE LA NORMA

6.1. Aspectos que deben ser considerados e incluidos para facilitar la implementación

Basándonos en los conceptos que se incorporaron en la Norma de Riesgo Operativo emitida por la Superintendencia de Bancos, los principios de Basilea que cobran vigencia cada vez más a nivel mundial, las mejores prácticas que de alguna manera hemos incluido en cada uno de los capítulos anteriores, y la experiencia de formar parte del proceso de implementación de la norma, podemos definir algunos aspectos que pueden ayudar a que la misma se realice de una manera ordenada, pero sobre todo que contribuya a optimizar los servicios que las Instituciones del Sistema Financiero proporcionan en beneficio de todos.

Entre los beneficios más significativos que esta implementación propone obtener están:

- Beneficios operativos a través de una mayor productividad en cada proceso crítico del negocio, por ende beneficio económico.

- Mejores calificaciones externas (AAA+).

- Percepción de mercado elevada.

- Ser una Institución atractiva para los clientes.

- La norma exige que se lleve un registro de eventos de riesgo operacional, con lo cual se puede cuantificar el potencial impacto. Las instituciones que llevan con mayor detalle con bases históricas y proyecciones reales, y demuestran las medidas tomadas para mitigar los riesgos a los que se han encontrado expuestas, tendrán una “premiación” respecto al nivel de provisiones que deben realizar.

- La adecuada administración de este riesgo genera una cultura de control en la institución, con lo cual los nuevos procesos tienden a desarrollarse con un concepto integral de identificar riesgos, tomar medidas para mitigarlos o evitarlos y con ello mejorar el servicio y la calidad.

- El cliente se ve beneficiado con productos y servicios de mejor calidad.

- Se reducen costos de reprocesos, errores, ineficiencias.

- La entidad trabaja bajo el concepto de autocontrol, facilitando el trabajo del Organismo de Control, y convirtiendo en un aliado para fortalecer el Sector Financiero y Bancario.

COMENTARIO:

Existe una serie de ventajas que las Instituciones del sector financiero obtienen con la implementación de la norma, beneficios que se pueden reflejar por ejemplo en la optimización de recursos, eficiencia de procesos, capacitación de sus funcionarios, ventaja frente a la competencia al mejorar la calidad de sus servicios, mejoramiento en los sistemas tecnológicos, actualización permanente de sus políticas y procedimientos, etc.

Como hemos mencionado en el desarrollo del presente trabajo, hay diferentes aspectos que deben ser tomados en cuenta para que esta implementación resulte exitosa, no obstante queremos con este resumen enfocarnos en temas esenciales y que muchas veces pueden pasar desapercibidos sin embargo de ser muy importantes a la hora de avanzar en el proyecto de implementación.

En primero lugar, mucho se habla de contar con el respaldo de la Directiva y Alta Gerencia de las Instituciones, pero qué significa en realidad y cuál es el nivel de participación dentro de este proyecto?

Para nosotros es la aceptación formal al proyecto con lo que esto significa: apoyar con recursos necesarios, aprobar políticas y procedimientos que faciliten la implementación, dar seguimiento permanente a los planes de ejecución de los

diferentes Departamentos o Áreas de la Institución, fijar objetivos estratégicos, entre otros aspectos.

Esto se puede lograr a partir de la designación del personal que se encargará de llevar adelante el proyecto, si bien es cierto toda la Institución deberá contribuir al logro de este objetivo, es necesario que la Unidad de Riesgos sea el líder y que reciba el empoderamiento necesario por parte de la Alta Gerencia, de tal forma que el resto de Unidades cumpla con las tareas asignadas.

A través del Comité Integral de Riesgos, presidido por el Gerente General o Presidente Ejecutivo, se informará periódicamente del avance, adicionalmente si se cuenta con un Comité de Tecnología, se adoptan las decisiones que corresponden a las inversiones de tipo tecnológico que el proyecto considere necesario y se el seguimiento correspondiente.

En lo que se refiere a seguimiento también la Unidad de Auditoría Interna juega un papel muy importante, ya que al tener la disposición de informar de manera mensual el avance del proyecto, a la Superintendencia de Bancos y Seguros, debe permanentemente impulsar el cumplimiento de tareas, así como brinda asesoría a la Unidad de Riesgos y resto de Unidades sobre la implementación de controles u optimización de procesos.

Esta labor permanente también contribuye a mejorar el clima laboral institucional, toda vez que muchas de las brechas identificadas en el diagnóstico efectuado para cumplir la norma, involucran a varias Unidades que deben trabajar en equipo para conseguirlo, haciendo posible una mejor comunicación.

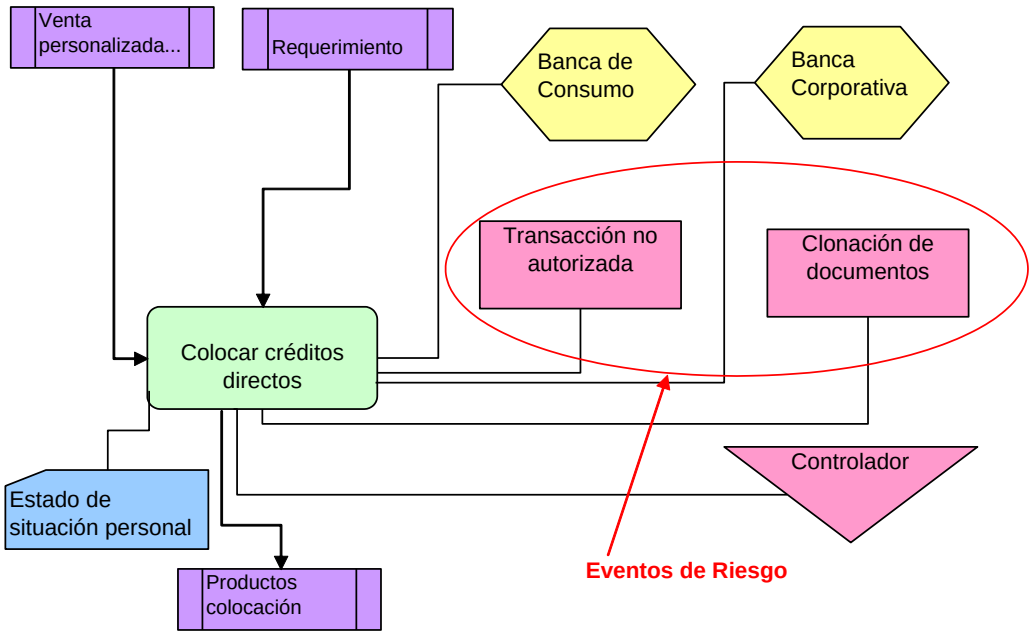
Otro aspecto básico a considerar es la implementación o adopción de varias metodologías para administración de riesgos, seguridad de la información, administración de proyectos de tecnología, etc. En este punto creemos que no hay que pensar que la herramienta más costosa es la mejor, o la asesoría internacional tiene la última palabra en cuanto a diagnosticar las necesidades de la organización. Más bien es una oportunidad para que la Institución haga un auto análisis y reflexione sobre las soluciones que se acoplan mejor a su realidad.

Sobre las mejores prácticas mundiales y casos de éxito cercanos a nuestra idiosincrasia, se pueden hacer estudios y comparaciones que sean de utilidad a la hora de seleccionar los métodos. No nos olvidemos que es muy importante tener un adecuado proceso de contrataciones y compras que contribuya al éxito de la implementación.

La resolución tiene en un alto porcentaje de aspectos relacionados con la tecnología y seguridad de la información, así como también mucho énfasis en documentar políticas y procedimientos.

En cuanto a las políticas y procedimientos es importante generar estándares para unificar formatos y lenguaje de tal manera que toda la Institución tenga la capacidad de entender claramente estos documentos. De igual forma disponer de un sitio de almacenamiento de esta documentación apropiado para que perdure en el tiempo y no exista pérdida o mal uso de la información. Mejor aún si se pueden adjuntar estos documentos a los mapas de procesos de tal manera que sea un repositorio completo, incluyendo la identificación de los riesgos del proceso, que facilite su comprensión.

Por ejemplo en la gráfica que se muestra a continuación se distingue el flujo del proceso, algunos enlaces a los procedimientos así como riesgos que se pueden identificar:



Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

En cuanto al factor de riesgo relacionado con la Tecnología y la Seguridad de la Información, existen algunas metodologías que la Institución puede implementar no únicamente con el fin de cubrir el cumplimiento de la norma, sino con el propósito de disponer de niveles de rendimiento más elevados, entre las más recomendables citamos: COBIT, ITIL, SIX SIGMA, ISO17799, ISO27001, ISO27005.

Existe mucha información y cursos que promueven la incorporación de estas metodologías, no obstante siempre habrá que partir del conocimiento que cada Institución tenga de sus procesos internos, como lo hemos dicho se deben tomar los aspectos que se acoplen a nuestra realidad y a los objetivos que perseguimos.

Con el avance tecnológico, y los negocios nuevos que promueven el uso de sistemas integrados, e-commerce, alianzas entre empresas, fusiones, nuevos productos en general, el riesgo es diferente del que se pudiera conocer anteriormente, por ello es necesario que se fomente en Tecnología una capacitación y cultura de identificación y mitigación del riesgo y de seguridad de la información de manera permanente.

Sobre todo con lo relacionado a los cambios que se realizan a las aplicaciones principales, se debe tener especial cuidado y contar con controles como: independencia de ambientes de prueba, testing y producción, control apropiado de versiones, certificaciones previas a todos los cambios críticos, autorizaciones formales de los responsables de los procesos, autorización del Oficial de Seguridad que tiene la aprobación final de los cambios, etc.

Para una Institución Financiera el tema de seguridad de la información cobra mayor relevancia no sólo por la normativa sobre riesgo operativo sino por toda la regulación anterior, es por ello que se debe otorgar un tratamiento especial. Desde la estructuración del área de Seguridad de la Información con el Oficial a la cabeza, hasta el monitoreo del cumplimiento de las políticas y procedimientos que se dicten, son prioritarios e importantes.
El plan de seguridad se puede plantear considerando algunas fases no es bueno que se pretenda implementar todo de una sola vez, esto también es un proceso progresivo que indiscutiblemente requiere el compromiso y labor de toda la Institución, una de los métodos que se pueden adoptar muestra cuatro fases o etapas a seguir:

Fuente: Presentación Grupo Implementación Riesgo Operacional Banco X

Una vez que se disponga de un entendimiento de toda la infraestructura de tecnología que se tiene: hardware, software, comunicaciones, estructura organizacional, procesos de tecnología, políticas y procedimientos, etc. Se deben identificar los riesgos principales con la ayuda de plantillas o elaborando una propia para luego priorizar aquellos aspectos más relevantes con los que se debe iniciar el plan.

Posteriormente se analizan los controles existentes para determinar su eficacia, y la conveniencia o no de nuevas estrategias o soluciones (costo-beneficio) para en función del resultado armar un cronograma de trabajo que es parte del plan

que se debe presentar a la Alta Gerencia para que con su aceptación se pueda hacer realidad.

Entender el impacto en riesgos y oportunidades requiere más conocimiento técnico que otras disciplinas, por lo que con el apoyo de todas las áreas de la Institución y el patrocinio de la alta gerencia, el plan de seguridad de la información obtendrá los objetivos planteados.

Otro aspecto fundamental que va de la mano con todo lo dicho anteriormente, es la capacitación y concientización constante de todo el personal de la Institución Financiera, de manera permanente y con evaluaciones que evidencien el nivel de compromiso de todos.

El factor de riesgo que hace posible que todos estos planes realmente se conviertan en realidad es el humano, por tanto otra Área muy importante en este camino es sin duda alguna Recursos Humanos, si la Institución cuenta con el personal adecuado, bien capacitado, y con niveles de cultura de riesgo y control interno apropiados, estamos precautelando los activos de la Institución de manera eficaz.

Es importante recordar que de acuerdo con estadísticas que manejan diferentes informes a nivel mundial sobre fraudes, el mayor porcentaje se pueden cometer con la ayuda de personal interno de las Instituciones, por lo que se debe prestar mucha atención y aplicar políticas orientadas al conocimiento del personal, sus antecedentes, su formación, seguimiento y evaluación, sin descuidar que cuando un funcionario se desvincula se lleva consigo un grado de conocimiento muy importante, debemos aplicar políticas de backups o formar equipos multi disciplinarios que eviten que la Institución pierda continuidad en sus procesos evitando posibles fallas o errores, así como documentar adecuadamente los diferentes procesos, procedimientos, sistemas. Esto ayuda a evitar dependencias del personal. También es necesario contar con claras políticas de vacaciones, descanso y remuneración.

Otro punto importante es contar políticas de clima laboral que aseguren un ambiente cálido y confortable para los funcionarios, desde diferentes aspectos

desde el entorno de trabajo, aspectos personales, capacitación, trabajo en equipo, etc. Solo un funcionario feliz consigo mismo y con su trabajo contribuye en un nivel superior a los objetivos de la Institución

Lo más importante de la implementación de esta norma, es que debe identificarse que todo lo actuado debe convertirse en un proceso continuo, que tuvo un inicio pero que no debe terminar. El sistema financiero es sumamente dinámico, y por tanto su estructura, políticas, procedimientos, sistemas, servicios y demás elementos sufren permanentes cambios, por lo que deben diseñárselos de manera flexible, que puedan adaptarse a los cambios a la velocidad que se requiere sin necesidad de grandes inversiones, y en forma oportuna.

6.2. Aspectos que deben ser evitados

COMENTARIO:

La norma de riesgo operacional abarca una serie de aspectos cruciales para las Instituciones Financiera, si bien muchos de ellos nos parecen normales y rutinarios, al realizar una evaluación a fondo podemos determinar que en muchos casos las políticas y procedimientos no se hallan debidamente documentadas, publicadas y difundidas.

Esto sucede especialmente en el área de Tecnología, debido a que el desarrollo tecnológico ha sido sumamente acelerado, y los profesionales en dicha rama no tienen una formación fuerte en el sentido de documentar, formalizar los procedimientos y acogerse a normas que en otras áreas de la Institución han sido tradicionalmente acatadas, y especialmente controladas y auditadas.

Y en general en toda la Institución se debe evitar el desorden en la documentación que manejan a través de políticas y estándares que faciliten su creación, actualización y mantenimiento.

Otro punto esencial es la evaluación previa que para que una Institución pueda llegar a cumplir la norma de riesgo operacional dentro de lo previsto y en el

tiempo límite que permite el Organismo de Control, se realiza con el apoyo de profesionales que han tenido experiencia previa en este tipo de evaluaciones.

Este trabajo puede convertirse en una experiencia enriquecedora para la institución, puesto que para realizar el levantamiento e identificación de brechas, pero siempre es necesaria la colaboración mutua. En este proceso debe tenerse mucho cuidado, evitando asignar a personas sin el suficiente conocimiento de la realidad, o personal que por evitar ser observado por la falta de cumplimiento de cada uno de los elementos que permiten cumplir la norma, o por falta de conciencia sobre la importancia de realizar un trabajo adecuado, proporcionen información incorrecta, inexacta o diferente de la realidad, con lo que habrán perdido la oportunidad de encontrar los aspectos que deben ser mejorados.

Una institución que asigne el tiempo, recursos y personal adecuado para la etapa de evaluación de la situación, invierte significativamente en la mitigación del riesgo operacional.

Se ha podido conocer que hay instituciones que, una vez realizada la evaluación de la situación actual, no dieron importancia suficiente a cubrir el gap, y lo hicieron únicamente con el ánimo de presentar a tiempo las brechas cubiertas, pero en el fondo no implementan con el énfasis e importancia suficiente las normas, políticas, procedimientos, sistemas, etc., por lo que se convierten en documentos que pronto se vuelven obsoletos por no haber recibido la importancia del caso. Este es un error realmente fuerte, pues se pierden de administrar adecuadamente el riesgo, quedan rezagados respecto a sus competidores que sí lo hacen conscientemente, y si bien pueden alardear de no haber “gastado” tanto dinero en sistemas, políticas, procedimientos, etc., en el fondo no realizaron oportunamente las inversiones en esos campos, con lo que son más susceptibles frente al sistema y más tarde o más temprano se verán más afectados que quienes lo hicieron de una manera adecuada.

Otro riesgo que hemos podido observar en la implementación de esta norma, es la tendencia a contratar demasiadas asesorías para la implementación de ciertos aspectos que antes no fueron tomados en cuenta por las instituciones, así por ejemplo:

- Desarrollo del BCP (Bussiness Continuity Plan), o Plan de Continuidad del Negocio.

- Implementación de metodologías adecuadas en el área de Tecnología, para su administración y control, si la entidad no cuenta ya con alguna.

- Desarrollo o adquisición de un software adecuado para llevar el registro de eventos de riesgo, su ocurrencia, responsables, determinación de medidas para mitigar, eliminar o transferir el riesgo, cuantificación, etc.

- Metodología para identificar y cuantificar los riesgos en cada proceso y realizar un mapeo de riesgos de la institución,

Podríamos mencionar más ejemplos, sin embargo lo que nos interesa es resaltar que las instituciones normalmente cuentan con experiencia y personal calificado que conoce a fondo su realidad, por lo que es necesario que al realizar la evaluación se determine en qué aspectos se necesitará apoyo de consultores externos y en qué medida, y no desperdiciar recursos en aspectos que muchas veces pueden ser adecuadamente atendidos por el personal con más criterio y experiencia. Por otro lado, es necesario también determinar qué áreas sí deben ser reforzadas y en qué medida deben ser acompañadas durante el desarrollo de estos temas.

Hemos conocido que algunas instituciones han contratado personal externo para realizar algunos de los aspectos que deben ser cubiertos para cumplir la norma. A nuestro criterio, consideramos que no es la situación ideal, pues no hay personal más conocedor de la realidad de la empresa que quienes laboran en ella por un determinado tiempo, y por otro lado, una vez realizado el trabajo, es el personal interno quien debería mantener un mecanismo que permita identificar las necesidades de cambio y actualización que se presentan día a día

Finalmente, queremos mencionar que como actoras en los procesos de evaluación tanto en la etapa inicial como en el monitoreo de la implementación de las brechas para cubrir los aspectos establecidos en la Resolución sobre riesgo operacional, quien gana a fondo es la institución, su personal, sus clientes, proveedores y la comunidad en general. Los errores que pueden cometerse en esta transición permiten finalmente retroalimentar el proceso y perfeccionarlo.

Es tan enriquecedor el proceso, que al mitigar los riesgos cubre las posibles pérdidas generadas por los eventos operacionales, convirtiéndose en una poderosa inversión, por lo que nuestra recomendación es que las empresas de diferente tipo deberían tomar los conceptos y aplicarlos para obtener los mismos beneficios, obviamente previa adaptación a su realidad.

6.3. Resumen

Como hemos mencionado, no existe una receta única que se pueda seguir al pie de la letra para lograr adecuada administración del Riesgo Operacional, sino que depende mucho de la realidad de cada organización, no obstante nos permitimos enumerar los principales aspectos a tomar en cuenta como Ayuda Memoria, y que han sido analizados a lo largo del presente trabajo:

PRIMERA ETAPA

1. Se debe entender el alcance y objetivos de la norma.

2. Conseguir el compromiso formal de la Alta Gerencia para que el proceso de implementación sea parte de los objetivos estratégicos del Banco. Esto facilita la toma de decisiones y la obtención de los recursos que se necesitan para llevar adelante el proyecto.

3. La Institución debe formar o definir la Unidad de Riesgos Integrales, su alcance y responsabilidades.

4. Si aún no existe, crear o definir el Comité de Riesgos Integrales, estructura y responsabilidades.
5. Nombrar un responsable de coordinar todas las acciones que todas las Unidades de la organización deben realizar durante este proceso, debe pertenecer a la Unidad de Riesgos.

6. Elaborar un inventario de los procesos de la Institución, y clasificarlos por niveles de criticidad, frente a los objetivos estratégicos de la Institución. Establecer además los responsables de cada proceso.

7. Establecer la estrategia a seguir con el fin de obtener un diagnóstico de la situación actual de la Institución frente a las especificaciones emitidas en la norma de riesgo operacional. Como hemos mencionado anteriormente es preferible asesorarse con Empresas o Consultores especializados que puedan dar valor agregado al diagnóstico inicial pero siempre con el acompañamiento del personal del Banco responsable, de manera que exista un traspaso de conocimientos.

8. Con el diagnóstico inicial establecer las brechas que deben cerrarse para cumplir lo normado, identificando los responsables de cada una de ellas y coordinando fechas de seguimiento y cumplimiento.

9. Establecer un plan de capacitación y concientización para todo el personal del Banco, considerando que todos somos responsables de administrar apropiadamente el riesgo operacional. Este aspecto debe siempre estar acompañado de la coordinación con Recursos Humanos.

10. Si no existe crear la Unidad de Seguridad de la Información, nombrar al Oficial de Seguridad, definir sus responsabilidades y atribuciones.

11. Establecer el responsable o coordinador para el Plan de Continuidad del Negocio, de igual manera recomendamos que esta persona pertenezca a la Unidad de Riesgos. Es importante aclarar que si bien es cierto es responsable frente a la Administración por la implementación de planes,

no significa que los tenga que desarrollar. Esta tarea también depende de los dueños de los procesos y líderes de continuidad.

SEGUNDA ETAPA

1. Establecer las principales políticas y procedimientos relacionados con Administración de Riesgos Operacionales, Seguridad de la Información, Plan de Continuidad del Negocio, Recursos Humanos, Tecnología, Legal. Todas las políticas y procedimientos deben estar orientados hacia los objetivos que persigue la norma. De acuerdo a lo conocemos la mayoría de las Instituciones Financieras disponen de una base documental importante relacionada con muchos de sus procesos. Aquí la tarea es más fácil porque se debería partir de un inventario de la misma e ir comparando con lo emitido en la norma para determinar cuáles serían las políticas o procedimientos que deben ser ajustados o incorporados, estableciendo igualmente un cronograma de trabajo con responsables y fechas de cumplimiento para poder hacer el seguimiento correspondiente.

2. Establecer las metodologías que se implementarán para las necesidades derivadas del análisis de brechas producto del diagnóstico efectuado, por ejemplo: Metodología para evaluar riesgos (escalas, plantillas, técnicas, etc), Metodología para implementar el plan de continuidad, método de evaluación de riesgos, estándares para documentar las políticas y procedimientos de todo el Banco, etc. En este aspecto es recomendable buscar asesoría con personas que ya han pasado por el proceso, conversar con el resto de Instituciones, capacitar al personal responsable. Un valor agregado para la organización es tener un buen proceso de contratación que permita revisar las ventajas de cada propuesta con el fin de tomar la mejor decisión.

3. Analizar y definir los recursos tecnológicos que deben ser adquiridos como soporte del proyecto, por ejemplo: un servidor para almacenar la base documental del Banco, herramientas de monitoreo, herramientas para evaluación de riesgos, infraestructura para el sitio alternos de procesamiento, etc. Obviamente con la colaboración del personal de

Tecnología que permitirá optimizar los recursos disponibles y no incurrir en gastos adicionales que no contribuyan con el proyecto.

4. Si no existe, determinar el procedimiento para registrar los eventos de riesgo. Tal como se indicó en el capítulo III del presente trabajo, existen diversas maneras de registrar los incidentes, con la ventaja de lo expresado en la norma la Superintendencia permite estandarizar el registro y poder mantener un control apropiado. Esta información es valiosa para la toma de decisiones y dirección de la organización, toda vez que permitirá tener información detallada de la realidad de sus procesos en todo momento. Este es uno de los pilares más importantes en este proceso, conocerse a sí mismos y poder autoevaluarse con el fin de establecer en qué se puede mejorar es un beneficio muy valioso.

5. Definir las prioridades que deben ser atendidas desde las mayores o críticas hasta las menores, pretender abarcar todo al mismo tiempo resulta imposible, siempre se deben atender aquellos aspectos que representan mayor exposición al riesgo. Para llegar a esto se debe haber efectuado el análisis de riesgos y controles, establecer brechas, recomendaciones, observaciones, etc. Sobre los aspectos que deben mejorar o cambiar para minimizar los riesgos. Generalmente los responsables de los procesos y el coordinador de la Unidad de Riesgos presenta al Comité alternativas de solución y prioridades que son formalmente aprobadas.

6. Elaborar el plan de seguridad de la información en función de los resultados de la evaluación de riesgos de los procesos críticos, que puede construirse en etapas para que su ejecución sea más fácil. Establecer el alcance y objetivos incluyendo responsables y plazos.

7. Tal como se indica en el capítulo IV del presente trabajo, la elaboración de planes de continuidad es un proceso de mediano y largo plazo, en el que se conjuga el trabajo de todas las Unidades de la Institución, el planteamiento del plan y su elaboración deben apuntar principalmente a los procesos críticos que el Banco, basado en sus objetivos de negocio, no puede dejar de operar en caso de eventos de riesgo mayor o

catastróficos. En este sentido podría ser una alternativa muy válida asesorarse con personal especializado en el tema con el fin de establecer un plan de acción con miras a conseguir este objetivo.

TERCERA ETAPA

1. Al tratarse de un proceso continuo, es importante establecer un esquema de seguimiento permanente al avance del cierre de brechas y al mantenimiento en general de todo lo implementado.

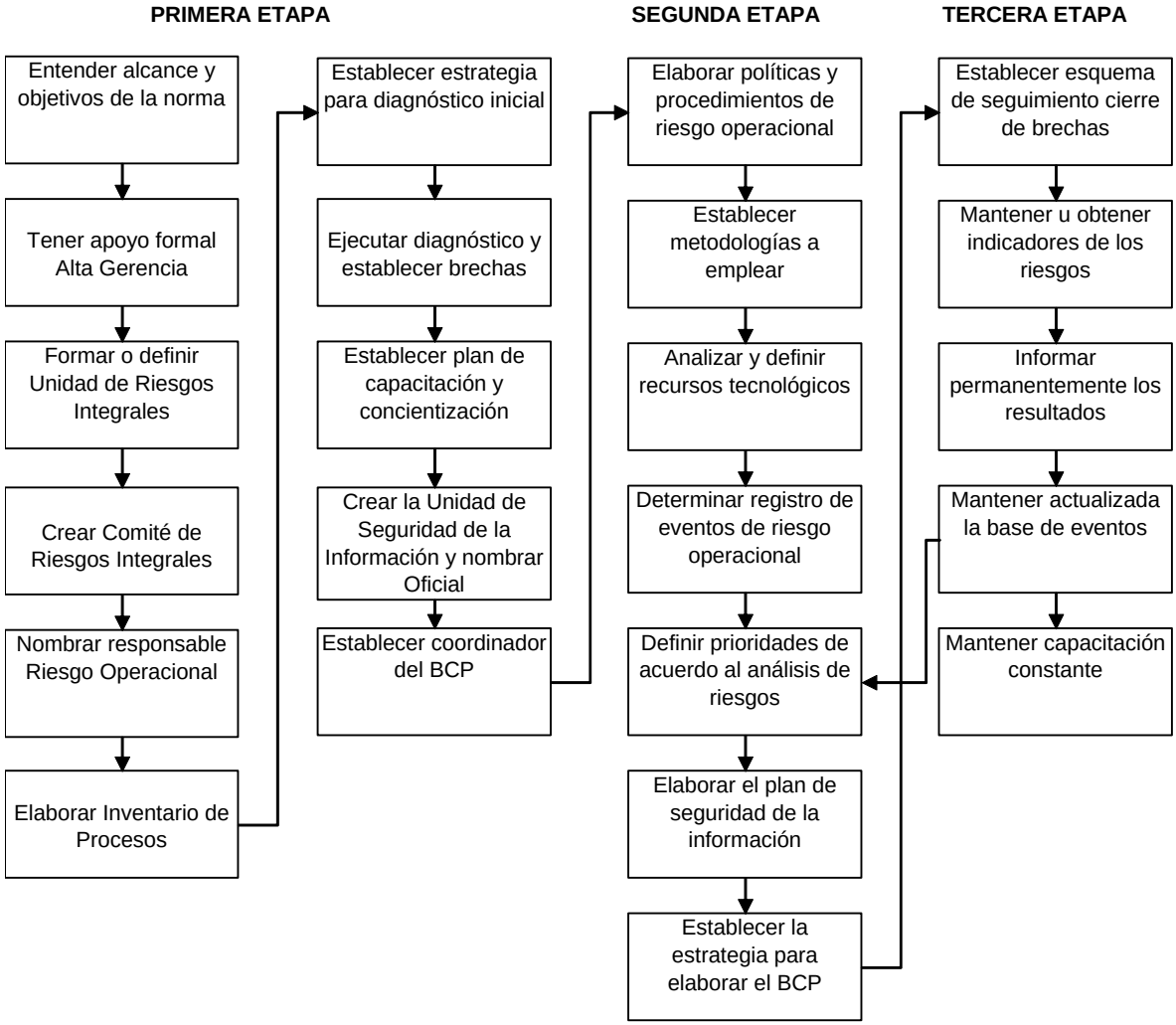
2. Otro aspecto adicional es darle mantenimiento o generar indicadores de riesgos operativos por proceso, su evolución o tendencia en el tiempo, si ha cambiado el proceso sobre todo se deben hacer los ajustes que correspondan.

3. Informar permanentemente de los resultados y avance en general al Comité de Riesgos Integrales, con el fin de adoptar las decisiones de este organismo frente al apetito del riesgo.

4. Mantener actualizada la base de eventos de riesgos.

5. Aplicar la estrategia de capacitación y concientización planteada con el apoyo de Recursos Humanos de forma permanente.

Si colocamos estas etapas de manera gráfica podemos obtener:


PRIMERA ETAPA
SEGUNDA ETAPA
TERCERA ETAPA
Entender alcance y objetivos de la norma
Tener apoyo formal Alta Gerencia
Formar o definir Unidad de Riesgos Integrales
Crear Comité de Riesgos Integrales
Nombrar responsable Riesgo Operacional
Elaborar Inventario de Procesos
Establecer estrategia para diagnóstico inicial
Ejecutar diagnóstico y establecer brechas
Establecer plan de capacitación y concientización
Crear la Unidad de Seguridad de la Información y nombrar Oficial
Establecer coordinador del BCP
Elaborar políticas y procedimientos de riesgo operacional
Establecer metodologías a emplear
Analizar y definir recursos tecnológicos
Determinar registro de eventos de riesgo operacional
Definir prioridades de acuerdo al análisis de riesgos
Elaborar el plan de seguridad de la información
Establecer la estrategia para elaborar el BCP
Establecer esquema de seguimiento cierre de brechas
Mantener u obtener indicadores de los riesgos
Informar permanentemente los resultados
Mantener actualizada la base de eventos
Mantener capacitación constante

CONCLUSIONES Y RECOMENDACIONES

A raíz de las crisis bancarias de los años 80, se impulsó a nivel mundial un acuerdo de cooperación internacional que fue emitido por el Banco de Liquidaciones Internacionales (BIS) en 1988- Este acuerdo fue denominado Basilea I, y regulaba los requerimientos mínimos que los bancos debían mantener para cubrir su exposición al riesgo crediticio, con lo cual pretendían dar solidez y seguridad a las instituciones financieras mejorando su nivel de capital, administración de riesgo y competitividad.
En un inicio, el acuerdo fue suscrito por los Bancos Centrales de 11 países. Actualmente más de 100 países lo han suscrito.

El acuerdo inicial no contempló todos los riesgos, por lo que posteriormente, en 1996 se incluyeron normas para el riesgo de mercado. Luego se han ido implementando nuevas normas y acuerdos para ampliar la cobertura de los riesgos, incluyendo nuevas técnicas de calificación y medición de los riesgos, asignando el capital en base a la rentabilidad ajustada por riesgo. Esto dio como consecuencia el Acuerdo de Basilea II, publicado en el 2004, que adoptó un nuevo estándar para medir el riesgo en los bancos, incluyendo el riesgo operacional
Basilea II busca a través de su normativa mejorar la infraestructura para medir el riesgo, reconocer las técnicas avanzadas para medir el riego, disminuir los requerimientos de capital para los bancos que gestionen mejor su riesgo, desarrollar e implementar nuevas metodologías para medirlo. Implementar la cultura de riesgos en la banca a nivel mundial, e implementar mejores procesos y controles en las instituciones.

La adopción de esta normativa permite mejorar la cuantificación y entendimiento de los riesgos en que se incurre, proporcionando mayor información para la toma de decisiones al momento de otorgar los créditos, mejorar la metodología de asignación de capital regulatorio y económico, y concentrar y administrar la información relacionada al riesgo.

La Superintendencia de Bancos del Ecuador ha ido implementando paulatinamente las diferentes normas tendientes a adoptar las normas emitidas por el BIS, entre ellas, la Norma de Riesgo Operacional, emitida en octubre del 2005 por la Junta Bancaria, a través de la Resolución JB-2005-834. Esta norma pretende que las instituciones financieras implementen un sistema de gestión de riesgo operativo a fin de identificar, medir, controlar, mitigar y monitorear los riesgos por fallas o insuficiencias en los procesos, personas,

tecnologías de información y eventos externos, inclusive el riesgo legal. El plazo de implementación para bancos tenía como fecha límite el 31 de octubre del 2008, y fue posteriormente aplazado hasta agosto del 2009.
En el primer semestre del 2009 la Superintendencia de Bancos inició el monitoreo “in situ” de los avances de la implementación de esta norma, a fin de determinar en base a las instituciones más significativas el estado general en que se encuentra.

Al momento, una vez transcurrido el tiempo e implementada la norma, ajustado, monitoreado, informados sus avances al Organismo de Control, es oportuno hacer un análisis, lo cual nos permite identificar una serie de conclusiones y recomendaciones, desde la óptica de una institución cuya cultura de cumplimiento y control han permitido que se interiorice en la institución las políticas y procedimientos desarrollados para dar cumplimiento a los aspectos normados.

Entre los principales beneficios que la aplicación de la norma trae como consecuencia podemos mencionar:

- Permite asegurar que los Objetivos y metas se cumplan de mejor manera, al tomar medidas preventivas que nos evitan sorpresas costosas y catastróficas. Por tanto previene la ocurrencia de pérdidas tanto tangibles como intangibles, pues las consecuencias de la ocurrencia de eventos no previstos puede generar pérdidas monetarias, de imagen, de clientes, etc. En ocasiones las pérdidas intangibles como clientes importantes, deterioro de la imagen, etc., pueden ser más significativas que las tangibles.

- La toma de decisiones se torna más eficaz, pues la aplicación sistemática de las normas y procedimientos que se adoptan implica que se documente de mejor manera los riesgos, las medidas tomadas para prevenirlos, las medidas tomadas cuando estos ocurren y sus consecuencias, generando una base de información valiosa para aplicar medidas oportunamente, cuantificar los costos y evitar la ocurrencia de nuevos eventos por las mismas causas.

- Se generan altos estándares de calidad en la entrega de productos y servicios a los clientes. La aplicación de las normas se asemeja significativamente a la aplicación de normas de calidad que se implantan para un adecuado control de calidad de los procesos.

- Favorece la reputación y las relaciones de la Institución con todos los involucrados (Accionistas, Directores, Empleados, Clientes, Organismos de Control, etc.), al divulgar y compartir información sobre el manejo de riesgos en la organización.

- Apoyo en los procesos de auto evaluación y mejora continua, potenciando la explotación de las oportunidades y nuevos negocios. Permite ofrecer productos más robustos con controles adecuados, mejora de tiempos de ejecución, etc.

- Mejora el clima organizacional pues se mitigan los errores, se proporciona un servicio al cliente con mayor calidad, existen estándares más claros de medición de objetivos y resultados, al trabajar con indicadores (índices) previamente establecidos y asignado el grado de cumplimiento y las desviaciones a las que puede llegar.

- Consigue un mayor valor agregado de la Auditoría, mediante un proceso de monitoreo integral de los riesgos operativos de la Institución. La evaluación de riesgos pasa de ser una tarea a cargo de Auditoría a ser responsabilidad de muchas áreas y personas.

- La implantación de un modelo de gestión de riesgo operacional definitivamente genera un cambio cultural significativo. Una vez que el personal interioriza acerca de la importancia y los beneficios de su implantación, se produce una sinergia que empuja a toda la organización hacia el logro de procesos más seguros. De hecho, el medio en que nos desenvolvemos de alguna manera nos mantiene más alertas en lo que se refiere a ciertos riesgos externos. La concienciación de los diferentes tipos de riesgo y sus consecuencias en caso de no tomar medidas oportunas hace que las personas actúen de forma diferente, inclusive en aspectos no normados.

Podemos por tanto decir que el riesgo operacional nos involucra a todos: el negocio, los procesos, los sistemas, la relación con los proveedores, los procesos, las políticas del negocio, etc.

La preocupación por el riesgo operacional en la gestión bancaria obedece a una serie de factores, entre los cuales podemos destacar:

- Las nuevas tecnologías disponibles para el procesamiento.
- Disposición de nuevos canales, especialmente electrónicos, para realizar las transacciones, trae asociado un riesgo implícito mayor.
- La gran variedad de servicios bancarios nuevos, que no están relacionados con los riesgos de crédito, mercado o liquidez.
- Los clientes son cada vez más exigentes.
- Mayor preocupación por parte del Organismo de Control.

Por todo lo expuesto, podemos compartir estas experiencias, en base a lo cual emitimos las siguientes conclusiones y recomendaciones:

CONCLUSIONES:

1. Esta norma es una fuerte guía que insta a las Entidades a partir de un diagnóstico inicial, a identificar sus fortalezas y debilidades. Es así que como punto de partida, el Organismo de Control solicitó a cada Entidad elaborar un cronograma de implementación de la norma. En el avance de la implementación, Auditoría Interna debe participar con una evaluación permanente del avance, informando mensualmente al Organismo de Control el estado de avance. Normalmente, cada institución parte de un estudio que lo realiza un equipo interdisciplinario con fuerte conocimiento de los aspectos normados. En muchos casos, las Entidades acuden a

Consultores Externos que ya han participado anteriormente en otras implementaciones, por lo cual se les facilita identificar punto por punto, detalladamente, a partir de un listado, los aspectos a cubrir, indicando qué recursos requieren, cuánto tiempo implicaría su desarrollo e implementación, hasta su conclusión.

2. Existen muchas metodologías para cada uno de los aspectos de la norma. Los consultores expertos pueden sugerir una o varias opciones. En ocasiones se complementa con la implementación de software especializado.

3. Es sumamente importante que para el levantamiento de los procesos se identifiquen y clasifiquen adecuadamente, pues es el punto de partida para desarrollar los diferentes temas. La matriz de procesos que se levante debe aprovecharse para documentar adecuadamente. La asignación o identificación de los dueños de los procesos es fundamental.

4. En casos de Grupos Financieros, es ampliamente recomendable que las normas que se establezcan se apliquen a nivel de todas las empresas del mismo, pues facilita su implementación y control.

5. Respecto a las políticas y procedimientos para proveedores, una vez que se estandarizan los contratos, se implementan las cláusulas de confidencialidad de la información, manejo de incidencias y contingencias, alcance de la responsabilidad, niveles de calidad de servicio, entre otros, la cultura institucional se fortalece, pues el personal de la institución se vuelve más estricto en determinar qué aspectos deben ser controlados.

6. Las normas de seguridad de la información en muchos casos han existido tácita o implícitamente. Sin embargo, es necesario ponerlas por escrito, ser sumamente estrictos en su implementación, controlar adecuadamente y complementarlas.

7. Como se mencionó en el punto anterior, gran parte de la información de un banco reside en su sistema automático. Esto implica que el área de Tecnología deba tener una adecuada estructura física y su correspondiente organización que garantice la correcta custodia de los datos, controles en el desarrollo de los sistemas, establecimiento de una adecuada infraestructura física y lógica que separe los diferentes ambientes, normas claras para desarrollo, puesta en producción, control

de versionamiento, selección del personal altamente calificado tanto técnicamente como en cuando a sus antecedentes personales, entre otros.

8. La administración del riesgo operacional es un procedimiento continuo, perfectible y dinámico. Una vez que se implemente a conciencia, es un proceso que nunca termina, sino que por el contrario fortalece a la Entidad, a su personal, que administra de una manera más técnica y especializada cada uno de los aspectos considerados en la norma.

RECOMENDACIONES:

A continuación emitimos las recomendaciones, con la aclaración de que cada una de ellas corresponde a una conclusión, es decir, son complementarias:

1. El proyecto debe ser interiorizado a nivel de la Alta Gerencia y el Directorio, pues son quienes asignarán los recursos, priorizarán su implementación y realizarán un seguimiento hasta su total implementación.

   El personal que se escoja tanto para identificar las brechas como para liderar el desarrollo de los aspectos debe ser muy profesional, tener experiencia y ser imparcial, pues deben identificarse correctamente las mencionadas brechas. Debe formarse un equipo interdisciplinario, y de ser posible y necesario, contratar una consultoría especializada que guíe a los bancos y en general instituciones financieras en los temas que considere polémicos o que implican algún tipo de preparación previa. Sin embargo, es necesario que sean los líderes de los diferentes procesos del GFP. La participación de Auditoría Interna es fundamental, la Unidad de Riesgos Integrales es quien debe liderar el proceso.

2. Cada institución debe elegir libremente la metodología, software especializado, etc., de acuerdo a su organización, políticas, estructura, la mejor opción que considere. No siempre es necesario realizar tareas muy sofisticadas. Lo perfecto es enemigo de lo bueno. Toda implementación tiene un punto de partida, y en el camino se va implementando, ajustando, perfeccionando. Este es un proceso continuo, que busca la mejora permanente y va encontrando la forma de adaptar a las necesidades institucionales. Lo importante es que el grupo responsable de su implementación busque las mejores opciones y las vaya adaptando.

3. La identificación de los dueños de los procesos debe ir complementada con la clara definición de sus funciones. El dueño del proceso debe convertirse en un coordinador, un facilitador del mismo. Es ideal que el dueño de cada proceso tenga un perfil establecido, pues es quien en adelante velará porque el proceso se norme, grafique, desarrolle, documente y controle adecuadamente. Esto no significa que el dueño deba realizar todas las tareas, sino que tenga un liderazgo adecuado y el suficiente conocimiento para saber identificar sus soportes en las demás áreas que contribuirán a que el proceso sea de calidad. Los dueños de los procesos deberían tener un adecuado entrenamiento en temas de calidad, ser capaces de establecer indicadores y monitorear su evolución, delegar funciones, coordinar con Tecnología los desarrollos necesarios, velar porque sus procesos sean flexibles y satisfagan las necesidades de los clientes internos y externos. Esto asegura el éxito en sus funciones.

4. La implementación a nivel de Grupo Financiero (en los casos que aplique) no solamente estandariza, sino que finalmente permite el ahorro de costos, la especialización del personal, la optimización de los procesos, una mejor relación con los proveedores, la creciente formación de cultura de control institucional y el fortalecimiento del control interno.

5. Al implementar las políticas para proveedores, es necesario establecer que ellos deben ser reconocidos como socios estratégicos, para lo cual se deben establecer normas de “ganar – ganar”, es decir, no por poner controles el proveedor debe sentirse doblegado o utilizado, sino que por el contrario, mientras más claras estén las responsabilidades, las dos partes (cliente/proveedor) ganan, debe venderse la idea de que el control es una herramienta que beneficia mutuamente y que la cooperación ayuda a mejorar la relación e inclusive el servicio. Solamente si las dos partes se ven beneficiadas un contrato puede ser sustentable en el tiempo. Por tanto hay que trabajar en ese sentido.

6. La seguridad de la información debe ser interiorizada por el personal de la Entidad, no es una función específica de la Unidad de Riesgos o de Auditoría. Debe ser parte de la cultura de la Institución. Si no se la interioriza, no habrá norma que sirva, pues aún las seguridades más sofisticadas se vulneran fácilmente si las personas no están conscientes y las aplican adecuadamente. Esto se logra en primer lugar, con el ejemplo de los directivos, con aplicación clara e imparcial, con normas claras y controles estrictos.

Por otro lado, la delincuencia ha progresado tanto que aún cuando el personal y las normas sean las adecuadas, nunca es suficiente. La información en las instituciones financieras reside en gran parte en el sistema informático, que debe ser protegido con alta tecnología, para lo cual deben establecerse claras políticas y complementar con el uso de hardware y software que proteja, permita el monitoreo y el bloqueo de intrusiones cuando estas se detectan. La seguridad de la información en un banco es vital, es uno de los activos más valiosos que deben ser protegidos.

Estas normas deben ser dinámicas, es decir, sometidas a permanente evaluación y ajuste, a fin de satisfacer los requerimientos de un mundo que cambia con mucha rapidez.

7. El área de Tecnología ha sido típicamente un área menos consciente de los riesgos, inclusive por cuanto el personal técnico en muchas ocasiones no cuenta con una adecuada formación administrativa y de control. Es necesario concientizar al personal responsable de los sistemas y comunicaciones sobre la necesidad de establecer políticas y procedimientos claros, documentar sus procesos y las aplicaciones, y establecer controles, es vital. Una vez que se logra ese nivel de concientización la administración del área se la realiza en forma más profesional, con lo cual se beneficia la Institución. Es necesario trabajar en forma más técnica, en la actualidad existen metodologías que guían su implementación y normativa, entre ellos tenemos Cobit, ITIL, normas ISO, etc., que deben ser implementadas para lograr una administración integral de los recursos tecnológicos.

8. Las entidades deben asignar la prioridad del caso, escoger adecuadamente a los responsables de la administración del riesgo operacional, asignar los recursos necesarios. La única conclusión posible como producto de una implementación realizada profesionalmente es que la Institución crece, se tecnifica más y está más preparada para enfrentar las diversas situaciones que se presenten mitigando los impactos. Es una situación de mejora continua que nunca se detiene.

Los últimos acontecimientos acaecidos con instituciones financieras a nivel mundial han permitido difundir el hecho de que cuando existe un desmedido apetito por el riesgo, sumado a una legislación y supervisión débil, que permite desarrollar nuevos

productos fuera de sus legislaciones, la imaginación humana no tiene límite. Si bien los riesgos que corrieron estas instituciones son catalogados como riesgo de mercado, riesgo de crédito, etc., también existió en gran medida un riesgo operacional y legal no identificado ni mitigado, transferido inadecuadamente y peor evaluado. Es necesario que se identifiquen estas debilidades y se las legisle. Un riesgo tan elevado debió haber sido oportunamente advertido. Hay mucho por hacer todavía, y en ello el auditor tiene un gran campo de desarrollo profesional. Cada vez se requerirá personal más especializado en la administración de riesgo, no solamente para la banca, sino en empresas de diferente índole. Insistimos, hay mucho por hacer.

BIBLIOGRAFÍA

- International Organization for Standarization, Código de Práctica para la administración de la seguridad de la información, Norma ISO 17799.

- Governance Institute, Modelo COBIT versión 4.1 (Control Objectives for Information and related Technology), mejores prácticas para la administración de riesgos en Tecnología, 2007.

- Committee of Sponsoring Organization of the Tradeway Commission, Modelo COSO ERM, marco integral para la administración de riesgos corporativos.

- Instituto de Auditores Internos, Marco internacional para la práctica profesional de Auditoría.

- ESTUPIÑAN GAITAN, Rodrigo, CONTROL INTERNO Y FRAUDES con base en los ciclos transaccionales Análisis de Informe COSO, Ecoe Ediciones.

- ESTUPIÑAN GAITAN, Rodrigo, CONTROL INTERNO Y FRAUDES con base en los ciclos transaccionales Análisis de Informe COSO I y II, Segunda Edición, Ecoe Ediciones.

- MARTÍNEZ, Juan Gaspar, PLANES DE CONTINGENCIA, Díaz De Santos Ediciones.

- LEY GENERAL DE INSTITUCIONES DEL SISTEMA FINANCIERO.

- RESOLUCIÓN JUNTA BACARIA JB-2005-834 “De la gestión y administración de riesgos”.

- Publicaciones en Internet:

  - “Riesgo Operacional, Control Interno y papel de la Auditoría Interna”, 7mo Congreso Latinoamericano de Auditoría Interna y Administración de Riesgos.

  - Bank for International Settlements (BIS)-Comité de Supervisión Bancaria de Basilea:

    - Publicación Buenas prácticas para la gestión y supervisión del Riesgo Operativo, Febrero 2003.

    - Metodología de los Principios Básicos, Octubre de 1999.

    - Implementación de Basilea II: Consideraciones Prácticas, Julio 2004. Traducción de la Asociación de Supervisores Bancarios de las Américas – ASBA).

    - Principios Básicos para una supervisión bancaria eficaz, Octubre de 2006.

    - La mejora del gobierno corporativo en organizaciones bancarias, Febrero de 2006.

- El Nuevo Acuerdo de Capital de Basilea, Documento Consultivo Emitido para Consulta, Enero 2001.
- Customer due dilligence for banks, October, 2001.
- Buenas Prácticas para la gestión del riesgo operativo.
- Orientaciones para la apertura de cuentas y la identificación del cliente, febrero 2003.

- Páginas Web:
  - www.superban.gov.ec
  - http://www.buniak.com/
  - www.isec-global.com
  - www.bis.org