UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE CIENCIAS

METODOLOGÍA DE RIESGO OPERACIONAL Y CONTROL INTERNO PARA BANCO

REPORTE DE TRABAJO PROFESIONAL

QUE PARA OBTENER EL TÍTULO DE:

ACTUARÍO

P R E S E N T A :

ANABEL CABALLERO GONZÁLEZ

TUTOR:
M EN A.O. OSCAR ARANDA MARTÍNEZ

2015

CONTENIDO

REFERENCIA DE SIGLAS

CNBV	Comisión Nacional Bancaria y de Valores
BASILEA	Comité de Basilea, compuesto por los gobernadores de los bancos centrales del G-10
SARBANES OXLEY	Ley que nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores.
COSO	Proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías: • Eficacia y eficiencia de las operaciones. • Confiabilidad de la información financiera. • Cumplimiento de las leyes, reglamentos y normas (que sean aplicables).

INTRODUCCIÓN

La administración de Riesgo Operacional y Control Interno se han vuelto indispensables en las Instituciones, la crisis financiera, la inestabilidad económica, los constantes cambios en la regulación aplicable, las múltiples necesidades en el sector financiero, en el caso particular para la banca, reflejan la necesidad de tener una administración de riesgos operacionales y control interno eficiente que permita preservar el valor de la Institución.

Para enfrentar los desafíos que presentan actualmente las Instituciones se debe definir el apetito de riesgo y las medidas que coadyuven a su aplicación, fortalecer las tres líneas de defensa las cuales son la unidad de negocios, unidad independiente de riesgos y la auditoría interna, crear una cultura de riesgos sólida que facilite integrar un ambiente de control adecuado en todos los niveles de la institución, encaminar los objetivos de la gestión de riesgos hacia el incremento de la rentabilidad y el valor de los accionistas, evitando pérdidas, garantizando la seguridad a los usuarios y manteniendo la reputación de la Institución, además se debe alinear a las normas internacionales y solicitado por las Autoridades reguladoras y supervisoras.

El riesgo operativo tiene como objetivo principal detectar los riesgos (actuales y potenciales) que incluyen los tecnológicos y legales, además de reflejar de manera anticipada el impacto (económico, reputacional, entre otros) que pueden causar en caso de que se materialicen, apoya a mejoramiento continuo de los procesos y crea conciencia en la Institución sobre el nivel y la raíz de los eventos de pérdida. El control interno funciona como elemento evaluador de los controles que se tienen en la empresa, además de verificar la eficacia para minimizar dichos riesgos en su impacto y/o frecuencia.

El contar con una metodología de administración de riesgos, en la cual se unifique la correcta detección de los riesgos operativos, así como el evaluar la eficacia de los controles internos por medio de atributos, apoyará a la Institución a alcanzar sus objetivos a través de la prevención y administración de los riesgos operacionales, asegurara que los riesgos operacionales existentes y los controles requeridos estén debidamente identificados, evaluados y alineados con la estrategia de riesgos establecida por la organización y monitoreara los riesgos potenciales (riesgos de alto impacto), para proponer controles compensatorios que permitan reducir la calificación del riesgo residual,

adicionalmente conduce a tener de forma oportuna, situaciones que pueden tener como consecuencias pérdidas financieras, fraudes, lavado de dinero, entre otros.

La metodología propuesta en este documento, contiene elementos establecidos en el comité de Basilea, el cual menciona cual es el adecuado proceso de gestión del riesgo operacional, el cual describe como “gestión” al proceso de “identificación, evaluación, seguimiento y control o cobertura” del riesgo operacional, así mismo para implementar un adecuado entorno de Control, mantiene lo indicado en el informe COSO y la ley de Sarbanes Oxley SOX, con el fin de ser competitivos y responder a las nuevas exigencias empresariales, mencionando que el control interno debe poseer cinco componentes que pueden ser implementados de acuerdo a las características administrativas, operacionales y de tamaño; los componentes son: un ambiente de control, una valoración de riesgos, las actividades de control (políticas y procedimientos), información, comunicación y finalmente el monitoreo o supervisión.

El documento consta de 8 capítulos, en los cuales se presentan los antecedentes que dan origen a la necesidad del riesgo operacional y el control interno incluyendo lo que dicta BASILEA y la Ley SOX, así como lo dictado en las mejores prácticas descritos en el informe de COSO, adicionalmente se cuenta con fragmentos de la Circular Única de Bancos CUB que emite la CNBV, en la cual se describe el cumplimiento al que está obligado el área de la Administración de Riesgos, el Anexo 12 de la CUB describe la elaboración de la base de eventos de pérdida y su clasificación, con respecto a Control Interno se cuenta con una obligación de tener un sistema de control interno adecuado de los cuales se tiene como base los artículos de la Ley Sarbanes Oxley.

Adicionalmente, se describe la búsqueda del modelo de gestión que reúna a estas dos disciplinas con la descripción de las ventajas que tiene el contar con dicha metodología.

Finalmente se desarrolla el modelo matemático y actuarial así como la metodología para la gestión de riesgos operacionales y la evaluación de los controles internos.

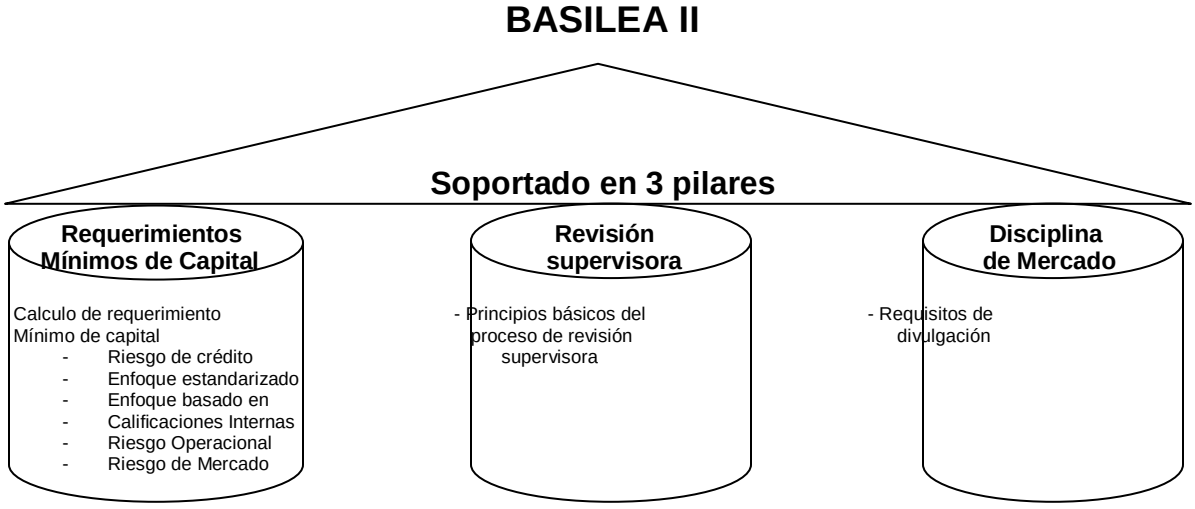
Por último se presentan las conclusiones del presente documento.

1. MARCO TEÓRICO

1.1. Antecedentes

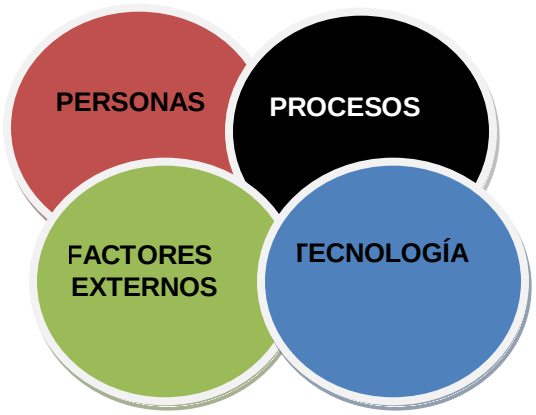
La totalidad de la evolución de la regulación bancaria refiere a la implicación de la alta dirección y del consejo de administración en el conocimiento de los riesgos para la creación y diseminación de una cultura adecuada, las reglas de capitalización en función del nivel de riesgo, los criterios contables acordes a los riesgos financieros, asignación y seguimiento de calificaciones de riesgo , medición de factores de riesgo e imposición de límites, reglas de conducta y **medidas de control interno**, políticas y procedimientos documentados, herramientas de autoevaluación, mapas de procesos, eventos de pérdida, indicaciones y alertas, análisis de escenarios, modelos internos y cumplimiento de mejores prácticas.

El Comité de Supervisión Bancaria de Basilea (Basilea II y III) al ser integrada por supervisores de diferentes países del mundo, tiene como objetivo primario el aseguramiento de la solvencia de los sistemas financieros objeto de su supervisión, Al amparo de dicho objetivo, sus temas de interés con vistas a la determinación de requerimientos de cobertura de capital, abarcan la modalidad de riesgo operacional incluyendo el riesgo legal y tecnológico como parte de esta modalidad.



Basilea define al **riesgo operacional**, como la pérdida derivada de la inadecuación o fallos en los procesos internos en los sistemas, en la actuación del personal, o por eventos externos.

De acuerdo con la definición de riesgo operacional los eventos se producen como resultado de la intervención de cualquiera de los siguientes elementos.



Un ejemplos de la diferencias del riesgo operacional con respecto a otros riesgos es que el riesgo de mercado está asociado a productos, el de crédito a contrapartes y el operacional a procesos, en el sentido común no basta con gestionar el riesgo, es preciso realizar formas serias para su identificación, evaluación, transferencia, mitigación, seguimiento y registro.

Algunos de los principios básicos de la gestión del riesgo operacional se refieren a:

- Que el riesgo se traduce en la buena gestión de los procesos.
- La complejidad de una organización, un proyecto o un proceso añade riesgo a su operación, demandando actividades de anticipación o reacción.
- Un riesgo desconocido es “más peligroso” que un riesgo conocido.
- No hay gestión posible de los riesgos sin información acerca de ellos, por lo que la perfección e integridad de datos, información y sistemas son esenciales
- Se debe tener cuidado en los supuestos subyacentes utilizados en el modelo de riesgo operacional ya que puede arrojar resultados que no dan valor agregado a la Institución por lo que “no serviría de mucho”.
- Igual que el modelo de gestión al riesgo operacional, es importante contar con una adecuada cultura institucional de atención al riesgo ya que los dueños de los

procesos darán a conocer la información de los riesgos inherentes a las actividades diarias que realizan.

Una de las funciones indispensables del **control interno** es garantizar, alcanzar, cumplir los objetivos propuestos de la Institución, y lograr así la dirección acertada de las actividades de una organización.

La importancia del control interno y del interés creciente sobre el mismo en los últimos años han originado distintas opiniones sobre la naturaleza, el objetivo y la forma de conseguir un control interno eficiente y eficaz.

El control interno surgió de la necesidad de disponer de información cada vez más confiable, como un medio indispensable para llevar a cabo un control eficaz además de asegurar que se protejan los activos de la empresa teniendo evaluaciones de los controles que tienen impacto al negocio y a los estados financieros, principalmente. Los directivos deben asignar más importancia al empleo de información financiera y no financiera para controlar las actividades de las entidades bajo su dirección.

La Ley Sarbanes Oxley, creada el 30 de julio de 2002, es una ley de Estados Unidos también conocida como el Acta de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. También conocida como SOx, SarbOx o SOA.

La Ley Sarbanes Oxley nace en Estados Unidos con el fin de monitorear a las empresas que cotizan en bolsa de valores, evitando que las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversor. Es una Ley federal que fue originada a raíz de los escándalos financieros de algunas grandes corporaciones, como Enron, Tyco International, WorldCom y Peregrine Systems. Estos escándalos hicieron caer la confianza de la opinión pública en las empresas de auditoría y contabilidad. La Ley toma su nombre del senador del partido demócrata Paul Sarbanes y el congresista del partido republicano Michael G. Oxley. Abarca y establece nuevos estándares de actuación para los consejos de administración y dirección de las sociedades así como los mecanismos contables de todas las empresas que cotizan en bolsa en Estados Unidos. Introduce también responsabilidades penales para los consejos de administración y unos requerimientos por parte de la SEC (Securities and Exchanges Commission), organismo encargado de regular el mercado de valores de Estados Unidos. Los partidarios de esta

Ley afirman que la legislación era necesaria y útil, mientras los críticos creen que causará más daño económico del que previene.

La primera y más importante parte de la Ley establece una nueva agencia privada sin ánimo de lucro, “the Public Company Accounting Oversight Board", es decir, una compañía reguladora encargada de revisar, regular, inspeccionar y sancionar a las empresas de auditoría. La Ley también se refiere a la independencia de las auditoras, el gobierno corporativo y la transparencia financiera. Se considera uno de los cambios más significativos en la legislación empresarial, desde el New Deal de 1930.

Esta ley, más allá del ámbito nacional, involucra a todas las empresas que cotizan en NYSE (Bolsa de Valores de Nueva York), así como a sus filiales. En México se ha adoptado de acuerdo a las mejores prácticas internacionales.

El informe COSO apoya a la ley de Sarbanes Oxley, tratándo los siguientes puntos en común: Definición, Componentes, Evaluación de Riesgos, las Actividades de Control, Supervisión, Normas Generales del Control Interno, Misión y Objetivos, Asignación de Autoridad y Responsabilidad.

1.2. Normatividad

Se cuenta con entidades regulatorias que verifican el cumplimiento en los bancos en el tema de Riesgo Operacional, así como leyes internacionales para Control Interno, a continuación se presentan los artículos que legislan los 2 temas.

En dicha normativa se concentran los temas que se deben de tener como mínimo para dar cumplimiento a las disposiciones de carácter general aplicables a los bancos en tema de Riesgo Operacional y Control Interno.

1.2.1 Disposiciones de Carácter General aplicables a las Instituciones de Crédito. Circular única (CUB)

Capítulo IV
Administración de Riesgos
Sección Primera
Artículo 66.- Los riesgos a que se encuentran expuestas las Instituciones, así como sus Subsidiarias Financieras, podrán clasificarse en los tipos siguientes: **Discrecionales y no Discrecionales.**
Riesgos no discrecionales, que son aquéllos resultantes de la operación del negocio, pero que no son producto de la toma de una posición de riesgo, tales como el riesgo operacional, que se define como la pérdida potencial por fallas o deficiencias en los controles internos, por errores en el procesamiento y almacenamiento de las operaciones o en la transmisión de información, así como por resoluciones administrativas y judiciales adversas, fraudes o robos, y comprende, entre otros, al riesgo tecnológico y al riesgo legal, en el entendido de que:
1. El riesgo tecnológico se define como la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios con los clientes de la Institución.
2. El riesgo legal se define como la pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que las Instituciones llevan a cabo.

162) XII. Prever las medidas que se estimen necesarias para que la Administración Integral de Riesgos y el Sistema de Control Interno, sean congruentes entre sí.

Apartado B

De los riesgos cuantificables no discrecionales

Artículo 86.- En materia de riesgos cuantificables no discrecionales las Instituciones se sujetaran a lo siguiente:

(162) Asimismo, deberán contar con políticas y procedimiento que contemple:

(162) a) La identificación, evaluación, seguimiento y control de los riesgos operacionales implícitos a los procesos de la Institución por categoría de riesgo.

(162) b) Los criterios para recabar y administrar las pérdidas por eventos de riesgo operacional.

III. En adición a lo expuesto, las Instituciones deberán como mínimo desarrollar las funciones siguientes respecto de:

(18) a) La administración del riesgo operacional:

1. Identificar y documentar los procesos que describen el quehacer de cada unidad de la Institución.

(161) 2. Identificar y documentar en un inventario, los riesgos operacionales implícitos a los procesos a que hace referencia el numeral anterior. Lo anterior cada vez que se dé de baja, modifique o identifique un nuevo riesgo operacional. Dicho inventario deberá contener, como mínimo:

(161) i. La descripción del riesgo operacional identificado;

(161) ii. Tipo de riesgo operacional;

(161) iii. Línea de negocio;

(161) iv. Proceso;

(161) v. Producto;

(161) vi. Cuantificación;

(161) vii. Controles, y

(161) viii. En su caso, planes de mitigación y área responsable de su mitigación.

(161) 3. Evaluar e informar por lo menos trimestralmente, el perfil de exposición al riesgo operacional, así como las posibles consecuencias que sobre el negocio generaría la materialización de los riesgos identificados e informar los resultados a los responsables de las unidades implicadas, a fin de que se evalúen las diferentes medidas de control de dichos riesgos.

4. Establecer los Niveles de Tolerancia al Riesgo para cada tipo de riesgo identificado, definiendo sus causas, orígenes o Factores de Riesgo.

(18) 5. Para el registro de eventos de pérdida por riesgo operacional, incluyendo el tecnológico y legal, deberán:

i. Obtener una clasificación detallada de las distintas Unidades de Negocio y líneas de negocio al interior de la Institución.

(161) ii. Contar con criterios, políticas y metodologías que permitan identificar y clasificar los diferentes tipos de eventos de pérdida y cercanos a pérdida conforme al numeral anterior.

(18) iii. Mantener una base de datos histórica que contenga el registro sistemático de los diferentes tipos de pérdida y su costo, en correspondencia con su registro contable, debidamente identificados con la línea o Unidad de Negocio de origen, según las clasificaciones al efecto definidas por los subincisos i y ii anteriores. Para la generación y actualización de dicha base de datos, se deberá cumplir con lo establecido en el Anexo 12-A de las presentes disposiciones.

(4) El desempeño de las funciones descritas en los numerales 1, 2, 3 y 4 a que hace referencia el presente inciso, será responsabilidad del comité de riesgos de la Institución de que se trate, pudiendo auxiliarse en el área que se estime conveniente, siempre y cuando con ello no se susciten conflictos de interés.

(18) Por lo que toca a las funciones relativas al riesgo operacional a que hace referencia el numeral 5 anterior, su desempeño corresponderá a la unidad de Administración Integral de Riesgos de la Institución correspondiente. Para ello, las Instituciones deberán establecer mecanismos que aseguren un adecuado flujo, calidad y oportunidad de la información entre la referida unidad de Administración Integral de Riesgos y el resto de las unidades al interior de la entidad, a fin de que estas últimas provean a la primera los elementos necesarios para llevar a cabo su función.

(162) 6. Implementar políticas, procedimientos y criterios para la identificación, priorización, cuantificación, seguimiento y control de los riesgos operacionales, así como para su asignación a las diferentes líneas de negocio.

(162) 7. Establecer indicadores de riesgo operacional, que permitan medir la evolución de cada uno de los riesgos operacionales que la Institución defina como prioritarios.

(162) 8. Generar información del perfil de riesgo operacional de la Institución para la toma de decisiones que al menos deberá incluir:

(162) i. El inventario de riesgos operacionales prioritarios.

(162) ii. Los mapas de perfil de riesgo.

(162) iii. La calificación de riesgo operacional a nivel Institución o unidad de negocio.

(162) iv. Los procedimientos de control y/o mitigación de los riesgos operacionales.

(162) v. Los casos relevantes de eventos por riesgo operacional, así como las acciones correctivas implementadas.

1.2.2 ANEXO 12 A CUB. Requisitos para la elaboración y actualización de la base de datos histórica que contenga el registro sistemático de los diferentes tipos de pérdida asociada al Riesgo Operacional de los diferentes tipos de pérdida asociada al riesgo operacional de las Instituciones de Crédito.

Las Instituciones deberán generar una base de datos histórica que contenga el registro sistemático de los diferentes tipos de pérdida y su costo, el cual deberá incluir la pérdida económica originada por el evento así como todos los gastos adicionales en los que incurrió la Institución como consecuencia de dicho evento, en correspondencia con su registro contable, el cual deberá realizarse de forma global en las cuentas de gastos y, de forma específica, a través de auxiliares en la contabilidad. En caso de haber recuperaciones, éstas deberán estar registradas por separado.

Los eventos de riesgo operacional deberán ser clasificados en cuando menos uno de los distintos tipos de eventos de pérdida señalados en la sección II del presente Anexo, sin que ello limite a las Instituciones a realizar una clasificación interna más detallada de las pérdidas.

Las Instituciones deberán corresponder los eventos de riesgo operacional señalados en el párrafo anterior con las líneas de negocio contenidas en la sección III del presente Anexo.

Sección I.

Consideraciones para la recolección de datos internos de eventos de pérdida por riesgo operacional

1. La Institución debe contar, dentro de sus objetivos, lineamientos y políticas para la Administración Integral de Riesgos, con criterios preestablecidos y documentados bajo los cuales sea posible identificar eventos de pérdida por riesgo operacional de las distintas líneas de negocio de la entidad e incorporarlos a la base de datos de eventos de pérdida por riesgo operacional.

2. En la constitución de la base de datos de eventos de pérdida por riesgo operacional, la Institución deberá identificar eventos simples, es decir aquellos que generan un solo impacto en la contabilidad, así como eventos múltiples que generen varios impactos en la contabilidad. Asimismo, identificará eventos que afecten a una sola o múltiples líneas de negocio.

El área o unidad de negocio en la cual se genere el evento de pérdida, debe contar con evidencia del seguimiento que se le de a cada uno de los eventos de pérdida por riesgo operacional. Dicho seguimiento se podrá dar por concluido si no se presentan durante los siguientes 12 meses posteriores a su ocurrencia, eventos subsecuentes.

En el caso que se presenten eventos subsecuentes conforme a lo establecido en el párrafo anterior, se les deberá dar seguimiento junto con el evento que les dio origen, y se podrá dar por concluido el seguimiento cuando no haya nuevos eventos subsecuentes en un período de 12 meses.

En caso de presentarse diversas pérdidas por causa de un evento en común, éstas deberán agregarse y asociarse a un mismo evento. Para efectos de lo anterior, se podrá asociar cada registro en la base de datos con un mismo evento para identificar la totalidad de sus consecuencias.

Cuando haya un evento subsecuente que se presente después del periodo de referencia, se deberá considerar como si se tratara de un nuevo evento.

Para efectos de este numeral, no se considerarán como eventos subsecuentes a las recuperaciones.

3. La base de datos de eventos de pérdida por riesgo operacional se deberá actualizar de forma trimestral. La Institución podrá corresponder todos sus procesos a sus datos internos de pérdida, y deberá corresponder sus datos internos de pérdida a sus riesgos y líneas de negocio.

4. La Institución deberá establecer un umbral mínimo adecuado de pérdidas brutas, es decir, antes de cualquier recuperación, para la recopilación de datos internos de pérdida para posteriormente ser incorporados a la base de eventos de pérdida por riesgo operacional. El umbral que se considere adecuado podrá variar dependiendo de cada línea de negocio y/o tipo de evento, pero deberá estar considerado dentro de los manuales, objetivos, lineamientos y políticas para la Administración Integral de Riesgos de cada Institución.

La base de datos debe incorporar a todos los eventos de pérdida por riesgo operacional que surjan en la entidad, así como los montos de pérdida asociados conforme al umbral establecido en el párrafo anterior. El banco deberá ser capaz de justificar que las actividades o posiciones excluidas, tanto de forma individual como conjunta, no tendrían un efecto significativo sobre las estimaciones generales de riesgo.

5. Además de la información sobre pérdidas brutas, el banco deberá recopilar información sobre la fecha del evento así como cualquier recuperación con respecto a las cantidades brutas de las pérdidas.

6. Asegurar que en los eventos de pérdida donde se involucre un proceso legal, se agreguen a las pérdidas, los gastos legales directamente imputables a dichos eventos de pérdida, no así los gastos propios de la operación jurídica. Los gastos directamente imputables serán los que se generen a partir del evento de pérdida, tales como honorarios, viáticos, etcétera.

7. Las pérdidas por riesgo operacional que estén relacionadas con el riesgo de crédito y que históricamente se hayan incluido en las bases de datos de riesgo de crédito de los bancos (por ejemplo, fallos en la gestión de la garantía) continuarán recibiendo el tratamiento del riesgo de crédito a efectos del cálculo del capital regulatorio. En consecuencia, tales pérdidas no estarán sujetas a un requerimiento de capital por riesgo operacional.

8. Las pérdidas operacionales relacionadas con el riesgo de mercado se consideran como riesgo operacional a efectos de cálculo de capital regulatorio, por lo que estarán sujetas a la exigencia de capital por riesgo operacional.

Sección II.

Categorías de tipos de eventos de pérdida por riesgo operacional

1. **Fraude Interno**: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar regulaciones, leyes o políticas empresariales (excluidos los eventos de diversidad / discriminación) en las que se encuentra implicada, al menos, una parte interna a la empresa. Dentro de esta categoría se encuentran tres clases de eventos de pérdida las cuales son:

a) Actividades no Autorizadas

- Uso indebido de facultades y poderes
- Operaciones no reveladas (intencionalmente)
- Operaciones no autorizadas (con pérdidas pecuniarias)
- Valoración errónea de posiciones (intencional)

b) Hurto y Fraude Internos

- Fraude / fraude crediticio / depósitos sin valor
- Hurto / extorsión / malversación / robo
- Apropiación indebida de activos
- Destrucción dolosa de activos
- Falsificación Interna
- Utilización de cheques sin fondos

- Contrabando
- Apropiación de cuentas, de identidad, entre otros.
- Incumplimiento / evasión de impuestos (intencional)
- Soborno / cohecho
- Abuso de información privilegiada (no a favor de la empresa)

c) Seguridad de los Sistemas

- Vulneración de sistemas de seguridad
- Daños por ataques informáticos
- Robo de información (con pérdidas pecuniarias)
- Utilización inadecuada de claves de acceso y/o niveles de autorización

2. **Fraude Externo**: Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte de un tercero. En esta categoría se encuentran dos clases de eventos de pérdida:

a) Hurto y Fraude Externos

- Hurto / robo / estafa / extorsión /soborno
- Falsificación Externa / Suplantación de personalidad
- Utilización fraudulenta de cheques
- Uso y/o divulgación de información privilegiada
- Espionaje industrial
- Contrabando

b) Seguridad de los Sistemas

- Vulneración de sistemas de seguridad
- Daños por ataques informáticos
- Robo de información (con pérdidas pecuniarias)
- Utilización inadecuada de claves de acceso y/o niveles de autorización

3. **Relaciones Laborales y Seguridad en el Puesto de Trabajo**: Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con la diversidad / discriminación. Dentro de esta categoría se encuentran las siguientes clases de eventos de pérdida:

a) Relaciones Laborales

- Cuestiones relativas a la remuneración, prestaciones sociales, extinción de contratos y recursos humanos
- Organización laboral

b) Higiene y Seguridad en el Trabajo

- Responsabilidad en general
- Casos relacionados con las normas de higiene y seguridad en el trabajo
- Indemnización a los trabajadores

c) Diversidad y Discriminación

- Todo tipo de discriminación
- Invasión a la intimidad y/o acoso

4. **Clientes, Productos y Prácticas Empresariales**: Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto. Las clases de eventos de pérdida que se encuentran dentro de esta categoría son:

a) Adecuación, Divulgación de Información y Confianza

- Abusos de confianza / incumplimiento de pautas
- Aspectos de adecuación / divulgación de información
- Quebrantamiento de la privacidad de información sobre clientes minoristas
- Quebrantamiento de privacidad
- Ventas agresivas
- Confusión de cuentas
- Abuso de información confidencial
- Responsabilidad del prestamista

b) Prácticas Empresariales o de Mercado Improcedentes

- Prácticas restrictivas de la competencia
- Prácticas comerciales / de mercado improcedentes
- Manipulación del mercado
- Abuso de información privilegiada (a favor de la empresa)
- Actividades no autorizadas
- Lavado de dinero

c) Productos Defectuosos

- Defectos del producto
- Error de los modelos

d) Selección, Patrocinio y Riesgos

- Ausencia de investigación a clientes conforme a las directrices

e) Actividades de Asesoramiento

- Litigios sobre resultados de las actividades de asesoramiento

5. **Desastres naturales y otros acontecimientos**: Pérdidas derivadas de daños o perjuicios activos materiales como consecuencia de desastres naturales u otros acontecimientos. Dentro de esta categoría sólo existe una clase de evento de pérdida la cual se llama:

a) Desastres y otros Acontecimientos

- Pérdidas por desastres naturales
- Pérdidas por causas externas (terrorismo, vandalismo)

6. **Incidencias en el Negocio y Fallos en los Sistemas**: Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas. De igual modo, en esta categoría sólo existe una clase de evento de pérdida la cual se define como:

a) Sistemas

- Hardware
- Software
- Telecomunicaciones
- Interrupción / incidencias en el suministro

7. **Ejecución, Entrega y Gestión de Procesos:** Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores. Esta categoría está compuesta por seis clases de eventos de pérdida, los cuales son los siguientes:

a) Recepción, Ejecución y Mantenimiento de Operaciones

- Comunicación defectuosa
- Errores de introducción de datos, mantenimiento o descarga
- Incumplimiento de plazos o de responsabilidades
- Ejecución errónea de modelos / sistemas
- Error contable / atribución a entidades erróneas
- Errores en otras tareas
- Fallo en la entrega

- Fallo en la gestión del colateral
- Mantenimiento de datos de referencia

b) Seguimiento y Presentación de Informes

- Incumplimiento de la obligación de informar
- Inexactitud de informes externos (con generación de pérdidas)

c) Aceptación de Clientes y Documentación

- Inexistencia de autorizaciones / rechazos de clientes
- Documentos jurídicos inexistentes / incompletos
- Errores en los contratos (diseño deficiente, errores tipográficos, cláusulas erróneas, entre otros.)

d) Gestión de Cuentas de Clientes

- Acceso no autorizado a cuentas
- Registros incorrectos de clientes (con generación de pérdidas)
- Pérdida o daño de activos de clientes por negligencia

e) Pérdidas derivadas del incumplimiento de la Normativa

- De la normativa fiscal.
- De la normativa bancaria
- De otras normas.

f) Contrapartes Comerciales

- Fallos de contrapartes distintas de clientes
- Otros litigios con contrapartes distintas de clientes
- Errores en los contratos (diseño deficiente, errores tipográficos, cláusulas erróneas, entre otros.)

g) Distribuidores y Proveedores

- Subcontratación
- Litigios con distribuidores
- Errores en los contratos (diseño deficiente, errores tipográficos, cláusulas erróneas, entre otros.)

Sección III.

Definición de las Líneas de Negocio

Para efectos del presente Anexo, las Instituciones deberán dividir sus actividades en ocho líneas de negocio de acuerdo con la tabla siguiente:

Nivel 1	Nivel 2	Grupos de Actividades
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, bursatilizaciones, servicio de estudios, deuda, acciones, sindicaciones, ofertas públicas iniciales, colocaciones privadas en mercados secundarios.
	Finanzas de Administraciones locales / públicas	
	Banca de inversión	
	Servicios de consultoría	
Negociación y ventas	Compras y ventas	Renta fija, renta variable, divisas, crédito, posiciones propias en valores, préstamo de valores, reportos y operaciones similares, operaciones financieras derivadas, intermediación y servicios adicionales, y deuda.
	Formación de mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Créditos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarias
	Banca privada o patrimonial	Créditos y depósitos de clientes de banca privada o patrimonial, servicios bancarios, fideicomisos y testamentarías, y asesoría de inversión.
	Servicios de tarjetas	Tarjetas de empresa / comerciales, de marca privada y minoristas
Banca comercial	Banca comercial	Financiamiento de proyectos, bienes raíces, financiamiento de exportaciones, financiamiento comercial, factoraje, arrendamiento financiero, préstamo, garantías, letras de cambio.
Pago y liquidación	Clientes externos	Pagos y cobranzas, transferencia de fondos, compensación y liquidación.
Servicios de agencia	Custodia	Depósitos en custodia, certificados de depósito, operaciones de sociedades (clientes) para préstamo de valores.
	Agencia para empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrados, abiertos, participaciones accionarias.

	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable
Intermediación minorista / operaciones de corretaje al menudeo	Intermediación minorista / operaciones de corretaje al menudeo	Recepción, registro, ejecución y asignación.

Para la asignación de las líneas de negocio antes mencionadas, las Instituciones observarán los siguientes principios:

a) Todas las actividades bancarias deberán asignarse entre las ocho líneas de negocio de nivel 1 de forma que a cada una de las actividades le corresponda una sola línea de negocio y no permanezca ninguna actividad sin asignar. Esto requiere que la Institución pueda demostrar que cuenta con información y procedimientos sistemáticos de asignación de los ingresos netos, lo que conlleva la asignación tanto de los ingresos como de los costos financieros.

b) Cualquier actividad bancaria o no bancaria que no pueda asignarse con facilidad al marco de las líneas de negocio, pero que represente una función auxiliar a una actividad incluida en dicho marco, deberá ser asignada a la línea de negocio a la que preste apoyo. Si la actividad auxiliar presta apoyo a más de una línea de negocio, deberá utilizarse un criterio de asignación objetivo y consistente.

c) La asignación de actividades a líneas de negocio deberá ser coherente con las definiciones de líneas de negocio utilizadas en los cálculos de capital regulatorio en otras categorías de riesgo (es decir, riesgo de crédito y de mercado). Cualquier desviación de este principio, deberá estar justificada y documentada con claridad por las Instituciones.

d) El proceso de asignación de las actividades a las líneas de negocio, deberá documentarse con claridad. En particular, las definiciones por escrito de las líneas de negocio, deberán ser suficientemente claras y detalladas para que la asignación de líneas de negocio realizada, pueda ser reproducida por terceros. Entre otras cosas, la documentación deberá argumentar con claridad cualquier excepción o salvedad existente y deberá conservarse.

e) La Dirección General de las Instituciones será responsable de la política de asignación, misma que deberá ser sometida a la aprobación del Consejo.

f) El proceso de asignación a líneas de negocio deberá someterse a una revisión independiente al área que la elabore, pudiendo ser interna o externa.

1.2.1 Disposiciones de Carácter General aplicables a las Instituciones de Crédito. Circular única (CUB)

Capítulo VI

Controles Internos

Sección Primera

Del objeto

Artículo 140 - El presente Capítulo tiene por objeto establecer los objetivos del Sistema de Control Interno y los lineamientos a los que deberán apegarse las Instituciones en su implementación, así como la participación que al respecto comprenderá a los órganos de administración y vigilancia de dichas sociedades.

Sección Segunda

Del Consejo

Artículo 141.- El Consejo, a propuesta del Comité de Auditoría deberá conocer y, en su caso, aprobar los objetivos del Sistema de Control Interno y los lineamientos para su implementación.

Artículo 142.- El Consejo, una vez aprobados los objetivos del Sistema de Control Interno y los lineamientos para su implementación, deberá en el ámbito de su competencia:

I. Aprobar, al menos, hasta el segundo nivel jerárquico la estructura orgánica de la Institución, presentada por el director general, así como las eventuales modificaciones hasta ese nivel, habiendo escuchado el Consejo previamente la opinión del comité de recursos humanos y desarrollo institucional, en el caso de las instituciones de banca de desarrollo.

II. Analizar mediante reportes elaborados al efecto por la Dirección General y el Comité de Auditoría, que el Sistema de Control Interno esté funcionando adecuadamente.

III. Aprobar, en su caso, el código de conducta de la Institución, así como promover su divulgación y aplicación en coordinación con la Dirección General.

El código de conducta deberá contener normas acordes con la legislación vigente y demás disposiciones legales aplicables, con las sanas prácticas y usos bancarios. Adicionalmente, deberá incorporar lineamientos que detallen las obligaciones relativas a la confidencialidad de la información de la Institución, otras entidades o su clientela.

V. Revisar, por lo menos anualmente, los objetivos del Sistema de Control Interno y los lineamientos para su implementación, así como evaluar las funciones del Comité de Auditoría y de la Dirección General al respecto.

VI. Determinar las acciones que correspondan a fin de subsanar las irregularidades que sean de su conocimiento e implementar las medidas correctivas correspondientes.

(151) VII. Aprobar el Plan de Continuidad de Negocio, así como sus modificaciones, que le presente el Comité de Auditoría.

Para el caso de las instituciones de banca múltiple, la totalidad de los asuntos que conforme a las presentes disposiciones deben ser autorizados por el Consejo, serán presentados para tal efecto directamente por el Comité

de Auditoría. Tratándose de las instituciones de banca de desarrollo, se presentarán por conducto del propio comité o del director general, según determine el Consejo.

Sección Sexta

De la Dirección General

Artículo 164.- La Dirección General será la responsable de la debida implementación del Sistema de Control Interno; lo anterior, en el ámbito de las funciones que correspondan a dicha dirección.

En la implementación deberá procurarse que su funcionamiento sea acorde con las estrategias y fines de la Institución, aplicando las medidas preventivas y correctivas necesarias para subsanar cualquier deficiencia detectada.

Sección Séptima

De las funciones de Contraloría Interna

Artículo 166.- Las Instituciones deberán desarrollar permanentemente las funciones de Contraloría Interna que consistirán, por lo menos, en el desempeño cotidiano y permanente de las actividades relacionadas con el diseño, establecimiento y actualización de medidas y controles que:

I. Propicien el cumplimiento de la normatividad interna y externa aplicable a la Institución en la realización de sus operaciones.

II. Permitan que la concertación, documentación, registro y liquidación diaria de operaciones, se realicen conforme a las políticas y procedimientos establecidos en los manuales de la Institución y en apego a las disposiciones legales aplicables.

III. Propicien el correcto funcionamiento de los sistemas de procesamiento de información conforme a las políticas de seguridad, así como la elaboración de información completa, correcta, precisa, íntegra, confiable y oportuna, incluyendo aquélla que deba proporcionarse a las autoridades competentes, y que coadyuve a la adecuada toma de decisiones.

IV. Tengan como finalidad el verificar que los procesos de conciliación entre los sistemas de operación y contables sean adecuados.

(16) V. Preserven la seguridad de la información generada, recibida, transmitida, procesada o almacenada en los sistemas informáticos y de telecomunicaciones de las instituciones de crédito, así como la aplicación de las medidas preventivas y correctivas necesarias para subsanar cualquier deficiencia detectada en materia de seguridad informática.

(149) Último párrafo.- Derogado.

Artículo 167.- Las funciones de Contraloría Interna que, en principio, corresponden a la Dirección General de la Institución, podrán ser asignadas a un área específica o, en su caso, a personal distribuido en varias áreas, pudiendo llegar, incluso, a ser independientes jerárquicamente de la Dirección General; sin embargo, en ningún caso podrán atribuirse al personal integrante del área de Auditoría Interna a que hace referencia el Artículo 159 de las presentes disposiciones, o a personas o unidades que representen un conflicto de interés para su adecuado desempeño. Las citadas funciones de Contraloría Interna, así como su asignación al interior de la Institución, deberán estar documentadas en manuales.

El personal responsable de las funciones a que hace referencia el presente Artículo, deberá entregar un reporte de su gestión, cuando menos semestralmente, al auditor interno o bien al Comité de Auditoría, así como al director general.

Artículo 168.- Las Instituciones deberán observar lo establecido en los Artículos 166 y 167 anteriores, sin perjuicio de otras funciones específicas que se señalen en la demás regulación que les sea aplicable.

Sección Novena

Disposiciones finales

Artículo 169.- Las Instituciones deberán documentar en manuales, las políticas y procedimientos relativos a las operaciones propias de su objeto, las cuales deberán guardar congruencia con los objetivos y lineamientos del Sistema de Control Interno, así como describir las funciones de Contraloría Interna de la Institución.

Los objetivos del Sistema de Control Interno y los lineamientos para su implementación, así como sus modificaciones, al igual que los manuales referidos en el párrafo anterior, deberán hacerse del conocimiento de los consejeros, directivos, empleados y personal de la Institución, de acuerdo a su ámbito de competencia y serán la base para la operación de la misma.

Artículo 170.- El código de conducta, en su caso, elaborado por la Dirección General y que el Comité de Auditoría propondrá para aprobación del Consejo, establecerá un marco autorregulatorio que norme la conducta de los directivos y demás personal al interior de la

Institución, con otras entidades y la clientela, así como la conducta de sus consejeros acorde con las actividades y funciones de estos últimos. Las Instituciones deberán hacer del conocimiento de sus consejeros, directivos y demás personal el código de conducta que, en su caso emitan, además de comunicar a las personas relacionadas con su operación, que la conducta del referido personal se rige por el mencionado código.

(147) **Artículo 171**.- Las facultades que de acuerdo con lo dispuesto en las presentes disposiciones, corresponden al Consejo, a los comisarios, al Comité de Auditoría y al director general, serán ejercidas sin perjuicio de otras que se contengan en las demás disposiciones legales que les sean aplicables a las Instituciones.

(148) **Artículo 171 Bis**.- Los servidores públicos de las instituciones de banca de desarrollo deberán presentar sus denuncias por escrito ante el titular del órgano interno de control de la institución en la que prestan sus servicios, cuando en ejercicio de sus funciones llegaran a advertir actos u omisiones de cualquier otro funcionario de la institución, que pudiera constituir responsabilidad administrativa en los términos de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.

Artículo 172.- La Comisión podrá requerir a las Instituciones la información que en ejercicio de sus facultades estime necesaria, relacionada con estas disposiciones

1.2.3 Ley Sarbanes Oxley

Artículo (404) La novedad que introduce el artículo 404 de la Ley SARBANES-OXLEY es la exigencia de redactar un informe de control interno al final de cada ejercicio fiscal. Dentro de este informe de control interno se establece la responsabilidad del equipo directivo de tener una estructura de control interno adecuada. Anteriormente esta exigencia no existía y ahora el equipo directivo es responsable ante posibles fraudes. Por ejemplo, en el caso Enron no existía control interno declarado y los movimientos de ingeniería financiera entre filiales de Enron en paraísos fiscales y la central en EEUU quedaban sin ser vigilados ni controlados, de lo cual un caso extremo fue lo ocurrido en el año 2001 anteriormente mencionado.

Este informe de control interno es revisado y evaluado por la empresa auditora, que certificara la anterior evaluación hecha por la comisión de los directivos encargados de realizar dicho informe.

(Sarbanes-Oxley Act, 2002) Ley SARBANES-OXLEY, Artículo 404 EVALUACION DE LA GERENCIA DE LOS CONTROLES INTERNOS.

a) REGULACIONES REQUERIDAS. La Comisión prescribirá regulaciones requiriendo que cada informe anual {…} contenga un informe de control interno, el cual: 1. determinará la responsabilidad de la gerencia por establecer y mantener una estructura adecuada de control interno y los procedimientos, 2. contendrá una evaluación, al final del año fiscal más reciente del emisor, de la estructura de control interno y los procedimientos para la información financiera.

b) EVALUACIÓN E INFORME DEL CONTROL INTERNO. Con respecto a la evaluación del control interno requerido por el inciso (a), cada firma de contabilidad pública que prepara o emite el informe de auditoría para el emisor testificará e informará sobre la evaluación hecha por la gerencia de emisor. Una testificación bajo esta subsección será hecha de acuerdo con las normas para compromisos de testificación emitidas o adoptadas por la Junta. La testificación no estará sujeta a un compromiso separado.

Artículo (906)

La Ley establece una modificación en el código penal de los Estados Unidos. El artículo 906 de la Ley Sarbanes-Oxley establece una nueva disposición en el código penal donde se especifican las multas y penas para los responsables legales de infracción de los requerimientos expuestos en la Ley SARBANES-OXLEY.

El responsable “será multado con no más de 1.000.000 $ o encarcelado por no más de 10 años, o ambos” en el caso de certificar el informe periódico sabiendo que no cumple con todos los requerimientos de la ley”.

El responsable “será multado con no más de 5.000.000 $ o encarcelado por no más de 20 años, o ambos” en el caso de certificar el informe periódico intencionadamente sabiendo que no cumple con todos los requerimientos de la ley”.

Esta sección del código penal que ha introducido la Ley Sarbanes-Oxley es toda una novedad, porque específica la pena del tipo de delito financiero en cuestión, y endurece las penas anteriormente existentes para este tipo de delitos.

Además de especificar la pena, también aclara sobre quién recae la responsabilidad, a diferencia de lo ocurrido con el caso de los escándalos de Enron y otras compañías donde la responsabilidad penal no fue fácil de establecer en unos culpables claros.

2. EN BUSCA DE UN MODELO DE GESTIÓN

Fortalezas

- La confianza en los empleados es, en el negocio bancario y en un sentido amplio imprescindible, sin embargo, la complejidad añadida con el tamaño de las organizaciones demanda el uso complementario de herramientas apropiadas.
- Cada área de negocio o de apoyo deba gestionar su propio riesgo operacional. No se le puede quitar al dueño del negocio la responsabilidad sobre su cuenta de resultados.
- Se identificaran ineficiencia de los controles por medio de muestras y de evaluaciones realizadas los cuales determinaran si se requiere un control compensatorio.
- Es importante que la auditoría continúe realizando su trabajo. Lo prudente es que su labor no sea sustitutiva de la del gestor, sino complementaria.
- Son importantes los apoyos recibidos de otras áreas relacionadas.

Modelos organizacionales

- Se cuenta con tres modelos organizacionales de gestión:
    - Apoyado en una unidad de gestión del riesgo operacional y control interno.
    - Un segundo modelo tiene funciones dedicadas pero soportadas en forma descentralizada.
    - El que se lleva a cabo a través de la función del liderazgo de la auditoría interna.
- La elección de alguno de ellos es determinada por la cultura de la organización más por el tipo de institución.
- El modelo que está ganando la mayor aceptación es el primero. Es encabezado por un responsable que reporta a la figura encargada de la función global de riesgos, complementada por un equipo dedicado a dar soporte a las unidades de negocio.

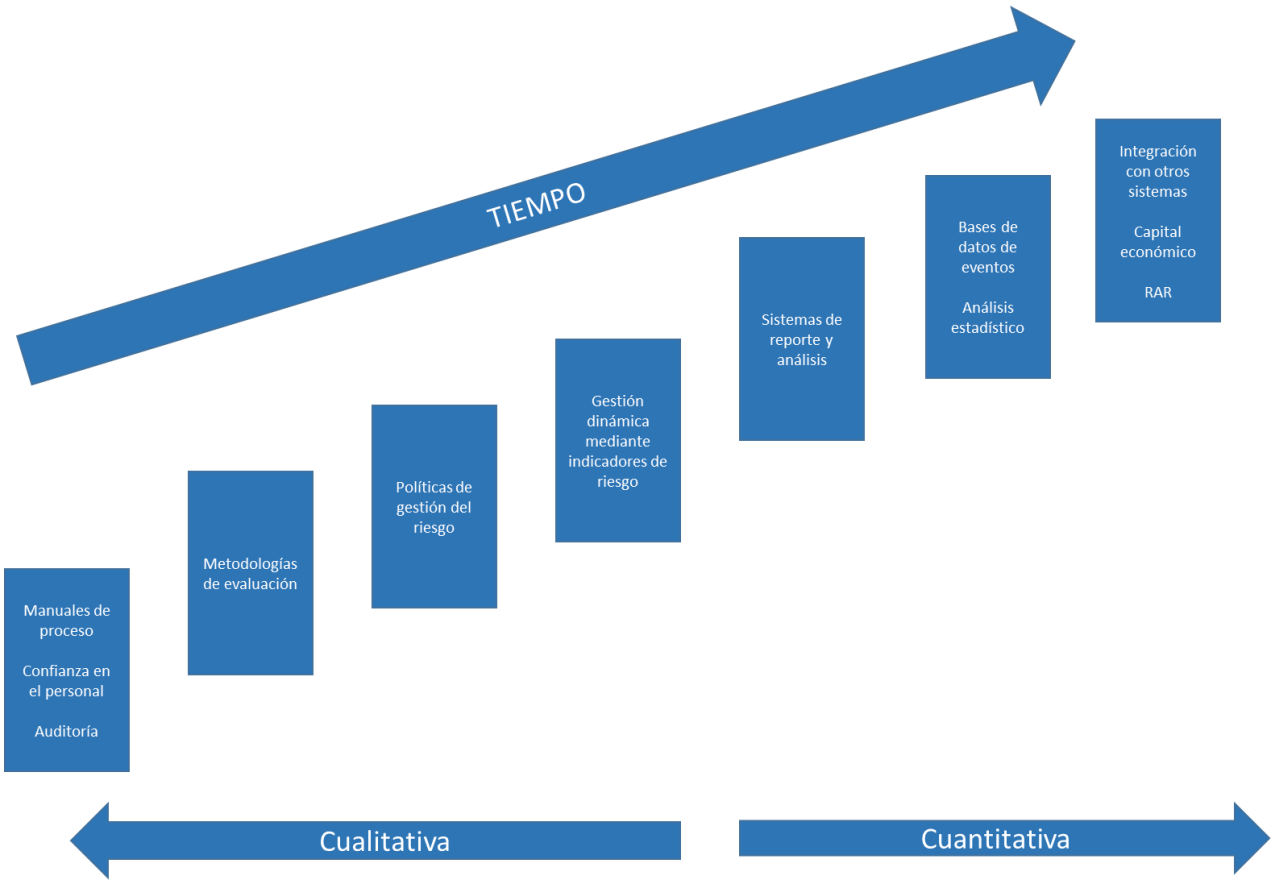
Competencias de los coordinadores de riesgo operacional y control interno

- Depuración de textos y homologación de términos
    - En preparación a la evaluación de los riesgos, el coordinador de la unidad revisará y enmendará, cuando sea necesario, las redacciones de los textos descriptivos de los factores de riesgos identificados n las sesiones de lluvia de ideas

- Clasificación/etiquetado de los riesgos identificados
    - Asimismo el coordinador de la unidad asignará cada factor de riesgo identificando la categoría de riesgo que mejor se le ajusta, de acuerdo a la taxonomía en uso por la institución.
- Preparación de los materiales para el ejercicio colegiado de evaluación
    - Cumplimentación de las plantillas/formas de registro de la evaluación
- Convocatoria al personal designado para participar en la evaluación de los riesgos identificados previamente y conducción de las sesiones necesarias para completar el ejercicio.
- Conducción de las sesiones de evaluación
    - El coordinador de riesgo operacional conducirá, individual o colectivamente, sesiones de evaluación de los riesgos con la plantilla elegida al efecto, asegurando el arribo a consenso respecto de la estimación de los valore de frecuencia e ipacto asignables a cada riesgo.
- Validación y suscripción de las evaluaciones
    - El coordinador validará el riesgo de las estimaciones realizadas en las plantillas formas (tarjetas de puntuación) elaboradas exprofeso, asegurando sean suscritas en forma autógrafa por los participantes en el ejercicio, con fines de testimonio y auditoría.
- Registro de los riesgos identificados y sus evaluaciones en la plataforma de riesgo operacional.
    - El coordinador de la unidad realizará el registro en la plataforma el sistema de riesgo operacional de todos los datos recogidos durante los ejercicios de identificación y evaluación de los riesgos de su unidad.
- Identificación, registro y seguimiento de controles, planes de mitigación en la plataforma de riesgo operacional
- Identificación y registro de incidentes contabilizables en su unidad de adscripción y validación de importes con el área contable.
- Conducción de los ejercicios de evaluación de escenarios.
    - El coordinador hará acopio de la transformación relevante de evaluaciones de riesgo, indicadores de seguimiento, datos de pérdida y datos externos de la industria respecto de los riesgos de su unidad con fines de elaboración de escenarios para las estimaciones de capital por riesgo operacional.

- Explotación de los contenidos de la plataforma de riesgo operacional para su unidad.

EVOLUCIÓN DE LA GESTIÓN DEL RIESGO OPERACIONAL



Competencias de la unidad de gestión de riesgo operacional

La Unidad de Gestión de Riesgo Operacional debe:

- Tener competencia profesional en materia de administración de riesgo operacional
- Tener capacidad decisora en los teas de la agenda de riesgo operacional
- Tener independencia de los órganos de control de las áreas de operaciones, tecnologías y legales y de cualquier función que dé lugar a la existencia de conflictos de interés

Situaciones especiales

- Funciones de control
    - El modelo de tres líneas de defensa

        - La línea de negocio
        - La figura de control interno
        - La auditoría
    - Una vertiente cada vez más en boga es la de alojar a las funciones de riesgo operacional y de control interno bajo una misma figura
- Riesgo Operacional
    - Hay entidades y reguladores que consideran o no al riesgo operacional como riesgo financiero. Quienes si le consideran riesgo financiero son proclives a ubicarle, junto con los de mercados y crédito bajo la misma unidad. Entre quienes no, los modelos organizativos varían entre entidades.

Quienes son los responsables de la gestión del riesgo operacional es la alta dirección, donde alguien tiene la visión y el interés de incentivar un nuevo enfoque. Un enfoque adicional es la percepción de incremento en los riesgos operacionales debido al crecimiento en los servicios financieros y a la difusión de los riesgos de crédito y mercado. Otro factor importante es la reacción ante eventos mayores de pérdida ocurridos ya sea internamente o a terceros.

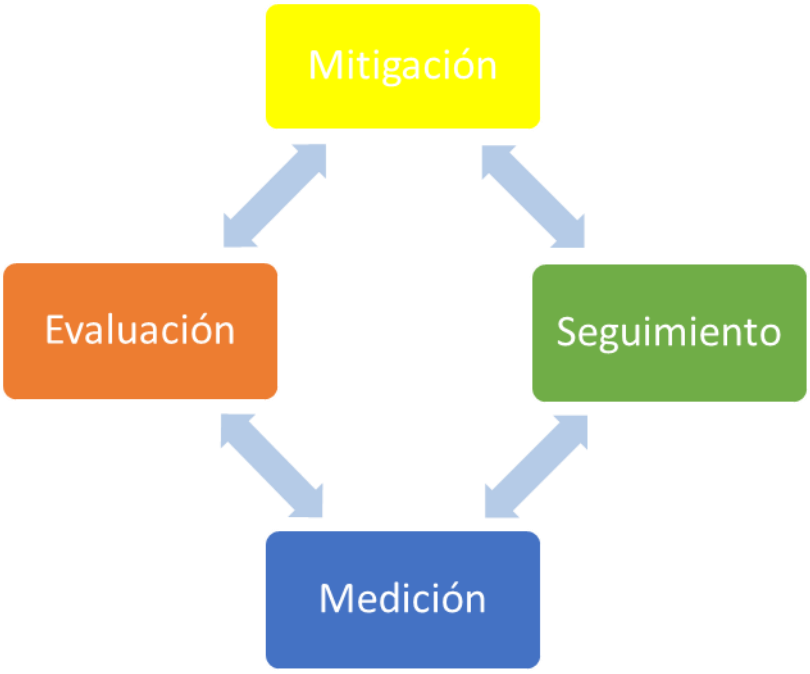
La atención a la gestión global de los riesgos tras el desarrollo de procesos para la gestión de los riesgos de mercado y de crédito, los operacionales parecen ser el siguiente paso lógico. Y la atención reguladora, la industria responde y adelanta expectativas.

Competencias de los coordinadores de riesgo operacional

Para facilitar la identificación de los riesgos y sobre todo para asegurar que se ha sido exhaustivo en el ejercicio es preciso, primeramente, identificar los procesos que describe el quehacer de la institución. El funcionario responsable de cada área de común acuerdo con el coordinador de riesgo operacional, seleccionará al personal que habrá de participar en la identificación de los riesgos y en su evaluación, pudiendo no ser los mismos, el cual harpa acopio de la documentación descriptiva de los proceso de la unidad.

El coordinador de riesgo operacional organizará sesiones con el personal elegido con el objetivo de identificar colectivamente los factores de riesgo presentes en cada uno de los procesos de la unidad. Está encargado de conducir sesiones cuyo objetivo será asegurar la integridad en el inventario de los riesgos, evitando los sesgos propios de los ejercicios

colectivos de opinión. El coordinador también llevará el registro de los factores identificados y elaborará las minutas de las sesiones con fines de auditoría.



Para elaborar la gestión de riesgo operacional y de control interno se debe tomar en cuenta las siguientes herramientas, las cuales tendrán que estar basadas en metodologías documentadas dentro de sus manuales internos, los cuales son:

- Diagrama de procesos por área
- Identificación de riesgos y controles
- Matriz de Riesgos y controles
- Matriz de eventos de pérdida
- Matriz de calificación de controles
- Mapas de calor

3. LA DIAGRAMACIÓN DE PROCESOS

Siendo los procesos el centro de la atención en la búsqueda de los riesgos operacionales, son éstos un punto de partida para la identificación de los factores de riesgo.

Definición del Mapa de Procesos

- Un diagrama o mapa de proceso es la representación gráfica de la secuencia lógica de las actividades que conforman dicho proceso.
- Tradicionalmente el mapeo debe realizarse con un enfoque de procesos y no de áreas.
- Conjunto de las fases sucesivas de un fenómeno natural o de una operación artificial.
- Secuencia de acciones sistemáticas repetitivas mediante las cuales los insumos iniciales (entradas) se transforman en productos o servicios finales (salidas)

Las ventajas de realizar un diagrama de flujo es el tener la visualización gráfica de:

- La secuencia lógica de las actividades que conforman un proceso.
- La interconexión de los procesos de la institución relacionados entre sí.
- La interconexión de los procesos con entidades externas y sistemas, entre otros.
- Permite la inclusión de las propiedades asociadas a cada actividad del proceso
- La definición de las propiedades a levantar por cada actividad, varía dependiendo del objetivo.

El funcionamiento de una empresa está sustentado en el conjunto de procesos enlazados. Describen el quehacer de los individuos, equipos y la infraestructura implicados en las funciones representativas de la actividad de una empresa u organización.
Es posible alinear casa proceso son los objetivos estratégicos de la empresa

Se debe designar a los dueños de los procesos de los cuales recaerá la responsabilidad de la autorización del documento, generalmente son los Gerentes del área mapeada, los cuales indicaran, cuales son los procesos críticos o de alto impacto y que tendrán importancia estratégica para el Banco.

Se puede contar con una metodología básica o sofisticada como se requiera, pero lo mínimo requerido de información en el documento debe ser lo siguiente:

- Definir número de actividades en cada flujo
- área en donde se ejecuta la actividad o actividades
- Puesto de quien hace la actividad y área

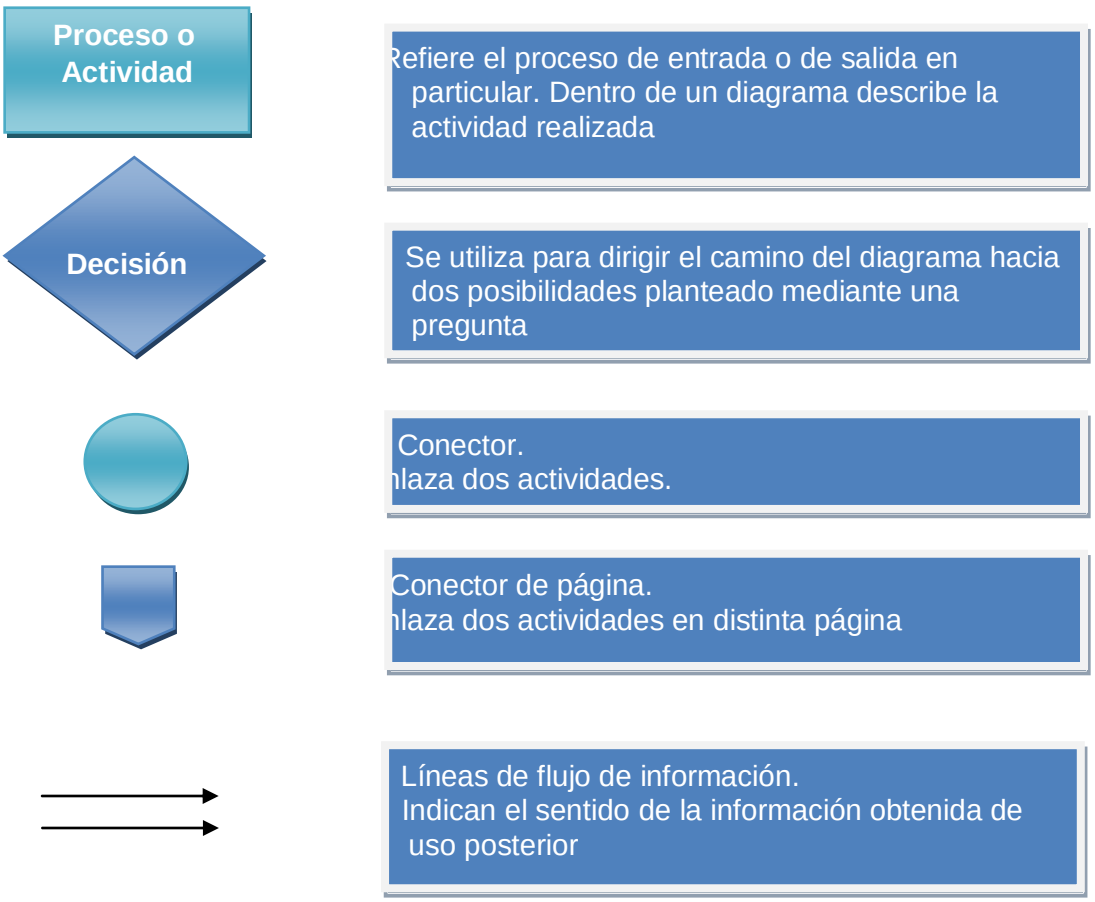
- Entradas y salidas del proceso (Procesos relacionados y/o áreas)

Los elementos con los que debe contar un proceso son:

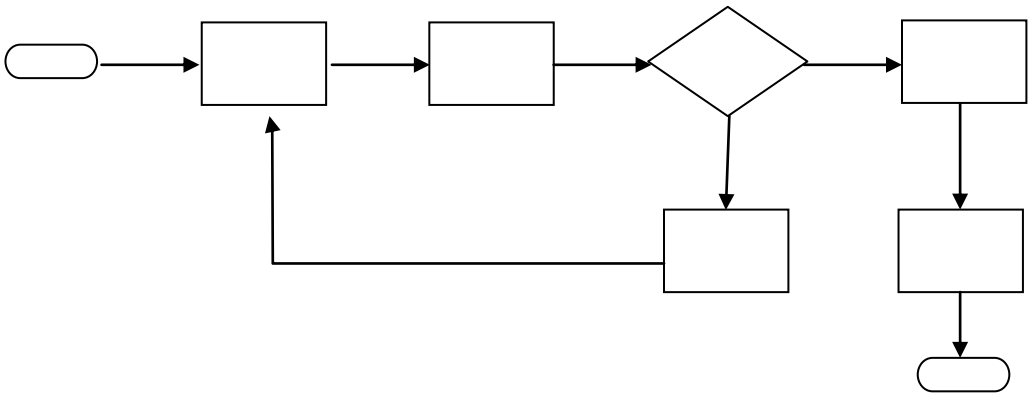
- 1. Identificar el objetivo del proceso
- 2. Identificar el “cliente” (interno o externo)
- 3. Identificar el desde y el hasta (alcance)
- 4. Identificar las entradas
- 5. Definir los sub procesos, actividades, etapas, etc.(niveles de detalle)
- 6. Describirlos (presentando las interrelaciones)
- 7. Identificar las salidas

Adicionalmente y cuando la metodología sea más sofisticada se podrá agregar sistemas relacionados, documentos resultantes de la actividad realizada, entre otros.

En cuanto a la simbología utilizada, se pueden tener distintos criterios y símbolos para realizar la diagramación, a continuación se presentan los símbolos más representativos en la diagramación de procesos:



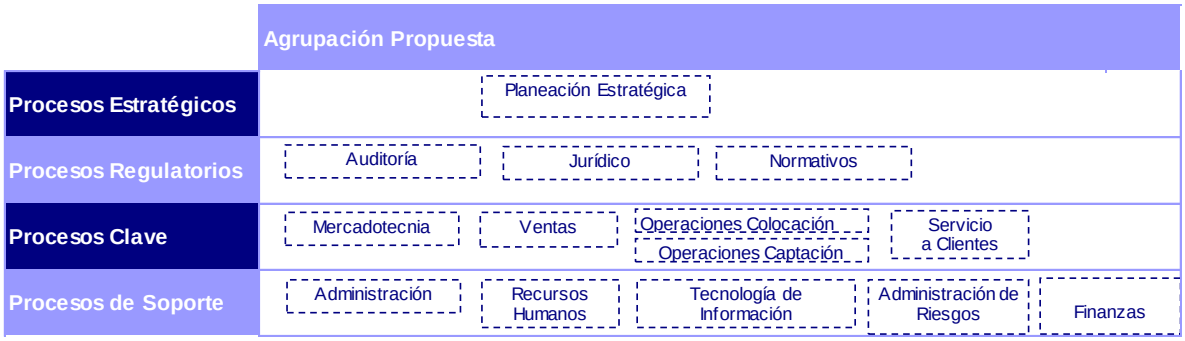
La herramienta que se debe utilizar para realizar la diagramación de los procesos es VISIO ya que es una herramienta que trabaja bajo ambiente windows y es amigable, además que las métricas capturadas en los mapas pueden ser exportadas a Excel para su explotación mediante filtros y tablas dinámicas.



Los procesos se deben mapear de acuerdo a la siguiente clasificación:

	Objetivos
Procesos Estratégicos	Introducen las acciones tácticas de la organización, producen y actualizan el rumbo de la organización con apego a las directrices del consejo del grupo.
Procesos Regulatorios	Monitorean el cumplimiento a los lineamientos que establecen las entidades internas y externas.
Procesos Clave	Diseñan, producen y entregan los productos al cliente.
Procesos de Soporte	Encargados de mantener el correcto funcionamiento del resto de los procesos.

La propuesta realizada para el banco en cuanto a la clasificación de los procesos es la siguiente:



4. IDENTIFICACION DE RIESGOS

Para tener una adecuada gestión del riesgo operacional se debe seguir con un esquema de identificación, evaluación, mitigación y monitoreo, para lo cual se necesitan diagramas de flujo que permitan identificar los riesgos asociados y controles para iniciar con la gestión de los mismos.

La descripción del riesgo debe contener la causa y el efecto ya que las causas definen el origen del riesgo y permiten identificar la esencia de lo que se considera como riesgo operacional y su clasificación (tipología), mientras que los efectos son las consecuencias o resultados que las causas producen y tienen la característica de indicar su cuantificación y medir el riesgo.

Los riesgos operacionales se encuentran en los procesos de los cuales se identificarán las debilidades, las implicaciones que se tienen al realizar cambios, identifica las áreas de ataque de defraudadores externos e internos, los puntos naturales de falla, etc.

Para los criterios de clasificación se busca que el riesgo identifique las causas, eventos y consecuencias, así mismo las categorías de riesgo operacional recaerán en 4 principales clasificaciones las cuales son:

- Personas
- Procesos
- Sistemas
- Externos

La identificación de riesgos operacionales en el Banco, se puede efectuar por medio de talleres los cuales son efectuados con el responsable del área y con algunos participantes

que llevan a cabo los procesos para identificar cuáles son los principales riesgos que ellos detectan en su trabajo diario.

Los riesgos operacionales serán descritos en la **matriz de riesgos** y controles para evaluar la calificación que se le otorgará, de acuerdo a lo solicitado por la Normatividad deben estar clasificados en 3 calificaciones:

Riesgo Alto. Riesgo que debe ser el más vigilado por el área de riesgo operacional ya que implica que en caso de que se materialice, tenga como consecuencia quebranto de la Institución o bien tenga una situación de dimensiones severas para la institución, cliente o tercero.
Riesgo Medio Riesgo que debe ser vigilado de manera permanente pero no tiene consecuencias de quebranto en la institución, pero deben ser factibles para mantener bajo cierto control.
Riesgo Bajo. Riesgo vigilado de manera moderada, las consecuencias o dimensiones de la detonación del riesgo serían pocas y de magnitudes pequeñas cayendo en el punto de que sean prácticamente imperceptibles.

Teniendo la descripción del riesgo se debe efectuar una adecuada calificación de riesgos se la cual cuenta con dos factores, la frecuencia y el impacto.

Frecuencia

Al evaluar la frecuencia pretendemos conocer el número de veces en el año que se podría materializar el riesgo identificado los siguientes niveles se pueden utilizar de manera estándar para cualquier banco.

Nivel de Frecuencia	Número de Eventos
1	De 1 a 4 veces al año
2	De 5 a 8 veces al año
3	Más de 8 veces al año

Impacto Económico:

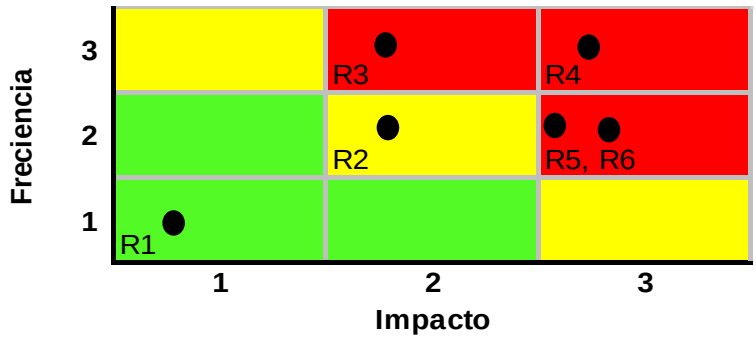
Al evaluar el Impacto Económico pretendemos conocer cuál sería la máxima pérdida económica que se podría sufrir en caso de que se materialice el riesgo. El siguiente cuadro se debe de considerar las utilidades de la institución para determinar el impacto de los montos máximos y mínimos.

	Importe	
Nivel	**Mínimo**	**Máximo**
1	$ 1	$ 850,000
2	$ 850,001	$ 4´800,000
3	más de $4´800,000	

El personal designado para determinar la calificación de los riesgos, deberá considerar las dos tablas anteriores para determinar si el riesgo es alto, medio o bajo.

Estas tablas se calculan de acuerdo a las utilidades de la empresa en el año fiscal anterior, y se pueden dejar como base para realizar la clasificación durante el tiempo determinado que la empresa lo requiera.

Los riesgos y controles son representados mediante un “mapa de calor”, el cual es un gráfico que representa los riesgos gráficos en cuadrantes y se definen por el color del riesgo, teniendo como el riesgo alto representado en color rojo, los riesgos medios en color amarillo y los riesgos bajos en color verde.



Frecuencia	Impacto	Calificación
1	1	Bajo
1	2	Bajo
1	3	Medio
2	1	Bajo
2	2	Medio
2	3	Alto
3	1	Medio
3	2	Alto
3	3	Alto

Los riesgos que ya se han materializado y que se les denominarán eventos de pérdida se registran en una matriz anexa.

5. EVENTOS DE PÉRDIDA

De acuerdo a la definición de Basilea II, un evento de riesgo operacional es la pérdida resultante de una falta de adecuación o de un fallo de los procesos el personal y los sistemas internos o bien de acontecimientos externos, en términos más coloquiales el evento de pérdida es el riesgo ya materializado y que generó una pérdida en la Institución.

Para registrar los eventos de pérdida el gestor de Riesgo Operacional envía una matriz a los responsables de cada área del Banco, en donde se registre el evento de pérdida por caso, fecha en que ocurrió, origen del evento de pérdida, monto de pérdida (en caso de que se pueda calcular) y código relacionado al riesgo operacional.

Se deberá realizar una conciliación de la base de datos de eventos de pérdida en relación con los riesgos operacionales de cada área, para verificar que la calificación de frecuencia e impacto del riesgo sea más acertada y más “real”, que cuando no se conoce el riesgo materializado.

La legislación actual menciona que se tiene que tener una base de eventos de pérdida de por lo menos 5 años atrás para el cálculo del VAR (valor en Riesgo) Operacional.

Base de Datos de Eventos de Pérdida

Núm	Unidad Organizacional	Área	Tipo de			Categoría de Tipo de Evento de Pérdida	Problema	Solución (En su caso)	Ciclo de Negocio Afectado	Fecha en que Ocurrió	Fecha en que se detectó	Costo por Evento		Código de Identificación	Observaciones	Tipificación del evento	Tema
			RO	RL	RT							Estimado	Real				
11	Banco	Jurídico	X			Ejecución, entrega y gestión de procesos	Multa de $13,692 debido a que se realizó una operación con Valores, cuya fecha de liquidación fue posterior al cuarto día hábil bancario a partir de su fecha de concertación		Mercado de dinero	21/07/2010	13/10/2011					Incumplimiento a la normatividad	

Para realizar el cálculo del VAR Operacional se necesitan 5 años de datos de la base de eventos de pérdida, sin embargo, no se cuenta con esta información a la fecha debido a que el Banco no contaba con la información necesaria.

6. MATRIZ DE RIESGOS Y CONTROLES

La matriz de riesgos y controles es el documento que conjunta los dos temas: la identificación y evaluación de los riesgos operacionales y los controles relacionados, en la matriz de controles está identificado por área y línea de negocio cuales son los riesgos y controles relacionados.

Para requisitar la matriz de riesgos y controles se necesitaran de catálogos establecidos para el llenado de algunos rubros por lo que en el siguiente cuadro se encuentran el significado de cada tema:

Guía de llenado Matriz CI-RO

		Rubros	Definición de llenado
REF	RO	No. Evento de riesgo	Se coloca el número de riesgo de acuerdo al código de la matriz y se agrega el número de riesgo.
	CI	Codigo Mat. Ctrl	Código de matriz de acuerdo a la unidad de negocio.
Riesgo	CI	Evento de Riesgo (Descripción del Riesgo)	Describir este rubro de acuerdo a cuál es el riesgo y cuál su consecuencia.
	RO	Tipo de RO CNBV	Catálogo nivel 1 RO. Elegir una opción.
		Tipo de RO CNBV (Nivel 2)	Catálogo nivel 2 RO. Elegir una opción y se determina de acuerdo a lo que se selecciono en el nivel 1.
		Riesgo Operativo	Se llenan con una **"x"** de acuerdo al tipo de riesgo, si tiene afectación legal, si es un riesgo tecnólogico (Sistema), o bien si no afecta ae ninguno de los 2 rubros anteriores, se selecciona como es operacional.
		Riesgo Legal	
		Riesgo Tecnológico	
		Frecuencia	Al evaluar la frecuencia pretendemos conocer el número de veces en el año que se podría materializar el riesgo identificado, se llena con una calificación del 1 al 5 (de acuerdo a la tabla de frecuencia del área de R.O)
		Impacto	Al evaluar el Impacto Económico pretendemos conocer cual sería la máxima pérdida económica que se podría sufrir en caso de que se materialice el riesgo, , se llena con una calificación del 1 al 5 (de acuerdo a la tabla de impacto del área de R.O)
		Evaluación	Es la ponderación de la calificación de la frecuencia e impacto rubro automático ***(no se llena).***
Control	CI	Descripción de la Actividad de Control que realiza la entidad (Objetivo del Control) (Actividad de Control)	Describir el control iniciando con cuál es el puesto de la persona que lo ejecuta seguido de un verbo como concilia, confirma, revisa y terminando en la descripciónd de cómo realiza el control.
	CI	La actividad de control es preventiva o detectiva (Tipo de Control)	-**Control preventivo**. Control que se define su existencia antes de que se materialice el riesgo. Anticipan eventos no deseados antes de que sucedan. -**Control Detectivo.** Cuando el riesgo ya se materializo y se aplica este control. Identifican los eventos en el momento en que aparecen. Cuando no es preventivo.
	CI y/o RO	Frecuencia del control (D, S, Q, M, T, SEM, A ó PE)	Se requisita dependiendo cada vez que se ejecuta el control: '-**D** (diario) -**S** (semanal) -**Q** (quincenal) -**M** (mensual) -**T** (trimestral) -**SEM** (semestral) -**PE** (Por evento) varias veces al día, o sin tener una temporalidad definida.
	CI	Manual	Se llenan con una **"x"** y es una sola opción, de acuerdo al tipo de control, si es automático (TI) verificar si se ejecuta la actividad de control por parte de un sistema. En caso de escoger automático llenar rubro de **"nombre de la aplicación /sistema"**
	CI	TI	
	CI	La actividad de control esta correctamente diseñada	Contestar sí o no de acuerdo a la evaluación del diseño
	CI	Documentación soporte de la actividad de control (Evidencia del control)	Es el documento que se genera derivado del control realizado, (evidencia).
	CI	Cuentas Contables Relacionadas	En caso de que la respuesta sea **"Si"** en el rubro de **"¿Genera registro contable?"** indicar la cuenta contable relacionada, en caso de no existir poner NE (No existe)
	CI	Integridad	Se llenan con una "x", y es posible llenar más de una opción, el significado de cada tema se encuentra en el catálogo de "Aseveraciones financieras".
	CI	Existencia	
	CI	Ocurrencia	
	CI	Valuación	
	CI	Derechos y Obligaciones	
	CI	Presentación y Revelación	
	CI	Identificación de controles COSO	Verificar pestaña COSO

Guía de llenado Matriz CI-RO

		Rubros	Definición de llenado
Control	CI	Integridad	Se llenan con una "x", y es posible llenar más de una opción, el significado de cada tema se encuentra en el catálogo de "Aseveraciones financieras".
	CI	Existencia	
	CI	Ocurrencia	
	CI	Valuación	
	CI	Derechos y Obligaciones	
	CI	Presentación y Revelación	
	CI	Identificar el componente COSO	Verificar cátalogo COSO
	CI	Procedimientos de revisión realizados (a detalle)	Detallar como se realizará la prueba del control
	CI	Referencia a papeles de trabajo de walkthrough	Documento que se utilizó para la evaluación del control
	CI	¿Genera registro contable?	Se responde con **"Sí"** o **"No"** en función a que si se materializa el riesgo existirá una afectación contable o no, va en función en la descripción del riesgo y está debe ser una información del riesgo no del control. (en posición debe de ir antes de las cuentas contables relacionadas).
	CI	Potencial de fraude	Se responde **"Si"** o **"No"** de acuerdo a la descripción del riesgo y debe de estar descrito con la palabra fraude.
	CI	Descripción del Procedimiento de Auditoría que probará la efectividad del control (prueba de la efectividad de control interno)	Se describe la prueba de eficacia operativa según el riesgo y el control asociado, esta descripción se encuentra en la matriz de pruebas de control.
	CI	Alcance	Identificar cual será el alcance de la revisión
	CI	Técnica de Auditoría (Estudio general, análisis, inspección, confirmación, investigación, declaración, certificación, observación)	Elegir una opción
	CI	Observaciones	Descripción o texto libre, si se requiere poner alguna información que no corresponda a ninguno de los rubros de la matriz.
	CI	Referencia a papeles de trabajo de la prueba	Nombre de las carpetas de las evidencias otrogadas en cada una de las pruebas.
	CI	¿El control es efectivo? Si/No	Se responde con **"Sí"** o **"No"**, y se escribe en función de pruebas de eficacia operativa, en caso de que la respuesta sea "No" se requiere un plan de remediación *(llenar rubro plan de remediación).*
	CI	Porcentaje de efectividad de la prueba	Se requisita en base a los atributos de cada prueba y se coloca el porcentaje en número, dividiendo los atributos que cumplen, entre el total de atributos: **# de atributos que cumplen /** **# de atributos totales de la prueba**
	CI	Plan de Remediación	Este requisito debe ser llenado siempre que el rubro de "el control es efectivo" tenga una respuesta negativa **"No"**, el cual debe de describir cual es el plan de remediación, con fechas compromiso y se dará seguimiento en el área de Control Interno (disparadores ORCA).
Áreas responsables	CI	Responsable Subproceso (nombre y puesto)	Requisitar nombre y puesto de la persona responsable del subproceso, de acuerdo al Organigrama Corporativo.
	CI	Responsable de la Actividad de Control Área/usuario	Requisitar nombre y puesto de la persona que ejecuta el control, de acuerdo al Organigrama Corporativo.
	CI	Director del Área	Requisitar nombre y puesto del Director de área (en caso de que no haya entonces el Director Corporativo responsable), de acuerdo al Organigrama Corporativo.
	CI	Dirección Responsable (Nombre del área dueña del proceso) (Nombre del área dueña del proceso de control)	Requisitar nombre de la Dirección Responsable de acuerdo al Organigrama.
Catálogo CNBV	RO	Entidad	Debe ser llenado de acuerdo a si es un proceso de Casa de Bolsa, Operadora de Fondos o Banco, y debe ser llenado con una sola selección.
	RO	Producto CNBV	Verificar catálogo. Se debe elegir una sola opción.
	RO	Proceso CNBV	Verificar catálogo. Se debe elegir una sola opción.
	RO	Linea de Negocio CNBV	Verificar catálogo. Se debe elegir una sola opción.

Catálogo Tipo de pérdida de RO 1er. Nivel.

Generales / Tipo pérdida RO CNBV 1er nivel
100 Fraude Interno
200 Fraude Externo
300 Relaciones Laborales y Seguridad en el Puesto de Trabajo
400 Clientes Productos y Prácticas Empresariales
500 Desastres naturales y otros acontecimientos
600 Incidencias en el Negocio y Fallos en los Sistemas
700 Ejecución Entrega y Gestión de Procesos

Catálogo Tipo de pérdida de RO 2do. Nivel

	Generales / Tipo pérdida RO CNBV 2do nivel
100 Fraude Interno	101 Actividades no Autorizadas_Uso indebido de facultades y poderes
	101 Actividades no Autorizadas_Operaciones no reveladas intencionalmente
	101 Actividades no Autorizadas_Operaciones no autorizadas con pérdidas pecuniarias
	101 Actividades no Autorizadas_Valoración errónea de posiciones intencional
	102 Hurto y Fraude Internos_Fraude
	102 Hurto y Fraude Internos_Fraude crediticio
	102 Hurto y Fraude Internos_Depósitos sin valor
	102 Hurto y Fraude Internos_Hurto
	102 Hurto y Fraude Internos_Extorsión
	102 Hurto y Fraude Internos_Malversación
	102 Hurto y Fraude Internos_Robo
	102 Hurto y Fraude Internos_Apropiación indebida de activos
	102 Hurto y Fraude Internos_Destrucción dolosa de activos
	102 Hurto y Fraude Internos_Falsificación Interna
	102 Hurto y Fraude Internos_Utilización de cheques sin fondos
	102 Hurto y Fraude Internos_Contrabando
	102 Hurto y Fraude Internos_Apropiación de cuentas de identidad entre otros.
	102 Hurto y Fraude Internos_Incumplimiento intencional
	102 Hurto y Fraude Internos_Evasión de impuestos intencional
	102 Hurto y Fraude Internos_Soborno
	102 Hurto y Fraude Internos_Cohecho
	102 Hurto y Fraude Internos_Abuso de información privilegiadano a favor de la empresa
	103 Seguridad de los Sistemas_Vulneración de sistemas de seguridad
	103 Seguridad de los Sistemas_Daños por ataques informáticos
	103 Seguridad de los Sistemas_Robo de informacióncon pérdidas pecuniarias
	103 Seguridad de los Sistemas_Utilización inadecuada de claves de acceso yo niveles de autorización
200 Fraude Externo	201 Hurto y Fraude Externos_Hurto
	201 Hurto y Fraude Externos_Robo
	201 Hurto y Fraude Externos_Estafa
	201 Hurto y Fraude Externos_Extorsión
	201 Hurto y Fraude Externos_Soborno
	201 Hurto y Fraude Externos_Falsificación Externa
	201 Hurto y Fraude Externos_Suplantación de personalidad
	201 Hurto y Fraude Externos_Utilización fraudulenta de cheques
	201 Hurto y Fraude Externos_Uso yo divulgación de información privilegiada
	201 Hurto y Fraude Externos_Espionaje industrial
	201 Hurto y Fraude Externos_Contrabando
	202 Seguridad de los Sistemas_Vulneración de sistemas de seguridad
	202 Seguridad de los Sistemas_Daños por ataques informáticos
	202 Seguridad de los Sistemas_Robo de informacióncon pérdidas pecuniarias
	202 Seguridad de los Sistemas_Utilización inadecuada de claves de acceso yo niveles de autorización

Generales / Tipo pérdida RO CNBV 2do nivel	
300 Relaciones Laborales y Seguridad en el Puesto de Trabajo	301 Relaciones Laborales_Cuestiones relativas a la remuneraciónprest. soc.ext. de cont. y rr.hh.
	301 Relaciones Laborales_Organización laboral
	302 Higiene y Seguridad en el Trabajo_Responsabilidad en general
	302 Higiene y Seguridad en el Trabajo_Casos relacionados con las normas de hig. y seg. en el trab.
	302 Higiene y Seguridad en el Trabajo_Indemnización a los trabajadores
	303 Diversidad y Discriminación_Todo tipo de discriminación
	303 Diversidad y Discriminación_Invasión a la intimidad yo acoso
400 Clientes Productos y Prácticas Empresariales	401 AdecuaciónDivulgación de Información y Confianza_Abusos de confianza
	401 AdecuaciónDivulgación de Información y Confianza_Incumplimiento de pautas
	401 AdecuaciónDivulgación de Información y Confianza_Aspectos de adecuación
	401 AdecuaciónDivulgación de Información y Confianza_Divulgación de información
	401 AdecuaciónDivulgación de Información y Confianza_Quebr. de la priv. de info. sobre cli. min.
	401 AdecuaciónDivulgación de Información y Confianza_Quebrantamiento de privacidad
	401 AdecuaciónDivulgación de Información y Confianza_Ventas agresivas
	401 AdecuaciónDivulgación de Información y Confianza_Confusión de cuentas
	401 AdecuaciónDivulgación de Información y Confianza_Abuso de información confidencial
	401 AdecuaciónDivulgación de Información y Confianza_Responsabilidad del prestamista
	402 Prácticas Empresariales o de Mercado Improcedentes_Prácticas restrictivas de la competencia
	402 Prácticas Empresariales o de Mercado Improcedentes_Prácticas comer. o de mercado improcedentes
	402 Prácticas Empresariales o de Mercado Improcedentes_Manipulación del mercado
	402 Prácticas Empresariales o de Mercado Improcedentes_Abuso de info. privileg. a favor de la emp.
	402 Prácticas Empresariales o de Mercado Improcedentes_Actividades no autorizadas
	402 Prácticas Empresariales o de Mercado Improcedentes_Lavado de dinero
	403 Productos Defectuosos_Defectos del producto
	403 Productos Defectuosos_Error de los modelos
	404 SelecciónPatrocinio y Riesgos_Ausencia de investigación a clientes conforme a las directrices
	405 Actividades de Asesoramiento_Litigios sobre resultados de las actividades de asesoramiento
500 Desastres naturales y otros	501 Desastres naturales y otros acontecimientos_Pérdidas por desastres naturales
	501 Desastres naturales y otros acontecimientos_Pérdidas por causas externasterrorismovandalismo
600 Incidencias en el Negocio y Fallos en los Sistemas	601 Sistemas_Hardware
	601 Sistemas_Software
	601 Sistemas_Telecomunicaciones
	601 Sistemas_Interrupción o incidencias en el suministro
700 Ejecución Entrega y Gestión de Procesos	701 Recepción Ejecución y Mantto. de Operaciones_Comunicación defectuosa
	701 Recepción Ejecución y Mantto. de Operaciones_Errores de introd. de datos mantto. o descarga
	701 Recepción Ejecución y Mantto. de Operaciones_Incumplimiento de plazos o de responsabilidades
	701 Recepción Ejecución y Mantenimiento de Operaciones_Ejecución errónea de modelos o sistemas
	701 Recepción Ejecución y Mantenimiento de Operaciones_Error contable o atribución a ent. erróneas
	701 Recepción Ejecución y Mantenimiento de Operaciones_Errores en otras tareas
	701 Recepción Ejecución y Mantenimiento de Operaciones_Fallo en la entrega
	701 Recepción Ejecución y Mantenimiento de Operaciones_Fallo en la gestión del colateral
	701 Recepción Ejecución y Mantenimiento de Operaciones_Mantenimiento de datos de referencia
	702 Seguimiento y Presentación de Informes_Incumplimiento de la obligación de informar
	702 Seguimiento y Presentación de Informes_Inexactitud de informes externos con generación de pérd.
	703 Aceptación de Clientes y Documentación_Inexistencia de autorizaciones
	703 Aceptación de Clientes y Documentación_Rechazos de clientes
	703 Aceptación de Clientes y Documentación_Documentos jurídicos inexistentes o incompletos
	703 Aceptación de Clientes y Documentación_Errores en los contratos
	704 Gestión de Cuentas de Clientes_Acceso no autorizado a cuentas
	704 Gestión de Cuentas de Clientes_Registros incorrectos de clientes con generación de pérdidas
	704 Gestión de Cuentas de Clientes_Pérdida o daño de activos de clientes por negligencia
	705 Pérdidas derivadas del incumplimiento de la Normativa_De la normativa fiscal.
	705 Pérdidas derivadas del incumplimiento de la Normativa_De la normativa bancaria
	705 Pérdidas derivadas del incumplimiento de la Normativa_De otras normas.
	706 Contrapartes Comerciales_Fallos de contrapartes distintas de clientes
	706 Contrapartes Comerciales_Otros litigios con contrapartes distintas de clientes
	706 Contrapartes Comerciales_Errores en los contratos
	707 Distribuidores y Proveedores_Subcontratación
	707 Distribuidores y Proveedores_Litigios con distribuidores
	707 Distribuidores y Proveedores_Errores en los contratos

Cátalogo Producto

TABLA : PRODUCTO			
NIVEL 1	REFERENCIA	NIVEL 2	DEFINICION
Gestión Financiera	101	Emisión de Acciones	Prestaciones de servicios relacionados con la oferta publica inicial o posterior en el mercado de inversión de capital cualquier empresa
	102	Emisión de Bonos	Prestación de servicios relacionados con la emisión y colocación de la deuda en el mercado, para cualquier entidad emisora
	103	Productos Estructurados de Emisión	Prestación de servicios relacionados con la emisión y colocación de productos financieros estructurados
	104	Bursatilizaciones	Prestación de servicios relacionados con la emisión y colocación de bursatilizaciones
	105	Colocaciones Privadas	Gestión de una colocación fuera de canje de instrumentos a un inversos o aun grupo de inversores
	106	Sindicaciones	Prestación de Servicios en apoyo de un financiamiento sindicado
Asesoría Financiera	201	Fusiones y Adquisiciones	Servicios de Asesoría y/o financiamiento en la búsqueda de fusiones y/o adquisiciones
	202	Servicios de Asesoría Corporativa	Servicios de asesoría de investigación para empresas privadas y publicas
Tesorería y Mercados	301	Renta Fija	Comercio y venta de efectivo basado en las tasas de interés de un producto.
	302	Renta Variable	comercio y venta de efectivo basado en productos de renta variable
	303	Divisas y mercados monetarios	comercio y venta de productos al contado y a plazo en divisas
	304	Préstamos de Valores	El comercio y la venta de la cesiones temporales y las operaciones de préstamo de valores.
	305	Fondos de Inversión	Comercio y venta de fondos de inversión y fondos negociados en bolsa. Los instrumentos subyacentes pueden o no ser cotizados y negociados en bolsa
	306	OTC y Bursatilizaciones Tasas de Interés Derivada	Referente a los instrumentos renta variable. Comercio y veta de productos derivados se incluyen warrants y productos estructurados de deuda en su caso
Clientes Minoristas	401	Tarjetas de Crédito	La disposición de crédito para facilitar el pago y extender temporalmente el crédito revolvente
	402	Préstamos de vehículos	Prestamos para la compra de coches y otros vehículos para uso domestico, tales como barcos, motos, etc. Cuya garantía es propio vehículo
	403	Arrendamiento de Vehículos	arrendamiento de automóviles u otros vehículos en las que al final y no siempre se tiene opción a compra cuando caduca la concesión
	404	Hipotecas	Prestamos para la compra de viviendas u otros inmuebles para uso personal, con garantía del propio inmueble
	405	Préstamos Garantizados y Líneas de Crédito	El otorgamiento de prestamos o líneas de crédito revolventes para cualquier propósito cuya garantía es el capital propio
	406	Otros Préstamos de Consumo con Garantía	Préstamo de crédito al consumo garantizados por un activo que no sea de bienes inmuebles y/o vehículos
	407	Otros Préstamos de Consumo sin garantía	Préstamo de crédito al consumo sin garantía
	408	Otros Arrendamientos de Consumo	Financiamiento para los activos arrendados que no sean aquellos destinados para vehículos
	409	Cartas de Crédito y Créditos Garantizados	Cartas crédito o acuerdos similares, los cuales representan la obligación del beneficiario por parte de emisor de devolver el dinero prestado o hacer los pagos necesarios a cuenta del crédito concedido
Clientes Mayoristas	501	Préstamos Comercial & Industrial	Otorgamiento de créditos a empresas para su funcionamiento a plazo fijo, se incluyen instalaciones, equipos y otros activos fijos
	502	Prestamos Bienes Raíces	Otorgamiento de créditos para la compra de bienes inmuebles con fines de apoyar el desarrollo comercial de la empresa
	503	Préstamos para la Construcción, Adquisición & Desarrollo	Financiamiento a clientes principalmente de bienes raíces para el desarrollo o la construcción de un proyecto destinado este ultimo a la preventa.
	504	Arrendamiento Comercial	Créditos otorgados para el arrendamiento de equipos utilizables en la compañía por algún tiempo a cambio de una serie de pagas periódicas.
	505	Servicios y Funciones de las Tarjetas de Crédito	La disposición de crédito para la prestación de servicios de infraestructura y de apoyo para las mismas
	506	Préstamos para Proyectos de Financiación	Otorgamiento de créditos para para proyectos específicos de capital, principalmente, para flujos de efectivo
	507	Cartas de Crédito, Certificados Bancarios, Aceptaciones Bancarias	Créditos otorgados sobre los cuales se constituye una garantía financiera a favor del banco con la obligación de los clientes al pago o anticipación del monto total en caso de incumplimiento.
	508	Factoraje	Alternativa de financiamiento dirigida preferentemente a pequeñas y medianas empresas

TABLA : PRODUCTO			
NIVEL 1	REFERENCIA	NIVEL 2	DEFINICION
Depósitos	601	Cuenta Corriente	Servicios que proporcionan los bancos en satisfacer las demandas de las cuentas corrientes que gestiona
	602	Depósitos a Plazo, Certificados de Depósito y Certificados de Inversión Garantizados, etc.	La prestación de servicios bancarios relacionados con una cuenta con restricciones de acceso, como la frecuencia, tiempo o los requisitos de notificación.
	603	Depósitos a la Vista	La prestación de servicios bancarios relacionados con la demanda de cuentas bancarias incluyendo cuentas corriente, cuentas a la vista y depósitos a la vista
	604	Depósitos a Plazo Fijo	Suministro de productos de deposito a plazo fijo a los clientes comerciales
	605	Productos de Inversión con Renta Variable	Fondos de jubilación, fondos de ahorro para el retiro
	606	Tarjeta de Debito	La Disposición de debito así como, la prestación de servicios operativos y servicios de infraestructura de apoyo para las mismas
Administración de efectivos, Pagos y Liquidaciones	701	De Clientes: Edo. Cuenta Bancarios, Domiciliaciones, Transferencias, etc.	Servicios que proporcionan los bancos de manera electrónica para dar soporte a sus entradas y salidas de efectivo
	702	De Empresas: Edo. Cuenta, Cuentas por Cobrar, Domiciliaciones, Transferencias, Giros, etc.	Prestación de Servicios de banca electrónica para soporte a empresas en el manejo de sus flujos de entrada y salidas de efectivo.
	710	Pagos manuales: Cheques de Viajero, Ordenes de Pago, Instrucciones de Pago vía Fax, etc.	Todas las formas de pago iniciadas manualmente y/o por medios no electrónicos
	711	Letras de Cambio, Cheques de Caja, Notas de Crédito.	Se incluyen todas aquellas operaciones que tras un proceso de adaptación agregación y /o compensación se puedan intercambiar por efectivo y/o transferencias de valores libres de pago entre compradores y vendedores
	712	Liquidación	Ejecución de operaciones de valores por parte de una organización de liquidación o un custodio de la instituciones comerciales. Incluye intercambio de títulos de efectivo y transferencia de títulos en efectivo.
Gestión de Fideicomisos e Inversión	801	Servicios de Custodia	La custodia de los activos físicos y no físicos y otros artículos de valor en nombre de los clientes
	802	Fideicomisos Corporativos	La prestación de los servicios de agente registrador y en nombre de un emisor
	803	Intermediación Primaria "Fondos de Cobertura"	Custodia, compensación liquidación y otras funciones ("back office") a entidades comerciales
	804	Planeación Financiera y Patrimonial	Prestación de asesoría planificación y servicios relacionados con la gestión de la riqueza y estructuras de propiedad, incluyendo impuestos, legales, asesoría financiera, testamentos, sucesiones y servicios albacea
	805	Gestión discrecional de carteras	Gestión discrecional de cartera de clientes de banca minorista y empresas para tomar decisiones de inversión en nombre del cliente
	806	Servicios de Ejecución	Prestación de servicios de ejecución exclusiva para clientes, en virtud de un mandato que requiere del cliente de todas la decisiones de inversión
	807	Asesor de Gestión de la Cartera	Prestación de servicios a clientes de banca privada bajo los términos de un mandato que puede requerir alguna entrada del cliente o donde el tiempo el cliente puede, de vez en cuando, ofrecer alguna aportación
Productos de Inversión	901	Administración de Fondos	Prestación de fondos se gestión operativa y admón. de servicios
	902	Gestión de Activos Institucionales	Gestión de inversiones y ejecución de servicios por cuenta de clientes institucionales que posean una cartera de activos tradicionales y no tradicionales.
Productos no Bancarios	2001	Otros	Si el producto no esta asociado a ninguna de las categorías anteriores

Catálogo Proceso

TABLA: PROCESO			
ÁMBITO	REFERENCIA	DESCRIPCIÓN	DEFINICION
Negocio	010	Desarrollo, Diseño, y Mantenimiento de Productos & Servicios	Identificar, diseñar , producir y mantener nuevos productos financieros, servicios y capacidades de negocios, incluyendo los modelos y metodologías que se basan.
	020	Mercado de Productos y Servicios	Promover la empresa y sus productos y servicios a través de marketing o publicidad, incluyendo la producción de tasas estándar, tasas, cambios y precios de productos específicos y servicios generales.
	030	Vender o alcanzar acuerdos para Conductas Específicas en los Negocios	Concerniente a la venta de productos específicos o delos servicios que se ofrecen a los clientes individuales incluyendo la cotización de honorarios firmes o indicativos, tasas, cargos o similares con la intención de concluir un acuerdo especifico para la venta de productos específicos o prestación de servicios.
	040	Asumir y mantener Clientes/Usuarios, Contrapartes & Relaciones de Comercio	Referente a mantener el cliente o las cuentas de las contrapartes, incluidos los relacionados con la debida diligencia, datos y documentación.
	050	Captura y Documentación de Operaciones	Condiciones especificas del registro de las transacciones y las instrucciones de los temas de procesamiento de la empresa; también producen documentos de transacción relacionada.
	060	Entregar productos y servicios	Ofrecer o cumplir productos y servicios, incluida en la configuración y mantenimiento de transacciones y acuerdos necesarios y acordados no transacción servicios financieros.
	070	Operaciones Contables	Registro de operaciones y/o información de la posición de la empresa en los libros de (mayor) y registros contables.

TABLA: PROCESO			
ÁMBITO	REFERENCIA	DESCRIPCIÓN	DEFINICION
Corporativos	100	Administración de Recursos Humanos	Gestión de los recursos humanos, además de las funciones de gestión de negocios.
	110	Administración de Información Tecnológica	Adquirir, diseñar y/o desarrollar información tecnología y aplicar medidas de seguridad y respuesta a incidentes.
	120	Reporte de Gestión Financiera y Tributación	Realizar los informes financieros y de control, basado (pero sin incluir) en las entradas al libro mayor durante la operación contable.
	130	Gestión de Capital, Fondos y Liquidez	Administrar las cuentas de capital de la empresa, la liquidez y el balance.
	140	Gestión de Proveedores y Servicios Outsourcing	Selección, embarque, gestión y supervisión de vendedores y proveedores de servicios outsourcing
	150	Administración de los Bienes e Instalaciones Físicas	Suministro y gestión física de las instalaciones, equipos y entornos de trabajo seguro.
	160	Gestionar el cumplimiento, Legal, Gobierno Corporativo y Auditoria	Establecer y mantener políticas de la empresa, normas, procedimientos, códigos de conducta, y el cumplimiento de controles asociados a los procedimientos de prueba.
	170	Administración de Sistemas de Riesgo	Establecer procesos de gestión de riesgos y metodologías (aparte del proceso de trabajo habitual y los controles de supervisión) para registrar, controlar evaluar o administrar la exposición al riesgo dentro de la empresa.
Procesos no Relacionados	200	Situaciones en las que no está implicando ningún proceso específico	Se usa para situaciones en las que no esta implicando ningún proceso especifico.

Catálogo Línea de Negocio

Tabla : Lineas de Negocio				
REFERENCIA	NIVEL1	REFERENCIA	NIVEL2	GRUPO DE ACTIVIDADES
100	Finanzas Corporativas	101	Finanzas Corporativas	Fusiones y adquisiciones suscripción de emisiones , privatizaciones, bursatilizaciones, servicio de estudios, deuda,acciones,sindicaciones, ofertas publicas iniciales, colocaciones privadas en mercados secundarios.
		102	Finanzas de Administraciones Locales / publicas	
		103	Banca de Inversion	
		104	Servicios de Consultoria	
200	Negociacion y Ventas	201	Compras y Ventas	Renta fija, renta Variable, divisas, credito,posiciones propias en valores, préstamo de valores, reportos y operaciones similares, operaciones financieros derivadas, intermediación y servicios adicionales, y
		202	Formacion de mercado	
		203	posiciones propias	
		204	Tesoreria	
300	Banca Minorista	301	Banca Minorista	Créditos y depósitos de Clientes minoristas, servicios bancarios, fideicomisos y testamentarias, créditos y depósitos de clientes de banca privada o patrimonial,
		302	Banca privada o patrimonial	
		303	Servicios de Tarjetas	
400	Banca Comercial	401	Banca Comercial	Financiamiento de proyectos, bienes raíces, financiamiento de exportaciones, financiamiento de exportaciones, financiamiento comercial,fatoraje,arrendamiento financiero, préstamo de garantías, letras de cambio.
500	Pago y Liquidacion	501	Clientes Externos	Pagos y cobranzas, transferencia de fondos, compensación y liquidación
600	Servicios de Agencia	601	Custodia	Depósitos en custodia, certificados de deposito, operaciones de sociedades (clientes) para prestamos de valores.
		602	Agencia para empresas	
		603	Fideicomisos de empresas	
700	Administracion de Activos	701	Administracion discrecional de fondos	Agrupados, segregados, minoristas institucionales, cerrados, abiertos, participaciones accionarias.
		702	Administracion no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo de capital variable.
800	Intermediacion minorista/operaciones de corretaje al menudeo	801	Itermediacion minorista/operaciones de cor	Recepción,registro,ejecucion y asignación

Catálogo Aseveraciones Financieras

ASEVERACIONES FINANCIERAS.
1.Integridad (columna T) - Identifica que las transacciones, acontecimientos o circunstancias se encuentran efectivamente registrados y presentados.
2. Existencia (columna U) - existe un activo o pasivo en una fecha dada, y ocurrió una transacción o clase de transacción durante el período cubierto por los estados financieros. Un sinónimo de existencia, en algunos contextos, es validez.
3.Ocurrencia / Exactitud (columna V) - los detalles de los activos, pasivos y clases de transacciones se han registrado y procesado correctamente y se han emitido correctamente informes con respecto a parte, fecha, descripción, cantidad y precio.
4.Valuación (columna W) - los activos y los pasivos se han registrado a un valor apropiado en libros.
5.Derechos y obligaciones (columna X)- la entidad tiene los derechos apropiados (por ejemplo, título) con respecto a los activos reflejados en los estados financieros y los pasivos son propiamente las obligaciones de la entidad (a veces se refiere a éstos como derechos y obligaciones).
6.Presentación y revelación - la información apropiada se revela, se clasifica y se describe de acuerdo con políticas aceptables de contabilidad y requerimientos legales, si aplican.

Catálogo COSO

COSO
ENTORNO O AMBIENTE DE CONTROL
El ambiente de control define al conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.
EVALUACION DE RIESGOS
El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza se evalúa la vulnerabilidad del sistema. Para ello debe adquirirse un conocimiento practico de la entidad y sus componentes de manera de identificar los puntos débiles, enfocando los riesgos tanto al nivel de la organización (internos y externos) como de la actividad
ACTIVIDAD DE CONTROL
Las actividades de control son las normas y procedimientos (actividades necesarias para implementar las políticas), cuyo fin es asegurar el cumplimiento de las directrices establecidas por la dirección para controlar los riesgos.
INFORMACION Y COMUNICACIÓN
Así como es necesario que todos los agentes conozcan el papel que les corresponde desempeñar en la organización (funciones, responsabilidades), es imprescindible que cuenten con la información periódica y oportuna que deben manejar para orientar sus acciones en consonancia con los demás, hacia el mejor logro de los objetivos.
SUPERVISION
Incumbe a la dirección la existencia de una estructura de control interno idónea y eficiente, así como su revisión y actualización periódica para mantenerla en un nivel adecuado. Procede la evaluación de las actividades de control de los sistemas a través del tiempo, pues toda organización tiene áreas donde los mismos están en desarrollo, necesitan ser reforzados o se impone directamente su reemplazo debido a que perdieron su eficacia o resultaron inaplicables. Las causas pueden encontrarse en los cambios internos y externos a la gestión que, al variar las circunstancias, generan nuevos riesgos a afrontar.

Teniendo en cuenta los catálogos antes mencionados se procede a tener la matriz de riesgos y controles segregada por tema y cumpliendo con lo que solicitan las disposiciones.

La matriz de riesgos es una herramienta de control en el cual se identificaran los procesos documentados y va a permitir evaluar el riesgo de una institución y realizar un diagnóstico objetivo de la situación global de riesgo de una entidad.

Para la requisición de dicha matriz debe existir participación activa de las unidades de negocio, operativas y funcionales en la definición de la estrategia institucional de riesgo de la empresa, una efectiva matriz de riesgo permite el que se hagan comparaciones objetivas entre áreas, procesos, y actividades.

Entre los organismos Supervisores de diferentes países están en proceso de implementación de metodologías de supervisión con base en la gestión del riesgo por lo que consideran que la matriz de riesgo constituye una herramienta clave en el proceso de supervisión de riesgos, debido a que la misma les permite efectuar una evaluación cualitativa y cuantitativa de los riesgos inherentes de cada unidad

Matriz de Riesgos Riesgo Operacional y Control Interno

ENTIDAD:
EMPRESA:
FECHA:
MATRIZ DE RIESGOS Y CONTROLES
CICLO DE NEGOCIO
CODIGO DEL CICLO:

REF		RIESGO									CONTROL						
No. Evento de riesgo	Codigo Mat. Ctrl	Evento de Riesgo (Descripción del Riesgo)	Tipo de RO CNBV	Tipo de RO CNBV (Nivel 2)	Riesgo Operativo	Riesgo Legal	Riesgo Tecnológico	Frecuencia	Impacto	Evaluación	Descripción de la Actividad de Control que realiza la entidad (Objetivo del Control) (Actividad de Control)	La actividad de control es preventiva o detectiva (Tipo de Control)	Frecuencia del control (D, S, Q, M, T, SEM, A ó PE)	Manual	TI	La actividad de control esta correctamente diseñada	Documentación soporte de la actividad de control (Evidencia del control)

MATRIZ DE RIESGOS Y CONTROLES
CICLO DE NEGOCIO
CODIGO DEL CICLO:

CONTROL																	AREAS RESPONSABLES				CATALOGO CNBV			
	ASEVERACIONES																							
Cuentas Contables Relacionadas	Integridad	Existencia	Ocurrencia	Valuación	Derechos y Obligaciones	Presentación y Revelación	Identificar el componente COSO	Procedimientos de revisión realizados (a detalle)	Referencia a papeles de trabajo de walkthrough	¿Genera registro contable?	Potencial de fraude	Descripción del Procedimiento de auditoría que probará la efectividad del control (prueba de efectividad de control interno)	Muestra	Técnicas de Auditoría (Estudio general, análisis, inspección, confirmación, investigación, declaración, certificación, observación)	Observaciones	Referencia a papeles de trabajo de la prueba	¿El control es efectivo? SI/No	Porcentaje de efectividad de la prueba	Plan de Remediación	Responsable de la actividad de Control usuario	Responsable Subproceso	Director del Área	Dirección Responsable (Nombre del área dueña del proceso (Nombre del área dueña del proceso de control)	Entidad	Producto CNBV	Proceso CNBV	Linea de Negocio CNBV

7. EVALUACIÓN DE LOS CONTROLES

Las actividades de control que tienen que evaluarse están en función de los objetivos establecidos, por lo tanto la evaluación tendrá en cuenta si las actividades de control están relacionadas con el proceso de evaluación de riesgos y si son apropiadas para asegurar el cumplimiento de los objetivos.

La evaluación se iniciará verificando la eficacia de los controles para llevar esto a cabo se observará que su diseño sea apropiado, que exista un responsable de ejecutar el control, que tenga una frecuencia y que el control este documentado.

Los criterios para evaluar la efectividad de los controles son que debe existir evidencia de la muestra que se examinará, el control implementado está siendo utilizado, que el control previene o mitiga el riesgo y se calificará como efectivo o no efectivo de acuerdo al cumplimiento de los atributos.

Para la evaluación de los controles se utiliza una matriz, la cual cuenta con criterios de evaluación los cuales se describen a continuación:

- Descripción del riesgo. Se describirá el riesgo contestando a las preguntas ¿cuál es el riesgo? y ¿cuál es su consecuencia?.

- Control. La descripción del control se realizará describiendo ¿quién hace el control (puesto)? y ¿cuál es el control?.

- Tipo de control. Se contestará si es detectivo o preventivo.

- Evidencia. Se requiere la evidencia que se traduce en un documento el cual es el resultado de haber aplicado dicho control.

- Frecuencia del Control. Se refiere a la periodicidad del control los cuales se resumen en anual, semestral, trimestral, mensual, semanal, diario y por evento.

- Tamaño de la muestra. Es el número de documentos que se solicitan para realizar la revisión de acuerdo a la siguiente tabla:

Frecuencia del control	No. De items sugeridos a ser testeados.
Anual	1
Trimestral	2
Mensual	3 a 6
Semanal	10, 15, 20
Diario	20, 30, 40
Por evento	30, 45, 60

- Esta tabla se utiliza para saber cuántos documentos se tienen que solicitar, si la revisión del control a realizar es de una base de datos y se refiere a revisar la integridad de la información, se recomienda utilizar la fórmula descrita en la sección 8 del presente documento.

- Descripción de la prueba. En este rubro se describe que es lo que se va a revisar y como se realizará dicha revisión.

- Atributos. Los atributos son los elementos que utilizaras para calificar si el control cumple con la efectividad que se requiere, es decir, puedes determinar los atributos por lo que te pide la normatividad aplicable, por las mejores prácticas, por prácticas internacionales, tendrá la función de mitigar o bajar la calificación del riesgo, etc. Se deberá determinar por cada Institución cuál es el criterio para determinar si un control es efectivo o no, lo más recomendable es pedir que cumpla con por lo menos el 85% de los atributos totales, pero este porcentaje podrá cambiar de acuerdo a lo que se determine con la Dirección General.

La matriz de evaluación de controles debe contener la evidencia de la prueba realizada y deberá describir si el control es eficaz o ineficaz.

#	Descripción del riesgo	Control	Tipo de control	Evidencia	Frecuencia del control	Tamaño de la muestra	Descripción de la prueba

Eficacia operativa de los controles							
ATRIBUTOS							
Se tienen los documentos mínimos mencionados en el anexo 49 de la CUB (C/I)	Se encuentran cotejados los documentos del expediente con la firma del ejecutivo (C/I)	Los datos capturados en el sistema coinciden con la documentación del cliente. (C/I)	Se cuenta con el KYC.(C/I)	Se encuentra completo el formato del KYC. (C/I)	DESVIACIONES ENCONTRADAS	CONCLUSIÓN (EFICAZ/ INEFICAZ)	OBSERVACIONES

8. MUESTREO ESTADISTICO DE LA REVISIÓN DE LOS CONTROLES.

El objetivo de contar con herramientas cuantitativas para el muestreo estadístico, permiten determinar el número de evidencias a solicitar de la actividad que implique una revisión mediante la selección de una muestra de datos o información.

Los conceptos del muestreo estadístico se presentan a continuación:

Universo. El conjunto de todos los posibles resultados de un fenómeno, se denomina elemento a cada uno de sus componentes, conjunto total de datos sobre los cuales el auditor va selecciona una muestra sobre la que desea hacer sus conclusiones.
Muestra. Selección de elementos del universo, también denominado subconjunto del universo.
Muestreo. Proceso que consiste en la selección de elementos:

- Muestreo Estadístico. Procedimiento de muestreo realizado de manera aleatoria o al azar mediante técnicas estadísticas.
- Muestreo No Estadístico. Procedimiento de muestreo realizado en base al juicio profesional, sin utilizar alguna técnica estadística.

Tamaño de la muestra: Número de elementos a seleccionar en el proceso de muestreo. Es la población a seleccionar mediante la cual el auditor realizará su análisis y podrá emitir sus conclusiones.

Consideraciones sobre el tamaño de la muestra.

•El tamaño estará en función al margen de error que el auditor está dispuesto a asumir.

- •Nivel de confianza.
- •Tamaño del universo.

Análisis cuantitativo, dimensión finita conocida el cual se utiliza cuando se conoce el tamaño o dimensión del universo del cual se va a extraer la muestra.

El método se utiliza para estudios donde la variables de carácter cuantitativo, es decir que se pueda medir como por ejemplo los saldos de una cuenta contable.

Fórmula para estimar el tamaño de la muestra.**

$$n= \frac{Z\alpha^2 * N * p * q}{e^2 * (N-1) + Z\alpha^2 * p * q}$$

Donde:

n: Tamaño de la muestra.

N: Tamaño del universo.

e: Error muestral deseado. $Z\alpha$: Z, es el valor correspondiente a la distribución Normal Estándar, al nivel de confianza α.

p: prevalencia esperada del parámetro a evaluar.

q: q=(1-p).

El parámetro p es desconocido, por lo que es recomendable asignarle el valor de 0.5, el cual hace que el tamaño muestral aumente.

Tabla de valores de la función de distribución normal estándar, valuada a los niveles de confianza comúnmente utilizados.

Nivel de Confianza	75%	80%	85%	90%	95%	99.00%
Valor de α	1.15	1.28	1.44	1.65	1.96	2.58

**Fórmula estadística

Ejemplo:

Universo: 10,000 registros

.

Error muestral deseado: 5%.

Nivel de confianza del 95%.

Valor de α.= 1.96

n=(1.96)2∗10,000∗0.5∗0.5(0.05)2∗10,000−1+1.962∗0.5∗0.5

$\therefore \boldsymbol{n}=\mathbf{370}$

Técnicas de muestreo. Para fines de las revisiones de control interno, la selección de los elementos se basan dentro del término considerado muestreo sin remplazo, es decir el ejercicio no permitirá seleccionar en más de una ocasión al mismo elemento.

Muestreo Aleatorio Simple. Una vez definido el tamaño de la muestra sobre la población, el proceso de muestreo aleatorio consiste en extraer al azar los elementos sin hacer distinción entre los distintos tipos de elementos.

Algoritmo

•Crear un identificador único para cada elemento dentro de la población.

•Generar un número aleatorio, definido entre 1 y el número de registros de la población.

1. Fórmula en excel, aleatorio.entre(1,n)
2. Se asigna un número aleatorio a cada elemento dentro de la población.

•Copiar como valores el número aleatorio, para que no se recalcule tantas veces se actualice la hoja de cálculo.•Ordenar de forma ascendente la base de datos o población, tomando como base la columna donde se generó el número aleatorio.

•Tomar los elementos uno a uno hasta llegar al tamaño de la muestra.

Ejemplo:

		Selección de datos		
Número de registro	Aleatorios	Número de registro	Aleatorio ordenado	Contador
1	13	72	2	1
2	11	14	3	2
3	18	89	4	3
4	48	50	5	4
5	10	6	7	5

6	7	22	7	6
7	88	102	7	7
8	50	5	10	8
9	81	15	10	9

:

• Población de 107 elementos.

• Error estándar 5%.

• Nivel de Confianza: 95%

• Tamaño de muestra: 84 elementos.

9. CONCLUSIONES.

La Dirección General de Banco debe de tomar acciones, validando políticas, solicitando que los objetivos del control cumplan con las expectativas y apoyando al desarrollo de una cultura de declaración de riesgos operacionales en todas las área de la Institución.

Se debe identificar, evalúar y gestionar los riesgos operacionales y en la mismo sentido se debe realizar la evaluación de los controles para conocer su eficacia como mitigantre de los riesgos.

Las metodologías cualitativas integran una forma de analizar la información generada, sin embargo, el área de Riesgo Operacional y Control Interno debe encontrar la manera de desarrollar métricas para definir de manera general tomando en cuenta la importancia de las actividades que se realizan en cada una de las áreas, cuales son los riesgos de alto impacto que deben de tener un tratamiento inmediato, para reducir la calificación del riesgo y evitar lo más posible quebrantos o multas a la Institución, las cuales tienen como consecuencia impactos negativos en el rendimiento accionario del banco y en la reputación a nivel sectorial (riesgo reputacional),

La captura de eventos de pérdida en la base de datos, requiere un análisis individualizado y documentado para determinar de manera real como se calificó el riesgo en un principio. Se debe contar con una base de datos de 5 años para poder calcular el VAR operacional.

La gestión del Riesgo Operacional y Control Interno conlleva a la asunción de responsabilidades para mitigar y evaluar, por lo que se requiere un equipo de trabajo especializado y certificado que analice la información en base a las metodologías aprobadas en el Banco.

10. BIBLIOGRAFIA BÁSICA

- Administración integral de riesgos de Negocio, Deloitte & Touch, fundación de investigación.
- CUB, Circular Única de Banco, Comisión Nacional Bancaria de Valores.
- Libro. La gestión del riesgo operacional: de la teoría a su aplicación. Autora Ana Fernández Laviada