Scotia Securities™
Sociedad Comisionista de Bolsa

SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERACIONAL O SARO

La Superintendencia Financiera de Colombia SFC mediante la expedición de las Circulares Externas 048 del 22 de Diciembre y 049 del 27 de Diciembre del 2006, fijó las bases y los lineamientos mínimos que deben ser implementados para el desarrollo de un Sistema de Administración del Riesgo Operacional (SARO) en el sistema financiero colombiano, posteriormente expidió la Circular Externa 041 del 29 de Junio del 2007 y estableció como fecha límite el primero de julio del 2008 para implementar en su totalidad el SARO.

Pues bien, conscientes del mejoramiento continuo en nuestra organización y de las responsabilidades institucionales, la Junta Directiva en la reunión No. 456, realizada el 25 de enero del 2006, aprobó la conformación del Grupo de Trabajo que se denominó PROYECTO BASILEA - SARO – SARLAFT, el cual desarrolló e implementó en el Banco el Sistema de Administración de Riesgo Operacional (SARO), el cual no solo nos permite cumplir con la normatividad de la Superintendencia Financiera de Colombia, sino que nos ubica en los estándares internacionales de competitividad.

El Sistema está compuesto por elementos mínimos (Políticas, Procedimientos, Documentación, Estructura Organizacional, Registro de Eventos de Riesgo Operacional, Órganos de Control, Plataforma Tecnológica, Divulgación de Información y Capacitación) mediante los cuales se busca obtener una efectiva administración, que permita a la Comisionista Identificar, Medir, Controlar y Monitorear eficazmente éste Riesgo y de ésta forma obtener la satisfacción de los clientes y grupos de interés, mediante la mejora continua de sus procesos.

En consideración a lo anterior, se presentó a la organización, una vez aprobado por la Junta Directiva, el documento denominado **MANUAL DEL SISTEMA DE ADMINISTRACIÓN DE RIESGO OPERACIONAL SARO de** SCOTIA SECURITIES SSC, con el propósito de brindar un marco conceptual y metodológico para la gestión y supervisión efectiva del Riesgo Operacional, que es de aplicación y actualización permanente y de estricto cumplimiento en toda la organización.

Gestión del Riesgo Operacional (RO)

La gestión de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales.
Es un proceso iterativo que consta de una serie de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.
Para gestionar adecuadamente el riesgo operacional es fundamental contar con un proceso de seguimiento eficaz, que, realizado periódicamente facilite la rápida detección y corrección de deficiencias en las políticas, procesos y procedimientos de gestión del riesgo operacional, lo que a su vez reduzca sustancialmente la frecuencia y la severidad de las perdidas.

Estructura Organizacional Del Saro

El Banco que soporta Scotia Securities tiene un modelo de estructura organizacional centralizada para la Gestión del Riesgo Operacional, que permitirá desarrollar, establecer, implantar y mantener el Sistema de Administración de Riesgo Operacional SARO.

La estructura de la Gerencia de Enterprise:

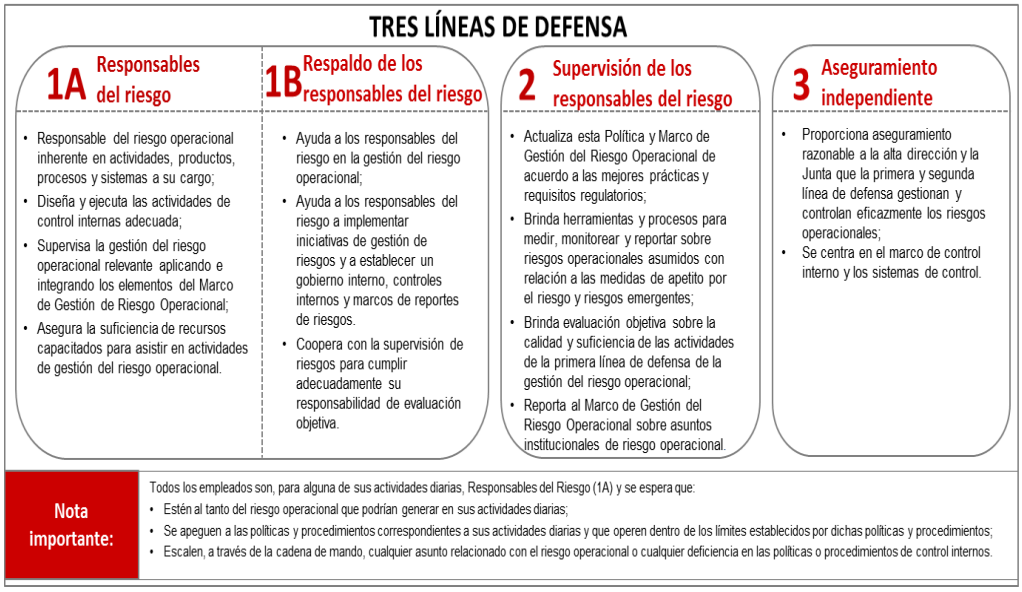
El marco de gestión de riesgos del Banco se basa en el modelo de tres líneas de defensa. Dentro de este modelo, la Primera Línea de Defensa compuesta por las líneas de negocio y la mayoría de las funciones de soporte, es responsables de identificar y gestionar los riesgos en los productos, las actividades, los procesos y los sistemas que existen en su línea de negocios.

Para reforzar el desarrollo del Marco de Gestión del Riesgo Operacional, el Banco ha implementado un nuevo modelo de administración del riesgo el cual está definido como la Línea de Defensa 1B – Control Interno, equipo centralizado responsable de coordinar, aportar una visión integral del riesgo para que las Unidades de Negocio 1A, cumplan con las políticas, procedimientos y programas, promoviendo conciencia sobre las tendencias globales en materia de riesgo regulatorio y operacional, definidos por la 2ª. Línea de defensa.

La Segunda Línea de Defensa compuesta por funciones de control tales como Unidades de Riesgos, Cumplimiento, Control Financiero, Legal, PCN, Seguridad de la Información, tiene como función aportar liderazgo, proporcionar supervisión independiente y someter a prueba eficazmente las actividades de gestión del riesgo operacional.

La Tercera Línea de Defensa está compuesta por el departamento de Auditoría Interna que le proporciona a la Alta Dirección y a la Junta Directiva un nivel de seguridad independiente y objetivo respecto a la eficacia del Marco de Gestión del Riesgo Operacional.

En esta estructura de gobierno de riesgos, los empleados en todas las áreas de la organización son responsables de la gestión de riesgos.



Gerencia Enterprise Risk

La Gerencia de Riesgo Operacional debe cumplir como mínimo con las siguientes condiciones:

- Contar con personal que tenga conocimiento en administración de riesgo operacional.
- Ser organizacionalmente de alto nivel y tener capacidad decisoria.
- No tener dependencia de los órganos de control, ni de las áreas de operaciones o de tecnología, ni relaciones que originen conflictos de interés.
- Contar con los recursos suficientes para desarrollar sus funciones.

En virtud de lo anterior, la Gerencia de Riesgo Operacional tendrá como mínimo las siguientes funciones:

- Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus riesgos operacionales, en concordancia con los lineamientos, etapas y elementos, mínimos previstos en la Circular Externa 049 del 2006 y Circular Externa 041 del 2007 de la Superintendencia Financiera de Colombia SFC.
- Desarrollar e implementar el sistema de reportes internos y externos, del riesgo operacional de la entidad.
- Administrar el registro de eventos de riesgo operacional.
- Coordinar la recolección de la información para alimentar el registro de eventos de riesgo operacional.
- Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos operacionales medidos.
- Establecer y monitorear el perfil de riesgo de la entidad e informarlo al órgano correspondiente, en los términos establecidos por la Circular Externa 049 del 2006 y Circular Externa 041 del 2007 de la Superintendencia Financiera de Colombia SFC.
- Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO y proponer sus correspondientes actualizaciones y modificaciones.
- Desarrollar los modelos de medición del riesgo operativo.
- Desarrollar los programas de capacitación de la entidad relacionados con el SARO.
- Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.

- Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo, en los términos de la Circular Externa 041 del 2007 de la Superintendencia Financiera de Colombia SFC.

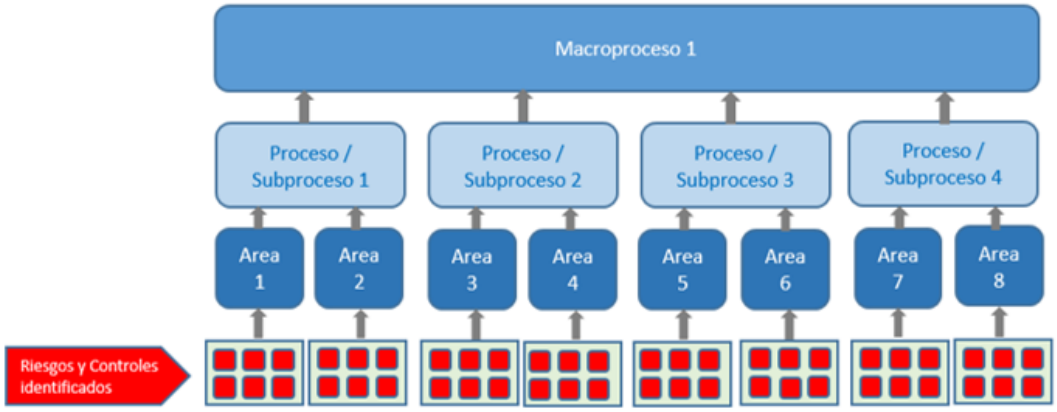
Etapas para la Administración de Riesgo Operacional

Para lograr una adecuada gestión de riesgos en la organización y dentro del ciclo PHVA (planear, hacer, verificar y actuar) el Banco ha implementado los siguientes pasos que aplican a Scotia Securities con el fin de identificar los riesgos operacionales a los que se encuentra expuesta la organización en el desarrollo de sus servicios

- **Identificación**:

- **Contexto estratégico y organizacional**: Consiste en la relación de la Comisionista y su entorno incluyendo aspectos financieros, operativos, competitivo, clientes, legales y de imagen; es decir, todos los aspectos de la organización. Se encuentra definido por el Código de Buen Gobierno Empresarial y Código de Conducta, la misión, la visión, los principios, los valores y los objetivos estratégicos del Banco que aplican a la Comisionista

  En cuanto al contexto organizacional se ha tomado como referencia el Mapa de Procesos y estructura administrativa. El Mapa de Procesos es la definición grafica de las actividades principales de la organización ilustrando la interrelación entre ellos y el exterior. Dentro de cada uno de los procesos principales se agrupan subprocesos que abarcan las actividades o tareas realizadas en cada una de las áreas del Banco y Filiales, para un mejor entendimiento se relaciona el siguiente esquema:



  Para la Scotia Securities se ha determinado el Mapa de Procesos que consta de:
  Procesos Estratégicos: involucra todas las actividades que se encuentran en la estrategia que definen y direccionan al demás proceso para la toma de decisiones acertadas, fortalecer la operativa del negocio y contribuir a mejorar la perspectiva del cliente.

  Procesos Misionales: Es un conjunto de actividades, que comienza con el cliente y termina con el cliente. Son aquellos que contribuyen directamente al cumplimiento de la razón de ser de la organización, son actividades que realiza el Banco para agregar valor y entregar su resultado para satisfacción de nuestros clientes y el cumplimiento de los objetivos estratégicos.

  Procesos de Apoyo: con procesos menores que permiten el desempeño de procesos superiores y determinando el éxito o el fracaso. Las actividades y los procesos se encuentran

relacionados con el abastecimiento de materias primas, con las herramientas, aplicaciones y equipos informáticos o con la formación del personal

Procesos de Control: permite a los directivos medir, comparar y corregir las actividades de la organización con la finalidad de cumplir con los objetivos estratégicos y desarrollar adecuadamente los planes establecidos.

- **Identificación de Riesgos Inherentes:**

La identificación y evaluación de riesgos es una parte fundamental de la gestión eficaz del riesgo operacional en el Scotia Securities y un componente básico del Marco de Gestión del Riesgo Operacional. Los riesgos se identifican, clasifican y evalúan, y su posible impacto se evalúa y reporta a la Gerencia y la Junta Directiva. Las herramientas y programas de gestión del riesgo operacional operan para respaldar la identificación y evaluación del riesgo operacional, cada uno de ellos con su metodología y/o estándares definidos. Las metodologías y los estándares también describen las expectativas con respecto a la frecuencia con la que se deben realizar, repetir o actualizar las actividades, y con la que se debe revisar y actualizar los resultados a fin de asegurar que las evaluaciones de riesgo reflejen la exposición del riesgo actual.

Las herramientas y metodologías se revisan y actualizan de manera regular para mantenerse al día con los cambios regulatorios y las mejores prácticas.

De acuerdo con la anterior, el Scotia Securities cuenta con la "Matriz de Riesgos y Controles" para que las unidades de negocio puedan identificar y documentar los riesgos inherentes a sus procesos, y definan los controles idóneos para su mitigación. Para ello el Banco cuenta con el documento ***"*Metodología para Documentación de Riesgos y Controles"** y ***"*Procedimiento para la documentación y actualización de las Matrices de Riesgos y Controles*"*** en la cual se describen los pasos para identificar los procesos, subprocesos, riesgos y controles, que permiten calificar el nivel de riesgo al cual se encuentra expuesto Scotia Securities

- **Medición Identificación de riesgos inherentes**

Una vez identificados los riegos inherentes asociados a los procesos de las áreas, la valoración de estos se realiza evaluando el impacto en caso de su materialización y la probabilidad de ocurrencia.

- **Impacto:** Mide la magnitud o posible consecuencia que puede ocasionar a la organización la materialización del riesgo. Es una variable que detalla de manera cualitativa y cuantitativa el nivel de severidad con el que se puede o pudo presentar el riesgo. Para una adecuada valoración, el Scotia Securities ha definido criterios de evaluación para que las Unidades de Negocio puedan determinar el posible impacto que este riesgo puede generar los cuales se describen a continuación:

IMPACTO FRAUDE Posibilidad que este riesgo pueda generar pérdidas económicas por fraude externo y/o interno	IMPACTO SEGURIDAD DE LA INFORMACIÓN - CYBER-SEGURIDAD Posibilidad que este riesgo pueda generar pérdida, robo o fuga de información sensible o confidencial de clientes o productos?	IMPACTO REGULATORIO Posibilidad que este riesgo pueda generar incumplimientos regulatorios ante el supervisor o entes de control (multas o sanciones ante Superfinanciera, Banrepublica, DIAN, Ministerios, Asobancaria, etc.)	IMPACTO REPUTACIÓN Posibilidad que este riesgo pueda afectar negativamente la Imagen y/o Reputación del Banco frente a los clientes, medios de comunicación o redes sociales	IMPACTO ECONÓMICO Este riesgo podría generar pérdidas económicas que afecte el PyG del Banco y/o filiales? Elija una opción según su criterio: BAJA ($0 COP hasta $33 MM COP) MEDIA (Entre $33 MM COP hasta $66 MM COP) ALTA (Entre $66 MM COP hasta $99 MM COP) EXTREMA (Mayor a $100 MM COP)
Extrema	Extrema	Extrema	Extrema	Extrema
Alta	Alta	Alta	Alta	Alta
Media	Media	Media	Media	Media
Baja	Baja	Baja	Baja	Baja

Cada uno de estos criterios son evaluados por las Unidades de Negocio, quienes de acuerdo con su experiencia deben medir el impacto en una escala de 4 alternativas (Extremo, Alto, Medio o Bajo). Para mitigar la subjetividad en este proceso, el Banco ha definido una tabla descriptiva dentro de cada criterio evaluado para que la Unidad de Negocio seleccione la opción más apropiada.

VARIABLES DE IMPACTO						
Nivel	Variable	RIESGOS ASOCIADOS Y PESO				
		Fraude	Seguridad de la Información	Regulatorio / Legal	Reputacional	Económico
1	Bajo	Los eventos de fraude pueden ser fácilmente detectados al inicio del proceso o no aplica.	Perdida de información no confidencial	Ninguna acción o sin impacto legal	Sin afectación a la marcao o clientes. Los medios de comunicación no son impactados.	$0 COP hasta $33 MM COP
2	Medio	Los eventos de fraude son detectados durante la ejecución del proceso.	Perdida de información confidencial	Glosa de ente regulador que requieren atención inmediata o demandas	Los clientes pueden cuestionar la confianza (recuperable en el tiempo). No se impactan los medios de comunicación.	$33 MM COP hasta $66 MM COP
3	Alto	Los eventos de fraude son detectados durante la ejecución del proceso y pueden representar montos importantes para la organización.	Extorsión al Banco por venta de información confidencial	Violación de leyes o regulaciones que repercutan en multas o procesos legales ante autoridades o entes de control.	Clientes y proveedores se ven afectados, junto con la marca. Dificultad para recuperar la confianza. Redes sociales afectadas.	$66 MM COP hasta $99 MM COP
4	Extremo	Los eventos de fraude no son de fácil identificación, las perdidas representan gastos significativos.	Demandas de clientes por fuga de información	Intervención del ente regulador, sanciones de entes de control.	Afectación directa a los clientes y proveedores. Medios de comunicación formales afectados. Perdida total de la confianza.	Mayor a $100 MM COP

- **Probabilidad:** Corresponde a la posibilidad de que algo suceda, mide la posibilidad de ocurrencia del riesgo, al considerar criterios de frecuencia y teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Se establece los siguientes criterios de valoración.

PROBABILIDAD - EXPOSICIÓN La probabilidad que usted considera que podría ocurrir este riesgo es: BAJA (1-50 veces al año) MEDIA (De 50 a 100 veces al año) ALTA (De 100 a 250 veces al año) EXTREMA (Mas de 250 veces al año)	COMPLEJIDAD La ejecución del proceso se requiere un nivel de complejidad: BAJA (Nivel de conocimiento Bajo) MEDIA (Nivel de conocimiento General) ALTA (Se requiere experiencia general) EXTREMA (Se requiere amplio conocimiento y experiencia específica)	NIVEL DE PROCESAMIENTO El proceso requiere de un nivel de procesamiento: BAJA (Procesamiento automático) MEDIA (Semiautomático) ALTA (Manual sin complejidad) EXTREMA (Altamente manual)
Extrema	Extrema	Extrema
Alta	Alta	Alta
Media	Media	Media
Baja	Baja	Baja

Cada uno de estos criterios son evaluados por las Unidades de Negocio, quienes de acuerdo con su experiencia deben medir la probabilidad de ocurrencia en una escala de 4 alternativas (Extremo, Alto, Medio o Bajo). Para mitigar la subjetividad en este proceso, el Scotia Securities ha definido una tabla descriptiva dentro de cada criterio evaluado para que la Unidad de Negocio seleccione la opción más apropiada.

VARIABLES DE PROBABILIDAD				
Nivel	Variable	VARIABLES		
		Frecuencia	Complejidad	Nivel de procesamiento
1	Bajo	1-50 veces al año	Se requiere un nivel de procesamiento y conocimiento bajo	Procesamiento automático
2	Medio	51-100 veces al año	Se requiere conocimiento general del proceso a ejecutar	Procesamiento semi - automático
3	Alto	100-250 veces al año	Se requiere de experiencia para ejecutar el proceso	Manual sin complejidad
4	Extremo	>250 veces al año	Conocimiento ampliado de información y experiencia específica para ejecutarlo	Altamente manual

La combinación de las anteriores variables de probabilidad (eje Y) y de impacto (eje X) determinan una calificación cuantitativa y cualitativa que permite ubicar el riesgo inherente en el siguiente mapa colorimétrico 4X4:

RIESGO INHERENTE

		IMPACTO			
		Bajo	Medio	Alto	Extremo
FRECUENCIA	Extrema	0	0	0	0
	Alta	0	0	0	0
	Medio	0	0	0	0
	Bajo	0	0	0	0

PERFIL DE RIESGO INHERENTE

Bajo
Medio
Alto
Extremo

- **Definición y Medición de Controles**

  Los controles corresponden a las medidas de tratamiento, prevención o protección de los riesgos, las cuales permiten reducir o mitigar el impacto de estos; con la prevención se actúa sobre las causas de los riesgos y por tanto se disminuye su probabilidad o frecuencia de ocurrencia, y con la protección se minimiza el nivel de impacto que el riesgo puede llegar a presentar una vez se materialice.

  El diseño de los controles debe contener lo siguiente:

DESCRIPCIÓN DEL CONTROL Describa el control existente especificando Quien?, Como? Que?, y Cuándo? (si aun no tiene un control definido, coloque No "Existe Control"	TIPO DE CONTROL (Seleccione uno)	NATURALEZA DEL CONTROL (Seleccione uno)	PERIODICIDAD DEL CONTROL (Seleccione uno)	EL CONTROL ESTA DOCUMENTADO Y APROBADO? (Flujograma, Manual de Funciones)	SE EVIDENCIA CONTROL DUAL?	EXISTE EVIDENCIA DEL CONTROL? (Seleccione uno)
	Preventivo	Automático	A demanda	SI	SI	SI
	Detectivo	Manual	Diario	NO	NO	NO
	Correctivo	No existe	Semanal			
	No Existe		Trimestral			

DESCRIBA BREVEMENTE EL SOPORTE DE LA EVIDENCIA (Reportes de conciliacón, Correos, Informes…)	DESCRIBA LA PRUEBA A REALIZAR	FRECUENCIA DE LA PRUEBA	CARGOS RESPONSABLES DEL CONTROL	EL CARGO ES EL ADECUADO PARA EJECUTAR EL CONTROL?
		Mensual		Deficiente
		Trimestral		Promedio
		Semestral		Adecuado

- **Monitoreo**

La Gerencia de Enterprise Risk realiza de manera permanente el monitoreo y seguimiento de los riesgos operacionales para identificar los riesgos potenciales y ocurridos, y de esta manera establecer estrategias de evaluación de los controles asociados para cuestionar a las áreas dueñas de tales controles, y mitigar la probabilidad de materialización o reincidencia.
Para lo anterior, la Gerencia de Enterprise Risk ha establecido criterios para definir e identificar los riesgos como potenciales y ocurridos así:

- Riesgos o eventos materializados que hayan generado pérdidas contabilizadas en las cuentas del gasto de riesgo operativo. (estos riesgos son identificados mediante el proceso de monitoreo de pérdidas, con sus criterios de relevancia definidos)

- Riesgos derivados del reporte de eventos no monetarios, que de acuerdo con los criterios definidos en el proceso de monitoreo de pérdidas sean considerados relevantes

- Issues de Auditorías relevantes, que estén asociados a deficiencias o ausencias de controles operativos mitigantes, que puedan generar la materialización de un riesgo operacional.

- Controles mitigantes cuya última evaluación realizada con esta metodología por la Gerencia de Enterprise Risk, haya sido considerada como “Insatisfactoria”

- Otros Riesgos o procesos definidos por la Gerencia Enterprise Risk.

De acuerdo con lo anterior, la Gerencia de Enterprise Risk define el cronograma de trabajo para monitorear y evaluar los controles asociados a los focos de riesgo más relevantes. Este plan de trabajo debe ser proyectado y ejecutado en los próximos 6 (seis) meses, y antes del próximo proceso de monitoreo para la identificación de nuevos riesgos potenciales.

La ejecución de los controles es responsabilidad de todos los empleados de Organización. Todos los controles establecidos hacen parte del Sistema de Control Interno de la Scotia Securities - Sociedad Comisionista de Bolsa