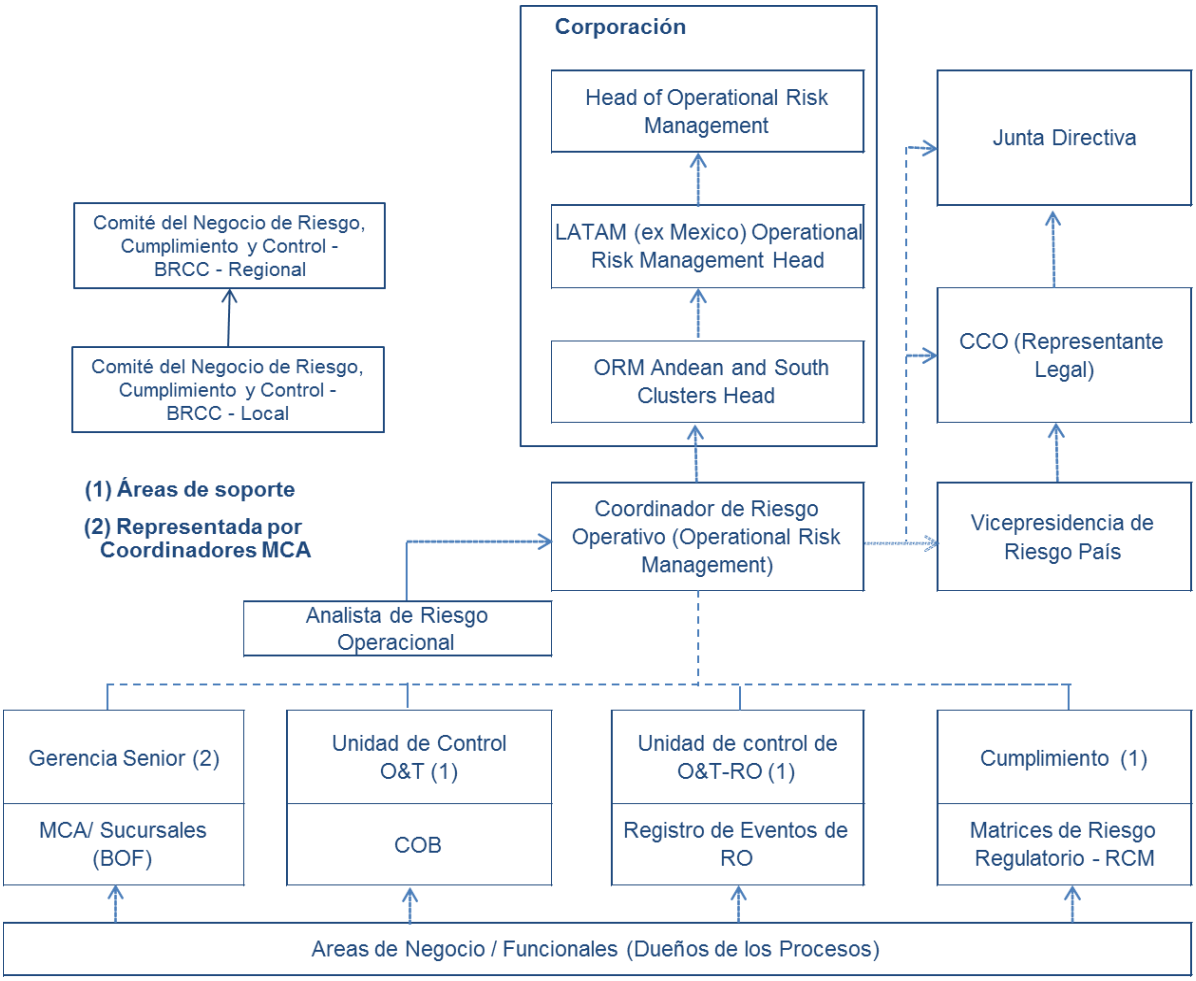
RIESGO OPERATIVO

El Capítulo XXIII de la Circular Básica Contable y Financiera expedida por la hoy Superintendencia Financiera de Colombia define Riesgo Operativo como "*la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y reputacional, asociados a tales factores.*"

ESTRUCTURA DEL SARO

La estructura para la administración del riesgo operativo de Cititrust-Colombia S.A. es la siguiente:



Unidad de Riesgo Operacional

La Unidad de Riesgo Operacional pertenece al área denominada corporativamente como "Operational Risk Management" – ORM. Entre sus principales funciones se encuentran:

- Hacer seguimiento a la administración y control del Riesgo Operativo
- Presentar para aprobación de la Junta Directiva los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente su riesgo operativo
- Monitorear el perfil de riesgo individual y consolidado de la entidad e informarlo a la Junta Directiva
- Realizar seguimiento a las medidas adoptadas para mitigar el Riesgo Inherente, con el propósito de evaluar su efectividad
- Proveer las instrucciones a los Coordinadores de Riesgo Operativo para la conformación del perfil individual de cada una de las áreas y conformar el perfil de riesgo consolidado por Entidad. Monitorear su evolución y hacer su presentación semestral a la Junta Directiva.
- Desarrollar los programas de capacitación de la entidad relacionados con Riesgo Operativo.

Comité del Negocio de Riesgos, Cumplimiento y Control – (BRCC por sus siglas en inglés)

El Comité del Negocio de Riesgos, Cumplimiento y Control (BRCC) sesiona trimestralmente y está conformado por las siguientes unidades:

- Representante Legal – CCO, o su delegado
- Legal
- Cumplimiento
- Finanzas
- Operaciones y Tecnología
- Negocios/Segmentos
- Recursos Humanos
- Vicepresidente de Riesgo País
- Auditoría Interna
- Representante del Negocio para Riesgo y Control
- Unidad de Riesgo Operativo

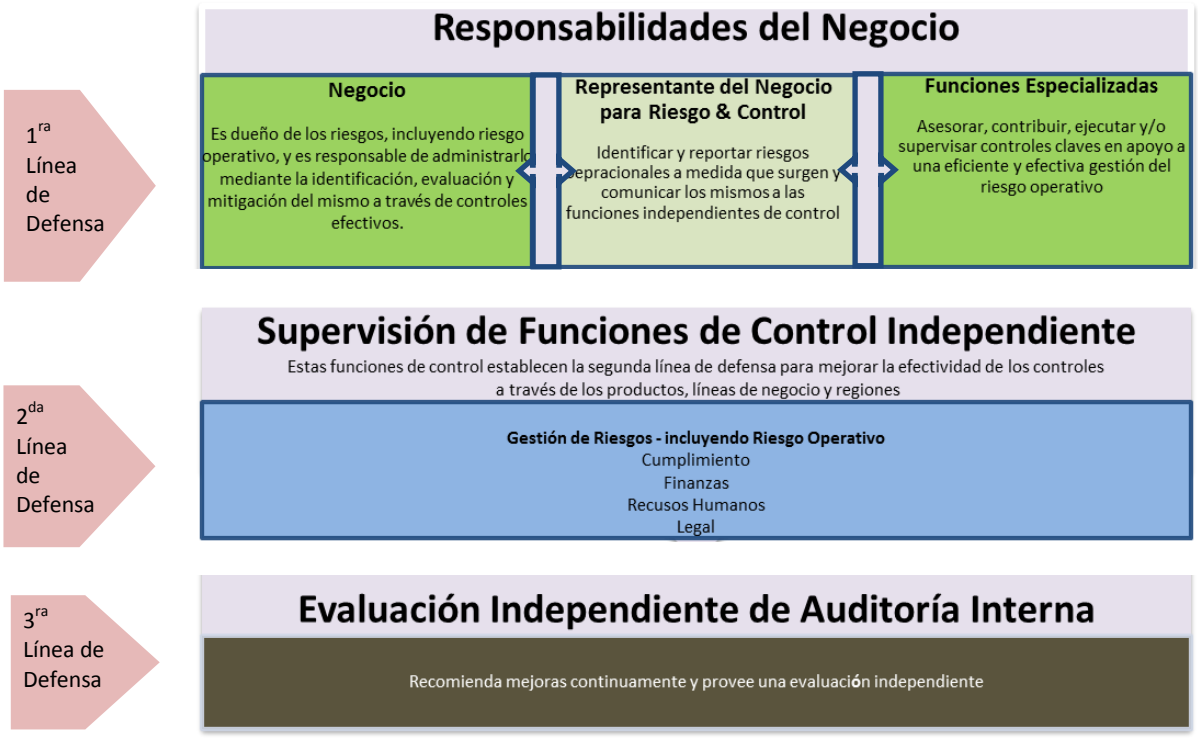
Las principales responsabilidades del Comité del Negocio de Riesgos, Cumplimiento y Control son las siguientes:

- Analizar y discutir las situaciones y debilidades de control y cumplimiento, incluyendo temas regulatorios, más importantes que impacten las actividades de negocio, así como evaluar y dar seguimiento a los planes de acción para la corrección y mitigación de dichas debilidades.

- Revisar y analizar la calificación asignada a la entidad, considerando la información presentada por las diferentes áreas en cuanto a los resultados de la herramienta de autoevaluación denominada "Evaluación de Control de la Gerencia (MCA por sus siglas en ingles), y de la información de las fuentes independientes (Revisoría Fiscal, Auditoria Interna, Cumplimiento, etc.)

3 Líneas de Defensa para la Gestión de Riesgo Operativo

En el esquema de "Autocontrol" aplicado, los dueños de las áreas funcionales, negocios y productos, son quienes identifican los riesgos, diseñan e implementan los controles, así como las herramientas de monitoreo para verificar su eficacia e implementación. Dicho esquema se blinda a través de tres niveles de defensa que se definen como sigue:



- ✓ **Gerencia del Negocio y Funciones Especializadas**
  La gerencia de las unidades de negocio junto con las gerencias funcionales y de operaciones, son dueñas de sus riesgos operativos y por ende, son el primer frente para el manejo de los mismos. Como dueñas de sus riesgos, estas gerencias son responsables de la mitigación de posibles riesgos identificados por medio del desarrollo e implementación de sistemas de control interno y la verificación del diseño y efectividad de los controles.

  La gerencia del negocio y las gerencias funcionales, tienen un representante denominado Representante del Negocio para Riesgo y Control, responsable de coordinar con las áreas la aplicación apropiada del programa diseñado corporativamente para la Gestión del Riesgo Operacional y velar por el cumplimiento de la normatividad local al interior de las mismas. Este representante estará en permanente contacto con la Unidad de Riesgo Operativo (URO) y demás áreas con funciones de control.

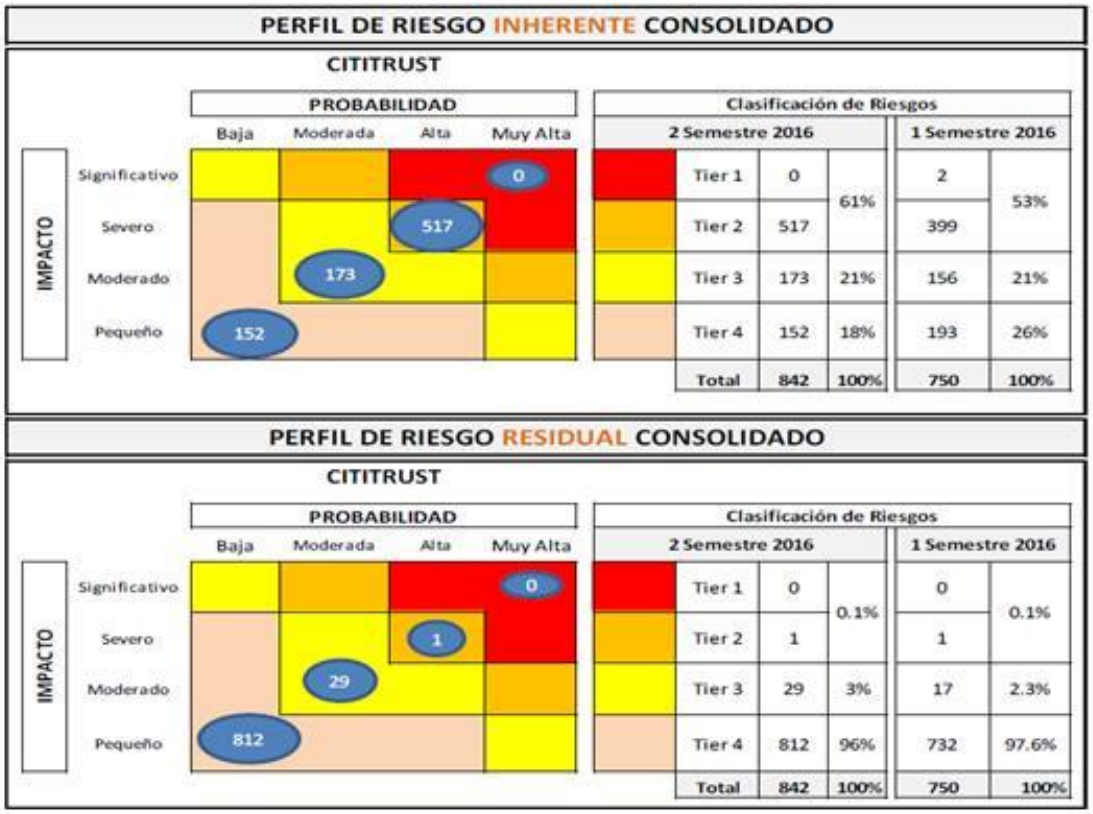
- ✓ **Unidad de Riesgo Operativo (URO) y Otras Funciones de Control**
  La URO y demás áreas de control, tales como Cumplimiento, Finanzas, Recursos Humanos y Legal, comprenden la segunda línea de defensa. Esta segunda línea de defensa colabora directamente con las áreas responsables de la gestión de riesgo operativo para identificar, prevenir y conducir las acciones que aseguren que las causas raíces y temas recurrentes sean manejados con un mayor alcance y de forma más amplia.

- ✓ **Auditoría Interna**
  El área de Auditoría Interna es el tercer frente de defensa. Esta área, ejecuta revisiones independientes para evaluar y calificar las distintas áreas de negocio y funciones de acuerdo a los requerimientos corporativos y regulatorios locales con el fin de informar su opinión de la efectividad de los procesos pertinentes y con base en ellas formula recomendaciones para llevar a cabo mejoras en los mismos.

FASES PARA LA GESTION DEL RIESGO OPERATIVO

Fases en la Gestión del Riesgo Operativo		
Evaluación de Riesgo Anual	**Periódicamente**	**Trimestralmente**
• Inventario Procesos Significativos • Actualizar y/o documentar procesos clave. • Riesgos Importantes ⟹ Riesgos Significativos • Identificar/diseñar los controles clave. • Identificar/diseñar los Métodos de Monitoreo • Identificar vulnerabilidades y riesgos emergentes	• Ejecutar actividades de Monitoreo	• Evaluación de resultados del monitoreo a los controles. • Análisis integral de las debilidades de control y planes de acción correctivos. • Revisión integral de los riesgos emergentes. • Análisis consolidado de otras fuentes de información. • Determinar rating de control para cada área • Realizar el Comité de Riesgo y Control donde se define el rating de control para la Entidad
Semestralmente	**Cuando sea requerido**	
• Evaluar efectividad de los controles claves validando eficacia del diseño y grado de implementación. • Definir perfil de riesgo inherente y residual.	• Documentar y escalar las deficiencias de control. • Implementar Planes de Acción para corregir las deficiencias identificadas. • Registrar las deficiencias en los sistemas Corporativos para su seguimiento. • Implementar programa de Gestión para: cambios en procesos, nuevos servicios, productos.	

PERFIL DE RIESGO INHERENTE Y RESIDUAL AL 28 DE FEBRERO DEL 2017



El perfil de riesgo inherente y residual consolidado de la Entidad, está representado por las gráficas anteriores, donde se visualiza cómo están distribuidos los riesgos inherentes y residuales en su conjunto según su nivel de criticidad (rating asignado).

Realizando un análisis comparativo entre Junio 2016 y Febrero 2017 evidenciamos que el perfil de riesgo residual ha mostrado un comportamiento estable evidenciando una baja concentración en los riesgos de mayor severidad. Para los riesgos residuales clasificados en las escalas de mayor severidad se tienen identificadas Deficiencias de Control a fin dar seguimiento a la mejora de los controles mitigantes.

Las Principales fuentes de detección de deficiencias han sido:

- Auditoria Interna
- Gerencia
- MCA
- Seguridad de la Información
- Regulador (AML-Reportes Regulatorios)

Calificación del Perfil de Riesgo Residual: Aceptable con Oportunidades de Mejora

Entendimiento de la escala de criticidad:
Los riesgos clasificados en Tier 1 y 2 son considerados los riesgos significativos.
Los riesgos clasificados en Tier 3 son los riesgos medios
Los riesgos clasificados en Tier 4 son los riesgos bajos

En caso que se identifiquen deficiencias de control deben implementarse controles compensatorios, donde sea posible, o identificar los controles complementarios, en caso de existir, que permitan mitigar los riesgos relacionados a niveles aceptables mientras se implementan los controles claves respectivos.