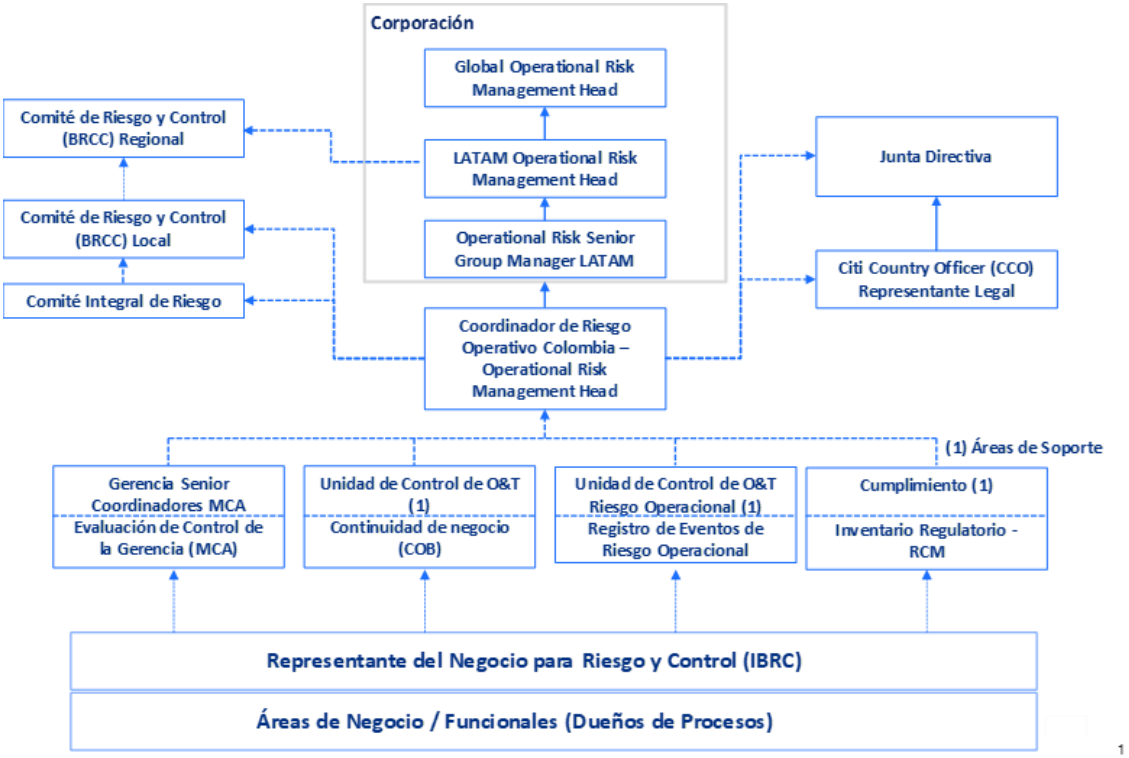
# *Sistema de Administración de Riesgo Operativo*
# *Citibank Colombia S.A.*

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 Citibank 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 BRCC es un comité que hace parte integral del marco de sistema de control y cumplimiento de la unidad, es decir, pertenece a la estructura a través de la cual cada vehículo legal da cumplimiento al SARO.

Este es el comité clave de riesgo y control en Citi. Tiene un rol de gobierno importante en la identificación, evaluación, monitoreo, reporte y gestión de los riesgos de GRC. Este reúne las tres líneas de defensa con un objetivo común: garantizar que se mantenga un sólido marco de control y riesgo y una cultura del riesgo en toda la franquicia. El BRCC ayuda a la alta gerencia a centrarse en los riesgos más importantes, los problemas de control y los riesgos emergentes que afectan los objetivos del negocio, así como en la oportunidad y la eficacia de las medidas correctivas adoptadas para mejorar los controles, incluidas las deficiencias relacionadas con el incumplimiento de los requerimientos regulatorios, normas y políticas corporativas. Como parte de este proceso, deben: (i) conocer y entender los riesgos residuales agregados de Evaluación de Control de la Gerencia (en adelante "MCA", por sus siglas en inglés Manager´s Control Assessment), que exceden el apetito por el riesgo y revisar las acciones de gestión de riesgos residuales propuestas para reducir el riesgo a un nivel aceptable. (ii) Revisar la idoneidad y efectividad de los resultados del programa de MCA incluyendo la calificación general de la entidad y de las unidades de evaluación.

Este comité es dirigido por el Representante Legal, CCO, en coordinación con el Representante de Riesgo y Control del Negocio "IBRC".

Las principales responsabilidades de este comité son:

- Reunirse trimestralmente de acuerdo con los miembros permanentes establecido en sus estatutos.
- Analizar y discutir las situaciones de control y cumplimiento, incluyendo temas regulatorios, que impacten las actividades de negocio durante el trimestre en evaluación.
- Evaluar y dar seguimiento a los planes de acción para la corrección y mitigación de las situaciones de control y cumplimiento reportadas.
- Reportar los riesgos emergentes significativos para la entidad, así como los riesgos operativos residuales identificados por el negocio o las áreas independientes.
- Revisar la calificación asignada a la(s) entidad(es) como resultado del ejercicio de "Evaluación de Control de la Gerencia", y se cuente con los informes independientes de cada fuente de información (incluido Auditoría Interna, Revisoría Fiscal).

***Tres 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:

| Línea de Defensa | Unidades Organizacionales | Roles y Responsabilidades |
|---|---|---|
| **1ra Línea de Defensa** | Negocio<br>Representantes del Negocio para Riesgo y Control<br>Especialistas Funcionales<br>Gerencia de País y Región<br>Funciones Corporativas<br>Infraestructura, Operaciones y Tecnología (EIO&T)<br>Finanzas | La primera línea de defensa es la dueña de los riesgos inherentes o emergentes de su negocio y es responsable de identificar, evaluar y controlar efectivamente esos riesgos a los que están expuestos para que estén dentro del apetito de riesgo definido en el Marco de Gestión de Riesgo Operacional. |
| **2da Línea de Defensa** | Gerencia Independiente de Riesgo (incluyendo Riesgo Operacional)<br><br>Gerencia Independiente de Riesgo de Cumplimiento (ICRM) | La 2da línea de defensa establece los estándares de riesgo y control para la 1ra Línea de defensa y los gestiona y supervisa activamente en toda la entidad.<br><br>La Unidad de Riesgo Operacional es responsable de establecer los requisitos para la gestión del riesgo operacional, supervisando y evaluando la implementación del Marco de Gestión de Riesgo Operacional, y las actividades ejecutadas por la 1ra Línea de Defensa.<br><br>ICRM está diseñada para supervisar y evaluar productos, funciones, actividades y las entidades legales en la gestión del riesgo de cumplimiento, así como para promover una conducta de negocio que sea consistente con la Misión y Propuesta de Valor de Citi y el Apetito de Riesgo de Cumplimiento |
| **3ra Línea de Defensa** | Auditoría Interna | La 3ra línea de defensa es responsable de entregar a la Alta Gerencia evaluaciones independientes sobre la efectividad de la Gestión de Riesgo Operacional. |
| **Funciones de Control y Soporte** | Recursos Humanos<br><br>Legal<br><br>Servicios de Seguridad e Investigación (CSIS)<br><br>Asuntos Públicos (Global Public Affairs) | Estas unidades prestan funciones de control y soporte a las tres líneas de defensa.<br>Las funciones de control y soporte están sujetas a los procesos de evaluación independiente de acuerdo con las categorías de riesgo que generan (es decir, riesgo operativo, riesgo de cumplimiento, riesgo de reputación). |

## Procedimientos y metodologías para la administración y gestión del riesgo operativo

Los procedimientos y actividades para la gestión del Riesgo Operativo han sido diseñados para dar cumplimiento a lo establecido en el capítulo XXIII de la Circular Básica Contable y siguiendo las políticas corporativas globales de Citi, entre las cuales se ha establecido un marco estándar de trabajo llamado Gobierno Riesgo y Control - GRC, (en adelante "GRC" por sus siglas en inglés Governance, Risk and Control), para lograr una mayor convergencia a nivel global en la gestión del riesgo operativo, incluyendo también los riesgos de cumplimiento regulatorio, de conducta, reputacional y legal. Así mismo, se ha establecido como base fundamental para el manejo de las etapas del SARO, el programa corporativo denominado MCA.

### 1. Marco estándar de GRC

El marco estándar de GRC está fundamentado en los siguientes pilares:

#### i. Estructura de evaluación:

El riesgo se identifica, evalúa y gestiona por distintas jerarquias de Citi. El objetivo de la estructura de evaluación de GRC es estandarizar, en la medida de lo posible, el nivel más apropiado en el que los riesgos son evaluados y gestionados, mientras se mantiene la alineación con la gerencia. Esta estandarización mejora la agregación, el reporte y el análisis de datos en la 1ra y 2da línea de defensa. La estructura de evaluación de GRC esta categorizada en 3 niveles: (i) Unidades de Evaluación (AU por sus siglas en inglés Assessment Unit), (ii)Entidades de Gobierno de MCA (MGE por sus siglas en inglés MCA Governance Entities) (iii) Segmentos/Geografías.

**ii. Taxonomía de GRC:**

Se utiliza para la identificación, evaluación y reporte de los riesgos de GRC en la 1ra y 2da línea de defensa. La taxonomía de GRC consiste en una base de datos de búsqueda que contiene un inventario oficial y estándar de actividades, riesgos, controles, y herramientas de monitoreo.

**iii. Gestión y administración de deficiencias de control "Issues":**

Una deficiencia de control o "Issue" ocurre cuando un negocio no es capaz de mitigar el riesgo a un nivel aceptable debido a un diseño inadecuado, ejecución inefectiva o a la ausencia de un control adecuado. Estas deficiencias de control "issues" se incluyen en el MCA desde una perspectiva tanto de propiedad como de impacto, deben tener un plan de acción asociado que debe atender la causa raíz del problema y la implementación de cambios en los procesos y/o controles necesarios para mitigar el riesgo. El ciclo de vida de la gestión de las deficiencias de control "Issues" se utiliza para soportar al negocio en la gestión del riesgo: identificación, evaluación, remediación y cierre.

## 2. Estándares de la evaluación de control de la gerencia – MCA

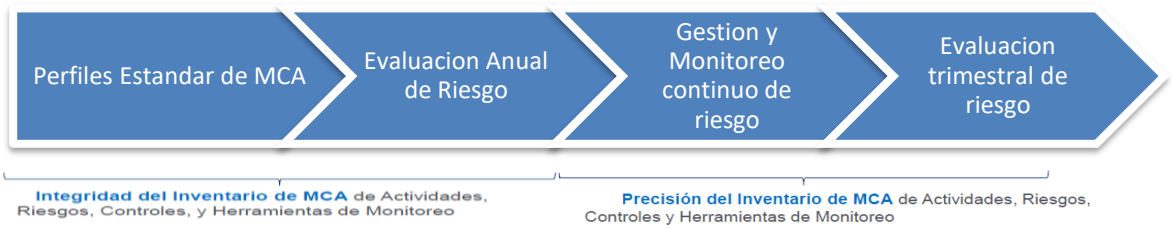
Por su parte, los estándares del MCA proporcionan el marco y las herramientas para enfocarse en: (i) La evaluación, monitoreo y mitigación de los riesgos inherentes más significativos, (ii) Identificar y evaluar los controles clave utilizados para mitigar dichos riesgos inherentes significativos, (iii) Administrar los riesgos residuales significativos para asegurar que se ejecuten de una manera que sea congruente con el apetito de riesgo de la entidad. El marco de trabajo de MCA cubre el ciclo de vida de la gestión de riesgo y está diseñado para ayudar a diagnosticar e identificar proactivamente deficiencias en el control y establecer e implementar planes correctivos para resolver o prevenir su potencial impacto en los objetivos del negocio y en pérdidas operativas.

El MCA está diseñado para asegurar que:

- Cada unidad de los vehículos legales de Citi tenga un enfoque dirigido a la identificación de deficiencias de control.
- La infraestructura de control sea adecuada para soportar las actividades de negocio y mitigar el Riesgo Operativo.
- Asegurar el escalamiento formal de las deficiencias de control identificadas en el monitoreo continuo que involucra esta herramienta, así como el establecimiento de planes de acción inmediatos ante fallas de control detectadas.
- Los activos de Citi y de los clientes están salvaguardados.

### i. Herramientas del MCA

El MCA utiliza 4 herramientas clave interconectadas para la gestión del riesgo operativo. Estas herramientas permiten la identificación del riesgo y control y la evaluación, monitoreo y gestión del riesgo residual dentro del marco de trabajo de GRC.




A continuación, se detallan los procedimientos y actividades incluidas para cada una de estas herramientas:

1. **Perfiles estándar de MCA:**

Es el inventario de las actividades, los riesgos, los controles y las herramientas de monitoreo (ARCM por sus siglas en ingles), que los productos/funciones identifican globalmente (Top-down) como base del MCA y se asignan a cada una de las unidades de evaluación aplicables. Cada perfil estándar de MCA incluye todos los riesgos significativos dentro de cada una de sus actividades principales. Las descripciones que complementan las actividades, riesgos, controles y herramientas de monitoreo deben ser claras, concisas, sin utilizar términos especializados y comprensibles para cualquier tercero o revisor independiente.

2. **Evaluación anual de riesgo: (ARA "Annual Risk Assessment" por sus siglas en ingles")**

El objetivo de la evaluación anual de riesgo "ARA" es asegurar la integridad y precisión del MCA dentro de una o más unidades de evaluación, y es la base de referencia para todos los demás procesos de MCA. Consta de las siguientes 6 actividades: (i)identificación de las actividades, riesgos, controles y herramientas de monitoreo a nivel global, (ii)identificación de las actividades, riesgos, controles y herramientas de monitoreo a nivel local, (iii)identificación de los riesgos de cumplimiento y controles asociados a regulaciones y políticas corporativas para mitigar riesgos incumplimiento, (iv)identificación de la exposición al riesgo debido a la dependencia de tecnología y proveedores de servicios externos e internos, (v)evaluación de riesgos inherentes, siguiendo la medición de criterios de frecuencia anticipada e importancia del impacto,(vi) evaluación del diseño del control y monitoreo, se identificar si los controles claves que hayan sido implementados cuentan con un diseño adecuado para mitigar los riesgos inherentes al nivel de riesgo aceptable para la organización y si los métodos de monitoreo que hayan sido implementados cuenten con un diseño adecuado para monitorear el desempeño de los controles clave. Esta evaluación de riesgo se debe hacer de forma anual.

3. **Gestión y monitoreo continuo del riesgo**

De acuerdo con el Capítulo XXIII de la mencionada circular cada vehículo legal debe hacer un monitoreo periódico del perfil de riesgo y de la exposición a pérdidas. El cumplimiento de lo anterior se realiza a través de la tercera herramienta del proceso de MCA que es la gestión y monitoreo continuo del riesgo. Los dueños de las Unidades de Evaluación deben considerar la siguiente información para evaluar el entorno de riesgo

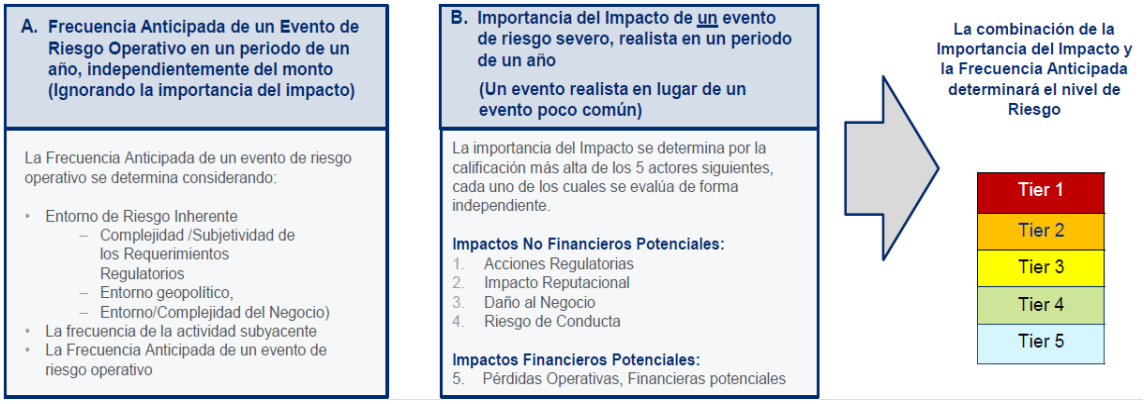
y el control operacional: (i)identificación y vinculación de deficiencias de control "issues" a las Actividades, Riesgos, Controles y Monitoreos (ARCM) de la Unidad de Evaluación.
(ii)vinculación de los eventos de riesgo operacional a las Actividades, Riesgos, Controles y Monitoreos (ARCM) de la Unidad de Evaluación. Para aquellos eventos en los que no existe un control clave en el MCA, debe documentarse como un control faltante para la unidad de evaluación que corresponda, (iii)análisis de lecciones aprendidas (Lessons Learned): Se requiere que los negocios y los especialistas funcionales de primera línea elaboren y publiquen un informe con el análisis de las lecciones aprendidas (Lessons Learned Report) para eventos adversos que ocurran dentro o fuera de Citi y que se consideren significativo de acuerdo con los lineamientos establecidos en esta política, (iv)documentación y revisión de los resultados de monitoreo: los dueños del control deben considerar las herramientas que proporcionan información relevante y oportuna del desempeño de los controles. Existen 3 tipos de herramientas de monitoreo en el MCA, métricas, pruebas y herramientas de gobierno y supervisión.

**4. Evaluación trimestral del riesgo**

La cuarta herramienta del proceso de MCA es la evaluación trimestral del riesgo. Su objetivo es consolidar las evaluaciones de riesgo y control para validar la precisión del MCA e implementar las acciones de gestión de riesgo residual en donde el riesgo es superior al apetito. Como resultado se obtiene calificaciones automáticas de riesgo residual individual y agregadas a nivel de unidad de evaluación y grupo de unidades de evaluación.

**Evaluación y medición de los riesgos operativos**

• Riesgos inherentes: El objetivo principal de esta evaluación es la identificación de los riesgos operativos más significativos en ausencia de controles. Los riesgos inherentes individuales se evalúan por medio de dos criterios independientes: frecuencia anticipada y la importancia del impacto. Se clasifican en 5 niveles (Tiers), siendo 5 el de menor riesgo y 1 el de mayor riesgo.




• Riesgos residuales: Los riesgos residuales individuales se determinan automáticamente utilizando la matriz definida abajo, que considera el nivel de riesgo del inherente individual y la calificación del desempeño de control a nivel de riesgo individual. Citi utiliza una escala con un nivel 1 al 5, en donde el nivel 1 es el riesgo más alto y 5 el más bajo.

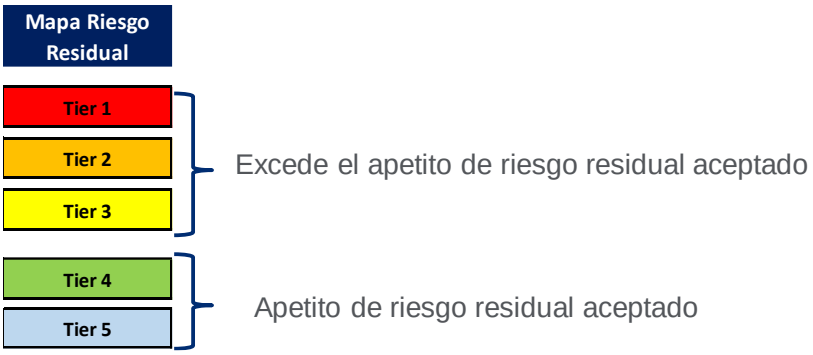
| Calificacion Riesgo Inherente | Evaluación total del Control según el riesgo | | | | |
|---|---|---|---|---|---|
| | - 3 Tier | - 2 Tier | - 1 Tier | Sin Cambio | |
| | Altamente Efectivo | Efectivo | Parcialmente Inefectivo | Inefectivo | |
| Tier 1 | Tier 4 | Tier 3 | Tier 2 | Tier 1 | |
| Tier 2 | Tier 5 | Tier 4 | Tier 3 | Tier 2 | |
| Tier 3 | Tier 5 | Tier 5 | Tier 4 | Tier 3 | |
| Tier 4 | Tier 5 | Tier 5 | Tier 5 | Tier 4 | |
| Tier 5 | Tier 5 | Tier 5 | Tier 5 | Tier 5 | |

Calificaciones agregadas de riesgo: La agregación se base en un promedio ponderado de los riesgos inherentes y residuales de cada categoría de la calificación y aplica un mayor peso al riesgo más alto para evitar el efecto de diluir excesivamente una gran cantidad de riesgos bajos. El resultado de la agregación es una calificación entre un nivel 1 a 5 en donde el nivel 1 es el más alto y 5 el más bajo.

**Perfil definido de riesgo operativo**

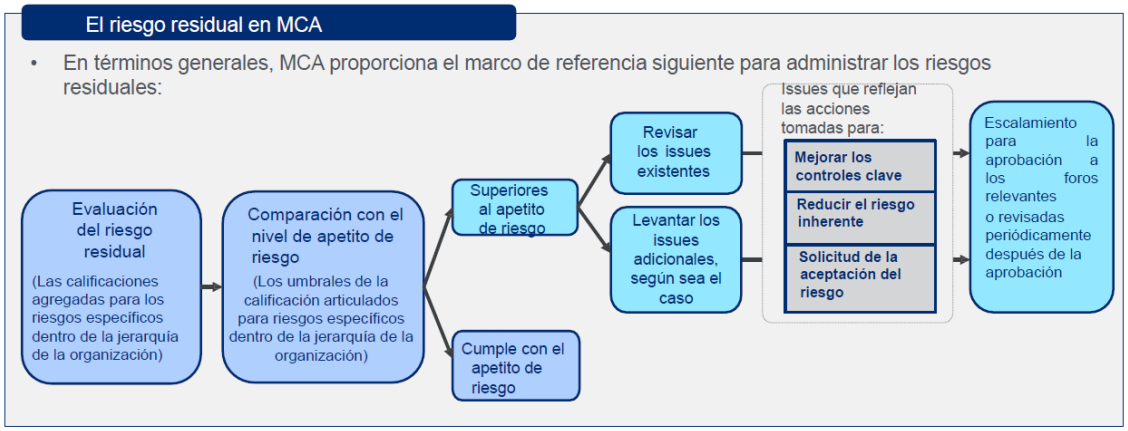
Cada vehículo legal, a través de su Junta Directiva, define el de riesgo operativo residual en el cual debe quedar acotado el perfil de riesgo aceptado, buscando lograr los objetivos de la organización. Este perfil de riesgo aceptado refleja la filosofía de gestión de riesgos de la entidad, y a su vez influye en la cultura y estilo operativo de la misma.

El siguiente gráfico, define el perfil de riesgo residual aceptado, el cual espera que todas las áreas se mantengan en niveles de Riesgo Residual dentro del nivel 4 Y 5.




Las unidades cuyo riesgo residual agregado excedan el Apetito al Riesgo Residual general aceptado deben realizar una gestión del riesgo residual a través de la apertura de "Deficiencias de Control" en el Sistema de Administración de Deficiencias (iCAPs); estas acciones se revisan en el comité trimestral de control y cumplimiento (BRCC) y se presentan a la Junta Directiva semestralmente.

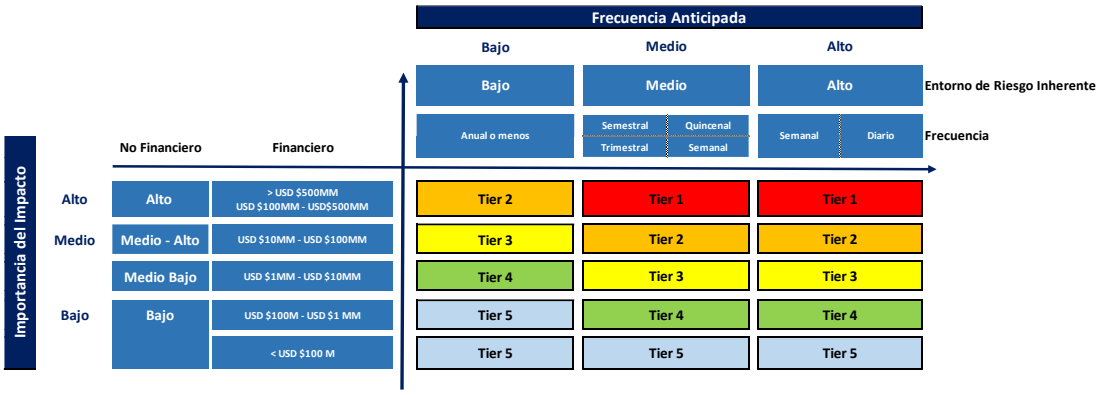
Si el riesgo residual supera el apetito de riesgo aceptado por la organización, el dueño de cada unidad de evaluación debe seguir las siguientes acciones para gestionar el riesgo residual:




## Mapa perfil de riesgo inherente y residual a diciembre 2022

El perfil de riesgo inherente y residual consolidado del vehículo legal está representado por las siguientes gráficas, donde se visualiza cómo están distribuidos los riesgos inherentes y residuales en su conjunto según su nivel de criticidad (calificación asignada).

## Evolución perfil de riesgo inherente por riesgo individual




| Mapa Riesgo Inherente 2021 | | | Mapa Riesgo Inherente 2022 | | |
|---|---|---|---|---|---|
| Tier 1 | 37 | 1.03% | Tier 1 | 17 | 0.46% |
| Tier 2 | 715 | 19.94% | Tier 2 | 883 | 23.69% |
| Tier 3 | 1814 | 50.60% | Tier 3 | 1775 | 47.61% |
| Tier 4 | 570 | 15.90% | Tier 4 | 411 | 11.02% |
| Tier 5 | 449 | 12.52% | Tier 5 | 642 | 17.22% |
| Total | 3585 | 100% | Total | 3728 | 100% |

La variación en instancias de riesgo obedece a la identificación de nuevos riesgos por parte de las unidades de negocio y funcionales que prestan servicios a los vehículos legales de Citi Colombia.

Fuente: Citi Risk and Controls - Group Aggregation Backup Data Report 28/1/2023

## Evolución perfil de riesgo residual por riesgo individual

| Calificacion Riesgo Inherente | Evaluación total del Control según el riesgo | | | |
|---|---|---|---|---|
| | - 3 Tier | - 2 Tier | - 1 Tier | Sin Cambio |
| | Altamente Efectivo | Efectivo | Parcialmente Inefectivo | Inefectivo |
| Tier 1 | Tier 4 | Tier 3 | Tier 2 | Tier 1 |
| Tier 2 | Tier 5 | Tier 4 | Tier 3 | Tier 2 |
| Tier 3 | Tier 5 | Tier 5 | Tier 4 | Tier 3 |
| Tier 4 | Tier 5 | Tier 5 | Tier 5 | Tier 4 |
| Tier 5 | Tier 5 | Tier 5 | Tier 5 | Tier 5 |

| Mapa Riesgo Residual 2021 | | | Mapa Riesgo Residual 2022 | | |
|---|---|---|---|---|---|
| Tier 1 | 10 | 0.28% | Tier 1 | 6 | 0.16% |
| Tier 2 | 121 | 3.38% | Tier 2 | 101 | 2.71% |
| Tier 3 | 182 | 5.08% | Tier 3 | 142 | 3.81% |
| Tier 4 | 691 | 19.27% | Tier 4 | 872 | 23.39% |
| Tier 5 | 2581 | 71.99% | Tier 5 | 2607 | 69.93% |
| Total | 3585 | 100% | Total | 3728 | 100% |

La variación en instancias de riesgo obedece a la identificación de nuevos riesgos por parte de las unidades de negocio y funcionales que prestan servicios a los vehículos legales de Citi Colombia.

**Fuente: Citi Risk and Controls - Group Aggregation Backup Data Report 28/1/2023**

## Perfil de riesgo inherente y residual consolidado

| Legal Vehicle | Inherent Risk Rating | % Controls Designed Adequately (#) | # Issues linked to AU (Not Mapped) | # Op Risk Events linked to AU | % Monitoring Result Pass/Green | % Controls Highly Effective & Effective (#) | Residual Risk Rating (most recent quarter) |
|---|---|---|---|---|---|---|---|
| Citibank Colombia | Tier 3 | 96.92%(4972) | 1124(499) | 34 | 79.83% | 89.77%(4605) | Tier 4 |

El ejercicio de perfil de riesgo incluye 38 unidades de evaluación bajo la entidad de Colombia y 29 unidades de evaluación regionales y globales que ejecutan procesos y controles para el vehículo legal.

La calificación de riesgo inherente y residual y el porcentaje de efectividad de controles agrega las calificaciones de las 38 Unidades de Evaluación dentro de la Entidad de Colombia y de 29 Unidades de Evaluación Regionales y Globales que ejecutan procesos y controles para el país.

La entidad reporta 3.728 riesgos identificados al cierre de 2022, y presenta un aumento del 4% en los riesgos reportados frente al 2021 (3.585), este incremento obedece a la identificación de nuevos riesgos de las unidades de negocio y funcionales que hacen parte del vehículo legal.

La concentración de riesgos inherentes: Tier 1 – 2: 24.15%; Tier 3: 47.61% y Tier 4 – 5: 28.24%.

La concentración de riesgos residuales fuera del perfil definido es de 6.68% para Tier 1 - 3. Tanto las taxonomías de riesgo como las unidades que cerraron el 4 trimestre de 2022 con riesgo residual agregado en Tier 3 tienen deficiencias de control asociadas para mitigar el riesgo residual a niveles aceptados. Como parte de este ejercicio se reforzará la importancia del mapeo

de los issues a nivel de control para las AUs globales y Regionales que concentran el mayor número de issues sin mapear.

Los dueños de las unidades de evaluación (AUs) deben seguir trabajando en el proceso de Gestión del Riesgo Residual para aquellos riesgos residuales individuales clasificados en nivel 2 y 3, poder mitigarlos a los niveles aceptados por la corporación y la Junta Directiva nivel 4 y 5.