SUPERINTENDENCIA DE BANCOS
REPÚBLICA DOMINICANA

CIRCULAR SB:

CSB-REG-2026000021

A las: **Entidades de intermediación financiera (EIF) e Intermediarios cambiarios.**

Asunto: **Poner en vigencia el "Instructivo para la implementación del Reglamento de Riesgo Operacional".**

Visto: El literal (e) del artículo 21 de la Ley núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002 (en lo adelante la "Ley Monetaria y Financiera"), que faculta al Superintendente de Bancos a emitir Instructivos, Circulares y Reglamentos Internos.

Visto: El literal f) del artículo 46 de la Ley Monetaria y Financiera que contempla la posibilidad de determinar exigencias adicionales de patrimonio técnico en función de los distintos riesgos que asumen las entidades de intermediación financieras, en lo adelante, EIF, entre ellos, el Riesgo Operacional.

Visto: Los literales a) y b) del artículo 55 de la citada Ley Monetaria y Financiera, que requieren a las EIF contar con adecuados sistemas de control de riesgos, control interno y políticas actualizadas para la administración de los diferentes riesgos a que pueden quedar expuestas.

Visto: El Reglamento sobre Normas Prudenciales de Adecuación Patrimonial, aprobada por la Junta Monetaria mediante la Tercera Resolución del 30 de marzo del 2004 y sus modificaciones.

Visto: El Reglamento Cambiario, aprobado por la Junta Monetaria en la Primera Resolución del 11 de septiembre del 2025.

Visto: El Reglamento sobre Riesgo Operacional, aprobado por la Junta Monetaria en la Cuarta Resolución del 27 de noviembre del 2025.

Vista: La Circular SB: No. 011-10 del 9 de agosto de 2010, que pone en vigencia la primera versión del Instructivo para la aplicación del Reglamento sobre Riesgo Operacional.

Vista: La Circular SB: núm. 013-21 del primero de septiembre de 2021, que modifica el "Manual de Contabilidad para Entidades Supervisadas" y sus modificaciones.

Vista: La Circular SB: núm. 018/22 del 15 de diciembre de 2022, que pone en vigencia la versión actualizada del "Manual de Requerimientos de Información de la Administración Monetaria y Financiera (MRI)" y sus modificaciones.

Vista: La Circular SB: CSB-REG-202500007, del 7 de abril de 2026 que pone en vigencia el "Manual de solicitudes de autorización, no objeción y notificaciones de las entidades supervisadas por la Superintendencia de Bancos".

Considerando: Que resulta necesario establecer una metodología para la determinación del requerimiento de capital por riesgo operacional alineada con las mejores prácticas y estándares internacionales, que permita una medición prudente y consistente de la exposición a este riesgo, fortalezca la capacidad de absorción de pérdidas derivadas de eventos operacionales y contribuya a la solvencia, estabilidad y sostenibilidad de los intermediarios financieros y cambiarios.

Considerando: Que, en virtud de que el Reglamento sobre Riesgo Operacional establece para los intermediarios financieros la incorporación del requerimiento de capital por riesgo operacional en la determinación del coeficiente de solvencia, se hace necesario disponer de lineamientos metodológicos y operativos que regulen su cálculo, registro, monitoreo y aplicación, con el propósito de garantizar una implementación consistente, transparente y acorde con las disposiciones regulatorias vigentes.

POR TANTO:

El Superintendente de Bancos en uso de las atribuciones que le confiere el literal (e) del artículo 21 de la Ley núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002, dispone lo siguiente:

1. Aprobar y poner en vigencia el "Instructivo para la aplicación del Reglamento sobre Riesgo Operacional", que se adjunta a la presente Circular, a fin de establecer los criterios, metodologías, procedimientos y lineamientos requeridos para la implementación efectiva de las disposiciones previstas en dicho Reglamento.

2. El requerimiento de capital por riesgo operacional será exigible a partir del 1º de abril del 2027, de conformidad con lo establecido en el Reglamento.

3. Las entidades dispondrán hasta el 31 de marzo de 2027 para la implementación de las disposiciones del presente instructivo y adecuaciones en sus sistemas.

4. Se deroga la primera versión del Instructivo para la aplicación del Reglamento sobre Riesgo Operacional puesto en vigencia con la Circular SB: No. 011-10 del 9 de agosto de 2010 y cualquier otra disposición emitida por la Superintendencia de Bancos que le sea contraria a la presente Circular.

5. Las entidades que infrinjan las disposiciones contenidas en la presente circular en cualquiera de sus aspectos serán pasibles de la aplicación de sanciones por la Superintendencia de Bancos, con base en la Ley núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002, el Reglamento de Sanciones aprobado por la Junta Monetaria en la Quinta Resolución del 18 de diciembre de 2003 y su modificación.

6. La presente circular deberá ser notificada a las partes interesadas y publicada en la página web de esta institución <www.sb.gob.do> de conformidad con el literal (h) del artículo 4 de la Ley núm. 183-02 Monetaria y Financiera y el mecanismo de notificación de los Actos Administrativos de la Superintendencia de Bancos, dispuesto en la Circular SB: No. 015/10 del 21 de septiembre de 2010 emitida por este ente supervisor.

Dada en la ciudad de Santo Domingo de Guzmán, Distrito Nacional, capital de la República Dominicana, a los doce (12) días del mes de noviembre del año dos mil veintiséis (2026).

Enmanuel Cedeño Brea
SUPERINTENDENTE

Anexo: IT-SB-009, instructivo para la aplicación del reglamento sobre riesgo operacional, versión 2.

Documento firmado digitalmente por:
Stephanie Cristina Hernandez Tejeda (VB) (13/11/2026 VET), José Guillermo López (VB) (13/11/2026 VET)
Mirna Midian García Santana (En nombre de Olimpia Gonzalez Matos) (VB) (13/11/2026 VET)
Yulianna Marie Ramon Martinez (VB) (13/11/2026 VET), Enmanuel Cedeño Brea (13/11/2026 VET)
https://www.viafirma.com.do/inbox/app/sib/v/ff9b98b1-145f-4f66-8ad3-9aee5fc7bbb3

SUPERINTENDENCIA DE BANCOS
REPÚBLICA DOMINICANA

IT-SB-009

INSTRUCTIVO PARA LA APLICACIÓN DEL REGLAMENTO SOBRE RIESGO OPERACIONAL



Versión 2
NOVIEMBRE, 2026

TABLA DE CONTENIDO

I. FINALIDAD, ALCANCE Y ÁMBITO DE APLICACIÓN 3
I.1. Finalidad 3
I.2. Alcance 3
I.3. Ámbito de aplicación 3

II. GLOSARIO DE TÉRMINOS 3

III. DISPOSICIONES GENERALES 4

IV. MARCO DE GESTIÓN DE RIESGO OPERACIONAL 5

IV.1. COMITÉ DE RIESGO OPERACIONAL 6
IV.1.1. Criterios para la conformación del Comité de Riesgo Operacional 7
IV.1.2. Funciones del Comité de Riesgo Operacional 7
IV.1.3. Informes al Comité de Riesgo Operacional 8
IV.1.4. Reuniones del Comité de Riesgo Operacional 9

IV.2. MODELO DE TRES LÍNEAS DE DEFENSA 9
IV.2.1. Primera línea de defensa (Líneas de negocio) 9
IV.2.2. Segunda línea de defensa (Unidad especializada de Riesgo Operacional) 10
IV.2.3. Tercera línea de defensa (Auditoría interna y externa) 10

IV.3. GESTIÓN DEL RIESGO LEGAL 11

IV.4. GESTIÓN DE LA CONTINUIDAD 13
IV.4.1. Gestión de contingencias 13
IV.4.2. Plan de continuidad 14
IV.4.3. Gestión de incidentes 15

IV.5. MANUALES DE POLÍTICAS Y PROCEDIMIENTOS 16

V. HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO OPERACIONAL 17

VI. EVENTOS DE RIESGO OPERACIONAL 23
VI.1. Reporte y registro de los eventos 23
VI.2. Base de datos de eventos 25
VI.3. Cuentas contables para registro de pérdidas 28
VI.4. Informe de eventos materiales 29

VII. RESILIENCIA OPERATIVA 30

VIII. LINEAMIENTOS PARA LAS SOLICITUDES DE RIESGO OPERACIONAL 31

IX. REQUERIMIENTO DE CAPITAL 32
IX.1. Metodología para cálculo del capital por riesgo operacional (ORC) 32
IX.2. Cálculo del componente del indicador de negocios (BIC) 33
IX.3. Cálculo del multiplicador de pérdidas internas (ILM) 34

X. LINEAMIENTOS PARA LOS INTERMEDIARIOS CAMBIARIOS 35
X.1. Gestión del riesgo operacional 35
X.2. Requerimiento de capital 37

XI. SANCIONES 37

ANEXOS 38

Tabla 1. Criterios de evaluación de materialidad operativa 39
Tabla 2. Características de los tipos de eventos de riesgo operacional 40
Tabla 3. Cuentas contables para registro de pérdidas de eventos de riesgo operacional 42
Tabla 4. Fórmulas para el cálculo del ORC y definición de los componentes 45
Tabla 5. Asignación de cuentas contables para determinación del Indicador de Negocios (BI) 48

I. FINALIDAD, ALCANCE Y ÁMBITO DE APLICACIÓN

I.1. Finalidad

El presente instructivo tiene por finalidad establecer los lineamientos que deberán seguir las entidades de intermediación financiera (EIF) e intermediarios cambiarios, para dar cumplimiento a lo dispuesto en el Reglamento sobre Riesgo Operacional, aprobado mediante la Cuarta Resolución de la Junta Monetaria de fecha 27 de noviembre de 2025.

I.2. Alcance

Este instructivo comprende los requisitos mínimos que deberán cumplir las entidades en lo relativo a políticas, procedimientos y criterios para la gestión de riesgo operacional, incluyendo las matrices de riesgos, herramientas para su gestión, eventos de riesgo operacional, monitoreo de indicadores, la resiliencia operativa, la continuidad del negocio, así como la metodología estandarizada para el cálculo del requerimiento de capital por riesgo operacional.

I.3. Ámbito de aplicación

Las disposiciones establecidas en este instructivo son aplicables a las entidades siguientes:

a) Bancos múltiples;
b) Bancos de ahorro y crédito;
c) Asociaciones de ahorros y préstamos;
d) Corporaciones de crédito;
e) Entidades públicas de intermediación financiera;
f) Agentes de cambio; y,
g) Agentes de remesas y cambio.

Párrafo: Las disposiciones de este instructivo que serán aplicables a los intermediarios cambiarios, se encuentran incluidos en el ordinal X. Lineamientos para los intermediarios cambiarios y XI. Sanciones.

II. GLOSARIO DE TÉRMINOS

Para la aplicación de las disposiciones de este instructivo, los términos y expresiones que se indican más adelante, tanto en mayúscula como minúscula, singular o plural, tendrán los significados siguientes:

a) Efectividad del control: Se refiere al grado con el que el control mitiga el riesgo para el cual fue implementado. Un control no efectivo podría resultar en una valoración de riesgo residual igual a la del riesgo inherente;

b) Gestión de contingencias: Proceso continuo de planificación, preparación, respuesta y mejora mediante el cual la entidad establece las medidas, procedimientos y recursos necesarios para gestionar eventos disruptivos, minimizar su impacto y asegurar la continuidad o recuperación oportuna de los procesos críticos del negocio;

c) **Incidente:** Cualquier suceso que cause una interrupción de las operaciones o una reducción de la calidad de este;

d) **Incidente operacional grave:** Suceso que afecte operaciones críticas, comprometan la disponibilidad y confidencialidad de información sensible, genere pérdidas financieras relevantes, impliquen indisponibilidad significativa de servicios, afecte el cumplimiento regulatorio o produzcan impacto reputacional significativo;

e) **Procesos de apoyo:** Brindan soporte a los procesos esenciales garantizando los recursos que se necesitan para operar;

f) **Procesos estratégicos:** Establecen los lineamientos generales de la organización, así como la dirección estratégica que deben seguir todos los procesos; y

g) **Procesos esenciales**: Son los procesos que conforman la razón de ser de la entidad, así como también la cadena de valor de la organización y son los que transforman los requisitos de las partes interesadas en un producto o servicio.

III. DISPOSICIONES GENERALES

Las entidades deberán cumplir con las disposiciones establecidas en este instructivo para la gestión de riesgo operacional, conforme a su naturaleza, tamaño, perfil de riesgo, complejidad e importancia sistémica. Para tales fines se aplicarán los criterios siguientes:

a) Las entidades que dependan de un mismo controlador o conformen un grupo financiero deberán dar cumplimiento a las disposiciones establecidas en el presente instructivo respecto de la entidad radicada en el país, aun cuando la gestión del riesgo operacional sea realizada, por su casa matriz u otra entidad del grupo, sin perjuicio de las disposiciones aplicables a nivel individual o consolidado.

b) Cada entidad deberá definir los criterios para la determinación de la criticidad de sus servicios y procesos, y evaluar los riesgos identificados para las operaciones de la entidad ante eventos disruptivos.

c) La gestión del riesgo operacional y la resiliencia operativa deberán desarrollarse, a través de un sistema eficaz que reduzca la frecuencia e impacto de los eventos de riesgo operacional y fortalezca/garantice la continuidad y estabilidad de las operaciones.

d) Establecer un marco de apetito de riesgo, tolerancia y capacidad de riesgo, conforme a lo establecido en el Reglamento sobre Riesgo Operacional y el Instructivo sobre Lineamientos para la Definición del Apetito de Riesgo, que contemple una declaración formal y documentada del nivel agregado de exposición al riesgo operacional que la entidad está dispuesta a asumir, mitigar o evitar para alcanzar sus objetivos estratégicos. Dicho marco deberá contemplar métricas cualitativas y cuantitativas, límites de riesgo operacional, así como políticas, procedimientos y controles para su gestión y monitoreo. Asimismo, deberá definir roles y responsabilidades, e integrarse con la estrategia, el plan de negocios y la planificación de capital de la entidad.

IV. MARCO DE GESTIÓN DE RIESGO OPERACIONAL

La gestión del riesgo operacional será un proceso continuo y permanente debiendo las entidades mantener adecuadamente documentado, de forma integral y por escrito, el marco de gestión de riesgo operacional, el cual deberá ser aplicable a toda la organización, e incluirá como mínimo, y de manera no limitativa, los aspectos siguientes:

a) Identificar la estructura de gobierno utilizada para gestionar el riesgo operacional, incluidas las líneas de reporte, sus jerarquías, así como sus responsabilidades;

b) Contemplar que los procesos de gestión del riesgo operacional estén sujetos a una supervisión integral, continua y dinámica, y que se encuentren plenamente integrados con el marco general de gestión de riesgos de la entidad. Para tales fines, el Consejo podrá delegar en su comité de apoyo competente la aprobación de dichos procesos, así como su seguimiento y actualización;

c) Hacer referencia a las políticas y procedimientos relevantes de gestión de riesgos operacionales;

d) Detallar las herramientas utilizadas para la identificación, evaluación y monitoreo del riesgo operacional;

e) Establecer las funciones y responsabilidades de las tres líneas de defensa, asegurando una adecuada segregación de funciones

f) Especificar la estrategia de la entidad para establecer y monitorear umbrales o límites de exposición al riesgo inherente y residual, así como referenciar al documento donde se establecen los controles para su efectividad;

g) Incorporar en el Marco de Apetito de Riesgos de la entidad los niveles de apetito, tolerancia y capacidad aceptados para el riesgo operacional de la entidad, indicando los umbrales, detonadores de actividad o límites para el riesgo inherente y residual, así como las estrategias e instrumentos de mitigación de riesgos aprobados;

h) Documentar un inventario de riesgos, controles y procesos, clasificarlos según las tipologías y procesos de la entidad, asegurando su aplicación en todas las unidades de negocio;

i) Disponer revisiones y actualizaciones del mapeo de riesgos y controles, con una frecuencia definida que refleje oportunamente los cambios en procesos, productos, sistemas, proveedores, canales y el contexto interno y externo de la entidad;

j) Establecer una evaluación periódica de la efectividad de los controles y su relación con la determinación de los riesgos residuales de acuerdo con el tamaño, complejidad y perfil de riesgo;

k) Establecer el perfil de riesgo operacional de la entidad, así como sistemas de información y reportes de gestión de riesgos que permitan identificar, medir y monitorear oportunamente la exposición a riesgo operacional;

l) Disponer la realización de una revisión independiente del proceso de gestión de riesgos, que evalúe la efectividad de sus metodologías, controles y resultados de acuerdo con el tamaño, complejidad y apetito de riesgo;

m) Definir la realización de un monitoreo continuo de los resultados derivados del proceso de gestión de riesgos, verificando la adecuada implementación de las medidas correctivas y el cumplimiento de los límites establecidos por la entidad;

n) Establecer revisiones periódicas de las políticas según corresponda, en función de la evaluación continua de la calidad del entorno de control que aborde los cambios del contexto interno y externo, y adicionalmente, cuando se produzcan cambios importantes en el perfil de riesgo operacional de la entidad; y,

o) Establecer planes de acción para abordar las deficiencias identificadas.

Las entidades deberán contar con una estructura funcional responsable de coordinar, supervisar y dar seguimiento a la gestión de riesgo operacional, atendiendo a su naturaleza, complejidad y perfil de riesgo.

Esta estructura podrá estar integrada por el Consejo, el Comité de Gestión Integral de Riesgos, el Comité de Riesgo Operacional, la Unidad de Gestión Integral de Riesgos y la Unidad Especializada de Riesgo Operacional. Las responsabilidades de las funciones que integran esta estructura están definidas, de manera no limitativa, en los reglamentos de Riesgo Operacional y el de Lineamientos para la Gestión Integral de Riesgos.

Las funciones del Comité de Riesgo Operacional se complementan con las funciones que se detallan a continuación:

IV.1. COMITÉ DE RIESGO OPERACIONAL

Este comité será responsable de supervisar los riesgos operacionales de la entidad, incluyendo el riesgo legal, que pudieran impactar el logro de los objetivos y estrategias de la entidad, el cual reportará al Comité de Gestión Integral de Riesgos. Asimismo, le corresponderá conocer y evaluar los riesgos tecnológicos y de ciberseguridad en aquellos aspectos relacionados con la operación; la disponibilidad, integridad y confidencialidad de la información; la gestión de terceros; la resiliencia operativa y la continuidad de las actividades de la entidad. Los eventos relevantes identificados, así como las medidas de gestión, mitigación o seguimiento que correspondan, deberán ser presentados al Comité de Gestión Integral de Riesgos.

Las funciones del Comité de Riesgo Operacional relativas al riesgo tecnológico, la ciberseguridad y la seguridad de la información se ejercerán sin perjuicio de las atribuciones asignadas al Comité Funcional de Seguridad Cibernética y de la Información por la normativa aplicable.

La conformación y participación de la Alta Gerencia en el comité se definirá en atención a la naturaleza, tamaño, complejidad y perfil de riesgo de la entidad, asegurando la incorporación de miembros que posean idoneidad técnica, experiencia comprobada y capacidad decisoria. Dicha integración se realizará de forma proporcional al modelo de negocio y al nivel de exposición al riesgo, incluyendo perfiles con

competencias en áreas claves tales como: gestión integral de riesgos, asuntos legales, tecnología de la información, seguridad cibernética y de la información, cumplimiento regulatorio y gestión financiera.

La composición de miembros con voto de este comité debe ser impar, considerando que el representante de la unidad especializada de riesgo operacional tendrá voz, pero no voto en las decisiones tomadas en este comité.

IV.1.1. Criterios para la conformación del Comité de Riesgo Operacional

El Comité de Riesgo Operacional se constituirá considerando la naturaleza, tamaño, complejidad de las operaciones, y el perfil de riesgo de la entidad, el cual deberá contar con independencia funcional.

Las entidades deberán establecer un Comité de Riesgo Operacional, si cumplen como mínimo, con uno de los criterios de proporcionalidad siguientes:

a) Importancia sistémica;
b) Alto nivel de complejidad operativa y tecnológica;
c) Volumen y diversidad de productos, servicios y canales;
d) Alto nivel de tercerización de procesos críticos; y,
e) Alto nivel de exposición a eventos de pérdida operacional (frecuencia y/o severidad).

Para las entidades a las que no se les exija regulatoriamente la existencia del Comité de Riesgo Operacional, será opcional el establecimiento de este Comité, pudiendo ejecutar dichas funciones como parte del Comité de Gestión Integral de Riesgos.

Si como resultado de las revisiones realizadas, la Superintendencia de Bancos o el Banco Central determina que, en función de los criterios previamente señalados u otros elementos relevantes asociados al perfil de riesgo, tamaño o complejidad de la entidad, resulta necesario fortalecer la gestión del riesgo operacional, podrá requerir la conformación de este comité, incluso en aquellos casos en los que dicha instancia no hubiera sido inicialmente prevista por la entidad.

IV.1.2. Funciones del Comité de Riesgo Operacional

El comité de Riesgo Operacional deberá realizar cómo mínimo las funciones siguientes:

a) Revisar, recomendar y someter a la aprobación del Consejo u órgano competente delegado por este, las políticas, procedimientos y lineamientos internos para la adecuada gestión, medición, control y monitoreo del riesgo operacional.

b) Definir las responsabilidades de los gestores de riesgo operacional asegurando la adecuada segregación de funciones y la prevención de conflictos de interés.

c) Supervisar el registro, clasificación, consolidación y actualización oportuna de los eventos de pérdida por riesgo operacional.

d) Evaluar de forma periódica los indicadores claves de riesgo y las herramientas de autoevaluación de riesgos.

e) Verificar que los nuevos productos, servicios, actividades o proceso de externalización cuenten con una evaluación integral basada en riesgo previo a su aprobación e implementación. Asimismo, el Comité de Riesgo Operacional deberá conocer aquellos casos que, conforme a los criterios de materialidad y escalamiento definidos por la entidad, presentan exposición operacional relevante; los demás casos podrán gestionarse mediante los niveles de aprobación establecidos.

f) Monitorear el Plan de Continuidad del Negocio, incluyendo pruebas periódicas de su efectividad y la actualización de estrategias de recuperación ante interrupciones.

g) Supervisar el proceso de tercerización de servicios y actividades críticas, asegurando que la identificación, evaluación, monitoreo y control de los riesgos asociados a proveedores y terceros se realice de conformidad con las políticas internas y la normativa vigente.

h) Dar seguimiento al avance y cumplimiento de los planes de acción derivados de la gestión del riesgo operacional, verificando su ejecución oportuna y efectividad en la mitigación de los riesgos identificados, sin perjuicio de las responsabilidades asignadas a la función de Auditoría Interna en materia de evaluación independiente.

i) Velar por la adecuada gestión de los riesgos asociados a la tecnología de la información y la seguridad cibernética, asegurando la implementación y efectividad de los controles, así como la asignación eficiente de recursos para la protección de los activos de información.

j) Presentar informes periódicos al Comité de Gestión Integral de Riesgos, sobre el perfil de riesgo operacional, tendencias de pérdidas, nivel de exposición y estado de las acciones de mitigación.

k) Establecer y mantener mecanismos y canales efectivos de reporte, que permitan la comunicación oportuna de incidentes relevantes al Consejo u órgano competente y a las autoridades supervisoras, conforme a la normativa vigente.

l) Verificar la existencia de planes de capacitación y concienciación en riesgo operacional, fomentando una cultura de gestión de riesgos operacional en toda la entidad.

IV.1.3. Informes al Comité de Riesgo Operacional

La unidad especializada en riesgo operacional será la encargada de presentar en este Comité los informes sobre los resultados de la gestión. Dichos informes deben describir el perfil de riesgo operacional de la entidad al proporcionar indicadores financieros, operativos y de cumplimiento interno, así como información externa del mercado sobre eventos y condiciones que son relevantes para la toma de decisiones. Estos deben incluir como mínimo lo siguiente:

a) Monitoreo de indicadores e incumplimientos del apetito de riesgo y tolerancia, así como umbrales, límites o requisitos cualitativos;

b) Evaluación de los riesgos claves y emergentes;

c) Detalles de eventos significativos internos recientes de riesgo operacional (incluyendo análisis de causa raíz y consecuencias); y

d) Eventos externos relevantes, cambios regulatorios y cualquier impacto potencial en la entidad.

IV.1.4. Reuniones del Comité de Riesgo Operacional

Las reuniones del Comité deben celebrarse con al menos la misma frecuencia establecida para el Comité de Gestión Integral de Riesgos, o de manera extraordinaria cuando se requiera por algún riesgo emergente o eventos de riesgo de alto impacto. Deberá quedar constancia en acta de las discusiones, acuerdos y decisiones tomadas en estas reuniones, de manera que permita una revisión y evaluación de la efectividad del Comité. Las actas deben ser firmadas por todos los miembros y ser presentadas y validadas por el Comité de Gestión Integral de Riesgos.

IV.2. MODELO DE TRES LÍNEAS DE DEFENSA

Las entidades deberán implementar el modelo de tres líneas de defensa para el riesgo operacional, con funciones debidamente segregadas y separadas, por lo que no podrán existir áreas o departamentos que compartan funciones entre diferentes líneas de defensa.

Las entidades deben asegurarse de que cada línea de defensa cuente con:
a) Recursos en términos de presupuesto, herramientas y personal;
b) Funciones y responsabilidades claramente definidas;
c) Formación continua y adecuada;
d) Cultura sólida de gestión de riesgos en toda la organización;
e) Comunicación con las demás líneas de defensa para reforzar el Marco de Gestión del riesgo operacional; y
f) Rendición de cuentas efectiva para la gestión del riesgo operacional.

Las responsabilidades específicas de cada línea se describen a continuación:

IV.2.1. Primera línea de defensa (Líneas de negocio)

En esta primera línea están las áreas de negocios y soporte de la entidad, que entre sus funciones se incluyen la responsabilidad y rendición de cuentas de actividades propias del negocio, y la definición, implementación y gestión de controles para la mitigación de los riesgos relacionados. En adición, en esta línea se asume el uso de herramientas de gestión del riesgo operacional para identificar y gestionar los riesgos, evaluando y mejorando los controles, así como monitoreando y reportando oportunamente el perfil de riesgo operacional de sus áreas, para asegurar que este se adhiera al apetito y tolerancia al riesgo establecido. Esta línea también debe dar cumplimiento a las políticas, normas y lineamientos establecidos para promover la cultura del riesgo de la entidad.

Dentro de la primera línea de defensa, la entidad puede optar por establecer grupos de control o gestores de riesgos directos de cada área o línea de negocio, con responsabilidad específica de las actividades de riesgo operacional de sus respectivas áreas o líneas de negocio, que incluyen:

a) Identificar, medir, administrar, monitorear y reportar el riesgo operacional que surge de las actividades e iniciativas operativas de acuerdo con las políticas establecidas.
b) Establecer una estructura de control interno adecuada para gestionar los riesgos operativos en su área específica.
c) Escalar, de manera oportuna, los riesgos operativos y eventos descubiertos hacia el área de riesgo operacional y la alta gerencia.
d) Desarrollar e implementar, de manera oportuna, acciones correctivas para los problemas de riesgo operacional que se han identificado.
e) Informar sobre riesgos operativos residuales no mitigados por los controles, incluidos eventos de pérdida operativa, deficiencias de control, insuficiencias de procesos e incumplimiento de las tolerancias de riesgo operacional.

IV.2.2. Segunda línea de defensa (Unidad especializada de Riesgo Operacional)

Las responsabilidades de la segunda línea de defensa incluyen el diseño, desarrollo y mantenimiento de políticas, estándares, lineamientos y herramientas de gestión de riesgos operativos utilizados para identificar y gestionar los riesgos, aplicando revisión independiente al uso y salida de dichas herramientas en la gestión del riesgo operacional por parte de la primera línea de defensa. Asimismo, deberá monitorear y reportar el perfil agregado de riesgo operacional, debiendo a su vez, diseñar y brindar capacitación y concientización sobre el riesgo operacional, promoviendo una adecuada cultura de riesgo en toda la entidad.
La segunda línea de defensa debe proporcionar una evaluación efectiva y objetiva a los sistemas de gestión de riesgo operacional, que debe evidenciarse y documentarse, para que luego sea observable por la primera línea de defensa. Esta evaluación abarca una visión objetiva con respecto a la calidad y la suficiencia de las actividades de gestión de riesgos operacionales de la primera línea de defensa, incluyendo la identificación y evaluación de los riesgos operacionales, identificación y evaluación de controles, suposiciones y tratamiento de riesgos. Además, incluye la realización de evaluaciones independientes al sistema de gestión de riesgo.

La evaluación objetiva debe realizarse basada en un proceso estructurado y repetible que se adapta a la mejora continua, permitiendo la flexibilidad cuando sea apropiado. Esta debe ser compartida de manera constructiva y de forma oportuna, y su efectividad debe medirse por los resultados, al influir en decisiones y/o acciones de gestión.

IV.2.3. Tercera línea de defensa (Auditoría interna y externa)

Esta línea proporciona una revisión y pruebas objetivas de los controles, procesos y sistemas de gestión de riesgo operacional, y de la efectividad de las funciones de primera y segunda línea de defensa. La tercera línea de defensa observa y revisa de manera independiente la idoneidad de la gestión de los riesgos operacionales de manera general dentro del contexto de las funciones de gestión de riesgos y de gobierno corporativo, y evalúa además la efectividad operativa de los controles existentes.

El personal de esta función no debe participar en el desarrollo, la implementación ni en la operación de los procesos de gestión del riesgo operacional de las otras dos líneas de defensa. Las revisiones de la tercera línea de defensa podrían ser realizadas por auditoría interna o externa de las entidades, pero también pueden involucrar a terceros independientes debidamente calificados, sin que dicha participación sustituya la responsabilidad de auditoría interna de evaluar el marco de gestión del riesgo operacional y dar seguimiento a sus resultados.

IV.3. GESTIÓN DEL RIESGO LEGAL

La estrategia legal deberá ser definida por la Alta Gerencia, con el apoyo técnico de la unidad responsable de la gestión legal y debe contar con la aprobación del Consejo o en su defecto el órgano en que este delegue. La implementación de la gestión del riesgo legal debe estar integrada con la estrategia de la entidad, y el marco de gestión de riesgos, los objetivos y los sistemas de gestión dentro de la entidad.

La Alta Gerencia deberá asignar los recursos humanos, financieros, tecnológicos y de infraestructura necesarios para llevar a cabo una adecuada Gestión del Riesgo Legal dentro de la entidad.

La unidad responsable de la función de la gestión del riesgo legal, junto con la unidad especializada de gestión de riesgo operacional, deberá identificar y evaluar los riesgos y controles de índole legal, con la finalidad de definir estrategias para su mitigación.
Dicha unidad deberá mantener una base de datos que registre los procedimientos administrativos y los procesos judiciales y arbitrales en los que haya participado la entidad, estén o no relacionados con eventos de riesgo operacional. Dicha base de datos deberá identificar las causas, costos, fechas relevantes, estado y resultados de estos procesos, así como las demandas y denuncias iniciadas por la entidad y aquellas presentadas en su contra.

La misma deberá contar con la identificación de multas y sanciones regulatorias, así como las resoluciones jurídicas y administrativas. El Comité de riesgo operacional deberá ser informado de los resultados de la incidencia de demandas, multas y sanciones.

Para la definición de las políticas y procedimientos, así como para la toma de decisiones sobre tratamientos de riesgos legales, se deberá considerar y estructurar, sin ser limitativo, los siguientes aspectos:

a. Las leyes y regulaciones locales e internacionales relevantes y sus modificaciones a través del tiempo;
b. Acuerdos internacionales;
c. Alcance de la gestión del riesgo legal;
d. Las expectativas de los organismos reguladores y supervisores, gobierno, organizaciones de la sociedad civil, comunidades de interés y medios de comunicación;
e. Condiciones de mercado relacionadas a la entidad;
f. Naturaleza jurídica de la entidad, estructura legal interna y funciones de gobierno;
g. Estado de los asuntos legales de la entidad;
h. Derechos y obligaciones legales de la entidad, incluyendo las derivadas de los contratos;
i. Historial de casos legales en donde haya participado directa o indirectamente la entidad;
j. Prácticas corrientes de la entidad para el tratamiento del riesgo legal;
k. Requisitos derivados de asuntos civiles, laborales, medioambientales, fiscales, administrativos o de otro tipo;

l. Definición de los niveles de riesgo empleados por la entidad para medir su exposición al riesgo;
m. Apetito, tolerancia y capacidad del riesgo legal;
n. Definición de roles y responsabilidades para la gestión del riesgo legal;
o. Medios y flujos de comunicación y consulta;
p. Política de provisiones para el riesgo legal;
q. Periodicidad de revisión de los informes de gestión del riesgo legal; y,
r. Monitoreo y seguimiento del riesgo legal.

La unidad especializada de riesgo operacional deberá realizar el debido seguimiento a las acciones de tratamiento de los riesgos legales identificados, y deberá informar al Encargado de la Función de Gestión Integral de Riesgos y al Comité de riesgo operacional, acerca de la evolución de la exposición al riesgo legal dentro de la entidad, con la finalidad de que este sea monitoreado periódicamente. Para el seguimiento y revisión de la gestión del riesgo legal, la entidad deberá mantenerse al tanto de los cambios en el entorno, tales como introducción de nuevas leyes y su aplicación, monitoreo de eventos desencadenados por riesgo legal, y alertas tempranas para identificar riesgos legales que puedan surgir.

Provisión por riesgo legal.

La entidad deberá identificar, cuantificar y estimar razonablemente el monto de la pérdida esperada derivada de litigios asociados a procedimientos administrativos y a procesos judiciales y arbitrales en los que participe. Con base en dicha estimación, deberá constituir provisiones para aquellos casos respecto de los cuales se prevea un resultado desfavorable, considerando la probabilidad de ocurrencia y el impacto financiero potencial.

Estas provisiones deberán ser revisadas y actualizadas de manera periódica, en función de la evolución del proceso, la incorporación de nueva información relevante, cambios en la estrategia legal, decisiones judiciales o administrativas intermedias y cualquier otro factor que pueda modificar la estimación inicial de la pérdida.

La entidad puede realizar provisiones si así lo decide para posibles eventos legales, aunque no se hayan formalizado, sin embargo, estos no requieren ser incluidos en la base de datos de eventos a reportar a la Superintendencia de Bancos, hasta tanto se asignen a eventos de riesgo operacional, por ejemplo, un documento extraviado, un cargo cobrado no correspondiente, una adjudicación no procedente por fallas en el contrato, entre otros.

Una vez realizada una asignación de provisión, se debe dar seguimiento y mantener la base de datos de eventos con las provisiones actualizadas. Cuando el evento provisionado se concretiza, la provisión se sustituye por el importe definitivo en la cuenta por pagar requerida; y en caso contrario, si hay un fallo a favor de la entidad y no se concretiza una pérdida, el monto registrado como provisión se libera del evento. En todo caso, se debe reportar la provisión actualizada, ya sea por reducción o aumento.

El registro contable de provisión puede ser realizado de forma particular o de forma genérica agrupando la reserva para varias demandas, sin embargo, al momento de reportar los eventos provisionados en el periodo, se deben reportar de forma individual colocando la porción de provisión asignada que corresponde, si estas cumplen el mínimo requerido de reporte individual.

Asimismo, las entidades deberán establecer de forma expresa, en sus políticas y procedimientos internos, la etapa del proceso legal o administrativo a partir de la cual se iniciará el reconocimiento contable de la provisión por riesgo legal, así como definir la metodología, supuestos y criterios técnicos utilizados para su estimación, asegurando consistencia, trazabilidad y alineación con el marco normativo contable y prudencial aplicable.

IV.4. GESTIÓN DE LA CONTINUIDAD

La gestión de la continuidad del negocio constituye un elemento esencial dentro del marco de gestión del riesgo operacional al contribuir en la identificación, preparación y respuesta ante eventos que puedan afectar la continuidad de las operaciones. Su adecuada implementación permite asegurar la prestación sostenida de las funciones críticas, minimizar el impacto de interrupciones y reforzar la resiliencia operativa de la entidad. En este contexto, dicha gestión deberá abarcar, de manera enunciativa pero no limitativa, los aspectos siguientes:

IV.4.1. Gestión de contingencias

El proceso para desarrollar y mantener la gestión de contingencias, así como sus resultados, debe estar formalmente documentado, y considerar como mínimo los aspectos siguientes:

a. Implementación de una política de gestión de contingencias para restablecimiento de operaciones. Los elementos claves de esta política incluyen: roles y responsabilidades, alcance que cubre la política (procesos del negocio, localidades, infraestructuras, etc.), entrenamientos requeridos, calendarización de actualización y pruebas de los planes.

b. Identificación de procesos y servicios críticos o esenciales, y la determinación de cómo estos pueden verse afectados por la ocurrencia de eventos imprevistos (Análisis de Impacto del Negocio). Para este análisis se deben incluir los riesgos que tendrían un impacto significativo en las operaciones, aunque tengan una baja probabilidad de ocurrencia o que no se cuente con precedentes de eventos de su naturaleza en la entidad, en caso de que ocurrieran, así como los recursos necesarios y la prioridad de recuperación de los procesos identificados. Se debe considerar el apetito, la tolerancia y el perfil de riesgo de la entidad para las interrupciones.

c. Identificación e implementación de controles preventivos que reduzca la probabilidad de interrupción de las operaciones consideradas como críticas por la entidad, entre estos se incluye la oportuna gestión de las incidencias sobre los procesos de apoyo y esenciales o de negocio.

d. Implementación de estrategias con las acciones que la entidad ha definido para restablecer las operaciones normales en los plazos aceptados por la entidad y minimizar los impactos, incluyendo los recursos que se necesitarían para ello. Estas deben ser desarrolladas con la colaboración de las áreas funcionales de la entidad relacionadas a los procesos afectados.

e. Capacitación, concientización, revisión y actualización periódica de los componentes de la gestión de contingencias, incluyendo las pruebas de las acciones que la entidad ha definido para restablecer sus operaciones, considerando las mejoras por lecciones aprendidas.

IV.4.2. Plan de continuidad

Las acciones que la entidad ha definido para restablecer las operaciones normales y minimizar los impactos como parte de la gestión de contingencia estarán documentadas en un plan de continuidad que describa la capacidad de la entidad para llevar a cabo sus actividades normales y poder funcionar después de que hayan ocurrido eventos inesperados, estableciendo expectativas de resiliencia operativa que sean necesarias.

El propósito del plan de continuidad de negocios es proveer procedimientos para mantener las operaciones de los procesos de apoyo que la entidad ha definido como críticos, así como sus procesos de negocio, mientras se recupera de una interrupción. Este debe considerar los aspectos siguientes:

a. Entendimiento del contexto de la entidad, incluyendo todo el marco legislativo, normativo, contractual y estratégico.
b. Alcance global, abarcando todas las áreas de la entidad para dar respuesta a situaciones que puedan escapar a las medidas de seguridad habituales. Se debe considerar la participación de los dueños de los procesos, los dueños de los recursos (información, sistemas, equipos, facilidades, etc.), y con la aprobación del Consejo de forma posterior a la socialización con las partes internas y externas involucradas.

c. Mapeo de Interconexiones e interdependencias de los procesos, incluyendo aquellas a través de relaciones con terceros y entidades intragrupo, reguladoras y supervisoras.

d. Escenarios de riesgos que pueden afectar el normal desarrollo de las actividades de los procesos de la entidad, incluyendo la identificación de los recursos que se afectarían.

e. Análisis de impacto que tendrían la indisponibilidad y/o falta de integridad de recursos (equipos, sistemas, personas, etc.) críticos sobre los procesos de la entidad. Se deberá identificar y evaluar los riesgos y el impacto potencial de varios escenarios de interrupción.

f. Tiempo máximo tolerable de inactividad, que representa la cantidad máxima de tiempo de interrupción de los procesos de apoyo considerados críticos, y de los misionales o de negocio que sus dueños están dispuestos a aceptar.

g. Tiempo objetivo de recuperación, que define el tiempo que el proceso puede permanecer no disponible antes de que represente un impacto significativo a los objetivos del propio proceso y/u otros relacionados. Este por lo general es menor al tiempo máximo tolerable de inactividad definido.

h. Punto de recuperación, que representa la cantidad de información que los dueños de los procesos están dispuestos a perder ante la interrupción de sus operaciones. Este permitirá determinar la frecuencia con que deben ser respaldadas las informaciones relacionadas a los procesos.

i. Estrategias de recuperación, incluyendo los recursos, así como las actividades detalladas con secuencia de pasos que deberán realizarse para restablecer las operaciones de los procesos afectados.

j. Designación de una persona responsable de declarar que las operaciones afectadas serán realizadas según las acciones descritas en el plan de continuidad. Esta declaración deberá estar fundamentada en hechos concretos y la persona designada deberá contar con las facilidades de comunicación con los órganos de gobierno y alta gerencia.

k. Programas de pruebas periódicas, que deben quedar documentadas y generar los planes de acción correspondientes. Esto incluye los planes de continuidad propios de la entidad y de proveedores para servicios tercerizados.

l. Programas de formación, sensibilización, comunicación y gestión de crisis.

IV.4.3. Gestión de incidentes

Los dueños de cada proceso en las entidades deben mantener registros documentados de las incidencias ocurridas en procesos internos y tercerizados, y las soluciones aplicadas (estrategias de respuesta y recuperación) que permitan el mantenimiento de una base de conocimiento consultable para la prevención y solución de futuras incidencias.

Las lecciones aprendidas de incidentes anteriores, incluidos los incidentes experimentados por otros, deben ser debidamente reflejadas en la actualización del programa de gestión de incidencias, dicho programa debe gestionar todos los incidentes que afectan a la entidad, incluidos los atribuibles a las dependencias de terceros y entidades intragrupo.

Los dueños de proceso de las áreas relacionadas deberán considerar los incidentes ocurridos para la actualización de sus matrices de riesgos, evaluación de los controles existentes, determinación de planes de acción, y reportar al área de Riesgo Operacional para verificación. De igual forma, estos se deberán incluir en la base de datos de eventos de riesgo operacional si tienen algún tipo de consecuencia negativa para la entidad.

Los procedimientos de respuesta y recuperación ante incidentes deben considerar los riesgos relacionados a la postergación de soluciones y la selección de estrategias para dar solución a la incidencia. En adición, deben abordar las causas fundamentales de los incidentes para prevenir o minimizar la recurrencia.

El alcance de la gestión de incidentes debe capturar el ciclo de vida de este, incluyendo, pero no limitado a:

a) La clasificación de la gravedad del incidente en función de criterios predefinidos (por ejemplo: tiempo esperado para regresar a la normalidad del negocio), lo que permite la priorización adecuada y la asignación de recursos para responder al incidente.

b) Los procedimientos de respuesta y recuperación del incidente, incluida su vinculación con la continuidad del negocio, la recuperación ante desastres y otros planes y procedimientos de gestión asociados.

c) La implementación de planes de comunicación para reportar incidentes tanto internamente como a la Superintendencia de Bancos y al Banco Central, incluidas las métricas de rendimiento durante el incidente y el análisis de lecciones aprendidas después del incidente.

IV.5. MANUALES DE POLÍTICAS Y PROCEDIMIENTOS

Las entidades deberán elaborar manuales de políticas y procedimientos tomando en consideración todos sus productos, servicios, procesos, infraestructuras y sistemas, aplicables a todos los niveles de la entidad. Los manuales de políticas incluirán como mínimo los aspectos relativos a los objetivos, alcance, lineamientos generales, responsabilidades, niveles de exposición o riesgo, criterios generales de control y supervisión, lineamientos para la difusión y comunicación, parámetros para la actualización, revisión, seguimiento y aprobación.

De igual manera, los manuales de procedimientos deberán mínimamente contener la descripción de procesos, tareas, asignación de responsabilidades operativas, controles operativos, herramientas y metodología, indicadores de seguimiento y desempeño.

Los manuales de políticas y procedimientos deben abarcar los aspectos señalados, conforme a los criterios siguientes:

a. **Procesos internos:** Se deberán definir políticas y procedimientos que regulen de forma estructurada los procesos estratégicos, los procesos esenciales y los procesos de apoyo, asegurando su adecuada articulación y alineación con los objetivos de la entidad. Estos deberán contemplar, entre otros aspectos, la definición de roles y responsabilidades, flujos de trabajo, controles internos, indicadores de desempeño, mecanismos de seguimiento y mejora continua, así como la documentación y estandarización de las actividades críticas.

b. **Recursos humanos:** Se deberán establecer políticas y procedimientos orientados a garantizar una adecuada planificación, gestión y desarrollo del capital humano. Esto incluye, como mínimo, los procesos de reclutamiento, selección, contratación, inducción y capacitación continua del personal, que englobe también lo relativo a la gestión de riesgos y el código de conducta o política de ética; así como la evaluación del desempeño, sucesión, gestión del clima organizacional y procesos de desvinculación.

c. **Tecnología y seguridad de la información:** Se deberán definir políticas y procedimientos que aseguren una gestión eficaz de los recursos tecnológicos y la protección de la información. De manera no limitativa podría comprender la planificación, adquisición, desarrollo, implementación y mantenimiento de sistemas de información, así como la gestión de riesgos tecnológicos, la ciberseguridad, control de accesos, integridad, disponibilidad y confidencialidad de la información.

   Además, deberán incluirse lineamientos para la continuidad del negocio, respaldo de información, recuperación ante desastres y cumplimiento de estándares y regulaciones aplicables en materia de seguridad de la información.

d. **Eventos externos:** Se deberán establecer políticas y procedimientos para la identificación, evaluación y gestión de eventos externos que puedan afectar a la entidad. Esto incluye, de manera no limitativa,

la definición de planes de contingencia y respuesta ante crisis, protocolos de comunicación, monitoreo del entorno, análisis de riesgos externos (económicos, regulatorios, naturales, tecnológicos, entre otros) y mecanismos de coordinación con autoridades y terceros.

e. **Nuevos productos, servicios, actividades, procesos, canales y sistemas**: Las entidades deben contar con políticas y procedimientos para la revisión y aprobación de nuevos productos, servicios, actividades, procesos, canales y sistemas, incluyendo las métricas para evaluar y monitorear el riesgo inherente de estos. El proceso de revisión y aprobación deberá considerar:

   i. Los riesgos inherentes, incluidos riesgos legales, de tecnología y seguridad de la información, en el lanzamiento de nuevos productos, servicios, actividades, y canales, incluyendo los de mercados desconocidos, así como en la implementación de nuevos procesos, infraestructuras y sistemas, considerando las posibles subcontrataciones;

   ii. Posibles cambios en el perfil de riesgo operacional, el apetito y la tolerancia de la entidad, incluidos los cambios en el riesgo de productos o actividades existentes;

   iii. El diseño y verificación de la segregación de funciones en los procesos, nuevos o modificados, para lo cual se deberá utilizar herramientas que permitan identificar quienes deben ejecutar y aprobar las tareas, así como quienes deben ser consultados e informados sobre estas. Por ejemplo: matriz de asignación de responsabilidades (RACI, por sus siglas en inglés de *Responsible, Accountable, Consulted, Informed*);

   iv. Las estrategias de tratamiento de los riesgos inherentes, incluyendo los controles existentes y los necesarios a implementar para mantener el apetito y tolerancia, y la evaluación de su efectividad para la determinación del riesgo residual; y

   v. Los cambios en los umbrales o límites de riesgo relevantes.

V. HERRAMIENTAS PARA LA GESTIÓN DEL RIESGO OPERACIONAL

Las entidades deberán tener implementadas herramientas para recopilar, analizar y comunicar información relevante para la gestión del riesgo operacional, adecuadas a su estructura organizacional y complejidad de sus operaciones y mantenerlas en un proceso de desarrollo y mejora continua. De manera enunciativa pero no limitativa, las entidades deberán contar con las herramientas siguientes:

1. Mapeo de procesos: Herramienta utilizada para identificar y administrar los riesgos operacionales en los procesos de la entidad, con especial atención a aquellos significativos o transversales. Implica identificar las entradas y sus fuentes, los pasos dentro del proceso, las salidas y sus receptores, así como los riesgos operacionales propios a los mismos, incluyendo los factores generadores de riesgos. Esta herramienta se considera el primer paso para el levantamiento de riesgos a través de matrices.

2. Recopilación y análisis de eventos de riesgo operacional: La información derivada de la recopilación y el análisis de eventos de riesgo operacional debe utilizarse para evaluar la exposición de la entidad a este

riesgo, mediante la agregación y el monitoreo de dichos eventos a lo largo del tiempo, así como para evaluar la efectividad general del entorno de controles operacionales.

La recopilación y registro de datos internos de eventos de riesgo operacional debe ser gestionada por la primera línea de defensa, en función de su conocimiento directo de los procesos y operaciones. Por su parte, la administración, custodia y resguardo de la base de datos de eventos de pérdidas deberá recaer en la segunda línea de defensa, la cual será responsable de establecer los mecanismos necesarios para garantizar la integridad, calidad, consistencia y disponibilidad de la información.

En el caso de los eventos de riesgo operacional considerados como materiales, la primera línea debe identificar la causa, así como definir e implementar las acciones correctivas necesarias, con el objetivo de prevenir la ocurrencia de eventos similares o mitigar adecuadamente sus impactos. La segunda línea de defensa debe revisar de manera independiente y retar el análisis y acciones realizadas por la primera línea de defensa.

Adicionalmente, la entidad deberá mantener la vigilancia de eventos de riesgo operacional ocurridos en otras entidades similares o que resulten relevantes para su perfil de riesgo, a fin de identificar posibles vulnerabilidades, fortalecer su entorno de control y anticipar la materialización de riesgos.

3. Taxonomía de riesgo operacional: Se trata de una clasificación común de tipos de riesgos operacionales que contribuye a la consistencia de las actividades de identificación y evaluación de riesgos, y a la articulación de la naturaleza y el tipo de riesgo operacional al que la entidad está potencialmente expuesta. Las entidades pueden optar por la taxonomía de riesgos proporcionada por el ente supervisor para los reportes de riesgos y eventos partiendo de lo indicado en la “Tabla 2. Características de los tipos de eventos de riesgo operacional” (Ver anexos). Esto no limita que las entidades internamente puedan identificar una nueva taxonomía para los riesgos operacionales que se le presenten, en cuyo caso deberá tener correspondencia con la regulatoria.

La taxonomía deberá contemplar a su vez la vinculación de los eventos de riesgo operacional con los factores de riesgo establecidos en el Reglamento sobre Riesgo Operacional (procesos internos, personas, tecnología de información y eventos externos), a fin de facilitar una adecuada identificación de las causas que los originan.

4. Inventario de controles: Relación de los controles con los que cuenta la entidad para mitigar los riesgos inherentes del negocio y/o relacionados a un contexto particular. Por su función, pueden ser tipificados según su naturaleza en:

a) Preventivos;
b) Detectivos;
c) Correctivos;
d) Directivos; y
e) Compensatorios.

En adición, pueden agruparse en:

a) Controles administrativos (leyes, regulaciones, políticas, procedimientos, normativas, etc.);

b) Controles técnicos (validaciones automáticas, encriptación, autenticación, etc.) y
c) Controles físicos (cámaras de circuito cerrado, sistemas de alarmas, guardias de seguridad, validación biométrica, etc.).

5. Evaluaciones de riesgos y controles: Esta herramienta de gestión del riesgo operacional es realizada luego del mapeo de procesos para evaluar los riesgos y la efectividad de los controles. Como resultado de la evaluación se identifican debilidades de control existentes, así como las acciones de gestión necesarias para su corrección. Dichas acciones deben ser implementadas por las unidades de negocio correspondientes, incluidos los grupos de control, con el asesoramiento de la unidad especializada de riesgo operacional a nivel de toda la entidad. Estas acciones deben reflejar no sólo el entorno operativo actual, sino también incorporar un enfoque prospectivo.

Asimismo, esta evaluación debe integrarse como parte del proceso de gestión de cambios relacionados con productos, servicios, canales, procesos, sistemas e infraestructuras de la entidad. Este proceso de evaluación de riesgos y controles debe considerar al menos lo siguiente:

a) Riesgos inherentes al producto, servicio, canal o actividad;
b) Perfil del riesgo en relación con el apetito de riesgo de la entidad;
c) Conjunto de controles requeridos, procesos de gestión de riesgos y estrategias de mitigación de riesgos;
d) Evaluación de la efectividad de los controles y el riesgo residual resultante; y
e) Justificación de cambios a límites y/o umbrales de riesgo.

6. Mapa de Calor de Riesgo: Es una herramienta de gestión del riesgo operacional que debe ser implementada por las entidades con el propósito de representar de forma gráfica y resumida los niveles de exposición a los riesgos, tanto inherentes como residuales, mediante el uso de una escala de colores. Esta herramienta permite visualizar la combinación de la probabilidad de ocurrencia y el impacto de los riesgos identificados.

La representación deberá realizarse mediante una matriz que permita clasificar los riesgos según su nivel de probabilidad e impacto, utilizando una escala cromática que facilite su interpretación, la cual deberá servir como insumo para la priorización de los riesgos, permitiendo enfocar los esfuerzos de mitigación en aquellos de mayor criticidad.

La entidad deberá asegurar que el Mapa de Calor sea consistente con su estructura organizacional, naturaleza y complejidad de sus operaciones. Deberá ser actualizado periódicamente o cuando ocurran cambios significativos en el entorno de riesgos.

La herramienta deberá integrarse con las demás herramientas de gestión de riesgos operacionales utilizadas por la entidad, a fin de fortalecer el proceso de toma de decisiones.

7. Indicadores de riesgo operacional: Se utilizan para monitorear los principales factores de exposición asociados con los riesgos operacionales clave o con mayor nivel de impacto y/o probabilidad. Estos indicadores también pueden proporcionar información sobre las debilidades de control y ayudar a determinar el riesgo residual de la entidad. En adición, los indicadores de riesgos deben servir para

identificar tendencias de riesgo, advirtiendo cuando los niveles de riesgo se acercan o exceden los umbrales o límites, para lo cual se requiere la adopción oportuna de acciones y planes de mitigación.

Los indicadores representan medidas que indican la presencia potencial, estado o tendencia de una condición de riesgo, por lo que, debido a su valor predictivo, pueden actuar como alertas tempranas para permitir acciones anticipadas. Estos a la vez ayudan a cuantificar el perfil de riesgo de la entidad. Para su diseño se deben considerar los aspectos siguientes:

a) **Características de los indicadores:** Los indicadores seleccionados deben ser medibles y cuantificados en monto o porcentajes, y según aplique, pueden expresarse como número de incidentes, días de atraso, frecuencias, ratios, entre otros, con valores que muestran evolución en el tiempo. En adición deben ser relativamente fáciles de obtener y entender, y aplicables a riesgos específicos.

b) **Límites, frecuencia y responsabilidades:** Los indicadores deben ser definidos con los límites de apetito, tolerancia y capacidad, frecuencia de medición y responsable de su generación y monitoreo. Estos serán propuestos por el Comité de Gestión Integral de Riesgos, y aprobados por el Consejo o equivalente.

c) **Monitoreo de indicadores:** Se requiere el monitoreo periódico de los indicadores para verificar cualquier tendencia o desviación. Se deberán identificar medidas a tomar cuando los resultados de los indicadores monitoreados excedan el apetito de riesgo definido.

8. Análisis de escenarios: Es una herramienta para considerar posibles fuentes de riesgo operacional y la necesidad de mejoras en los controles de gestión de riesgos o soluciones de mitigación, que deben prepararse conforme a lo establecido en el Instructivo para realizar Pruebas de Estrés en las Entidades de Intermediación Financiera.

9. Análisis Comparativo: Son comparaciones de los resultados de diferentes herramientas de medición y gestión de riesgos implementadas dentro de la entidad, con la finalidad de mejorar la comprensión del perfil de riesgo operacional.

10. Cuantificación y/o estimación de la exposición al riesgo operacional: Este corresponde al monto estimado de pérdida por riesgo operacional agregado para la entidad, que deberá ser reservado en el patrimonio técnico para mantener la estabilidad ante la ocurrencia de eventos de alto impacto. Este puede estimarse a través de diferentes metodologías, sin embargo, se deberá mantener como mínimo el capital requerido por riesgo operacional de acuerdo con la metodología establecida en el presente instructivo.

11. Matriz de riesgo operacional: En esta se documentan los resultados de los procesos de identificación, medición, evaluación y mitigación de los riesgos de las diferentes unidades de negocio, funciones organizativas o procesos. El conjunto de matrices de riesgo operacional debe estar centralizado en la unidad especializada de riesgo operacional. Esta debe ser exhaustiva para todos los riesgos con posibilidad de ocurrencia, no solo para los riesgos materializados en eventos, por lo que la gestión debe ser preventiva y proactiva.

Las matrices definidas por la entidad para el registro de los riesgos operacionales deben funcionar como una herramienta que puede dejar al descubierto ámbitos que presenten deficiencias y ayudar a

determinar cuáles son las prioridades de gestión. Estas deben incluir como mínimo la estructura especificada en el Manual de Requerimientos de Información de la Administración Monetaria y Financiera (MRI), y en adición, considerar los aspectos siguientes:

a) **Descripción del riesgo:** Para cada registro en la matriz, la descripción del riesgo debe ser específica para un único riesgo. Esta descripción muestra el resultado del proceso de identificación del riesgo y debe ser clara, permitiendo identificar el efecto de su materialización. Los riesgos se deberán identificar por proceso o área, indicando los productos y servicios afectados. Estos deberán ser identificados partiendo de la base más granular posible, por ejemplo, en un proceso la base más granular pudieran ser las tareas o actividades de este. Los riesgos que se identifiquen para diferentes procesos deberán ser medidos y evaluados de forma individual para cada proceso afectado.

b) **Medición del riesgo Inherente:** Para medir el riesgo inherente se deberá medir la probabilidad de ocurrencia y el posible impacto a la entidad en caso de que se materialice el riesgo descrito en ausencia de controles. Para esta medición se requiere definir criterios específicos para categorizar en al menos 3 escalas de probabilidad e impacto de forma cuantitativa y cualitativa. El nivel de riesgo resultará del producto de los valores cuantitativos de la escala asignada de la probabilidad y del impacto. El resultado será evaluado según escala definida por la entidad que deberá de ser de al menos 3 niveles (Bajo, Medio y Alto, o equivalentes). Para realizar la medición y análisis de la probabilidad e impacto de los riesgos, se deberán utilizar metodologías y criterios generales aprobadas por el Consejo, pudiendo delegarse en el Comité de Gestión Integral de Riesgos.

   La unidad especializada deberá monitorear la frecuencia de incidencia de eventos relacionados con los riesgos, así como los factores de riesgos existentes.

c) **Informaciones del control:** Se requiere establecer claramente los controles implementados para mitigar cada riesgo, indicando la descripción del control, el tipo, frecuencia de su ejecución (diario, semanal, mensual, por evento, continuo, etc.) y responsable del mismo.

d) **Calificación de efectividad del control:** Se refiere a un calificativo (ejemplo: fuerte, moderado, débil) que permite reflejar el resultado de la más reciente evaluación de la efectividad del control. Los controles deberán ser evaluados de manera periódica para verificar su eficacia en mitigar el riesgo inherente.

e) **Medición del riesgo residual:** Se debe determinar si la efectividad de los controles mitiga la probabilidad y/o el impacto del riesgo, con lo que se determina el nivel de riesgo residual, utilizando la misma escala definida para el riesgo inherente.

f) **Tratamiento del riesgo residual:** Dependiendo del nivel de riesgo residual, y luego de comparar los resultados contra el apetito y tolerancia de riesgo establecidos por el Consejo, se determinará la estrategia de tratamiento propuesta por la primera línea de defensa ante el riesgo identificado, de acuerdo con su impacto y probabilidad. El plan de tratamiento de los riesgos operacionales materiales, riesgos fuera de apetito, aceptaciones relevantes o incumplimientos significativos identificados deberán contener las medidas a ser adoptadas, responsables y plazo para su implementación y deberá ser aprobado por el Comité de Gestión Integral de Riesgos. Los demás planes podrán aprobarse mediante los niveles delegados definidos por la entidad, con reporte

agregado y escalamiento por excepción. Dichos planes deberán ser monitoreados de forma periódica por la unidad especializada de riesgo operacional y actualizado según el avance de las medidas determinadas.

g) **Actualización de las matrices de riesgos:** Las matrices de riesgos son documentos dinámicos, por lo que deberán ser actualizados de forma continua, debido a cambios en el contexto interno o externo a la entidad (nuevos productos, cambio de procesos o sistemas, cambios en el organigrama o estructura organizacional, cambio en los controles establecidos, tercerización de procesos, cambio de suplidores o personal clave, condiciones sociales, nuevas amenazas o nuevos riesgos, etc.) o producto de la gestión de riesgos realizada en la entidad (nuevos controles, cambio de estrategias, mejora de procesos, identificación de debilidades en la efectividad de los controles, materialización de riesgos, tendencias en indicadores, etc.). Los dueños de procesos deben velar por la actualización de la matriz de riesgos de sus procesos.

h) **Resumen de perfil de riesgo:** El nivel de riesgo inherente y residual en las matrices de riesgo operacional deberán poderse visualizar de forma gráfica o en una tabla resumen por macroprocesos o área y a nivel general, para establecer el mapa de calor según el nivel de riesgos resultante.

i) **Evaluación de riesgos por cambios:** Se deberá realizar una evaluación de riesgos previo a la toma de decisiones que involucren cambios significativos en el contexto interno de la entidad, tales como: introducción de nuevos productos, nuevos sistemas, cambios en los procesos, canales o servicios, tercerización de servicios, cambios organizacionales, etc. Estas evaluaciones deberán incluir detalle de los riesgos relacionados al contexto del cambio o decisión y sus componentes claves. Asimismo, esta evaluación se deberá repetir luego de la implementación del cambio para verificar el nivel de los riesgos residuales y las acciones implementadas.

j) **Divulgación de resultados:** Los resultados de la evaluación de la matriz de riesgos general de la entidad, así como de las evaluaciones de riesgos realizadas como parte de proyectos de cambios significativos, deberán ser conocidas por la instancia que corresponda conforme al esquema de escalamiento basado en riesgo. En ese sentido, el Consejo deberá conocer el perfil de riesgo agregado y los casos que modifiquen significativamente el perfil de riesgo de la entidad, así como aquellos que presenten exposición residual fuera del apetito o, tolerancia o capacidad, requieran una aceptación relevante o que el riesgo corresponda a materias reservadas a dicho órgano. Las demás evaluaciones podrán ser conocidas por el Comité de Gestión Integral de Riesgos, el Comité de Riesgo Operacional u otro órgano competente delegado.

k) **Revisión de auditoría interna:** La Función de Auditoría Interna deberá verificar el cumplimiento de las políticas y criterios para el levantamiento, medición, evaluación, mitigación y monitoreo de los riesgos identificados en la matriz de riesgos, así como la suficiencia del diseño y proceso de elaboración, actualización y la efectividad de los controles indicados en esta, de acuerdo con el alcance definido. En adición, deberá verificar el estatus de las acciones detalladas en los planes de acción elaborados por las áreas propietarias de los riesgos, así como otros aspectos relacionados. Los resultados de estas verificaciones deberán ser comunicados oportunamente a las partes interesadas.

A partir de los resultados de la aplicación de estas herramientas se generan planes de acción, los cuales son compromisos que deben ser rastreados y monitoreados en función del hallazgo identificado y las áreas involucradas para facilitar que las mejoras y controles requeridos se implementen adecuadamente.

VI. EVENTOS DE RIESGO OPERACIONAL

Las entidades deberán identificar los eventos de riesgo operacional agrupados por tipo de fallas o insuficiencias en los procesos, las personas, infraestructuras, sistemas y/o los eventos externos.

VI.1. Reporte y registro de los eventos

Las entidades para el registro y reporte de eventos de riesgo operacional deberán considerar lo siguiente:

a) **Código único:** Los eventos de riesgo operacional deberán tener un código único para cada suceso o agrupación y, por lo tanto, no debe repetirse para diferentes eventos, aunque estos sean de naturaleza similar.

b) **Agrupación de pérdidas:** Un evento puede tener como efecto una o más pérdidas o registros contables (impactos múltiples), por lo que la entidad debe estar en la capacidad de agrupar las pérdidas ocurridas por eventos. Para determinar las pérdidas a agrupar, se debe verificar que sean consecuencia del mismo evento con fecha de inicio y finalización determinada. A modo de ejemplo, de manera no limitativa, se mencionan algunas situaciones aplicables:

   i. Transacciones fraudulentas que afectan al mismo cliente originadas por robo de identidad en un periodo determinado.
   ii. Actividades fraudulentas realizadas por un mismo empleado o vinculado a la entidad en un periodo determinado.
   iii. Interrupciones repetitivas o intermitentes en una o varias sucursales debido a fallas ocasionadas por la misma causa raíz.

c) **Umbral de pérdidas económicas a ser reportadas de forma individual:** Las bases de datos internas de eventos por riesgo operacional deberán recoger la información de todos los eventos que hayan afectado a la entidad sin importar el monto de pérdida correspondiente, pero solo será requerido el reporte individual de eventos cuya pérdida económica bruta, es decir, sin considerar lo recuperado, sea igual o supere los DOP $50,000.00.

d) **Criterio de pérdidas no económicas a ser reportadas:** Los eventos con pérdidas no económicas, es decir, que no involucren un registro de un gasto o pérdida contable, deberán ser reportados conforme a la magnitud de sus consecuencias y el impacto que provoque a la entidad. Asimismo, se deberán agrupar cuando el evento ocurra repetidas veces en el mismo mes, especificando la cantidad de veces en el reporte. El umbral para reportar dichas pérdidas es de al menos DOP $50,000.00 de manera individual o por agrupación de eventos repetitivos de similar naturaleza en el mismo mes y corresponde a la estimación de costo de oportunidad que representa el evento Cuando no se pueda estimar monetariamente los efectos, se deberá considerar los siguientes criterios:

Tipo de consecuencias	Criterio para reporte
• Pérdida de eficiencia o eficacia y reprocesos. • Interrupción de las operaciones o del servicio. • Incapacidad para proporcionar servicio.	Interrupción o denegación del servicio dirigido a los clientes y/o procesos críticos para la operación de la entidad (por ejemplo: servicio al cliente, consulta de transacciones, monitoreo transaccional, registros contables, etc.) por 4 horas o más.
• Impacto negativo a la imagen de la marca, la reputación o credibilidad de la entidad.	Evento publicado en prensa digital o escrita, redes sociales u otro medio de comunicación reconocido.
• Pérdida de clientes, personal o proveedores.	Reclamaciones o quejas de más de cinco (5) clientes, o de uno (1) o más proveedores o colaboradores que corresponda al mismo tipo de eventos.
• Pérdida de la ventaja competitiva.	Pérdida de valores o cualidades con las que cuenta la entidad y que la ayudan a diferenciarse positivamente de su competencia.
• Afectación a la salud o integridad física de colaboradores y funcionarios. • Afectación a la salud o integridad física de clientes o terceros dentro del perímetro de su localidad.	Licencia otorgada a lesionados de más de 5 días laborables, internamientos o fallecimientos.

e) **Eventos con efecto contable positivo:** Los eventos de riesgo operacional provocados por errores, fallas u omisiones que generen un beneficio económico a la entidad y haya sido registrado contablemente, por ejemplo, comisiones cobradas por error, sobrantes de efectivo en caja, entre otros, no deberán ser reportados como eventos de pérdida económica, ni considerarse el monto contable positivo como monto de pérdida. En su lugar, estos deberán incluirse en la base de datos de eventos y ser reportados como pérdida no económica si cumplen con los criterios establecidos para su reporte. El monto para reportar corresponderá a la estimación de la pérdida que se generará como consecuencia del error cometido (riesgo reputacional, pérdida de clientes, etc.). Por tanto, el monto de pérdida no debe reflejar el monto percibido como ingresos dado el error.

f) **Reporte de eventos con pérdidas económicas menores al umbral:** Aquellos eventos de similar naturaleza que se produzcan en el mismo mes, y que individualmente sus pérdidas brutas no alcancen el umbral definido para el reporte individual de DOP $50,000.00, deberán ser reportados en forma consolidada bajo un mismo código de evento sin restricción del monto total que sume dicha agrupación (monto de pérdida total puede ser menor, igual o mayor al umbral definido para el reporte de eventos individuales), indicando la cantidad de eventos agrupados. Esta agrupación debe considerar que los eventos ocurran por el mismo canal, para el mismo tipo de producto, aunque hayan ocurrido para clientes diferentes, y que las pérdidas se hayan registrado en la misma cuenta contable.

En cuanto a las fechas de descubrimiento, inicio, finalización y contabilización se deberá utilizar una fecha de referencia del grupo de eventos, que pudiera corresponder a la fecha más antigua de inicio y descubrimiento y la más reciente para la finalización y contabilización. De igual manera, si de forma posterior se recupera o actualiza algunas de las pérdidas de los eventos agrupados, se deberá remitir el monto recuperado correspondiente con la misma referencia de código de evento donde fue incluido el mismo.

Por ejemplo:

Evento	Cantidad de eventos	Fecha inicio	Fecha finalización	Fecha descubrimiento	Fecha contabilización	Cuenta contable	Monto de pérdida
EVENTO 1		01/04/2022	02/04/2022	02/04/2022	20/04/2022	147.13.1	4,500
EVENTO 2		15/04/2022	17/04/2022	17/04/2022	25/04/2022	147.13.1	5,000
GRUPO	2	01/04/2022	17/04/2022	02/04/2022	25/04/2022	147.13.1	9,500

g) **Pérdidas adicionales y recuperaciones posteriores:** Los registros de pérdidas deben ser agrupados por cada cuenta contable afectada para el reporte de eventos, a menos que se contabilicen nuevas pérdidas del mismo evento en un periodo posterior, para lo cual se deberán identificar los montos de dichas pérdidas adicionales, y reportar con el mismo código de evento asignado previamente. Para reportar las pérdidas adicionales o recuperaciones posteriores, se debe remitir la actualización del evento con los montos de pérdida o recuperaciones no reportados previamente, incluyendo los datos de la fecha de contabilización y cuenta contable relativas a la pérdida o recuperación adicional que se esté registrando, y estas deben coincidir con los registros contables.

h) **Tipo de registro para reporte de eventos:** Se deberá identificar el tipo de registro del reporte de eventos con el fin de poder segregar los que aplican como pérdidas o recuperaciones adicionales, de los que corresponden a la reclasificación contable de pérdidas o provisiones reportadas.

i) **Múltiples cuentas contables:** Los eventos cuyas pérdidas afecten más de una cuenta contable, se deberán reportar en diferentes registros utilizando el mismo código de evento e indicando cada cuenta contable con su correspondiente monto y fecha de contabilización.

j) **Moneda:** Las pérdidas por eventos de riesgo operacional deberán registrarse en moneda nacional. Cuando la pérdida se origine en moneda extranjera se deberá realizar la conversión en base a la tasa de compra del mercado spot publicada por el Banco Central de la República Dominicana para el día del registro contable del evento.

VI.2. Base de datos de eventos

Las bases de datos de eventos de riesgo operacional solo deberán contener los eventos materializados con algún tipo de consecuencia, ya sea económica o no económica, recuperada o no recuperada. En este sentido, no deberán incluirse los sucesos cuyas consecuencias hayan sido evitadas debido a la efectividad de los controles internos o por circunstancias fortuitas, tales como: los intentos de fraudes a tarjetas de créditos detectados cuyas transacciones no son aprobadas, la detección de un intento de ataque cibernético, no autorización de un cambio de cheque fraudulento, transferencia incorrecta detectada que es reversada de forma inmediata, entre otros.

Los tipos de eventos sin consecuencia deberán ser considerados a través de indicadores por las entidades para el monitoreo de riesgos inherentes de los procesos, manteniendo registros verificables, de su ocurrencia y el tratamiento dado. El análisis de esos registros deberá ser considerado como parte de las informaciones cuantitativas para la determinación de las probabilidades de esos riesgos y la efectividad histórica de los controles relacionados.

Las entidades deberán preparar la base de datos siguiendo los lineamientos siguientes:

a) **Criterios de calidad de base de datos de eventos:** La calidad, integridad y solidez de los datos sobre pérdidas por riesgo operacional resulta indispensable, por lo que es necesaria una correcta identificación, recopilación y tratamiento de los datos. Para esto se requiere que la entidad, en adición a lo antes expuesto cumpla con los requisitos siguientes:

   i) **Procedimientos:** Contar con procesos y procedimientos documentados para la identificación, recopilación y tratamiento de los datos de eventos de riesgo operacional. Tales procesos y procedimientos deberán estar sujetos a validación y a revisiones independientes periódicas de las unidades de auditoría interna o externa.

   ii) **Criterios de asignación de tipos de eventos:** Contar con criterios documentados de asignación de las pérdidas a los tipos de eventos definidos en la "Tabla 2. Características de los tipos de eventos de riesgo operacional" en Anexos. Las entidades deberán organizar la base de datos de eventos considerando el nivel 3 de la taxonomía de tipos de eventos de riesgo operacional que se establece en la Tabla "T097. Tipo de eventos de riesgo" definida en el Manual de Requerimientos de Información de la Administración Monetaria y Financiera (MRI). En caso de que la entidad tenga una taxonomía propia, esta deberá tener correspondencia con la establecida para el reporte de eventos.

   iii) **Integralidad de la base de datos:** Los datos internos sobre pérdidas deben ser integrales e incluir la totalidad de las actividades y exposiciones relevantes en todos los subsistemas y en todas las ubicaciones geográficas pertinentes.

   iv) **Integridad de los datos:** La instrumentación de la base de datos de eventos de riesgo operacional, independientemente del medio utilizado para su registro, deberá contemplar la preservación de la integridad de los datos ya registrados, no permitiendo, una vez ingresados, su posterior alteración o modificación, a menos que sea para registrar nuevas pérdidas o recuperación de pérdidas y sus correspondientes fechas, así como las fechas de finalización y cierre del evento. En caso de identificarse un error involuntario en la información contenida en el registro o en el reporte, la entidad deberá contar, como mecanismo de control, con una autorización previa interna para efectuar la corrección correspondiente en el registro. Asimismo, toda modificación que impacte la información remitida a la Superintendencia de Bancos deberá contar con la autorización previa de este ente supervisor.

   v) **Fechas de referencia del evento:** Las entidades deben recopilar las fechas de referencia de los eventos de riesgo operacional, siguientes:

      - Fecha en que se produjeron o se iniciaron (materialización o de inicio);

- Fecha en que finalizaron los efectos del evento (finalización);
- Fecha en la que la entidad tuvo conocimiento de dicho evento (descubrimiento);
- Fecha (o fechas) en la que el evento dio lugar al reconocimiento de una pérdida, reserva o provisión en las cuentas de ganancias y pérdidas (contabilización); y,
- Fecha (o fechas) en la que se registraron recuperaciones de pérdidas por seguros u otros medios (recuperación).

La fecha de finalización del evento puede quedar pendiente o en blanco si el evento o los efectos del evento no han finalizado a la fecha del reporte, y la fecha de cierre puede quedar pendiente si aún quedan gestiones de recuperación por agotar o contabilización de pérdidas por registrar. Posteriormente, debe ser remitida una actualización del evento con la fecha de finalización y cierre del evento, así como con los datos contables que apliquen, utilizando el mismo código del evento.

b) **Construcción de base de datos y reporte de eventos:** Los eventos deben ser reportados de forma oportuna a la Superintendencia de Bancos, por lo que las entidades deben recopilar las informaciones del evento para ser informados según el periodo correspondiente al reporte.

i) Para el registro sobre eventos de riesgo operacional con pérdida económica se deberá utilizar la fecha de contabilización del evento para construir la base de datos, así como para su reporte.

ii) En el caso de eventos con contingencias legales, la fecha de contabilización será aquella en la que se constituye o asigna una provisión para esta reserva legal en el Estado de Situación Financiera, con su reflejo correspondiente en el Estado de Resultados. Para fines de reporte, se considerará como fecha de contabilización la fecha de asignación de las provisiones constituidas que son asignadas a eventos con posterioridad.

iii) Los eventos con pérdidas no económicas o con pérdidas económicas pendientes de contabilizar, se deberá utilizar la fecha de descubrimiento como referencia para el reporte.

c) **Asignación de pérdidas en la contabilidad:** Las pérdidas causadas por un evento de riesgo operacional común o por varios eventos de riesgo operacional relacionados a lo largo del tiempo, pero contabilizadas en el transcurso de varios años, deberán asignarse a los años correspondientes en la base de datos sobre pérdidas, en consonancia con su tratamiento contable.

d) **Recuperación de pérdidas:** Se debe recoger información sobre recuperaciones de importes brutos de pérdidas. Las pérdidas por riesgo operacional podrán ser recuperadas a través de diferentes medios, lo cual debe especificarse en la base de datos de registros de pérdidas, incluyendo las siguientes: compañías de seguros, acciones judiciales, otros. Para el reporte de eventos debe especificarse el monto recuperado por seguros y el monto recuperado por otros medios.

e) **Información descriptiva:** Se debe recoger información descriptiva sobre los factores determinantes o las causas del evento. El grado de detalle de la información descriptiva deberá estar en proporción al importe bruto de la pérdida. Para el registro y reporte de eventos de riesgo operacional, se deberán seleccionar de manera cautelosa los caracterizadores correspondientes a cada evento registrado y

reportado (tipo de evento, producto o servicio, canal de distribución, departamento, causa, consecuencia, etc.).

f) **Eventos relacionados a otros tipos de riesgos:** Los eventos de riesgo operacional relacionados con riesgos financieros deberán registrarse en la base de datos de riesgo operacional cuando la principal causa de la pérdida sea de naturaleza operacional y no se tengan en cuenta en los activos ponderados por riesgos.

g) **Revisión de datos:** Las entidades deben contar con procesos concebidos para revisar de forma independiente la integridad y precisión de los datos sobre pérdidas. Las bases de datos internas de eventos de riesgo operacional deben ser conciliadas periódicamente con la contabilidad, para asegurar que las cuentas contables utilizadas y los montos registrados en la base de datos, ya sean recuperados o no, coincidan con lo contabilizado. Esta verificación debe incluir además la conciliación de las pérdidas por eventos de riesgo operacional reportados a la Superintendencia de Bancos contra la contabilidad y la base de datos interna.

h) **Aplicabilidad de recuperaciones:** Las recuperaciones solo pueden utilizarse para reducir las pérdidas netas cuando la entidad haya recibido el pago. Los derechos de cobro no cuentan como recuperaciones. Las entidades deberán conservar los comprobantes de los pagos recibidos utilizados para compensar pérdidas por un período mínimo de diez (10) años, contados a partir de la fecha de su registro, garantizando su disponibilidad para fines de verificación, auditoría y supervisión.

Los sucesos cuyas consecuencias hayan sido evitadas, deberán ser considerados a través de indicadores por las entidades para el monitoreo de riesgos inherentes de los procesos, manteniendo registros verificables, de su ocurrencia y el tratamiento dado. El análisis de esos registros deberá ser considerado como parte de las informaciones cuantitativas para la determinación de las probabilidades de esos riesgos y la efectividad histórica de los controles relacionados.

VI.3. Cuentas contables para registro de pérdidas

Las entidades utilizarán las cuentas previstas en el Manual de Contabilidad para Entidades Supervisadas, según la “Tabla 3. Cuentas contables para registro de pérdidas de eventos de riesgo operacional” (ver anexo). Estas cuentas no son exclusivas para reporte de eventos de riesgo operacional por lo que se deberá identificar la relación con el evento en el registro contable como parte de los auxiliares de dichas cuentas, así como en la base de datos de eventos.

Las partidas que se deben tomar en consideración para el registro de las pérdidas brutas en la base de datos, por tipo de pérdida económica, son las siguientes:

a) **Pérdida directa:** Cargos directos, incluidos cargos por deterioro y liquidaciones, registradas en las cuentas de pérdidas y ganancias, así como cancelaciones contables parciales como consecuencia del evento de riesgo operacional.

Para el registro de las pérdidas directas por eventos de Riesgo Operacional de los que se tiene certeza de recuperación, las entidades utilizarán cuentas transitorias específicas por un tiempo limitado

según las normas contables aplicables. Los importes contabilizados deben reflejar una estimación prudente de los montos a recibir.

En el caso de las pérdidas que se prevén no serán recuperadas debe reconocerse inmediatamente como gasto por eventos de pérdidas operacionales.

b) **Pérdida indirecta:** Gastos incurridos como consecuencia de un evento, incluyendo gastos externos con una relación directa al evento por riesgo operacional (ej. gastos legales directamente relacionados al evento y comisiones pagadas a los asesores, abogados o proveedores) y costos de reparación o reemplazo incurridos para restaurar la posición que prevalecía antes del evento de riesgo operacional.

c) **Provisiones:** Se deberán registrar las provisiones de las pérdidas esperadas ante demandas formalizadas y sanciones en apelación, en función de las estimaciones que realice la entidad en base a la probabilidad de pérdida de eventos legales, contabilizadas en las cuentas del Estado de Resultados contra el impacto potencial de pérdidas por riesgo operacional.

d) **Partidas a excluir:** Las siguientes partidas se deben excluir en el registro de las pérdidas económicas brutas en la base de datos de pérdidas:

i. Gastos incurridos para el establecimiento o mejora de controles con la finalidad de evitar la recurrencia de un evento.
ii. Costos de contratos de mantenimiento general de bienes raíces, planta y equipo.
iii. Gastos internos o externos destinados a mejorar el negocio después de las pérdidas por riesgo operacional: actualizaciones, iniciativas y mejoras en la gestión de riesgo.
iv. Primas de seguro.
v. Lucro cesante.
vi. Concesión comercial que la entidad asume con clientes como estrategia propia en función a un análisis costo beneficio, siempre que esta no sea originada por un evento de riesgo operacional.

Las pérdidas pendientes de contabilizar son aquellas provenientes de eventos por riesgo operacional con un impacto financiero definitivo, que aún no están reflejadas en las cuentas del Estado de Resultados. Las pérdidas pendientes deben ser incluidas en la base de datos y podrán permanecer con este estatus de acuerdo con el tamaño de la pérdida y tiempo requerido para la finalización de la investigación y contabilización.

VI.4. Informe de eventos materiales

Los eventos materiales deberán ser informados a la Superintendencia de Bancos a través del Portal SB Interactivo en los plazos establecidos en el Manual de Solicitudes y comunicado una vez tenga conocimiento al Punto Central de Contacto (PCC). Deberán ser reportados los eventos que presenten, de manera no limitativa, alguna de las características siguientes:

i. Pérdida significativa de activos equivalente o mayor a los DOP $5,000,000.00 de pérdida neta, o pendiente de recuperar;

ii. Indisponibilidad o interrupción prolongada de un servicio dirigido al cliente y/o procesos críticos de la entidad por un periodo igual o mayor a 4 horas;
iii. Ataques cibernéticos que afecten los objetivos de seguridad de la información (confidencialidad, integridad, disponibilidad); deberán seguir el protocolo establecido en la normativa relativa a la Seguridad Cibernética y de la Información;
iv. Eventos con pérdida de vida humana u hospitalizaciones;
v. Robo y/o divulgación de información confidencial de la entidad o de los clientes; y
vi. Eventos con impacto en la imagen y reputación de la entidad que hayan requerido un pronunciamiento oficial.

Se deberá remitir el detalle del "Informe Eventos Materiales de Riesgo" en un plazo no mayor a diez (10) días calendario luego de identificar el evento. Este informe deberá contener una descripción detallada del incidente, causas identificadas y consecuencias estimadas, así como los planes de acciones correctivas y preventivas en proceso. Las áreas involucradas con los procesos y/o la naturaleza del evento deberán participar en la elaboración de este informe.

En adición, el evento debe ser reportado al corte correspondiente junto con el resto de los eventos contabilizados y/o descubiertos en el periodo.

VII. RESILIENCIA OPERATIVA

La resiliencia operativa requiere una visión integral de las operaciones críticas, así como la capacidad de ejecutarlas eficazmente ante escenarios severos pero plausibles, dentro de los niveles de interrupción tolerables. Si bien estas operaciones deben ser atendidas con carácter prioritario, un enfoque consolidado de resiliencia operativa incorpora progresivamente otras actividades que, aunque no críticas, podrían generar impactos relevantes. Las entidades deberán considerar medidas que fomenten y contemplen la resiliencia operativa, atendiendo como mínimo los aspectos siguientes:

a) Gobernanza: El consejo aprobará la estrategia de la resiliencia operativa y la alta gerencia, es responsable de desarrollarla, asignar roles y responsabilidades, y supervisar su implementación;

b) Mapeo de procesos de negocio: Deben mapear sus procesos de negocio críticos y de apoyo, identificando las interdependencias y los recursos necesarios para su funcionamiento;

c) Resiliencia de la Infraestructura de la Tecnología y Seguridad de la Información (TSI): Garantizar la resiliencia de su infraestructura de TSI, incluyendo la ciberseguridad, para soportar la continuidad de los procesos de negocio críticos;

d) Resiliencia de servicios tercerizados: Gestionar los riesgos de resiliencia operacional asociados con los proveedores de servicios tercerizados o terceros contratados;

e) Planes de continuidad de negocio: Desarrollar, mantener y probar planes de continuidad de negocio para asegurar la recuperación oportuna de los procesos de negocio críticos; y

f) Plan de comunicación: Establecer estrategias de comunicación efectivas para gestionar las comunicaciones internas y externas durante una interrupción.

g) Aprendizaje y mejora continua: Las entidades deberán evaluar los incidentes y resultados de las pruebas, documentar las lecciones aprendidas y actualizar oportunamente sus estrategias, niveles tolerables, mapas de dependencias, planes, controles y capacidades de resiliencia.

VIII. LINEAMIENTOS PARA LAS SOLICITUDES DE RIESGO OPERACIONAL

Las entidades deberán comunicar a la Superintendencia de Bancos, la ocurrencia de las situaciones que involucren una evaluación de riesgo operacional por representar cambios significativos a nivel de riesgo operacional para la entidad, previstas en el "Manual de solicitudes de autorización, no objeción y notificaciones de las entidades supervisadas por la Superintendencia de Bancos".

Las solicitudes de riesgo operacional que requieran un informe o una matriz de riesgo deberán considerar, sin ser limitativo, lo siguiente:

a) **Informe de evaluación de riesgos operacionales.** Este debe incluir como mínimo los puntos siguientes:

   i. Descripción detallada del proyecto, incluyendo el detalle de los procesos a modificar y los nuevos procesos a crear.
   ii. Descripción de la metodología de la evaluación de la materialidad del producto, servicio, sistema, proceso o canal evaluado y calificación resultante. (ver anexo "Tabla 1. Criterios de evaluación de materialidad operativa").
   iii. Descripción de la metodología de la evaluación de riesgos, que muestre cómo se determina el nivel de probabilidad, impacto, niveles de riesgo inherente y residual, y calificación de efectividad de controles.
   iv. Mapa de calor de riesgos inherentes y residuales identificados.
   v. Plan de implementación de medidas para controlar el riesgo.
   vi. Opinión del área de riesgo operacional.

b) **Matriz de riesgos operacionales identificados y controles.** Esta matriz debe presentarse de manera tabular en formato de hoja de cálculo, y también puede ser incluida como parte del informe de evaluación de riesgos operacionales. Debe contener como mínimo:

   i. Descripción de los riesgos operacionales (entre estos, los de tecnología y seguridad de la información relacionados al proyecto).
   ii. Evaluación del riesgo inherente (probabilidad, impacto y nivel resultante).
   iii. Descripción de los controles para mitigar dichos riesgos, incluyendo sin ser limitativo el tipo de control, naturaleza del control (p.ej.: manual, automático), calificación de la efectividad del control (p. ej.: fuerte, moderado, débil).
   iv. Evaluación del riesgo residual (probabilidad, impacto y nivel resultante). Para los controles que no estén implementados, el nivel de riesgo residual se asignará en función de la expectativa de efectividad del control seleccionado (Formato Excel). La valoración prospectiva de controles no

implementados aplica a nuevos productos, servicios, procesos, sistemas, proyectos o cambios que todavía no hayan entrado en operación, y no reduce el riesgo residual vigente de procesos actualmente operativos.

v. Planes de acción (descripción de la acción, responsable y fechas).

IX. REQUERIMIENTO DE CAPITAL

IX.1. Metodología para cálculo del capital por riesgo operacional (ORC)

Las entidades de intermediación financiera deberán reservar capital por el riesgo operacional de sus actividades. Para determinar este capital requerido por riesgo operacional (ORC, por sus siglas en inglés), se utilizará la metodología del método estándar propuesta por el Comité de Basilea, en el marco de Basilea III, el cual deberán multiplicar el capital requerido por 10.0 (la recíproca del coeficiente de solvencia de 10%) y el resultado se adiciona al monto de los activos y contingentes ponderados por riesgo.

Esta metodología fundamenta su cálculo en la multiplicación de dos componentes: el componente de indicador de negocios (BIC, por sus siglas en inglés) y el multiplicador de pérdidas internas (ILM, por sus siglas en inglés).

$$ORC = BIC \,.\, ILM$$

Donde:
ORC = Capital requerido por riesgo operacional
BIC = Componente de indicador de negocios
ILM = Multiplicador de pérdidas internas

La metodología estándar para el cálculo del ORC tiene variación de acuerdo con los resultados del Indicador de Negocios (BI, por sus siglas en inglés) de la entidad y con la calidad de la base de datos de pérdidas de esta, según lo describe el siguiente cuadro:

Categoría del BI	Cumple criterios de calidad de base de datos de eventos	No cumple criterios de calidad de base de datos de eventos
Tramo 1	ORC = BIC	ORC = BIC x (ILM > 1)
Tramo 2	ORC = BIC . ILM	ORC = BIC x (ILM > 1)
Tramo 3	ORC = BIC . ILM	ORC = BIC x (ILM > 1)

Tal como se indica en el cuadro, el ORC de las entidades cuyo BI se encuentre en el tramo 1, no será afectado por el componente de pérdidas internas (ILM), ya que su ORC = BIC. Las entidades cuyo BI se encuentre en los tramos 2 y 3 deberán utilizar el ILM para el cálculo del ORC, cuando cumplan con los requisitos mínimos de calidad en la recolección de datos de pérdidas operacionales definidos en este instructivo.

El cálculo del promedio de pérdidas para el componente de pérdidas (LC, por sus siglas en inglés) debe basarse en los últimos diez (10) años, lo que equivale a 120 meses de datos. Las entidades que no dispongan de datos requeridos deberán mantener un capital por riesgo operacional igual al 100% del BIC.

Párrafo transitorio: Para la aplicación de este cálculo será utilizado el promedio de pérdidas de los últimos cinco (5) años, hasta tanto la Superintendencia de Bancos notifique la ampliación de la cantidad de años a requerir.

Asimismo, aquellas entidades que no cumplan con los criterios de calidad de los datos de pérdidas o presenten deficiencias en la gestión del riesgo operacional deberán mantener un capital por riesgo operacional igual al resultado de multiplicar el BIC por un ILM mayor a uno (1). El valor del ILM será determinado y notificado por la Superintendencia de Bancos.

El detalle de las fórmulas para el cálculo del ORC y la definición de los componentes de estas, se encuentran en la "Tabla 4".

IX.2. Cálculo del componente del indicador de negocios (BIC)

El cálculo del BIC está basado en la multiplicación del indicador de negocios (BI) por una serie de coeficientes marginales (∝). El BI es una aproximación al riesgo operacional basada en los estados financieros de las entidades y se obtiene a través de la suma de tres componentes:

1) Componente de intereses, arrendamientos y dividendos (ILDC, por sus siglas en inglés)
2) Componente de servicios (SC, por sus siglas en inglés)
3) Componente financiero (FC, por sus siglas en inglés)

$$BI = ILDC + SC + FC$$

Para obtener estos componentes se utiliza la información contable del promedio de tres (3) años de las cuentas detalladas en la "Tabla 5. Asignación de cuentas contables para determinación del Indicador de Negocios (BI)" (ver anexos). Se deberá calcular el valor absoluto de las partidas netas (por ejemplo, ingresos por intereses - gastos por intereses) para cada año, para después calcular el promedio de los tres años.

Considerando lo anterior, se procede a calcular cada componente del BI de la siguiente manera:

$$\text{ILDC= Min}[Abs(\overline{II - GI}); 2.25\%.\overline{ADI}\ ] + \overline{ID}$$

Donde:
II = Ingresos por intereses
GI = Gastos por intereses
ADI = Activos que devengan intereses
ID = Ingresos por dividendos

$$\text{SC= Max}[\overline{OIO};\ \overline{\text{OGO}}] + Max[\overline{IHC}; \overline{GHC}]$$

Donde:
OIO = Otros ingresos operacionales
OGO = Otros gastos operacionales
IHC = Ingresos por comisiones
GHC = Gastos por comisiones

$$FC=Abs(\overline{ICN}) + Abs(\overline{ICI})$$

Donde:

ICN = Beneficio o pérdida neto (a) de la cartera de negociación

ICI = Beneficio o pérdida neto (a) de la cartera del libro bancario

Para las cuentas de gastos e ingresos, se consideran los valores acumulados de los últimos treinta y seis (36) meses. Para las cuentas de activos y pasivos se considera el valor registrado al cierre del mes correspondiente al requerimiento abarcando los dos (2) años anteriores y el año en curso.

Por ejemplo, para el requerimiento a mayo de 2026 se considera el promedio de los siguientes periodos según el tipo de cuenta:

Cuentas de ingresos y gastos:
Año 1: junio 2023 a mayo 2024
Año 2: junio 2024 a mayo 2025
Año 3: junio 2025 a mayo 2026

Cuentas de activos y pasivos:
Año 1: mayo 2024
Año 2: mayo 2025
Año 3: mayo 2026

El BIC es el resultado de la suma ponderada del valor del BI, conforme a la categoría correspondiente, por su coeficiente marginal ($\propto$), los cuales aumentan conforme incremente el tamaño del BI. Las diferentes categorías y sus coeficientes marginales se definen en el siguiente cuadro en millones de DOP:

Categoría del BI	Tramo de BI (en millones de DOP$)	Coeficientes marginales de BI ($\propto$)
Tramo 1	BI ≤ 10,501	12%
Tramo 2	10,501 < BI ≤ 150,000	15%
Tramo 3	BI > 150,000	18%

Para este ejemplo, una entidad con un BI de DOP$ 200,000,000,000 (200,000 millones) tendría un BIC de: (10,501,000,000 x 12%) + (150,000,000,000 – 10,501,000,000) x 15% + (200,000,000,000 - 150,000,000,000) x 18% = DOP$31,184,970,000 (31,184.97 millones).

IX.3. Cálculo del multiplicador de pérdidas internas (ILM)

El ILM es un factor exponencial fundamentado en el promedio de pérdidas históricas de la entidad y el BIC. A través de este, las pérdidas internas por riesgo operacional de la entidad pueden impactar el cálculo del capital por riesgo operacional. El ILM se determina a partir de la siguiente fórmula:

$$ILM = Ln\left(\exp(1) - 1 + \left(\frac{LC}{BIC}\right)^{0.8}\right)$$

Donde:

Ln = Logaritmo natural
Exp = Función exponencial
LC = Componente de pérdidas, igual a quince (15) veces el promedio de pérdidas anuales netas, incurridas durante los diez (10) años
BIC = Componente de Indicador de negocios

Por ejemplo, para una entidad con un promedio de pérdidas anuales netas de DOP 10,000,000 durante los últimos diez (10) años, el componente de pérdidas (LC) ascendería a DOP 150,000,000.

Si adicionalmente la entidad presenta un BIC de DOP 300,000,000, el cálculo del ILM sería el siguiente:

$$ILM = Ln\left(\exp(1) - 1 + \left(\frac{150{,}000{,}000}{300{,}000{,}000}\right)^{0.8}\right)$$

$$ILM = Ln\,(2.7183 - 1 + (0.5)^{0.8})$$

$$ILM = Ln\,(2.7183 - 1 + 0.5743)$$

$$ILM = Ln\,(1.7183 + 0.5743)$$

$$ILM = Ln\,(2.2926)$$

$$ILM = 0.8297$$

X. LINEAMIENTOS PARA LOS INTERMEDIARIOS CAMBIARIOS

X.1. Gestión del riesgo operacional

Los intermediarios cambiarios deberán gestionar el riesgo operacional conforme a su naturaleza, volumen y cantidad de operaciones, complejidad y su interconexión con otras entidades.

Los intermediarios cambiarios deberán mantener una base de registro de incidentes que les permita identificar, documentar, monitorear reportar los incidentes de riesgo operacional categorizados como graves.

Se considerarán incidentes operacionales graves sujetos a reporte aquellos originados por fallas en procesos, personas o sistemas internos, o por eventos externos, cuyo impacto económico sea igual o superior al cero punto cinco por ciento (0.5 %) del capital regulatorio mínimo requerido vigente y que cumplan con al menos uno alguno de los siguientes criterios, los cuales se presentan de manera enunciativa y no limitativa:

a) Errores operativos con afectación significativa: errores o incidentes operativos que ocasionen impactos sobre múltiples operaciones, clientes, servicios o canales, independientemente de que hayan sido identificados y corregidos posteriormente.

b) Daños físicos o eventos externos que afecten la operación: incendios, inundaciones, fenómenos naturales, fallas de energía, disturbios u otros eventos externos que comprometan la disponibilidad de instalaciones, personal, sistemas o servicios críticos.

c) Amenacen la confidencialidad, integridad o disponibilidad de la información: tales como fuga, acceso no autorizado, alteración o posible filtración de datos de clientes, operaciones, tasas, credenciales, archivos regulatorios y *malware/ransomware* en sistemas que soporten operaciones cambiarias.

d) Identificación de acceso no autorizado a sistemas críticos o plataformas regulatorias: acceso indebido a la plataforma cambiaria y aquellas requeridas por los reguladores, integración de pagos y *core* cambiario.

e) Fraude material interno o externo: fraude consumado que afecte caja, divisas, transferencias, operaciones con cuentas bancarias, remesas o conciliaciones.

f) Cualquier otro evento que, por su naturaleza, magnitud o potencial impacto, pueda comprometer la continuidad operativa, la seguridad de la información, la integridad de las operaciones, el cumplimiento regulatorio, la situación financiera o la reputación de la entidad.

Los incidentes que no generen una pérdida económica o contable directa deberán ser reportados cuando, por la magnitud de sus consecuencias, afecten de manera significativa las operaciones, la prestación de servicios, la reputación o el cumplimiento de las obligaciones de la entidad. Cuando un mismo tipo de incidente ocurra repetidamente durante un mismo mes y, en conjunto, alcance los criterios de gravedad establecidos, estos podrán reportarse de forma consolidada, indicando la cantidad de ocurrencias asociadas. Para fines de reporte, se deberán considerar los siguientes criterios:

TIPO DE CONSECUENCIAS	CRITERIO PARA REPORTE
• Interrupción de las operaciones o de la prestación de servicios	Interrupción, degradación o indisponibilidad de los servicios críticos de la entidad por un período igual o superior a cuatro (4) horas consecutivas.
• Afectación a la reputación o imagen de la entidad	Incidente que haya generado difusión en medios de comunicación, plataformas digitales o redes sociales con potencial impacto negativo para la imagen o credibilidad de la entidad.
• Reclamaciones o quejas de clientes	Recepción de más de cinco (5) reclamaciones o quejas relacionadas con un mismo evento o causa raíz.
• Afectación a la salud o integridad física de colaboradores, clientes o terceros	Incidentes que ocasionen lesiones que requieran licencia médica superior a cinco (5) días laborables, hospitalización o fallecimiento.
• Afectación significativa de procesos críticos	Incidentes que impidan o limiten la ejecución oportuna de procesos críticos relacionados con

TIPO DE CONSECUENCIAS	CRITERIO PARA REPORTE
	operaciones cambiarias, remesas, atención al cliente, monitoreo transaccional, registros o conciliaciones.

X.2. Requerimiento de capital

Los intermediarios cambiarios, de acuerdo con la categorización definida por el Reglamento Cambiario, deberán mantener un capital por riesgo operacional, conforme a lo establecido a continuación:

Tipo de entidad	Porcentaje aplicable sobre el capital regulatorio mínimo requerido vigente
Agentes de remesas y cambio	5% del capital regulatorio mínimo requerido vigente
Agentes de cambio categoría 'A'	3% del capital regulatorio mínimo requerido vigente
Agentes de cambio categoría 'B'	1% del capital regulatorio mínimo requerido vigente

Este requerimiento será adicional a cualquier otro capital regulatorio aplicable y deberá mantenerse de forma permanente para garantizar la cobertura ante eventos de riesgo operacional.

XI. SANCIONES

Las entidades que infrinjan las disposiciones del presente Instructivo serán pasibles de la aplicación de sanciones por parte de la Superintendencia de Bancos, conforme lo dispuesto en la Ley Núm. 183-02 Monetaria y Financiera del 21 de noviembre de 2002, y en base a las tipificaciones establecidas en el Reglamento de Sanciones aprobado mediante la Quinta Resolución de la Junta Monetaria de fecha 18 de diciembre del 2003 y sus modificaciones, así como el Reglamento Cambiario aprobado mediante la Primera Resolución de la Junta Monetaria de fecha 11 de septiembre del 2025 y sus modificaciones.

ANEXOS

Tabla 1. Criterios de evaluación de materialidad operativa

Para fines regulatorios, la metodología utilizada por las entidades para evaluar la materialidad de un proceso, producto o servicio deberá considerar como mínimo, sin perjuicio de otros que la entidad determine incorporar en función de su naturaleza, tamaño, complejidad y perfil de riesgo los criterios siguientes:

	Criterio	Proceso o Servicio Material
1	Contribución estratégica	El proceso o servicio está orientado a contribuir de manera directa al logro de uno o varios de los objetivos del plan estratégico de la entidad.
2	Contribución a procesos esenciales	El proceso o servicio está orientado a contribuir de manera directa al buen desempeño de uno o varios de los procesos esenciales de la entidad.
3	Contribución a procesos de apoyo considerados críticos	El proceso o servicio está orientado a contribuir de manera directa al buen desempeño de uno o varios de los procesos de apoyo que la entidad ha considerado crítico.
4	Impacto en la reputación	El proceso o servicio está concebido como mitigante de riesgos relacionados a la reputación de la entidad, y/o para la gestión de eventos que hayan tenido impacto en la reputación.
5	Impacto en personas	El proceso o servicio está concebido como mitigante de riesgos sobre la integridad física de las personas (empleados, contratistas, clientes, etc.).
6	Impacto sobre la seguridad de la información	El proceso o servicio está concebido como mitigante de riesgos sobre los objetivos de la seguridad de la información (confidencialidad, integridad y disponibilidad).
7	Contribución a la gestión del riesgo y al cumplimiento regulatorio	El proceso o servicio está concebido para lograr la gestión del riesgo y/o el cumplimiento regulatorio requerido a la entidad.
8	Impacto presupuestario	El presupuesto estimado para la puesta en marcha o mantenimiento del proceso o servicio representa al menos un 5% del presupuesto general aprobado por la entidad, o al menos el 15% del presupuesto del área a la que corresponde.
9	Exclusividad del proceso o servicio	Las opciones de oferta para la implementación y/o ejecución del proceso o servicio está limitada a no más de 2 proveedores, lo que dificulta las alternativas de elección y/o reemplazo.

Tabla 2. Características de los tipos de eventos de riesgo operacional

Tipo de evento (Nivel 1)	Definición	Características del tipo de evento
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.	• Hay intencionalidad. • Existe ánimo de lucro (beneficio ilícito personal o de un tercero) • Interviene una persona vinculada a la entidad (colaboración o participación). • Se violan políticas internas, sistemas internos o leyes nacionales.
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.	• Hay intencionalidad. • Existe ánimo de lucro. • Interviene una persona externa a la entidad (sin colaboración interna).
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.	• Implica litigios, multas, o indemnizaciones relacionadas a aspectos laborales. • Infracciones de las normas laborales de seguridad e higiene, • Acusaciones de discriminación, • Daños a la salud física, mental o emocional, u otro tipo de pérdida relacionada.
Clientes, productos y prácticas empresariales	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.	• Involucra la inobservancia de regulaciones, excluyendo los errores involuntarios de ejecución de actividades habituales. • Existe un beneficio directo para la entidad o para un tercero (económico o de otro tipo para la estrategia comercial). • Implica litigios o multas por infracciones de la normativa vigente y del marco jurídico existente, o indemnización a clientes que hayan sido perjudicados. • Relacionado con el proceso de comercialización.

Tipo de evento (Nivel 1)	Definición	Características del tipo de evento
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.	• No existe ánimo de lucro • Aplica cuando ocurre por una de estas causas: a) Generan pérdidas por eventos naturales o por accidentes (incendios, inundaciones, etc.). b) Generan pérdidas por eventos externos cuya ocurrencia está fuera del control de la entidad (vandalismo, terrorismo, huelgas, etc.).
Incidencias en el Negocio y Fallos en los Sistemas	Pérdidas derivadas de incidencias en el negocio y de fallos en los sistemas.	• Aplica cuando ocurre por una de estas causas: a) Producen fallas en infraestructura y/o sistemas que involucre un impacto financiero o afecte la operatividad. b) Ocurren interrupciones de algún servicio básico (agua, electricidad, etc.).
Fallas en la Ejecución, Entrega o Gestión de los 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.	• La pérdida es provocada por acción u omisión en la ejecución de operaciones. • Errores cometidos de forma involuntaria en la operativa y gestión de procesos. • La transacción origen de la pérdida no se encuentra vinculada al proceso de comercialización de productos o servicios.

Tabla 3. Cuentas contables para registro de pérdidas de eventos de riesgo operacional

Tipo de pérdida económica	Naturaleza de las pérdidas	Cuentas contables	Registro contable de recuperación y pérdidas definitivas
Pérdidas Directas e indirectas	Pérdidas definitivas sin certeza de recuperación.	**562.01** Pérdidas por fraude interno **562.02** Pérdidas por fraude externo **562.03** Pérdidas por relaciones laborales y seguridad en el puesto de trabajo **562.04** Pérdidas por clientes, productos y prácticas empresariales **562.05** Pérdidas por daños a activos materiales **562.06** Pérdidas por interrupción del negocio y fallos en los sistemas **562.07** Pérdidas por ejecución, entrega y gestión de procesos	Los casos extraordinarios de recuperación se deben registrar contablemente por Ingresos en la cuenta "439.03 - Ingresos por recuperación de gastos".
	Pérdidas con certeza de recuperación a través de compañías de seguro.	**147.06** Indemnizaciones reclamadas a compañías de seguros	Las recuperaciones se reducen de las cuentas 147.06 y 147.13, y las pérdidas definitivas se reclasifican a la cuenta 562.00 correspondiente.
	Pérdidas con certeza de recuperación por otros medios.	**147.13** Cuentas por recuperar por eventos de Riesgo Operacional **147.13.M.01** Cuentas por recuperar por fraudes de tarjetas de crédito y débito por contracargos a marcas **147.13.M.02** Cuentas por recuperar del personal, cliente, proveedor o relacionado	
Provisiones	Contraparte de la cuenta 253.05 para las provisiones previas asignadas por probables pérdidas esperadas atribuibles a la materialización	**561.05** Constitución de provisión por eventos de riesgo operacional	La reducción de provisiones se registra por la cuenta "435.02 - Disminución de provisión por otros conceptos". No se reporta recuperación. Para reflejar la liberación de provisión en el reporte,

Tipo de pérdida económica	Naturaleza de las pérdidas	Cuentas contables	Registro contable de recuperación y pérdidas definitivas
	del riesgo operacional que puedan surgir para la entidad.		se remite el monto actualizado de pérdida. Las pérdidas definitivas pasan a la cuenta de pasivo 251.20.
	Contraparte de la cuenta 253.03 para las provisiones registradas por las probables obligaciones que puedan surgir para la entidad a consecuencia del resultado desfavorable de demandas en su contra que se encuentran pendientes de solucionar.	**561.04** Constitución de provisión para pasivos contingentes	
	Provisiones registradas por las probables obligaciones que puedan surgir para la entidad a consecuencia del resultado desfavorable de demandas en su contra que se encuentran pendientes de solucionar.	**253.03** Provisiones por litigios pendientes	
	Pérdidas definitivas que fueron previamente provisionadas	**251.20** Cuenta por pagar por eventos de riesgo operacional	No aplica recuperación debido a que corresponde a una cuenta por pagar para un fallo definitivo que fue

Tipo de pérdida económica	Naturaleza de las pérdidas	Cuentas contables	Registro contable de recuperación y pérdidas definitivas
	en la cuenta 561.05/253.03 253.05/561.04		previamente provisionado.
	Provisiones previas asignadas por probables pérdidas esperadas atribuibles a la materialización del evento de riesgo operacional que puedan surgir para la entidad.	**253.05** Provisiones por eventos de riesgo operacional	

Tabla 4. Fórmulas para el cálculo del ORC y definición de los componentes

Componentes	Definición
$\mathrm{ORC} = \mathrm{BIC}\,.\,\mathrm{ILM}$	**ORC - capital requerido por riesgo operacional**
	BIC - Componente de indicador de negocios Es el resultado de la suma ponderada del valor del Indicador de Negocio (BI), conforme a la categoría correspondiente, por su coeficiente marginal (∝), los cuales aumentan conforme incrementa el tamaño del BI.
	ILM - Multiplicador de pérdidas internas Es el factor de ajuste y se calcula determinando el promedio de pérdidas operacionales históricas internas y afecta el componente de indicador de negocios.
BIC= BI **(∝)**	**BI - Indicador de negocios** Es una aproximación al riesgo operacional basada en los estados financieros, fundamentando su cálculo en la suma del Componente de intereses, arrendamiento y dividendos (ILDC), del Componente de Servicios (SC) y el Componente Financiero (FC).
	(∝) - coeficientes marginales
$\mathrm{BI} = \mathrm{ILDC} + SC + FC$	**ILDC - Componente de intereses, arrendamientos y dividendos:** Es uno de los componentes utilizados para el cálculo del indicador de negocios (BI), el cual se obtiene sumando el menor valor entre: 1) el promedio anual para los últimos tres años a la fecha del cálculo, del valor absoluto de la diferencia entre los ingresos por intereses (II) y los gastos por intereses (GI), y 2) 2.25% del promedio anual para los últimos tres años a la fecha del cálculo, de los activos que devengan intereses (AI), más el promedio anual para los últimos tres años a la fecha, de los ingresos por dividendos (ID).
	SC - Componente de servicios Es uno de los componentes utilizados para el cálculo del indicador de negocios (BI), el cual se obtiene sumando el mayor valor absoluto entre 1) el promedio anual para los últimos tres años a la fecha del cálculo de los otros ingresos de operacionales (IO) y 2) los otros gastos de operacionales (GO), más el promedio anual para los últimos tres años a la fecha del cálculo, del

Componentes	Definición
	mayor absoluto de 1) los ingresos por honorarios y comisiones (IH) y 2) los gastos por honorarios y comisiones (GH).
	FC - Componente financiero Es uno de los componentes utilizados para el cálculo del indicador de negocios (BI), el cual se obtiene del promedio anual para los últimos tres años a la fecha del cálculo, del valor absoluto del beneficio (pérdida) neto (a) en la cartera de negociación (BCN), más el promedio anual para los últimos tres años a la fecha del cálculo, del valor absoluto del beneficio (pérdida) neto (a) en la cartera del libro bancario (BCI).
ILDC= Min$[Abs(\overline{II - GI}); 2.25\%.\overline{ADI}] + \overline{ID}$	**II: Ingresos por intereses** Ingresos por intereses de todos los activos financieros.
	GI: Gastos por intereses Gastos por intereses de todos los pasivos financieros.
	ADI: Activos que devengan intereses Importe bruto total de la cartera de créditos, activos que devengan intereses y activos adquiridos para arrendamiento financiero medidos al final de cada ejercicio financiero.
	ID: Ingresos por dividendos Ingresos por dividendos de inversiones en acciones no consolidadas en los estados financieros de la entidad, incluidos los ingresos por dividendos de sociedades asociadas y negocios conjuntos.
SC= Max$[\overline{OIO}; \overline{OGO}] + Max[\overline{IHC}; \overline{GHC}]$	**OIO: Otros ingresos operacionales** Ingresos de operaciones ordinarias no incluidas en otras partidas del indicador de negocios (BI) pero de naturaleza similar (deberán excluirse los ingresos de arrendamientos operativos).
	OGO: Otros gastos operacionales Gastos y pérdidas de operaciones ordinarias no incluidas en otras partidas del indicador de negocios (BI) pero de naturaleza similar y pérdidas por eventos de riesgo operacional (deberán excluirse los gastos de arrendamientos operativos).
	IHC: Ingresos por comisiones

Componentes	Definición
	Ingresos percibidos por asesoramiento y servicio. Se excluyen los ingresos asociados a la comercialización de seguros.
	GHC: Gastos por comisiones Gastos pagados por asesoramiento y servicios. Se excluyen los servicios no financieros (por ejemplo, logísticos, informáticos o de recursos humanos).
FC=$Abs(\overline{ICN}) + Abs(\overline{ICI})$	**FC- Componente financiero (Financial Component)** Es uno de los componentes utilizados para el cálculo del indicador de negocios (BI), el cual resulta de obtener el promedio anual para los últimos tres años a la fecha del cálculo del valor absoluto del beneficio (pérdida) neto (a) en la cartera de negociación (BCN), más el promedio anual para los últimos tres años a la fecha del cálculo del valor absoluto del beneficio (pérdida) neto (a) en la cartera del libro bancario (BCI).
	ICN: Beneficio o pérdida neto(a) en la cartera de negociación.
	ICI: Beneficio o pérdida neto (a) de la cartera del Libro bancario
$ILM = Ln\left(\exp(1) - 1 + \left(\frac{LC}{BIC}\right)^{0.8}\right)$	**ILM: Multiplicador de Pérdidas Internas**
	Ln: Logaritmo natural.
	Exp: Función exponencial.
	LC: Componente de pérdidas, igual a quince (15) veces el promedio de las pérdidas operacionales netas, incurridas durante los cinco (5) años anteriores.
	BIC: Componente de indicador de negocios.

Tabla 5. Asignación de cuentas contables para determinación del Indicador de Negocios (BI)

- **Componente intereses, arrendamientos y dividendos (ILDC)**

Cuenta	Descripción Manual de Contabilidad
Ingresos por intereses Ingresos por intereses asociados a: Disponibilidades, cartera de créditos y de inversiones.	
411.01.M.01.01	Rendimientos por créditos comerciales
411.01.M.02.01	Rendimientos por créditos de consumo
411.01.M.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.02.M.01.01	Rendimientos por créditos comerciales
411.02.M.02.01	Rendimientos por créditos de consumo
411.02.M.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.03.M.01.01	Rendimientos por créditos comerciales
411.03.M.02.01	Rendimientos por créditos de consumo
411.03.M.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.04.M.01.01.01	Rendimientos por créditos comerciales
411.04.M.01.02.01	Rendimientos por créditos de consumo
411.04.M.01.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.04.M.02.01.01	Rendimientos por créditos comerciales
411.04.M.02.02.01	Rendimientos por créditos de consumo
411.04.M.02.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.04.M.03.01.01	Rendimientos por créditos comerciales
411.04.M.03.02.01	Rendimientos por créditos de consumo
411.04.M.03.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.05.M.01.01.01	Rendimientos por créditos comerciales
411.05.M.01.02.01	Rendimientos por créditos de consumo
411.05.M.01.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.05.M.02.01.01	Rendimientos por créditos comerciales
411.05.M.02.02.01	Rendimientos por créditos de consumo
411.05.M.02.03.01	Rendimientos por créditos hipotecarios para la vivienda
411.05.M.03.01.01	Rendimientos por créditos comerciales
411.05.M.03.02.01	Rendimientos por créditos de consumo
411.05.M.03.03.01	Rendimientos por créditos hipotecarios para la vivienda
412.01.M.01.01	Rendimientos por inversiones a valor razonable con cambios en resultados
412.01.M.02.01	Rendimientos por inversiones a valor razonable con cambios en resultados
412.01.M.03.01	Rendimientos por inversiones a valor razonable con cambios en resultados
412.01.M.04.01	Rendimientos por inversiones a valor razonable con cambios en resultados
412.02.M.01.01	Rendimientos por inversiones a valor razonable con cambios en el patrimonio

Cuenta	Descripción Manual de Contabilidad
412.02.M.02.01	Rendimientos por inversiones a valor razonable con cambios en el patrimonio
412.02.M.03.01	Rendimientos por inversiones a valor razonable con cambios en el patrimonio
412.02.M.04.01	Rendimientos por inversiones a valor razonable con cambios en el patrimonio
412.03.M.01.01	Rendimientos por inversiones a costo amortizado
412.03.M.02.01	Rendimientos por inversiones a costo amortizado
412.03.M.03.01	Rendimientos por inversiones a costo amortizado
412.03.M.04.01	Rendimientos por inversiones a costo amortizado
412.04.M.02.01	Rendimientos por otras inversiones en instrumentos de deuda
412.04.M.04.01	Rendimientos por otras inversiones en instrumentos de deuda
415.03.M.01.01.02	Rendimientos por intereses (cupones) de valores entregados en préstamo
415.03.M.01.01.03	Rendimientos por intereses (premio) del contrato de préstamo de valores
415.03.M.01.02.02	Rendimientos por intereses (cupones) de valores entregados en préstamo
415.03.M.01.02.03	Rendimientos por intereses (premio) del contrato de préstamo de valores
415.03.M.01.03.02	Rendimientos por intereses (cupones) de valores entregados en préstamo
415.03.M.01.03.03	Rendimientos por intereses (premio) del contrato de préstamo de valores
415.03.M.01.05.02	Rendimientos por intereses (cupones) de valores entregados en préstamo
415.03.M.01.05.03	Rendimientos por intereses (premio) del contrato de préstamo de valores
419.01	Rendimientos por depósitos en el Banco Central de la República Dominicana
419.02	Rendimientos por depósitos en entidades de intermediación financiera del país
419.03	Rendimientos por depósitos en entidades financieras del exterior
419.04	Rendimientos por disponibilidades restringidas
Gastos por intereses Gastos de intereses por: depósitos a la vista, de ahorro y a plazo, valores emitidos, financiamientos obtenidos, obligaciones por operaciones de venta de títulos con pacto de recompra.	
511.01	Cargos por depósitos a la vista
511.02	Cargos por depósitos de ahorro
511.03	Cargos por depósitos a plazo
511.04	Cargos por fondos interbancarios
512.01.M.01.01	Cargos por bonos
512.01.M.02.01	Cargos por bonos
512.01.M.03.01	Cargos por bonos
512.01.M.04.01	Cargos por bonos
512.03.M.01.01	Cargos por certificados financieros
512.03.M.02.01	Cargos por certificados financieros
512.03.M.03.01	Cargos por certificados financieros
512.03.M.04.01	Cargos por certificados financieros
512.06.M.01	Cargos por cédulas hipotecarias
512.06.M.02	Cargos por contratos de participación hipotecaria
512.06.M.03	Cargos por valores contrapartida de mutuos endosables

Cuenta	Descripción Manual de Contabilidad
512.06.M.04	Cargos por valores contrapartida de mutuos no endosables
512.06.M.05.01.01.01	Cargos por bonos hipotecarios
512.06.M.05.01.02.01	Cargos por bonos hipotecarios
512.06.M.05.01.03.01	Cargos por bonos hipotecarios
512.06.M.05.01.04.01	Cargos por bonos hipotecarios
512.06.M.05.02.01.01	Cargos por letras hipotecarias
512.06.M.05.02.02.01	Cargos por letras hipotecarias
512.06.M.05.02.03.01	Cargos por letras hipotecarias
512.06.M.05.02.04.01	Cargos por letras hipotecarias
512.07.M.01.01	Cargos por letras
512.07.M.02.01	Cargos por letras
512.07.M.03.01	Cargos por letras
512.07.M.04.01	Cargos por letras
513.01	Cargos por financiamientos del Banco Central de la República Dominicana
513.02	Cargos por obligaciones en venta de títulos con pacto de recompra
513.03	Cargos por financiamientos de entidades financieras del país hasta un año
513.04	Cargos por financiamientos de entidades financieras del país a más de un año
513.05	Cargos por financiamientos de entidades financieras del exterior hasta un año
513.06	Cargos por financiamientos de entidades financieras del exterior a más de un año
513.07	Cargos por otros financiamientos hasta un año
513.08	Cargos por otros financiamientos a más de un año
513.09.M.01	Cargos por obligaciones asimilables de capital
515.03.1.01.01.02	Cargos por intereses (cupones) de valores recibidos en préstamo
515.03.1.01.01.03	Cargos por intereses (premio) del contrato de préstamo de valores
515.03.1.01.02.02	Cargos por intereses (cupones) de valores recibidos en préstamo
515.03.1.01.02.03	Cargos por intereses (premio) del contrato de préstamo de valores
Activos que devengan intereses (partida del balance) • Depósitos en el Banco Central, depósitos en bancos del país, depósitos en el exterior. • Instrumentos de deuda en el país y en el exterior. • Bienes adquiridos para arrendamiento financiero medidos al final de cada ejercicio financiero.	
112	Depósitos en el Banco Central de la República Dominicana (BCRD)
113	Depósitos en entidades de intermediación financiera del país
114	Depósitos en entidades financieras del exterior
117	Disponibilidades restringidas
121	Créditos vigentes
122	Créditos en mora (de 31 a 90 días)
123	Créditos vencidos (más de 90 días)
124	Créditos reestructurados

Cuenta	Descripción Manual de Contabilidad
125	Créditos en cobranza judicial
131	Inversiones a valor razonable con cambios en resultados
132	Inversiones a valor razonable con cambios en el patrimonio
133	Inversiones a costo amortizado
134	Otras inversiones en instrumentos de deuda
176.01	Bienes adquiridos para arrendamiento financiero
183.00	Contratos de préstamo de valores
Ingresos por dividendos Utilidades por dividendos en acciones de inversiones en sociedades no consolidadas en los estados financieros de la entidad, incluyendo ingresos por dividendos de sociedades asociadas y negocios conjuntos.	
433.01	Ganancias por participaciones en el capital de otras sociedades

- **Componente de Servicios (SC)**

Cuenta	Descripción Manual de Contabilidad
Ingresos por comisiones Ingresos recibidos por asesoramientos y servicios. Se excluyen las asociadas a remuneraciones por comercialización de seguros (439.04- Ingresos por gestión de pólizas de seguros).	
423.00	Comisiones por servicios
427.00	Comisiones por servicios fiduciarios
429.01	Comisiones por cartas de crédito
429.02	Comisiones por garantías otorgadas
429.03	Comisiones por líneas de crédito
439.02	Ingresos por servicios de asesoría
Gastos por comisiones Gastos pagados por asesoramiento y servicios. Se excluyen las asociadas a servicios no financieros (por ejemplo, logísticos, informáticos o de recursos humanos).	
523.00	Comisiones por servicios
529.01	Comisiones por líneas de crédito obtenidas
529.02	Comisiones por garantías contratadas
Otros ingresos operacionales Ingresos de operaciones ordinarias no incluidas en otras partidas del indicador de negocios (BI) pero de naturaleza similar. Se excluyen los ingresos de arrendamientos operativos.	
422.02	Rendimientos por títulos recibidos en recuperación de créditos
424.01	Ganancias por cambio de divisas
433.02	Ganancias por venta de participaciones en otras sociedades
434.01	Ganancias por venta de activos fijos
434.02	Ganancias por venta de bienes recibidos en recuperación de créditos
434.04	Ganancias por venta de bienes en fideicomiso
435.00	Disminución de provisiones por activos contingentes
Otros gastos operacionales Gastos y pérdidas de operaciones ordinarias no incluidas en otras partidas del indicador de negocios (BI) pero de naturaleza similar y pérdidas por eventos de riesgo operacional. Se excluyen los gastos de arrendamientos operativos.	
524.01	Pérdidas por cambio de divisas
541.04	Constitución de provisión para bienes recibidos en recuperación de créditos
542.00	Gastos por participaciones en otras sociedades
543.00	Gastos de bienes recibidos en recuperación de créditos
546.00	Gastos por provisiones por activos contingentes
544.01	Pérdida por venta de activos fijos
544.02	Pérdida por venta de bienes en recuperación de créditos
544.03	Pérdidas por venta de bienes entregados en fideicomiso
549.01	Gastos por incobrabilidad de cuentas por cobrar

562.00	Gastos por eventos de pérdidas operacionales
561.04	Constitución de provisión para pasivos contingentes
561.05	Constitución de provisión por eventos de riesgo operacional

- **Componente de Finanzas (FC)**

Cuenta	Descripción Manual de Contabilidad (Estados de Resultados)
Beneficio (pérdida) neto(a) en la cartera de negociación Corresponde al resultado neto (ganancias/pérdidas) de: • Instrumentos financieros para negociación: reajustes, ajuste a valor razonable, utilidad y pérdida por venta y resultado inversiones en fondos mutuos e instrumentos de deuda para negociación. • Utilidad (pérdida) neta de derivados de negociación. • Utilidad (pérdida) de cambio neta por diferencias de cambio de estos instrumentos.	
412.01.M.01.02	Ganancias por cambios en el valor razonable de inversiones con cambios en resultados
412.01.M.02.02	Ganancias por cambios en el valor razonable de inversiones con cambios en resultados
412.01.M.03.02	Ganancias por cambios en el valor razonable de inversiones con cambios en resultados
412.01.M.04.02	Ganancias por cambios en el valor razonable de inversiones con cambios en resultados
412.98.M.01	Diferencia de cambio por inversiones a valor razonable con cambios en resultados
415.01	Ingresos financieros por cambios en el valor razonable de los contratos de compraventa al contado
415.02	Ingresos financieros por cambios en el valor razonable de los derivados
415.03.M.02	Ingresos financieros de obligaciones por contratos de préstamo de valores - Ganancias por cambios en el valor razonable
498.11	Diferencia de cambio por otros pasivos financieros
498.12	Diferencia de cambio por otros activos financieros
515.01	Gastos financieros por cambios en el valor razonable de los contratos de compraventa al contado
515.02	Gastos financieros por cambios en el valor razonable de los derivados
515.03.M.02	Gastos financieros por contratos de préstamo de valores - Pérdidas por cambios en el valor razonable
517.01	Gastos financieros por inversiones a valor razonable con cambios en resultados
598.02.M.01	Diferencia de cambio por inversiones a valor razonable con cambios en resultados
598.07	Diferencia de cambio por otros activos financieros
598.11	Diferencia de cambio por otros pasivos financieros
Beneficio (pérdida) neto(a) en la cartera del libro bancario Corresponde al resultado neto (ganancias/pérdidas) de: • Ingresos por reajustes de la cartera de créditos. • Ingresos por reajustes de instrumentos de inversión y otros ingresos por reajustes ganados.	

Cuenta	Descripción Manual de Contabilidad (Estados de Resultados)
• Gastos por reajustes de: depósitos a la vista, obligaciones por operaciones de venta de títulos con pacto de recompra, depósitos y captaciones a plazo, obligaciones con bancos, instrumentos de deuda emitidos y otras obligaciones financieras. • Utilidad (pérdida) neta de instrumentos disponibles para la venta, venta de cartera de créditos y resultado neto de otras operaciones. • Utilidad (pérdida) de cambio neta por diferencias de cambio de estos instrumentos.	
411.01.M.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.01.M.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.01.M.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.02.M.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.02.M.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.02.M.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.03.M.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.03.M.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.03.M.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.04.M.01.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.04.M.01.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.04.M.01.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.04.M.02.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.04.M.02.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.04.M.02.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.04.M.03.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.04.M.03.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.04.M.03.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.05.M.01.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.05.M.01.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.05.M.01.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.05.M.02.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.05.M.02.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.05.M.02.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda
411.05.M.03.01.02	Ganancias por amortización descuento en compra de créditos comerciales
411.05.M.03.02.02	Ganancias por amortización descuento en compra de créditos de consumo
411.05.M.03.03.02	Ganancias por amortización descuento en compra de créditos hipotecarios para la vivienda

Cuenta	Descripción Manual de Contabilidad (Estados de Resultados)
411.98	Diferencia de cambio por cartera de créditos
412.02.M.01.03	Amortización descuento en compra de inversiones a valor razonable con cambios en el patrimonio
412.02.M.02.03	Amortización descuento en compra de inversiones a valor razonable con cambios en el patrimonio
412.02.M.03.03	Amortización descuento en compra de inversiones a valor razonable con cambios en el patrimonio
412.02.M.04.03	Amortización descuento en compra de inversiones a valor razonable con cambios en el patrimonio
412.03.M.01.03	Amortización descuento en compra de inversiones a costo amortizado
412.03.M.02.03	Amortización descuento en compra de inversiones a costo amortizado
412.03.M.03.03	Amortización descuento en compra de inversiones a costo amortizado
412.03.M.04.03	Amortización descuento en compra de inversiones a costo amortizado
412.98	Diferencia de cambio por inversiones
413.00	Ganancias en venta de cartera de créditos
414.02	Ganancias en venta de inversiones a valor razonable con cambios en el patrimonio
414.03	Ganancias en venta de inversiones a costo amortizado
417.00	Ganancias por amortización prima de valores emitidos
418.00	Ganancias por amortización prima de obligaciones asimilables de capital
498.01	Diferencia de cambio por depósitos del público
498.03	Diferencia de cambio por financiamientos obtenidos
498.05	Diferencia de cambio por obligaciones asimilables de capital
498.07	Diferencia de cambio por obligaciones financieras
511.98	Diferencia de cambio por depósitos del público
512.01.M.01.02	Pérdidas por amortización descuento de bonos
512.01.M.02.02	Pérdidas por amortización descuento de bonos
512.01.M.03.02	Pérdidas por amortización descuento de bonos
512.01.M.04.02	Pérdidas por amortización descuento de bonos
512.03.M.01.02	Pérdidas por amortización descuento de certificados financieros
512.03.M.02.02	Pérdidas por amortización descuento de certificados financieros
512.03.M.03.02	Pérdidas por amortización descuento de certificados financieros
512.03.M.04.02	Pérdidas por amortización descuento de certificados financieros
512.06.M.05.01.01.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.01.02.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.01.03.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.01.04.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.02.01.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.02.02.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.02.03.02	Pérdidas por amortización descuento de bonos hipotecarios
512.06.M.05.02.04.02	Pérdidas por amortización descuento de bonos hipotecarios

Cuenta	Descripción Manual de Contabilidad (Estados de Resultados)
513.09.M.02	Pérdidas por amortización descuento de obligaciones asimilables de capital
513.98	Diferencia de cambio por financiamientos obtenidos
514.00	Pérdidas por amortización prima en compra de cartera de créditos
517.02	Gastos financieros por inversiones a valor razonable con cambios en el patrimonio
517.03	Gastos financieros por inversiones a costo amortizado
518.00	Pérdidas en venta de cartera de créditos
519.02	Pérdidas en venta de inversiones a valor razonable con cambios en el patrimonio
519.03	Pérdidas en venta de inversiones a costo amortizado
529.04	Amortización costo emisión de obligaciones subordinadas
529.05	Amortización costo emisión de obligaciones convertibles en capital
549.07	Pérdidas por deterioro de inversiones a valor razonable con cambios en el patrimonio
598.01	Diferencia de cambio por cartera de créditos
598.02.M.02	Diferencia de cambio por inversiones a valor razonable con cambios en el patrimonio
598.02.M.03	Diferencia de cambio por inversiones a costo amortizado
598.02.M.04	Diferencia de cambio por otras inversiones en instrumentos de deuda
598.08	Diferencia de cambio por obligaciones financieras

Documento firmado digitalmente por:
Stephanie Cristina Hernandez Tejeda (VB) (13/11/2026 VET), José Guillermo López (VB) (13/11/2026 VET)
Mirna Midian García Santana (En nombre de Olimpia Gonzalez Matos) (VB) (13/11/2026 VET)
Yulianna Marie Ramon Martinez (VB) (13/11/2026 VET), Enmanuel Cedeño Brea (13/11/2026 VET)
https://www.viafirma.com.do/inbox/app/sib/v/b1d5eadc-aa94-4f00-9323-a4e9a77f55ac