

**Pontificia Universidad Católica Madre y Maestra
Vicerrectoría Académica
Decanato de Postgrado**



**Trabajo Final para optar por el título de
Magister en Gestión Financiera y Bancaria**

**Diagnóstico del riesgo operacional en la banca dominicana: fraude, ciberseguridad y
continuidad del negocio.**

Sustentante(s):

Jesús Ismael Díaz Madera (10148390)

Francheco de los Santos (10162396)

Santo Domingo

Abril, 2026.



**Pontificia Universidad Católica Madre y Maestra
Vicerrectoría Académica
Decanato de Postgrado**

Formulario de Cesión Derechos de Autor al Repositorio Institucional Investigare

Este documento establece los derechos que usted otorga relacionados a la publicación de su trabajo académico, mediante su inclusión en el *repositorio del sistema de biblioteca de esta institución (PUCMM)*. No habrá ningún pago para usted por esta publicación y por el otorgamiento de los derechos de esta.

Usted confirma que

Este trabajo académico es original propio que no infringe los derechos de autor de otros; en caso de no ser un trabajo completamente original, declara que tiene los permisos necesarios por escrito de este otorgamiento por parte de demás autores.

El contenido de este trabajo académico no contiene ningún material que sea difamatorio, viole los derechos de privacidad, o revele la información confidencial.

Este trabajo académico no se ha publicado en parte o en su totalidad, y usted no publicara este trabajo académico en ningún otro lugar sin el consentimiento del repositorio institucional.

Este trabajo académico se ha conducido respetando los principios éticos establecidos por la institución.

Usted otorga los derechos de autor de este trabajo académico al repositorio institucional (PUCMM), a nivel mundial, de manera perpetua y sin pagos; y en la medida requerida por los términos de este acuerdo. Conservara en todo momento el derecho a ser reconocido como el autor del trabajo académico. Además, acepta que el repositorio de la PUCMM tiene el derecho de tratar este trabajo académico como se considere oportuno (por ejemplo, derecho a imprimir, publicar, comercializar, comunicar y distribuir en todos los medios, editar la forma del trabajo, registrar los derechos de autor, cumplir con la política editorial establecida por el repositorio, entre otros).

He leído, entiendo y acepto los términos anteriores.

Nombre del Programa: Maestría en Gestión Bancaria y Financiera

Título del Trabajo: Diagnóstico del riesgo operacional en la banca dominicana: fraude, ciberseguridad y continuidad del negocio

Nombre (s) y Apellidos: Jesús Ismael Diaz Madera

Matrícula: 10148390

Cédula de Identidad y Electoral: 001-1785509-8

Fecha (día, mes, año): 26/03/2026

Firma

Jesús I. Diaz

Nombre (s) y Apellidos: Franchesco de los Santos Veras

Matrícula: 10162396

Cédula de Identidad y Electoral: 001-1941916-6

Fecha (día, mes, año): 26/03/2026

Firma

Franchesco de los Santos

Contenido

Resumen ejecutivo	vi
Introducción	1
1.1 Antecedentes del problema.....	1
1.2 Descripción del problema	2
1.3 Preguntas de investigación	2
1.4 Objetivo general.....	3
1.5 Objetivos específicos	3
1.6 Justificación de la investigación	4
1.7 Limitaciones y delimitaciones de la investigación	4
Marco Teórico y Conceptual	5
2.1 Definición y alcance del riesgo operacional.....	5
2.2 Evolución del riesgo operacional en el sistema financiero.....	6
2.3 Fraude y riesgo operacional.....	7
2.4 Riesgo operacional y ciberseguridad	8
2.5 Continuidad del negocio y resiliencia operativa	8
2.6 Gestión del riesgo operacional en la República Dominicana.....	9
2.7 Modelos y metodologías de valoración del riesgo operacional	10
Metodología.....	10
3.1 Diseño, enfoque, alcance y tipo de investigación.....	11
3.2 Población y muestra.....	13
3.3 Instrumentos de recolección, análisis y medición de datos.....	14

3.4 Operacionalización de las variables	17
3.5 Consideraciones éticas	18
Resultados del Estudio.....	19
4.1 Evolución del riesgo operacional en el sistema bancario dominicano	19
4.2 Transformación estructural del riesgo operacional a nivel internacional	21
4.3 Fraude: análisis comparativo internacional y República Dominicana	22
4.4 Ciberseguridad y resiliencia tecnológica	23
4.5 Continuidad del negocio y resiliencia operativa.....	24
Conclusiones y Discusión.....	25
5.1 Síntesis general de la investigación	25
5.2 Limitaciones del estudio	26
5.3 Alternativas estratégicas para fortalecer la resiliencia operativa	27
5.4 Estrategia recomendada para el sistema bancario dominicano	28
Bibliografía.....	31
Anexos.....	33
Entrevista 1.....	33
Entrevista 2.....	36
Verificación Anti-Plagio.....	38
Certificado Citi Program Jesús Díaz	39
Certificado Citi Program Franchesco de los Santos	39

Resumen ejecutivo

La presente investigación aplicada analiza las brechas existentes en la gestión del riesgo operacional en la banca dominicana, con énfasis en tres dimensiones críticas: fraude, ciberseguridad y continuidad del negocio. En un entorno caracterizado por la digitalización acelerada de los servicios financieros y el aumento de amenazas tecnológicas, la gestión del riesgo operacional se ha convertido en un componente fundamental para la estabilidad del sistema financiero y la continuidad de las operaciones bancarias.

El estudio se desarrolló mediante revisión documental y análisis comparativo de marcos regulatorios, estándares internacionales, literatura especializada y estadísticas del sistema financiero dominicano.

Los resultados evidencian una tendencia creciente en las pérdidas operacionales del sistema bancario dominicano, así como una alta concentración de estas pérdidas en eventos de fraude externo.

El análisis comparativo también muestra que, aunque el sistema financiero dominicano ha avanzado en la formalización normativa mediante la implementación del Sistema de Administración del Riesgo Operacional (SARO) y el fortalecimiento de la supervisión basada en riesgos, persisten brechas en la madurez tecnológica, en la adopción de herramientas analíticas avanzadas y en la integración de modelos de resiliencia operativa.

En este contexto, la investigación concluye que la adopción progresiva de un enfoque integral de resiliencia operativa, alineado con estándares internacionales, podría contribuir a fortalecer la capacidad del sistema bancario dominicano para enfrentar eventos operacionales y preservar la estabilidad del sistema financiero.

Introducción

1.1 Antecedentes del problema

El riesgo operacional ha adquirido una relevancia creciente en el sector financiero global, especialmente en contextos de alta digitalización. Según el Comité de Basilea, este tipo de riesgo se refiere a pérdidas derivadas de fallos en procesos internos, errores humanos, deficiencias tecnológicas o eventos externos. A diferencia de los riesgos de crédito o mercado, el riesgo operacional es transversal y puede afectar cualquier área de una institución financiera.

En los últimos años, el auge de las transacciones digitales ha incrementado la exposición a fraudes electrónicos, ciberataques y fallas en infraestructuras críticas. Informes de firmas como KPMG (2022) y Deloitte (2023) evidencian un aumento sostenido de incidentes de ransomware y phishing en la banca internacional. Asimismo, eventos disruptivos como pandemias y desastres naturales han resaltado la importancia de contar con planes robustos de continuidad del negocio.

En República Dominicana, el sistema financiero ha experimentado una modernización acelerada, lo que ha ampliado la superficie de exposición a riesgos operacionales, especialmente los relacionados a fraude.

Información estadística publicada en el Sistema de Información del Mercado Bancario Dominicano (SIMBAD) indica que el 62% de las pérdidas operacionales del sector corresponden a eventos de fraude externo.

La Superintendencia de Bancos ha respondido a esto con regulaciones que exigen políticas formales de gestión del riesgo, notificación de incidentes y pruebas de continuidad, alineadas con los estándares de Basilea III.

1.2 Descripción del problema

El sector bancario dominicano enfrenta desafíos importantes en la gestión del riesgo operacional, particularmente en las áreas de fraude, ciberseguridad y continuidad del negocio. Aunque existen normativas locales y marcos de referencia internacionales, aún no se cuenta con un diagnóstico integral que permita identificar brechas en la implementación, monitoreo y adaptación de estas prácticas frente a los riesgos emergentes. Esta ausencia de evaluación genera opacidad respecto a la efectividad real de los controles y mecanismos actualmente utilizados por las entidades financieras.

La evidencia proveniente de mercados financieros más desarrollados muestra avances significativos en la reducción de incidentes de fraude y ciberataques, derivados de la adopción de prácticas más consolidadas y de una actualización continua en la gestión del riesgo operacional (Bank for International Settlements, 2023; International Monetary Fund, 2022; World Bank, 2021). Al contrastar estas tendencias con el contexto dominicano, se identifican diferencias relevantes en el grado de madurez de los controles, la incorporación de estándares internacionales y la capacidad de respuesta ante amenazas emergentes.

Estas brechas sugieren la necesidad de fortalecer la resiliencia operativa del sector mediante la alineación con marcos globales más robustos y mecanismos de monitoreo más efectivos.

1.3 Preguntas de investigación

- ¿Cuáles son las brechas actuales en la gestión del riesgo operacional en la banca dominicana en las áreas de fraude, ciberseguridad y continuidad del negocio?
- ¿Cuáles son las prácticas internacionales más actualizadas y efectivas en la gestión del riesgo operacional para estas tres áreas en mercados financieros desarrollados?

- ¿Qué evidencia existe sobre la relación entre la adopción de estándares internacionales de riesgo operacional y la reducción de incidentes de fraude y ciberataques en dichos mercados?
- ¿Qué elementos de estas prácticas internacionales podrían ser adoptados para fortalecer la resiliencia operativa del sistema bancario dominicano?

1.4 Objetivo general

Analizar las brechas actuales en la gestión del riesgo operacional en la banca dominicana, específicamente en fraude, ciberseguridad y continuidad del negocio, y contrastarlas con las mejores prácticas internacionales, con el fin de analizar su relación con la reducción de incidentes operacionales y formular recomendaciones que fortalezcan la resiliencia operativa del sistema financiero dominicano.

1.5 Objetivos específicos

- Identificar las brechas existentes en la gestión del riesgo operacional en fraude, ciberseguridad y continuidad del negocio dentro del sistema bancario dominicano.
- Sistematizar las mejores prácticas y estándares internacionales actuales en la gestión del riesgo operacional aplicados en mercados financieros desarrollados.
- Comparar las tendencias de evolución del riesgo operacional y la efectividad de los controles en mercados desarrollados frente al contexto dominicano.
- Analizar la influencia que tiene la adopción de prácticas y estándares internacionales en la reducción de incidentes de fraude y ciberataques.
- Proponer recomendaciones estratégicas que contribuyan al fortalecimiento de la resiliencia operativa del sistema bancario dominicano, alineadas con los marcos internacionales más robustos.

1.6 Justificación de la investigación

La creciente complejidad del entorno financiero global, marcada por el incremento de incidentes de fraude, ataques cibernéticos y fallas operativas, ha llevado a organismos internacionales a resaltar la importancia de marcos robustos de gestión del riesgo operacional como requisito para la estabilidad del sistema financiero (Bank for International Settlements, 2023). En este contexto, la banca dominicana enfrenta desafíos asociados a brechas en la implementación y actualización de prácticas vinculadas a fraude, ciberseguridad y continuidad del negocio, lo que limita su capacidad de respuesta ante riesgos emergentes. Esto se refleja en estadísticas de la Superintendencia de Bancos (SIMBAD), donde el mayor porcentaje de pérdidas operacionales se deben a eventos de fraude externo.

Los mercados financieros más desarrollados han logrado avances significativos mediante la adopción de estándares internacionales y mecanismos de monitoreo continuo, los cuales han demostrado reducir la frecuencia e impacto de incidentes operacionales (International Monetary Fund, 2022). Analizar estas experiencias resulta fundamental para identificar prácticas aplicables al contexto dominicano. La presente investigación se justifica en su potencial para ofrecer un diagnóstico comparativo sólido y derivar recomendaciones estratégicas que contribuyan al fortalecimiento de la resiliencia operativa de las entidades bancarias nacionales, beneficiando a reguladores, instituciones financieras y profesionales del sector.

1.7 Limitaciones y delimitaciones de la investigación

Limitaciones:

- Acceso limitado a datos cuantitativos sobre incidentes operacionales en mercados desarrollados.
- Variabilidad en la disponibilidad y profundidad de información pública entre países.
- Dificultad para establecer causalidad directa entre adopción de prácticas y reducción de incidentes.

Propuesta para afrontarlas:

Se utilizarán fuentes secundarias confiables (informes de organismos internacionales, literatura académica, estudios de consultoras globales) y se aplicará un enfoque cualitativo-comparativo que permita extraer patrones y tendencias relevantes.

Delimitaciones:

- **Temática:** Gestión del riesgo operacional en banca, con énfasis en fraude, ciberseguridad y continuidad del negocio.
- **Enfoque:** Comparativo, centrado en mercados financieros desarrollados vs. mercado dominicano
- **Espacio:** Mercados internacionales; y su aplicación contextual a República Dominicana.
- **Tiempo:** Análisis de tendencias y prácticas entre 2020 y 2025.
- **Metodología:** Revisión documental, análisis comparativo de literatura técnica y regulatoria, utilizando métodos cualitativos y cuantitativos para analizar la evolución del riesgo operacional en mercados financieros desarrollados y su relación con la adopción de mejores prácticas internacionales.
- **Población:** Sistemas bancarios de referencia internacional como fuentes de mejores prácticas y el sistema bancario dominicano.

Marco Teórico y Conceptual

2.1 Definición y alcance del riesgo operacional

El riesgo operacional constituye un eje fundamental dentro de la gestión integral de riesgos en el sector financiero y se reconoce hoy como un pilar de la estabilidad bancaria global. El Basel Committee on Banking Supervision (BCBS, 2011) lo define como el riesgo de pérdida derivado de procesos internos inadecuados o fallidos, fallas humanas, deficiencias en sistemas o eventos externos. La definición incluye los riesgos legales, pero excluye los riesgos estratégicos y

reputacionales, pese a que estos pueden verse afectados de manera indirecta por incidentes operacionales.

Este riesgo tiene un carácter transversal, pues permea todas las áreas de una institución financiera. La Federal Deposit Insurance Corporation (FDIC, 2023) señala que puede materializarse por errores humanos, fraudes internos o externos, ciberataques, fallas tecnológicas, interrupciones operativas o deficiencias culturales dentro de la organización. A diferencia del riesgo de crédito o de mercado, su origen radica en la estructura interna de la operación, lo que demanda controles internos sólidos, monitoreo continuo, capacitación del personal y tecnologías de prevención.

En la República Dominicana, la Superintendencia de Bancos (SIB, 2023) ha incorporado los lineamientos de Basilea III mediante la implementación del Sistema de Administración del Riesgo Operacional (SARO). Este exige políticas, metodologías y procedimientos para la identificación, evaluación, control y monitoreo del riesgo. La gestión moderna exige una visión integral que articule cultura de riesgo, ciberseguridad, resiliencia y continuidad del negocio, alineada con estándares internacionales como la ISO 31000:2018.

2.2 Evolución del riesgo operacional en el sistema financiero

El reconocimiento formal del riesgo operacional en la regulación bancaria se consolidó con Basilea II (2004), donde se incorporó como un tercer pilar junto al riesgo de mercado y crédito. En este marco se introdujeron tres metodologías de cálculo de capital: el Basic Indicator Approach (BIA), el Standardized Approach (TSA) y el Advanced Measurement Approach (AMA). Posteriormente, Basilea III (2010–2021) amplió el enfoque regulatorio e incorporó mayores exigencias en materia de capital y liquidez, consolidando la resiliencia financiera (Deloitte, 2023).

En 2023, el BCBS publicó el Standardized Measurement Approach (SMA), que reemplaza los modelos anteriores con una metodología más homogénea y basada en datos internos de pérdidas

y exposición (KPMG, 2022). El objetivo es mejorar la comparabilidad entre jurisdicciones, promover una cultura de datos más madura y simplificar la evaluación del riesgo.

En República Dominicana, la SIB ha adoptado estos lineamientos dentro del enfoque SARO y del modelo de Supervisión Basada en Riesgos. Los bancos dominicanos han avanzado hacia la digitalización y automatización del monitoreo, empleando auditorías de procesos, tableros de riesgo y análisis predictivos. Esto marca la transición de un enfoque meramente regulatorio hacia una gestión estratégica y proactiva del riesgo operacional, alineada con Basilea III, la ISO 31000:2018 y las exigencias tecnológicas actuales.

2.3 Fraude y riesgo operacional

El fraude, tanto en su modalidad interna como externa, figura entre las principales causas de pérdidas operativas a nivel mundial. KPMG (2022) y PwC (2023) indican que los fraudes digitales, el uso indebido de credenciales y los errores humanos representan más del 60 % de los eventos operativos reportados globalmente, tendencia que se incrementa con la digitalización de los servicios bancarios.

El Basel Committee (2011) establece que una gestión antifraude eficaz requiere un ambiente de control robusto, mecanismos de prevención, canales de denuncia, análisis de datos y una supervisión activa del gobierno corporativo. La norma ISO 37001:2016 complementa este enfoque mediante directrices para prevenir, detectar y responder ante actos de soborno o fraude dentro de las organizaciones.

En República Dominicana, la SIB exige políticas antifraude integrales, controles automatizados, monitoreo transaccional, fortalecimiento de procesos de “conozca a su cliente” (KYC) y capacitación constante del personal. La integración de estos elementos reduce la frecuencia y

severidad de los incidentes, fortalece la confianza del público y refuerza la gestión institucional del riesgo.

2.4 Riesgo operacional y ciberseguridad

La ciberseguridad se ha convertido en uno de los dominios más críticos del riesgo operacional contemporáneo. El BCBS (2021) reconoce que ataques de denegación de servicio, filtraciones de datos e interrupciones tecnológicas representan amenazas significativas para la estabilidad financiera global. En este contexto, la ciber resiliencia, entendida como la capacidad de resistir, adaptarse y recuperarse ante incidentes cibernéticos, se ha integrado como un atributo estratégico de la banca moderna (Ernst & Young, 2024).

Las normas ISO/IEC 27001:2022 y 27002:2022 proporcionan el marco internacional para implementar Sistemas de Gestión de Seguridad de la Información (SGSI), abarcando gestión de accesos, protección de datos, criptografía, continuidad tecnológica y respuesta ante incidentes. Por su parte, el NIST Cybersecurity Framework 2.0 (2023) estructura la seguridad en cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar.

En República Dominicana, la Circular SB-REG-202300014 (SIB, 2024) obliga a las entidades de intermediación financiera a establecer políticas robustas de seguridad tecnológica, ejecutar pruebas de penetración, garantizar la trazabilidad de los eventos y proteger los datos personales. Con ello, la ciberseguridad se consolida como un componente estructural del SARO y un indicador clave de madurez operativa.

2.5 Continuidad del negocio y resiliencia operativa

La continuidad del negocio constituye un elemento fundamental de la resiliencia organizacional frente a eventos disruptivos. La ISO 22301:2019 define los requisitos para un Sistema de Gestión de Continuidad del Negocio (SGCN) que permita a las organizaciones mantener sus operaciones

críticas durante interrupciones significativas. Este estándar exige la realización de análisis de impacto al negocio (BIA), planes de contingencia, estrategias de recuperación, comunicaciones en crisis y evaluación continua mediante auditorías y simulacros.

La norma ISO 22313:2020 provee lineamientos para la implementación del SGCN, mientras que la ISO 22317:2021 profundiza en las metodologías de análisis de impacto. En el sector financiero, estos estándares se integran con los Principles for Operational Resilience del BCBS (2021), que recomiendan fortalecer la continuidad operativa y tecnológica dentro del marco del riesgo operacional.

En República Dominicana, la SIB (2023) exige planes actualizados de continuidad y recuperación tecnológica (BCP y DRP), así como pruebas periódicas de validación. Esto no solo reduce pérdidas económicas potenciales, sino que fortalece la estabilidad del sistema y la confianza del público.

2.6 Gestión del riesgo operacional en la República Dominicana

El marco normativo dominicano para la gestión del riesgo operacional se fundamenta en la Resolución de la Junta Monetaria (2009), que formalizó los lineamientos del SARO. Posteriormente, la SIB adoptó el enfoque de Supervisión Basada en Riesgos (SBR), alineado con las recomendaciones de Basilea III y centrado en evaluar la gestión según el nivel de exposición, complejidad y perfil de riesgo de cada entidad.

El Informe Anual de Riesgo Operacional (SIB, 2024) destaca avances en automatización de reportes de incidentes, estandarización de matrices de riesgo y fortalecimiento de la capacitación técnica. Sin embargo, persisten desafíos importantes, incluyendo la integración de plataformas tecnológicas, la consolidación de una cultura de riesgo y la madurez de los modelos de análisis.

Para cerrar estas brechas, la SIB ha promovido la adopción de marcos complementarios como ISO 22301, ISO 31000 e ISO/IEC 27001. Esto impulsa un modelo de supervisión más integral, donde

el riesgo operacional se articula con la gobernanza, la continuidad del negocio y la protección tecnológica.

2.7 Modelos y metodologías de valoración del riesgo operacional

La evaluación del riesgo operacional combina enfoques cualitativos y cuantitativos que permiten identificar vulnerabilidades, evaluar controles y priorizar riesgos.

Los modelos cuantitativos, influenciados por Basilea II y reforzados en Basilea III, emplean datos históricos para estimar frecuencia y severidad de eventos. El enfoque SMA incorpora el Internal Loss Multiplier (ILM), que vincula las pérdidas históricas con los ingresos operativos de la entidad (KPMG, 2022), permitiendo calcular el capital requerido frente al riesgo operacional.

En la práctica dominicana, los bancos de mayor tamaño utilizan modelos híbridos que incluyen análisis de escenarios, datos internos, simulaciones y proyecciones financieras. Esto se alinea con la ISO 31010:2019, que recomienda técnicas de evaluación como el análisis Monte Carlo, diagramas causa-efecto y matrices de probabilidad-impacto. La adopción de estos modelos mejora la calidad de la información reportada a la SIB y fortalece la transparencia institucional.

Metodología

La metodología constituye una fase esencial del proceso investigativo, ya que establece el conjunto de procedimientos, técnicas y métodos utilizados para dar respuesta al problema de investigación planteado. En esta sección se describe de manera detallada cómo se condujo la investigación, permitiendo al lector evaluar la pertinencia del diseño metodológico, así como la validez, confiabilidad y rigor científico de los resultados obtenidos.

El presente estudio se orienta al análisis del riesgo operacional en la banca dominicana, con énfasis en fraude, ciberseguridad y continuidad del negocio, mediante un enfoque comparativo con las

mejores prácticas internacionales. En coherencia con los objetivos planteados, se adopta una metodología que combina técnicas cualitativas y cuantitativas, sustentadas principalmente en el análisis documental y en la recopilación de información de fuentes secundarias especializadas.

3.1 Diseño, enfoque, alcance y tipo de investigación

Diseño de la investigación

El diseño de la investigación es no experimental, dado que no se manipulan deliberadamente las variables objeto de estudio ni se interviene directamente en el entorno de las entidades financieras analizadas. Las variables relacionadas con el riesgo operacional, fraude, ciberseguridad y continuidad del negocio se observan tal como se manifiestan en la realidad, a partir de información histórica, normativa y documental.

Este tipo de diseño resulta adecuado para estudios que buscan analizar fenómenos complejos dentro de su contexto real, especialmente cuando las condiciones éticas, regulatorias y prácticas impiden la experimentación directa, como ocurre en el sector financiero.

Tipo de investigación

Desde la perspectiva temporal, la investigación es de tipo transversal, ya que analiza la situación del riesgo operacional en un periodo determinado, comprendido entre los años 2020 y 2025, intervalo en el cual se concentran los datos cuantitativos utilizados para dimensionar la magnitud e impacto de los eventos operacionales.

No obstante, el análisis documental y comparativo incorpora marcos normativos, estándares internacionales y literatura especializada que pueden ser anteriores a dicho periodo, en la medida en que resultan necesarios para comprender la evolución histórica del riesgo operacional, el desarrollo de las mejores prácticas internacionales y su influencia en los modelos actuales de gestión.

En este sentido, aunque el estudio no persigue un seguimiento longitudinal de las variables, sí identifica tendencias, brechas y patrones relevantes, apoyándose en una base documental más amplia que contextualiza los hallazgos dentro de una perspectiva evolutiva y comparativa.

Enfoque metodológico

El estudio adopta un enfoque mixto, con predominio cualitativo y apoyo cuantitativo:

- Enfoque cualitativo: se utiliza para analizar marcos normativos, estándares internacionales, regulaciones locales, informes técnicos y literatura académica, permitiendo comprender en profundidad la evolución, estructura y madurez de la gestión del riesgo operacional.
- Enfoque cuantitativo: se emplea de manera complementaria mediante el análisis de datos secundarios, tales como estadísticas de pérdidas operacionales, reportes regulatorios y estudios sectoriales, que permiten dimensionar la magnitud e impacto de los riesgos analizados.

La combinación de ambos enfoques fortalece la robustez del análisis, al integrar la interpretación conceptual con evidencia empírica documentada.

Alcance de la investigación

El alcance del estudio es descriptivo y comparativo:

- Descriptivo, porque caracteriza el estado actual de la gestión del riesgo operacional en la banca dominicana, identificando sus principales componentes, prácticas, marcos regulatorios y niveles de madurez.
- Comparativo, porque contrasta dichas prácticas con estándares y experiencias de mercados financieros desarrollados, permitiendo identificar brechas y oportunidades de mejora.

No se pretende establecer relaciones causales directas, sino analizar asociaciones y tendencias que sirvan de base para formular recomendaciones estratégicas.

3.2 Población y muestra

Población de estudio

La población de la investigación está conformada por:

- El sistema bancario dominicano, en particular las entidades de intermediación financiera reguladas por la Superintendencia de Bancos de la República Dominicana.
- Sistemas bancarios de referencia internacional, principalmente de economías con mercados financieros desarrollados, cuyos marcos regulatorios y prácticas son considerados referentes en la gestión del riesgo operacional.
- Documentos normativos, informes técnicos y estudios especializados emitidos por organismos internacionales, firmas consultoras, entes reguladores y asociaciones financieras.

Dado el carácter no experimental y documental del estudio, la población no se define en términos de individuos, sino de fuentes de información relevantes y confiables.

Muestra

La muestra es de tipo no probabilística e intencional, seleccionada en función de criterios de pertinencia, actualidad, relevancia técnica y reconocimiento institucional. Se incluyen:

- Informes y publicaciones del Comité de Basilea, el Banco de Pagos Internacionales, el Fondo Monetario Internacional y el Banco Mundial.

- Normativas y circulares emitidas por la Superintendencia de Bancos de la República Dominicana.
- Estándares internacionales ISO relacionados con gestión de riesgos, ciberseguridad y continuidad del negocio.
- Estudios y reportes de firmas consultoras internacionales especializadas en riesgo financiero.
- Estadísticas oficiales sobre pérdidas operacionales y eventos de fraude publicadas en el SIMBAD.

Adicionalmente, se incorporó una muestra de expertos del sector financiero dominicano con experiencia en gestión del riesgo operacional, fraude y ciberseguridad. La selección de los participantes se realizó mediante un muestreo no probabilístico por criterio experto, considerando su conocimiento técnico y experiencia profesional en áreas relacionadas con la gestión de riesgos en entidades financieras.

3.3 Instrumentos de recolección, análisis y medición de datos

Instrumentos de recolección de datos

Para el logro de los objetivos de la investigación se utilizaron los siguientes instrumentos:

- Análisis documental: principal instrumento del estudio, aplicado a normativas, estándares, informes técnicos, literatura académica y reportes estadísticos. Este instrumento resulta pertinente al enfoque cualitativo y al alcance descriptivo–comparativo de la investigación.
- Revisión de bases de datos secundarias: se emplearon estadísticas oficiales y reportes públicos sobre pérdidas operacionales, fraude y eventos de riesgo, permitiendo un análisis cuantitativo complementario.
- Entrevistas semiestructuradas: se realizaron entrevistas a 3 expertos del sector financiero dominicano, con el objetivo de complementar y validar los hallazgos obtenidos mediante

el análisis documental. Las entrevistas incluyeron preguntas abiertas orientadas a identificar percepciones sobre fraude, ciberseguridad, continuidad del negocio y madurez en la gestión del riesgo operacional.

Validez y confiabilidad de los instrumentos

La validez de los instrumentos se garantizó mediante:

- Validez de contenido, asegurando que los instrumentos cubrieran de manera adecuada las dimensiones del riesgo operacional definidas en los objetivos de la investigación.
- Uso de fuentes reconocidas y oficiales, lo que reduce sesgos y aumenta la credibilidad de la información.
- Triangulación de fuentes, contrastando información normativa, académica y estadística.

Técnicas de análisis de datos

Los datos cualitativos fueron analizados mediante técnicas de análisis de contenido, identificando categorías temáticas relacionadas con fraude, ciberseguridad, continuidad del negocio y resiliencia operativa. Los datos cuantitativos secundarios fueron analizados mediante estadística descriptiva simple, permitiendo identificar tendencias y magnitudes relevantes.

3.4 Operacionalización de las variables

Objetivo específico	Variable	Definición	Indicadores	Qué mide el indicador	Fuente
Identificar brechas en la gestión del riesgo operacional	Nivel de madurez de la gestión del riesgo operacional	Grado en que las instituciones implementan controles, políticas y herramientas para gestionar el riesgo operacional	Proporción de pérdidas por fraude externo	Nivel de exposición del sistema financiero a eventos de fraude	SIMBAD / SIB
			Nivel de adopción de controles bajo SARO	Grado de implementación del marco regulatorio dominicano	SIB
			Existencia de programas de ciberseguridad y continuidad	Nivel de preparación institucional frente a eventos operacionales	Regulaciones SIB
Sistematizar mejores prácticas internacionales	Estándares internacionales	Conjunto de marcos regulatorios globales de gestión de riesgo operacional	Basilea III	Uso de estándares prudenciales internacionales	BIS
			ISO 27001	Gestión formal de seguridad de la información	ISO
			NIST Cybersecurity Framework	Capacidad de gestión estructurada de ciberseguridad	NIST
Comparar tendencias internacionales	Evolución del riesgo operacional	Comportamiento de pérdidas operacionales en distintos sistemas financieros	Evolución de pérdidas operacionales	Tendencia en frecuencia y severidad de eventos	BIS / SIB
			Distribución por tipo de evento	Concentración del riesgo operacional	BCBS
Analizar la influencia de estándares	Impacto de prácticas internacionales	Efectos potenciales de herramientas avanzadas de gestión de riesgo	Uso de analítica avanzada	Capacidad de detección temprana de fraude	Deloitte
Proponer recomendaciones	Resiliencia operativa	Capacidad del sistema financiero para resistir y recuperarse de eventos operacionales	Integración de riesgo tecnológico y operacional	Nivel de coordinación institucional	Literatura

3.5 Consideraciones éticas

La investigación se desarrolló respetando los principios éticos establecidos por la Pontificia Universidad Católica Madre y Maestra. La información utilizada proviene principalmente de fuentes secundarias públicas y documentos oficiales, lo que minimiza riesgos éticos.

La metodología adoptada resulta coherente con los objetivos de la investigación y con la naturaleza del problema estudiado, permitiendo realizar un diagnóstico comparativo sólido sobre la gestión del riesgo operacional en la banca dominicana y su alineación con las mejores prácticas internacionales.

En el caso de las entrevistas realizadas, se garantizó el uso responsable de la información, limitando su utilización exclusivamente a fines académicos. Las respuestas fueron analizadas de manera agregada, evitando la identificación directa de los participantes.

Resultados del Estudio

4.1 Evolución del riesgo operacional en el sistema bancario dominicano

El análisis del riesgo operacional en el sistema financiero dominicano permite observar la evolución reciente de las pérdidas asociadas a eventos operacionales y su comportamiento a lo largo del tiempo. En los últimos años, la creciente digitalización de los servicios financieros ha transformado la forma en que las instituciones bancarias operan, generando nuevas oportunidades de eficiencia operativa, pero también ampliando la exposición a eventos de riesgo operacional.

Para este análisis se utilizaron estadísticas publicadas por la Superintendencia de Bancos de la República Dominicana y datos agregados del Sistema de Información del Mercado Bancario Dominicano (SIMBAD).

Durante el período analizado se observa una tendencia general creciente, aunque con fluctuaciones interanuales en algunos años en las pérdidas operacionales del sistema bancario dominicano. Las pérdidas brutas pasaron de aproximadamente RD\$739 millones en 2018 a valores superiores a RD\$2,700 millones en 2024, lo que evidencia un incremento significativo en la materialización de eventos de riesgo operacional dentro del sistema financiero.

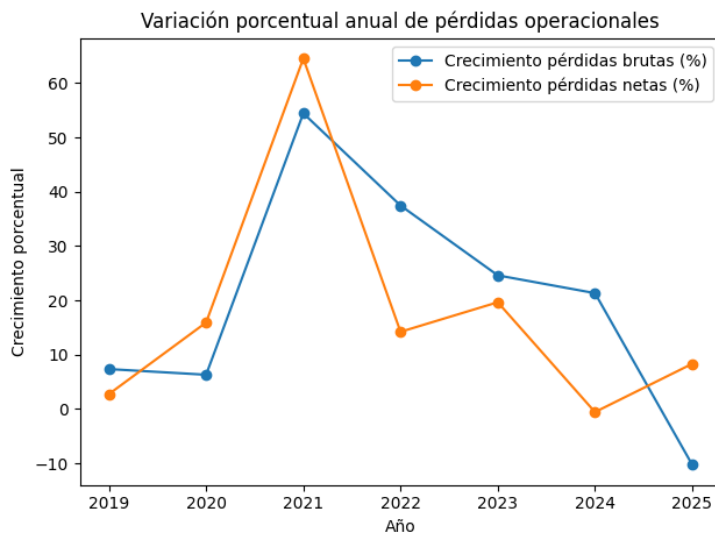


Figura 1

Variación porcentual anual de pérdidas operacionales en el sistema bancario dominicano.

Fuente: Elaboración propia con base en datos de la Superintendencia de Bancos de la República Dominicana (SIMBAD).

El análisis de la variación porcentual anual muestra que el crecimiento de las pérdidas operacionales no ha sido uniforme a lo largo del período analizado. En particular, se observa

un incremento significativo entre los años 2020 y 2021, período en el cual las pérdidas brutas crecieron aproximadamente un 54% y las pérdidas netas cerca de un 64%.

Posteriormente, aunque las pérdidas operacionales continúan creciendo, se observa una moderación gradual en las tasas de crecimiento. Durante el período 2022–2024 las tasas de incremento se mantienen positivas, aunque con menor intensidad en comparación con el crecimiento observado en 2021.

Este comportamiento sugiere que, si bien el sistema financiero dominicano continúa experimentando una mayor exposición al riesgo operacional, las instituciones financieras han comenzado a fortalecer progresivamente sus mecanismos de control y gestión del riesgo.

Además del análisis de la evolución de las pérdidas en términos absolutos, resulta relevante evaluar la intensidad del riesgo operacional en relación con la capacidad de generación de ingresos del sistema financiero.

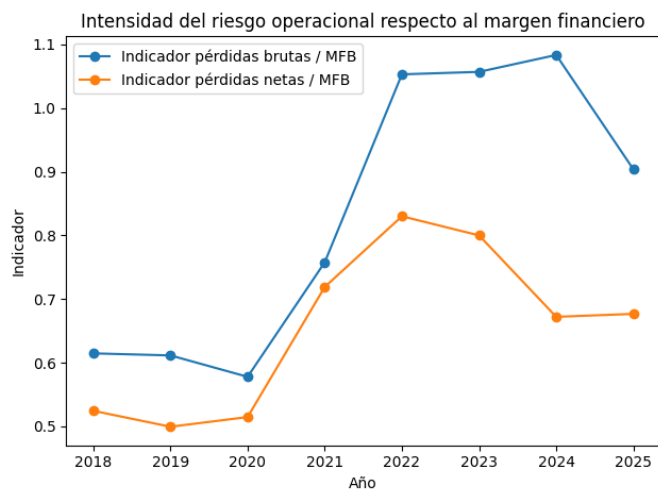


Figura 2

Intensidad del riesgo operacional respecto al margen financiero bruto.

Fuente: Elaboración propia con base en datos de la Superintendencia de Bancos de la República Dominicana (SIMBAD).

El análisis de este indicador muestra que el impacto relativo del riesgo operacional dentro del sistema financiero ha aumentado durante los últimos años. Aunque las

pérdidas operacionales representan una proporción relativamente moderada del margen financiero bruto, su crecimiento sostenido evidencia que el riesgo operacional se ha convertido en un componente cada vez más relevante dentro de la gestión de riesgos de las instituciones financieras.

Este resultado es consistente con tendencias observadas en otros sistemas financieros internacionales, donde la digitalización del sector bancario ha incrementado la exposición a eventos operacionales asociados a fraude digital, interrupciones tecnológicas y fallas en sistemas de información.

Este comportamiento es consistente con la percepción de expertos del sector financiero dominicano, quienes señalan que la incorporación de nuevas tecnologías, el desarrollo de nuevos canales digitales y los cambios constantes en los procesos operativos han incrementado la exposición a eventos de riesgo operacional, especialmente en contextos donde los controles aún se encuentran en proceso de adaptación.

4.2 Transformación estructural del riesgo operacional a nivel internacional

Diversos informes de organismos internacionales, como el Banco de Pagos Internacionales (BIS) y el Fondo Monetario Internacional (IMF), indican que los incidentes relacionados con fraude externo y ciberseguridad representan una proporción cada vez mayor de las pérdidas operacionales reportadas por instituciones financieras a nivel global.

En este contexto, el fraude externo se ha consolidado como una de las principales categorías de riesgo operacional dentro del sistema financiero internacional. De acuerdo con el Basel Committee on Banking Supervision, esta tipología de evento representa entre el 45% y el 55% de las pérdidas operacionales reportadas por bancos internacionalmente activos. (Basel Committee, 2023)

Este fenómeno se encuentra estrechamente vinculado con el crecimiento del comercio electrónico, la expansión de los sistemas de pagos digitales y el aumento de los servicios financieros ofrecidos a través de canales remotos.

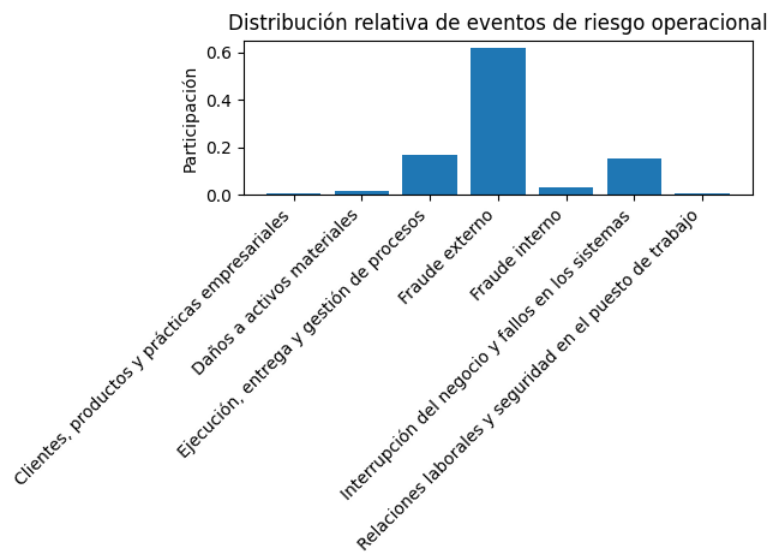
4.3 Fraude: análisis comparativo internacional y República Dominicana

El fraude externo constituye una de las principales fuentes de pérdidas dentro del riesgo operacional tanto a nivel internacional como en el sistema financiero dominicano. En los últimos años, la expansión de los servicios financieros digitales ha incrementado significativamente la exposición de las instituciones financieras a este tipo de eventos. En el caso de la República Dominicana, las estadísticas disponibles muestran que el fraude externo representa la mayor proporción de pérdidas operacionales dentro del sistema bancario

Figura 3

Distribución de eventos de riesgo operacional en el sistema bancario dominicano.

Fuente: Elaboración propia con base en datos de la Superintendencia de Bancos de la República Dominicana (SIMBAD).



El análisis de la distribución de pérdidas por tipología de evento evidencia una concentración significativa en eventos de fraude externo. Esta categoría supera ampliamente a otras tipologías de riesgo operacional, como fallas en procesos, daños a activos o interrupciones del negocio.

Esta concentración refleja la creciente importancia del fraude digital dentro del sistema financiero, particularmente en productos asociados a tarjetas de crédito, transferencias electrónicas y servicios de banca en línea.

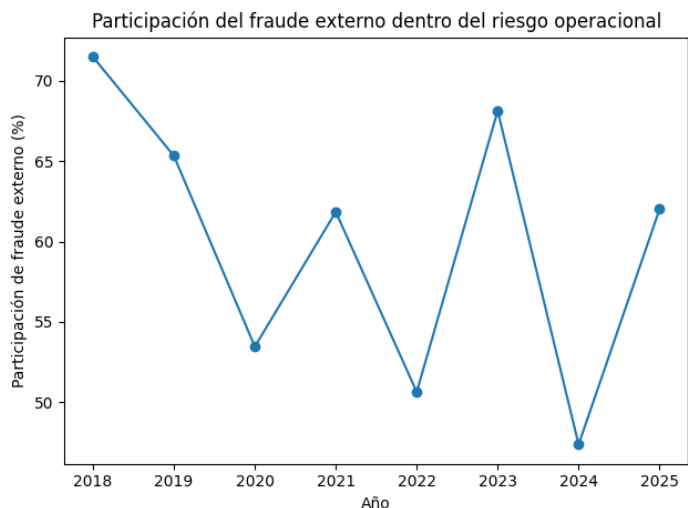
Figura 4

Participación del fraude externo dentro de las pérdidas por riesgo operacional.

Fuente: Elaboración propia con base en datos de la Superintendencia de Bancos de la República Dominicana (SIMBAD).

El análisis de la participación del fraude externo dentro del total de pérdidas operacionales confirma su relevancia estructural dentro del sistema financiero dominicano. Durante varios años del

período analizado, el fraude externo representa más del 60% del total de pérdidas por riesgo operacional.



Este comportamiento sugiere que el fraude constituye uno de los principales desafíos para la gestión del riesgo operacional dentro del sistema bancario dominicano, especialmente en un contexto caracterizado por la expansión de los servicios financieros digitales.

Este resultado es consistente con las entrevistas realizadas a expertos del sector, quienes coinciden en que el fraude externo constituye el principal riesgo operacional en el sistema bancario dominicano. Asimismo, destacan que estos eventos han evolucionado hacia esquemas cada vez más sofisticados, impulsados por la digitalización de los servicios financieros y el incremento de la actividad de ciberdelincuencia.

4.4 Ciberseguridad y resiliencia tecnológica

La creciente digitalización del sistema financiero ha incrementado la importancia de la ciberseguridad como componente fundamental dentro de la gestión del riesgo operacional. Los incidentes cibernéticos pueden generar pérdidas financieras directas, interrupciones en los

servicios financieros y daños reputacionales significativos para las instituciones bancarias. (NIST, 2023; ISO 27001, 2022)

En respuesta a estas amenazas, los reguladores financieros han promovido la adopción de marcos de gestión de ciberseguridad basados en estándares internacionales, como ISO 27001 y el NIST Cybersecurity Framework. (European Central Bank, 2022)

En la República Dominicana, la Superintendencia de Bancos ha establecido disposiciones regulatorias que obligan a las entidades financieras a implementar controles de seguridad tecnológica, mecanismos de gestión de incidentes y pruebas periódicas de vulnerabilidad.

Las entrevistas realizadas evidencian una percepción no homogénea sobre el nivel de madurez tecnológica del sistema financiero dominicano, oscilando entre niveles medios y adecuados en comparación con economías similares. Esta variabilidad sugiere diferencias estructurales entre entidades, así como brechas en capacidades tecnológicas, recursos y nivel de preparación frente a amenazas cibernéticas emergentes.

4.5 Continuidad del negocio y resiliencia operativa

La continuidad del negocio constituye un elemento fundamental para garantizar la estabilidad del sistema financiero frente a eventos disruptivos. Tradicionalmente, las instituciones financieras han abordado este aspecto mediante la implementación de planes de continuidad del negocio y planes de recuperación ante desastres.

No obstante, en los últimos años el enfoque internacional ha evolucionado hacia un modelo más amplio de resiliencia operativa, el cual busca garantizar la continuidad de los servicios financieros críticos incluso en escenarios adversos. (BCBS, 2021; ISO 22301, 2019)

Este enfoque ha sido promovido por organismos internacionales como el Basel Committee on Banking Supervision, que ha desarrollado principios específicos para fortalecer la resiliencia operativa del sistema financiero.

En el caso del sistema bancario dominicano, la implementación de planes de continuidad del negocio y mecanismos de recuperación tecnológica constituye un componente esencial dentro de la gestión del riesgo operacional.

En línea con estos hallazgos, los expertos consultados destacan la necesidad de fortalecer la identificación de servicios críticos, la definición de tolerancias al impacto y la ejecución de pruebas de escenarios disruptivos bajo un enfoque práctico. Asimismo, enfatizan la importancia de gestionar de manera más efectiva los riesgos asociados a terceros críticos y fortalecer la preparación ante eventos operacionales emergentes.

De igual forma, los expertos resaltan la importancia de fortalecer la cultura de ciberhigiene y la concientización de los usuarios como elementos clave dentro de una estrategia integral de resiliencia operativa.

Conclusiones y Discusión

5.1 Síntesis general de la investigación

La presente investigación evidencia que el riesgo operacional ha adquirido una relevancia creciente dentro del sistema bancario dominicano, impulsado principalmente por la digitalización de los servicios financieros y el incremento de amenazas asociadas a fraude y ciberseguridad.

Los resultados muestran una tendencia sostenida al alza en las pérdidas operacionales, así como una alta concentración en eventos de fraude externo, lo que posiciona esta categoría como el principal desafío dentro de la gestión del riesgo operacional en el país. En comparación con

mercados financieros desarrollados, se identifican brechas relevantes en el nivel de madurez tecnológica, en la adopción de herramientas analíticas avanzadas y en la integración de un enfoque integral de resiliencia operativa.

Si bien el sistema financiero dominicano ha avanzado en la formalización normativa, particularmente mediante la implementación del Sistema de Administración del Riesgo Operacional (SARO) y la supervisión basada en riesgos, persisten desafíos en la ejecución práctica, la integración tecnológica y la gestión estratégica del riesgo.

En este contexto, la evidencia sugiere que la evolución hacia un modelo integral de resiliencia operativa constituye un elemento clave para fortalecer la capacidad del sistema bancario dominicano de anticipar, resistir y recuperarse ante eventos operacionales en un entorno cada vez más digitalizado y complejo.

5.2 Limitaciones del estudio

En primer lugar, el estudio se basa principalmente en fuentes secundarias de información, incluyendo informes de organismos internacionales, literatura académica y estadísticas regulatorias. Aunque estas fuentes son ampliamente reconocidas y confiables, el acceso limitado a bases de datos detalladas sobre incidentes operacionales en distintos países restringe la posibilidad de realizar comparaciones cuantitativas más precisas.

Asimismo, la disponibilidad de información pública sobre incidentes cibernéticos y pérdidas operacionales puede variar entre jurisdicciones, lo que introduce cierto grado de imprecisión en el análisis comparativo.

En este contexto, diversos incidentes de fraude y ciberataques registrados en el sistema financiero internacional durante los últimos años han puesto de manifiesto la creciente vulnerabilidad de las

infraestructuras tecnológicas bancarias. Casos ampliamente documentados, como el ataque al sistema SWIFT del Banco Central de Bangladesh o diversos incidentes de ransomware que han afectado a instituciones financieras y proveedores tecnológicos, han reforzado la necesidad de fortalecer la resiliencia operativa y la gestión del riesgo tecnológico en el sector financiero.

Finalmente, el diseño metodológico de carácter documental y descriptivo no permite establecer relaciones causales directas entre la adopción de determinadas prácticas internacionales y la reducción de incidentes operacionales. En su lugar, el estudio identifica asociaciones y tendencias observadas en la literatura especializada.

5.3 Alternativas estratégicas para fortalecer la resiliencia operativa

Un elemento adicional que debe considerarse al evaluar estas alternativas es la heterogeneidad estructural del sistema financiero dominicano. Las entidades de intermediación financiera presentan diferencias significativas en tamaño, complejidad operativa y capacidad de inversión tecnológica, lo que puede limitar la adopción uniforme de soluciones avanzadas basadas en analítica de datos, inteligencia artificial y monitoreo transaccional en tiempo real.

La implementación de transformaciones tecnológicas profundas requiere inversiones significativas en infraestructura tecnológica, sistemas de información y capital humano especializado. En este sentido, las restricciones de capital pueden constituir un factor relevante, particularmente para entidades de menor tamaño dentro del sistema financiero, cuya capacidad de inversión en tecnología puede ser más limitada en comparación con instituciones de mayor escala.

En el marco de Basilea III, el tratamiento del riesgo operacional incorpora un mecanismo de incentivos prudenciales a través del enfoque Standardized Measurement Approach (SMA), el cual vincula el requerimiento de capital por riesgo operacional con el historial de pérdidas internas de las instituciones. Bajo este esquema, mayores pérdidas operacionales implican mayores

requerimientos de capital, generando incentivos regulatorios para fortalecer controles internos y reducir la exposición al riesgo operacional.

Sin embargo, en el contexto dominicano, aunque existen marcos regulatorios para la gestión del riesgo operacional, el requerimiento específico de capital por riesgo operacional bajo metodologías equivalentes al SMA no constituye actualmente una exigencia obligatoria dentro del esquema prudencial. Como resultado, los incentivos regulatorios directos para invertir en la reducción del riesgo operacional pueden ser menos intensos que en jurisdicciones donde estos requerimientos se aplican formalmente.

En este contexto, se identifican tres alternativas estratégicas principales:

- Alternativa 1: Fortalecimiento del marco regulatorio

Ampliar el marco regulatorio mediante disposiciones que promuevan la adopción de estándares internacionales en ciberseguridad, gestión antifraude y resiliencia operativa.

- Alternativa 2: Transformación tecnológica del sistema financiero

Promover la adopción de herramientas avanzadas de analítica de datos, inteligencia artificial y monitoreo transaccional en tiempo real para mejorar la detección y prevención de eventos operacionales.

- Alternativa 3: Implementación de un modelo integral de resiliencia operativa

Adoptar un enfoque integral que articule la gestión del fraude, la ciberseguridad, la continuidad del negocio y el riesgo operacional dentro de un marco estratégico común.

5.4 Estrategia recomendada para el sistema bancario dominicano

A partir del análisis realizado, esta investigación considera que la alternativa más adecuada para fortalecer la resiliencia operativa del sistema bancario dominicano es la adopción progresiva de un modelo integral de resiliencia operativa. (BCBS, 2021; IMF, 2024)

El riesgo operacional contemporáneo presenta una naturaleza interconectada, donde los eventos de fraude, los incidentes cibernéticos y las interrupciones tecnológicas comparten causas comunes relacionadas con procesos, sistemas y fallas de control, por lo que abordarlos de manera aislada puede limitar la efectividad de las estrategias de mitigación, mientras que un enfoque de resiliencia operativa permite integrar estas dimensiones dentro de un mismo marco de gestión.

A nivel internacional, organismos como el Comité de Basilea han promovido este enfoque mediante los Principles for Operational Resilience, los cuales enfatizan la identificación de servicios críticos, la definición de tolerancias de impacto y la realización de pruebas de escenarios adversos.

En el caso de la República Dominicana, la adopción de este enfoque podría desarrollarse de forma progresiva a partir del fortalecimiento del Sistema de Administración del Riesgo Operacional (SARO) y su integración con los marcos de gestión tecnológica y continuidad del negocio ya existentes. Esta transición podría ser promovida por la autoridad supervisora mediante lineamientos técnicos y criterios de evaluación dentro del modelo de Supervisión Basada en Riesgos.

Asimismo, es importante considerar la heterogeneidad estructural del sistema financiero dominicano, donde las entidades presentan diferencias en tamaño y capacidad de inversión tecnológica. En este sentido, un modelo de resiliencia operativa permite una implementación gradual y proporcional al perfil de riesgo de cada institución.

En este contexto, evaluaciones internacionales del sistema financiero dominicano, incluyendo el Financial Sector Assessment Program (FSAP) del Fondo Monetario Internacional y el Banco Mundial, así como las consultas periódicas del Artículo IV del FMI, han señalado la importancia de continuar fortaleciendo el marco de supervisión financiera y las herramientas de gestión de riesgos, destacando la necesidad de avanzar en la modernización regulatoria y en el monitoreo de

vulnerabilidades dentro de un entorno financiero cada vez más digitalizado (Fondo Monetario Internacional, 2024).

Los resultados obtenidos a partir del análisis documental fueron consistentes con la percepción de expertos del sector financiero dominicano, quienes confirmaron la alta concentración del riesgo operacional en eventos de fraude externo, así como la existencia de brechas en la madurez tecnológica y en la gestión integral del riesgo. De igual forma, las entrevistas evidencian la persistencia de un enfoque predominantemente orientado al cumplimiento regulatorio, en lugar de una gestión estratégica del riesgo operacional, lo que limita la efectividad de los mecanismos de prevención y respuesta ante eventos disruptivos.

Asimismo, se identifican factores adicionales como la vulnerabilidad de los usuarios ante esquemas de ingeniería social y la escasez de talento especializado en ciberseguridad, los cuales representan desafíos relevantes para la gestión del riesgo operacional en el sistema financiero dominicano.

En este sentido, la evidencia analizada sugiere que el principal desafío del sistema bancario dominicano no radica únicamente en la existencia de marcos regulatorios, sino en la evolución hacia una gestión del riesgo operacional más integrada, proactiva y orientada a la resiliencia, capaz de anticipar y adaptarse a un entorno financiero cada vez más digitalizado y complejo.

Por lo tanto, consideramos que la adopción progresiva de marcos de resiliencia operativa representa una estrategia viable para fortalecer la gestión del riesgo operacional en el sistema bancario dominicano, contribuyendo a mejorar la capacidad del sistema financiero para enfrentar eventos operacionales complejos y preservar la estabilidad del sector en un entorno cada vez más digitalizado.

Bibliografía

1. Bank for International Settlements. (2022). Operational risk newsletter. BIS.
2. Bank for International Settlements. (2023). Operational risk data collection exercise. BIS.
3. Basel Committee on Banking Supervision. (2011). Principles for the sound management of operational risk. Bank for International Settlements.
4. Basel Committee on Banking Supervision. (2017). Basel III: Finalising post-crisis reforms. Bank for International Settlements.
5. Basel Committee on Banking Supervision. (2021). Principles for operational resilience. Bank for International Settlements.
6. Basel Committee on Banking Supervision. (2023). Operational risk newsletter. Bank for International Settlements.
7. Committee on Payments and Market Infrastructures, & International Organization of Securities Commissions. (2016). Guidance on cyber resilience for financial market infrastructures. Bank for International Settlements.
8. Deloitte. (2023). Transforming risk management in financial services. Deloitte Insights.
9. Ernst & Young. (2024). Transforming Financial Services with Operational Resilience. EY Global.
10. European Central Bank. (2022). Cyber resilience oversight expectations for financial market infrastructures. European Central Bank.
11. Federal Deposit Insurance Corporation. (2023). Risk management manual of examination policies. FDIC.
12. International Monetary Fund. (2022). Global financial stability report. International Monetary Fund.
13. International Monetary Fund. (2024). Dominican Republic: Article IV consultation report. International Monetary Fund.
14. International Organization for Standardization. (2016). ISO 37001: Anti-bribery management systems

15. International Organization for Standardization. (2018). ISO 31000: Risk management Guidelines.
16. International Organization for Standardization. (2019). ISO 22301: Security and resilience Business continuity management systems
17. International Organization for Standardization. (2021). ISO 22317: Security and resilience Business impact analysis (BIA).
18. International Organization for Standardization. (2022a). ISO/IEC 27001: Information security management systems
19. International Organization for Standardization. (2022b). ISO/IEC 27002: Information security controls.
20. KPMG. (2022). Global banking risk outlook. KPMG International.
21. National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). U.S. Department of Commerce.
22. National Institute of Standards and Technology. (2023). NIST cybersecurity framework (Version 2.0). U.S. Department of Commerce.
23. PwC. (2023). Global economic crime and fraud survey. PricewaterhouseCoopers.
24. Superintendencia de Bancos de la República Dominicana. (2009). Reglamento sobre el Riesgo Operacional. SIB.
25. Superintendencia de Bancos de la República Dominicana. (2018). Reglamento sobre Seguridad Cibernética y de la Información. SIB.
26. Superintendencia de Bancos de la República Dominicana. (2023). Informe anual de riesgo operacional. SIB.
27. Superintendencia de Bancos de la República Dominicana. (2025). Sistema de Información del Mercado Bancario Dominicano (SIMBAD). SIB.
28. World Bank. (2021). Financial sector resilience and risk management. World Bank.
29. World Economic Forum. (2022). Global cybersecurity outlook 2022. World Economic Forum.
30. World Economic Forum. (2023). Global risks report 2023. World Economic Forum.

Anexos

Entrevista 1

1. Desde su experiencia profesional, ¿cuáles considera que son actualmente los principales factores que explican la ocurrencia de fraude externo y otros incidentes operacionales en el sistema bancario dominicano?

Con relación a los fraudes externos, es importante tener presente que estos constituyen uno de los principales flagelos que afectan tanto a nivel global como a la sociedad dominicana, y que, además, evolucionan constantemente hacia esquemas cada vez más complejos y sofisticados.

Asimismo, debe considerarse que el sector bancario, por la propia naturaleza de sus operaciones y el manejo de recursos financieros, es inherentemente un objetivo atractivo para ciberdelincuentes y otros actores fraudulentos, quienes buscan vulnerar el sistema, afectar su integridad y generar impactos tanto en las entidades como en los clientes.

Con relación a los demás eventos de riesgo operacional, es importante tener presente que los sistemas bancarios son entornos altamente complejos, que integran múltiples procesos, la participación de numerosas personas y un fuerte soporte tecnológico.

En este contexto, dicha complejidad incrementa la exposición a posibles fallas o errores en cualquiera de sus componentes, ya sean humanos, tecnológicos o de proceso, lo que hace que este tipo de riesgos sea inherente a la operación.

2. ¿Cómo evaluaría el nivel de madurez tecnológica del sistema financiero dominicano para enfrentar los riesgos cibernéticos y tecnológicos actuales?

A mi entender, el nivel de madurez tecnológica en la República Dominicana es adecuado. Si bien aún no se encuentra al nivel de países más desarrollados, al compararnos con economías de

características similares, se evidencia que nuestro ecosistema tecnológico está alineado con estándares relevantes e incluso, en algunos aspectos, por encima de otros sistemas comparables. No obstante, este nivel de avance no implica que estemos exentos de riesgos. Persisten vulnerabilidades inherentes y una exposición constante a amenazas, particularmente en materia de ciberseguridad,

3. En su opinión, ¿el marco regulatorio vigente en la República Dominicana es suficiente para abordar los riesgos operacionales emergentes en el sistema bancario?

Entiendo que no. Si bien en los últimos cinco años se ha otorgado mayor relevancia al riesgo operacional, en la práctica aún se percibe que su gestión ha quedado limitada, en ciertos casos, a un enfoque técnico o de cumplimiento puntual.

El riesgo operacional, como hemos comentado, es un concepto amplio y transversal, que abarca múltiples aristas. Por ello, requiere ser abordado con mayor profundidad, fortaleciendo aquellos aspectos que no solo respondan a las exigencias regulatorias, sino que también reflejen la realidad del negocio bancario y su operatividad diaria, la cual es inherentemente compleja.

En este sentido, resulta clave evolucionar hacia una gestión más integral y práctica, que combine cumplimiento, entendimiento del negocio, cultura organizacional y capacidades operativas, a fin de lograr una efectiva gestión de riesgo.

4. ¿Cuáles considera que deberían ser las principales prioridades para fortalecer la resiliencia operativa del sistema bancario dominicano frente a eventos disruptivos o incidentes operacionales?

Entiendo que, en materia de situaciones disruptivas en el sistema bancario, el aspecto más relevante es la adecuada identificación de los posibles eventos y su análisis bajo un enfoque realista. Con frecuencia, estos ejercicios se abordan desde una perspectiva teórica; sin embargo, resulta clave orientarlos hacia escenarios prácticos, alineados con la realidad operativa y el contexto país.

Asimismo, es importante reconocer una tendencia cultural hacia la reacción más que la prevención, así como la subestimación de eventos de alto impacto bajo la premisa de que “no ocurrirán” o que, en caso de materializarse, podrán resolverse oportunamente. Este enfoque limita la efectividad de la preparación ante escenarios críticos.

En este sentido, se hace necesario fortalecer los procesos de identificación, evaluación y gestión de eventos disruptivos, bajo un enfoque integral y coordinado. La respuesta debe articularse de manera conjunta entre los diferentes miembros del sistema, considerando la naturaleza del evento, ya que no es equivalente gestionar un incidente de ciberseguridad de alcance nacional que un evento de origen natural, aunque ambos representan riesgos relevantes a los cuales el país se encuentra expuesto.

5. Desde su área de especialización (fraude, ciberseguridad, continuidad u otras funciones relacionadas), ¿cómo evalúa el nivel de preparación de las entidades financieras dominicanas para gestionar eventos de riesgo operacional?

Considero que los colaboradores del sector bancario, a raíz de la relevancia que ha adquirido el riesgo operacional en los últimos años, han venido fortaleciendo sus capacidades y nivel de conocimiento en esta materia.

No obstante, se identifican dos aspectos clave de mejora. En primer lugar, la capacitación debe orientarse hacia un enfoque más práctico. En muchos casos, se abordan los temas desde una perspectiva teórica o meramente regulatoria; sin embargo, es fundamental que se enfoquen en la gestión real del riesgo y en situaciones aplicables a la operatividad diaria, más allá del cumplimiento normativo.

En segundo lugar, es importante que la gestión del riesgo operacional no recaiga únicamente en los equipos especializados o en los gestores de riesgo. La alta gerencia y los consejos de administración deben involucrarse activamente, comprendiendo la relevancia estratégica del riesgo operacional y su impacto potencial en los resultados y la sostenibilidad de la organización.

6. ¿Cuáles considera que son las principales brechas o desafíos que aún enfrenta el sistema bancario dominicano en materia de gestión del riesgo operacional?

Entiendo que las principales brechas son las señaladas anteriormente. Por un lado, la necesidad de hacer la gestión del riesgo operacional más práctica, trascendiendo un enfoque estrictamente regulatorio, para convertirla en una herramienta real de gestión que evidencie el valor agregado que aporta a la organización.

Por otro lado, resulta fundamental fortalecer el involucramiento de la alta gerencia, de manera que conozca, comprenda y valore la importancia estratégica del riesgo operacional, así como su impacto directo en los resultados, la continuidad del negocio y la sostenibilidad de la entidad.

Entrevista 2

- 1. Desde su experiencia profesional, ¿cuáles considera que son actualmente los principales factores que explican la ocurrencia de fraude externo y otros incidentes operacionales en el sistema bancario dominicano?**

Los factores que más influyen en la materialización de eventos de riesgo operacional son principalmente los cambios constantes de procesos, incorporación de nuevas tecnologías y desarrollo de nuevos productos y canales. Esto es porque con cada cambio surgen brechas para las cuales las organizaciones no están completamente preparadas, así como mayor posibilidad de error humano debido a la curva de aprendizaje, y nuevos aspectos tecnológicos para los cuales no necesariamente se han implementado controles suficientes y probados. En adición la dependencia de terceros aumenta las posibilidades de ocurrencia de eventos que no están totalmente en control de la entidad.

- 2. ¿Cómo evaluaría el nivel de madurez tecnológica del sistema financiero dominicano para enfrentar los riesgos cibernéticos y tecnológicos actuales?**

El nivel de madurez a nivel general es medio, debido a que el desarrollo de la inteligencia artificial y de nuevos desarrollos tecnológicos a nivel internacional, ha sofisticado los ataques cibernéticos

y no todas las entidades cuenta con los recursos y conocimientos necesarios para estar a la vanguardia. Sin embargo, muchas entidades tienen un alto nivel de protección sin embargo esto no asegura que estén exentas de vulnerabilidades ante la evolución tan rápida de los peligros tecnológicos.

3. En su opinión, ¿el marco regulatorio vigente en la República Dominicana es suficiente para abordar los riesgos operacionales emergentes en el sistema bancario?

No, el marco regulatorio de RD está desactualizado y carece de muchos aspectos importantes que deben ser considerados. Con la actualización del reglamento de riesgo operacional y sus instructivos se espera cerrar estas brechas. En adición se requiere instructivos sobre la gestión de riesgo tecnológico y cibernético ante la alta relevancia de estos riesgos.

4. ¿Cuáles considera que deberían ser las principales prioridades para fortalecer la resiliencia operativa del sistema bancario dominicano frente a eventos disruptivos o incidentes operacionales?

Las principales prioridades deben ser fortalecer las capacidades y conocimientos de los equipos para tratar con eventos disruptivos y establecer planes de continuidad y emergencia que sean probados y efectivos. En adición, se debe realizar una identificación clara de servicios y procesos críticos y la tolerancia al impacto de estos eventos, fortalecer la infraestructura tecnológica, y gestionar el riesgo de los terceros críticos.

5. Desde su área de especialización (fraude, ciberseguridad, continuidad u otras funciones relacionadas), ¿cómo evalúa el nivel de preparación de las entidades financieras dominicanas para gestionar eventos de riesgo operacional?

En sentido general, las entidades están preparadas para ciertos eventos, sin embargo, falta preparación para la gestión de los eventos de riesgos emergentes y de aspectos tecnológicos.

6. ¿Cuáles considera que son las principales brechas o desafíos que aún enfrenta el sistema bancario dominicano en materia de gestión del riesgo operacional?

Las principales brechas de la gestión de riesgo operacional son principalmente la persistencia de un enfoque muy orientado a cumplimiento regulatorio debido a la falta de cultura de riesgo en las entidades. Esto se puede evidenciar en la falta de registro de pérdidas por eventos de riesgo operacional, así como integración deficiente entre los equipos de riesgo operacional y ciberseguridad. En adición debido a la alta incidencia de tercerización de servicios, especialmente de carácter tecnológico, hay una dependencia muy alta ante la gestión de los riesgos de estos proveedores críticos, lo cual no es gestionado de forma proactiva en muchas entidades.

Por otro lado, en riesgo operacional aún hay un uso limitado de análisis prospectivo y pruebas de estrés debido principalmente a las limitaciones en datos y analítica de este tipo de riesgo.

Verificación Anti-Plagio

Diagnóstico del riesgo operacional en la banca dominicana: fraude, ciberseguridad y continuidad del negocio.

Sustentante(s):
Jesús Ismael Diaz Madera (10148390)
Francheco de los Santos (10162396)

Introducción

1.1 Antecedentes del problema

El riesgo operacional ha adquirido una relevancia creciente en el sector financiero global, especialmente en contextos de alta digitalización. Según el Comité de Basilea, este tipo de riesgo a pérdidas derivadas de fallos en procesos internos, errores humanos, deficiencias

14% Similitud general

Fuente	Similitud
1 Internet: www.coursera.com	-1%
2 Internet: issuu.com	-1%
3 Internet: www.bcb.gob.do	-1%
4 Internet: auditoriauc20162mju02.wikispa...	-1%
5 Internet: hdl.handle.net	-1%
6 Internet: www.researchgate.net	-1%
7 Internet: repositorioacademico.upc.edu.pe	-1%
8 Internet: www.federalreserve.gov	-1%

Certificado Citi Program Jesús Diaz



Completion Date 15-Feb-2026
Expiration Date 15-Feb-2028
Record ID 73258174

This is to certify that:

Jesus Diaz

Has completed the following CITI Program course:

Not valid for renewal of certification through CME.

Human Subject Research Spanish
(Curriculum Group)
Curso de Ética en la Investigación para Estudiantes
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Pontificia Universidad Católica Madre y Maestra (Santo Domingo- República Dominicana) Training Initiative

101 NE 3rd Avenue, Suite 320
Fort Lauderdale, FL 33301 US
www.citiprogram.org

CITI

Generated on 15-Feb-2026. Verify at www.citiprogram.org/verify/?w3ed73e2b-c299-45d6-a15d-7216c0ab8fd8-73258174

Certificado Citi Program Franchesco de los Santos



Completion Date 13-Jan-2026
Expiration Date 13-Jan-2028
Record ID 74560364

This is to certify that:

FRANCHECO DE LOS SANTOS VERAS

Has completed the following CITI Program course:

Not valid for renewal of certification through CME.

Human Subject Research Spanish
(Curriculum Group)
Curso de Ética en la Investigación para Estudiantes
(Course Learner Group)
1 - Basic Course
(Stage)

Under requirements set by:

Pontificia Universidad Católica Madre y Maestra (Santo Domingo- República Dominicana) Training Initiative

101 NE 3rd Avenue, Suite 320
Fort Lauderdale, FL 33301 US
www.citiprogram.org

CITI

Generated on 26-Mar-2026. Verify at www.citiprogram.org/verify/?w2387bc2a-b2f6-4187-aa6d-59f4a601b336-74560364