ATMIRE

Title	Herramienta para evaluar el nivel de madurez de la gestión del riesgo operacional en una empresa del sistema financiero en el Perú
Item Type	http://purl.org/coar/resource_type/c_bdcc
Authors	Alfaro Bejarano, Maria Eugenia;Machado Moreno, Roxana Janeth;Salazar Cuya, Jhon Alexander
Publisher	Universidad Peruana de Ciencias Aplicadas (UPC)
Rights	http://purl.org/coar/access_right/c_abf2
Download date	2026-11-27 01:23:02
Item License	https://creativecommons.org/licenses/by/4.0/
Link to Item	https://hdl.handle.net/10757/689619

UNIVERSIDAD PERUANA DE CIENCIAS APLICADAS

ESCUELA DE POSTGRADO

PROGRAMA DE MAESTRÍA EN AUDITORÍA Y GESTIÓN DE RIESGOS

HERRAMIENTA PARA EVALUAR EL NIVEL DE MADUREZ DE LA GESTIÓN DEL RIESGO OPERACIONAL EN UNA EMPRESA DEL SISTEMA FINANCIERO EN EL PERÚ

TRABAJO DE INVESTIGACIÓN

Presentado como parte de los requisitos para optar el grado académico de Maestro en Auditoría y Gestión de Riesgos

AUTOR(ES)

Alfaro Bejarano, Maria Eugenia	0009-0000-0281-5295
Machado Moreno, Roxana Janeth	0009-0005-2303-1680
Salazar Cuya, Jhon Alexander	0009-0009-1204-8275

ASESOR(ES)

Guerra Vargas, Juan Luis	0009-0001-6955-826X

Lima, 25 de marzo de 2026

Resumen

Este estudio buscó diseñar una herramienta para evaluar el nivel de madurez de la gestión del riesgo operacional en entidades del sistema financiero peruano, tomando como estructura los cinco componentes y veinte principios de COSO ERM 2017. Se utilizó un diseño aplicado, de alcance descriptivo y enfoque documental. A partir de la recopilación de normativa y referentes de buenas prácticas internacionales y nacionales, se extrajeron y depuraron contenidos, los cuales fueron categorizados e integrados para traducirlos en criterios observables. Los hallazgos mostraron la factibilidad de operacionalizar los principios de COSO ERM en un instrumento estandarizado compuesto por 60 criterios, formulados como preguntas con seis niveles de respuesta (0 a 5), desde inmaduro hasta optimizado. La calificación se definió sin ponderaciones, mediante medias aritméticas sucesivas (criterio–principio–componente–global) y con redondeo conservador, favoreciendo trazabilidad y comparabilidad de resultados. En conjunto, la propuesta permite establecer una línea base de madurez, identificar brechas por principio y componente, y facilitar el seguimiento de mejoras a lo largo del tiempo.

Palabras clave: gestión de riesgo operacional; modelo de madurez; control interno; sistema financiero.

A Tool to Assess the Maturity Level of Operational Risk Management in a Peruvian Financial Sector Institution

Abstract

This study aimed to design a tool to assess the maturity level of operational risk management in Peruvian financial system entities, using the five components and twenty principles of COSO ERM 2017 as the structure. An applied, descriptive, document-based design was used. Based on the compilation of regulatory requirements and international and national good-practice references, content items were extracted and refined, then categorized and integrated to translate them into observable assessment criteria. The findings showed the feasibility of operationalizing COSO ERM principles into a standardized instrument comprising 60 criteria, formulated as questions with six response levels (0 to 5), ranging from immature to optimized. Scoring was defined without weightings, using successive arithmetic means (criterion–principle–component–overall) and conservative rounding, which supports traceability and comparability of results. Overall, the proposed tool enables the establishment of a maturity baseline, the identification of gaps by principle and component, and the monitoring of improvements over time.

Keywords: operational risk management; maturity mode; internal control; financial institutions.

e201585397_Alfaro Bejarano, Maria Eugenia_HERRAMIENTA PARA EVALUAR EL NIVEL DE MADUREZ DE LA GESTIÓN DEL RIESGO OPERACIONAL EN UNA EMPRESA DEL SISTEMA FINANCIERO EN EL PERÚ

INFORME DE ORIGINALIDAD

7%	7%	5%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	upc.aws.openrepository.com Fuente de Internet	1%
2	hdl.handle.net Fuente de Internet	1%
3	dspace-uh-tmp.igniteonline.la Fuente de Internet	<1%
4	Submitted to Universidad de Chile - CN-038051 Trabajo del estudiante	<1%
5	ri.ues.edu.sv Fuente de Internet	<1%
6	cybertesis.uni.edu.pe Fuente de Internet	<1%
7	auditoresinternos.es Fuente de Internet	<1%
8	oldri.ues.edu.sv Fuente de Internet	<1%
	repositorio.uasb.edu.bo	

1. Introducción

En las últimas décadas, el sistema financiero internacional ha acelerado su transformación, impulsado por la digitalización, la mayor interconexión de los mercados y la creciente dependencia de ecosistemas tecnológicos y de terceros. En este escenario, el riesgo operacional se ha convertido en una prioridad.

El Basel Committee on Banking Supervision (BCBS, 2004) incorporó en el Acuerdo de Basilea II el concepto de riesgo operacional, reconociéndolo como una fuente de pérdidas que debía ser gestionada y cubierta mediante requerimientos de capital específicos y al hacerlo sentó las bases para que los sistemas financieros a nivel mundial incorporen este tipo de riesgo dentro de sus modelos de gestión integral de riesgos

Dicha decisión se tomó ya que en su momento existía una limitación de los enfoques regulatorios iniciales, centrados en riesgo de crédito y de mercado. Las pérdidas y fallas registradas por diversas instituciones a nivel internacional mostraron que una proporción relevante del riesgo proviene de errores humanos, procesos internos deficientes, fallos tecnológicos y eventos externos, factores que no eran capturados adecuadamente.

Ante ello surgieron modelos en gestión integral de riesgos como COSO ERM (2017) e ISO 31000 (2018) que consolidaron una visión más integral y estratégica, orientada no solo a evitar el riesgo sino a gestionarlo para generar valor alineado con la estrategia, objetivos y desempeño de una organización.

En el ámbito peruano, la Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS, 2009) adaptó estos estándares internacionales en el Reglamento para la gestión del Riesgo Operacional aprobado mediante la resolución SBS N.º 2115-2009, el cual sería aplicable a las entidades bajo su supervisión. En consecuencia, el sistema financiero peruano cuenta hoy con un marco regulatorio con bases sólidas alineado con las buenas prácticas internacionales y orientado a promover una gestión del riesgo operacional efectiva y estandarizada.

En el sistema financiero peruano existe un indicador indirecto para medir el nivel de madurez de la gestión de riesgo operacional, conocido como Método Estándar Alternativo (ASA, por sus siglas en inglés), dicho método requiere la autorización de la SBS, quien evalúa el cumplimiento de trece (13) requisitos asociados a buenas prácticas para su uso. Según la información de la SBS (s.f.), de las 47 empresas que conforman sistema financiero a agosto 2025, únicamente el 21% (10) ha logrado y acreditado un nivel de madurez que le permitió usar el método ASA[1]; sin embargo, el 40% (4) de estás cuentan con requerimientos adicionales[2] debido al cumplimiento parcial de los requisitos. Por otro lado, cinco (5) empresas que tenían la autorización en el 2020 han dejado de tenerla en el tiempo.

Esta situación evidencia no solo la dificultad de las entidades para consolidar prácticas maduras de gestión de riesgo operacional, sino también la ausencia de mecanismos sistemáticos de diagnóstico que permitan identificar brechas específicas y priorizar mejoras de manera estructurada. La carencia de herramientas estandarizadas de autoevaluación limita la capacidad de las entidades para: (i) establecer una línea base

[1] BBVA, Scotiabank, Banco Falabella, Compartamos Banco, Mi Banco y Caja Arequipa.
[2] Banco de Crédito del Perú, Banbif, Interbank y Financiera Confianza

comparable de su nivel de madurez, (ii) identificar debilidades por componente o principio antes de que se materialicen en pérdidas, y (iii) demostrar ante la supervisión avances tangibles y trazables en el fortalecimiento de su gestión de riesgo operacional. En este contexto, se vuelve especialmente relevante contar con instrumentos que permitan diagnosticar y comparar el nivel de madurez de la gestión del riesgo operacional, más allá del mero cumplimiento, para identificar brechas estructurales y prioridades de mejora de forma objetiva.

Ante esta problemática, surge la interrogante: ¿existen en la literatura instrumentos que integren marcos conceptuales reconocidos (como COSO ERM) con normativas regulatorias específicas y que permitan a las entidades del sistema financiero peruano evaluar sistemáticamente su nivel de madurez en gestión de riesgo operacional?

La revisión sistemática de la literatura académica y normativa revela desarrollos significativos en tres áreas independientes, pero evidencia una brecha metodológica relevante en su integración aplicada al contexto del sistema financiero peruano.

En primer lugar, respecto a modelos generales de madurez en gestión de riesgos, existen marcos evolutivos consolidados, como el *ERM Maturity Model* de la Organisation for Economic Co-operation and Development (OECD, 2021), que define cinco niveles progresivos (Emergente, En Progreso, Establecido, Líder y Aspiracional) centrados en administraciones tributarias, y el modelo CMMI V2.0 (Capability Maturity Model Integration Institute [CMMI], 2018). , orientado principalmente a la madurez de procesos de desarrollo de software. Si bien estos modelos aportan estructuras robustas de evolución por niveles, carecen de especificidad sectorial para riesgo operacional en instituciones financieras y no incorporan criterios evaluables contextualizados a marcos regulatorios particulares.

En segundo lugar, en cuanto a marcos de evaluación de riesgo operacional, la literatura identifica propuestas principalmente normativas del Comité de Basilea. El documento "Operational Risk – Supervisory Guidelines for the Advanced Measurement Approaches" (BCBS, 2011a) reconoce que el marco de Basilea II prevé que, con el tiempo, la disciplina de riesgo operacional madurará y convergirá hacia prácticas de gestión y medición de riesgos más efectivas, pero no establece niveles de madurez específicos ni herramientas de autoevaluación. Asimismo, estudios de organismos regulatorios como la Office of the Superintendent of Financial Institutions Canada (OSFI, 2024) y análisis recientes del Banco Central Europeo sobre madurez de riesgo operacional Ernst & Young (EY, 2025, enero) enfatizan que las instituciones financieras presentan niveles variables de madurez debido a dificultades en el modelamiento de pérdidas, escasez de datos de eventos extremos y taxonomías inconsistentes, sin proporcionar instrumentos estandarizados de medición de madurez.

Recientemente, Van der Westhuizen (2025) desarrolló un conjunto de 30 criterios para evaluar la madurez de la gestión de riesgo operacional mediante una revisión de literatura no sistemática, motivada por las pérdidas organizacionales causadas por la pandemia de COVID-19 como evento externo de riesgo operacional. Si bien este estudio representa un avance en la identificación de criterios evaluables de madurez, su enfoque no está específicamente orientado al sector financiero regulado, no integra marcos de referencia como COSO ERM con normativas regulatorias específicas (como Basilea o regulaciones locales), y no establece una metodología de agregación de resultados ni escalas de

madurez operacionalizadas que permitan comparabilidad sistemática entre organizaciones.

En tercer lugar, sobre aplicación de COSO ERM en instituciones financieras, la investigación muestra que el marco COSO ERM 2017 se utiliza ampliamente como referencia conceptual para alinear controles internos con objetivos empresariales y cumplir con regulaciones (Ncontracts, 2024; UpGuard, 2025). Documentos de consultoras especializadas como KPMG (2017) y Deloitte (2024) describen componentes de programas maduros de riesgo operacional (gobierno, identificación, evaluación, monitoreo, control y tecnología) y proponen niveles evolutivos básicos (básico, en desarrollo, establecido, avanzado), pero estos marcos se enfocan principalmente en aspectos conceptuales y de consultoría sin operacionalizar criterios medibles específicos ni reglas de agregación estandarizadas que permitan comparabilidad entre entidades.

Finalmente, en el contexto latinoamericano y peruano, la búsqueda reveló desarrollos aislados en áreas adyacentes. Gutierrez Alayo et al. (2021) proponen un modelo de madurez de ciberseguridad para el sector financiero peruano con cinco niveles, pero circunscrito exclusivamente a seguridad informática y capacidades de nube, sin abordar la gestión integral de riesgo operacional. Asimismo, estudios de organismos multilaterales sobre madurez digital y ciberseguridad en entidades peruanas (Lee et al., 2024; Porrúa et al., 2025) confirman brechas en marcos de evaluación contextualizados, pero no abordan específicamente riesgo operacional conforme a COSO ERM ni a la normativa SBS. Esta revisión evidencia tres vacíos metodológicos concretos: primero, no se identificaron herramientas que integren de manera coherente y operativa los principios de COSO ERM 2017 con los lineamientos de Basilea II (BCBS, 2004) así como con las disposiciones establecidas en la Resolución SBS 2115-2009 (2009) y la Resolución SBS 2116-2009 (2009); segundo, los modelos existentes no traducen estos marcos conceptuales en instrumentos de autoevaluación con criterios medibles, niveles de madurez claramente definidos y reglas de agregación transparentes que faciliten comparabilidad y trazabilidad; y tercero, no se hallaron metodologías estandarizadas que permitan a las entidades del sistema financiero peruano diagnosticar de forma sistemática y autónoma su nivel de madurez en gestión de riesgo operacional. En consecuencia, esta brecha se define como la ausencia de instrumentos integrados de COSO ERM, Basilea y la normativa de la SBS, operacionalizados (con criterios evaluables, escalas de madurez y métodos de calificación) y contextualizados al sistema financiero peruano, que faciliten la autoevaluación, identificación de brechas y mejora continua en la gestión del riesgo operacional.

A partir de ello, se plantean las siguientes proposiciones (P) que sustentan la relevancia y pertinencia del estudio: - P1. Si se identifican los principios y criterios clave de la madurez en la gestión de riesgo operacional, es posible estructurar una propuesta que, de ser puesta en práctica, podría eventualmente reflejar los niveles de madurez existentes en las entidades financieras. - P2. La revisión de las normas internacionales y locales permitiría construir una propuesta basada en un instrumento contextualizado y técnicamente sólido. - P3. Si la propuesta establece un diseño claro en la construcción de la herramienta, una vez aplicada, facilitará la evaluación del nivel de madurez en la gestión del riesgo operacional dentro del sistema financiero.

Bajo este enfoque, el presente trabajo de investigación tiene como objetivo: Diseñar y operacionalizar una herramienta que permita evaluar el nivel de madurez de la gestión de riesgo operacional en una empresa del sistema financiero peruano. Dicha herramienta

estará fundamentada en los principios del COSO ERM además estará alineada con la normativa de la SBS.

En este contexto, el objetivo de la presente investigación es diseñar y operacionalizar una herramienta de autoevaluación que permita medir el nivel de madurez de la gestión del riesgo operacional en las empresas del sistema financiero peruano, integrando la estructura de COSO ERM con los lineamientos de Basilea y normativa emitida por la SBS.

Este trabajo tiene un alcance aplicado y de carácter documental, centrado en el análisis, sistematización y traducción de dichos marcos conceptuales y normativos en **c**riterios evaluables, niveles de madurez y reglas de agregación, que faciliten su uso práctico por parte de las entidades financieras. En tal sentido, la investigación no contempla la validación empírica de la herramienta en instituciones específicas, limitándose al diseño metodológico del instrumento y a la definición de su estructura conceptual y operativa.

En ese sentido, la herramienta propuesta ofrecerá, a las empresas que la apliquen, una evaluación objetiva y práctica sobre el grado de desarrollo e integración de los procesos asociados al riesgo operacional, además permitirá identificar brechas, priorizar mejoras, fortalecer la cultura organizacional del riesgo y promoverá además una gestión más proactiva, eficiente y orientada a la resiliencia.

Con todo lo mencionado, esta investigación contribuirá al fortalecimiento del sistema financiero peruano, ya que impulsará el cambio de enfoque del riesgo operacional para migrar de un factor de control a un activo estratégico generador de confianza, optimizador de decisiones que refuerce la sostenibilidad institucional.

2. Marco conceptual y normativo

El presente artículo de investigación se centra en los siguientes conceptos: modelos de gestión de riesgos, gestión del riesgo operacional y modelos de madurez. Los modelos de gestión de riesgos promueven un enfoque integral, transversal y alineado con la estrategia y la toma de decisiones organizacionales. La gestión de riesgo operacional en el sistema financiero se sustenta en buenas prácticas internacionales y marcos normativos. Por su parte, los modelos de madurez son útiles para evaluar el grado de desarrollo, formalización y mejora continua tanto de los procesos como de las capacidades organizacionales.

A continuación, se presentan los marcos conceptuales y normativos considerados para respaldar el diseño de la herramienta propuesta:

2.1 Modelos de gestión de riesgos

Entre los modelos de gestión de riesgos más relevantes están COSO ERM 2017 e ISO 31000:2018. El marco COSO ERM 2017, propone un enfoque integral para la gestión de riesgos, enfatizando su integración con la estrategia, los objetivos y el desempeño organizacional. El marco establece que la gestión de riesgos debe ser transversal y apoyar la creación de valor, anticipando eventos que puedan afectar el logro de objetivos. Se organiza en cinco componentes y veinte principios que orientan prácticas

como la definición del apetito de riesgo, la evaluación del desempeño, el monitoreo continuo y la comunicación efectiva. Su estructura flexible permite aplicarlo a distintos sectores, fortaleciendo la toma de decisiones y la resiliencia organizacional (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 2017).

Por su parte, la International Organization for Standardization (ISO, 2018), a través de la norma ISO 31000:2018, establece principios y directrices para una gestión del riesgo efectiva en cualquier tipo de organización. Su enfoque se basa en integrar la gestión del riesgo en todos los procesos institucionales y en la toma de decisiones, promoviendo una cultura que considere el riesgo de manera sistemática y proactiva. La norma se estructura en tres componentes principales: los principios que orientan una gestión del riesgo sólida, el marco de trabajo que facilita su integración y mejora continua, y el proceso de gestión del riesgo que abarca la identificación, análisis, evaluación, tratamiento, monitoreo y comunicación del riesgo. Su flexibilidad permite adaptarla a distintos sectores y contextos, fortaleciendo la capacidad de las organizaciones para anticipar eventos, reducir incertidumbres y mejorar el desempeño.

Tabla 1

Comparativo COSO ERM 2017 – ISO 31000:2018

Criterio	COSO ERM 2017	ISO 3100:2018	Decisión
Estructura	5 componente, 20 principios	3 elementos (principios, marco, proceso)	COSO más granular para evaluación
Orientación Sectorial	Enfasis en gobierno corporativo y finanzas	Aplicable a cualquier sector	COSO más alineado al sector financiero
Operacionalización	Principios específicos evaluables	Directrices generales	COSO permite traducir a criterios medibles
Alineación regulatoria	Compatible con Basilea y SBS	Más genérico	COSO facilita integración normativa

Nota. Elaborado a partir de COSO, 2017 y ISO, 2018.

Tras analizar los modelos de gestión de riesgos, se seleccionó a COSO ERM 2017 como referencia principal para la construcción de la herramienta de evaluación del

nivel de madurez del riesgo operacional en empresas del sistema financiero. Esta decisión se fundamenta en que COSO ERM ofrece una estructura más granular compuesta por cinco componentes y veinte principios que permiten evaluar de forma integral y desagregada la gobernanza, la estrategia, la cultura de riesgos y el desempeño organizacional. Adicionalmente, su orientación hacia el sector financiero y su compatibilidad con marcos regulatorios como Basilea facilitan la integración con la normativa SBS, mientras que su nivel de especificidad permite traducir principios conceptuales en criterios medibles y verificables, aspecto fundamental para el diseño de un instrumento de autoevaluación operativo y comparable.

2.2 Gestión de riesgo operacional

A nivel internacional, el Acuerdo de Basilea II sentó las bases para la inclusión formal del riesgo operacional dentro de los requerimientos mínimos de capital de las entidades financieras. Este marco establece tres pilares que buscan fortalecer la solvencia y transparencia del sistema financiero: el requerimiento de capital, la supervisión y la disciplina de mercado. Dicho acuerdo define al riesgo operacional como "el riesgo de pérdida resultante de procesos internos inadecuados o fallidos, de las personas y sistemas, o de eventos externos. Esta definición, incluye el riesgo legal, pero excluye los riesgos estratégicos y de reputación." (BCBS, 2004, p. 149). Con ello, Basilea II impulsa la adopción de metodologías estandarizadas y promueve una cultura de gestión de riesgos empresariales orientada a la prevención y la resiliencia organizacional.

En el contexto peruano, la SBS ha incorporado y adaptado los lineamientos internacionales en materia de gestión del riesgo operacional mediante diversas normativas. Entre ellas destaca la ya mencionada Resolución N.º 2115-2009, que regula el requerimiento de patrimonio efectivo por riesgo operacional, la cual ha sido objeto de sucesivas actualizaciones, tales como las Resoluciones SBS N.º 5570-2019, N.º 3955-2022, N.º 2467-2023 y N.º 525-2024. Asimismo, la Resolución N.º 2116-2009, que tiene su origen en la Resolución SBS N.º 006-2002, establece el Reglamento para la Gestión del Riesgo Operacional, que fue modificada y complementada por normas posteriores, tales como las Resoluciones SBS N.º 877-2020, N.º 504-2021 y N.º 2429-2021. En conjunto, estas disposiciones normativas exigen que las entidades del sistema financiero cuenten con estructuras de control adecuadas y metodologías formalizadas para la gestión del riesgo operacional, incorporando la identificación y registro de eventos de pérdida, la implementación de planes de mitigación y la adopción de mecanismos de continuidad operativa que fortalezcan la resiliencia institucional frente a posibles interrupciones o contingencias.

2.3 Modelos de madurez

Entre los modelos de madurez más relevantes desarrollados por la OCDE destaca el Enterprise Risk Management (ERM) Maturity Model, parte de la serie Tax Administration Maturity Models (OECD, 2021). Este modelo propone cinco niveles evolutivos de madurez: Emergente, En Progreso, Establecido, Líder y Aspiracional, que permiten diagnosticar el grado de institucionalización de la gestión de riesgos dentro de una administración tributaria (OECD, 2021). La progresión inicia con un enfoque reactivo y poco estructurado (Emergente), avanza hacia la adopción de prácticas formales y mayor coordinación institucional (En Progreso y Establecido), y culmina en capacidades altamente integradas, basadas en datos y sostenidas por una

cultura madura de riesgos (Líder y Aspiracional) (OECD, 2021). La versión 2021 representa un avance significativo respecto de sus versiones anteriores ya que ha incorporado una mayor cantidad de datos de autoevaluación de 29 administraciones tributarias; ha introducido el concepto de “tolerancia al riesgo” como complemento al “apetito de riesgo” además de aumentar el énfasis en la tecnología, los datos y la cultura organizacional como factores de madurez avanzada. Todo esto evidencia una evolución desde un modelo centrado en estructuras básicas hacia un enfoque que integra estrategia organizacional, el uso de tecnologías de información y el intercambio sistemático de información para la toma de decisiones.

De manera complementaria, el Capability Maturity Model (CMM) desarrollado por el Software Engineering Institute (Paulk et al., 1993) presenta cinco niveles de evolución de capacidades, desde un nivel Inicial, caracterizado por prácticas reactivas y poco estructuradas, hasta un nivel Optimizado, centrado en la mejora continua. Con el tiempo, la necesidad de integrar diversas áreas organizacionales llevó a la creación del Capability Maturity Model Integration (CMMI), cuya versión más reciente, publicada por el CMMI Institute (2018), amplía el enfoque original incorporando prácticas más avanzadas y una visión transversal de procesos. El CMMI V2.0 mantiene cinco niveles de madurez: Inicial, Gestionado, Definido, Cuantitativamente Gestionado y Optimizado (CMMI Institute, 2018). Esta versión introduce una mayor orientación hacia la gestión basada en datos, el control cuantitativo del desempeño y la alineación con los objetivos estratégicos de la organización, fortaleciendo su aplicabilidad en distintos sectores más allá del desarrollo de software.

Finalmente, tras analizar los modelos de madurez, se identificó que ambos coinciden en una estructura evolutiva de cinco niveles, aunque con enfoques complementarios. Mientras el modelo de la OECD enfatiza la integración estratégica, cultural y organizacional de la gestión de riesgos, el CMMI aporta una perspectiva orientada a la estandarización, medición cuantitativa y mejora continua de procesos. Con base en esta complementariedad conceptual, se propone la construcción de un modelo híbrido de madurez que incorpora seis niveles (0 a 5), a diferencia de los cinco niveles de los modelos OECD y CMMI. La inclusión del Nivel 0 (Inmaduro) responde a la necesidad de capturar con precisión diagnóstica aquellas situaciones en las que una entidad carece por completo de prácticas formales, documentadas o sistematizadas en algún criterio específico de gestión de riesgo operacional. Si bien esta condición no debería presentarse de manera generalizada en entidades del sistema financiero regulado, su inclusión permite evitar forzar la clasificación de prácticas inexistentes dentro del Nivel 1 (Inicial), que ya presupone el reconocimiento de la necesidad de gestionar el riesgo y la existencia de esfuerzos incipientes, aunque informales. Esta distinción conceptual entre "ausencia total" (Nivel 0) y "reconocimiento con prácticas incipientes" (Nivel 1) aumenta la sensibilidad del instrumento, facilita la identificación de brechas críticas por principio, y permite trazar con mayor precisión la trayectoria de mejora desde la situación inicial hasta niveles de madurez consolidados.

Esta estructura busca ofrecer una evaluación más precisa y contextualizada para organizaciones del sistema financiero, manteniendo coherencia con los estándares internacionales. Los niveles propuestos son: Nivel 0 (Inmaduro), Nivel 1 (Inicial), Nivel 2 (En Progreso), Nivel 3 (Definido), Nivel 4 (Gestionado) y Nivel 5 (Optimizado).

2.4 Integración conceptual de los marcos de referencia

La propuesta de investigación se sustenta en la complementariedad estratégica de tres marcos de referencia que, si bien tienen origen y propósitos distintos, convergen en la necesidad de evaluar el grado de desarrollo institucional en la gestión del riesgo operacional. COSO ERM 2017 aporta la estructura de evaluación, organizando el análisis en cinco componentes (Gobierno y Cultura; Estrategia y Establecimiento de Objetivos; Desempeño; Revisión y Monitoreo; Información, Comunicación y Reporte) y veinte principios que permiten desagregar dimensiones clave de la gestión de riesgos. Esta estructura proporciona el "armazón" conceptual sobre el cual se construye la herramienta. Los lineamientos de Basilea II (BCBS, 2004, 2011, 2021) y la normativa de la SBS, en particular la Resolución SBS 2115-2009, la Resolución SBS 2116-2009 y sus modificatorias, aportan el contenido específico de riesgo operacional: requisitos mínimos, prácticas esperadas, definiciones técnicas y criterios de cumplimiento aplicables al sistema financiero peruano. Estos marcos normativos permiten "llenar" los principios de COSO ERM con contenidos verificables y trazables a regulación vigente. Finalmente, los modelos de madurez de la OCDE (2021) y CMMI Institute (2018) aportan la lógica evolutiva, es decir, la progresión por niveles que diferencia entre prácticas inexistentes, incipientes, formalizadas, gestionadas y optimizadas. Esta perspectiva permite transformar el instrumento de una evaluación binaria de cumplimiento (sí/no) a un diagnóstico gradual de desarrollo institucional. La integración de estos tres elementos constituye el fundamento metodológico de la herramienta propuesta: la estructura de COSO ERM define qué evaluar, la normativa de Basilea y SBS define qué esperar en cada principio, y los modelos de madurez definen cómo medir el grado de avance. Esta articulación permite construir un instrumento que no solo verifica el cumplimiento formal de requisitos regulatorios, sino que diagnostica el nivel de institucionalización, consistencia y efectividad de las prácticas de gestión de riesgo operacional, facilitando así la identificación de brechas específicas y la priorización de mejoras según el nivel de desarrollo actual de cada entidad.En síntesis, los marcos internacionales como Basilea II y COSO ERM 2017, normativas regulatorias de la SBS y modelos de madurez, son independientes y aislados entre sí. En ese sentido, no se identificaron, en la literatura académica y normativa revisada, herramientas específicas para evaluar la madurez del riesgo operacional que integren estos marcos y se encuentren contextualizadas al sistema financiero peruano. En consecuencia, las entidades del sistema financiero carecen de una herramienta que facilite medir su grado de madurez y orientar la mejora continua en la gestión de riesgo operacional.

A partir de ello, se plantean las siguientes proposiciones (P) que sustentan la relevancia y pertinencia del estudio:

- P1. Si se identifican los principios y criterios clave de la madurez en la gestión de riesgo operacional, es posible estructurar una propuesta que, de ser puesta en práctica, podría eventualmente reflejar los niveles de madurez existentes en las entidades financieras.
- P2. La revisión de las normas internacionales y locales permitiría construir una propuesta basada en un instrumento contextualizado y técnicamente sólido.
- P3. Si la propuesta establece un diseño claro en la construcción de la herramienta, una vez aplicada, facilitará la evaluación del nivel de madurez en la gestión del riesgo operacional dentro del sistema financiero.

3. Metodología del estudio

El estudio es de carácter aplicativo con enfoque documental-analítico, cuyo propósito es diseñar una herramienta que permita evaluar el nivel de madurez de la gestión del riesgo operacional en entidades del sistema financiero peruano (en adelante, **herramienta**). No se contempla la validación empírica ni la aplicación en campo, dado que el objetivo se centra en la construcción conceptual y metodológica de un instrumento sólido y contextualizado. El estudio considera únicamente documentos emitidos y vigentes al 31.12.2025.

La herramienta consiste en realizar un diagnóstico en formato de **cuestionario** que integra cuatro (4) elementos clave: i) **contenido**, unidad normativa (artículo o literal) o técnica trazable (principio o numeral) que expresa un requisito o práctica, ii) **criterio**, aspecto evaluado formulado como pregunta, iii) **madurez**, estado que mejor refleja el estado alcanzado por la entidad frente al criterio, con seis niveles, iv) **calificación**, resultado numérico obtenido por media aritmética según el procedimiento descrito en el punto 3.2.

Los **criterios** se organizan con la estructura del modelo de gestión de riesgos COSO ERM 2017 (componentes y principios) y se diseñan metodológicamente a través de un análisis documental y normativo, cuyo procedimiento comprende cuatro fases secuenciales que parten desde la selección rigurosa de fuentes normativas, continúan con la extracción y sistematización de **contenidos**, avanzan hacia la redacción de criterios alineados a los componentes y principios de COSO ERM, y culminan con la síntesis en la herramienta mediante la definición de **criterios** y niveles de **madurez**, cuyas reglas de agregación se establecen a través de una **calificación** calculada por media aritmética.

Los componentes y principios de COSO se adecuaron al contexto de riesgo operacional en el sistema financiero peruano, cuya descripción se señala en la Tabla 2 y se detallan en el Apéndice A:

Tabla 2
Principios de COSO ERM contextualizados.

Componente	Principio
1. Gobierno y Cultura	1. Ejerce la supervisión de riesgos a través del Directorio
	2. Establece estructuras operativas
	3. Define la cultura deseada
	4. Demuestra compromiso con los valores clave
	5. Atrae, desarrolla y retiene a profesionales capacitados
2. Estrategia y Establecimiento de Objetivos	6. Analiza el contexto empresarial
	7. Define el apetito al riesgo operacional
	8. Evalúa estrategias alternativas
	9. Formula objetivos de negocio
3. Desempeño	10. Identifica los riesgos operacionales
	11. Evalúa la severidad de los riesgos operacionales
	12. Prioriza riesgos operacionales
	13. Implementa respuestas ante los riesgos operacionales
	14. Desarrolla una visión a nivel de portafolio
4. Revisión y monitoreo	15. Evalúa los cambios sustantivos
	16. Revisa el riesgo operacional y su desempeño
	17. Persigue la mejora de la gestión del riesgo operacional
	18. Aprovecha la información y la tecnología

Componente	Principio
5. Información, Comunicación y Reporte	19. Comunica información sobre riesgos operacionales
	20. Informa sobre el riesgo operacional, la cultura y el desempeño

Nota. Adaptado de "Enterprise Risk Management—Integrating with Strategy and Performance", por el COSO, 2017 (https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance.pdf).

3.1 Procedimiento de análisis

3.1.1 Recopilación documental y normativa

Conformada principalmente por documentos emitidos por organismos internacionales como el BCBS y la normativa de la SBS.

Se establecieron criterios de inclusión, tales como: vigencia al 31.12.2025, documentos oficiales o reconocidos internacionalmente y aporte a la investigación. Se documenta: Fuente, año de publicación, título de documento y cumplimiento de criterios de inclusión.

La búsqueda y selección de documentos se llevó a cabo de manera sistemática en bases de datos como Compendio de normas SBS[3], Publicaciones BCBS[4], con ecuaciones de búsqueda en español e inglés de las siguientes palabras clave: *operational risk management, maturity model, internal control, and financial institutions.* En esa línea, se recuperaron 23 documentos, se excluyeron dieciséis (16) debido a que no cumplieron con los criterios de inclusión o porque correspondian a modificaciones de los documentos base, y como resultado quedaron siete (7) documentos.

3.1.2 Extracción de datos

Se utiliza una matriz de extracción (Excel) para registrar de forma ordenada los siete (7) documentos de la fase anterior, cuyos campos mínimos, adicionales al paso 3.1.1, son: estado de acceso (descargado, pendiente o restringido), ubicación (físico o digital), asociación preliminar a los componentes de COSO ERM, elementos clave, tipo de referencia respecto a nivel de madurez (implícita o explícita).

3.1.3 Categorización de datos

Se realizó un análisis de contenido cuyos hallazgos se ordenaron por los 20 principios de COSO ERM. Se permitió mapeos de uno o muchos principios cuando la literalidad lo respaldaba. Cuando hubo discrepancias en el mapeo, se resolvieron por consenso y se registró la decisión en una bitácora; la evidencia se sustenta en cita literal.

Por ejemplo, como resultado del análisis del contenido, se identificó que el numeral 14 del principio 1 del documento emitido por elBasel Committee on Banking Supervision, *Revisions to the Principles for the Sound Management of Operational Risk* (BCBS,

[3] https://www.sbs.gob.pe/app/pp/INT_CN/Paginas/Busqueda/BusquedaPortal.aspx
[4] https://www.bis.org/bcbs/publications.htm

2021a), se relacionó con, al menos, dos principios: “2. Establece estructuras operativas” y “3. Define cultura deseada”.

3.1.4 Síntesis y construcción de herramienta

Se analizaron los contenidos asociados a los 20 principios de COSO ERM y se redactaron criterios con base en su literalidad empleando el juicio de experto de los investigadores y las siguientes reglas: i) describir una condición observable, ii) enfocarse en qué se evalúa y no en cómo, iii) mutuamente excluyentes, iv) colectivamente exhaustivos, y v) procurar el uso de terminología alineada a la regulación peruana aplicable al sistema financiero.

Adicionalmente, se consideró determinar una cantidad máxima de criterios por principio en base a la cantidad de contenidos aplicables, con la finalidad de asegurar el equilibrio entre la cobertura normativa, la granularidad evaluativa, y la viabilidad operativa. En consecuencia, la cantidad máxima de criterios totales será de 60 (ver Tabla 4) y los rangos por principio se muestran en la Tabla 3.

Tabla 3
Rangos para determinar el número de criterios por principio.

Nº de rango	Rango	Nº máximo de criterios por principio
1	De 1 a 20	2
2	De 21 a 40	3
3	De 41 a 60	4
4	De 61 a 80	5
5	Más de 81	6

Luego, se redactaron preguntas y respuestas que permitieron identificar el nivel de madurez, las cuales se consolidaron en un cuestionario que por cada criterio incorpora 6 opciones asociadas a diferentes niveles de madurez.

Por ejemplo, como resultado de la integración se identificó que el principio “*1. Ejerce la supervisión de riesgos a través del Directorio*” se relaciona con 27 contenidos, por lo tanto, se encuentra en el rango 2 y le corresponden 3 criterios, los cuales son “*1.1 Aprobación de Manual de GRO*”, “*1.2 Apetito, tolerancia y límites de RO*” y “*1.3 Implementación del sistema de GRO*”.

3.2 Reglas de calificación y agregación

Como se describió en la sección 2.4, la herramienta integra la estructura de COSO ERM, el contenido normativo de Basilea y SBS, y la lógica evolutiva de modelos de madurez. Esta integración se operacionaliza mediante un sistema de calificación que traduce la evaluación cualitativa de cada criterio en valores numéricos (0 a 5), permitiendo agregación por niveles jerárquicos y comparabilidad entre principios, componentes y entidades.

La **calificación** prescinde de ponderaciones y se basa exclusivamente en medias aritméticas redondeadas por defecto a cero dígitos. Al eliminar ponderaciones, cada criterio aporta el mismo peso dentro de su principio, cada principio aporta el mismo peso

dentro de su componente, y cada componente aporta el mismo peso a la calificación global. Por otro lado, el redondeo por defecto a cero dígitos genera un resultado conservador y reduce la posibilidad de que la madurez pueda ser percibida con un nivel que aún no ha alcanzado.

3.3 Herramientas y control de calidad

El trabajo se realizó en Microsoft Excel, utilizando validaciones (listas controladas, protección de celdas y control de cambios). Se ejecutaron chequeos automáticos de consistencia y revisión cruzada entre los tres investigadores para asegurar la coherencia entre la cita literal y la formulación del criterio.

3.4 Consideraciones éticas y limitaciones

Se empleó información pública, no se evaluaron entidades específicas. Al tratarse de un diseño teórico, la herramienta propuesta evalúa el nivel de madurez del diseño e implementación formal de la gestión del riesgo operacional, a partir de evidencia documental y prácticas institucionalizadas, y no la efectividad real ni el desempeño operativo de los controles en funcionamiento. La interpretación en mapeos uno a muchos se acota mediante cita literal y reglas explícitas de resolución.

3.5 Productos de salida

1. Cuestionario con criterios y niveles de madurez.
2. Matriz de trazabilidad entre contenido de documentos y criterios.
3. Libro de cálculo con calificaciones individuales y agregadas.

4. Resultados

4.1 Arquitectura de la herramienta

Como resultado del procedimiento de análisis, se identificaron 60 criterios evaluables, contados en la Tabla 4 y descritos en el Apéndice B, los cuales se encuentran relacionados a los 20 principios y 5 componentes:

Tabla 4
Número de criterios definidos por principio.

Componente	Principio	Nº de criterios
1. Gobierno y Cultura	1. Ejerce la supervisión de riesgos a través del Directorio	3
	2. Establece estructuras operativas	4
	3. Define la cultura deseada	2
	4. Demuestra compromiso con los valores clave	2
	5. Atrae, desarrolla y retiene a profesionales capacitados	3
	6. Analiza el contexto empresarial	2
	7. Define el apetito al riesgo operacional	3

Componente	Principio	Nº de criterios
2. Estrategia y Establecimiento de Objetivos	8. Evalúa estrategias alternativas	2
	9. Formula objetivos de negocio	2
3. Desempeño	10. Identifica los riesgos operacionales	6
	11. Evalúa la severidad de los riesgos operacionales	4
	12. Prioriza riesgos operacionales	3
	13. Implementa respuestas ante los riesgos operacionales	4
	14. Desarrolla una visión a nivel de portafolio	4
4. Revisión y monitoreo	15. Evalúa los cambios sustantivos	3
	16. Revisa el riesgo operacional y su desempeño	3
	17. Persigue la mejora de la gestión del riesgo operacional	3
5. Información, Comunicación y Reporte	18. Aprovecha la información y la tecnología	2
	19. Comunica información sobre riesgos operacionales	2
	20. Informa sobre el riesgo operacional, la cultura y el desempeño	3

Nota. ~~Elaborado a partir~~Adaptado de COSO, 2017, "Enterprise Risk Management—Integrating with Strategy and Performance~~.~~", COSO, 2017 (https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance.pdf)**.**

4.2 Modelo de madurez

Se definió un modelo de madurez que consta de 6 escalas, las cuales muestran en la Tabla 5 los estadios del nivel de madurez, desde "inmadura" hasta "optimizado", se listan ejemplos en el Apéndice C:

Tabla 5
Modelos de madurez definidos para la herramienta.

Nivel de madurez	Descripción
0 - Inmadura	No cuenta con prácticas formales ni sistematizadas de gestión del riesgo operacional.
1 - Inicial	Se reconoce la necesidad de gestionar el riesgo operacional, pero las prácticas son incipientes, informales y poco consistentes.
2 - En progreso	Existe avance hacia la formalización de prácticas básicas.
3 - Definido	La gestión del riesgo operacional cuenta con procesos formalizados, documentados y aplicados de manera consistente.
4 - Gestionado	La gestión está consolidada y apoyada en datos, métricas e indicadores.

Nivel de madurez	Descripción
5 - Optimizado	La gestión es avanzada, con enfoque en la mejora continua e innovación.

Nota. Elaborado a partir de OECD (2021) y del CMMI Institute (2018).

4.3 Reglas de calificación

La calificación se realiza sin ponderaciones y se construye de manera jerárquica en cuatro niveles: criterio, principio, componente, y global. En todos los casos se emplea la media aritmética simple y el resultado se redondea por defecto (hacia abajo) a cero decimales, manteniendo un enfoque conservador, al evitar fracciones que podrían elevar la calificación y reduce el riesgo de interpretar que se alcanzó un nivel de madurez que aún no se consolida.

4.3.1 Calificación de criterios

Corresponde a la entrada del modelo. Cada criterio **c** recibe una calificación $\mathbf{x_c}$ correspondiente a un nivel de madurez en el rango 0 a 5:

$$\mathbf{x_c} \in \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}\}$$

4.3.2 Calificación de principios

Para cada principio p, con n_p criterios asociados, la calificación del principio se calcula como el promedio simple de sus criterios y luego se redondea por defecto a cero decimales:

$$S_p = \left\lfloor \frac{\sum_{c=1}^{n_p} X_c}{n_p} \right\rfloor$$

Donde:

- S_p= calificación del principio p
- x_c= calificación del criterio c del principio p
- n_p= número de criterios del principio p
- $\lfloor \cdot \rfloor$= redondeo por defecto (hacia abajo)

4.3.3 Calificación de componentes

Para cada componente k, con m_k principios, la calificación del componente se calcula como el promedio simple de las calificaciones de sus principios y se redondea por defecto a cero decimales:

$$C_k = \left\lfloor \frac{\sum_{p=1}^{m_k} S_p}{m_k} \right\rfloor$$

Donde:

- C_k= calificación del componente k
- S_p= calificación del principio pdel componente k
- m_k= número de principios del componente k

4.3.4 Calificación global

Finalmente, con K componentes ($K = 5$), el índice global se obtiene como el promedio simple de los componentes, redondeado por defecto a cero decimales:

$$G = \left\lfloor \frac{\sum_{k=1}^{K} C_k}{K} \right\rfloor$$

Donde:

- G= índice global de madurez
- C_k= calificación del componente k
- K= número total de componentes

4.4 Operacionalización de la herramienta

La herramienta se aplica bajo un enfoque de autoevaluación estandarizada, en el cual la propia entidad valora su nivel de madurez para cada criterio utilizando evidencia verificable. La autoevaluación inicia con la revisión integral del cuestionario, conformado por 60 criterios formulados como preguntas y una escala de respuesta de seis niveles (0 a 5) el detalle se encuentra en el Apéndice D. La entidad recopila y organiza evidencia general que sustente cada respuesta, privilegiando documentos y registros que demuestren existencia, aplicación y seguimiento de prácticas, sin depender únicamente de declaraciones.

A continuación, la entidad asigna un nivel de madurez a cada criterio seleccionando la opción que mejor represente su situación actual. Para asegurar trazabilidad, por cada criterio se registra el nivel asignado, una justificación breve y una referencia a la evidencia que respalda la decisión. Cuando la evidencia sea insuficiente, inconsistente o no permita verificar el grado de implementación, se aplica un enfoque prudente, asignando el nivel inferior compatible con lo observado.

Concluida la calificación, la herramienta consolida los resultados mediante medias aritméticas sucesivas y sin ponderaciones: se calcula el promedio de criterios por principio, luego el promedio de principios por componente y, finalmente, el promedio de componentes para obtener el índice global. Los puntajes se expresan con redondeo por defecto a cero decimales, manteniendo un criterio conservador.

El resultado de la autoevaluación se presenta como un conjunto de puntajes desagregados por criterio, principio y componente, además del puntaje global. Esto permite identificar brechas de madurez de forma comparable dentro de la entidad y establecer una línea base para mediciones posteriores, orientadas al seguimiento de avances en el tiempo bajo una metodología consistente.

5. Discusión

Los resultados de esta investigación confirman que es viable traducir el enfoque de COSO ERM 2017 a criterios verificables para evaluar la madurez de la gestión del riesgo operacional en entidades del sistema financiero peruano, atendiendo así la brecha metodológica identificada en la revisión de literatura: la ausencia de instrumentos que integren marcos conceptuales reconocidos con normativas regulatorias específicas y que permitan autoevaluación sistemática y comparable.

La discusión confirma que es viable traducir el enfoque de COSO ERM 2017 a criterios verificables para evaluar la madurez de la gestión del riesgo operacional en entidades del sistema financiero peruano, sin perder la lógica de componentes y principios. La consistencia del instrumento se fortalece al integrar, como insumos, referentes internacionales de buenas prácticas en riesgo operacional y exigencias regulatorias aplicables en el Perú. En conjunto, esta articulación permite evaluar no solo la existencia de lineamientos, sino también elementos clave de implementación, tales como responsabilidades, identificación y evaluación de riesgos, monitoreo, reporte para la toma de decisiones y mejora continua. En particular, el instrumento cubre con mayor solidez aquellos ámbitos donde los marcos convergen de manera natural: gobierno, procesos de evaluación, seguimiento del desempeño del control y mecanismos de información para la gestión. Estos hallazgos coinciden con la literatura que sostiene que los modelos de madurez aportan una lectura evolutiva del desempeño y permiten priorizar brechas de manera progresiva; sin embargo, difieren de enfoques centrados en listas de verificación, dado que el presente trabajo prioriza el desarrollo gradual por niveles antes que una evaluación binaria de cumplimiento.

Los hallazgos de esta investigación convergen con esfuerzos recientes por desarrollar criterios de madurez en gestión de riesgo operacional. Van der Westhuizen (2025) identificó 30 criterios para evaluar madurez organizacional ante eventos de riesgo operacional, con énfasis a la pandemia de COVID-19. El presente estudio se diferencia sustancialmente al: (i) integrar explícitamente la estructura de COSO ERM 2017 como marco organizador, (ii) incorporar contenidos trazables de Basilea II y normativa SBS, contextualizando la evaluación al sistema financiero peruano, (iii) establecer una metodología formal de agregación con reglas claras de calificación que permite comparabilidad entre entidades, y (iv) operacionalizar seis niveles de madurez con descriptores específicos. Mientras que Van der Westhuizen aporta criterios valiosos para evaluación general, este instrumento los operacionaliza en un marco integrado, regulatoriamente alineado y metodológicamente estandarizado, facilitando su aplicación práctica como herramienta de autoevaluación y seguimiento en el sistema financiero peruano. Investigaciones futuras podrían explorar la complementariedad entre ambos enfoques, evaluando si la integración de criterios adicionales enriquecería la cobertura del instrumento sin comprometer su operabilidad.

Una fortaleza central del enfoque propuesto es su simplicidad operativa y trazabilidad. La definición de niveles de madurez de 0 a 5 permite diferenciar estados desde prácticas incipientes hasta prácticas optimizadas, lo que incrementa la utilidad diagnóstica frente a esquemas dicotómicos. Asimismo, el uso de promedios aritméticos sin ponderaciones favorece la comparabilidad entre entidades y en el tiempo, y reduce la discrecionalidad asociada a la asignación de pesos. No obstante, esta decisión implica compensaciones: la ausencia de ponderaciones puede subestimar la criticidad de ciertos criterios o principios que condicionan el desempeño global del marco, y la agregación por promedios puede diluir debilidades relevantes si existen fortalezas en otros criterios del mismo principio o componente. En términos prácticos, el instrumento resulta adecuado para construir una

línea base y comparar perfiles de madurez, pero podría requerir reglas complementarias cuando se busque orientar decisiones de priorización o seguimiento focalizado, por ejemplo, mediante umbrales mínimos por principio o la identificación explícita de debilidades críticas.

Entre las principales limitaciones del instrumento destaca la ausencia de validación empírica. En consecuencia, aún no se cuenta con evidencia suficiente para afirmar que los puntajes obtenidos reflejan de manera consistente la madurez real en operación ni que sean estables entre distintos evaluadores. Otra limitación proviene de la dependencia documental: aun cuando los criterios procuran ser observables, su aplicación puede sesgarse hacia evidencia formal, favoreciendo a entidades con mayor capacidad de documentación sin que ello garantice efectividad en la práctica. Este riesgo de evaluación basada en "papel" es especialmente relevante en riesgo operacional, donde la evidencia de funcionamiento y resultados es determinante. Adicionalmente, la traducción de contenidos normativos y buenas prácticas a criterios puede generar solapamientos o diferencias en el nivel de exigencia entre principios, lo que exige depuración para mejorar la precisión del instrumento. Finalmente, el redondeo conservador, si bien prudente, podría reducir la sensibilidad para capturar avances marginales, aspecto que debe valorarse según el uso previsto.

De cara al trabajo futuro, resulta prioritario realizar una revisión experta para ajustar redacción, eliminar ambigüedades y precisar evidencia mínima por nivel de madurez. Posteriormente, un piloto con entidades de distinta complejidad permitiría evaluar aplicabilidad, carga de levantamiento de información y capacidad discriminante de los criterios. También se recomienda medir la consistencia entre evaluadores y definir reglas de aplicación que estandaricen el tratamiento de evidencia parcial y criterios de suficiencia. Para mitigar el efecto de dilución por promedios, es pertinente explorar ajustes que mantengan comparabilidad, como umbrales mínimos por principio o criterios habilitantes, complementando el puntaje agregado con señales explícitas sobre debilidades críticas. En conjunto, estas acciones permitirían consolidar el instrumento como una base robusta para diagnóstico, comparación y seguimiento de la madurez en la gestión del riesgo operacional.

6. Conclusiones

1. Se desarrolló una herramienta de evaluación de madurez aplicable al sistema financiero peruano, estructurada en torno a los 5 componentes y 20 principios de COSO ERM 2017, y traducida a criterios observables para valorar el grado de desarrollo de la gestión del riesgo operacional en entidades supervisadas por la SBS. La herramienta permite un diagnóstico consistente en múltiples entidades, sin depender exclusivamente de la revisión narrativa de políticas o descripciones generales.
2. La herramienta integra referentes internacionales y exigencias locales, al articular COSO ERM con buenas prácticas y lineamientos relevantes para riesgo operacional y con el marco regulatorio peruano aplicable. Esta integración favorece que el instrumento sea útil tanto para gestión interna (autoevaluación) como para fines de supervisión (diagnóstico comparativo y seguimiento).
3. El enfoque de madurez por niveles (0 - 5) habilita una lectura evolutiva del desempeño, diferenciando entre implementación incipiente, ejecución consistente, estandarización y optimización. Esto aporta mayor valor que una

evaluación binaria de cumplimiento, ya que permite identificar brechas graduales y priorizar mejoras con una ruta de progresión.

4. La calificación basada en medias aritméticas sin ponderaciones prioriza simplicidad, trazabilidad y comparabilidad, reduciendo arbitrariedad y facilitando la replicabilidad del resultado entre evaluadores. Asimismo, el redondeo conservador refuerza el principio de prudencia al evitar clasificaciones optimistas cuando la evidencia aún no es suficiente.
5. El producto desarrollado es metodológicamente útil, pero requiere validación empírica para su consolidación. Al basarse en análisis documental y en una traducción de fuentes a criterios evaluables, el instrumento necesita pruebas de confiabilidad (consistencia entre evaluadores) y validez (capacidad de medir efectivamente la madurez) antes de recomendar su uso como referencia estándar.
6. La herramienta propuesta responde a una necesidad concreta del sistema financiero peruano, donde solo el 21% de las entidades han logrado acreditar niveles de madurez suficientes para utilizar el método ASA, y donde la ausencia de instrumentos estandarizados de autoevaluación limita la capacidad de las entidades para identificar brechas específicas antes de que se materialicen en pérdidas. Al integrar COSO ERM, Basilea y normativa SBS en un instrumento operacionalizado con criterios medibles, niveles de madurez y reglas de agregación transparentes, la herramienta permite a las entidades: (i) establecer una línea base comparable de su nivel de madurez, (ii) identificar debilidades por componente o principio de manera trazable, (iii) demostrar ante la supervisión avances tangibles en el fortalecimiento de su gestión de riesgo operacional, y (iv) priorizar recursos y esfuerzos de mejora con base en evidencia objetiva de brechas estructurales.

7. Referencias

Basel Committee on Banking Supervision. (2004). *International convergence of capital measurement and capital standards: A revised framework* (Basel II). Bank for International Settlements. www.bis.org/publ/bcbs107.pdf

Basel Committee on Banking Supervision. (2011a). *Operational risk – Supervisory guidelines for the advanced measurement approaches*. Bank for International Settlements. https://www.bis.org/publ/bcbs196.pdf

Basel Committee on Banking Supervision. (2011b). *Principles for the sound management of operational risk.* Bank for International Settlements. www.bis.org/publ/bcbs195.pdf

Basel Committee on Banking Supervision. (2021a). *Revisions to the principles for the sound management of operational risk (BCBS D515).* Bank for International Settlements. https://www.bis.org/bcbs/publ/d515.pdf

Basel Committee on Banking Supervision. (2021b). *Principles for operational resilience*. Bank for International Settlements. www.bis.org/bcbs/publ/d516.pdf

Capability Maturity Model Integration Institute. (2018). *CMMI for development,* version 2.0. ISACA.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *Enterprise risk management - Integrating with strategy and performance.* AICPA.

Deloitte. (2024, 14 de diciembre). *Basel final rules: Takeaways and highlights for US banks.* Deloitte. Recuperado de https://www2.deloitte.com/us/en/pages/risk/articles/basel-final-rules-takeaways-highlights-us-banks.htmlRecuperado el 15 de julio del 2025, de https://www2.deloitte.com/us/en/pages/risk/articles/basel-final-rules-takeaways-highlights-us-banks.html

Ernst & Young (2025, enero). *Operational risk: Proactively controlling the unavoidable.* EY. https://www.ey.com/content/dam/ey-unified-site/ey-com/en-uk/industries/banking-capital-markets/documents/ey-uk-operational-risk-01-2025.pdf

Gutierrez Alayo, J., Necochea Mendoza, P., Armas-Aguirre, J., & Madrid Molina, J. (2021). *Cybersecurity maturity model for providing services in the financial sector in Peru* [Conferencia]. Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI), Bogotá, Colombia. https://ieeexplore.ieee.org/document/9619733

International Organization for Standardization. (2018). *Risk management -Guidelines* (Norma ISO 31000:2018). https://www.iso.org/standard/65694.html

KPMG. (2017). *Operational risk management framework.* World Bank Group.

Lee, G., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2024). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *The Electronic Journal of Information Systems in Developing Countries*, e12350. https://doi.org/10.1002/isd2.12350

Ncontracts. (2024). *Enterprise risk management 101: COSO.* Ncontracts. Recuperado el 15 de julio del 2025, de https://www.ncontracts.com/nsight-blog/erm-101-whats-coso-and-why-should-i-care

Office of the Superintendent of Financial Institutions Canada. (2024). *Operational risk management and resilience guideline.* OSFI. Recuperado el 15 de julio del 2025, de https://www.osfi-bsif.gc.ca/en/guidance/guidance-library/operational-risk-management-resilience-guideline

Organisation for Economic Co-operation and Development. (2021). *ERM maturity model for tax administrations.* OECD Publishing. Recuperado el 15 de julio del 2025, de https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/enterprise-risk-management-maturity-model.pdf

Organización Internacional de Normalización. (2018). *Gestión del riesgo — Directrices* (Norma ISO No. 31000:2018). https://www.iso.org/standard/65694.html

Paulk, M. C., Curtis, B., Chrissis, M. B., & Weber, C. V. (1993). *Capability maturity model for software (Version 1.1).* Software Engineering Institute, Carnegie Mellon University. Recuperado el 15 de julio del 2025, de https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11955

Porrúa, M., Moncayo, G., Paz, S., Nowersztern, A., Bejarano, J. F., Baudino, M. F., Bordese, M. P., Barret, K., Baena, C. E., Jaramillo, M., Garces, O., & Isidro, A. (2025). *2025 cybersecurity report: Vulnerability and maturity challenges to bridging the gaps in Latin America and the Caribbean.* IDB-OEA https://publications.iadb.org/en/2025-cybersecurity-report-vulnerability-and-maturity-challenges-bridging-gaps-latin-america-and

Organisation for Economic Co-operation and Development. (2021). *ERM maturity model for tax administrations.* OECD Publishing. Recuperado de https://www.oecd.org/content/dam/oecd/en/topics/policy-issues/tax-administration/enterprise-risk-management-maturity-model.pdf

Resolución SBS 2115-2009. (2009). Aprueban el Reglamento para el requerimiento de patrimonio efectivo por riesgo operacional. Superintendencia de Banca, Seguros y AFP del Perú.

Resolución SBS 2116-2009. (2009). Aprueban el Reglamento para la gestión del riesgo operacional. Superintendencia de Banca, Seguros y AFP del Perú.

Superintendencia de Banca, Seguros y AFP. (s.f.). *Sistema financiero* [Estadísticas]. Recuperado el 17 de enero de 2026, de https://www.sbs.gob.pe/estadisticas-y-publicaciones/estadisticas-/sistema-financiero

UpGuard. (2025). *Effective risk management: The COSO ERM framework.* UpGuard. Recuperado el 1 de diciembre de 2025 de https://www.upguard.com/blog/coso-erm-framework

Van der Westhuizen, E. (2025). Navigating operational risk: Developing criteria for operational risk management maturity in the wake of COVID-19. *Journal of Governance Risk Management Compliance and Sustainability*, 5(1), 41–54. https://doi.org/10.31098/jgrcs.v5i1.2665

Apéndice A

Descripción de principios adecuados

Componente	Principio	Descripción del principio
1. Gobierno y Cultura	1. Ejerce la supervisión de riesgos a través del Directorio	El Directorio asume la responsabilidad final sobre la gestión de riesgo operacional. Define el *tono desde arriba*, supervisa la efectividad del sistema de gestión del riesgo operacional y exige rendición de cuentas a la Alta Gerencia respecto a decisiones, controles y resultados.
1. Gobierno y Cultura	2. Establece estructuras operativas	La Alta Gerencia diseña y sostiene estructuras de gobierno y de gestión (comités, funciones, líneas de reporte) que permitan aplicar la gestión del riesgo operacional de manera integrada y consistente**.** Define roles y responsabilidades alineadas a un enfoque de tres líneas**.**
1. Gobierno y Cultura	3. Define la cultura deseada	El Directorio y la Alta Gerencia establecen explícitamente la cultura de riesgo operacional esperada: valores, comportamientos y criterios que orientan cómo se identifican, comunican y gestionan los riesgos operacionales. La cultura debe ser coherente con el apetito, tolerancia y límites.
1. Gobierno y Cultura	4. Demuestra compromiso con los valores clave	La organización refuerza la ética, integridad y transparencia mediante mecanismos concretos (p. ej., código de conducta, sistema de incentivos, programa de formación asociadas a riesgo operacional) para prevenir conductas que incrementen la exposición al riesgo operacional.
1. Gobierno y Cultura	5. Atrae, desarrolla y retiene a profesionales capacitados	La Alta Gerencia asegura que la organización cuente con talento competente para gestionar riesgos operacionales: perfiles, formación, continuidad en roles críticos y capacidades técnicas para aplicar la metodología de RO de manera sostenible.
2. Estrategia y Establecimiento de Objetivos	6. Analiza el contexto empresarial	La Alta Gerencia evalúa el contexto interno y externo (regulatorio, económico, tecnológico, mercado y terceros) para anticipar impactos en la estrategia, en los procesos críticos y en el perfil de riesgo operacional**.**
2. Estrategia y Establecimiento de Objetivos	7. Define el apetito al riesgo operacional	El Directorio, con soporte de la Alta Gerencia, establece una declaración formal de apetito, tolerancia y límites de riesgo operacional. Define el nivel y tipo de exposición aceptable para alcanzar objetivos estratégicos, en coherencia con la capacidad real de gestión y control.
2. Estrategia y Establecimiento de Objetivos	8. Evalúa estrategias alternativas	La Alta Gerencia compara alternativas estratégicas incorporando explícitamente el balance entre retorno y exposición al riesgo operacional. Evalúa compromisos, controles necesarios y coherencia con apetito y tolerancias antes de ejecutar decisiones relevantes.
2. Estrategia y Establecimiento de Objetivos	9. Formula objetivos de negocio	La organización traduce la estrategia en objetivos claros y medibles, asegurando que dichos objetivos sean consistentes con el apetito y el perfil de RO, e integren riesgos operacionales y oportunidades que pueden afectar el desempeño.

Componente	Principio	Descripción del principio
3. Desempeño	10. Identifica los riesgos operacionales	La organización identifica riesgos operacionales asociados a procesos, productos, sistemas, NPCI y terceros, considerando eventos internos y externos. Se apoya en herramientas como autoevaluaciones, registros de eventos y pérdidas (BDEP) y análisis de cambios relevantes.
3. Desempeño	11. Evalúa la severidad de los riesgos operacionales	La organización evalúa la severidad del riesgo operacional estimando probabilidad e impacto (financiero y no financiero). Considera riesgo inherente, efectividad de controles y riesgo residual para determinar su importancia relativa y necesidad de tratamiento.
3. Desempeño	12. Prioriza riesgos operacionales	La organización prioriza los riesgos en función de severidad, apetito y tolerancia, interdependencias y capacidad de control. Esto permite enfocar recursos en los riesgos operacionales más relevantes y gestionar concentraciones o recurrencias.
3. Desempeño	13. Implementa respuestas ante los riesgos operacionales	La entidad define e implementa respuestas al riesgo operacional (aceptar, reducir, evitar o transferir) coherentes con el apetito y la estrategia. Establece planes de acción con responsables, plazos, recursos y seguimiento trazable.
3. Desempeño	14. Desarrolla una visión a nivel de portafolio	La función de la unidad de riesgos consolida una visión integral del riesgo operacional a nivel entidad (portafolio), integrando KRIs, eventos y pérdidas (BDEP), tendencias y concentraciones. Permite comprender el riesgo “de punta a punta”, evitando silos y evaluando impactos agregados.
4. Revisión y monitoreo	15. Evalúa los cambios sustantivos	La organización identifica y evalúa cambios internos o externos que puedan modificar el perfil de riesgo operacional (nueva regulación, incidentes relevantes, cambios tecnológicos, tercerización, crisis, cambios operativos). Funciona como un “radar” para evitar decisiones basadas en información desactualizada.
4. Revisión y monitoreo	16. Revisa el riesgo operacional y su desempeño	Se revisa periódicamente si el desempeño de la organización y su exposición al riesgo operacional permanecen dentro de los umbrales, límites y tolerancias definidos. Ante desviaciones, se ejecutan acciones correctivas (refuerzo de controles, ajustes de procesos o decisiones).
4. Revisión y monitoreo	17. Persigue la mejora de la gestión del riesgo operacional	La organización implementa un proceso formal de mejora continua de la GRO: aprende de pérdidas, hallazgos, indicadores, evaluaciones internas e independientes y cambios del entorno. Ajusta metodología, controles, formación y coordinación para elevar la efectividad y el valor para la toma de decisiones.
5. Información, Comunicación y Reporte	18. Aprovecha la información y la tecnología	La entidad utiliza información confiable, datos integrados y tecnología adecuada para soportar la gestión del riesgo operacional (registro, trazabilidad, analítica, automatización y reportes). Asegura calidad, oportunidad e integridad de los datos.
5. Información, Comunicación y Reporte	19. Comunica información sobre riesgos operacionales	La organización establece mecanismos de comunicación y escalamiento oportuno de eventos, alertas tempranas, KRIs y cambios relevantes del

Componente	Principio	Descripción del principio
		perfil de RO entre las tres líneas y niveles jerárquicos, evitando duplicidades y vacíos de responsabilidad.
5. Información, Comunicación y Reporte	20. Informa sobre el riesgo operacional, la cultura y el desempeño	La Alta Gerencia reporta al Directorio información útil, oportuna y accionable sobre riesgo operacional, cultura y desempeño: perfil agregado, tendencias, pérdidas relevantes (BDEP), desviaciones de apetito y tolerancias, riesgos emergentes y acciones correctivas. El objetivo es apoyar decisiones y supervisión efectiva mediante reportes claros y consistentes.

Apéndice B

Criterios evaluables

Componente	Principio	Criterio	Definición del criterio
1. Gobierno y Cultura	1. Ejerce la supervisión de riesgos a través del Directorio	**1.1 Manual de GRO aprobado.**	El Directorio define y aprueba el manual de GRO. El manual de GRO define de manera consistente el RO, eventos de pérdidas y metodología; así como políticas y procedimientos aplicables a toda la empresa, con control de versiones y disponibilidad para toda la empresa.
1. Gobierno y Cultura	1. Ejerce la supervisión de riesgos a través del Directorio	**1.2 Apetito, tolerancia y límites de RO aprobados.**	El Directorio conoce los principales riesgos operacionales aprobando y revisando periódicamente el apetito, tolerancia y límites para RO; así mismo supervisa el cumplimiento y corrección oportuna de desviaciones.
1. Gobierno y Cultura	1. Ejerce la supervisión de riesgos a través del Directorio	**1.3 Gobierno, recursos, independencia de la GRO**	El Directorio asegura una estructura de gobierno de la GRO (comités y tres líneas), asigna recursos (infraestructura, metodología y personal), resguarda independencia de la función de RO, y obtiene aseguramiento razonable.
1. Gobierno y Cultura	2. Establece estructuras operativas	**2.1 Gobierno para la GRO**	El manual de GRO identifica las estructuras de gobierno para gestionar el RO, incluyendo líneas de reporte, responsabilidades y composición de comités relevantes. La estructura es proporcional a la naturaleza, tamaño y complejidad de las operaciones de la empresa.
1. Gobierno y Cultura	2. Establece estructuras operativas	**2.2 Roles del modelo de tres líneas para la GRO definidos.**	Se definen y documentan roles, funcione y responsabilidades para RO (Directorio, Gerencia, Comité, Unidad de RO, negocio y apoyo), alineados al modelo de tres líneas.
1. Gobierno y Cultura	2. Establece estructuras operativas	**2.3 Segregación de funciones para la GRO.**	Se establece segregación de funciones que asegure una separación adecuada entre la GRO, unidades

Componente	Principio	Criterio	Definición del criterio
			de negocio o apoyo, y auditoría interna; incluye procesos de aprobación para rendición de cuentas.
1. Gobierno y Cultura	2. Establece estructuras operativas	**2.4 Capacidad y soporte de función de RO.**	Existe función y una unidad especializada RO con autoridad y posición suficientes, recursos adecuados y capacidad para coordinar y asistir la aplicación de la metodología RO, de forma consistente, documentada e integrada a la gestión de riesgos.
1. Gobierno y Cultura	3. Define la cultura deseada	**3.1 Tono del Directorio y Gerencia de RO**	El Directorio lidera y la Gerencia implementa una cultura de RO basada en gestión sólida de riesgos y ética, estableciendo expectativas corporativas consistentes con el manual de GRO.
1. Gobierno y Cultura	3. Define la cultura deseada	**3.2 Conducta ética, incentivos y programa de formación en RO**	La empresa cuenta con los siguientes instrumentos un código de conducta ética de RO aplicable al Directorio y personal (incluye conflictos de interés y prácticas prohibidas) supervisado y revisado periódicamente; un sistema de incentivos (monetarios/no monetarios) que promueve la adecuada gestión de RO y no incentiva riesgos inapropiados; y un programa de formación en RO basado en necesidades, roles y jerarquías.
1. Gobierno y Cultura	4. Demuestra compromiso con los valores clave	**4.1 Liderazgo visible y ética aplicada a la GRO.**	El Directorio y la Gerencia demuestran compromiso visible con los valores institucionales y con el comportamiento ético vinculados a la GRO definidos para la empresa.
1. Gobierno y Cultura	4. Demuestra compromiso con los valores clave	**4.2 Aplicación de código de conducta ética, incentivos y programa de formación para la GRO**	La empresa refuerza los valores clave a través de la aplicación del código de conducta ética (difusión, certificación y supervisión), incentivos alineados a la gestión de RO (sin promover riesgos inapropiados) y programa de formación para la GRO basada en necesidades y roles; con métricas, sanciones, correctivos y mejora continua.

Componente	Principio	Criterio	Definición del criterio
1. Gobierno y Cultura	5. Atrae, desarrolla y retiene a profesionales capacitados	**5.1 Capacitación diferenciada en RO**	Las empresas (con soporte de la unidad de riesgos) aseguran capacitación en RO acorde a jerarquía, rol y responsabilidades. El programa de formación responde a necesidades identificadas, tiene cobertura suficiente para personal especializado y responsables en unidades de negocio y apoyo.
1. Gobierno y Cultura	5. Atrae, desarrolla y retiene a profesionales capacitados	**5.2 Recursos suficientes para la GRO**	El Directorio asigna recursos necesarios (infraestructura, metodología, presupuesto y personal) y la empresa asegura recursos suficientes para aplicar la metodología de RO en unidades de negocio, apoyo y control, preservando independencia de la función de RO.
1. Gobierno y Cultura	5. Atrae, desarrolla y retiene a profesionales capacitados	**5.3 Organización y coordinación del talento para RO**	La empresa define y aplica roles y responsabilidades para RO (función RO, responsables por líneas, comités) y asegura coordinación efectiva con otras funciones de riesgos y control, con diversidad de experiencia para decisiones.
2. Estrategia y Establecimiento de Objetivos	6. Analiza el contexto empresarial	**6.1 Monitoreo del entorno y disparadores de ajuste**	La empresa monitorea factores internos y externos (económicos, regulatorios, mercado, tecnológicos) y define disparadores (criterios, situaciones, eventos) para revisar y ajustar el Manual de GRO y el perfil de RO cuando cambia el entorno o el entorno de control.
2. Estrategia y Establecimiento de Objetivos	6. Analiza el contexto empresarial	**6.2 Análisis prospectivo del contexto crítico**	La empresa anticipa riesgos emergentes mediante análisis de escenarios y evalúa el contexto tecnológico y la dependencia de terceros significativos, integrando resultados en decisiones, controles y planes.
2. Estrategia y Establecimiento de Objetivos	7. Define el apetito al riesgo operacional	**7.1 Apetito RO alineado a estrategia y capacidad de la entidad**	Existe una declaración de apetito y tolerancia al RO, aprobada y revisada por el Directorio; es entendible, incluye contexto y supuestos, y

Componente	Principio	Criterio	Definición del criterio
			muestra coherencia entre estrategia, objetivos y capacidad real de gestión.
2. Estrategia y Establecimiento de Objetivos	7. Define el apetito al riesgo operacional	**7.2 Apetito RO operacionalizado y monitoreado**	El apetito RO se traduce en límites, umbrales, gatillos y estrategias de mitigación; se despliega a unidades; se monitorea el cumplimiento y se gestionan brechas con escalamiento y medidas correctivas oportunas.
2. Estrategia y Establecimiento de Objetivos	7. Define el apetito al riesgo operacional	**7.3 Apetito RO revisado y ajustado**	El Directorio revisa y ajusta periódicamente el apetito, tolerancias, umbrales y límites de RO con base en evidencia (cambios del entorno, volumen de operaciones, calidad del entorno de control, efectividad de mitigación, historial de pérdidas y desviaciones de límites), asegurando acciones correctivas y seguimiento trazable.
2. Estrategia y Establecimiento de Objetivos	8. Evalúa estrategias alternativas	**8.1 Análisis comparativo de alternativas estratégicas con enfoque RO**	La empresa realiza un análisis comparativo de alternativas que reconoce explícitamente la compensación entre retorno y exposición RO para decisiones estratégicas relevantes.
2. Estrategia y Establecimiento de Objetivos	8. Evalúa estrategias alternativas	**8.2 Gobierno para selección y ejecución estratégica**	Existe un esquema de gobierno que define responsables y criterios para seleccionar y ejecutar estrategias. La ejecución se mantiene coherente y alineada al apetito de riesgo y asociado a decisiones estratégicas.
2. Estrategia y Establecimiento de Objetivos	9. Formula objetivos de negocio	**9.1 Objetivos de negocio alineados a RO**	Los objetivos de negocio se formulan de manera coherente con el perfil y apetito de RO. Se evidencia que la empresa reconoce el RO como inherente a la operación y lo integra con el marco de gestión de RO.
2. Estrategia y Establecimiento de Objetivos	9. Formula objetivos de negocio	**9.2 Seguimiento y rendición de cuentas de objetivos**	La empresa cuenta con mecanismos de control que incluyen revisiones del progreso de los objetivos y reporte periódico al Directorio, asegura la implementación oportuna de acciones correctivas.

Componente	Principio	Criterio	Definición del criterio
3. Desempeño	10. Identifica los riesgos operacionales	**10.1 Herramientas y responsabilidades para identificar RO**	La empresa define herramientas para identificar RO y asigna responsabilidades claras para su aplicación. Se evidencia uso consistente en toda la organización y coordinación entre las tres líneas para asegurar cobertura y calidad de la identificación.
3. Desempeño	10. Identifica los riesgos operacionales	**10.2 Taxonomía y criterios de clasificación de RO**	La empresa utiliza una taxonomía común de RO y criterios objetivos de clasificación. Se evidencia consistencia transversal en la asignación de eventos y riesgos a tipologías y líneas, facilitando agregación, análisis y comparabilidad interna.
3. Desempeño	10. Identifica los riesgos operacionales	**10.3 Autoevaluación de RO**	La empresa realiza autoevaluaciones exhaustivas que identifican RO y valoran el entorno de control. Se evidencia evaluación de riesgo inherente y residual, con registros suficientes para sustentar resultados y priorizar acciones.
3. Desempeño	10. Identifica los riesgos operacionales	**10.4 Identificación de RO en NPCI**	Los NPCI incorporan identificación previa de RO durante su ciclo de vida. Se evidencia que la identificación se realiza antes de aprobaciones relevantes y que existe trazabilidad de responsables y decisiones asociadas a la gestión del RO.
3. Desempeño	10. Identifica los riesgos operacionales	**10.5 Identificación de RO mediante BDEP**	La empresa utiliza eventos y pérdidas registrados en la BDEP para identificar RO. Se evidencia análisis periódico y capacidad para detectar riesgos emergentes a partir de tendencias, concentración o patrones observables en los registros.
3. Desempeño	10. Identifica los riesgos operacionales	**10.6 Identificación de RO en servicios provistos por terceros**	La empresa identifica RO asociado a terceros significativos antes de contratar y durante la vigencia del servicio. Se evidencia seguimiento y revisiones que reflejan materialidad del tercero y cambios relevantes en el desempeño o condiciones del servicio.

Componente	Principio	Criterio	Definición del criterio
3. Desempeño	11. Evalúa la severidad de los riesgos operacionales	**11.1 Metodología para evaluar el RO**	Existe una metodología definida para evaluar severidad de RO. Se evidencia consideración diferenciada de riesgo inherente, efectividad de controles y riesgo residual, con criterios y escalas consistentes que permiten comparabilidad y seguimiento.
3. Desempeño	11. Evalúa la severidad de los riesgos operacionales	**11.2 Medición de la criticidad de RO con BDEP**	La empresa mide criticidad de RO con base en la BDEP. Se evidencia valoración consistente de pérdidas, recuperaciones y provisiones, así como trazabilidad por evento y agregado, permitiendo análisis de severidad y soporte a decisiones de gestión.
3. Desempeño	11. Evalúa la severidad de los riesgos operacionales	**11.3 Escenarios para eventos severos de RO**	La empresa desarrolla escenarios para estimar consecuencias de eventos severos de RO. Se evidencia sustento en información interna disponible y uso de resultados para ajustar los controles internos.
3. Desempeño	11. Evalúa la severidad de los riesgos operacionales	**11.4 Monitoreo y reporte de criticidad de RO**	La empresa monitorea la criticidad de RO mediante indicadores (KRI) vinculados a riesgos. Se evidencia reporte oportuno de riesgos y pérdidas significativas a Directorio y Comités, con acciones y responsables definidos ante desviaciones.
3. Desempeño	12. Prioriza riesgos operacionales	**12.1 Priorización de RO según nivel de riesgo**	La empresa prioriza RO con criterios y variables consistentes basados en niveles de riesgo. Se evidencia distinción entre riesgos inherente, efectividad de controles y riesgo residual, y una priorización que orienta planes y recursos de gestión.
3. Desempeño	12. Prioriza riesgos operacionales	**12.2 Actualización periodica de la priorización de RO**	La priorización de RO se actualiza con una periodicidad definida. Se evidencia uso de información de monitoreo, KRIs y análisis de

Componente	Principio	Criterio	Definición del criterio
			pérdidas para ajustar prioridades, manteniendo trazabilidad de cambios y sustentos.
3. Desempeño	12. Prioriza riesgos operacionales	**12.3 Ajuste de priorización de RO ante eventos**	La empresa ajusta la priorización de RO ante eventos internos o externos relevantes. Se evidencia que sucesos que cambian materialmente el perfil de RO gatillan revisión y reordenamiento de prioridades con decisiones trazables.
3. Desempeño	13. Implementa respuestas ante los riesgos operacionales	**13.1 Tratamiento de RO fuera del nivel aceptable**	La empresa define y ejecuta medidas de tratamiento para RO fuera del nivel aceptable. Se evidencia planes con responsables, plazos y recursos, así como seguimiento del avance y cierre de acciones asociadas a riesgos priorizados.
3. Desempeño	13. Implementa respuestas ante los riesgos operacionales	**13.2 Respuestas a eventos de RO**	La empresa define procesos para responder ante eventos de RO, que contemplan protocolos preestablecidos, incorpora análisis de causas raíz y de deficiencias de control, y define acciones correctivas y para evitar recurrencia; soportado por datos de eventos y pérdidas.
3. Desempeño	13. Implementa respuestas ante los riesgos operacionales	**13.3 Tratamiento de RO en cambios internos**	La empresa define tratamiento de RO asociado a NPCI y a terceros. Se evidencia que medidas de tratamiento se establecen antes de la ejecución y se implementan con seguimiento, conforme a responsabilidades y materialidad del riesgo.
3. Desempeño	13. Implementa respuestas ante los riesgos operacionales	**13.4 Transferencia de RO y programa de seguros**	La empresa gestiona la transferencia de RO mediante instrumentos como seguros cuando corresponde. Se evidencia coherencia con el apetito y capacidad financiera, y revisiones periódicas del programa, con decisiones y responsables trazables.
3. Desempeño	14. Desarrolla una visión a nivel de portafolio	**14.1 Perfil consolidado de RO para decisiones**	La empresa consolida y presenta una visión agregada del perfil y exposiciones significativas de RO para soportar decisiones del Directorio, Comité de Riesgos y Gerencia.

Componente	Principio	Criterio	Definición del criterio
3. Desempeño	14. Desarrolla una visión a nivel de portafolio	**14.2 Integración metodológica de RO**	La empresa implementa una metodología RO consistente e integrada en procesos de gestión de riesgos, habilitando agregación por productos, procesos, unidades y un lenguaje común para ver el portafolio completo.
3. Desempeño	14. Desarrolla una visión a nivel de portafolio	**14.3 Inventarios centralizados para exposición a RO**	La empresa mantiene registros centralizados (productos, procesos, servicios provistos por terceros) para mapear exposición RO y facilitar seguimiento de cambios.
3. Desempeño	14. Desarrolla una visión a nivel de portafolio	**14.4 Análisis de tendencias de RO con BDEP**	La empresa usa la BDEP para analizar tendencias, concentraciones, y cuenta con taxonomías y reglas consistentes (tipos de evento, líneas, eventos múltiples y categorías especiales).
4. Revisión y monitoreo	15. Evalúa los cambios sustantivos	**15.1 Gobierno de los NPCI**	Existe un proceso integral para identificar, aprobar y supervisar NPCI, con criterios objetivos, roles claros, controles específicos y revisión periódica independiente de metodología, políticas y procedimientos.
4. Revisión y monitoreo	15. Evalúa los cambios sustantivos	**15.2 Evaluación de RO a NPCI**	Se evalúa RO asociados a NPCI, desde concepción hasta post-implementación, incluyendo riesgo inherente, impacto en perfil, apetito y tolerancia; controles o medidas de mitigación; riesgo residual; límites y métricas de monitoreo.
4. Revisión y monitoreo	15. Evalúa los cambios sustantivos	**15.3 Reporte y remisión de NPCI**	Los NPCI se sustentan en informes estructurados, se presentan y aprueban por los órganos competentes y se remiten a la SBS dentro de plazos establecidos.
4. Revisión y monitoreo	16. Revisa el riesgo operacional y su desempeño	**16.1 Revisión del manual de GRO**	La empresa revisa periódicamente la eficacia del Manual de GRO y la idoneidad de su contenido, incorporando los cambios del entorno, negocio, pérdidas y brechas, y activando ajustes.
4. Revisión y monitoreo	16. Revisa el riesgo operacional y su desempeño	**16.2 Monitoreo del perfil de RO frente a umbrales**	Se monitorean perfiles y exposiciones significativas con indicadores (KRIs) vinculadas a

Componente	Principio	Criterio	Definición del criterio
			riesgos; se analiza desempeño vs umbrales, se reporta y se ejecutan acciones ante desviaciones.
4. Revisión y monitoreo	16. Revisa el riesgo operacional y su desempeño	**16.3 Aseguramiento y pruebas de controles clave de RO**	Se evalúan y prueban el diseño y eficacia operativa de los controles clave con segregación y cobertura adecuada; y se ejecutan acciones ante desviaciones.
4. Revisión y monitoreo	17. Persigue la mejora de la gestión del riesgo operacional	**17.1 Gestión de observaciones de RO**	La empresa asegura el cierre oportuno y efectivo de las observaciones sobre RO de Auditoría interna, externa y SBS mediante planes de acción, seguimiento, evidencias.
4. Revisión y monitoreo	17. Persigue la mejora de la gestión del riesgo operacional	**17.2 Definición del proceso de mejora continua de GRO**	La empresa define y documenta un proceso de mejora continua de la GRO que establece fuentes de mejora (evaluaciones internas, independientes, métricas, pérdidas, análisis comparativo, cambios del entorno), roles de las tres líneas, periodicidad y criterios de priorización y aprobación de mejoras.
4. Revisión y monitoreo	17. Persigue la mejora de la gestión del riesgo operacional	**17.3 Ejecución y verificación de mejoras de la GRO**	La empresa ejecuta el proceso de mejora continua mediante planes de acción trazables: prioriza mejoras, asigna responsables y recursos, define plazos e indicadores, realiza seguimiento y verifica cierre y efectividad (incluyendo ajustes a políticas o manuales, capacitación o difusión, y acciones concretas frente a desviaciones).
5. Información, Comunicación y Reporte	18. Aprovecha la información y la tecnología	**18.1 Sistema informático para la GRO**	La empresa cuenta con sistemas especializados para la GRO y soporte de la BDEP, que consolidan reportes por proceso y unidad, incluyendo datos precisos e íntegros, trazabilidad y registros relevantes.
5. Información, Comunicación y Reporte	18. Aprovecha la información y la tecnología	**18.2 Analítica de datos y automatización para la GRO**	La empresa cuenta con procesos para promover la analítica de datos (conjunto de métodos utilizadas para examinar, interpretar y extraer conocimiento a partir de datos) y automatización (uso de tecnología para ejecutar tareas con mínima o nula

Componente	Principio	Criterio	Definición del criterio
			intervención humana) de procesos relacionados a la GRO.
5. Información, Comunicación y Reporte	19. Comunica información sobre riesgos operacionales	**19.1 Coordinación y comunicación sobre RO**	La empresa asegura una adecuada coordinación y comunicación transversal sobre RO entre las tres líneas y niveles de la organización.
5. Información, Comunicación y Reporte	19. Comunica información sobre riesgos operacionales	**19.2 Flujo y escalamiento de información de RO**	La empresa define y aplica reglas para que eventos, alertas tempranas, indicadores y cambios sustanciales se comuniquen y escalen oportunamente a los niveles que corresponda según los canales establecidos.
5. Información, Comunicación y Reporte	20. Informa sobre el riesgo operacional, la cultura y el desempeño	**20.1 Gobierno del reporte de RO**	La empresa define formalmente la arquitectura de reportes de RO (destinatarios, forma, periodicidad, responsables), con capacidad de emitir reportes también en situaciones de contingencia.
5. Información, Comunicación y Reporte	20. Informa sobre el riesgo operacional, la cultura y el desempeño	**20.2 Contenido y calidad del reporte de RO**	Los reportes de RO son exhaustivos, precisos, coherentes y útiles; describen el perfil de RO e incluyen indicadores (KRIs), eventos y pérdidas relevantes (con análisis), incumplimientos de apetito o tolerancia, y riesgos clave o emergentes.
5. Información, Comunicación y Reporte	20. Informa sobre el riesgo operacional, la cultura y el desempeño	**20.3 Reporte regulatorio y divulgación pública de RO**	La empresa cumple con reportes regulatorios y cuenta con divulgación pública proporcional y controlada (política formal, aprobación, revisión periódica, controles del proceso).

Apéndice C

Ejemplos de niveles de madurez

A continuación, se presentan ejemplos referenciales de los niveles de madurez aplicables al criterio “Manual de GRO aprobado”, formulado a partir de la siguiente pregunta de evaluación: ¿El Directorio aprueba el manual de GRO, con definiciones y metodología unificada; y con referencias a políticas y procedimientos relevantes?

Nivel de madurez	Descripción	Ejemplos
0 - Inmadura	No cuenta con prácticas formales ni sistematizadas de gestión del riesgo operacional.	No existe manual de GRO aprobado.
1 - Inicial	Se reconoce la necesidad de gestionar el riesgo operacional, pero las prácticas son incipientes, informales y poco consistentes.	Documentación parcial o informal; sin definiciones ni estandarización.
2 - En progreso	Existe avance hacia la formalización de prácticas básicas.	Documentación aprobada con brechas (definiciones incompletas y referencias débiles).
3 - Definido	La gestión del riesgo operacional cuenta con procesos formalizados, documentados y aplicados de manera consistente.	Manual de GRO aprobado con definiciones, referencias claras y metodología, políticas y procedimientos unificados.
4 - Gestionado	La gestión está consolidada y apoyada en datos, métricas e indicadores.	Manual de GRO con revisiones y actualizaciones documentadas; estandarización verificable.
5 - Optimizado	La gestión es avanzada, con enfoque en la mejora continua e innovación.	Manual de GRO altamente consistente y mantenido; cambios controlados y trazables.

Apéndice D

Preguntas y respuestas de criterios

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
1.1 Manual de GRO aprobado.	¿El Directorio aprueba el manual de GRO, con definiciones y metodología unificada; y con referencias a políticas y procedimientos relevantes?	No existe manual de GRO aprobado.	Documentación parcial o informal; sin definiciones ni estandarización.	Documentación aprobada con brechas (definiciones incompletas y referencias débiles).	Manual de GRO aprobado con definiciones, referencias claras y metodología, políticas y procedimientos unificados.	Manual de GRO con revisiones y actualizaciones documentadas; estandarización verificable.	Manual de GRO altamente consistente y mantenido; cambios controlados y trazables.
1.2 Apetito, tolerancia y límites de RO aprobados.	¿El Directorio aprueba y revisa periódicamente el apetito, tolerancia y límites de RO; y supervisa la detección y corrección oportuna de desviaciones?	No existe definición de apetito, tolerancia y límites de RO.	Apetito, tolerancia y límites de RO declarativos sin aprobación, revisión ni seguimiento.	Límites definidos en algunos ámbitos; seguimiento irregular; correcciones no sistemáticas.	Aprobación y revisión periódica; monitoreo de cumplimiento; corrección documentada de desviaciones.	La revisión considera entorno, regulación, historial de pérdidas y desviaciones; la subsanación de desviaciones es oportuna y evidenciable.	Ajustes oportunos ante cambios previstos; gestión de desviaciones con trazabilidad completa.
1.3 Gobierno, recursos, independencia de la GRO	¿El Directorio asegura estructura, recursos e independencia para la gestión	No existe roles definidos, recursos y ni aseguramiento.	Roles generales, recursos insuficientes y aseguramiento reactivo o inexistente.	Estructura parcial; independencia con brechas; recursos limitados; revisiones	Estructura y roles documentados; independencia demostrable; recursos asignados; aseguramiento razonable.	Recursos suficientes según tamaño y complejidad; funcionamiento demostrable del enfoque de tres líneas. Aseguramiento de que	Ajustes oportunos de roles y recursos; independencia sostenida y verificable. Aseguramiento de

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	de RO; y obtiene aseguramiento razonable?			puntuales para aseguramiento.		Auditoría interna revisa una vez al año la GRO	una revisión independiente a la GRO una vez cada tres años
2.1 Gobierno para la GRO	¿El manual de GRO documenta la estructura de gobierno, líneas de reporte, responsabilidades y composición de comités para gestionar el RO?	No existe documentación de estructura de gobierno de RO, líneas de reporte, comités.	Existe mención general a comités y roles, sin composición o líneas de reporte claras.	Estructura definida parcialmente (p. ej., comités o líneas de reporte), con vacíos en composición o responsabilidades.	Estructura de gobierno RO documentada: líneas de reporte, responsabilidades y composición de comités; accesible y vigente; proporcional a su naturaleza, tamaño y complejidad de operaciones.	Evidencia de funcionamiento: reglamentos de comités, periodicidad y reportes al directorio; acuerdos registrados y seguimiento de acuerdos.	Estructura revisada y ajustada oportunamente ante cambios organizacionales; consistencia y trazabilidad completa entre documentación, comités y reportes.
2.2 Roles del modelo de tres líneas para la GRO definidos.	¿Los roles y responsabilidades para RO están documentados, alineados al modelo de tres líneas y aplicados consistentemente?	No existe roles definidos ni enfoque de tres líneas.	Roles generales y declarativos; tres líneas solo nominales, sin aplicación.	Roles definidos en algunos órganos y unidades; inconsistencias con manual o aplicación irregular.	Roles, funciones y responsabilidades de RO completos y documentados para Directorio, Gerencia, Comité, Unidad RO, negocio y apoyo; tres líneas formalizadas.	Evidencia de aplicación consistente: asignaciones formales, comunicaciones internas y ejecución alineada a roles (p. ej., actas/comités, reportes, responsabilidades por unidad).	Roles consolidados y actualizados; tres líneas opera de forma efectiva y verificable en toda la organización.
2.3 Segregación de funciones para la GRO.	¿La empresa tiene segregación de funciones y procesos de aprobación documentados y aplicados para la GRO?	No existe segregación de funciones formal ni procesos de aprobación para la GRO.	Segregación de funciones declarativa y aprobaciones informales.	Segregación de funciones definidas en algunas unidades; existen aprobaciones, pero con brechas o excepciones sin control.	Segregación de funciones formalizadas, aprobaciones y excepciones definidas.	Evidencia de funcionamiento de segregación de funciones y adecuada rendición de cuentas a niveles apropiados de forma periódica.	Segregación de funciones e independencia consistente entre si; ajustes oportunos ante conflictos y rendición de cuentas en toda la organización.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
2.4 Capacidad y soporte de función de RO.	¿La empresa cuenta con funciones y unidades de RO con posicióny autoridad suficiente; recursos suficientes para coordinar y asegurar la aplicación consistente y documentada de la metodología de RO en toda la empresa?	No existe función de la unidad de RO ni recursos definidos.	Función RO incipiente; recursos insuficientes; apoyo a unidades es ocasional; documentación limitada.	Función RO existe con recursos parciales; coordinación, apoyo y documentación se aplican en parte de la organización.	Función RO formalizada, con recursos suficientes; coordina y asiste a unidades; aplicación de metodología consistente y documentada; integrada a la gestión de riesgos.	Evidencia de autoridad y posición adecuada a nivel gerencial y reporte según corresponda (p. ej., sistemas de soporte cuando existen, coordinación permanente y reportes a comités/directorio).	Capacidad consolidada y proporcional a complejidad; continuidad y consistencia sostenida; mejoras continuas en la organización y en la aplicación de la metodología de RO.
3.1 Tono del Directorio y Gerencia de RO	¿El Directorio y la Gerencia lideran e implementan de forma explícita la cultura deseada para la GRO alineados al manual de GRO?	No existen lineamientos de cultura para la GRO; GRO es reactiva.	Mensajes aislados sobre RO, sin traducción a prácticas o decisiones.	Cultura de RO declarada, pero con implementación parcial o inconsistente por unidades.	Cultura RO definida y comunicada; roles de Directorio y Gerencia claros y consistentes con manual GRO.	Evidencia de refuerzo sostenido desde el Directorio y la Gerencia; y seguimiento a su aplicación.	Cultura RO integrada en la forma de operar y decidir; ajustes continuos basados en eventos y retroalimentación organizacional.
3.2 Conducta ética, incentivos y programa de formación en RO	¿Existe y se aplica un código de conducta de ética, incentivos y un programa de formación que refuerce la	No existe código de ética, incentivos ni programa de formación para RO.	Elementos aislados (código, incentivos y capacitación) sin vínculo a RO; incentivos sin métricas,	Elementos existentes pero incompletos con aplicación irregular; código de conducta ética no define	Elementos completos, aprobado y vinculados a RO; código de conducta ética aplicado a personal y Directorio con prácticas aceptables y prohibidas; sistema de incentivos	Elementos vigentes y con política de actualización periódica; se aplican medidas correctivas ante desviaciones; con trazabilidad del proceso.	Elementos revisados y calibrados periódicamente; mejoras continuas basadas en resultados y

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	cultura de RO, con revisión periódica?		criterios ni vínculo real al desempeño; capacitaciones puntuales sin diagnóstico de necesidades ni segmentación por rol.	claramente prácticas prohibidas, alcance limitado, sin periodicidad de revisión; incentivos aplicados solo algunas unidades o sin consistencia; programa de capacitación con cobertura incompleta y sin ajustes consistentes a roles y jerarquías.	formal e integrado a evaluación de desempeño; programa de formación en RO definido y comunicado, basado en necesidades y contenidos por rol.		eventos; cambio de comportamiento medible, define estándares por roles críticos cuando aplica.
4.1 Liderazgo visible y ética aplicada a la GRO.	¿El Directorio y la Gerencia demuestran compromiso sostenido y visible a la GRO y al comportamiento ético aplicado a RO, reflejado en decisiones, prioridades y mensajes consistentes?	No existe un compromiso en la GRO ni en la ética aplicada a RO.	Compromiso reactivo y esporádico.	Compromiso frecuente pero inconsistente entre unidades o periodos.	Compromiso formal y sostenido; GRO y ética aplicada a RO presentes en agenda y decisiones relevantes.	Evidencia de seguimiento y exigencia de cumplimiento (retroalimentación y correcciones).	Compromiso institucionalizado: se anticipan situaciones que comprometan la ética aplicada a RO y se ajustan prácticas preventivamente.
4.2 Aplicación de código de conducta ética,	¿La empresa aplica y supervisa el	No existe sustento de aplicación de	Difusión ocasional de elementos;	Difusión y certificación del código de	Aplicación consistente de elementos; cobertura razonable y ejecución en los	Efectividad demostrada; monitoreo por indicadores; definición de acciones	Calibración periódica por resultados; mejoras

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
incentivos y programa de formación para la GRO	código de conducta ética, sistema de incentivos y programa de formación para la GRO con evidencia de cumplimiento, métricas y acciones ante incumplimientos o brechas?	código de conducta ética, sistema de incentivos y programa de formación para la GRO	código de ética sin certificación ni control; incentivos con ejecución limitada; capacitaciones puntuales con limitada asistencia y sin control de cobertura.	conducta ética para RO incompleta; sistema de incentivos con otorgamiento parcial; programa de formación aplicado con cobertura incompleta.	plazos y oportunidades definidas.	correctivas ante brechas e incumplimientos.	continuas de la gestión; incentivos mejoran comportamientos y reducen exposiciones.
5.1 Capacitación diferenciada en RO	¿Existe un programa de capacitación en RO, por niveles y roles, basado en necesidades y ejecutado de forma continua?	No existe capacitación en RO.	Capacitación esporádica, no diferenciada por rol; sin diagnóstico de necesidades.	Se identifican necesidades y hay programa, pero cobertura parcial o ejecución irregular.	Programa formal, continuo y diferenciado por rol; necesidades identificadas por unidad de riesgos.	Se gestiona la capacitación como requisito de competencia (incluye entrenamiento de procesos RO donde aplica, p.ej. registro de eventos).	El programa de capacitación se mantiene y ajusta dinámicamente por cambios y roles, consolida capacidades técnicas en toda la empresa.
5.2 Recursos suficientes para la GRO	¿Se asignan y mantienen recursos suficientes para operar el RO y aplicar la metodología en toda la empresa?	No existe recursos asignados, RO no es operable o depende de esfuerzos puntuales.	Los recursos son mínimos, RO funciona de manera limitada y reactiva.	Los recursos son asignados parcialmente, existen brechas persistentes en líneas de negocio, apoyo y control.	Los recursos son suficientes para aplicar metodología y cumplir funciones; estructura de RO formal.	Los recursos están alineados al tamaño y complejidad; y revisados para sostener independencia y continuidad operativa.	Los recursos anticipan el crecimiento y cambios, la capacidad de RO es escalable y sostenida.
5.3 Organización y coordinación	¿La estructura de RO define roles (función RO,	No hay función RO ni responsables;	Roles difusos o solo declarativos; coordinación	Roles definidos parcialmente; coordinación con	Roles formalizados y comunicados; coordinación operativa estable; comités	Estructura que funciona de forma coordinada y consistente, las	Coordinación integrada y preventiva;

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
del talento para RO	responsables por línea y comités) y evidencia coordinación efectiva con otras funciones, con experiencia suficiente para decisiones?	coordinación inexistente entre Unidad de Riesgos y comités.	informal y puntual.	brechas; comités sin suficiente experiencia o cobertura.	con participación y capacidades adecuadas.	responsabilidades se ejercen y se articulan con comités cuando corresponde.	diversidad de experiencia sostenida; estructura se adapta y fortalece sin perder consistencia.
6.1 Monitoreo del entorno y disparadores de ajuste	¿Existe monitoreo del entorno y disparadores formales que gatillen revisiones del Manual de GRO y ajustes del perfil RO, con trazabilidad?	No existe análisis del entorno; decisiones reactivas.	Análisis ocasional o con alcance limitado (p.ej., solo regulatorio) sin criterios ni periodicidad.	Monitoreo sin disparadores ni criterios claros o sin aplicación consistente.	Monitoreo formal con periodicidad y fuentes mínimas; disparadores documentados para revisar el Manual de GRO	Revisiones ejecutadas por disparadores; cambios trazables y reportados a instancias de gobierno.	Monitoreo continuo con indicadores tempranos; mejoras por lecciones aprendidas; ajustes anticipados y medibles.
6.2 Análisis prospectivo del contexto crítico	¿Se realizan escenarios y evaluaciones de Tecnología y terceros para anticipar impactos en RO y ajustar decisiones y controles, con gobernanza y seguimiento?	No existe análisis de escenarios ni del contexto tecnológico y de terceros	Evaluaciones puntuales sin metodología; resultados no documentados ni implementados.	Metodología básica con cobertura limitada (solo algunas unidades y proveedores) o sin revisión y gobernanza suficiente; resultados documentos, pero con implementación parcial	Proceso periódico con metodología y escenarios documentados; evaluación de Tecnología y terceros significativos con criterios; resultados se incorporan a planes y controles.	Acciones correctivas seguidas; mejoras en la GRO; escalamiento y control del desempeño de terceros.	Mapas de dependencia y concentración; pruebas integradas; calibración por eventos y cambios del entorno; reducción demostrable de exposición y pérdidas.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
7.1 Apetito RO alineado a estrategia y capacidad de la entidad	¿La empresa tiene una declaración formal de apetito y tolerancia para RO, aprobada y revisada por el Directorio, entendible y alineada a la estrategia, objetivos y capacidad de gestión?	No existe declaración de apetito y tolerancia al RO.	Hay menciones generales (p.ej., “bajo riesgo”) sin documento formal ni criterios.	Documento con alineamiento parcial a estrategia capacidad; comunicación limitada.	Declaración aprobada y comunicada; incluye supuestos y alineamiento explícito a estrategia y capacidad.	Metodología de definición documentada; revisiones periódicas con trazabilidad de cambios.	Integración total con planificación estratégica; ajustes continuos por cambios del entorno, control y pérdidas; alta comprensión transversal.
7.2 Apetito RO operacionalizado y monitoreado	¿El apetito RO tiene límites, umbrales, gatillos y mitigaciones; está desplegado a unidades y se controla su cumplimiento con corrección de brechas?	No existen límites ni monitoreo; decisiones caso a caso.	Límites aislados por área, sin gatillos ni acciones definidas ante brechas.	Límites existen para algunos riesgos; monitoreo irregular; correcciones tardías.	Límites, umbrales, gatillos documentados e integrados a metodología; monitoreo periódico y escalamiento definido.	Brechas detectadas y corregidas en plazo; seguimiento y rendición de cuentas.	Límites calibrados por escenarios, pérdidas y calidad de control; alertas tempranas y mejora continua.
7.3 Apetito RO revisado y ajustado	¿El apetito y tolerancia de RO se revisan y recalibran con periodicidad definida y/o gatillos claros, considerando evidencia	No existe revisión ni ajustes del apetito y tolerancia de RO.	Ajustes reactivos y esporádicos (por incidentes), sin criterios ni trazabilidad.	Revisión ocasional; considera algunos insumos, pero sin metodología, gatillos ni seguimiento consistente.	Revisión periódica documentada; insumos definidos; ajustes aprobados y difundidos.	Metodología de recalibración documentada; análisis de tendencias (pérdidas y brechas), entorno de control y entorno externo.	Recalibración dinámica (por gatillos y periodicidad), integrada a estrategia; aprendizaje continuo y ajustes oportunos.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	(pérdidas, brechas, calidad de controles, cambios del entorno y del negocio), con decisiones, acciones y seguimiento trazables?						
8.1 Análisis comparativo de alternativas estratégicas con enfoque RO	¿Se comparan alternativas estratégicas considerando la compensación entre el retorno y la exposición RO y se documenta para sustentar la decisión?	No existe análisis de exposición al RO en alternativas; prima el retorno.	Evaluación de RO enfocada en una sola alternativa; sin comparación ni compensación.	Se comparan algunas alternativas, pero con criterios incompletos o sin trazabilidad de controles o acciones.	Análisis comparativo de RO, acciones y controles; documentado y usado en la aprobación.	Decisiones se ajustan por RO y se condicionan a mitigaciones verificables.	Comparaciones con escenarios adversos, resiliencia operativa y capacidad de respuesta; el aprendizaje post-implementación retroalimenta criterios.
8.2 Gobierno para selección y ejecución estratégica	¿La entidad asegura que las alternativas estratégicas se elijan y ejecuten en un esquema de gobierno, en línea con el apetito al riesgos y asociado a decisiones estratégicas?	No existen reglas claras para la elección de estrategias.	Reglas básicas, pero sin conexión a decisiones estratégicas ni seguimiento.	Ejecución parcial de reglas y sin condicionamiento de decisiones.	Esquema de gobierno definido con roles claros y alineado al apetito.	Se revisan iniciativas por desviación de apetito; seguimiento a responsables y medidas correctivas.	Revisiones periódicas de fallas que ajustan la gobernanza y los criterios de decisión.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
9.1 Objetivos de negocio alineados a RO	¿Los objetivos de negocio se formularn de manera coherente con el perfil y apetito de RO e integrados al marco de gestión?	Objetivos definidos sin considerar apetito ni perfil de RO	Se menciona RO de forma declarativa, sin criterios ni evidencia de alineamiento.	Algunos objetivos consideran apetito RO, pero sin consistencia transversal.	Objetivos formalizados y alineados al apetito RO; se consideran implicancias de RO.	Objetivos se ajustan cuando el perfil RO cambia; se documenta la justificación y la compensación entre el retorno y el riesgo.	Objetivos se recalibran con lecciones de pérdidas, incidentes y tendencias; integración consistente en toda la organización.
9.2 Seguimiento y rendición de cuentas de objetivos	¿La empresa cuenta con mecanismos para revisar y reportar periódicamente el avance de objetivos (incluyendo desvíos relevantes) y se toman acciones correctivas?	No existe seguimiento formal del avance de objetivos.	Seguimiento informal, sin periodicidad ni trazabilidad de acciones.	Monitoreo del avance con indicadores incompletos y acciones correctivas no sistemáticas.	Revisiones periódicas y reporte al Directorio; se registran desvíos y acciones correctivas	Acciones correctivas oportunas; se verifica cierre y cumplimiento de rendición de cuentas.	Seguimiento predictivo (alertas tempranas), aprendizaje institucional y mejora del sistema de control sobre objetivos.
10.1 Herramientas y responsabilidades para identificar RO	¿La empresa define en el Manual de GRO herramientas para identificar y evaluar el RO, así como roles de las tres líneas para su aplicación consistente?	El Manual GRO no incluye lineamientos para la identificación de RO.	Hay lineamientos generales, pero sin herramientas claras ni roles de las tres líneas formalizados.	Manual incluye herramientas y roles, pero está incompleto, desactualizado o no se usa de forma homogénea.	Manual vigente, aprobado y difundido; define herramientas, responsables de tres líneas y frecuencia mínima de aplicación.	Aplicación consistente; trazabilidad (quién/qué/cuándo); revisión independiente; hallazgos gestionados.	Ajustes por incidentes, auditorías, supervisión y cambios del negocio; control de calidad de la ejecución.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
10.2 Taxonomía y criterios de clasificación de RO	¿La empresa utiliza una taxonomía común de RO y criterios objetivos de clasificación aplicados de forma consistente y homogénea en los eventos y riesgos?	No existe una taxonomía común; cada área usa definiciones propias.	Taxonomía informal o parcial; se usa solo en algunas áreas/productos.	Taxonomía definida, pero con baja adopción o sin criterios claros de clasificación.	Taxonomía y criterios documentados, aprobados y difundidos; aplicación en procesos críticos.	Recodificación controlada (sin cambios constantes); control de calidad y revisiones cruzadas; reglas claras para integrar fronteras de otros tipos de riesgos.	Gobierno de taxonomía, actualizaciones por cambios regulatorios o tecnológicos, analítica para detectar inconsistencias y reentrenamiento focalizado.
10.3 Autoevaluación de RO	¿La empresa realiza la identificación y evaluación exhaustiva usando autoevaluaciones, con evidencia verificable?	No se realizan autoevaluaciones ni cuentan con registro de RO.	Evaluaciones puntuales, reactivas (post evento), sin metodología ni evidencia consistente.	Existen autoevaluaciones, pero con cobertura incompleta (no incluye procesos/sistemas críticos) o sin evaluación clara de controles y riesgo residual.	Autoevaluaciones definidas, periódicas y con cobertura mínima establecida; evidencia trazable permite revisión independiente; segunda línea consolida resultados.	Cobertura total de productos/procesos/sistemas; calidad del análisis (causas/controles); seguimiento de brechas; segunda línea desafía resultados.	Análisis formalizado y trazable con priorización basada en datos (pérdidas/KRIs) e integración con fuentes de información disponibles.
10.4 Identificación de RO en NPCI	¿La empresa identifica RO en NPCI durante todo el ciclo de vida, con responsabilidades claras y aprobaciones previas?	No existe proceso de identificación previo; los cambios se ejecutan sin evaluación de RO.	Evaluaciones puntuales, acotadas y no oportunas; sin roles claros.	Proceso existe, pero no cubre todo el ciclo de vida o no involucra oportunamente a la segunda línea.	Proceso formal, documentado y aplicado; incluye RO inherente/residual, responsables y checklists mínimos; evidencia de aprobaciones previas.	Seguimiento de medidas de mitigación, revisiones post-implementación, y lecciones aprendidas incorporadas.	Criterios calibrados para identificar NPCI calibrados; trazabilidad del flujo y aprobaciones; retroalimentación desde pérdidas/incidentes.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
10.5 Identificación de RO mediante BDEP	¿La empresa utiliza la BDEP y la analiza periodicamente para identificar nuevos RO?	No existe BDEP ni protocolo de gestión de eventos.	Registro parcial y reactivo; campos mínimos incompletos; sin criterios ni umbrales claros	Existe BDEP, pero con brechas: subregistro, baja calidad de datos, poco análisis para identificar riesgos.	BDEP implementada con reglas/expedientes; análisis periódico y evaluación formal de terceros significativos (con aprobaciones definidas).	Conciliaciones y controles de integridad periódicos y trazables, cuyos hallazgos son convertidos en riesgos/controles	Analítica avanzada y uso prospectivo (tendencias, causas raíz) con monitoreo periódico e integración con indicadores y autoevaluaciones.
10.6 Identificación de RO en servicios provistos por terceros	¿La empresa identifica RO en servicios provistos por terceros antes de su contratación y durante su vigencia, con responsabilidades claras y aprobaciones previas?	No existe proceso de identificación de RO previo a la contratación ni durante la vigencia del servicio.	Evaluaciones puntuales, acotadas y no oportunas; sin roles claros.	Existen evaluaciones, pero con cobertura incompleta (no incluye todos los servicios significativos) o sin evaluación clara de controles y riesgo residual.	Proceso formal, documentado y aplicado a todos los servicios significativos; incluye evaluación inicial y monitoreo periódico de RO, responsables, debida diligencia, contratos con acuerdos y SLA; evidencia de aprobaciones previas	Cobertura total de servicios significativos y subcontrataciones; seguimiento de medidas de mitigación; visitas insitu a proveedores; lecciones aprendidas incorporadas.	Analítica avanzada y uso prospectivo del desempeño de proveedores; criterios calibrados para identificar servicios significativos; trazabilidad del flujo y aprobaciones; retroalimentación desde pérdidas/incidentes.
11.1 Metodología para evaluar el RO	¿La empresa cuenta con una metodología para evaluar la severidad de los RO y la aplica consistentemente para medir el riesgo inherente y residual, considerando la	No existe metodología para evaluar el RO.	Evaluación puntual, acotada; sin criterios definidos ni distinción entre inherente y residual.	Evaluación con escalas definidas, pero sólo cualitativa o uso inconsistente; controles no ajustan el riesgo residual de forma clara.	Metodología formal, documentada y aplicada en productos, procesos y sistemas crítico; evaluación inherente y residual de forma cuantitativa trazable.	Metodología calibrada con umbrales y usada para priorizar medidas de mitigación; revisión y contraste por función independiente.	Recalibración de metodología periódica basada en resultados (pérdidas, desempeño de controles, tendencias) y mejoras demostrables.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	efectividad de controles?						
11.2 Medición de la criticidad de RO con BDEP	¿La empresa registra y valora pérdidas en la BDEP con reglas consistentes (monto bruto, recuperaciones y provisiones) que permitan medir la criticidad por evento y de manera agregada?	No existe BDEP o no se valora la criticidad.	Registro parcial y no estandarizado; valoración sin reglas; baja confiabilidad.	BDEP definida pero incompleta; aplicadas de forma irregular para reglas de monto bruto, provisiones y recuperaciones.	BDEP cumple con información mínima, clasificación objetiva, umbrales y expedientes; registros trazables de monto bruto, provisiones y recuperaciones.	Calidad de datos gestionada (validaciones, consistencia contable); análisis de criticidad por tipo de evento y línea; expedientes robustos.	Analítica avanzada y uso prospectivo de la BDEP; mejora continua y uso sistemático para tendencias, aprendizaje y priorización.
11.3 Escenarios para eventos severos de RO	¿La empresa desarrolla escenarios análisis de escenarios para eventos severos y usa sus resultados en la evaluación de cambios en el ambiente interno y externo?	No se analiza escenarios.	Ejercicios puntuales y teóricos; sin cuantificación, criterios de criticidad ni cobertura relevante.	Análisis sin criterios para su ejecución con insumos inconsistentes; sin aplicación a cambios internos y externos.	Proceso formal con participación multitarea; escenarios para eventos severos documentados; resultados trazables y revisables.	Resultados integrados a decisiones de tratamiento y aplicados a cambios internos y externos.	Monitoreo continuo con indicadores tempranos; mejoras por lecciones aprendidas; ajustes anticipados y medibles.
11.4 Monitoreo y reporte de criticidad de RO	¿La empresa monitorea la criticidad de RO mediante indicadores (KRIs) y reporta	No existe monitoreo ni reporte de criticidad.	Reportes reactivos post-evento; sin umbrales ni seguimiento formal.	Indicadores con monitoreo parcial o umbrales desactualizados; reportes irregulares; baja	Indicadores con monitoreo definido y revisión periódica de umbrales; reportes periódicos de riesgos y pérdidas	Resultados de los indicadores gatillan escalamiento; decisiones correctivas y verificación; análisis sistemático para	Tableros y alertas tempranas; revisión periódica del manual de GRO; decisiones basadas en resultados;

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	riesgos y pérdidas significativas al Directorio y Comité, con decisiones y acciones correctivas trazables?			trazabilidad de decisiones y acciones.	significativas; seguimiento trazable.	detectar criticidad emergente.	mejora continua demostrable.
12.1 Priorización de RO según nivel de riesgo	¿La empresa prioriza riesgos RO de manera consistente con exposición inherente y residual, considerando la efectividad de controles?	No existe priorización de RO.	Priorización por juicio de experto; sin criterios comunes ni trazabilidad.	Criterios de priorización definido con ejecución parcial (p.ej., solo algunas áreas/riesgos) o aplicada de forma inconsistente.	Metodología de priorización formal, documentada y aplicada en productos, procesos y sistemas crítico; evidencia trazable y criterios entendidos por las áreas.	Priorización integrada a decisiones; revisiones con periodicidad definida.	Recalibración de la metodología de priorización periódica basada en resultados; consistencia transversal y mejora continua demostrable.
12.2 Actualización periodica de la priorización de RO	¿La empresa actualiza de forma perídica la priorización de riesgos RO con base en en el perfil de RO, indicadores (KRIs) y análisis de la BDEP?	No existe periodicidad para actualizar la priorización.	Actualización reactiva; sin considerar la BDEP e indicadores.	Actualización sin periodicidad definida; considera Indicadores (KRIs) y BDEP.	Proceso formal de actualización de priorización que considera indicadores (KRIs) y BDEP utilizada; reportes periódicos con evidencia trazable.	Periodicidad diferenciada por productos/procesos/sistemas.	Mejora continúa basada en tendencias; trazabilidad del flujo y aprobaciones.
12.3 Ajuste de priorización de RO ante eventos	¿La empresa actualiza su priorización ante la ocurrencia de	No existe priorización ante eventos.	Actualización parcial y no estandarizada ante la ocurrencia	Actualización incompleta y no oportuna ante la ocurrencia de	Proceso formal de actualización de priorización ante eventos internos y externos;	Tiempo de análisis diferenciado por naturaleza de evento, producto, procesos y sistemas.	Mejora continua y trazabilidad de los cambios de las

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	eventos internos y externos severos, y cuenta con criterios que gatillean la revisión y reordenamiento de prioridades?		de eventos internos y externos.	eventos internos y externos.	decisiones documentadas y roles claros.		prioridades ante los eventos.
13.1 Tratamiento de RO fuera del nivel aceptable	¿La empresa define y ejecuta medidas de tratamiento y planes de acción para riesgos operacionales no aceptables, con seguimiento, responsables, plazos y mecanismos para asegurar cumplimiento?	No existen medidas de tratamiento ni planes de acción.	Lineamientos informales para el tratamiento de riesgos sin planes de acción, responsables ni trazabilidad.	Medidas de tratamiento y planes de acción definidos parcialmente; cobertura limitada o seguimiento inconsistente; recursos no asegurados.	Medidas de tratamiento formal y documentada para riesgos con nivel no aceptable; planes de acción formales con responsables, plazos y evidencias.	Lineamientos para el escalamiento por desvíos, incumplimientos y reprogramaciones; para definir medidas compensatorias para planes de acción cuya implementación supere los plazos definidos.	Medición de efectividad del tratamiento y mejora continua basada en resultados.
13.2 Respuestas a eventos de RO	¿La empresa cuenta con procesos y protocolos para responder ante eventos de RO; realiza análisis de causa raíz y deficiencias de control; y ejecuta acciones correctivas y	No existen protocolos ni análisis; no se generan acciones.	Acciones informales y puntuales ante eventos, sin identificar causa raíz ni trazabilidad.	Protocolos y análisis existen, pero incompletos o aplicados irregularmente; acciones no se cierran consistentemente.	Proceso formal, documentado y con aplicación consistente, incluye el registro del evento, análisis de causa raíz, y acciones correctivas con responsables y fechas; cierre trazable.	Análisis de tendencias y de diferencias de control; criterios para escalamiento definido; definición de acciones concretas para prevenir recurrencia.	Analítica y aprendizaje continuo; reducción demostrable de recurrencia y tiempos de cierre.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	para evitar recurrencia registradas y trazables?						
13.3 Tratamiento de RO en cambios internos	¿La empresa asegura la incorporación de medidas de tratamiento para NPCI y servicios provistos por terceros, con evaluación previa, aprobación y seguimiento post-implementación?	No se definen respuestas ante NPCI y servicios provistos por terceros.	Incorporación puntual, con poca anticipación o después de su ejecución; con participación no definida; medidas de mitigación definidas, pero no aprobadas.	Procedimiento definido parcialmente; medidas de mitigación no trazables.	Medidas de mitigación consistentes con evaluación de RO y definidas antes de la ejecución; responsabilidades definidas claras y evidencia de su cumplimiento.	Monitoreo post-implementación del NPCI y durante vigencia del servicio; aprobaciones y decisiones trazables.	Monitoreo de medidas de tratamiento de NPCI y servicios provistos por terceros integrado; reducción demostrable de recurrencia; mejoras continuas basadas en resultados e incidentes.
13.4 Transferencia de RO y programa de seguros	¿La empresa evalúa, aprueba y monitorea la transferencia de riesgos (p.ej., seguros) como medida de mitigación adicional a controles, alineada con apetito y capacidad financiera?	No existe evaluación para transferir el riesgo, ni procesos para contratar seguros.	Seguros contratados por costumbre; sin evaluación de cobertura, ni de riesgos asociados.	Proceso definido pero parcial; no se vincula consistentemente con apetito ni se revisa periódicamente.	Proceso formal; evaluación de alternativas para transferencia; responsabilidades definidas claras y evidencia de su cumplimiento.	Portafolio de transferencia monitoreado con revisión periódica y alineamiento al apetito y capacidad financiera.	Portafolio de transferencia balanceado con controles; simulación de escenarios para calibrar seguros; ajustes continuos y resultados verificables.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
14.1 Perfil consolidado de RO para decisiones	¿La empresa consolida y presenta una visión agregada del perfil de RO (KRIs, pérdidas y exposiciones significativas) de manera periodica y lo reporta con la forma/periodicidad definida para decisiones y acciones?	No existe consolidación ni reportes de perfil RO a nivel empresa.	Reportes aislados por áreas; sin periodicidad definida, ni responsable de consolidación, ni visión agregada.	Consolidación parcial (solo algunas unidades o datos); periodicidad irregular; no incluye KRIs, pérdidas o exposiciones significativas.	Reporte consolidado periódico con KRIs, pérdidas y principales exposiciones; responsable de consolidación definido.	Umbrales, tendencias y concentraciones gatillan escalamiento; trazabilidad de fuentes y criterios; reportes se usan en Comités o Directorio para priorizar acciones y recursos.	Analítica y alertas tempranas optimizadas; uso y mejora continua de tableros; proceso basado y ajustado por resultados y desempeño.
14.2 Integración metodológica de RO	¿La empresa aplica la metodología RO de forma consistente en toda la empresa e integrada a la GIR, permitiendo consolidar riesgos por productos, procesos, unidades con soporte de la Unidad de Riesgos?	No se aplica metodología de RO de forma consistente en toda la empresa.	Lineamientos generales; aplicación puntual; proceso susceptible a errores.	Metodología definida, pero cobertura parcial o aplicación inconsistente entre unidades.	Metodología formal y documentada con implementación consistente en unidades; consolidación por productos, procesos, unidades; soporte y coordinación efectiva de la Unidad de Riesgos.	Revisiones periódicas de calidad y consistencia; ajustes ante cambios relevantes; trazabilidad de revisiones y ajustes.	Mejora continua con métricas de desempeño y retroalimentación.
14.3 Inventarios centralizados	¿La empresa mantiene un	No existen inventarios	Listados aislados; sin	Registro definido pero incompleto;	Registro completo y actualizado de productos,	Actualización de registro integrada a cambios en la	Definición de criterios de

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
para exposición a RO	registro centralizado y actualizado de productos, procesos, servicios provistos por terceros, y usa ese inventario para evaluar y monitorear riesgos y cambios relevantes?	centralizados de RO.	criterios de significancia ni actualización controlada.	identificación parcial de productos, procesos, servicios provistos por terceros; uso limitado para gestión.	procesos, servicios provistos por terceros; mantenimiento de registros formal y documentado.	organización; trazabilidad de cambios y ajustes en los registros.	decisión ante cambios en inventario; alertas ante vencimientos y renovaciones.
14.4 Análisis de tendencias de RO con BDEP	¿La empresa registra y clasifica eventos de RO en la BDEP con criterios objetivos (tipos, líneas, agrupación), incluyendo eventos múltiples y categorías especiales (legal, reputación, etc.), para análisis de tendencias y concentraciones?	No existe BDEP, ni análisis.	Registro básico e incompleto; sin taxonomías ni reglas de agrupación ni clasificación clara.	Taxonomía y campos definidos pero aplicados de forma inconsistente; reglas incompletas de eventos múltiples y categorías.	Registro completo con criterios objetivos; reglas de pérdidas múltiples y categorías especiales aplicadas consistentemente; análisis periódico de portafolio descriptivo de BDEP.	Análisis periódico de portafolio de tendencias y concentraciones; hallazgos son convertidos en decisiones y acciones concretas para gestionar los riesgos; calidad de datos trazable.	Analítica avanzada e integración con indicadores y escenarios; mejora continua de taxonomía y calidad de datos basada en resultados.
15.1 Gobierno de los NPCI	¿La empresa cuenta con	No existen metodologías,	Documentación parcial o	Documentación aprobada con	Metodología, políticas y procedimientos unificados y	Metodología, políticas y procedimientos con	Metodología, políticas y

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	metodología, políticas y procedimientos que definan el flujo de gestión de NPCI, con responsabilidades definidas, criterios objetivos y revisiones periódicas independientes?	políticas ni procedimientos para gestión de NPCI.	informal; criterios y roles no definidos.	cobertura limitada (definiciones incompletas).	documentados; roles claros; criterios objetivos y controles de implementación definidos.	revisiones periódicas de efectividad documentadas; supervisión activa de NPCI (seguimiento, escalamiento, remediaciones).	procedimientos con métricas e indicadores (KRIS) del proceso, lecciones aprendidas y mejora continua; validación independiente robusta.
15.2 Evaluación de RO a NPCI	¿La evaluación del NPCI cubre de forma trazable el ciclo completo, considerando el riesgo inherente, impacto en perfil, apetito y tolerancia; controles o medidas de mitigación; riesgo residual; límites y métricas de monitoreo?	No se evalúan los RO de NPCI.	Evaluación acotada y tardía (solo antes de salir a producción).	Evaluación existe, pero no cubre desde la concepción hasta la post implementación.	Evaluación completa y documentada por etapas; con participación de la segunda línea desde la concepción hasta la post implementación.	Monitoreo post-implementación con métricas y umbrales; ajustes y remediaciones oportunas por hallazgos.	Retroalimentación sistemática y recalibración continua del perfil de riesgo del cambio.
15.3 Reporte y remisión de NPCI	¿Los informes de NPCI cumplen con contenido	No se realizan informes de NPCI.	Informes sin contenido mínimo ni	Informes con contenido mínimo; aprobaciones	Informes con contenido mínimo; aprobación formal previa; remisión a SBS dentro de plazos definidos.	Seguimiento post-aprobación; evidencia de acciones ante desviaciones.	Reportes con indicadores (KRIS) tempranos y control de calidad

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	mínimo exigido por SBS, se aprueban formalmente por los órganos competentes y se remiten dentro de los plazos regulatorios?		aprobaciones formales.	informales; plazos incumplidos.			de todo el flujo de reportes.
16.1 Revisión del manual de GRO	¿La empresa revisa periódicamente el manual de GRO incorporando los cambios del entorno, negocio, pérdidas y brechas y ajustes verificables?	No existe revisión del manual de GRO.	Revisión ocasional y reactiva; sin criterios ni periodicidad.	Revisión periódica definida, pero de alcance parcial o sin evidencia suficiente.	Revisión periódica integral documentada del manual de GRO con análisis de entorno, negocio, pérdidas y brechas.	Ajustes y medidas correctivas oportunas; seguimiento trazable a cumplimiento y cierre de brechas.	Revisión prospectiva (tendencias y escenarios) con aprendizaje continuo.
16.2 Monitoreo del perfil de RO frente a umbrales	¿Se monitorean indicadores (KRIs) y desempeño vs umbrales, con reportes periódicos y acciones efectivas ante desviaciones?	No existe monitoreo de indicadores ni umbrales definidos.	Monitoreo parcial; sin umbrales; sin reportes formales.	Indicadores (KRIs) existen, pero no se vinculan bien a riesgos y no se analiza el desempeño vs umbrales.	Indicadores (KRIs) relacionados correctamente a riesgos; reportes periódicos con análisis de desempeño vs umbrales y acciones ante desviaciones.	Procedimientos para tomar acciones; escalamiento y remediación trazable ante desviaciones.	Tableros y alertas tempranas con análisis de causa; medición de efectividad en ciclo cerrado.
16.3 Aseguramiento y	¿Se evaluan y prueban	No existe evaluación ni	Pruebas puntuales y	Procedimiento definido	Proceso formal y documentado considerando	Resultados se integran a decisiones y planes;	Aseguramiento continuo y mejora

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
pruebas de controles clave de RO	periódicamente controles clave con segregación y cobertura adecuada y se ejecutan acciones ante desviaciones?	pruebas de controles.	reactivas, sin enfoque de controles clave.	parcialmente; pruebas incompletas (alcance limitado, baja trazabilidad o sin seguimiento).	segregación y cobertura adecuada; controles clave identificados con diseño y efectividad operativa evaluada y probada.	verificación post-remediación; seguimiento periódico por criticidad.	sostenida del entorno de control.
17.1 Gestión de observaciones de RO	¿La empresa asegura el cierre oportuno y efectivo de observaciones sobre RO de Auditoría Interna, Auditoría Externa y SBS y cuenta con un control de recurrencia?	No se asegura el cierre de observaciones de RO.	Cierre de observaciones parcial, sin periodo definido; sin registro de avance y cierre.	Cierre de observaciones en plazo definido; registro básico de planes y responsables.	Seguimiento periódico de planes con responsables y plazos; reporte a los órganos correspondientes; cierre con evidencia.	Cuenta con un control de recurrencia histórico.	Reporte con indicadores de eficiencia en el cumplimiento del plazo de cierre de observaciones.
17.2 Definición del proceso de mejora continua de GRO	¿La empresa define y documenta un proceso de mejora continua de la GRO que define fuentes, roles (tres líneas), periodicidad y criterios para priorizar y aprobar mejoras?	No existe proceso de mejora continua.	Se reconoce la necesidad, pero es informal y sin documentación.	Proceso parcial, con cobertura de algunas fuentes o roles y sin criterios de priorización.	Proceso documentado con roles, fuentes y periodicidad definida; incluye criterios para aprobar y priorizar mejoras.	Proceso robusto, incluye fuentes externas, aprendizaje de mejores prácticas, cambios del entorno y control.	Proceso dinámico, revisado y ajustado periódicamente; mejora continua integrada a estrategia.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
17.3 Ejecución y verificación de mejoras de la GRO	¿La empresa ejecuta y verifica mejoras de la GRO mediante planes de acción trazables (responsables, recursos, plazos e indicadores), con seguimiento, cierre y evidencia de efectividad, incluyendo ajustes a documentos, capacitación e intervenciones por desviaciones?	No se ejecutan mejoras ni existe evidencia.	Mejoras reactivas y aisladas; sin seguimiento ni cierre verificable.	Planes de mejora existen, pero con brechas de priorización, responsables, plazos o evidencia de efectividad.	Ejecución con seguimiento periódico y cierres documentados; ajustes a manuales y procedimientos cuando corresponde.	Verificación de efectividad (tendencias de pérdidas, métricas, desviaciones); mejora de reportes y datos; acciones oportunas ante desviaciones.	Mejora continua demostrable y sostenida; incorpora mejores prácticas; resultados consistentes y trazables en toda la organización.
18.1 Sistema informatico para la GRO	¿La empresa cuenta con sistemas especializados para la GRO y soporte de la BDEP asegurando datos oportunos, precisos, íntegros y trazables?	No existen sistemas especializados para la GRO.	Gestión soportada en herramientas básicas o insuficientes; reportes sin consistencia ni control de calidad.	Sistemas con cobertura parciales (solo GRO o solo BDEP) o no integrados entre sí; controles de calidad de datos incipientes.	Sistema especializado para la GRO que soportan la BDEP; reportes periódicos por proceso y unidad; incluye datos precisos e íntegros.	Integración de fuentes; aseguramiento de calidad robusto (completitud, exactitud, puntualidad); trazabilidad y conciliaciones.	Arquitectura integrada de todos los sistemas con un repositorio oficial y confiable de datos; automatización de cargas y validaciones; métricas de calidad y mejora continua con auditoría de datos.
18.2 Analitica de datos y	¿La empresa cuenta con	No existe procesos de	Procesos de analítica y	Procesos de analítica y	Procesos para promover la analítica y automatización	Cuenta con revisiones y actualizaciones	Procesos altamente consistentes y

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
automatización para la GRO	procesos para promover la analítica de datos y automatización de procesos relacionados a la GRO?	analítica de datos ni automatización para la GRO.	automatización parciales e informales, sin roles ni responsabilidades definidas.	automatización documentado, pero con brechas; roles y responsabilidades definidos, pero no tiene una periodicidad establecida.	documentado y difundido; con roles y responsabilidades definidos; periodicidad establecida.	documentadas; trazabilidad; estandarización verificable.	mantenidos; cambios controlados.
19.1 Coordinación y comunicación sobre RO	¿La empresa tiene mecanismos de coordinación y comunicación transversal para gestionar RO entre las tres líneas y niveles de la organización, con roles claros y sin duplicidades?	No existe coordinación ni comunicación transversal de RO.	Coordinación y comunicación reactiva e informal para casos puntuales, sin responsables claros.	Coordinación y comunicación con instancias y canales parciales, solo algunas áreas; sin roles claros.	Mecanismos definidos y documentados; roles y responsabilidades claras por líneas y niveles de organización; uso consistente en áreas principales.	Coordinación y comunicación integrada a la estructura de gestión; seguimiento de brechas.	Coordinaciones y comunicaciones incluyen seguimiento de alertas y desviaciones de la GRO.
19.2 Flujo y escalamiento de información de RO	¿La empresa define y aplica reglas para comunicar y escalar oportunamente eventos, alertas, indicadores y cambios del perfil de entre prim RO era y	No se define ni aplica reglas; la información se queda en áreas.	Escalamiento informal y tardío; no se cuenta con criterios definidos.	Reglas puntuales para algunos temas (p.ej., incidentes), aplicación irregular.	Reglas definidas (qué, cuándo, a quién); canales establecidos; aplicación consistente.	Escalamiento oportuno y trazable (registros, tiempos objetivo); se monitorea cumplimiento y se corrigen retrasos.	Escalamiento predictivo y temprano (alertas, umbrales); mejora continua basada en análisis de “casi incidentes”, tendencias y lecciones aprendidas.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	segunda línea y niveles que corresponda según los canales establecidos?						
20.1 Gobierno del reporte de RO	¿La empresa tiene definidos formalmente los reportes de RO (forma, periodicidad, destinatarios y responsables) y puede emitirlos oportunamente en condiciones normales y de contingencia?	No existe esquema formal de reportes de RO.	Reportes puntuales; sin periodicidad definida.	Reportes con periodicidad parcial; responsabilidades poco claras; cobertura limitada.	Esquema formal y documentado de reportes (forma, frecuencia, responsables, destinatarios); cumplimiento consistente.	Reporte oportuno y trazable (SLAs, fechas); controles de calidad definidos; capacidad de reporte en contingencia.	Reporte con continuidad asegurada; revisiones periódicas y ajustes por cambios del perfil de riesgo.
20.2 Contenido y calidad del reporte de RO	¿Los reportes de RO incluyen información clave (perfil agregado, indicadores (KRIs) y tendencias, eventos y pérdidas relevantes, incumplimientos de límites, riesgos clave y emergentes) con	No existen reportes de RO.	Reportes incompletos o no confiables; contenido descriptivo; poca utilidad para decisión.	Reportes con contenido parcial, incluye algunos elementos (p.ej., incidentes o indicadores), sin consistencia ni análisis.	Reportes incluyen contenido mínimo de forma consistente; información precisa y coherente; orientado a decisión.	Reportes incluyen análisis de tendencias, concentraciones, causas, riesgos emergentes, y comparación con apetito y límites; se cuenta con controles de calidad.	Reportes con narrativa ejecutiva, y mejora continua del contenido según desempeño y comentarios del Directorio y Gerencia.

Criterio	Pregunta	0 - Inmadura	1 - Inicial	2 - En progreso	3 - Definido	4 - Gestionado	5 - Optimizado
	calidad y utilidad para decisiones y supervisión?						
20.3 Reporte regulatorio y divulgación pública de RO	¿La empresa cumple con reportes regulatorios de RO y realiza divulgación pública proporcional y controlada, con política formal y controles del proceso?	No existen lineamientos para reportes regulatorios ni divulgación.	Reportes con envío fuera de plazo; con ajustes frecuentes; sin controles formales.	Reportes con envío dentro del plazo; política de controles poco desarrollada.	Reportes en plazo y con responsables designados; política y procedimiento formal para divulgación cuando corresponda.	Cumplimiento robusto con controles de calidad y veracidad; validaciones y trazabilidad; revisión periódica de política de divulgación.	Evaluación sistemática de idoneidad de divulgación; aprendizaje continuo de observaciones regulatorias y mercado.