Metodología para el análisis y gestión de riesgos en seguridad de las Pymes considerando software OpenSource

Marco Tulio Silva Castillo

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2026

Metodología para el análisis y gestión de riesgos en seguridad de las Pymes considerando software OpenSource

Marco Tulio Silva Castillo

Tesis o trabajo de investigación presentado como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director:

Coordinador de la Maestría en Seguridad Informática, Héctor Fernando Vargas Montoya

Línea de Investigación:

Ciencias Computacionales en la que se enmarca la tesis o trabajo de investigación

Grupo de Investigación:

Automática, Electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2026

Dedicatoria

A la memoria de mi padre,
a la persistencia de mi madre
y al propósito valioso en mi hija.

Porque lo difícil se hace fácil
cuando se ha aprendido bien lo fácil.

Matusini

Agradecimientos

Primeramente dar gracias a Dios por su infinito amor incondicional, por sostenerme en los momentos de incertidumbre y por permitirme culminar este proceso con gratitud, aprendizaje y esperanza. No fue fácil; nunca lo fue. Sin embargo, al mirar el camino recorrido, reconozco que cada obstáculo superado hizo parte de una construcción más profunda de carácter, disciplina y fe. Hoy puedo decir con humildad: gracias, Dios.

Este documento es el resultado de un proceso investigativo desarrollado durante tres años intensos, exigentes y profundamente formativos. Fueron años de retos, altibajos, cuestionamientos, ajustes y decisiones que pusieron a prueba mi disciplina y mi tenacidad de avanzar aun cuando el camino parecía difícil. En ese recorrido fue fundamental el acompañamiento de mi director, Héctor Fernando Vargas Montoya, a quien he conocido con respeto y aprecio como don Héctor. Su orientación, sus aportes y su confianza fueron decisivos para darle rumbo, profundidad y sentido a esta investigación.

Dedico este logro a la memoria de mi padre, cuya partida al inicio de la maestría marcó un punto decisivo en mi vida. Su ausencia me acompañó de una manera silenciosa, profunda y transformadora. Este trabajo también es una forma de honrar su memoria, de agradecer lo que sembró en mí y de reconocer que, incluso en medio del dolor, fue posible seguir adelante. A mi madre, gracias por su amor, su fortaleza y su presencia constante; su apoyo ha sido refugio, impulso y ejemplo. A mi hija, mi mayor motor, gracias por recordarme cada día por qué valía la pena continuar. Pensar en su futuro me dio fuerza en los días difíciles y sentido en los momentos de cansancio.

Me llena de satisfacción reconocer que esta tesis tuvo una relación directa con mi participación como estudiante consultor en el proyecto de investigación titulado “Prototipo funcional de una plataforma informática para la gestión de riesgo de seguridad de la información y pentesting desarrollada con tecnologías de automatización y técnicas de inteligencia artificial”, específicamente en el componente de gestión de riesgos de seguridad de la información. Esa experiencia me permitió conectar la formación académica con un escenario aplicado, comprender

mejor las necesidades de las organizaciones y fortalecer la orientación práctica de la propuesta desarrollada.

Agradezco también a mis compañeros de estudio, con quienes compartí clases, conversaciones, dudas, aprendizajes y momentos de exigencia académica. Cada intercambio, cada discusión y cada experiencia compartida aportó a mi crecimiento personal y profesional. En muchos momentos, la compañía de quienes recorrían un camino similar permitió hacer más llevadera la carga y recordar que la maestría no solo se vive desde el esfuerzo individual, sino también desde la construcción colectiva.

Extiendo mi gratitud a los profesores que, a través de sus magistrales clases, experiencias y reflexiones, aportaron elementos fundamentales para comprender el riesgo, la incertidumbre y la seguridad informática desde distintas perspectivas. Sus enseñanzas, sumadas a la participación en espacios académicos, foros y seminarios, contribuyeron a enfocar este proyecto hacia una propuesta de profundización con valor metodológico y práctico para futuros procesos de análisis y gestión de riesgos en pequeñas y medianas empresas.

Agradezco al Instituto Tecnológico Metropolitano (ITM), mi alma máter, por el apoyo recibido durante este camino y por propiciar espacios de aprendizaje, bienestar y crecimiento personal. Reconozco de manera especial los programas y condiciones que facilitaron el cuidado de mi hija, así como los entornos físicos y humanos que me permitieron mantener la resiliencia, la tranquilidad y la motivación necesarias para avanzar.

También agradezco a todas las personas que, en distintos momentos, han visto en mí a alguien que ayuda, orienta o aporta, aun cuando yo mismo no siempre he sido consciente del impacto que puedo causar. Sus palabras, su confianza y su reconocimiento me han recordado que el conocimiento cobra verdadero sentido cuando se pone al servicio de otros. Este trabajo no solo representa un logro académico, sino también una invitación a seguir contribuyendo desde la seguridad informática, la gestión de riesgos y el acompañamiento a organizaciones que necesitan soluciones prácticas y posibles.

Finalmente, este logro representa una apuesta personal por el futuro. Cada palabra escrita, cada concepto revisado y cada análisis realizado fueron parte de una decisión sostenida: actuar con disciplina para alcanzar una meta significativa. Hoy miro este trabajo con orgullo, no solo por el esfuerzo invertido, sino porque confío en que puede aportar a la academia y a la industria en la identificación, valoración y tratamiento de riesgos de seguridad de la información, especialmente en pymes latinoamericanas que enfrentan desafíos crecientes en sus procesos de transformación digital.

Resumen

Las pymes del sector servicios en Colombia enfrentan dificultades para gestionar riesgos de seguridad informática debido a recursos limitados, baja madurez digital, ausencia de personal especializado y aplicación poco sistemática de referentes internacionales. Esta investigación propuso una metodología de análisis y gestión de riesgos orientada a fortalecer la protección de activos en este contexto. El diseño fue propositivo-aplicado, con enfoque mixto, y se desarrolló en cuatro fases: caracterización de referentes, selección de herramienta, instrumentación tecnológica y validación mediante prueba de escritorio. Se empleó AHP para priorizar cinco referentes internacionales, seleccionando OCTAVE-S v1.0 como base metodológica, y para evaluar herramientas de soporte, seleccionando MONARC. La metodología se instrumentó en un entorno controlado y se validó con el caso simulado "PyME Servicios Colombia", construido a partir de patrones identificados en un instrumento diagnóstico de apoyo aplicado previamente a 72 organizaciones. Los resultados permitieron identificar activos críticos, valorar riesgos, definir tratamientos, asignar responsables y generar evidencias documentales. Se concluye que la integración de referentes híbridos y software OpenSource ofrece una alternativa viable, trazable y aplicable para pymes con baja madurez digital.

Palabras clave: Gestión de riesgos, Seguridad Informática, Pymes, Software de código abierto, MONARC, Metodología, Estándares internacionales.

Abstract

Service-sector SMEs in Colombia face difficulties managing information security risks due to limited resources, low digital maturity, lack of specialized personnel, and unsystematic application of international references. This research proposed a risk analysis and management methodology aimed at strengthening asset protection in this context. The study followed an applied-propositional design with a mixed approach and was developed in four phases: characterization of references, tool selection, technological instrumentation, and validation through a desk-based test. AHP was used to prioritize five international references, selecting OCTAVE-S v1.0 as the methodological basis, and to evaluate support tools, selecting MONARC. The methodology was instrumented in a controlled environment and validated through the simulated case "PyME Servicios Colombia," built from patterns identified in a supporting diagnostic instrument previously applied to 72 organizations. The results made it possible to identify critical assets, assess risks, define treatments, assign responsibilities, and generate documentary evidence. It is concluded that the integration of hybrid references and OpenSource software offers a viable, traceable, and applicable alternative for SMEs with low digital maturity.

Keywords: Risk Management, Computer Security, SMEs, Open Source Software, MONARC, Methodology, International Standards.

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de abreviaturas

Abreviaturas

Abreviatura	Término
AN	Adopción de Normas
CI	Capacidad de Implementación
CISO	Chief Information Security Officer
CN	Cumplimiento Normativo
CS	Conciencia de Seguridad
CR	Razón de consistencia
DN	Directrices de Normas
EBIOS	Expression des besoins et Identification des Objectifs de Sécurité
ENISA	European Union Agency For Network And Information Security
EH	Efectividad de las Herramientas
ER	Evaluación de Riesgos
GR	Gestión de Riesgos
GPL	General Public License
HOS	Herramientas OpenSource
IEC	International Electrotechnical Commission
IH	Implementación de Herramientas
INCIBE	Instituto Nacional de Ciberseguridad de España
IR	Identificación de Riesgos
ISO	International Organization for Standardization
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones
MARC	Machine Readable Cataloging
MiPyME	Micro, pequeñas y medianas empresas

Abreviatura	Término
MR	Monitoreo y Revisión de Riesgos
NI	Normas Internacionales
NIST	National Institute of Standards and Technology
OCTAVE	Operational Critical, Threat, Asset and Vulnerability Evaluation
OE	Objetivo Específico
OET	Objetivo Específico Tesis
P	Pymes
PYME	Pequeña y mediana empresa
RD	Recursos Disponibles
RDA	Recursos, Descripción y Acceso
RI	Índice Aleatorio
RMF	Risk Management Framework
SGSI	Sistema de Gestión de Seguridad de la Información
SH	Selección de Herramientas
SUS	System Usability Scale
TI	Tecnologías de Información
TIC	Tecnologías de Información y las Comunicaciones
TR	Tratamiento de Riesgos
UIT	Unión Internacional de Telecomunicaciones
VM	Virtual Machine (máquina virtual)

Introducción

En primera instancia, para abordar este desafío, esta investigación establece el objetivo general: "Proponer una metodología para el análisis y gestión de riesgos de seguridad informática en PyMEs, basada en normas internacionales y software OpenSource disponibles, que fortalezca la seguridad y contribuya a la protección de sus activos y operaciones". Así mismo, plantea objetivos específicos:

- "1. Caracterizar normas internacionales para la gestión de riesgos comprendiendo los principios, directrices y requisitos que se puedan ajustar a la seguridad informática en las PyMEs.
- 2. Analizar herramientas y soluciones de software OpenSource que puedan ajustarse a la gestión de riesgos, seleccionando uno o varios softwares a utilizar.
- 3. Usar el (los) software OpenSource para la gestión de riesgos en seguridad informática en las PyMEs y que dé cumplimiento a la metodología propuesta.
- 4. Validar la metodología propuesta a través de su aplicación con un caso de estudio o prueba de escritorio en una PyME".

En el contexto actual, la creciente digitalización y dependencia tecnológica han hecho evidente la vulnerabilidad de las pequeñas y medianas empresas (PyMEs), particularmente aquellas pertenecientes al sector servicios en Colombia. Cada vez es más difícil ignorar la importancia que estas organizaciones tienen para la economía nacional; sin embargo, muchas de ellas enfrentan serios desafíos frente al incremento de las amenazas cibernéticas. En efecto, pese a que existen normativas internacionales como ISO/IEC 27001 o los marcos de ciberseguridad propuestos por el NIST, así como herramientas Open Source (código libre) accesibles para gestionar estos riesgos, muchas PyMEs carecen de metodologías integrales y sistemáticas que combinen ambos elementos [1].

Sin embargo, esta problemática no solo compromete la protección de sus activos críticos, sino que también genera consecuencias severas en su sustentabilidad y competitividad, impactando negativamente su capacidad para permanecer operativas en el largo plazo [2]. Esta situación se vuelve particularmente alarmante en un periodo clave como el comprendido entre julio de 2023 y junio de 2024. De ahí que, la relevancia de esta investigación radica en la creciente vulnerabilidad

de las PyMEs ante amenazas cibernéticas debido a la limitada adopción de prácticas estructuradas de gestión de riesgos.

A nivel internacional, diversos estudios y reportes basados en fuentes primarias han revelado cifras alarmantes, destacando la exposición que enfrentan las PyMEs a los desafíos en ciberseguridad. Por ejemplo, una encuesta realizada a 605 PyMEs en Singapur indicó que tan solo el 47% de sus ejecutivos estaban plenamente conscientes de los riesgos cibernéticos, cifra que descendió con respecto al año anterior [3]. Más aún, la ENISA reportó que más del 80 % de las PyMEs encuestadas consideró que los problemas de ciberseguridad tendrían un impacto serio negativo en su negocio dentro de una semana, y que el 57 % indicó que lo más probable sería volverse insolvente o salir del negocio [4].

Hay que mencionar, además que estas empresas no solo enfrentan pérdidas financieras significativas, sino también daños reputacionales irreparables y sanciones reglamentarias [5]. El Instituto Nacional de Ciberseguridad de España [6] indicó también, que más de la mitad de las PyMEs no cuentan con medidas efectivas de seguridad informática, lo cual las expone considerablemente frente a estos riesgos. Al mismo tiempo, este panorama coincide con otros análisis recientes en diversos sectores que destacan cómo las limitaciones financieras y la falta de experiencia técnica incrementan su vulnerabilidad [7], [8].

En efecto, esta problemática internacional resalta una brecha crítica: las PyMEs que no adoptan estrategias robustas de gestión de riesgos ni implementan metodologías estructuradas suelen enfrentar mayores impactos negativos ante incidentes de seguridad informática. Un estudio del NIST [9] destaca la importancia de integrar normativas internacionales con enfoques adaptativos específicos para PyMEs, y evidencia que aquellas empresas que implementan marcos como ISO/IEC 27001 y NIST logran mitigar efectivamente las amenazas cibernéticas [10]. Más aún, según un informe de SANS [11], [12], la adopción de estrategias alineadas con estándares internacionales mejora significativamente la prevención y gestión de incidentes, fortaleciendo la resiliencia organizacional frente a amenazas cada vez más sofisticadas [13].

En el contexto colombiano, región vulnerable a las ciberamenazas [14], esta situación es igualmente preocupante [15], [16]. Según la Cámara Colombiana de Informática y

Telecomunicaciones, con base en cifras del Centro Cibernético de la Policía Nacional, Colombia registró 77.666 denuncias por cibercrimen en 2024, lo que representó un aumento del 23 % frente a las 63.249 denuncias reportadas en 2023; entre las modalidades más frecuentes se identificaron el hurto por medios informáticos, el acceso abusivo a sistemas informáticos y la violación de datos personales [17], [18]. Este panorama reciente se conecta con antecedentes reportados por la misma Cámara en el informe Tendencias del Cibercrimen en Colombia 2019-2020, donde se informó que en 2019 se habían registrado 28.827 incidentes de ciberseguridad empresarial y que, en el caso de las infecciones por malware [19].

Además, informes de ColCERT señalaron en 2022 que cerca del 70% de las incidencias cibernéticas en Colombia involucraban directamente a las PyMEs, las cuales, además de la ausencia frecuente de personal capacitado en ciberseguridad, no realizan evaluaciones sistemáticas de sus infraestructuras tecnológicas [20]. Un reciente informe del Ministerio de Tecnologías de la Información y Comunicaciones resaltó que un alto porcentaje de estas empresas aún no integra adecuadamente estrategias de ciberseguridad en sus operaciones, lo que incrementa su vulnerabilidad y pone en riesgo su rentabilidad futura [21]. Esto conecta con la información que arrojó un proyecto de investigación que realizaron el ITM y el Grupo NEX, donde en Colombia solo el 50% de las pymes sobrevive el primer año y el 20% lo hace al tercero [22], en la cual se evidencia la fragilidad de este segmento empresarial.

Tal y como lo menciona la revista Forbes, las pymes cuando se trata de ciberseguridad, están ubicadas en una zona conocida como “zona de fuego” [23]. Cifras recientes de Fortinet advierten más de 36.000 millones de intentos de ciberataques en 2024 [24]. Además, argumento Forbes de que ColCERT indica que en ese mismo año, el reporte anual de vulnerabilidades registrado fue de 22.086, siendo el sector salud, manufactura, transporte y logística, automotriz, educación y gobierno los más afectados.

Es así como, estos hallazgos institucionales son consistentes con los datos primarios recolectados para esta investigación, donde se encuentra que un 32% de las PyMEs encuestadas no utiliza ninguna metodología formal para la gestión de riesgos y, de manera preocupante, un 32% de las organizaciones implementa controles de manera 'orgánica' (preventiva y reactiva), es decir, a menudo solo después de que el incidente ha ocurrido [25]. Mientras tanto, el costo promedio de

los incidentes de seguridad informática ha aumentado considerablemente en los últimos años, afectando gravemente su sostenibilidad económica [26].

Recientemente, distintos estudios han abordado la gestión de riesgos de seguridad informática en PyMEs, destacando tanto sus avances como sus limitaciones. Por ejemplo, Alahmari y Duncan [27] realizaron una revisión sistemática de literatura que revela cinco perspectivas clave en la gestión del riesgo cibernético: amenazas, comportamientos, prácticas, conciencia y toma de decisiones, pero concluyen que aún se requieren más estudios empíricos especialmente adaptados a países en desarrollo. Por su parte, Al-Dosari y Fetais [28] advierten que, aunque los marcos normativos como ISO/IEC 27001 y NIST son ampliamente reconocidos, su nivel de abstracción y complejidad técnica limita su aplicabilidad efectiva en PyMEs, y sugieren la necesidad de enfoques más dinámicos e integradores.

Avanzando en los antecedentes generales, Wilson y McDonald [29] argumentan que las estrategias de ciberseguridad no pueden ser uniformes, en efecto, las PyMEs presentan perfiles diversos que requieren enfoques personalizados, tanto en gestión como en estrategias de participación y formación. Además, Wang [30] plantea que el proceso de transformación digital ha incrementado significativamente los riesgos tecnológicos y organizacionales en estas empresas, y propone estrategias de gestión ajustadas al contexto digital como un camino necesario para mejorar su resiliencia.

Por consiguiente, estas contribuciones evidencian que, aunque existe una literatura especializada en constante y creciente expansión de conocimiento, persiste una brecha metodológica en la articulación de referentes internacionales para la gestión de riesgos con herramientas tecnológicas prácticas y accesibles para PyMEs, especialmente en países como Colombia.

De igual modo, la literatura técnica relacionada con PyMEs ha explorado ampliamente los marcos normativos y las soluciones tecnológicas por separado, de modo que, son escasos los estudios que propongan metodologías explícitas que integren ambos elementos de manera sistemática.

Un ejemplo relevante que sirve para ilustrar este frente, aunque fuera del ámbito empresarial, es el trabajo de Rodríguez y Briceño [31], quienes diseñaron y evaluaron una metodología didáctica

para enseñar la creación de catálogos de autoridades en el contexto bibliotecológico, combinando el uso del estándar RDA con el formato tecnológico MARC Autoridades mediante plantillas estructuradas y recursos digitales interactivos. Si aceptamos la limitante de que, su propuesta centrada en el ámbito educativo, en definitiva, demuestra la efectividad de vincular marcos normativos con herramientas tecnológicas específicas para facilitar su comprensión y aplicación práctica. En concreto, esta evidencia respalda la necesidad de metodologías similares, adaptadas a entornos empresariales, donde las PyMEs requieren enfoques accesibles y aplicables que integren normas internacionales de seguridad con soluciones Open Source disponibles en el mercado.

A pesar del reconocimiento y la adopción generalizada de marcos normativos como ISO/IEC 27001 y NIST para la gestión de riesgos en seguridad informática, varios estudios han evidenciado limitaciones importantes en su aplicación a las PyMEs. Sirva de ejemplificación la revisión sistemática de la literatura hecha por Al-Dosari y Fetais [28], anuncian que estos marcos presentan no sólo un alto grado de abstracción, sino también escasa adaptabilidad a entornos tecnológicos cambiantes, excesiva orientación al cumplimiento regulatorio, más que a la mitigación proactiva de riesgos.

Con esto quiere decir que advierten que la complejidad de implementación y la falta de herramientas de evaluación simples obstaculizan su adopción por parte de organizaciones con recursos limitados. Todo esto parece confirmar que los modelos existentes ignoran con frecuencia factores humanos y organizacionales, por tanto, reduce la efectividad de las evaluaciones de riesgo en contextos reales. Además del respaldo teórico y documental expuesto, la presente investigación se apoya en evidencia empírica que confirma la existencia real y vigente del problema de investigación en el contexto de las pymes colombianas del sector servicios.

En particular, esta justificación empírica se fundamenta en los resultados del Instrumento de Diagnóstico sobre Gestión de Riesgos de Seguridad de la Información, desarrollado en el marco de un proyecto de investigación de mayor alcance liderado conjuntamente por el Instituto Tecnológico Metropolitano (ITM) y el Grupo Nex, orientado al diseño de un prototipo funcional de plataforma informática para la gestión de riesgos y pruebas de penetración mediante automatización e inteligencia artificial [25]. Los resultados del instrumento, con una muestra válida de 72 organizaciones, evidenciaron brechas estructurales relevantes: un 32 % de las organizaciones

encuestadas no utiliza ninguna metodología formal de gestión de riesgos, mientras que un 42 % carece de planes de control definidos, y un 20 % actúa de forma reactiva ante incidentes de ciberseguridad. Adicionalmente, se identificó una alta dependencia de herramientas ofimáticas como Excel (39,6 %) y Word (21 %), lo cual evidencia una falta de procesos sistemáticos y automatizados que aseguren la trazabilidad y la eficiencia [25].

De manera significativa, estos hallazgos ponen en evidencia una disonancia entre la percepción y la práctica: aunque más del 78 % de las organizaciones reconoce la importancia de la gestión de riesgos, esta conciencia no se traduce en procesos formales ni en metodologías aplicadas, especialmente en el sector servicios. La brecha empírica resulta consistente con lo señalado por la literatura reciente y refuerza la necesidad de una propuesta metodológica práctica, accesible y contextualmente adaptada.

Es importante precisar que los resultados del Instrumento de Diagnóstico no constituyen el instrumento principal de recolección de datos de la presente tesis, sino que fueron utilizados exclusivamente como insumo empírico de apoyo a la justificación del problema de investigación y al desarrollo del cuarto objetivo específico. Se participó en dicho proyecto como joven investigador, colaborando específicamente en el diseño del módulo de gestión de riesgos, sin intervenir en otros módulos del instrumento, tales como pentesting o automatización avanzada, lo cual se expone de manera explícita como práctica ética y transparente de investigación.

A partir de esta evidencia empírica, se justifica la selección de una pyme del sector servicios colombiano como contexto de aplicación para la validación de la metodología propuesta. En adición, la literatura especializada muestra que, si bien los sectores financieros y de salud han sido ampliamente estudiados, el sector servicios presenta una alta criticidad debido al manejo intensivo de información de terceros, activos intangibles y procesos digitales, sin que exista una cobertura equivalente en investigaciones aplicadas. En consecuencia, el contexto seleccionado permite ilustrar de manera representativa una organización con: activos de información críticos, controles técnicos aislados, ausencia de metodología formal, gestión reactiva de incidentes, uso de herramientas ofimáticas como soporte documental.

Estas características convierten al sector servicios en un escenario pertinente para demostrar la aplicabilidad y el valor práctico de la metodología propuesta, sin que ello implique una generalización estadística, sino una validación conceptual y metodológica mediante una prueba de escritorio, coherente con el alcance propositivo–aplicado del estudio. Por lo tanto, el problema central de esta investigación se enfoca específicamente en Colombia (Lugar), tomando como recursos fundamentales las normas internacionales y herramientas Open Source (Recursos), y abordando la baja eficacia en la gestión estructurada de riesgos de seguridad informática por parte de las pymes (Problema). Teniendo en cuenta que entre las principales causas que contribuyen a este fenómeno se identifican la baja adopción de estándares internacionales, la limitada conciencia sobre la importancia de la gestión de riesgos y la escasez de personal capacitado. Así mismo, el limitado presupuesto de estas organizaciones dificulta aún más la inversión en medidas adecuadas de protección [32].

Otro rasgo del análisis del estudio es que existe una gran contradicción entre la percepción y la práctica. Aunque el 91% de los encuestados sin un proceso formal considera que la ciberseguridad debería gestionarse como tal, un 42% de este mismo grupo admite no tener 'ningún plan' ante problemas de ciberseguridad, y un 20% adicional simplemente responde de forma reactiva [25]. En cuanto a la barrera reconocida por las propias empresas, la escasez de personal y conocimiento especializado es otro dato recolectado del estudio. Su análisis infiere un 41% de los comentarios abiertos de la encuesta señalan explícitamente la 'falta de procesos de capacitación' y 'desconocimiento del tema' como un obstáculo principal. Además, se observa una confusión conceptual, donde las empresas listan herramientas de gestión de vulnerabilidades o tickets como si fueran de gestión de riesgos, demostrando así, la necesidad de una metodología que clarifique estos conceptos [25].

De manera semejante, las limitaciones presupuestarias mencionadas en la literatura obligan a las empresas a optar por soluciones que se perciben como más asequibles, razón por la cual se explica la dependencia de controles técnicos aislados como principal medida de seguridad en lugar de una estrategia holística [25]. De modo que, las consecuencias derivadas de esta problemática son preocupantes; incluyendo pérdidas significativas en activos digitales, interrupciones operativas por ransomware, phishing y suplantación, y daños reputacionales que comprometen la viabilidad y sostenibilidad futura de estas empresas [33].

En este contexto, la presente investigación tiene como aporte principal la propuesta de una metodología integral y sistemática, basada en normas internacionales y herramientas Open Source, orientada específicamente a mejorar la gestión de riesgos de seguridad informática en las PyMEs colombianas. Se puede decir que esta propuesta busca ofrecer soluciones prácticas y accesibles, adecuadas a las particularidades del sector servicios del país. Desde una perspectiva teórica, esta investigación contribuye al enriquecimiento del conocimiento académico y al fortalecimiento de la literatura existente sobre gestión de riesgos en ciberseguridad [34], [35].

Esta investigación caracteriza dichas normas relevantes, seleccionando y filtrando sus principios esenciales para una aplicación efectiva ante el problema observado. Luego, se procede al análisis crítico de herramientas OpenSource, identificando aquellas que se amoldan con destreza a la gestión de riesgos y a la idiosincrasia de las Pymes, culminando en la utilización de estas herramientas para conformar un bastión proactivo contra las amenazas digitales, actuales y emergentes. Por lo que se refiere al alcance, esta investigación se delimita a PyMEs colombianas del sector servicios, en el periodo comprendido entre julio de 2023 y junio de 2024. Además, es necesario recalcar que la propuesta metodológica para el análisis y gestión de riesgos se centra exclusivamente en el uso de herramientas Open Source, y se valida mediante una prueba de escritorio basada en un caso representativo.

Llegados a este punto, entre las principales limitaciones del presente trabajo se encuentra la validación de la propuesta metodológica en entorno controlado, es por esto que el resultado puede restringir su extrapolación en todos los sectores económicos. De manera semejante, el uso de herramientas Open Source puede implicar restricciones técnicas y de soporte a largo plazo. Además, otro rasgo limitante y que conviene subrayar es el reconocer que el enfoque propuesto no contempla la totalidad del ciclo de vida de implementación de medidas de seguridad que es cosa distinta, por tanto, es necesario aclarar que se enfoca en el análisis y gestión de riesgos.

Metodológicamente, se aplica un enfoque mixto que combina técnicas cuantitativas y cualitativas, utilizando herramientas validadas internacionalmente como el método AHP para recolectar y analizar datos [36], [37]. En el ámbito práctico, este trabajo proporcionará una metodología útil

que las PyMEs pueden implementar fácilmente, impactando positivamente en su capacidad para mitigar riesgos y garantizar la continuidad de sus operaciones [38].

Finalmente, desde el punto de vista académico y social, esta investigación contribuye a promover una cultura de seguridad informática entre las PyMEs colombianas, fomentando la sostenibilidad económica y generando una mayor confianza en el mercado nacional e internacional [39], [40]. De esta manera, no solo se aborda una problemática urgente y actual, sino que se aporta de manera significativa al desarrollo económico y social del país, mediante el fortalecimiento del tejido empresarial colombiano frente a las amenazas del entorno digital.

El presente informe de investigación se organiza de manera secuencial atendiendo al cumplimiento de los objetivos planteados y se estructura de la siguiente forma:

El documento inicia con el fundamento presentado en el Capítulo 1: Marco Teórico y Estado del Arte, donde se abordan los conceptos esenciales de la gestión del riesgo de seguridad de la información, el contexto de las pymes y la síntesis crítica de los marcos internacionales (ISO/IEC 27005, NIST SP 800-30, OCTAVE-S, entre otros), así como la base científica del método de decisión multicriterio AHP.

Posteriormente, el Capítulo 2: Marco Metodológico describe el diseño de la investigación de tipo propositivo-aplicado y enfoque mixto, detallando las cuatro fases secuenciales que permitieron transitar desde la caracterización normativa hasta la validación de la propuesta.

En el Capítulo 3: Desarrollo Técnico y Resultados, se exponen los hallazgos objetivo, derivados de la ejecución del estudio. Esta sección detalla la selección de marcos normativos y herramientas mediante el método AHP (OE1 y OE2), la instrumentación técnico-operativa realizada en el software MONARC (OE3) y la ejecución de la validación mediante el caso de estudio simulado "PyME Servicios Colombia" (OE4), donde se verificó la reducción cuantificable del riesgo residual.

Finalmente, el cierre del informe se presenta en el Capítulo 4: Conclusiones y Recomendaciones. En este apartado se sintetiza el cumplimiento del objetivo general y los específicos, se entregan las

lecciones aprendidas durante el proceso y se proponen líneas de trabajo futuro para la evolución de la metodología hacia modelos de gestión dinámica del riesgo.

1. Marco Teórico y Estado del Arte

Este capítulo reúne los fundamentos conceptuales y antecedentes investigativos que sustentan la metodología propuesta para el análisis y gestión de riesgos de seguridad informática en pymes. El Marco teórico precisa los conceptos de gestión del riesgo, seguridad de la información, seguridad informática y ciberseguridad; caracteriza el contexto operativo de las pymes; y examina los referentes internacionales, las herramientas tecnológicas y métodos multicriterio que orientan la investigación. El Estado del arte examina estudios recientes sobre gestión de riesgos en pymes, adaptación de referentes internacionales, uso de herramientas OpenSource o GRC, integración entre metodologías y software, y aplicaciones de AHP. Con ello, el capítulo establece la base conceptual y crítica necesaria para identificar el vacío metodológico abordado por la tesis.

1.1 Marco teórico

Este apartado desarrolla las bases conceptuales, terminológicas y metodológicas necesarias para comprender el alcance de la investigación. Su contenido inicia con los principios generales de la gestión del riesgo, incluyendo su definición, dimensiones de análisis y ciclo de tratamiento. Luego delimita el uso de los conceptos seguridad de la información, seguridad informática y ciberseguridad, con el fin de evitar ambigüedades en el desarrollo del documento. Desde esa base, se examina la gestión del riesgo de seguridad de la información y su aplicación al campo operativo de la seguridad informática en pymes, considerando las restricciones técnicas, organizacionales y económicas propias de estas empresas. El apartado también analiza los referentes internacionales aplicables, el enfoque sociotécnico, las herramientas tecnológicas de apoyo y los métodos de decisión multicriterio, especialmente AHP para justificar la selección de referentes y herramientas dentro de la metodología propuesta.

1.1.1 Fundamentos generales de la gestión del riesgo

El concepto de riesgo es el elemento central sobre el cual se construyen los modelos de seguridad y control organizacional. Desde una perspectiva normativa estandarizada, la norma NTC-ISO 31000 define el riesgo como el "efecto de la incertidumbre sobre los objetivos" [41, p. 4]. Esta definición implica que el riesgo no se limita exclusivamente a eventos negativos o daños, sino que representa una desviación —positiva o negativa— respecto a lo previsto. El componente fundamental de esta definición es la incertidumbre, entendida como “el estado, incluso parcial, de deficiencia de

información relacionada con la comprensión o el conocimiento de un evento, su consecuencia o probabilidad" [41, p. 4]. En este sentido, gestionar el riesgo consiste en reducir dicha incertidumbre para asegurar que la organización pueda alcanzar sus propósitos estratégicos y operativos.

La materialización del riesgo se analiza generalmente a través de dos dimensiones fundamentales: la probabilidad y el impacto. La probabilidad se refiere a la posibilidad de que ocurra un evento específico, la cual puede estimarse cuantitativamente mediante frecuencias estadísticas o cualitativamente a través de escalas de valoración [42]. El impacto, por su parte, representa la consecuencia o el efecto que dicho evento tendría sobre los activos o los objetivos de la organización si llegara a materializarse [41]. La combinación de estas dos variables permite determinar el nivel de riesgo y establecer prioridades para su tratamiento, diferenciando aquellos eventos que son tolerables de aquellos que requieren una intervención inmediata.

La gestión del riesgo se concibe como una disciplina transversal y un proceso sistemático, no como una actividad aislada. La ISO 31000:2018 define a la gestión de riesgos; "*coordinated activities to direct and control an organization with regard to risk*" [43, p. 7]. Según los principios rectores de la ISO 31000, este proceso debe ser estructurado, oportuno e integrado en todas las actividades de la organización, desde la planificación estratégica hasta las operaciones diarias. El ciclo de vida de la gestión del riesgo comprende actividades secuenciales que incluyen la comunicación y consulta, el establecimiento del contexto, la valoración del riesgo (que a su vez integra la identificación, el análisis y la evaluación), el tratamiento del riesgo y, finalmente, el monitoreo y revisión continua. Este enfoque cíclico garantiza que la organización se adapte a los cambios en el entorno interno y externo, manteniendo la gestión del riesgo dinámica y efectiva [43].

Dentro de la teoría general, es necesario distinguir entre diferentes tipologías de riesgo para delimitar el alcance de cualquier estudio. La literatura clasifica los riesgos empresariales en diversas categorías, tales como riesgos financieros, operacionales, estratégicos y de peligro (hazard) [44]. Una distinción clásica es la que existe entre el riesgo puro, que solo ofrece la posibilidad de pérdida o no-pérdida (como un incendio o un robo), y el riesgo especulativo, que implica la posibilidad de ganancia o pérdida (como una inversión financiera) [45]. La gestión del riesgo corporativo (ERM: por sus siglas en inglés Enterprise Risk Management) busca abordar estas categorías de manera

holística; sin embargo, para efectos de procedimientos técnicos, es indispensable la especialización en dominios concretos [46].

El riesgo de seguridad de la información, operativizado en esta investigación desde la seguridad informática, surge como una subdisciplina especializada dentro del marco general de la gestión del riesgo. Mientras que el riesgo general afecta a la organización en su conjunto, el riesgo de seguridad de la información se refiere específicamente a la posibilidad de que una amenaza explote una vulnerabilidad de un activo de información, causando un impacto en la confidencialidad, integridad o disponibilidad de los datos [47]. Esta delimitación es crucial pues, aunque los principios de gestión (identificar, analizar, evaluar) son los mismos que en el riesgo financiero u operativo, el objeto de protección —la información y los activos tecnológicos que la soportan— y las amenazas asociadas al entorno digital requieren metodologías adaptadas.

La justificación epistemológica para abordar la investigación desde esta perspectiva parte de lo general para llegar a lo particular, siguiendo la lógica planteada por organismos como INCIBE. Los responsables de la gestión empresarial son conscientes de la existencia de amenazas genéricas que ponen en peligro sus objetivos y dedican recursos a mantener los riesgos bajo un umbral aceptable para maximizar beneficios [44]. No obstante, dado que los entornos tecnológicos son cambiantes y las amenazas evolucionan, no basta con una gestión intuitiva. Es necesario aplicar los conceptos y procesos universales de la gestión del riesgo de forma metódica y estructurada al campo de la seguridad de la información y, para efectos de esta investigación, concretarlos en el ámbito operativo de la seguridad informática. Solo así, comprendiendo la arquitectura general del riesgo, es posible diseñar e implementar metodologías que apliquen los principios de seguridad de la información al ámbito operativo de la seguridad informática.

1.1.2 Delimitación conceptual: seguridad de la información, informática y ciberseguridad

Para evitar ambigüedades terminológicas en el desarrollo de este marco, se distinguen tres nociones relacionadas más no equivalentes, cuya diferenciación es clave para el alcance de esta investigación.

La seguridad de la información se consolida como el concepto integrador y holístico orientado a la protección de los datos y activos en cualquier forma y soporte, ya sea físico, digital o incluso el

conocimiento humano. Su objetivo central es garantizar la preservación de la confidencialidad, integridad y disponibilidad (tríada CIA o pilares de la seguridad), integrando además propiedades de autenticidad, confiabilidad y trazabilidad de la información [48]. Bajo este nivel, se utiliza el término de seguridad de la información como el "paraguas" normativo para definir el objeto de protección global y el marco de análisis estratégico [28].

En este contexto, la confidencialidad corresponde a la propiedad de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. Implica preservar las restricciones autorizadas sobre el acceso y la divulgación, incluyendo los medios para proteger la privacidad personal y la información propietaria [49]. En cuanto a la integridad, se define como el principio de seguridad que salvaguarda la exactitud y completitud de los activos, así como la propiedad de que la información no haya sido alterada o destruida de forma no autorizada o accidental, garantizando que el activo permanezca en la condición y para los propósitos previstos por su propietario [49]. Como último pilar, la disponibilidad se refiere a la propiedad de ser accesible y utilizable a petición de una entidad autorizada en el momento en que esta lo requiera. Su mantenimiento garantiza el acceso oportuno y confiable a la información y a los servicios de los sistemas [48].

Por su parte, la seguridad informática se refiere a la aplicación operativa de dichos principios específicamente en el entorno de las tecnologías de información (TI). Su enfoque es técnico y administrativo, centrándose en la protección de activos y sistemas como hardware, software, redes y datos en operación [4, 5].

Finalmente, la ciberseguridad se entiende como un subdominio especializado en la defensa de activos digitales interconectados y expuestos al ciberespacio, donde las amenazas se materializan principalmente a través de redes y servicios conectados [52]. Se define como el conjunto de herramientas y tecnologías utilizadas para proteger a los usuarios y activos en el entorno cibernético frente a ataques remotos [53].

Hecha esta delimitación, esta investigación adopta la seguridad de la información como marco conceptual amplio, en tanto proporciona los principios de protección de la confidencialidad, integridad y disponibilidad de la información. No obstante, su alcance aplicado se delimita a la seguridad informática, entendida como la protección de la infraestructura tecnológica, el software,

las redes, los sistemas y los datos en operación que soportan los procesos de las pymes. La ciberseguridad se emplea de manera específica para describir el contexto de amenazas digitales derivadas de la conectividad, tales como phishing, ransomware, malware, ataques remotos o exposición en el ciberespacio [54]. De esta forma, los tres términos no se utilizan como equivalentes, sino como niveles relacionados: la seguridad de la información aporta el marco general, la seguridad informática define el campo operativo de la tesis y la ciberseguridad describe el entorno de amenazas digitales que incide sobre dicho campo.

1.1.3 Gestión del riesgo de seguridad de la información

La gestión del riesgo de seguridad de la información se define como el proceso sistemático de identificar, evaluar y tratar los riesgos que amenazan la confidencialidad, integridad y disponibilidad de los activos de información. A diferencia del riesgo general, que puede abarcar incertidumbres financieras o de mercado, este dominio específico se centra en proteger la información y los sistemas que la soportan frente a amenazas accidentales o deliberadas. Según los estándares internacionales como ISO/IEC 27000 y NIST SP 800-39, el objetivo fundamental no es la eliminación total del riesgo, sino su mantenimiento dentro de niveles aceptables que permitan el cumplimiento de la misión organizacional [48], [55]. Para efectos de esta investigación, estos principios se aplican al campo de la seguridad informática, entendido como la protección de la infraestructura TI, los sistemas, las redes, el software y los datos en operación.

El modelo conceptual predominante en la literatura técnica estructura el riesgo a partir de la interacción de tres elementos centrales: activos, amenazas y vulnerabilidades [56]. Un activo se define como cualquier elemento que tiene valor para la organización y requiere protección, incluyendo información, software, hardware y personas susceptible de ser atacado con consecuencias para la organización [49]. Una amenaza es una causa potencial de un incidente no deseado que puede dañar un sistema o una organización [48], mientras que una vulnerabilidad es una debilidad intrínseca de un activo o control que puede ser explotada por una amenaza [49]. La relación causal es explícita: el riesgo se materializa cuando una amenaza aprovecha una vulnerabilidad existente para causar un impacto negativo sobre un activo).

Para dimensionar y priorizar estos riesgos, se emplean dos variables de medida fundamentales: la probabilidad y el impacto. La probabilidad (o verosimilitud) se refiere a la posibilidad de que una amenaza explote una vulnerabilidad en un periodo determinado, influenciada por factores como la motivación del atacante o la exposición técnica. El impacto representa la magnitud del daño resultante en caso de materialización, evaluado generalmente en términos de pérdida financiera, operativa, legal o reputacional. La combinación de estas variables permite determinar el nivel de riesgo inherente y residual, proporcionando la base necesaria para la toma de decisiones sobre su tratamiento [47].

El proceso operativo para gestionar estos elementos se encuentra estandarizado en referentes como la norma ISO/IEC 27005, estándar que propone un ciclo de vida iterativo y estructurado para la gestión del riesgo de seguridad de la información. Este ciclo inicia con el establecimiento del contexto, donde se definen los criterios de riesgo y el alcance. Posteriormente, se ejecuta la evaluación del riesgo, que se subdivide en tres fases: identificación (detectar activos, vulnerabilidades y amenazas), análisis (estimar probabilidad e impacto) y evaluación (comparar los resultados con los criterios de aceptación). Finalmente, se procede al tratamiento del riesgo, donde se identifican y seleccionan controles para mitigar, transferir, evitar o aceptar el riesgo. Todo el proceso debe estar acompañado de actividades transversales de monitoreo, revisión y comunicación) [47].

En el contexto actual, la gestión del riesgo de seguridad de la información evoluciona hacia enfoques más ágiles debido a la naturaleza cambiante del entorno digital. La literatura reciente destaca la transición desde evaluaciones estáticas y periódicas hacia modelos de riesgo dinámico, capaces de adaptarse a amenazas digitales o ciberamenazas emergentes. Asimismo, se identifica una tendencia creciente hacia la automatización de las fases de identificación y monitoreo, necesaria para procesar el volumen de datos que generan las infraestructuras tecnológicas modernas y reducir la dependencia de procesos manuales intensivos en tiempo [8], [57], [58].

Ante la amplitud que ofrecen los referentes internacionales para la gestión de riesgos, entre ellos ISO/IEC 27005, resulta necesario fijar una postura metodológica clara. Si bien estos referentes estructuran la gestión del riesgo bajo el marco amplio de la seguridad de la información, esta investigación delimita su alcance aplicado al campo de la seguridad informática. Por consiguiente,

el modelo se focaliza en vulnerabilidades y amenazas que afectan directamente la infraestructura tecnológica, el software, las redes, los sistemas y los datos en operación, dimensión especialmente crítica para las pymes del sector servicios. Es precisamente en esta dimensión tecnológica donde radica la urgencia de protección de las pequeñas y medianas empresas, sirviendo así de fundamento lógico para abordar su contexto a continuación.

1.1.4 Contexto operativo de las pymes frente a la gestión de riesgos de seguridad informática

Las pequeñas y medianas empresas poseen características organizacionales distintivas que condicionan su aproximación a la gestión de riesgos de seguridad informática, aunque esta se apoye en principios generales de seguridad de la información [59], [60]. A diferencia de las grandes corporaciones, estas entidades suelen operar bajo estructuras planas y centralizadas, donde la toma de decisiones recae en propietarios o gerentes generales sin especialización técnica [59], [61]. Esta configuración agiliza la operatividad, pero a menudo diluye la responsabilidad formal sobre la gestión de riesgos tecnológicos, careciendo de roles específicos como el de Director de Seguridad de la Información (CISO) [62].

La limitación de recursos constituye la variable crítica que define el contexto de operación de las Pymes [13], [59], [60], [63]. Las restricciones presupuestarias obligan a priorizar la continuidad operativa inmediata y la rentabilidad a corto plazo sobre la inversión en controles preventivos de seguridad [60], [62], [64]. Asimismo, la escasez de capital humano especializado impide la conformación de equipos dedicados, generando una dependencia de personal generalista de TI que debe asumir funciones de seguridad sin la formación adecuada [13], [61].

Como consecuencia de estas limitaciones estructurales, el nivel de madurez en seguridad informática y gestión de riesgos frente a amenazas digitales tiende a ser bajo en las pymes. La literatura académica señala que los procesos de seguridad suelen ser informales, intuitivos y carentes de documentación. Predomina una cultura reactiva, donde las medidas de protección se implementan principalmente como respuesta post-mortem a incidentes, en lugar de obedecer a una planificación estratégica basada en el riesgo [60]. Esta ausencia de políticas formalizadas dificulta la mejora continua y la auditoría de los controles [65].

En este entorno de baja madurez, las vulnerabilidades se manifiestan tanto en dimensiones técnicas como humanas [66]. La falta de programas de concienciación aumenta la exposición a amenazas digitales como el phishing [67], [68], mientras que las configuraciones predeterminadas débiles, la gestión inconsistente de parches y los respaldos no verificados facilitan impactos asociados a ataques como el ransomware [69], [70].

La aplicación directa de estándares internacionales robustos, como la serie ISO/IEC 27000, presenta barreras significativas para este segmento empresarial [71]. La exigencia de documentación extensiva, la complejidad de los procesos de gestión y la necesidad de roles definidos superan la capacidad administrativa de la mayoría de las Pymes. Los enfoques tradicionales de "talla única" resultan ineficaces porque presuponen una disponibilidad de datos y recursos que estas organizaciones no poseen, llevando a implementaciones superficiales o al abandono del sistema de gestión [59], [65].

Por lo tanto, se evidencia la necesidad teórica y práctica de desarrollar metodologías de gestión de riesgos contextualizadas y simplificadas. Estas aproximaciones deben abstraer la complejidad de los estándares formales, centrándose en la identificación ágil de activos críticos y amenazas prevalentes. En este escenario, el uso de herramientas de software Open Source emerge como un habilitador clave, permitiendo a las Pymes acceder a capacidades de gestión y análisis de riesgos que sean sostenibles financieramente y viables operativamente [13].

1.1.5 Referentes internacionales comparados de gestión del riesgo

En esta investigación, la expresión **referentes internacionales para la gestión de riesgos** se emplea como categoría integradora para agrupar estándares, guías, marcos de referencia y metodologías que orientan la identificación, análisis, evaluación y tratamiento del riesgo. Esta precisión evita asumir que todos los referentes revisados tienen naturaleza normativa, dado que algunos corresponden a normas técnicas o estándares, otros a guías especializadas, otros a marcos de referencia y otros a metodologías de análisis y gestión de riesgos.

La gestión del riesgo de seguridad de la información se apoya en diversos referentes internacionales que proporcionan principios, directrices y procesos estructurados para identificar, analizar, evaluar y tratar los riesgos que afectan a los activos digitales [73]--[75]. Aunque cada

referente surge en contextos distintos y responde a necesidades específicas, comparten fundamentos comunes derivados de la estandarización internacional y pueden resultar aplicables a pequeñas y medianas empresas (Pymes) con diferentes niveles de madurez [75], [76]. A continuación, se presentan de manera comparada los referentes más relevantes: ISO/IEC 27005, NIST SP 800-30, MAGERIT, OCTAVE-S y EBIOS RM [77].

ISO/IEC 27005 constituye un estándar internacional de referencia para la gestión del riesgo de seguridad de la información dentro del sistema de gestión definido por ISO/IEC 27001 [47], [78]. Su enfoque es sistemático y cíclico [79]. Propone un proceso continuo que abarca la identificación de activos, amenazas y vulnerabilidades, el análisis de probabilidad e impacto y la definición de tratamientos coherentes con el riesgo residual y los criterios organizacionales [73]. Se trata de una metodología flexible y adaptable, no prescriptiva [80], que permite ser aplicada en organizaciones de cualquier tamaño, siempre que exista capacidad básica para documentar procesos y mantener un ciclo de mejora continua [78], [79].

La publicación especial NIST SP 800-30, por su parte, adopta un enfoque más prescriptivo y orientado a amenazas [81]. Se centra en caracterizar sistemas, identificar amenazas específicas, analizar vulnerabilidades asociadas y determinar la probabilidad de ocurrencia e impacto, con un nivel de detalle técnico elevado [51]. Su estructura resulta útil para organizaciones que requieren claridad procedimental y un catálogo detallado de amenazas, aunque su aplicación puede demandar recursos y competencias técnicas que no siempre están disponibles en las Pymes [82], [83].

La metodología MAGERIT, ampliamente utilizada en el ámbito gubernamental hispano [84], [85], se caracteriza por su énfasis en el análisis de activos, dependencias y valor [86], [87]. Proporciona guías para identificar impactos, establecer niveles de riesgo acumulado y estimar el efecto de fallos o ataques a través de escenarios cuantitativos y semicuantitativos [88]. Su precisión analítica y su orientación a la documentación sistemática la convierten en una herramienta potente, pero su implementación puede resultar exigente para organizaciones con baja madurez en gestión de riesgos [89].

El enfoque OCTAVE-S se diferencia de los anteriores por privilegiar la perspectiva organizacional sobre los aspectos estrictamente técnicos [90]. Se enfoca en prácticas, contextos operativos,

cultura organizacional y percepción de riesgos por parte del personal clave [91]. Es menos dependiente de datos altamente estructurados y más orientado a identificar debilidades organizativas, procesos inseguros y prácticas que incrementan la exposición al riesgo [92]. Esta característica hace que resulte especialmente adecuado para Pymes que no disponen de inventarios detallados de activos ni capacidades avanzadas de análisis técnico.

La metodología OCTAVE-S (Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small Organizations) representa un enfoque autodirigido diseñado específicamente para organizaciones pequeñas (generalmente con 100 o menos empleados) que operan con medios y recursos limitados. Este método es una variación del enfoque OCTAVE original, adaptado a estructuras menos jerárquicas y con la premisa de que los participantes ya poseen un amplio conocimiento interno de la empresa.

La metodología OCTAVE-S se basa en los criterios fundamentales de OCTAVE y es dirigida por un equipo reducido e interdisciplinario (típicamente de tres a cinco personas) del propio personal de la organización. Este equipo asume la responsabilidad de establecer la estrategia de seguridad de la organización y debe tener un conocimiento suficiente de los procesos de negocio y seguridad para llevar a cabo todas las actividades por sí mismo, sin depender de talleres formales de obtención de conocimiento.

La evaluación se desarrolla a través de tres fases principales:

a. **Fase 1: Construcción de Perfiles de Amenazas Basados en Activos (Build Asset-Based Threat Profiles)**

Esta fase se centra en la evaluación organizacional, donde el equipo define los criterios de evaluación de impacto, identifica los activos más importantes (activos críticos), y evalúa las prácticas de seguridad actuales y organizacionales. El objetivo es establecer los requisitos de seguridad y definir un perfil de amenazas para cada activo crítico.

b. **Fase 2: Identificación de Vulnerabilidades de Infraestructura (Identify Infrastructure Vulnerabilities)**

Durante esta fase, se realiza una revisión de alto nivel de la infraestructura informática de la organización. El análisis se limita a examinar cómo el personal utiliza la infraestructura para acceder

a los activos críticos, identificando las clases clave de componentes y los responsables de su configuración y mantenimiento, más que en la ejecución de herramientas de evaluación de vulnerabilidades.

c. Fase 3: Desarrollo de Estrategias de Seguridad y Planes (Develop Security Strategy and Plans)

En la fase final, el equipo identifica y analiza los riesgos, y basándose en la información recopilada, crea una estrategia de protección general y planes específicos de mitigación de riesgos para los activos críticos.

Por otro lado, en lo que respecta a las limitaciones conceptuales y compatibilidad teórica, se tiene lo siguiente; debido a su diseño optimizado para recursos limitados, OCTAVE-S es una metodología altamente estructurada que minimiza las actividades.

Sin embargo, esta simplicidad implica una limitación conceptual: la metodología se centra en un alcance reducido de la infraestructura y carece de la granularidad de los catálogos o pasos detallados que se encuentran en marcos más exhaustivos. El análisis tecnológico en la Fase 2 es intencionalmente limitado, ya que muchas organizaciones pequeñas externalizan sus servicios de TI y carecen de la capacidad interna para ejecutar herramientas avanzadas de vulnerabilidad.

A pesar de esta limitación, el enfoque de gestión de riesgos de OCTAVE-S es compatible con estándares internacionales. Esta compatibilidad teórica con ISO/IEC 27005 es crucial, ya que permite a la organización emplear las directrices de este estándar, que ofrece orientación detallada para la gestión del riesgo de la seguridad de la información, para complementar y suplir la falta de granularidad en la identificación de amenazas o vulnerabilidades que OCTAVE-S omite debido a su enfoque simplificado. Es así que, si la organización lo requiere, pueda referenciarse a catálogos o procedimientos externos alineados con marcos reconocidos para obtener mayor profundidad en el análisis tecnológico.

Finalmente, EBIOS RM aporta un enfoque basado en escenarios y actores. Analiza intenciones, capacidades y oportunidades de potenciales adversarios, así como la plausibilidad de distintos escenarios de ataque. Propone una lógica modular en cinco etapas y es útil para organizaciones que necesitan estudiar riesgos avanzados o comprender la exposición de ecosistemas

interconectados. No obstante, su aplicación completa puede requerir sesiones facilitadas y personal con experiencia en análisis de amenazas.

En conjunto, estos referentes comparten elementos esenciales: la necesidad de identificar activos, amenazas y vulnerabilidades; la evaluación sistemática de probabilidad e impacto; la priorización de riesgos según criterios organizacionales; y la definición de tratamientos y controles. Todos reconocen la importancia de la gobernanza del riesgo, la participación de partes interesadas y la mejora continua. Sin embargo, difieren en su nivel de prescripción, profundidad técnica, necesidades de recursos y orientación conceptual.

Para esta investigación, estas diferencias permiten justificar la selección de referentes aplicables a la gestión de riesgos de seguridad informática en pymes, sin asumir que todos poseen la misma naturaleza normativa o metodológica. ISO/IEC 27005 ofrece un enfoque equilibrado y adaptable, aunque requiere cierta capacidad de documentación. NIST SP 800-30 es robusto en entornos con recursos técnicos, pero puede resultar complejo. MAGERIT aporta precisión analítica, útil para organizaciones que desean mayor control, aunque exige esfuerzo metodológico. OCTAVE-S es apropiado para contextos de baja madurez, pues prioriza prácticas organizativas por sobre análisis técnico. EBIOS RM, al centrarse en escenarios y actores, proporciona profundidad estratégica cuando se necesita comprender motivaciones de amenazas sofisticadas.

1.1.6 Enfoque sociotécnico y uso de software OpenSource

La gestión de riesgos de seguridad informática apoyada en principios de seguridad de la información, debe abordarse como un sistema sociotécnico que integra factores humanos, organizativos y tecnológicos [71], [93], [94], [95]. En las pymes, esta perspectiva es crucial para lograr un análisis de riesgos efectivo. Introducir una herramienta tecnológica por sí sola no garantiza resultados: se necesita también una cultura organizativa que apoye su uso y procesos adaptados a la realidad de la empresa.

Las pymes suelen carecer de recursos y experiencia para fortalecer su seguridad informática frente a amenazas digitales, debido a limitaciones de personal especializado, capacitación y formalización de procesos. Un enfoque sociotécnico reconoce que la eficacia en la gestión del riesgo depende de alinear personas, procesos y tecnología [75], [93], [96]. En la práctica, esto implica que tanto la

dirección como los empleados se involucren en el proceso (concienciación y formación) y que las herramientas se ajusten a las capacidades de la organización. Un estudio de Benz y Chatterjee [61], mostró que más de la mitad de las pymes encuestadas carecían de una estrategia formal de ciber-riesgos, en parte por la percepción equivocada de que “la seguridad informática es un problema solo de las grandes empresas”.

Es fundamental que las soluciones de seguridad sean accesibles para las pymes. Aquí “accesible” significa fáciles de adoptar y usar por organizaciones con recursos limitados. Una herramienta muy sofisticada pero difícil de entender o costosa de implementar puede ser más obstáculo que ayuda [70], [97]. Por tanto, cualquier metodología y su herramienta asociada deben tener interfaces sencillas, requerir mínimos recursos técnicos y conllevar costos bajos o nulos [98], [99], [100], [101].

El software de gestión de riesgos es una herramienta mediada por las TIC que ayuda a las organizaciones a identificar los riesgos asociados a sus activos y operaciones. El sistema de gestión de riesgos mide y supervisa los riesgos y le notifica/alerta sobre ellos. Permite mapear los riesgos y evitarlos antes de que perjudiquen a la organización y garantiza que todos sus procesos se desarrollen sin problemas [102].

En el contexto de los objetivos y metas organizacionales, una herramienta de gestión de riesgos puede realizar una serie de procesos como: gestión de riesgos (identificar, analizar y evaluar riesgos) y tratamiento de riesgos (planear estrategias, ejecución y monitoreo de estrategias, resultados de medición).

Para llevar a cabo estas actividades de manera eficaz, el software de gestión de riesgos sigue un proceso sistemático estructurado así: (i) identificación y priorización de riesgos, (ii) planificación, análisis y prueba de estrategias de riesgo, (iii) selección y ejecución de estrategias de riesgos, (iv) monitoreo de resultados y, (v) generación de reportes.

Muchos referentes formales de seguridad y gestión de riesgos resultan demasiado complejos para una empresa pequeña cuando se aplican sin adaptación [1], [73], [103], [104]. Esto ocurre tanto con estándares de seguridad de la información como con marcos de ciberseguridad o metodologías de análisis de riesgos. Por ello, diversos autores enfatizan la necesidad de metodologías simplificadas y herramientas asequibles específicas para pymes [107] - [109]. Se han publicado

incluso guías prácticas basadas en estándares (como NIST) adaptadas a negocios pequeños, precisamente porque muchas empresas “no saben por dónde empezar” a mejorar su postura de seguridad [9], [28], [110] - [113]. Aunque la investigación se centra en la gestión de riesgos de seguridad informática, la relación con el cumplimiento normativo resulta relevante porque muchas herramientas GRC integran ambos componentes [84], [112], [113].

En ese sentido, las herramientas abordan la gestión de riesgos como al proceso que se sigue para evitar factores internos y externos que pueden perjudicarles. Requiere hacer frente a las incertidumbres y a una gestión inadecuada que dan lugar al riesgo y perjudican los resultados en distintas áreas o factores como financieros y la reputación. La tecnología integrada con las habilidades puede ayudar a prever, medir, informar y tomar medidas rápidas que contribuyan a gestionar los riesgos de forma que proporcionen beneficios a largo plazo.

La gestión del cumplimiento normativo se refiere al cumplimiento de determinadas directrices y leyes establecidas por los organismos gubernamentales nacionales y locales. La organización puede enfrentarse a problemas legales si incumple las normas y procedimientos que apliquen [116] - [119]. El proceso de gestión del cumplimiento normativo permite fomentar una buena relación con los inversores, clientes, proveedores y partes interesadas, así como mantener una buena reputación en el mercado [120] - [123]. En Colombia, la gestión del cumplimiento normativo hace presencia legal a entidades públicas no privatizadas.

Un aporte al combinar la gestión de riesgos y la gestión del cumplimiento normativo es que no solo evita riesgos, sino también crear un valor tangible de negocio en la organización, particularizando en la pyme como motor económico, es un plus y más si la herramienta aplica estándares internacionales por cumplir a pesar de no ser exigidos en este país. Por lo tanto, antes de seleccionar un software de gestión de riesgos, se debe asegurar de que incluya funciones relevantes tanto para la gestión de riesgos como para la gestión del cumplimiento normativo [124] - [126].

Existen plataformas freemium, comerciales y OpenSource para apoyar la gestión de riesgos de seguridad informática [100], [102], [125], [126]. Muy pocas son de código abierto, cuyo bajo costo y flexibilidad resultan atractivos para Pymes [94], [99], [127], [128]. Entre ellas destacan PILAR (basada en el método MAGERIT alineado con ISO/IEC 27005 [129], robusta pero relativamente

compleja para una empresa pequeña) y SimpleRisk (solución ligera que permite registrar y evaluar riesgos siguiendo el ciclo de ISO/IEC 27005 e ISO 31000) [130].

Entre las herramientas tecnológicas disponibles para apoyar la gestión de riesgos se identifican soluciones OpenSource, open-core, propietarias y SaaS, con diferentes niveles de complejidad y alcance funcional.

- PILAR

La herramienta PILAR implementa la metodología Magerit, citada en las referencias de PILAR, corresponde a la versión 3 de la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" [133] - [135]. El enfoque metodológico que implementa PILAR para el análisis de riesgos requiere una aproximación metódica que incluye:

1. Identificar el valor a proteger (activos esenciales de información y servicio).
2. Identificar los elementos del sistema (activos de soporte) que respaldan ese valor y donde los ataques pueden causar daño.
3. Establecer medidas de seguridad (salvaguardas o contramedidas) para protegerse contra ataques o incidentes.
4. Estimar indicadores de la posición de riesgo para asistir a la toma de decisiones.

PILAR facilita la gestión de riesgos mediante el análisis y la identificación de riesgos potenciales e inherentes en un sistema de información y comunicaciones, y permite la evaluación de las medidas de seguridad utilizando niveles de madurez que van desde L0 (Inexistente) hasta L5 (Optimizado), siguiendo un modelo similar a CMM (Capability Maturity Model).

La herramienta PILAR también es compatible con la evaluación de perfiles de seguridad, como la norma ISO/IEC 27002, para asistir en el tratamiento de riesgos y el cumplimiento de requisitos de acreditación. La información recabada puede documentarse mediante informes generados en formatos RTF o CSV, usando plantillas o scripts XML [132].

Las versiones de PILAR (Magerit) varían en complejidad y enfoque, desde µPILAR para análisis rápidos en sistemas pequeños, Basic para pymes y administración local, hasta PILAR RM (Risk Management) para análisis detallados en sistemas complejos; además, PILAR BCM se enfoca en

Continuidad de Negocio, y RMAT (Risk Management Additional Tools) son personalizaciones, todas basadas en la metodología Magerit de análisis de riesgos.

Aquí están las diferencias clave [129]:

- **PILAR (Versión completa):** Es el entorno integral de herramientas que implementa Magerit, ofreciendo análisis completo.
- **µPILAR (Micro):** Versión simplificada para análisis muy rápidos en sistemas pequeños y homogéneos, con un perfil de seguridad.
- **PILAR Basic:** Versión más sencilla para pymes y administraciones locales, enfocada en análisis rápidos e informes normativos.
- **PILAR RM (Risk Management):** Para sistemas complejos, permite análisis de riesgos detallados e informes normativos exhaustivos.
- **PILAR BCM (Business Continuity Management):** Específica para análisis de impacto y planes de continuidad del negocio (BCP).
- **RMAT (Risk Management Additional Tools):** Son herramientas complementarias y personalizaciones adicionales para necesidades específicas de gestión de riesgos.

También son relevantes Eramba (suite GRC abierta que apoya la gestión de riesgos y el cumplimiento de normas como ISO 27001) y MONARC (herramienta de Luxemburgo que implementa ISO 27005 de forma iterativa y colaborativa) [134], [135].

- ERAMBA

Eramba es un software abierto de GRC de TI impulsado por la comunidad, diseñado para ser una solución simple y asequible para la Gobernanza, Riesgo y Cumplimiento. La plataforma ofrece una suite que cubre varios casos de uso:

1. Gestión de Cumplimiento (Compliance Management)

Permite a los usuarios demostrar el cumplimiento de diversos estándares como ISO 27001, PCI-DSS, NIST y SOC2, además de regulaciones financieras y legales, e incluso métricas ambientales y sociales (ESG). Las funcionalidades clave incluyen la importación de paquetes de cumplimiento (estándares populares de la comunidad o paquetes personalizados) en formato CSV, el mapeo de requisitos de cumplimiento entre diferentes marcos para simplificar esfuerzos, y la definición del

estado de cumplimiento (conforme, no conforme, no aplicable). El módulo también facilita la vigilancia de las revisiones de políticas y las pruebas de control para asegurar el cumplimiento continuo, además de generar informes rápidos para stakeholders internos y externos, como auditores.

2. Gestión de Riesgos (Risk Management)

Soporta la gestión de riesgos orientada a Activos, Terceros y Negocios. Permite a las organizaciones identificar, analizar, tratar y comunicar los riesgos en un solo lugar. Los usuarios pueden configurar sus propias clasificaciones, cálculos y matriz de riesgos. La versión Enterprise incluye la capacidad de realizar Evaluaciones de Riesgos Empresariales.

3. Controles Internos y Políticas

Permite la definición de Controles y Políticas, y la gestión de sus revisiones. La recopilación de evidencia se facilita mediante notificaciones y automatización.

4. Módulos Avanzados (Enterprise)

La versión Enterprise ofrece funcionalidades adicionales sobre la versión gratuita (Community), como Notificaciones, Campos Personalizados, Análisis de Flujo de Datos (para EU GDPR), revisiones automatizadas de cuentas, programas de concienciación sobre seguridad, y evaluaciones de proveedores (mediante cuestionarios en línea). La gestión de Incidentes y Proyectos también son capacidades de la versión Enterprise.

5. Arquitectura y Reportes

Eramba tiene una versión Enterprise On-Prem que se ejecuta en Docker, lo que permite la conexión a su base de datos MySQL para crear informes dinámicos utilizando herramientas externas como Power BI Desktop. La plataforma también soporta una API REST para recibir y enviar llamadas basadas en acciones configurables. Para la versión SaaS, el acceso directo a la base de datos no está disponible, pero se pueden utilizar sus APIs.

- MONARC

MONARC (Méthode Optimisée d'aNAlyse des Risques CASES) es tanto una herramienta como un método que permite una evaluación de riesgos optimizada, precisa y repetible. Desarrollado por

NC3 de Luxemburgo, se basa en la capitalización de análisis de riesgos previos realizados en contextos de negocio similares.

MONARC es un método de análisis de riesgos iterativo y cualitativo. El objetivo de este método es simplificar la gestión de riesgos y la gobernanza de la seguridad de la información, basándose en estándares de la industria. Sus metodologías y herramientas se desarrollaron de acuerdo con la familia de estándares ISO/IEC 27001 y con los principios de ISO 31000. En esta investigación, MONARC se analiza como herramienta de apoyo para operacionalizar la gestión de riesgos de seguridad informática en pymes. Dicho esto, sus cuatro fases respetan completamente la norma internacional ISO/IEC 27005, que proporciona directrices para la gestión de riesgos relacionados con la seguridad de la información [136].

El modelo iterativo de MONARC comprende las siguientes cuatro fases:

1. Establecimiento del Contexto (Context Establishment)

Esta fase inicial define el alcance y los objetivos del análisis de riesgos, establece y describe el contexto (incluyendo retos y prioridades), e identifica las actividades clave, los procesos críticos, las amenazas internas y externas, y las vulnerabilidades (organizativas, técnicas y humanas). También se definen los criterios de evaluación de riesgos.

2. Modelado del Contexto (Context Modelling)

Es la fase de desarrollo del modelo de riesgo, que incluye el modelado de objetos y árboles. Los activos (o assets) identificados se detallan y formalizan en un diagrama que muestra sus interdependencias. Los impactos se definen a nivel de los activos primarios (procesos o información), y los activos secundarios heredan el impacto del activo primario al que están asociados.

3. Evaluación y Tratamiento de Riesgos (Evaluation and treatment of risks)

La evaluación implica cuantificar las amenazas, vulnerabilidades e impactos para calcular los niveles de riesgo. Si un riesgo identificado supera el nivel aceptable (rejilla de aceptación de riesgos), se deben implementar medidas de tratamiento para reducirlo a nivel tolerable.

4. Implementación y Monitoreo (Implementation and monitoring)

Esta es una fase de gestión continua que incluye el monitoreo de la seguridad y el control recurrente de las medidas de seguridad para lograr una mejora sostenible. Esta fase también permite optimizar continuamente la seguridad aumentando el detalle de los objetos utilizados y expandiendo el alcance del análisis de riesgos.

En cuanto a su arquitectura, MONARC está compuesto por cuatro componentes principales:

- **Front Office:** Es la interfaz principal para realizar los análisis de riesgos.
- **Back Office:** Permite gestionar múltiples instancias de Front Office y administrarlas de manera eficiente, lo cual es útil para manejar varios clientes.
- **Global Dashboard:** Puede mostrar o enviar estadísticas, ofreciendo una vista general del uso de los diferentes componentes de MONARC.
- **MOSP (Monarc Object Sharing Platforms):** Ayuda a obtener contenido nuevo, como bases de conocimiento, que es compartido por otras organizaciones.

MONARC se distribuye bajo la licencia GNU Aero General Public License versión 3, lo que la convierte en una herramienta de código abierto.

- SimpleRisk

A continuación, se detallan las características funcionales de SimpleRisk [137]:

- Caracterización funcional

SimpleRisk es una plataforma de software de Gobernanza, Gestión de Riesgos y Cumplimiento (GRC) que fue lanzada en 2013 como un producto gratuito y de código abierto (SimpleRisk Core) [138]. Su misión es ofrecer una solución GRC simple, efectiva y asequible que pueda ser adoptada exitosamente por organizaciones de cualquier tamaño o industria.

Características Funcionales Clave (SimpleRisk Core):

El producto base, SimpleRisk Core, incluye todas las funcionalidades fundamentales necesarias para iniciar un programa GRC [139]. Estas capacidades incluyen:

- Gestión de Riesgos: Permite enviar riesgos (Submit Risk) y planificar mitigaciones (Plan Mitigation).
- Gobernanza: Permite definir frameworks y controles propios de la organización.

- Cumplimiento: Facilita la creación de pruebas y la realización de auditorías.
- Evaluaciones (Assessments): Permite tomar evaluaciones preconfiguradas para generar automáticamente riesgos pendientes.
- Gestión de Activos (Asset Management): Soporta el descubrimiento automatizado de activos y su asociación con los riesgos.
- Informes (Reporting): Ofrece paneles gráficos y reportes dinámicos para stakeholders técnicos y de negocio.

Ciclo de Vida del Riesgo y Análisis:

SimpleRisk permite a las organizaciones identificar, clasificar (rank), monitorear y rastrear los riesgos a lo largo de su ciclo de vida de mitigación. El ciclo de vida del riesgo soportado por SimpleRisk incluye las siguientes etapas clave: Envío de Nuevo Riesgo, Planificación de Mitigación, Aceptación de Mitigación, Revisión de Gestión y Revisión Regular [140].

La plataforma soporta la realización de un análisis de riesgos que incorpora técnicas tanto cualitativas como cuantitativas. La fórmula básica utilizada para el riesgo es **Riesgo = Probabilidad x Impacto**.

SimpleRisk ofrece múltiples metodologías de puntuación de riesgos (Risk Scoring Method), incluyendo:

- **Classic Risk Rating:** Utiliza valores de Probabilidad (Likelihood) e Impacto para calcular una puntuación de riesgo.
- **CVSS (Common Vulnerability Scoring System):** Se basa en un vector base con múltiples valores para estimar la probabilidad y el impacto, además de valores opcionales para el impacto temporal y ambiental.
- **DREAD:** Un modelo que clasifica las amenazas de seguridad en función de Daño, Reproducibilidad, Explotabilidad, Usuarios Afectados y Descubribilidad.
- **OWASP (Risk Rating Methodology):** Enfocado en la evaluación de la probabilidad e impacto de vulnerabilidades de aplicaciones web, evaluando Likelihood basado en factores de Agente de Amenaza y Vulnerabilidad, e Impacto basado en factores Técnicos y de Negocio.

- **Contributing Risk:** Evalúa el Impacto del riesgo contra múltiples valores ponderados y personalizables, como Seguridad, SLA, Finanzas y Regulación.
- **Custom:** Permite especificar un valor numérico simple de 0 a 10 para evaluar el riesgo.

Arquitectura y Plataforma GRC:

SimpleRisk utiliza el lenguaje de programación PHP y la base de datos back-end MySQL, ambas tecnologías de código abierto. La plataforma está disponible en modelos de despliegue On-Premise (en servidores propios) o Hosted (Software-as-a-Service en la nube de AWS) [141].

SimpleRisk actúa como la capa de gobernanza y rendición de cuentas (governance and accountability layer), enfocándose en la documentación, asignación de responsabilidades, seguimiento y mejora de los controles y riesgos. A través de módulos licenciados llamados SimpleRisk Extras, la funcionalidad de la plataforma se extiende para incluir características como Gestión de Incidentes, API, autenticación personalizada, bases de datos cifradas, y gestión de vulnerabilidades con integraciones nativas a herramientas como Tenable.io y Qualys [142].

SimpleRisk facilita la alineación con marcos de ciberseguridad como el NIST Cybersecurity Framework (CSF) al proporcionar herramientas para la documentación y gestión de políticas, controles, y mitigaciones a través de las cinco funciones del NIST (Identificar, Proteger, Detectar, Responder y Recuperar) [143].

SimpleRisk incluye un módulo de Planificación de Mitigación donde se definen y rastrean los planes de solución, incluyendo la estrategia de planificación, el esfuerzo requerido, el costo estimado, el propietario de la mitigación y el porcentaje de mitigación aplicado. También soporta un proceso de Revisión (Review Regularly) que asegura que los riesgos pasen por una revisión de gestión periódica para registrar la dirección y los próximos pasos del ciclo de vida del riesgo [146] - [148].

Por otra parte, existen plataformas comerciales con filosofía similar orientadas a Pymes, como Pirani Risk, que ofrecen interfaces sencillas y plantillas alineadas con estándares internacionales en un modelo freemium accesible [147], [148].

- Pirani Risk

Pirani es un software de gestión de riesgos diseñado para contribuir al éxito organizacional mediante una gestión simple de riesgos [149]. Pirani está disponible para empresas de cualquier

tamaño y sector, y se adapta a metodologías propias de la organización y a referentes reconocidos como ISO 31000, ISO 27001, COSO, entre otras regulaciones especializadas [102], [147].

El software permite una gestión integral de riesgos (GRC) al ofrecer diferentes sistemas de gestión, incluyendo gestión de riesgos operacionales (ORM), gestión de riesgos de seguridad de la información (ISMS), gestión de riesgos de lavado de activos (AML), cumplimiento normativo (Compliance) y gestión de auditorías [148].

Respecto a su modelo de negocio y planes, Pirani [150] ofrece opciones que se ajustan al nivel de madurez de la gestión de riesgos de las empresas:

- Planes de servicio: Dispone de una versión gratuita, denominada Plan Free, además de los planes Starter, Basic y Enterprise.
- Plan Free: Esta opción está diseñada para empresas que inician su proceso de gestión de riesgos. Es de uso indefinido y gratuito.
- Capacidades del Plan Free: Permite realizar una gestión básica que incluye la identificación de procesos y factores de riesgo, la evaluación de riesgos considerando su frecuencia e impacto, y el establecimiento de controles para su mitigación. Este plan incluye hasta 5 usuarios, 200 registros y 2GB de almacenamiento.

El objetivo de Pirani es acompañar a las organizaciones para que el proceso de gestión de riesgos sea más simple y eficiente, permitiendo la toma de decisiones oportuna y la protección del valor de la organización. El software facilita todas las etapas de la administración de riesgos, desde la identificación y medición hasta el control y monitoreo.

- **Criterios de alineación entre herramientas, referentes internacionales y necesidades de gestión del riesgo**

Por software open source (OSS) se entiendo que es un código fuente desarrollado y mantenido a través de una colaboración comunitaria abierta, es decir, cualquiera puede usar, examinar, alterar y redistribuir el OSS como mejor le parezca, normalmente sin costo alguno. Esto se contrasta con las aplicaciones de software patentadas o de código cerrado, donde el creador o titular de los derechos de autor vende el software patentado o de código cerrado a los usuarios finales [151].

Integrar un software de soporte en el proceso de gestión de riesgos aporta beneficios claros en orden y consistencia [112]. La herramienta estandariza el flujo de trabajo de análisis (identificar activos, valorar riesgos, definir tratamientos, etc.) según metodologías reconocidas, lo que previene omisiones en el proceso. Además, un software de riesgos centraliza la información: todos los activos, evaluaciones, controles y planes quedan documentados en un repositorio único, mejorando la trazabilidad y facilitando auditorías [74]. Muchas herramientas también automatizan tareas rutinarias (generación de informes, recordatorios de revisión), de modo que la Pyme puede pasar de una gestión reactiva a un enfoque proactivo basado en datos objetivos [152]. Las decisiones, como la priorización de controles, se toman así con fundamento en evaluaciones registradas y no solo en intuición [153].

La adopción de herramientas open source conlleva varias ventajas: bajo costo (sin licencias), flexibilidad para adaptar el sistema a necesidades específicas, e independencia del proveedor (evitando ataduras a un vendedor y aprovechando comunidades de apoyo) [97], [154], [155]. En cuanto a limitaciones, estas soluciones exigen contar con capacidad técnica interna para su instalación y mantenimiento; además, algunas ofrecen funcionalidades avanzadas solo en versiones de pago, lo que podría requerir inversión a futuro; finalmente, el soporte formal suele ser limitado, pues la ayuda comunitaria no garantiza niveles de servicio como un producto comercial [156]. Cada Pyme debe sopesar estas ventajas y desventajas según su contexto, recordando que la herramienta es un medio para apoyar la gestión del riesgo y no un sustituto del compromiso organizativo con la seguridad.

Las herramientas open source se distribuyen bajo distintos tipos de licencias que determinan los términos de uso, modificación y redistribución del software [157]. Entre las licencias más comunes se encuentran:

- GNU Affero General Public License v3 (AGPLv3): exige que las Modificaciones del código sean compartidas incluso cuando el software se ofrece como servicio en red [158].
- Mozilla Public License 2.0 (MPL 2.0): permite combinar código bajo esta licencia con software propietario, siempre que los archivos originales se mantengan bajo MPL [159], [160].
- Licencia MIT: una de las más permisivas, que permite uso comercial, modificación y distribución con mínimas restricciones [161].

- Licencias BSD (2-Clause y 3-Clause): también permisivas y similares a MIT, pero con algunas cláusulas adicionales sobre el uso del nombre de los autores originales [162].
- Apache License 2.0: además de ser permisiva incluye protección expresa sobre patentes [163].

La elección de una licencia específica es un criterio o filtro clave, puede influir en aspectos como la integración con otros sistemas, las obligaciones legales de la organización al modificar el código, y la sostenibilidad del proyecto a largo plazo. De ahí la importancia de comprender las implicaciones de cada tipo de licencia [164], esto resulta fundamental al momento de preseleccionar herramientas para la gestión de riesgos de seguridad de la información.

La capacidad de una herramienta de software para dar soporte efectivo a un referente de gestión de riesgos depende de factores técnicos y funcionales. Una de las funciones esenciales de esas herramientas es manejar una multitud de datos y sus combinaciones, también proporcionar flexibilidad para el tratamiento y modelado, con el fin de contextualizar la realidad particular de la organización.

Generalmente, los requisitos funcionales para que una herramienta pueda alinearse con referentes de gestión de riesgos incluyen [63], [167] - [169]:

1. Capacidad de Personalización y Modelado

Debe permitir la personalización de modelos y criterios de riesgo. Esto implica ser flexible para ajustarse al contexto, permitiendo al administrador y/o usuario modificar escalas de valoración y niveles de impacto para que los resultados sean coherentes con los objetivos del negocio. Además, un sistema de apoyo debe evaluar el impacto y el riesgo residual, y no debe ocultar el razonamiento que lleva a las conclusiones obtenidas.

2. Gestión de Catálogos

Debe manejar catálogos razonablemente completos de elementos fundamentales para el análisis de riesgos. Esto incluye:

- Activos y Dimensiones de Valoración: Debe gestionar los tipos de activos relevantes, las dimensiones de valoración (o aspectos de seguridad en los que es valioso el activo) y los criterios de valoración asociados.

- Amenazas y Salvaguardas: Debe incorporar catálogos de amenazas y salvaguardas (o contramedidas), facilitando la identificación de las medidas de protección y la evaluación de su eficacia.
- Compatibilidad e Intercambio de Información: Para homogeneizar los resultados y permitir la comparación o integración de análisis realizados por diferentes equipos, las herramientas deben ser capaces de importar y exportar los datos del modelo en formatos fácilmente procesables (como XML, CSV, entre otros).

3. Soporte a Opciones de Tratamiento de Riesgos

Una vez evaluados los riesgos, la herramienta tecnológica debe respaldar el registro y el análisis de la estrategia de gestión conforme a las directrices de referentes como ISO/IEC 27005 o a principios de ISO 31000 [168], [169]. El proceso de tratamiento de riesgos busca modificar el riesgo (es decir, reducir el riesgo a un nivel aceptable por la organización dentro de su apetito al riesgo) [81], y las opciones para lograrlo típicamente se agrupan en cuatro categorías principales:

- **Evitar el riesgo (risk avoidance)**, decidiendo no iniciar o continuar la actividad que lo genera.
- **Mitigar el riesgo (risk mitigation)**, cambiando su probabilidad de ocurrencia o sus consecuencias.
- **Compartir o transferir el riesgo (risk sharing)**, mediante contratos, seguros o externalización.
- **Aceptar o retener el riesgo (risk acceptance)**, asumiendo el riesgo residual por una decisión informada.

Al registrar esas estrategias de plan de tratamiento de riesgos, permite que la gestión de riesgos esté bien fundamentada, lo cual facilita que la dirección justifique la toma de decisiones.

1.1.7 Métodos de decisión multicriterio para selección de referentes y herramientas

La toma de decisiones multicriterio emerge como una necesidad en la gestión de riesgos de seguridad informática en pymes [170]. A diferencia de las grandes empresas, las pymes operan con recursos limitados y personal reducido, lo que dificulta la implementación de referentes robustos si no se eligen cuidadosamente. Seleccionar un referente de gestión de riesgos, como ISO/IEC 27005 o NIST SP 800-30, y una herramienta de apoyo, como MONARC o SimpleRisk, no puede

dejarse al azar o a la simple imitación de prácticas corporativas. Un enfoque intuitivo o simplista puede conducir a “shelfware”, es decir, software o metodologías adquiridas, pero nunca aplicadas efectivamente, desperdiciando tiempo y recursos escasos [57], [59], [124], [171].

Dentro de los métodos multicriterio, el Proceso Analítico Jerárquico (AHP) propuesto por Thomas Saaty es uno de los más utilizados por su equilibrio entre rigor y simplicidad. El AHP permite descomponer un problema complejo en una jerarquía de objetivos, criterios y alternativas. Este método fue desarrollado para ayudar a los responsables a manejar situaciones que requieren múltiples criterios o atributos [172].

El decisor compara por pares los elementos en cada nivel (por ejemplo, qué criterio es más importante, o qué alternativa es preferible respecto a un criterio dado) utilizando una escala fundamental de 1 a 9 puntos que refleja la intensidad de la preferencia. Estas comparaciones por pares producen matrices de juicio cuya solución proporciona un vector de prioridades – es decir, pesos numéricos para cada criterio y puntajes para cada alternativa.

Un aspecto valioso del AHP es que traduce valoraciones cualitativas en valores cuantitativos susceptibles de comparación. De acuerdo con Aladayleh y Aladaileh [173], el método incorpora mecanismos de verificación de coherencia lógica de los juicios emitidos mediante el cálculo del Índice de Consistencia y la Razón de Consistencia (CR). Cuando las comparaciones son demasiado inconsistentes o contradictorias, el AHP lo evidenciará a través de una CR elevada, advierte la necesidad de revisar los juicios antes de confiar y aceptar los resultados; de lo contrario, garantiza que las prioridades obtenidas son estables y confiables.

Para cuantificar esto, se determina primero el máximo autovalor (λ_{max}) de la matriz, el cual se utiliza para calcular el Índice de Consistencia mediante la siguiente expresión (ver Ecuación (1.1)):

$$\text{Índice de Consistencia} = \frac{\lambda_{max} - n}{n-1} \qquad (1.1)$$

Donde n es la dimensión de la matriz. Debido a que esta medida depende del orden de la matriz, Saaty propone la CR, obtenida al comparar el Índice de Consistencia con un Índice Aleatorio (RI) esperado para matrices de igual tamaño (ver Ecuación (1.2)):

$$\text{Razón de Consistencia} = \frac{\text{Índice de Consistencia}}{\text{Índice Aleatorio}} \quad (1.2)$$

En concordancia con los valores tabulados por Saaty y validados en la literatura técnica actual, se asumen los valores de Índice Aleatorio estándar (0.90 para $n = 4$ y 1.12 para $n = 5$) [173].

Aplicar AHP [174] requiere primero estructurar el objetivo y los criterios de decisión de forma jerárquica y clara. En el contexto de esta investigación, el objetivo global puede definirse así: Seleccionar la combinación más adecuada entre un referente internacional para la gestión de riesgos y una herramienta tecnológica de apoyo que permita fortalecer la gestión de riesgos de seguridad informática en la pyme. Para alcanzar este objetivo, se identifican criterios fundamentales que reflejan las restricciones típicas de una pyme en materia de gestión de riesgos de seguridad informática. La literatura y las guías para pequeñas empresas destacan algunos factores recurrentes [1], [8], [175], [176]:

- Costo total (incluyendo licencias, infraestructura y horas-hombre necesarias): Las Pymes suelen anteponer el costo debido a sus márgenes limitados [177]. Un referente o herramienta gratuita u económica, pero efectiva, tendrá prioridad sobre otra muy poderosa pero impagable.
- Usabilidad y simplicidad: Dado que muchas Pymes carecen de expertos en seguridad, la solución elegida debe ser intuitiva, con baja curva de aprendizaje y accesible para personal no técnicomdpi.com. Si la herramienta es demasiado compleja o el referente exige una carga documental excesiva, es probable que no se implementen correctamente.
- Adecuación normativa y metodológica: Se evalúa el grado en que la alternativa se alinea con estándares reconocidos (por ejemplo, si facilita cumplir ISO 27001 o requisitos regulatorios del sector). También abarca si el enfoque metodológico es sólido y reconocido (p. ej., basarse en ISO 31000 o NIST garantiza buenas prácticas).
- Soporte y sostenibilidad: Incluye la disponibilidad de soporte técnico o comunitario, Actualizaciones y la viabilidad de largo plazo. Por ejemplo, una herramienta Open Source con comunidad activa podría valorarse alto, mientras que una solución abandonada o sin soporte sería riesgosa de adoptar.
- Funcionalidad técnica: Se consideran las capacidades de la herramienta o del referente evaluado para cubrir necesidades específicas: integración con otros sistemas,

automatización de análisis, generación de reportes, gestión de vulnerabilidades, etc. En el caso de las metodologías, sería el alcance y profundidad del análisis de riesgo que proponen (¿cubren riesgos tecnológicos emergentes? ¿permiten análisis dinámico?).

Con estos criterios (u otros similares según el caso), se construye la jerarquía AHP: en el nivel superior el objetivo estratégico, en el nivel intermedio los criterios definidos, y en el nivel más bajo las alternativas concretas a evaluar. Las alternativas pueden ser, por un lado, distintos referentes de gestión de riesgos, y por otro lado diferentes herramientas software Open Source.

Como condición, si el conjunto de alternativas es muy heterogéneo o extenso, es posible estructurar decisiones por separado (primero seleccionar el referente internacional más apropiado, luego la herramienta más adecuada) y luego integrar ambos resultados. En ese sentido, a diferencia de variantes como el Fuzzy AHP (Proceso de Jerarquía Analítica Difusa) o el Proceso de Red Analítica (ANP), el AHP clásico mantiene la simplicidad, y la transparencia del proceso de decisión, características cruciales para organizaciones con recursos limitados. Aunque el ANP [178], [179] es una forma más general que permite interdependencias entre criterios, es más estricto y consume más tiempo, lo que lo hace menos adecuado para profesionales ocupados en pymes. Mientras que métodos como el Fuzzy AHP se integran para manejar la imprecisión y la incertidumbre, el AHP estándar es eficaz porque estructura problemas complejos en una jerarquía y valida los juicios subjetivos a través de un análisis de consistencia [180].

En cualquier caso, la jerarquización permite afrontar un problema multifacético de forma organizada: el decisor se enfoca en comparar dos elementos a la vez según un criterio, lo que reduce la carga cognitiva frente a considerar todos los factores simultáneamente [181].

Estudios previos [183] - [185] han demostrado que el AHP constituye un enfoque eficaz para ayudar a las Pymes a hacer explícitas sus preferencias reales y descubrir posibles discrepancias entre lo declarado y lo realmente valorado. Por ejemplo, un gerente podría afirmar que desea “lo mejor en seguridad”, pero al aplicar comparaciones por pares podría revelar que prioriza la simplicidad y bajo costo sobre funcionalidades avanzadas. Este hallazgo orienta la decisión hacia una solución pragmática antes que una sofisticada pero impracticable.

Al ponderar los criterios mencionados, es frecuente que las Pymes otorguen mayor peso relativo a la usabilidad y al costo [185], [186]. En la práctica, una herramienta ligeramente menos potente

pero mucho más fácil de adoptar puede superar a otra más completa pero compleja, ya que lo crucial es que la metodología se use realmente en la empresa [187], [188]. Por ejemplo, Benz & Chatterjee [61] documentan que muchas pequeñas empresas fracasan en su evaluación de riesgos por la dificultad de implementar frameworks rígidos y terminología técnica confusa.

Asimismo, un estudio reciente subraya que las Pymes suelen carecer de talento especializado y tienden a ignorar partes de los marcos formales por su complejidad [8]. Por lo tanto, el hecho de utilizar AHP espera que criterios como “Facilidad de implementación” o “Compatibilidad con los procesos de la Pyme” tengan una prioridad alta en el vector de pesos, junto con el “Costo” [56], [189].

Por lo que se refiere a criterios como la funcionalidad técnica avanzada o la cobertura exhaustiva de controles podrían recibir un peso menor si exceden la capacidad de la organización para aprovecharlos [190], [191]. De modo que este perfil de ponderaciones debe derivarse de los juicios de los propios interesados (dueños o gestores de la Pyme, apoyados por algún asesor en seguridad si lo hubiera), garantizando que el resultado final refleje la realidad y las prioridades de la empresa.

Un valor añadido del proceso es que obliga a explicitar trade-offs; por ejemplo, ¿cuánto más importa la facilidad de uso frente a la conformidad normativa? ¿Es preferible una herramienta gratuita con soporte comunitario limitado, o pagar por una con soporte profesional? Estas decisiones implícitas se vuelven transparentes en el AHP al asignar calificaciones numéricas a cada comparación.

La elección de AHP como método de apoyo metodológico se fundamenta en varios aspectos prácticos y teóricos. Primero, AHP equilibra la rigurosidad con la transparencia. Su base matemática (cálculo de autovectores y autovalores) brinda un sustento sólido para justificar la decisión final, lo cual es importante para documentar ante la gerencia de la Pyme por qué se recomienda tal o cual enfoque. Al mismo tiempo, el procedimiento es lo suficientemente accesible para que los decisores no expertos lo entiendan: se puede implementar con herramientas tan simples como una hoja de cálculo, y cada paso (comparaciones y pesos) puede auditarse fácilmente. Esta trazabilidad aumenta la confianza en el proceso de decisión y facilita el buy-in de los responsables del negocio, un factor crítico señalado por varios autores para el éxito de proyectos de seguridad en organizaciones con recursos limitados [178].

En segundo lugar, mantenernos en el AHP clásico (con valores nítidos 1–9) evita añadir complejidad innecesaria. Es cierto que la literatura reciente muestra una tendencia a emplear variantes más sofisticadas, como el AHP difuso o la combinación de métodos (por ejemplo, AHP integrado con TOPSIS o VIKOR) [192]. De hecho, en contextos muy inciertos algunos investigadores han utilizado lógica difusa para modelar la vaguedad de las preferencias o redes analíticas (ANP) para capturar dependencias entre criterios [193].

Sin embargo, dichos enfoques pueden convertir el proceso en una "caja negra" para el usuario final de la Pyme [194]. Por ejemplo, un modelo Fuzzy AHP requiere funciones de pertenencia y procesos de "difusificación/defusificación" que podrían dificultar a un gerente comprender cómo un juicio verbal se tradujo en un número. Lo cual supone que si al final del día el responsable de la decisión no confía o no entiende el método, entonces es menos probable que este adopte sus resultados. Todas las observaciones de estudios comparativos han encontrado que, en muchos casos, las clasificaciones resultantes del AHP tradicional y del Fuzzy AHP son muy similares, lo que indica que la ganancia en "precisión" no necesariamente justifica la pérdida de simplicidad y transparencia [58], [195].

De manera análoga, el ANP aporta un modelado teóricamente más completo al permitir relaciones de influencia mutua entre criterios [178]. Lo que pasa con este es que dispara exponencialmente el número de comparaciones requeridas y la complejidad computacional [128]. En ese sentido para una Pyme, llenar cientos de comparaciones con consistencia es casi que inviable. Los otros métodos demandan cuantificar cada criterio previamente en una matriz de decisión, que en mi opinión es poco práctico cuando varios criterios son cualitativos (¿cómo puntuar con exactitud "cultura de seguridad" o "usabilidad" sin caer en subjetividades arbitrarias?). Lo más importante es que el método AHP fue diseñado justamente para integrar criterios tanto cuantitativos como cualitativos mediante juicios relativos.

1.2 Estado del arte

Este apartado analiza cómo la literatura reciente aborda el problema de investigación planteado: muchas pymes colombianas del sector servicios carecen de metodologías integrales y sistemáticas que articulen referentes internacionales de seguridad de la información y herramientas OpenSource accesibles para gestionar riesgos de seguridad informática de manera efectiva,

afectando la protección de sus activos y operaciones [27], [109]. La revisión se concentra en los desafíos asociados a la gestión de riesgos de seguridad informática, con énfasis en enfoques híbridos, adaptación de referentes internacionales a entornos de baja madurez y el uso de herramientas OpenSource o GRC para el seguimiento y tratamiento del riesgo. Esta carencia de metodologías integrales y accesibles para pymes del sector servicios se evidencia en múltiples estudios [198]--[202].

La literatura revisada señala la necesidad de adoptar enfoques híbridos y adaptar referentes internacionales de gestión del riesgo a la problemática sociotécnica de las pymes latinoamericanas [202]--[206], así como el valor de herramientas GRC y soluciones de software libre u OpenSource como apoyo operativo para documentar, monitorear y tratar riesgos, siempre que su uso se articule con una metodología clara [131], [206], [207]. En consecuencia, el estado del arte organiza los antecedentes según su aporte a la caracterización del problema, la adaptación de referentes internacionales, el análisis de herramientas tecnológicas, la integración entre metodologías y software, y la selección multicriterio mediante AHP. A partir de esta organización, la revisión se orienta por la siguiente pregunta: ¿cómo se puede estructurar una metodología que, a partir de referentes internacionales para la gestión de riesgos y herramientas OpenSource, ayude a las pymes a gestionar riesgos de seguridad informática?

La obtención de fuentes se realizó mediante una revisión documental sistemática orientada por palabras clave asociadas con seguridad informática, seguridad de la información, ciberseguridad, gestión de riesgos, evaluación y tratamiento del riesgo, referentes internacionales, metodologías, herramientas, software libre y OpenSource. Con este procedimiento se buscó identificar investigaciones pertinentes al problema de investigación y clasificarlas según su aporte al desarrollo del estado del arte.

Una vez obtenidos los resultados, se aplicaron criterios académicos de filtrado para asegurar la coherencia metodológica y temática de las fuentes seleccionadas. Las referencias no fueron incorporadas de manera acumulativa, sino clasificadas según su aporte al desarrollo del Estado del arte: algunas permitieron caracterizar el problema de la gestión de riesgos de seguridad informática en pymes; otras aportaron al análisis de estándares, guías, marcos de referencia y metodologías internacionales; un tercer grupo permitió revisar herramientas OpenSource y soluciones GRC aplicables; y otro conjunto sustentó el uso de enfoques híbridos y métodos

multicriterio como AHP. De esta manera, cada fuente cumple una función dentro del análisis y contribuye a fortalecer la trazabilidad entre el problema de investigación, los referentes revisados, las herramientas evaluadas y la metodología propuesta.

El rango temporal se delimitó entre 2019 y 2025, permitiendo excepciones fundacionales como el trabajo de Moncayo y Montenegro [205] o Blanco y Cabrera [206] debido a su relevancia sectorial, conceptual o metodológica para el análisis de pymes, gestión de riesgos y software libre u OpenSource en la región. El enfoque se concentró en pymes o ambientes de baja madurez, con énfasis en referentes internacionales, metodologías y herramientas aplicables a la gestión de riesgos, así como en soluciones computacionales que soportan su implementación.

1.2.1 Estudios sobre gestión del riesgo de seguridad informática en pymes

La gestión de riesgos de seguridad informática, apoyada en principios de seguridad de la información, ha evolucionado desde la aplicación rígida de normas hacia modelos flexibles, adaptados a realidades organizacionales complejas y orientados por enfoques analíticos más robustos. Esta evolución resulta especialmente relevante para pymes del sector servicios, que operan en entornos dinámicos, con recursos limitados y necesidades crecientes de protección sobre sus activos tecnológicos, información en operación y continuidad de sus procesos.

Otros trabajos abordan la gestión de riesgos en seguridad de la información y seguridad informática en contextos institucionales y organizacionales diversos. Algunos comparan o aplican referentes ampliamente utilizados, como NIST CSF, NIST SP 800-30, ISO 31000 e ISO/IEC 27005, destacando su aporte en la estructuración de capacidades organizacionales para la identificación, análisis, tratamiento y seguimiento de riesgos [35], [171], [197], [201], [209]--[212]. En conjunto, estos estudios evidencian que, pese a la existencia de estándares, guías y metodologías reconocidas internacionalmente, su aplicación en pymes suele ser poco sistemática y depende de la capacidad directiva, administrativa y técnica disponible.

- Aplicaciones sectoriales

La gestión de riesgos en la literatura reciente se ha dirigido a sectores específicos con necesidades críticas, lo cual es altamente coherente con el interés de esta investigación en el sector servicios colombiano. Giraldo [212] propuso un modelo de ciberseguridad basado en el análisis de riesgos para fortalecer la gestión de incidentes en empresas de servicios informáticos [212, p. 170]. La metodología se basó en el establecimiento de riesgos de ciberseguridad utilizando ISO 27005:2018 y proponiendo un plan de tratamiento con controles de ISO 27001:2013 y/o NIST 800-53 [212, pp. 162–165]. Los resultados más relevantes sugieren que el modelo integra normas de riesgo y gestión de incidentes, lo cual permite la reducción y el tratamiento de los incidentes identificados para las empresas especializadas en servicios de seguridad informática [212, p. 164]. La autora concluyó que el modelo de ciberseguridad construido, validado positivamente en el sector de servicios informáticos, logra integrar la gestión de riesgos y el manejo de incidentes, aspecto clave para la ciberseguridad integral [212, p. 188].

En el ámbito latinoamericano, también aplicable a pymes, se encuentra el estudio *Information security risk management model for mitigating the impact on SMEs in Peru* [213]. Este trabajo propuso un modelo de gestión de riesgos de seguridad de la información para mitigar amenazas en las pymes peruanas [213, p. 137]. Su método articuló MAGERIT como metodología de análisis y gestión de riesgos, ISO 31000 como referente general de gestión del riesgo e ISO/IEC 27004 como estándar para la definición de indicadores de seguimiento [213, p. 137]. El resultado más notable fue una disminución del riesgo del 71% en una pyme farmacéutica tras implementar 15 controles, lo que evidencia la viabilidad de modelos adaptados en organizaciones con presupuestos limitados y de baja madurez [213].

Por su parte, Huaman, Raymunda, y Rodríguez Novoa [204], en su artículo *Evaluación de riesgos en activos de tecnologías de información en una MIPYME*, tuvieron como objetivo evaluar los riesgos en activos de TI empleando un modelo basado en buenas prácticas [204, p. 216]. La metodología empleó elementos de MAGERIT, OCTAVE-S, ISO/IEC 27005 e ISO 31000 [175, p. 221]. Tras la aplicación en una MiPyme de transporte urbano, se identificaron 248 riesgos potenciales, de los cuales seis se clasificaron como no aceptables, para los que se propusieron estrategias de planes de tratamiento [204, p. 213]. Los autores concluyeron que el modelo híbrido propuesto es una

herramienta útil para la evaluación de riesgos en MiPymes, proporcionando una base para el tratamiento de riesgos [204, p. 223].

- Enfoques híbridos (cuantitativo–cualitativo)

Metodologías con enfoques mixtos es una práctica establecida en la literatura como necesaria para dotar de pragmatismo la evaluación del riesgo, especialmente en pymes. Así por ejemplo, en el estudio *Information Security Risk in SMEs: A Hybrid Model Compatible with IFRS* [205], se propuso una solución práctica para la gestión de TI en pymes a través de un modelo híbrido compatible con IFRS [205, p. 242]. La metodología combinó ISO/IEC 27005, OCTAVE-S y MAGERIT para el enfoque cualitativo, e IFRS (por sus siglas en inglés: *International Financial Reporting Standards*) para la cuantificación del impacto sobre los activos [205, p. 242]. Como resultado, se demostró la aplicabilidad técnica y operacional de un modelo híbrido en pymes del sector automotriz, con un esfuerzo razonable y poca especialización en TIC (Tecnologías de la Información y las Comunicaciones).

En un enfoque similar, el estudio *Risk Assessment Using NIST SP 800-30 Revisión 1 and ISO/IEC 27005 Combination Technique in Profit-Based Organization: Case Study* [57], tuvo como objetivo realizar una evaluación de riesgos mediante la combinación de NIST SP 800-30 Revisión 1 e ISO 27005 [57, p. 1206]. La metodología utilizó esta integración para identificar, analizar, evaluar y tratar riesgos en un sistema de información. Los autores concluyeron que la técnica de combinación de ambos referentes resulta eficaz para la evaluación de riesgos en una organización con fines de lucro, al facilitar la priorización y la toma de decisiones por medio de un análisis de probabilidad, vulnerabilidades e impacto [57, p. 1206], [196, p. 251].

- Riesgo dinámico

La literatura reciente evidencia que la gestión de riesgos de seguridad informática en pymes no puede depender únicamente de evaluaciones estáticas o periódicas [28, p. 2]. El estudio *Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach* [28], revisó literatura publicada entre 2016 y 2021, para evaluar la adecuación de enfoques de gestión de riesgos en pymes. Sus resultados señalan la necesidad de evolucionar hacia modelos más adaptables, eficientes y efectivos frente al panorama cambiante de

amenazas digitales, incorporando alternativas como sistemas dinámicos y *machine learning*, debido a que referentes como NIST e ISO pueden resultar abstractos para pymes y requieren actualización continua frente a amenazas que aumentan en frecuencia [28].

Esta necesidad se explica por la naturaleza cambiante de las amenazas digitales, la dependencia creciente de activos tecnológicos y la limitada capacidad técnica de estas organizaciones, condiciones que exigen mecanismos capaces de apoyar la identificación, seguimiento y tratamiento continuo de riesgos de TI que afectan activos críticos de información. En consonancia, el estudio *Methodology for Dynamic Analysis and Risk Management on ISO 27001* [214] destacó la complejidad y el alto costo del análisis reiterativo de riesgos. Su objetivo fue desarrollar una metodología de análisis y gestión dinámica del riesgo integrable con ISO/IEC 27001 [214]. La metodología propuesta, MARISMA-AGR, se orienta a pymes y se basa en modelos asociativos que facilitan el análisis dinámico y la reducción de costos, aunque también puede aplicarse en grandes empresas y en el sector salud [214], [215].

1.2.2 Adaptación de referentes internacionales a pymes

La problemática abordada en esta investigación, relacionada con la falta de metodologías sistemáticas para pymes, se encuentra respaldada por estudios que cuestionan la rigidez de los estándares y enfoques tradicionales, y proponen adaptaciones específicas para organizaciones con baja madurez técnica y administrativa.

- Estudios comparativos

Las comparaciones entre referentes de gestión de riesgos resultan relevantes para determinar la base teórica de una propuesta adaptada. En el estudio *Análisis comparativo de metodologías de análisis de riesgos (MAGERIT vs. NIST SP 800-30)* [211], se analizaron ambos referentes con el propósito de ofrecer criterios de decisión a las organizaciones [211, p. 267]. La investigación empleó un diseño cuantitativo comparativo [211, p. 276] y concluyó que tanto MAGERIT como NIST SP 800-30 son aplicables para minimizar riesgos en sistemas de información, al seguir actividades generales de identificación, análisis de vulnerabilidades y determinación del riesgo [211, p. 266]. No obstante, el estudio advierte que MAGERIT ofrece una visión más integradora y transversal de la operación, lo que puede aumentar su complejidad de implementación, mientras que NIST SP

800-30 proporciona una orientación más focalizada para la administración del riesgo [211, pp. 279–282].

De manera complementaria, la revisión sistemática *A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0* [54] comparó referentes como NIST CSF, ISO/IEC 27001:2022 y MAGERIT en el contexto de organizaciones complejas [54, p. 25]. A partir de una revisión sistemática de literatura [54, p. 28], el estudio identificó que MAGERIT ha ganado aceptación en Latinoamérica debido a su lenguaje sencillo y a su proceso de gestión de riesgos basado en ISO 31000, lo que lo convierte en un referente pertinente para entornos regionales como el colombiano [54, p. 31].

- Propuestas simplificadas

La dificultad de aplicar enfoques complejos de gestión de riesgos en pymes es un hallazgo recurrente en la literatura [28, p. 2]. En el estudio *Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs* [216], se señala que las pymes presentan requisitos especiales debido a sus recursos limitados, por lo que no todas las políticas de ciberresiliencia son directamente aplicables a este tipo de organizaciones [216, p. 69]. De forma complementaria, en el estudio sobre un modelo de gestión de riesgos para pymes peruanas [201], se adoptó el enfoque cuantitativo de ISO/IEC 27005 junto con las tres fases de OCTAVE-S [201, pp. 150–152]. Su objetivo fue permitir a las pymes cuantificar el valor del riesgo de sus activos y las causas de sus vulnerabilidades [201, p. 152]. Tras su implementación en el proceso de ventas de una pyme del sector cerámico, el modelo demostró facilidad de uso y logró una reducción del riesgo del 53 % [201, p. 150].

- Pruebas de concepto en Pymes

La validación empírica en contextos de baja madurez, pertinente para el problema de investigación con alcance en Colombia, se evidencia en estudios aplicados en Perú y Ecuador. En el caso peruano, la implementación de un modelo híbrido basado en MAGERIT e ISO/IEC 27004 en una pyme farmacéutica permitió una reducción del riesgo residual del 71 %, validando la efectividad de estos enfoques adaptados [213, p. 137]. En el contexto ecuatoriano, un modelo híbrido evaluado en dos pymes del sector automotriz evidenció aplicabilidad regional, al requerir un esfuerzo razonable por parte del personal operativo y baja especialización en TIC [205, p. 242].

1.2.3 Uso de herramientas OpenSource para gestión del riesgo

La integración de herramientas OpenSource constituye un componente central de la presente investigación, en tanto permite explorar soluciones tecnológicas de bajo costo para apoyar la gestión de riesgos en organizaciones con recursos limitados. La literatura ha explorado y analizado la viabilidad de este tipo de software en entornos académicos, corporativos y pymes, especialmente cuando se requiere documentar, monitorear y tratar riesgos de manera estructurada. Por consiguiente, el interés no se limita a la disponibilidad tecnológica de las herramientas, sino a su capacidad para articularse con metodologías claras, criterios de riesgo y necesidades operativas específicas. Algunas fuentes examinan el uso de herramientas OpenSource y soluciones tecnológicas de apoyo en ámbitos relacionados con la seguridad informática, demostrando su capacidad para ofrecer beneficios de bajo costo frente a soluciones propietarias [124], [152].

- Plataformas analizadas en literatura reciente

SimpleRisk ha sido identificada como una herramienta GRC adecuada para apoyar procesos estructurados de gestión del riesgo. En el estudio *Implementación de un software basado en herramientas de software libre para la gestión del riesgo* [206], se implementó SimpleRisk en una institución de educación superior en Colombia, con el propósito de satisfacer requerimientos del área de gestión de calidad y alinear el proceso con referentes como la NTC ISO 31000 y la NTC-ISO 9001 [206]. Los resultados evidenciaron que la herramienta facilitó las actividades de identificación, análisis, evaluación y monitoreo de riesgos, confirmando la viabilidad operativa del software libre para apoyar procesos estructurados de gestión del riesgo [206, p. 60].

De manera complementaria, la literatura identifica otras herramientas GRC orientadas a la gestión de riesgos de seguridad de la información. Estas soluciones, junto con metodologías y marcos de referencia, permiten a los analistas seleccionar alternativas acordes con los resultados esperados y con el propósito organizacional definido [217, p. 104]. Por ello, el análisis de herramientas debe considerar no solo sus funcionalidades, sino también su capacidad de alinearse con los procesos internos, el nivel de madurez de la organización, la disponibilidad de recursos técnicos y la sostenibilidad de su adopción en el tiempo.

- Experiencias reales / casos de éxito

Según la literatura, la aplicabilidad del software libre en pymes ha sido abordada desde experiencias relacionadas con servicios de TI. En el estudio *Implementación de herramientas en software libre para la gestión de servicios de red en las pymes, caso ASFEP* [218], se evaluó cómo la implementación de software libre podía mejorar la gestión de servicios de red de las pymes de Lima Metropolitana [218, pp. 302–305]. Mediante un enfoque cuantitativo, deductivo e hipotético [225], el trabajo concluyó que el uso de software open source generó impactos positivos en los ámbitos tecnológico, administrativo y económico, fortaleciendo la competitividad de la empresa [218, p. 307].

- Factores de adopción tecnológica

La adopción de soluciones tecnológicas para la gestión de riesgos de seguridad informática en pymes del sector servicios se encuentra condicionada por factores que van más allá de la funcionalidad del software. La literatura identifica como criterios relevantes el costo total de propiedad, la usabilidad para personal no especializado, la posibilidad de integración con referentes internacionales y la capacidad de adaptación frente a la naturaleza dinámica del riesgo. Estos factores son especialmente importantes porque las pymes requieren herramientas adecuadas para mejorar sus operaciones y reducir costos, mientras sus gerentes o propietarios no siempre cuentan con el conocimiento necesario para implementar análisis de riesgos complejos [156, p. 65]. En este sentido, el software libre se presenta como una alternativa viable por su capacidad de generar impactos positivos en el ámbito económico de la organización [218, p. 245].

En contextos latinoamericanos, la selección de soluciones adaptadas suele responder a la búsqueda de una alternativa razonablemente buena y económica, capaz de cerrar las brechas de seguridad más relevantes sin exigir inversiones desproporcionadas [215, p. 384]. Este criterio es coherente con las restricciones operativas de las pymes, donde la viabilidad de adopción depende tanto de la utilidad técnica como de la facilidad de implementación y sostenibilidad. Además, la simplificación y reducción de costos asociadas a las TIC resultan determinantes para que estas soluciones sean accesibles a empresas pequeñas [218, p. 246].

Otro factor crítico es la adaptabilidad y la usabilidad de las herramientas a los procesos internos de la organización. Referentes como NIST e ISO a menudo son percibidos como abstractos o complejos para las pymes [28, p. 3], por lo que las soluciones tecnológicas deben permitir personalización y uso práctico en la administración del riesgo [206, p. 24]. En esa línea, VERINICE ISMS, como herramienta de código abierto para SGSI, ejemplifica cómo el software libre permite establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la Información basado en múltiples estándares como ISO/IEC 27001 e ISO/IEC 27005 [217, p. 62], lo cual es crucial para entornos que buscan flexibilidad y cumplimiento.

En el estudio *Evaluación de riesgos en activos de tecnologías de información en una MIPYME* [204], reconocen que las MiPymes están expuestas a riesgos que pueden generar pérdidas por interrupción del servicio o daños a la reputación [204, p. 71], así, se evaluaron los riesgos en activos de TI empleando un modelo de evaluación híbrido basado en buenas prácticas, integrando elementos de MAGERIT, OCTAVE-S, ISO 31000 e ISO/IEC 27005. La investigación identificó que las MiPymes perciben estos referentes y buenas prácticas para la gestión de riesgos como distantes de su operación diaria, debido a que priorizan el trabajo productivo y la solución inmediata de problemas, esto inhibe la inversión de tiempo y esfuerzo en implementar nuevos procesos [204, pp. 72, 141]. Frente a esta barrera, el modelo propuesto redujo la complejidad al requerir un equipo de trabajo pequeño, lo que confirma que la usabilidad y la simplicidad son criterios críticos para la adopción la adopción de metodologías y herramientas de gestión de riesgos en pymes [204, p. 141].

Las motivaciones institucionales y regulatorias también inciden en la adopción de herramientas. Algunas organizaciones buscan adoptar estándares como ISO/IEC 27005 para responder a exigencias de seguridad de la información, privacidad y expectativas de partes interesadas (stakeholders) [52]. A su vez, el aumento de ataques informáticos impulsa la adopción de sistemas de gestión basados en políticas, procesos y referentes reconocidos que permitan mitigar los riesgos inherentes a la adopción de TIC [177, p. 209, 210]. En organizaciones de habla hispana, la disponibilidad en español y los costos reducidos del software libre constituyen factores adicionales que favorecen su implementación.

1.2.4 Estudios que integran metodologías y herramientas

La presente investigación se orienta a la integración de referentes internacionales, metodologías y plataformas de software para sistematizar los procesos de gestión del riesgo y facilitar su aplicación en contextos organizacionales con recursos limitados. En la literatura reciente, los estudios que articulan de manera explícita una metodología de gestión de riesgos con una herramienta tecnológica son menos frecuentes que aquellos que analizan ambos componentes por separado. Por esta razón, los antecedentes identificados resultan relevantes para establecer cómo una herramienta puede operar como soporte práctico del análisis, tratamiento, seguimiento y documentación de riesgos.

- Modelos integrados entre metodologías y herramientas

Uno de los antecedentes relevantes es el estudio *Herramientas para la gestión de riesgos de la seguridad de la información. Aplicación de GlobalSUITE al método Magerit* [207], desarrollado como Proyecto Fin de Grado en la E.T.S.I. de Sistemas Informáticos de la Universidad Politécnica de Madrid. Este trabajo tuvo un enfoque didáctico basado en recursos educativos abiertos y abordó la aplicación de la metodología MAGERIT mediante la herramienta GlobalSUITE. Su aporte principal consiste en mostrar cómo una metodología de análisis y gestión de riesgos puede materializarse en un entorno tecnológico que permite configurar activos, amenazas, salvaguardas y tratamientos de manera sistemática.

La metodología empleada se fundamentó en el ciclo de gestión de riesgos de MAGERIT, que analiza cómo los activos se encuentran expuestos a amenazas y cómo, en caso de materializarse el riesgo, se verían impactados. Para mitigar dichos riesgos, el proceso implica definir e implementar salvaguardas, analizar los resultados obtenidos, y finalmente, llevar a cabo un tratamiento de los riesgos. Un aspecto que facilita la comprensión del método y uso en escenarios empresariales es el enfoque didáctico a través de píldoras formativos como recursos de aprendizaje en forma de video y documentación para la configuración práctica de GlobalSUITE [207].

Entre los resultados del proyecto se destaca la provisión de una serie de recursos formativos para la aplicación de GlobalSUITE y la comparación de sus funcionalidades con PILAR, otra de las herramientas más utilizadas para la gestión de riesgos. Este antecedente evidencia que la

integración entre una metodología formal y una herramienta tecnológica puede facilitar la implementación de salvaguardas y el tratamiento sistemático de riesgos. Su valor para esta investigación radica en mostrar que el soporte tecnológico no sustituye la metodología, sino que permite operacionalizarla, documentarla y hacerla más comprensible para los usuarios finales [207].

Otro antecedente relevante es el estudio *Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs* [216], cuyo propósito fue desarrollar una herramienta de autoevaluación de ciberresiliencia para pymes. El trabajo parte del reconocimiento de que los referentes tradicionales pueden resultar rígidos para organizaciones con recursos limitados, por lo que propuso una herramienta web orientada a simplificar la evaluación y evolución de políticas de ciberresiliencia. El modelo conceptual fue probado en tres estudios de caso: una empresa de logística portuaria de El Salvador, un fabricante de pinturas de España y una organización de farmacia clínica en Estados Unidos [216].

CR-SAT integra políticas, priorización y evolución de capacidades en una herramienta operativa basada en web, diseñada como extensión de referentes como NIST. Su aporte consistió en combinar una lógica de autoevaluación con una interfaz simplificada que permite priorizar acciones de mejora sin exigir la implementación directa de marcos completos. Es por esto que resulta pertinente para esta investigación porque demuestra que, en entornos de baja madurez, la integración entre metodología y herramienta debe orientarse a reducir la complejidad, facilitar la adopción y apoyar la toma de decisiones.

- Evaluaciones de impacto

La evaluación del impacto de la integración entre referentes, metodologías y herramientas suele medirse mediante la reducción del riesgo, la priorización de decisiones o la mejora de capacidades de seguimiento [197], [219]. La combinación de NIST SP 800-30 Rev 1 y ISO/IEC 27005 permitió clasificar escenarios de riesgo y priorizar decisiones informadas mediante la cuantificación de la probabilidad y el impacto [57], [200].

Un ejemplo concreto es el modelo aplicado en una pyme peruana, que integró el catálogo de controles de MAGERIT con el estándar ISO/IEC 27004 para diseñar indicadores de seguimiento que permitieran monitorear la eficacia de los controles implementados y cuantificar el Retorno de la Inversión en Seguridad (ROSI) [213, pp. 137, 141, 147]. Este caso ilustra cómo la integración entre

una metodología de análisis de riesgos y un estándar de medición genera resultados verificables, un aspecto crítico para justificar la inversión en seguridad en pymes.

Otro antecedente relevante corresponde al modelo propuesto para empresas de servicios informáticos, en el cual se integró el análisis y gestión de riesgos según ISO/IEC 27005:2018 con el manejo de incidentes de seguridad [212]. En este caso, la evaluación por expertos permitió valorar positivamente la pertinencia del modelo para identificar, evaluar y tratar riesgos críticos asociados a incidentes de seguridad, fortaleciendo la respuesta operativa en organizaciones prestadoras de servicios informáticos [212, p. 108]. Este aporte resulta pertinente para la presente investigación porque evidencia una aplicación práctica de la gestión de riesgos en el sector servicios, aunque su foco se orienta al manejo de incidentes y no a la selección multicriterio de referentes internacionales y herramientas OpenSource.

1.2.5 Aplicaciones de AHP en selección de referentes internacionales y herramientas

Aunque el Proceso de Jerarquía Analítica (AHP) no aparece de forma generalizada en todos los estudios sobre gestión de riesgos, la literatura evidencia la necesidad de utilizar métodos cuantitativos que fortalezcan la comparación rigurosa de alternativas y la toma de decisiones multicriterio. Esta necesidad resulta especialmente relevante en pymes, donde la selección de referentes o herramientas no debería depender únicamente de criterios intuitivos, disponibilidad inmediata o experiencia previa, sino de una ponderación explícita de factores técnicos, económicos y operativos [192].

La literatura reconoce la tendencia hacia métodos cuantitativos avanzados. En este sentido, algunos estudios identifican iniciativas basadas en *soft-computing*, modelos híbridos avanzados, AHP y métodos comprensivos difusos como alternativas para fortalecer la evaluación y priorización en escenarios de incertidumbre [193], [220]. De manera complementaria, otras investigaciones documentan el uso de métodos multicriterio, como la ponderación aditiva simple y el AHP, para clasificar activos de información y priorizar riesgos, lo que evidencia su utilidad para estructurar decisiones donde intervienen múltiples criterios de valoración [53], [192], [221].

La robustez de los modelos adaptados a pymes se puede verificar mediante herramientas estadísticas que validan la opinión experta [204], por ejemplo, algunos estudios han validado modelos híbridos mediante juicio de expertos y utilizando el Coeficiente de Concordancia W de Kendall para asegurar el acuerdo entre los especialistas [204]. De manera similar, otros han utilizado el Alfa de Cronbach para determinar la confiabilidad de los instrumentos de medición, obteniendo niveles reportados de "muy alta" [222]. En consecuencia, el uso de AHP en esta investigación se justifica como un mecanismo de priorización y selección multicriterio, no como una validación absoluta de la metodología. Su aporte consiste en hacer explícitos los criterios de decisión, transformar valoraciones cualitativas en prioridades cuantitativas y sustentar de manera trazable la selección de referentes internacionales y herramientas OpenSource para la gestión de riesgos de seguridad informática en pymes.

1.2.6 Síntesis crítica y vacío identificado

A partir del análisis desarrollado en los apartados 1.2.1 a 1.2.5, se evidencia que la literatura ha avanzado en tres líneas relevantes para esta investigación: la gestión de riesgos de seguridad informática en pymes, la adaptación de referentes internacionales a contextos de baja madurez, la utilización de herramientas OpenSource o GRC como apoyo operativo, la integración parcial entre metodologías y herramientas, y la aplicación de métodos multicriterio para priorizar riesgos, activos, controles o alternativas de decisión. Estos antecedentes permiten afirmar que el problema de investigación no surge por ausencia total de enfoques, instrumentos o herramientas, sino por la falta de una articulación sistemática entre ellos.

La evidencia recopilada demuestra la viabilidad conceptual de los componentes de la tesis: Por una parte, la literatura reconoce la necesidad de simplificar y adaptar los referentes de gestión de riesgos cuando se aplican a pymes, debido a sus restricciones técnicas, económicas, administrativas y de personal [28], [216]. Por otra parte, los estudios sobre modelos híbridos evidencian que la combinación de distintos referentes puede mejorar la aplicabilidad de la gestión de riesgos en organizaciones con baja madurez [204], [205]. Asimismo, los antecedentes sobre herramientas OpenSource y GRC muestran que soluciones como SimpleRisk o PILAR pueden apoyar actividades de identificación, análisis, evaluación, tratamiento, documentación y seguimiento del riesgo en contextos latinoamericanos [202], [206].

Sin embargo, estos aportes aparecen de manera fragmentada. Algunos estudios se concentran en adaptar referentes internacionales a pymes; otros proponen modelos híbridos; otros validan herramientas tecnológicas específicas; y otros emplean métodos multicriterio para priorizar activos, riesgos o controles. Por tanto, no se identifica una propuesta que articule de manera explícita ni mucho menos secuencial sobre la selección de referentes internacionales, la selección de una herramienta OpenSource y la validación práctica de una metodología de análisis y gestión de riesgos de seguridad informática en una pyme del sector servicios.

Esto es relevante porque los estudios previos adoptaron referentes o herramientas tecnológicas a partir de criterios implícitos, experiencia del investigador, disponibilidad inmediata o adecuación general al contexto. En consecuencia, no siempre queda claro por qué una alternativa resulta más adecuada que otra para una pyme con baja madurez técnica, restricciones presupuestales y necesidades operativas concretas. Allí entran preguntas como por qué OCTAVE-S puede ser preferible a NIST SP 800-30 en un contexto particular, o qué criterios justifican seleccionar MONARC frente a SimpleRisk, PILAR, ERAMBA o Pirani Risk, requieren un proceso de comparación trazable, documentado y técnicamente sustentado.

En atención a este vacío, la presente investigación utiliza el AHP en dos momentos críticos del diseño metodológico: primero, para caracterizar y seleccionar el referente internacional de gestión de riesgos aplicable a seguridad informática más adecuado para orientar una metodología dirigida a pymes colombianas del sector servicios; y segundo, para analizar y seleccionar la herramienta OpenSource que mejor satisface los requisitos funcionales derivados del diseño metodológico. Se aclara que el AHP no se asume como mecanismo de validación absoluta de la metodología, sino como instrumento de priorización y selección multicriterio que permite hacer explícitos los criterios de decisión y fortalecer la trazabilidad del proceso.

De este modo, la metodología propuesta no se limita a combinar elementos previamente estudiados, sino que fundamenta objetivamente por qué una combinación específica de referentes y una herramienta particular resultan pertinentes para el contexto investigado. Este aporte de tipo profundización permite superar una limitación frecuente en los enfoques revisados, es decir, la ausencia de una justificación sistemática sobre la selección metodológica y tecnológica. Así pues, la tesis aporta una ruta estructurada para pasar de la revisión documental a la selección

multicriterio, y de esta a la aplicación práctica mediante una herramienta OpenSource en un caso de estudio o prueba de escritorio.

Este vacío metodológico es el objeto de la presente tesis, cuyo objetivo es proponer una metodología para el análisis y gestión de riesgos de seguridad informática en pymes, basada en la articulación de referentes internacionales y software OpenSource disponibles, que fortalezca la protección de sus activos y operaciones. Con esta síntesis se cierra el Estado del Arte y se establece la base lógica para el capítulo metodológico, en el cual se describen las fases, criterios, instrumentos y procedimientos utilizados para diseñar, seleccionar, aplicar y validar la metodología propuesta.

2. Metodología

En este apartado se describen los procedimientos, técnicas, actividades e instrumentos empleados para cumplir cada objetivo específico planteado en la investigación. Se presenta el enfoque metodológico adoptado, método y diseño del estudio, la unidad de análisis y la secuencia de fases, de modo que el lector comprenda de forma organizada, precisa y lógica cómo se abordó el problema de investigación, cómo se alcanzaron los objetivos específicos y, por ende, el objetivo general de “Proponer una metodología para el análisis y gestión de riesgos de seguridad informática en pymes, basada en normas internacionales y software OpenSource disponibles, que fortalezca la seguridad y contribuya a la protección de sus activos y operaciones”.

2.1 Enfoque de la investigación

La investigación adopta un enfoque de métodos mixtos, integrando técnicas cualitativas y cuantitativas dada la naturaleza del problema de investigación, así, se aprovechan las fortalezas de ambos paradigmas, particularmente en escenarios organizacionales donde intervienen factores técnicos y humanos [223]. Según Johnson y Onwuegbuzie , la investigación mixta se define como “el tipo de investigación en el que se recopilan, analizan y combinan datos cuantitativos y cualitativos en un solo estudio o serie de estudios para responder preguntas de investigación” [224]. Diversos autores señalan que abordar una investigación mediante dos métodos puede producir resultados más confiables [225].

En términos operativos, la investigación se concreta en combinar un análisis documental cualitativo de normas internacionales y herramientas OpenSource, con un componente cuantitativo soportado en comparaciones multicriterio mediante el proceso de análisis jerárquico AHP.

En coherencia con lo anterior, el enfoque mixto se implementó de manera secuencial por fases, articulando la caracterización, análisis y selección (OE1 y OE2) con la materialización operativa de la propuesta (OE3) y su validación (OE4). En particular, OE3 se orienta a demostrar que la herramienta OpenSource seleccionada ejecuta el ciclo de gestión del riesgo definido desde los referentes normativos, evitando que el uso del software se limite a una configuración técnica aislada. Finalmente, OE4 consolida el enfoque pragmático al validar la metodología mediante un caso de estudio o prueba de escritorio, verificando su coherencia interna y viabilidad de aplicación en un escenario representativo.

2.1.1 Componente cualitativo

Desde el componente cualitativo, se realizó principalmente un análisis documental, entendiendo como técnica de revisión e interpretación sistemática de información proveniente de fuentes escritas relevantes que cumplieron con criterios para ser de alto impacto. Se consideraron, entre ellos, documentos de revisión sistemática de literatura científica y técnica sobre metodologías de análisis y gestión de riesgos en seguridad informática, enfocada en normativas internacionales relevantes para pymes.

La revisión documental permitió identificar y comprender principios, directrices y prácticas que se puedan ajustar a la seguridad informática en las pymes. Así mismo, como insumo contextual inicial, se aplicó un instrumento de diagnóstico a pymes como público específico, a fin de relevar el estado actual en gestión de riesgos de seguridad en pymes de Colombia. Dicho diagnóstico sirvió para comprender el contexto y necesidades, prácticas de riesgo y percepciones sobre adopción de normas y herramientas por parte de gerentes, administradores, auditores, especialistas, tecnólogos, ingenieros de TI y responsables de la seguridad informática y/o TIC; sin embargo, no se integró como fase central del método, sino como información de partida.

Paralelamente, se llevó a cabo un análisis funcional y documental de herramientas o soluciones tecnológicas OpenSource orientas a la gestión de riesgos.

Para la identificación de herramientas OpenSource, se realizó una exploración sistemática de plataformas especializadas en recopilación, evaluación y difusión de soluciones de software, entre las cuales se destacan Goodfirms, Capterra, SourceForge, GetApp, GitHub y G2, entre otras. Esos sitios fueron utilizados como fuentes primarias para la localización de herramientas activas, mantenidas por comunidades de desarrollo y con aplicabilidad real en escenarios organizacionales.

En particular, GitHub permitió evaluar aspectos asociados al nivel de madurez del proyecto, frecuencia de Actualizaciones, documentación técnica y actividad de la comunidad, mientras que plataformas como Capterra, SourceForge y G2 confirmaron las opiniones y percepciones de usuarios. De igual manera, se accedió a los sitios oficiales de las herramientas, con esto se facilitó la identificación de casos de uso, descripciones funcionales y competitividad en el mercado.

Durante este proceso, se evidenció que la literatura académica reciente ha abordado en investigaciones herramientas OpenSource como PILAR y SimpleRisk en estudios relacionados con la gestión de riesgos de seguridad de la información. Al mismo tiempo que han abordado herramientas pagas como GlobalSuite. No obstante, no se identificaron investigaciones que analicen de forma sistemática otras soluciones OpenSource relevantes como ERAMBA, MONARC o Pirani Risk, a pesar de su uso documentado en entornos profesionales y organizacionales.

Ante la ausencia de estudios previos sobre las herramientas mencionadas, justificó su inclusión dentro del análisis cualitativo, aportando un valor exploratorio y diferencial. Conforme a esto, es consistente con estudios metodológicos de tipo propositivo–aplicado, donde el análisis cualitativo constituye la base para la construcción y validación de modelos y metodologías ajustadas a un entorno específico [226].

Adicionalmente, el componente cualitativo no se restringe a la revisión documental de OE1–OE2, sino que se extiende a OE3–OE4 mediante la construcción y verificación del artefacto metodológico. En OE3, se realiza un mapeo normativo–funcional entre las etapas del ciclo de gestión de riesgos y las funcionalidades del software seleccionado, junto con la personalización de catálogos, escalas y flujo de trabajo para el contexto PyME. En OE4, se diseña un protocolo de

caso/prueba de escritorio para analizar cualitativamente la trazabilidad, coherencia y utilidad de los entregables producidos por la metodología, como parte del proceso propositivo–aplicado.

2.1.2 Componente cuantitativo

Desde el componente cuantitativo, la investigación recurrió al Proceso de Análisis Jerárquico (Analytic Hierarchy Process - AHP) como método de apoyo a la decisión multicriterio, con el fin de caracterizar y analizar las alternativas, tanto en lo relacionado con enfoques normativos y marcos de trabajo internacionales, como con herramientas OpenSource orientadas para el análisis y la gestión de riesgos de seguridad de la información que se puedan ajustar a la seguridad informática en las pymes.

Este tipo de aproximación cuantitativa resulta pertinente cuando se busca analizar relaciones entre variables y generar comparaciones objetivas apoyadas en datos numéricos [98].

El AHP permitió estructurar jerárquicamente el problema de decisión, definiendo un objetivo claro, criterios de evaluación acordes a las características de las pymes y un conjunto de alternativas a comparar, alineadas con los objetivos específicos de la investigación. Este enfoque facilitó el análisis sistemático de múltiples criterios a la vez, reconociendo que la selección de metodologías y de herramientas de gestión de riesgos no depende de un único factor, sino de la combinación de varios aspectos, entre ellos técnicos, metodológicos y organizacionales.

A partir de esa estructura, con el apoyo de juicios expertos, se realizaron comparaciones por pares, tanto entre los criterios definidos como entre las alternativas evaluadas frente a cada criterio. Esto permitió establecer la importancia relativa de los criterios y el posicionamiento de las alternativas, asegurando la coherencia interna de los juicios y la consistencia del análisis.

El uso del AHP aportó rigurosidad y objetividad al componente cuantitativo, transformó valoraciones cualitativas en insumos estructurados para el análisis comparativo. De esta manera, el método funcionó como un mecanismo de soporte decisional.

En ese sentido, el enfoque de la investigación facilitó triangulación metodológica, aumento de la validez al conjugar la profundidad contextual del análisis cualitativo con la precisión analítica del componente cuantitativo [98].

Por consiguiente, el AHP no solo respalda a los OE1 y OE2 al priorizar marcos normativos internacionales y herramientas OpenSource, sino que también habilita a los OE3 y OE4 al definir, con sustento cuantitativo, el referente y la tecnología sobre los cuales se implementa y valida la metodología.

Hay que mencionar, además, los pesos y rankings obtenidos constituyeron un insumo decisional para orientar la construcción del artefacto metodológico y su despliegue en el software seleccionado, reduciendo la subjetividad del proceso comparativo. De manera análoga, durante la prueba de escritorio se consideran insumos cuantificables generados por la herramienta (p. ej., niveles de riesgo y salidas de priorización) como apoyo descriptivo para la interpretación integral, complementando la lectura cualitativa del caso.

2.2 Método y diseño de la investigación

El método de investigación es propositivo–aplicado. Esto es adecuado para estudios cuyo propósito es diseñar una solución metodológica a un problema real, a partir del análisis sistemático de referentes teóricos, técnicos y prácticos, además de verificar su aplicabilidad en un contexto organizacional representativo. Este enfoque metodológico permitió articular la revisión documental, el análisis comparativo y la estructuración de una propuesta orientada a las necesidades de las pymes del sector servicios.

El diseño de la investigación es no experimental, dado que no se manipularon variables ni se establecieron condiciones de control, sino que se analizaron normas internacionales, marcos de trabajo y herramientas OpenSource existentes tal como se presentan en su entorno natural de aplicación. En coherencia, el estudio presenta un alcance descriptivo–propositivo: descriptivo, en tanto caracteriza y analiza enfoques normativos internacionales, herramientas y soluciones OpenSource; y propositivo, al concretarse en la propuesta de una metodología de gestión de riesgos ajustada al contexto de las pymes.

La presente investigación adopta una orientación pragmática, centrada en la generación de un resultado útil y aplicable, más que en la comprobación de hipótesis causales. La propuesta metodológica construida se sometió posteriormente a una validación mediante un caso de estudio o prueba de escritorio, con el fin de evaluar su coherencia interna y su viabilidad operativa en un escenario organizacional simulado, representativo de una pyme.

La secuencia detallada de actividades, técnicas e instrumentos empleados en cada fase de la investigación se describe de manera específica en el apartado correspondiente a las fases metodológicas.

2.3 Unidad de Análisis

La unidad de análisis estuvo conformada por los referentes metodológicos y tecnológicos empleados en la gestión de riesgos de seguridad de la información en pymes, considerando tanto normas internacionales como herramientas y soluciones de software OpenSource.

En el componente cualitativo, la unidad de análisis correspondió a: (i) normas internacionales y marcos de trabajo orientados a la gestión de riesgos de seguridad, analizados desde principios, directrices y requisitos; (ii) documentación técnica y funcional de herramientas de software OpenSource, analizadas en función de sus capacidades de aplicación en contextos organizacionales pyme.

En el componente cuantitativo, la unidad de análisis se centró en las alternativas normativas y tecnológicas consideradas para el análisis comparativo, las cuales fueron tratadas como opciones de decisión dentro de un esquema multicriterio de evaluación, y de acuerdo con criterios definidos para valorar su adecuación. De esta forma, se mantuvo coherencia entre enfoque, método y objetivo de investigación, concentrando el análisis en los elementos metodológicos y técnicos que sustentan la propuesta desarrollada.

2.4 Fases Metodológicas

El desarrollo metodológico se organizó en cuatro fases secuenciales, cada una orientada directamente al cumplimiento de los objetivos específicos planteados. Dichas fases articulan las técnicas cualitativas y cuantitativas descritas en los apartados anteriores del presente capítulo, manteniendo coherencia con el enfoque mixto y con el carácter propositivo–aplicado del estudio.

La secuencia metodológica permitió avanzar progresivamente desde la comprensión de los referentes normativos y TIC hasta la construcción y validación de la propuesta metodológica. A continuación, se describe el procedimiento realizado en cada fase, incluyendo las técnicas,

instrumentos, actividades desarrolladas y productos esperados (sin presentar resultados) para el cumplimiento de cada objetivo específico.

2.4.1 Fase I: Caracterización de normas internacionales para la gestión de riesgos en seguridad informática en pymes

Objetivo asociado: Caracterizar normas internacionales para la gestión de riesgos comprendiendo los principios, directrices y requisitos que se puedan ajustar a la seguridad informática en las pymes.

Técnica principal: Análisis documental comparativo complementado con evaluación multicriterio mediante AHP.

Descripción general de la Fase I:

La fase I tuvo como propósito identificar, analizar y comparar los marcos normativos más relevantes para la gestión de riesgos de seguridad de la información, con el fin de determinar cuáles ofrecen la estructura conceptual y metodológica más adecuada para el contexto operativo, considerando además las restricciones que pymes del sector servicios tienen típicamente.

La pertinencia de los marcos referentes para la gestión de riesgos analizados fue establecida previamente en el capítulo 1.2 Estado del Arte, allí se evidenció que la literatura reciente converge en la necesidad de metodologías simplificadas, aplicables y basadas en estándares, especialmente cuando se combinan con soportes herramientas y soluciones de software OpenSource.

En coherencia con ello, los estándares considerados incluyeron ISO/IEC 27005:2022, NIST SP 800-30, MAGERIT, OCTAVE-S y EBIOS RM, seleccionados por su reconocimiento global y potencial aplicabilidad al contexto de pymes.

Procedimiento:

El procedimiento se estructuró en tres etapas:

- Etapa 1: Revisión documental sistemática

Se consultaron fuentes primarias (documentación oficial de los estándares y marcos de trabajo) y fuentes secundarias (literatura científica indexada en bases de datos académicas especializadas).

Este procedimiento es consistente con el señalado en el Estado del Arte, donde se destacó la importancia de búsquedas bibliográficas y filtradas mediante criterios académicos de pertinencia, impacto y enfoque pyme.

La consulta se ejecutó empleando operadores booleanos y combinaciones de palabras clave, tales como “risk management SME”, “information security risk assessment”, “ISO 27005”, “MAGERIT”, “OCTAVE-S”, “EBIOS RM”, “NIST SP 800-30”, entre otras. La búsqueda inicial se centró en términos clave como "Ciberseguridad", "Metodología", "Gestión", "Riesgos", "Normas", y "Software Open-Source", utilizando además una vasta red de sinónimos y términos técnicos como "model", "methodology", "standard", "method", "framework", "analysis", "assessment", "information security", "information technology", "TIC", "cybersecurity", "risk management", "risk analysis", "risk assessment", "risk treatment", "using guidance", "software", "tool", "OSS", "open source software", "software free", "cybersecurity risk management software". Esta estrategia de búsqueda exhaustiva, similar a la utilizada en revisiones formales, permitió cubrir bases de datos académicas y literatura gris regional.

Para cada marco se analizaron los siguientes aspectos:

- Principios y fundamentos conceptuales.
- Secuencia metodológica del proceso de gestión de riesgos (etapas, actividades, entradas y salidas).
- Requisitos técnicos y recursos necesarios para su implementación.
- Elementos de coincidencia y divergencia entre marcos.
- Nivel de prescripción normativa o grado de flexibilidad aplicativa.

La información obtenida se organizó mediante un análisis documental comparativo, garantizando un abordaje homogéneo y permitiendo identificar con claridad los principios, directrices y requisitos de cada marco normativo.

- Etapa 2: Evaluación de adaptabilidad al contexto pyme.

Con base en la matriz de operacionalización (ver Anexo B) y en las conclusiones del Estado del Arte, se establecieron criterios cualitativos de evaluación derivados de restricciones operativas reales

típicas de pymes en Colombia: limitaciones de recursos, baja madurez digital, ausencia de personal especializado y necesidad de procesos simples pero robustos.

El siguiente paso responde a la necesidad, ampliamente documentada en la literatura, de adaptar el contenido normativo al contexto pyme, así, evitar la aplicación literal de estándares pensados originalmente para grandes organizaciones.

Se definieron cuatro criterios:

- **Practicidad y simplicidad.**
- **Consideraciones técnico-administrativas.**
- **Recomendaciones de tratamiento del riesgo.**
- **Directrices para implementación de controles.**

  - Etapa 3: Aplicación del método AHP

Para introducir rigor cuantitativo y reducir la subjetividad en la comparación de alternativas, se aplicó el AHP. Este método fue seleccionado en congruencia con los hallazgos del Estado del Arte, donde se observaron tendencias crecientes hacia métodos multicriterio para apoyar decisiones en escenarios caracterizados por incertidumbre, recursos limitados y necesidad de priorización estructurada.

La estructura jerárquica del modelo se definió así:

Objetivo: Determinar, entre los estándares, guías y metodologías internacionales analizados, el referente para la gestión de riesgos más adecuado para sustentar una metodología dirigida a pymes.

Criterios: Los cuatro criterios de adaptabilidad definidos en la Etapa 2.

Alternativas: ISO/IEC 27005, NIST SP 800-30, MAGERIT, OCTAVE-S y EBIOS RM.

En lo que respecta a la obtención de los juicios, cada integrante del panel de expertos realizó de manera independiente las matrices de comparación por pares. Posteriormente, se llevó a cabo una sesión de consenso deliberativo en la que el panel discutió cada una de las comparaciones, expuso sus razones, argumentó las diferencias de por qué su ponderación hasta alcanzar un acuerdo

explícito sobre el valor que mejor representaba la relación de importancia entre criterios y alternativas. Así, a partir de ese diálogo, se acordó colectivamente una única matriz consensuada, registrada como insumo definitivo para el cálculo de prioridades.

Ahora bien, debido a que la matriz final se construyó por consenso argumentado, más no por agregación matemática de valoraciones divergentes, entonces no fue necesario aplicar media geométrica como técnica de integración, esto se subraya a pesar de que ese procedimiento constituye el método recomendado cuando se combinan juicios individuales independientes en ausencia de deliberación grupal.

El proceso completo de aplicación del AHP se desarrolló utilizando una plantilla especializada proporcionada por uno de los expertos del panel. Esta herramienta automatizaba los cálculos matemáticos del método (vectores de prioridad, índices de consistencia y síntesis global), mientras que los juicios necesarios para construir las matrices de comparación por pares fueron ingresados manualmente por el equipo durante una sesión de consenso.

El proceso completo incluyó: (1) la construcción de matrices de comparación por pares entre los cuatro criterios de adaptabilidad; (2) la valoración comparativa de las cinco alternativas normativas respecto a cada criterio; (3) el cálculo automatizado de los vectores de prioridad; (4) la verificación de la Razón de Consistencia ($CR \leq 0.10$); y (5) la síntesis global para obtener el ranking final del marco normativo más adecuado para sustentar una metodología dirigida a pymes.

Productos de la fase:

- Análisis documental comparativo de referentes internacionales aplicables a la gestión de riesgos de seguridad informática, elaborado a partir de la revisión sistemática de estándares, guías y metodologías, entre ellos ISO/IEC 27005, NIST SP 800-30, MAGERIT, OCTAVE-S y EBIOS RM, integrado en los apartados 1.1 Marco Teórico y 1.2 Estado del Arte.
- Definición de criterios de adaptabilidad para pymes, derivados de la matriz de operacionalización y de la literatura reciente.
- Modelo jerárquico AHP, que incluye: a) matrices de comparación por pares entre los criterios; b) matrices comparativas de los cinco marcos internacionales para la gestión de riesgos aplicables a seguridad informática respecto a cada criterio; c) cálculo automatizado

de vectores de prioridad y verificación de consistencia; d) ranking final del marco referencial más adecuado, construido mediante consenso deliberativo del panel de expertos.

- Síntesis integradora de principios, directrices y requisitos aplicables al contexto pyme, insumo utilizado para el diseño de la metodología propuesta.

2.4.2 Fase II: Análisis de herramientas y soluciones de software para la gestión de riesgos

Objetivo asociado: Analizar herramientas y soluciones de software que puedan ajustarse a la gestión de riesgos, seleccionando uno o varios softwares a utilizar.

Técnica principal: Análisis técnico-funcional complementado con evaluación multicriterio mediante AHP.

Descripción general de la Fase II:

La Fase II tuvo como propósito identificar, analizar y comparar herramientas y soluciones de software orientadas a la gestión integral de riesgos de seguridad de la información, con el fin de seleccionar aquella que ofreciera mayor alineación con los requisitos metodológicos derivados del análisis normativo desarrollado en la Fase I.

El fundamento conceptual para esta fase se estableció en los apartados “1.1.6 Enfoque sociotécnico y uso de software OpenSource” y “1.2.3 Uso de herramientas OpenSource para gestión del riesgo” del Marco Teórico y Estado del Arte, donde se argumentó:

- El rol crítico del software en entornos con baja madurez de ciberseguridad y seguridad informática.
- La necesidad de herramientas TIC que gestionen activos, amenazas, vulnerabilidades y riesgos.
- La importancia de la usabilidad, accesibilidad técnica y adaptabilidad en contextos pyme.
- Los criterios funcionales de alineación entre herramientas y marcos normativos (capacidad de personalización, gestión de catálogos, soporte a opciones de tratamiento).

Procedimiento:

A partir de esa base conceptual se desarrolló un proceso sistemático en tres etapas.

- Etapa 1: Búsqueda y preselección de herramientas OpenSource

Se realizó una exploración estructurada en diversas fuentes especializadas, con el fin de identificar alternativas viables para la gestión de riesgos de seguridad de la información en contextos de pymes.

La búsqueda incluyó repositorios públicos de software libre, tales como GitHub, SourceForge y GitLab, en los cuales se evaluaron aspectos relacionados con la madurez de los proyectos, la actividad de desarrollo, el tipo de licenciamiento y la participación de la comunidad.

De manera complementaria, se consultaron plataformas de evaluación de software como Goodfirms, Capterra, GetApp, Software Advice y G2, que permitieron identificar percepciones de usuarios, casos de uso documentados y valoraciones asociadas a la experiencia de adopción en entornos organizacionales.

Asimismo, se revisaron los sitios oficiales de los proyectos OpenSource para obtener información sobre manuales de usuario, documentación técnica, arquitectura de las soluciones y lineamientos de implementación.

Finalmente, se consideró literatura académica y técnica reciente, en la cual se identificaron referencias a herramientas TIC como SimpleRisk y PILAR, utilizadas en estudios o experiencias prácticas relacionadas con la gestión de riesgos.

Se definieron criterios de inclusión mínimos:

- Licenciamiento OpenSource verificable.
- Proyecto activo (Actualizaciones recientes o comunidad activa).
- Funcionalidades orientadas a gestión de riesgos.
- Documentación técnica disponible.

  Uso reportado en organizaciones o estudios previos.

Como resultado de esta etapa se preseleccionaron cinco herramientas para gestión de riesgos: tres soluciones OpenSource (SimpleRisk, ERAMBA y MONARC) y dos herramientas de referencia con

modelos de licenciamiento alternativos (PILAR como software propietario de uso gratuito y Pirani Risk como solución freemium). La inclusión de estas últimas respondió a su representatividad metodológica en contextos hispanohablantes y a la necesidad de establecer benchmarks funcionales que permitieran evaluar comparativamente las capacidades de las alternativas de código abierto.

- Etapa 2: Análisis técnico-funcional de las herramientas

Una vez preseleccionadas las herramientas OpenSource, se llevó a cabo un análisis técnico-funcional con el propósito de evaluar su capacidad para dar soporte efectivo a procesos de gestión de riesgos de seguridad de la información en contextos pyme.

Este análisis se desarrolló a partir de la revisión sistemática de la documentación oficial de cada herramienta, incluyendo manuales de usuario, guías técnicas y descripciones de arquitectura. También se revisó el análisis de requisitos técnicos de implementación asociados a la infraestructura necesaria, procesos de instalación y dependencias tecnológicas.

Más aún, se revisaron funcionalidades clave con relación al ciclo de gestión de riesgos, y se exploraron casos de uso reportados y opiniones de comunidades de usuarios, con el fin de contrastar la descripción técnica con experiencias de implementación documentadas.

Este procedimiento responde a la necesidad, ampliamente documentada en la literatura, de evaluar no solo la disponibilidad técnica de las herramientas, sino también su adecuación funcional y operativa a organizaciones con recursos limitados, baja madurez en ciberseguridad y ausencia de personal especializado, características típicas de las pymes.

Acorde al enfoque sociotécnico desarrollado en el apartado “1.1.5 del Marco Teórico, en los criterios funcionales de alineación entre herramientas y marcos normativos” allí identificados (capacidad de personalización, gestión de catálogos y soporte a opciones de tratamiento de riesgos), y en las restricciones operativas propias de las pymes descritas en el apartado 1.1.3, se definieron cuatro criterios evaluativos para el análisis comparativo de las herramientas OpenSource:

- **Gestión organizacional.**
- **Análisis técnico.**

- **Gestión de riesgos.**
- **Viabilidad técnica y operativa.**

Estos criterios emergen de la intersección entre los requisitos funcionales identificados en el Marco Teórico (apartado 1.1.5), las limitaciones estructurales de las pymes (apartado 1.1.3), y los factores de adopción tecnológica documentados en el Estado del Arte (apartado 1.2.3).

- Etapa 3: Aplicación del método AHP

Dejando de lado lo cualitativo y la subjetividad inherente que conlleva, se introdujo rigor cuantitativo en la priorización de las herramientas OpenSource analizadas aplicando el AHP, técnica utilizada también en la Fase I de la investigación, con la diferencia de que ahora fue aplicada únicamente por el investigador principal, sin panel de expertos.

Su utilización es consistente con los hallazgos del Estado del Arte, donde se evidencian tendencias crecientes hacia el uso de métodos multicriterio para apoyar la toma de decisiones en escenarios caracterizados por múltiples variables, recursos limitados y necesidad de priorización estructurada.

La estructura jerárquica del modelo se definió de la siguiente manera:

Objetivo: Seleccionar la herramienta o solución de software OpenSource más adecuada para soportar la metodología propuesta de gestión de riesgos de seguridad en pymes.

Criterios: Los cuatro criterios funcionales definidos en la Etapa 2.

Alternativas: SimpleRisk, PILAR, ERAMBA, MONARC y Pirani Risk.

El proceso completo de aplicación del AHP se desarrolló utilizando la misma plantilla especializada empleada en la Fase I, la cual automatiza los cálculos matemáticos del método, incluyendo los vectores de prioridad, los índices de consistencia y la síntesis global. Las actividades desarrolladas incluyeron: (1) la construcción de matrices de comparación por pares entre los criterios definidos; (2) la valoración comparativa de las cinco herramientas respecto a cada criterio; (3) el cálculo automatizado de los vectores de prioridad; (4) la verificación de la Razón de Consistencia (CR ≤ 0.10); y (5) la síntesis global para obtener el ranking final de las alternativas evaluadas.

Dado que el análisis fue realizado por un solo investigador, no fue necesario emplear técnicas de agregación de juicios.

Productos de la fase:

- Matriz de preselección de herramientas OpenSource, elaborada a partir de la exploración sistemática de repositorios de software libre, plataformas de evaluación técnica y literatura especializada. Esta matriz permitió identificar y justificar la inclusión de las herramientas SimpleRisk, PILAR, ERAMBA, MONARC y Pirani Risk como alternativas viables para el contexto de PyMEs.
- Fichas técnicas de análisis funcional, una por cada herramienta evaluada, construidas a partir de la revisión de documentación oficial, análisis de requisitos técnicos y exploración de funcionalidades clave asociadas a la gestión de riesgos. Estas fichas sistematizaron la información necesaria para la evaluación comparativa posterior.
- Modelo jerárquico AHP para la selección de herramientas OpenSource, que incluye: a) matrices de comparación por pares entre los criterios funcionales definidos; b) matrices comparativas de las cinco herramientas respecto a cada criterio; c) cálculo automatizado de los vectores de prioridad y verificación de la Razón de Consistencia (CR ≤ 0.10); d) síntesis global para la obtención del ranking de las herramientas evaluadas.
- Archivo electrónico del modelo AHP, que consolida las matrices de comparación, los vectores de prioridad, los índices de consistencia y el ranking final de las herramientas analizadas, constituyéndose en un insumo técnico verificable del proceso metodológico.
- Selección de la herramienta OpenSource más adecuada, resultado del proceso de priorización multicriterio, la cual fue utilizada posteriormente como soporte tecnológico en la Fase III para el diseño y validación de la metodología propuesta.

2.4.3 Fase III: Uso del software OpenSource seleccionado para la gestión de riesgos en seguridad informática en pymes

Objetivo asociado: Usar el software OpenSource seleccionado para la gestión de riesgos en seguridad informática en pymes y que dé cumplimiento a la metodología propuesta.

Técnica principal: Instrumentación técnico-operativa controlada del software y verificación de correspondencia proceso-herramienta.

Descripción general de la Fase III:

La Fase III tuvo como propósito usar e instrumentar la herramienta OpenSource MONARC, seleccionada en la Fase II, para operacionalizar la metodología propuesta de análisis y gestión de riesgos de seguridad informática en pymes. En consecuencia, se buscó garantizar que el ciclo metodológico, con trazabilidad entre los requisitos normativos definidos en la Fase I fuera ejecutable y documentable dentro de la herramienta OpenSource. Asimismo, se procuró asegurar condiciones viables de adopción para su aplicación práctica en contextos organizacionales tipo pyme.

Para ello, se desarrolló una instrumentación técnico-operativa controlada del entorno y del análisis en MONARC. En particular, se configuraron parámetros mínimos necesarios para la ejecución del ciclo, relacionados con contexto, escalas de evaluación, umbrales de aceptación, estructura de activos y catálogos de tratamiento. De igual modo, se verificó sistemáticamente la correspondencia proceso–herramienta entre las etapas metodológicas definidas y los módulos funcionales disponibles en MONARC.

En coherencia con los principios del enfoque sociotécnico planteado en el apartado “1.1.5 Enfoque sociotécnico y uso de software OpenSource” del capítulo Marco Teórico, esta fase buscó alinear el proceso metodológico con la capacidad tecnológica disponible. Como resultado del procedimiento, se estructuraron productos operativos verificables asociados al uso del software, tales como, entorno reproducible, análisis base parametrizado, criterios configurados, modelo de activos, catálogos adaptados, workflow ejecutable y salidas documentales nativas. Dichos productos soportan y otorgan trazabilidad entre los requisitos normativos definidos en la Fase I y su instrumentación práctica.

Procedimiento:

El procedimiento se organizó en cinco etapas secuenciales. Estas etapas se alinearon tanto con el flujo operativo de la herramienta OpenSource como con el ciclo metodológico de gestión de riesgos propuesto:

- Etapa 0. Despliegue técnico y condiciones mínimas de entorno

Se habilitó un entorno controlado de ejecución para MONARC, utilizando una máquina virtual (VM) en VirtualBox como decisión de viabilidad para contexto pyme. En esta etapa se establecieron las condiciones mínimas de acceso, estabilidad y reproducibilidad del entorno de trabajo, incluyendo el registro de parámetros técnicos relevantes (versión del software, configuración base del entorno virtual y condiciones de acceso para su operación). Así mismo, se definió un punto de restauración (snapshot) que permitiera recuperar el estado inicial del entorno ante fallos o inconsistencias durante la instrumentación.

- Etapa 1. Creación del análisis base y parametrización inicial del contexto

Se creó un análisis en MONARC como unidad de trabajo. Allí se definieron los elementos básicos requeridos para instanciar el proceso metodológico dentro de la herramienta OpenSource. Se incluyó la parametrización inicial del contexto del análisis (alcance, idioma y condiciones generales), manteniendo consistencia terminológica y habilitación del flujo posterior. De forma complementaria, se identificaron los módulos y campos equivalentes en la herramienta OpenSource MONARC para representar los componentes del contexto metodológico definidos en la propuesta.

- Etapa 2. Configuración de criterios de evaluación del riesgo

Se parametrizaron los criterios mínimos de evaluación requeridos para permitir el cálculo y clasificación del riesgo en MONARC, incluyendo para los riesgos de la información escalas de impacto bajo las dimensiones C–I–D (Confidencialidad-Integridad-Disponibilidad), asociado a consecuencias de impacto (Reputacional, Operacional, Legal, Financiero, Personal), escalas de probabilidad y vulnerabilidad, además, se configuraron los umbrales de aceptación del riesgo que permiten clasificar la exposición y orientar el tratamiento dentro del flujo de la herramienta OpenSource MONARC. Esta etapa aseguró la coherencia entre los criterios metodológicos definidos para la investigación y su implementación paramétrica en la herramienta MONARC, de modo que el análisis posterior se ejecutara sobre una base consistente y controlada.

- Etapa 3. Modelado jerárquico de activos, dependencias y catálogos de análisis

Se implementó la estructura mínima de modelado requerida por MONARC para soportar el análisis de riesgos, incorporando activos primarios y secundarios, relación de dependencias necesarias para habilitar la herencia de impactos. En paralelo, se parametrizaron catálogos funcionales de amenazas, vulnerabilidades adaptadas al contexto pyme. De igual manera, se gestiónó en MONARC la creación y estructuración de los Conjuntos de recomendaciones en la Base de Conocimiento, asegurando que cada medida de mitigación estuviera vinculada a un contenedor lógico obligatorio para habilitar su reutilización sistemática.

Para cada recomendación, se definieron identificadores únicos (códigos), niveles de importancia fijos para priorizar la ejecución y descripciones detalladas de las táreas de control. También, cuando fue aplicable, se consolidó la posibilidad de reutilización mediante exportables disponibles (plantillas o blueprints) y la vinculación de medidas preexistentes mediante el mecanismo de enlace (icono de cadena), orientados a facilitar la replicabilidad técnica y la consistencia en el tratamiento de riesgos.

- Etapa 4. Verificación del flujo completo, tratamiento, seguimiento y salidas documentales

Se verificó la operatividad del flujo total del análisis en MONARC, recorriendo las etapas del ciclo desde contexto y modelado hasta evaluación, tratamiento e implementación/seguimiento, confirmando que los elementos configurados permitieran ejecutar el proceso de extremo a extremo. Finalmente, se verificó la capacidad de generar salidas documentales y exportables del sistema (reportes y formatos de intercambio), con el propósito de asegurar trazabilidad y soporte documental para la fase de validación posterior.

Como resultado del procedimiento desarrollado, se establecieron los siguientes productos verificables asociados al cumplimiento del OE3.

Productos de la fase:

- Entorno técnico operativo reproducible de MONARC en máquina virtual de VirtualBox, con parámetros mínimos de configuración documentados y condiciones de acceso definidas para su uso controlado en contexto pyme.

- Análisis base creado y parametrizado en MONARC, incluyendo configuración inicial del contexto como unidad de instrumentación del método.
- Escalas y criterios de evaluación configurados, incluyendo dimensiones C–I–D, probabilidad, vulnerabilidad y umbrales de aceptación del riesgo, alineados con la lógica metodológica propuesta.
- Modelo jerárquico de activos implementado, con activos primarios y secundarios, dependencias y herencia de impactos, como base estructural para la evaluación del riesgo en la herramienta.
- Catálogos funcionales adaptados al contexto pyme, correspondientes a amenazas, vulnerabilidades, referenciales y conjunto de recomendaciones, incluyendo estructuras de importación/exportación cuando aplique.
- Flujo completo de análisis ejecutable en MONARC (Etapas 0–4), documentado como workflow operable y consistente con el ciclo metodológico propuesto.
- Salidas documentales y exportables del sistema habilitadas, tales como reportes y formatos de intercambio (exportaciones en formatos soportados por la herramienta), como soporte de trazabilidad y auditabilidad para la aplicación posterior.

Remisión a anexos (detalle ampliado): El soporte técnico-metodológico de instrumentación, reglas mínimas de consistencia, restricciones identificadas y correspondencia proceso–herramienta se presenta en el **Anexo G**. Las evidencias técnicas y artefactos reproducibles asociados a los productos de esta fase (parámetros de entorno, capturas mínimas, exportaciones y catálogos) se consolidan en el **Anexo H**.

2.4.4 Fase IV: Validación de la metodología propuesta a través de su aplicación con un caso de estudio o prueba de escritorio en una pyme

Objetivo asociado: Validar la metodología propuesta a través de su aplicación con un caso de estudio o prueba de escritorio en una pyme.

Técnica principal: Validación por medio de una prueba de escritorio (estudio de caso instrumental simulado), empleando como unidad de análisis una pyme ficticia, denominada “PyME Servicios Colombia”, construida a partir de información y necesidades realistas contenidas en el Instrumento de Recolección de Datos del cliente.

La técnica se soportó en cuatro pilares:

- **Construcción del escenario simulado a partir de evidencia documental:** la información del instrumento permitió representar un contexto organizacional típico (procesos, dependencia tecnológica, necesidades de información, riesgos plausibles), cuidando la confidencialidad y evitando referencias identificables.
- **Duplicación (clonación) del análisis base del OE3:** se utilizó la funcionalidad nativa de la herramienta para duplicar el análisis desarrollado en la Fase III, heredando la parametrización (escalas, umbrales, catálogos, estructura jerárquica y recomendaciones) y enfocando el esfuerzo en la validación del caso simulado.
- **Aplicación controlada del flujo completo:** se ejecutaron secuencialmente las etapas del ciclo (contexto → activos → evaluación → tratamiento → seguimiento/documentación) sobre el análisis clonado, ajustando la narrativa y la parametrización puntual necesaria para reflejar el escenario simulado.
- **Análisis documental y técnico de evidencias:** se consolidaron salidas del sistema (reportes y exportaciones) y evidencias complementarias (capturas y matrices), para evaluar aplicabilidad, completitud y efectividad.

Se analizó y precisó la información en el caso simulado, se consideró realista porque las necesidades, activos, amenazas, vulnerabilidades, controles y recomendaciones se derivaron de un insumo empírico de apoyo y de catálogos previamente contextualizados, sin comprometer información reservada.

Descripción general de la Fase IV:

La Fase IV validó la metodología propuesta mediante su aplicación en una PyME simulada, construida como prueba de escritorio a partir del instrumento del cliente, con el fin de alcanzar cuatro propósitos verificables:

- Confirmar la ejecutabilidad del ciclo metodológico en condiciones representativas de pymes del sector servicios, verificando que las etapas definidas en la metodología fueran replicables y consistentes dentro de la herramienta OpenSource MONARC.

- Verificar la suficiencia de los productos generados para apoyar decisiones gerenciales, examinando si el proceso producía una matriz priorizada, un plan de tratamiento con responsables y plazos, y evidencia de seguimiento/documentación.
- Evaluar el desempeño metodológico identificando fortalezas, limitaciones y ajustes sugeridos, especialmente en términos de adopción por pymes con recursos limitados y madurez variable.
- Consolidar evidencia documental de validación como soporte del OE4, mediante productos reproducibles y trazables generados a partir de la ejecución del flujo completo.

Procedimiento:

La fase se ejecutó siguiendo cuatro etapas secuenciales, asegurando trazabilidad entre actividades, evidencias y productos.

- Etapa 1. Selección y preparación del caso de estudio o prueba de escritorio

En lugar de seleccionar una PyME real, se definió y preparó un escenario simulado ("PyME Servicios Colombia") a partir del Instrumento de Recolección de Datos del cliente, el cual aportó insumos para:

- **Caracterización organizacional simulada:** tipo de operación, dependencia de la información, procesos y necesidades típicas.
- **Contexto y alcance:** delimitación de procesos críticos y activos en alcance, con exclusiones explícitas cuando aplicó.
- **Supuestos y restricciones:** se establecieron supuestos controlados para completar información no disponible, manteniendo realismo y consistencia.
- **Criterios de confidencialidad:** se evitó incorporar nombres, cifras exactas o elementos que permitieran identificar al cliente o su operación.

Resultado Operacional: el caso quedó formalmente definido como prueba de escritorio realista, con un documento de preparación (perfil simulado, alcance, supuestos y restricciones) usado como entrada de aplicación.

- Etapa 2. Aplicación de la metodología propuesta en el caso simulado

La metodología se aplicó utilizando como base el análisis duplicado desde OE3, debido a que la Fase III ya había instrumentado los componentes estructurales. Por tanto, la clonación constituyó el mecanismo central para asegurar consistencia metodológica y acelerar la ejecución.

Actividades ejecutadas:

- **Duplicación y contextualización del análisis:** se duplicó el análisis base y se actualizó el contexto para reflejar el caso simulado.
- **Contexto:** se ajustó el alcance y la descripción del escenario de acuerdo con el instrumento, manteniendo escalas y umbrales.
- **Activos y dependencias:** se instanciaron activos coherentes con el escenario y se verificó herencia de impactos.
- **Escenarios:** se vincularon amenazas y vulnerabilidades realistas (derivadas del instrumento y catálogos contextualizados).
- **Evaluación:** se asignaron probabilidades e impactos acordes al escenario; el sistema calculó y clasificó riesgos.
- **Tratamiento:** se seleccionaron estrategias y se vincularon recomendaciones; se asignaron responsables y plazos; se recalculó riesgo residual.
- **Seguimiento/documentación:** se verificó la capacidad del sistema para gestionar el plan y producir salidas exportables.

Resultado Operacional: se obtuvo un análisis completo del caso simulado con matriz priorizada, plan de tratamiento y evidencia documental reproducible.

- Etapa 3. Documentación y presentación de resultados

Se consolidaron productos nativos del sistema y productos complementarios de análisis, asegurando evidencia verificable del cumplimiento del OE4. La evidencia incluyó reportes, exportaciones y capturas organizadas por etapas del flujo.

Productos de la fase:

- **Caso simulado preparado (prueba de escritorio):** documento de definición del escenario "PyME Servicios Colombia", construido a partir del instrumento del cliente, con perfil, alcance, supuestos y restricciones, cuidando confidencialidad.
- **Análisis de riesgos ejecutado para OE4:** análisis clonado del OE3 y contextualizado al caso simulado, con activos, escenarios, evaluación, tratamiento, riesgo residual y trazabilidad.
- **Productos documentales y de trazabilidad:** reportes generados por el sistema, exportaciones estructuradas y registro de evidencias (capturas y matrices consolidadas).

Transición OE3 → OE4: Los resultados de la instrumentación obtenida en la Fase III se utilizaron como insumo directo de validación en la Fase IV mediante duplicación del análisis base. Este método permitió mantener el análisis del OE3 como "modelo de referencia" y utilizar el análisis clonado como instancia aplicada para la prueba de escritorio, reutilizando evidencias y capturas, pero con narrativa orientada a validación.

Una vez descritas las cuatro fases metodológicas y sus productos asociados, la Tabla 2.4.4-1 presenta la trazabilidad entre los objetivos específicos, las fases metodológicas, los productos derivados y las evidencias documentales que permiten verificar su desarrollo en los capítulos de resultados y anexos.

Tabla 2.4.4-1: Matriz de trazabilidad entre objetivos específicos, fases metodológicas, productos derivados y evidencias documentales

OE / Fase	Técnica principal	Productos derivados	Evidencia documental / ubicación exacta
OE1 / Fase I. Caracterización de referentes internacionales para la gestión de riesgos	Análisis documental comparativo y evaluación multicriterio mediante AHP.	(a) Caracterización comparativa de referentes internacionales; (b) criterios de adaptabilidad al contexto pyme; (c) modelo jerárquico AHP y ranking del referente más adecuado; (d) síntesis integradora de principios, directrices y requisitos aplicables.	Sección 3.1. Tabla 3.1.1-1: síntesis comparativa de referentes. Tabla 3.1.2-1: criterios de adaptabilidad. Figura 3.1.3-1: estructura AHP. Tablas 3.1.3-1 a 3.1.3-6: pesos globales, priorización por criterio y ranking. Tabla 3.1.3-7: análisis de sensibilidad. Tablas 3.1.4-1, 3.1.4-2 y 3.1.4-3: síntesis integradora de principios, flujo metodológico y requisitos mínimos. Anexo C: matrices de comparación pareada, vectores de prioridad y síntesis jerárquica del modelo AHP.
OE2 / Fase II. Análisis y selección de herramientas y soluciones de software para la gestión de riesgos	Análisis técnico-funcional y evaluación multicriterio mediante AHP.	(a) Caracterización técnico-funcional de herramientas candidatas; (b) criterios evaluativos para el AHP; (c) modelo jerárquico AHP y ranking de herramientas; (d) selección del software base para la metodología, MONARC.	Sección 3.2. Tabla 3.2.1-1: síntesis comparativa técnico-funcional de herramientas. Tabla 3.2.2-1: criterios evaluativos. Figura 3.2.3-1: estructura AHP. Tablas 3.2.3-1 a 3.2.3-5: pesos globales y priorización por criterio. Tabla 3.2.3-6: ranking global. Anexo D: matriz de preselección. Anexo E: fichas técnicas de análisis funcional. Anexo F: matrices AHP, vectores de prioridad y verificación de consistencia.
OE3 / Fase III. Uso e instrumentación del software seleccionado	Instrumentación técnico-operativa controlada y verificación de correspondencia proceso-herramienta.	Entorno técnico reproducible; análisis base parametrizado; escalas y umbrales de evaluación configurados; modelo jerárquico de activos y dependencias; catálogos funcionales adaptados; flujo completo ejecutable; reportes y exportables del sistema.	Sección 3.3. Tabla 3.3.1-1: checklist de verificación del entorno. Tabla 3.3.2-1: mapeo componentes metodológicos–módulos MONARC. Figuras 3.3.1-1 a 3.3.5-8: configuración, activos, catálogos, tratamiento, seguimiento y reportes. Tabla 3.3.5-1: matriz consolidada de tratamiento antes/después. Anexo G: soporte técnico-metodológico de instrumentación. Anexo H: evidencias técnicas, capturas, exportaciones, checklists diligenciados y catálogos.
OE4 / Fase IV. Validación de la metodología propuesta	Prueba de escritorio mediante caso de estudio instrumental simulado, "PyME Servicios Colombia".	Caso simulado preparado; análisis de riesgos ejecutado; matriz de riesgos priorizada; plan de tratamiento con responsables, plazos y presupuestos; evidencias de trazabilidad y auditabilidad; reportes y exportaciones para validar aplicabilidad, completitud y coherencia.	Sección 3.4. Figuras 3.4.2-1 a 3.4.2-8: clonación del análisis, modelado, evaluación, tratamiento e implementación del plan. Figura 3.4.3-1: índice del documento consolidado generado por MONARC. Anexo I: soporte documental completo de la validación, incluyendo evaluación íntegra, matrices de riesgo, mapa de riesgo y plan de tratamiento del caso simulado.

Fuente: Elaboración propia a partir de la estructura metodológica definida en el apartado 2.4 Fases metodológicas y de los productos documentados en los capítulos de resultados y anexos.

3. Resultados

Este capítulo reúne los resultados obtenidos en las cuatro fases metodológicas desarrolladas para cumplir los objetivos específicos de la investigación. Abarca la caracterización de los referentes internacionales para la gestión de riesgos y la selección del referente base mediante AHP, incluye comparación documental, criterios de adaptabilidad, priorización multicriterio y la síntesis integradora que sustenta la metodología propuesta. Avanza mostrando los resultados del análisis técnico-funcional de herramientas de software y su priorización mediante AHP, proceso que condujo a la selección de MONARC como soporte tecnológico. El desarrollo continúa con la instrumentación técnico-operativa de MONARC, evidencia la configuración del entorno, el análisis base, las escalas, los activos, los catálogos, el tratamiento de riesgos y las salidas documentales generadas. Cierra exponiendo la validación de la metodología a través de una prueba de escritorio aplicada al caso simulado “PyME Servicios Colombia”, orientada a verificar la ejecutabilidad, trazabilidad, completitud y coherencia de la propuesta metodológica.

3.1 Resultados de la Fase I - OE1: Caracterización de referentes internacionales

En la Fase I se consolidaron cuatro productos metodológicos derivados de la triangulación entre (i) la revisión del Estado del Arte (literatura científica indexada y casos de estudio documentados) y (ii) la revisión de fuentes primarias oficiales de ISO/IEC 27005:2022, NIST SP 800-30 Rev. 1, MAGERIT v3.0, OCTAVE-S v1.0 y EBIOS Risk Manager (2018). Los productos se organizaron como: (a) caracterización comparativa homogénea de los referentes de gestión de riesgos, (b) criterios de adaptabilidad para pymes, (c) modelo AHP con consenso deliberativo del panel de expertos y verificación de consistencia, y (d) síntesis integradora de principios, directrices y requisitos aplicables al contexto pyme, utilizada para el diseño de la metodología propuesta.

3.1.1 Producto (a): Caracterización comparativa homogénea de los referentes internacionales para la gestión de riesgos

Se elaboró una caracterización comparativa bajo un esquema uniforme que contempló el enfoque conceptual predominante, la secuencia metodológica, los requisitos de recursos, el nivel de prescripción normativa y los rasgos de adaptabilidad al contexto pyme. La Tabla 3.1.1-1 sintetiza

comparativamente los cinco referentes internacionales para la gestión de riesgos analizados en la Fase I (OE1) en términos de enfoque, secuencia metodológica, requisitos, prescripción/flexibilidad y rasgos relevantes para pymes.

Tabla 3.1.1-1: Síntesis comparativa de referentes internacionales para la gestión de riesgos analizados (Fase I – OE1 – Producto a)

Marco	Principios / enfoque predominante	Secuencia metodológica (síntesis)	Requisitos/recursos (síntesis)	Prescripción / flexibilidad (síntesis)	Rasgo relevante para PyME (síntesis)
ISO/IEC 27005:2022	Ciclo iterativo y continuo de gestión de riesgos de seguridad de la información, orientado al riesgo y basado en un proceso flexible que busca evaluaciones consistentes y comparables, alineadas con los objetivos organizacionales	Establecimiento del contexto → Apreciación del riesgo (identificación → análisis → evaluación) → Tratamiento del riesgo → Comunicación y consulta / Seguimiento y revisión	Requiere definición de contexto, criterios de riesgo y de aceptación, y registro/documentación del proceso de valoración y tratamiento. No prescribe herramientas específicas; puede integrarse con un SGSI (p. ej., ISO/IEC 27001) cuando aplica	**Muy flexible.** Proporciona directrices generales sin prescribir un método único; permite enfoques cualitativos, cuantitativos o semicuantitativos, y alta adaptabilidad a distintos contextos	Alinea el proceso de gestión de riesgos con el enfoque de la familia ISO/IEC 27000; es integrable con esquemas formales de SGSI y aplicable a organizaciones de distinto tamaño mediante ajuste del método y la profundidad
NIST SP 800-30 Rev. 1	Marco de evaluación estructurado basado en factores de riesgo para identificar, estimar y priorizar riesgos mediante el análisis de amenazas, vulnerabilidades, impacto y probabilidad, con el propósito de informar la toma de decisiones y respaldar respuestas al riesgo	Preparación → Conducción de la evaluación (identificación de fuentes/eventos de amenaza → identificación de vulnerabilidades → determinación de probabilidad e impacto → determinación del riesgo) → Comunicación de resultados → Mantenimiento	Requiere reporte/documentación formal de la evaluación de riesgos y trazabilidad de supuestos, fuentes de amenaza, vulnerabilidades, impacto y probabilidad. No prescribe herramientas obligatorias y demanda capacidades técnicas para sostener la consistencia del análisis	**Estructurado.** Permite métodos cualitativos, cuantitativos o semicuantitativos, pero presenta alto nivel de detalle analítico y requiere capacidad técnica para aplicar el modelo con consistencia	Aporta trazabilidad analítica para la evaluación del riesgo y soporte a decisiones; su aplicación requiere capacidad técnica y disciplina documental para mantener comparabilidad entre evaluaciones
MAGERIT v3.0	Método sistemático orientado al activo para análisis y gestión de riesgos, con	Método de análisis (activos → amenazas → salvaguardas → estimación de impacto/riesgo) → Proceso de gestión	Demanda participación de dirección y un equipo de trabajo con roles definidos. Requiere documentación formal del inventario/valoración	**Estructurado / prescriptivo.** Proceso metódico con pasos definidos; admite ajuste de alcance y	Ofrece una visión exhaustiva del riesgo con fuerte énfasis en activos y

Marco	Principios / enfoque predominante	Secuencia metodológica (síntesis)	Requisitos/recursos (síntesis)	Prescripción / flexibilidad (síntesis)	Rasgo relevante para PyME (síntesis)
	énfasis en la valoración de activos, dependencias, amenazas, salvaguardas e impactos, buscando formalizar el conocimiento del riesgo y apoyar decisiones de tratamiento	(evaluación → decisión de tratamiento) → Plan de seguridad (identificación de proyectos → ejecución)	de activos, mapa de riesgos, salvaguardas y plan de seguridad/tratamiento. Puede apoyarse en herramientas de soporte (p. ej., PILAR)	profundidad, pero mantiene alta exigencia de modelado y documentación	dependencias; su aplicación demanda mayor esfuerzo de documentación y modelado, relevante cuando se dispone de capacidad técnica y organizacional suficiente
OCTAVE-S v1.0	Enfoque autodirigido, simplificado y centrado en activos, diseñado para organizaciones pequeñas (≤100 personas), orientado al riesgo Operacional y a prácticas de seguridad con mínima dependencia de evaluaciones tecnológicas complejas	Fase 1: construir perfiles de amenazas basados en activos → Fase 2: identificar vulnerabilidades de la infraestructura (caminos de acceso y procesos tecnológicos) → Fase 3: desarrollar estrategias y planes de seguridad (identificar/analizar riesgos, estrategia de protección y planes de mitigación)	Requiere un equipo interno reducido e interdisciplinario (típicamente 3–5 personas) con conocimiento del negocio y de los activos críticos. Utiliza cuestionarios y worksheets para estandarizar el análisis y producir una estrategia de protección; no exige herramientas sofisticadas y está concebida para aplicación en periodos cortos y reevaluación periódica	**Estructurado.** La estructura por worksheets guía el proceso y estandariza la aplicación; la adaptación requiere parametrización de activos, amenazas y prácticas internas. Predomina evaluación cualitativa (alto/medio/bajo)	Se diseñó explícitamente para organizaciones pequeñas y recursos limitados, priorizando participación del personal interno y enfoque operativo sobre riesgos clave del negocio
EBIOS RM (2018)	Método de evaluación y tratamiento de riesgos digitales con enfoque dual (cumplimiento y escenarios), que prioriza amenazas intencionales mediante un proceso iterativo en cinco talleres para vincular misiones de alto nivel con escenarios operacionales	Workshop 1: alcance y línea base → Workshop 2: orígenes del riesgo → Workshop 3: escenarios estratégicos → Workshop 4: escenarios operacionales → Workshop 5: tratamiento del riesgo (estrategia de tratamiento y plan de mejora continua)	Requiere coordinación de actores decisores y operacionales para ejecutar talleres estructurados y consolidar entregables (línea base, escenarios, plan de mejora continua). Incluye herramientas de apoyo (toolbox) y guías de aplicación. Su aplicación puede requerir facilitación y capacidades especializadas en análisis de escenarios y amenazas	**Flexible / estructurado.** "Geometría variable" para ajustar el nivel de detalle al objetivo del estudio; enfoque modular e iterativo con alta personalización, combinando cumplimiento y análisis por escenarios	Aporta estructuración por escenarios y actores del ecosistema, útil para amenazas modernas; su aplicación se adapta por profundidad, pero exige coordinación y capacidades para construir y validar escenarios

Fuente: Elaboración propia a partir de ISO/IEC 27005:2022, NIST SP 800-30 Rev. 1, MAGERIT v3.0, OCTAVE-S v1.0 y EBIOS Risk Manager.

La Tabla 3.1.1-1 consolidó, bajo un formato homogéneo, los elementos comparables identificados en los cinco referentes internacionales analizados para la gestión de riesgos, integrados por estándares, guías y metodologías. Esta caracterización constituyó el insumo documental para (i) la definición de criterios de adaptabilidad al contexto pyme (Etapa 2) y (ii) la estructuración del modelo AHP y su síntesis global (Etapa 3).

3.1.2 Producto (b): Criterios de adaptabilidad para pymes

A partir de la matriz de Operacionalización de variables (Anexo B) y de la triangulación con los hallazgos del Estado del Arte sobre restricciones problemáticas típicas de pymes, se definieron cuatro criterios cualitativos de adaptabilidad para evaluar los marcos normativos analizados. Esos criterios operacionalizaron, en términos comparables, los elementos considerados relevantes para la selección de un marco base aplicable al contexto pyme. Además, sirvieron como insumo directo para la construcción del modelo AHP de la Etapa 3.

La derivación de esos criterios se realizó mediante una síntesis conceptual que agrupó dimensiones evaluativas recurrentes en la literatura y en la matriz de Operacionalización, con el propósito de convertir las restricciones operativas de pymes en atributos comparables entre marcos internacionalmente referentes de seguridad informática para la gestión de riesgos.

Los criterios definidos en la Tabla 3.1.2-1 permitieron disponer de un marco evaluativo homogéneo para valorar la adaptabilidad de los referentes internacionales al contexto pyme en la Etapa 2, y se constituyeron posteriormente en la base para la estructuración del modelo jerárquico AHP y el cálculo de prioridades en la Etapa 3.

Tabla 3.1.2-1: Criterios de adaptabilidad definidos para evaluar referentes internacionales aplicables a la gestión de riesgos en pymes (Fase I – OE1 – Producto b)

Criterio	Definición operativa	Evidencia/indicadores de análisis (síntesis)	Relación con restricciones típicas pyme (síntesis)
Practicidad y simplicidad	Grado en que el marco puede aplicarse con pasos claros, carga documental acotada y resultados comprensibles para equipos no especializados.	Claridad de fases y actividades; uso de plantillas/guías; complejidad del proceso; nivel de formalidad requerido para producir resultados.	Prioriza implementación con recursos limitados y baja madurez, reduciendo fricción metodológica y dependencia de experticia avanzada.

Criterio	Definición operativa	Evidencia/indicadores de análisis (síntesis)	Relación con restricciones típicas pyme (síntesis)
Consideraciones técnico-administrativas	Nivel de requerimientos organizacionales y de gestión para ejecutar el marco (roles, responsabilidades, gobernanza, coordinación y recursos mínimos).	Necesidad de roles formales; participación de dirección; coordinación de actores; requisitos de gestión y administración del proceso.	Reconoce limitaciones de estructura, tiempo y capacidad de coordinación interna en pymes.
Recomendaciones para el tratamiento del riesgo	Capacidad del marco para orientar la selección y priorización de opciones de tratamiento, manteniendo trazabilidad entre riesgo y decisión.	Orientación explícita a tratamiento; priorización; criterios de aceptación; claridad en alternativas (mitigar, transferir, aceptar, evitar); trazabilidad decisión–riesgo.	Apoya la toma de decisiones con baja capacidad de análisis especializado y necesidad de actuar sobre riesgos críticos.
Directrices para implementación de controles	Grado de orientación que provee el marco para traducir decisiones de tratamiento en controles o medidas operativas implementables.	Relación con medidas/controles; guía para implementación; conexión con prácticas o catálogos; nivel de concreción para ejecución.	Facilita pasar de análisis a acción en contextos donde la ejecución suele ser reactiva o fragmentada.

Fuente: Elaboración propia a partir de la caracterización documental de estándares, guías y metodologías internacionales aplicables a la gestión de riesgos de seguridad informática en pymes.

En otras palabras, los criterios que se decidieron valorar son:

- Practicidad y Simplicidad

Se refiere a que la metodología pueda ser comprendida y aplicada de manera efectiva por el personal de las MiPymes, independientemente de su nivel técnico en seguridad informática. Además, se refiere a la implementación de manera efectiva sin comprometer operaciones.

- Consideraciones Técnicas y Administrativas

Se refiere a que la metodología proporcione entre directrices claras para implementar un balance óptimo de medidas técnicas y prácticas administrativas. También se refiere a garantizar un enfoque integral para la implementación.

- Recomendaciones para el Tratamiento de Riesgos

Se refiere a la capacidad de ofrecer recomendaciones para el tratamiento de riesgos en seguridad informática, abordando identificación, evaluación y mitigación, pudiéndose adaptar al contexto de la MiPyme.

- Directrices para la Implementación de Controles

Se refiere a que la metodología pueda proporcionar recomendaciones para implementar controles de seguridad o que en este aspecto haga referencia hacia otras guías, estándares y metodologías internacionales para la gestión de riesgos.

3.1.3 Producto (c): Modelo jerárquico AHP y priorización de referentes internacionales para la gestión de riesgos

El tercer producto consistió en la estructuración y ejecución matemática del modelo de decisión multicriterio basado en el método AHP. Este modelo integró los insumos de los productos anteriores: los referentes internacionales para la gestión de riesgos (Producto a) actuaron como alternativas en el Nivel 3, y los factores de adaptabilidad (Producto b) operaron como criterios de decisión en el Nivel 2.

Este procedimiento permitió cuantificar matemáticamente la idoneidad de cada estándar, obteniendo vectores de prioridad locales y globales que fundamentaron la selección objetiva del referente internacional base para la propuesta metodológica de gestión de riesgos de seguridad informática.

- Estructura jerárquica del modelo AHP

El modelo AHP se estructuró en tres niveles jerárquicos, como se muestra en la Figura 3.1.3-1:

3.1.3.1.1 Nivel 1 (Objetivo)

Determinar el referente internacional más adecuado para sustentar una metodología de gestión de riesgos de seguridad informática dirigida a pymes del sector servicios en Colombia.

3.1.3.1.2 Nivel 2 (Criterios)

Los cuatro criterios de adaptabilidad definidos en el Producto (b) son:

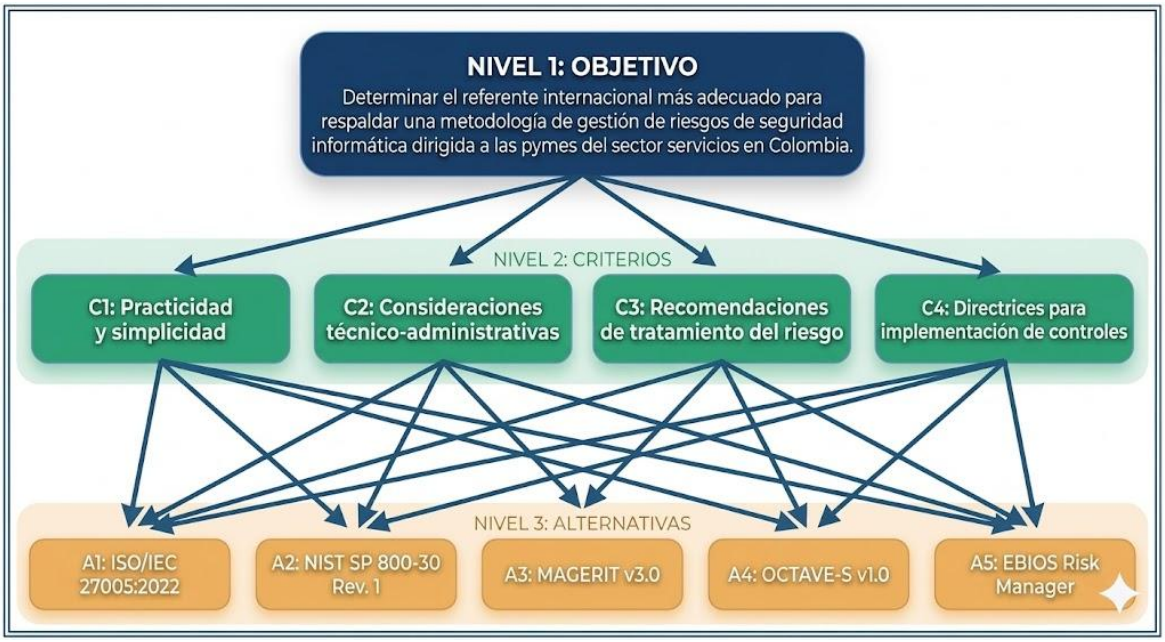
- C1: Practicidad y simplicidad
- C2: Consideraciones técnico-administrativas
- C3: Recomendaciones de tratamiento del riesgo
- C4: Directrices para implementación de controles

3.1.3.1.3 Nivel 3 (Alternativas)

Los cinco referentes para la gestión de riesgos de seguridad informática caracterizados en el Producto (a) son:

- A1: ISO/IEC 27005:2022
- A2: NIST SP 800-30 Rev. 1
- A3: MAGERIT v3.0
- A4: OCTAVE-S v1.0
- A5: EBIOS Risk Manager

Figura 3.1.3-1: Estructura jerárquica del modelo de decisión AHP para la selección del referente internacional orientado a la gestión de riesgos de seguridad informática



Fuente: Elaboración propia a partir de los criterios de adaptabilidad definidos en la Fase I y de la caracterización documental de estándares, guías y metodologías internacionales aplicables a la gestión de riesgos de seguridad informática. La representación gráfica fue apoyada mediante herramienta de inteligencia artificial generativa [227].

- Comparación por pares entre criterios

Tras aplicar la metodología AHP, se obtuvieron los vectores propios que representan la importancia relativa de cada criterio. En la

Tabla 3.1.3-1 se muestra que el criterio "Practicidad y simplicidad" obtuvo el mayor peso relativo

Criterio	Peso global (vector promedio)	CR (n=4)
C1: Practicidad y Simplicidad	0.57	0.1160 ✗
C2: Consideraciones Técnicas y Administrativas	0.24	
C3: Recomendaciones para el Tratamiento de Riesgos	0.13	
C4: Directrices para la Implementación de Controles	0.06	
$\lambda_{max} = 4.3131\ CI = 0.1044\ RI = 0.90$		

(57%), reflejando el consenso del panel sobre la prioridad de minimizar barreras de adopción en organizaciones con recursos limitados. Le siguieron "Consideraciones técnico-administrativas" (24%), "Recomendaciones de tratamiento del riesgo" (13%) y "Directrices para implementación de controles" (6%). Esta distribución de pesos es coherente con las restricciones operativas identificadas en el Estado del Arte para pymes del sector servicios (apartado 1.2.2).

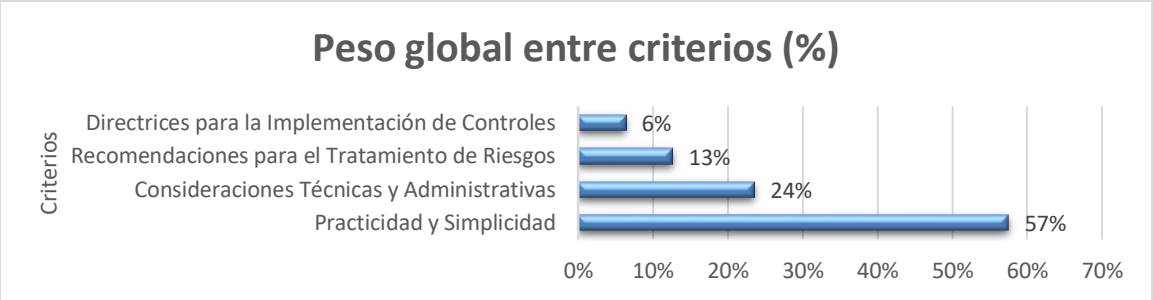
Tabla 3.1.3-1: Pesos globales de criterios AHP (Fase I)

Criterio	Peso global (vector promedio)	CR (n=4)
C1: Practicidad y Simplicidad	0.57	0.1160 ✗
C2: Consideraciones Técnicas y Administrativas	0.24	
C3: Recomendaciones para el Tratamiento de Riesgos	0.13	
C4: Directrices para la Implementación de Controles	0.06	
$\lambda_{max} = 4.3131\ CI = 0.1044\ RI = 0.90$		

Fuente: Elaboración propia a partir del Anexo C.

Cabe destacar que, para la matriz de comparación por pares entre criterios, el modelo AHP presentó un Índice de Consistencia (CI) y una Razón de Consistencia (CR) dentro de los rangos recomendados, lo cual es menor a 0.10, validando la coherencia de los juicios emitidos y cumpliendo el criterio de aceptación propuesto por Saaty. El detalle completo de la matriz de comparación pareada y los cálculos de normalización se encuentran disponibles en el **Anexo C**. Una representación gráfica se presenta en la Figura 3.1.3-2.

Figura 3.1.3-2: Distribución de los pesos globales de los criterios de adaptabilidad (Modelo AHP - Fase I)



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

- Comparación por pares de alternativas respecto a cada criterio

Para cada uno de los cuatro criterios, el panel de expertos comparó las cinco alternativas normativas por pares. A continuación, se presentan las matrices de comparación consensuadas y los vectores de prioridad resultantes.

C1: Practicidad y simplicidad

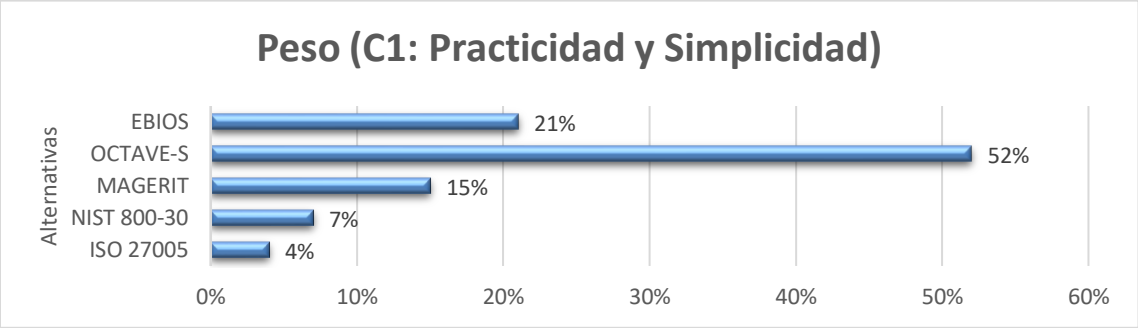
Se contrastaron las cinco alternativas mediante juicios expertos, priorizando aquellos referentes internacionales que requieren menor curva de aprendizaje y carga documental. Los cálculos detallados de la matriz de comparación pareada y su consistencia se encuentran detallados en el Anexo C. La Tabla 3.1.3-2: Priorización de alternativas respecto al criterio C1: Practicidad y Simplicidad resume los vectores de prioridad resultantes, evidenciando una clara preferencia hacia referentes de aplicación más ágil. Una representación gráfica se presenta en la Figura 3.1.3-3: Ponderación de alternativas vs C1: Practicidad y Simplicidad.

Tabla 3.1.3-2: Priorización de alternativas respecto al criterio C1: Practicidad y Simplicidad

Alternativa (referente internacional)	Vector de prioridad (peso local)	CR (n=5)
ISO/IEC 27005	0.04	
NIST SP 800-30	0.07	0.1283
MAGERIT	0.15	✗
OCTAVE-S	0.52	
EBIOS	0.21	
$\lambda_{max} = 5.5748 \;\; CI = 0.1437 \;\; RI = 1.12$		

Fuente: Elaboración propia a partir a partir de los cálculos de comparación pareada documentados en el Anexo C.

Figura 3.1.3-3: Ponderación de alternativas vs C1: Practicidad y Simplicidad



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

Los datos de la Tabla 3.1.3-2 muestran que OCTAVE-S v1.0 alcanzó un vector de prioridad de 0.52, cifra que supera a la segunda alternativa, EBIOS Risk Manager (0.21), por una diferencia de 0.31 puntos. MAGERIT v3.0 ocupó la tercera posición con 0.15. En contraste, NIST SP 800-30 Rev. 1 y ISO/IEC 27005:2022 obtuvieron valores de 0.07 y 0.04 respectivamente, acumulando entre ambas el 11% del peso total en este criterio.

C2: Consideraciones Técnicas y Administrativas

En lo referente al criterio C2: Consideraciones Técnicas y Administrativas, el panel de expertos evaluó el equilibrio entre la rigurosidad técnica necesaria y la carga burocrática o de recursos que cada marco exige para su mantenimiento. Los cálculos detallados de la matriz de comparación pareada, junto con su análisis de consistencia, se encuentran disponibles en el Anexo C.

La Tabla 3.1.3-3: Priorización de alternativas respecto al criterio C2: Consideraciones Técnicas y Administrativas resume los vectores de prioridad resultantes, mostrando un cambio en la preferencia hacia referentes internacionales con mayor estructura técnica formal. Una representación gráfica se presenta en la Figura 3.1.3-4: Ponderación de alternativas vs C2: Consideraciones Técnicas y Administrativas.

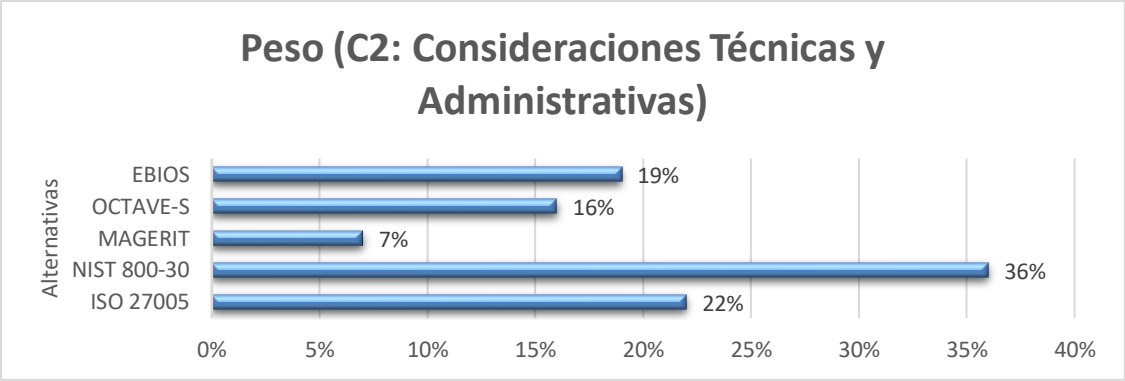
Tabla 3.1.3-3: Priorización de alternativas respecto al criterio C2: Consideraciones Técnicas y Administrativas

Alternativa (referente internacional)	Vector de prioridad (peso local)	CR (n=5)
ISO 27005	0.22	0.1695 ✗
NIST 800-30	0.36	
MAGERIT	0.07	

OCTAVE-S	0.16
EBIOS	0.19
$\lambda_{max} = 5.7596 \ CI = 0.1899 \ RI = 1.12$	

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo C.

Figura 3.1.3-4: Ponderación de alternativas vs C2: Consideraciones Técnicas y Administrativas



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

Bajo este criterio, se aprecia en la Tabla 3.1.3-3 que la distribución de pesos favoreció a NIST SP 800-30 Rev. 1, la cual obtuvo la valoración más alta con un vector de 0.36. Le sigue ISO/IEC 27005 con 0.22 y EBIOS Risk Manager con 0.19. Al comparar estos resultados con los del criterio anterior (C1), se observa un cambio en el ordenamiento de las alternativas. OCTAVE-S v1.0 descendió a la cuarta posición (0.16) y MAGERIT v3.0 registró el valor menor del grupo (0.07).

C3: Recomendaciones para el Tratamiento de Riesgos

En relación con el criterio C3, se compararon las alternativas basándose en la profundidad y claridad de las directrices ofrecidas para las opciones de tratamiento (mitigar, transferir, evitar o aceptar el riesgo). En ese sentido, los cálculos de la matriz pareada y la verificación de consistencia se encuentran detallados en el Anexo C. La Tabla 3.1.3-4 presenta los vectores de prioridad derivados de dicha comparación. En igual sentido, se muestra una representación gráfica en la Figura 3.1.3-5: Ponderación de alternativas vs C3: Recomendaciones para el Tratamiento de Riesgos.

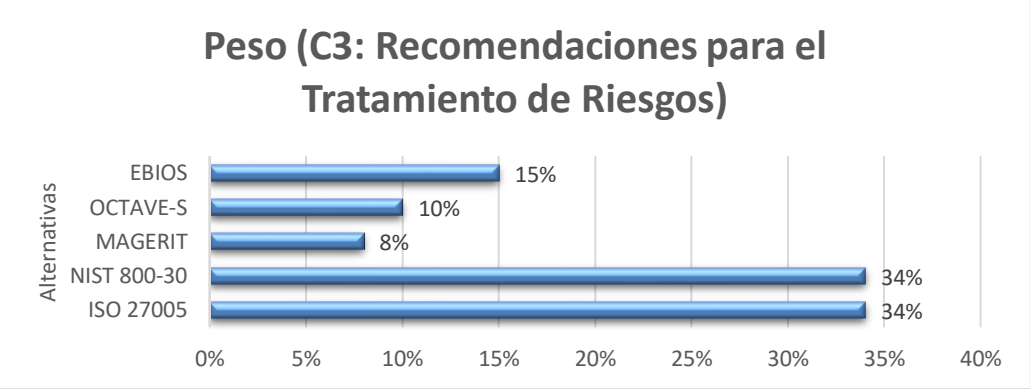
Tabla 3.1.3-4: Priorización de alternativas respecto al criterio C3: Recomendaciones para el Tratamiento de Riesgos

Alternativa (referente internacional)	Vector de prioridad (peso local)	CR (n=5)
ISO/IEC 27005	0.34	
NIST SP 800-30	0.34	0.0966
MAGERIT	0.08	

OCTAVE-S	0.10	✓
EBIOS	0.15	
$\lambda_{max} = 5.4326 \;\; CI = 0.1082 \;\; RI = 1.12$		

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo C.

Figura 3.1.3-5: Ponderación de alternativas vs C3: Recomendaciones para el Tratamiento de Riesgos



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

En la Tabla 3.1.3-4 se observa que ISO/IEC 27005:2022 y NIST SP 800-30 Rev. 1 obtuvieron idéntico vector de prioridad (0.34), compartiendo la primera posición. En conjunto, estas dos alternativas concentran el 68% del peso total asignado en este criterio. EBIOS Risk Manager se ubicó en tercer lugar con una ponderación de 0.15. Por su parte, OCTAVE-S v1.0 y MAGERIT v3.0 registraron los valores más bajos de la distribución, con 0.10 y 0.08 respectivamente.

C4: Directrices para la Implementación de Controles

Respecto al criterio C4, se evaluó la capacidad de cada referente internacional para proporcionar guías específicas, catálogos de controles o vínculos directos con estándares de seguridad, como ISO/IEC 27002 o NIST SP 800-53, que faciliten la fase de mitigación. Los detalles del cálculo matricial y la validación de la consistencia se presentan en el Anexo C. La Tabla 3.1.3-5 expone los vectores de prioridad resultantes para este criterio. De forma gráfica y con datos porcentuales se puede observar la información en la

Figura 3.1.3-6: Ponderación de alternativas vs C4: Directrices para la Implementación de Controles.

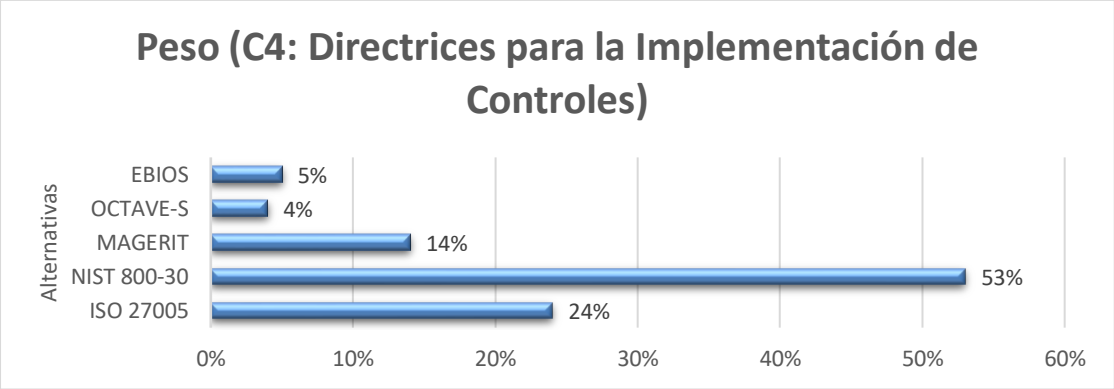
Tabla 3.1.3-5: Priorización de alternativas respecto al criterio C4: Directrices para la Implementación de Controles

Alternativa (referente internacional)	Vector de prioridad (peso local)	CR (n=5)
ISO/IEC 27005	0.24	0.2000
NIST SP 800-30	0.53	

MAGERIT	0.14	✕
OCTAVE-S	0.04	
EBIOS	0.05	
$\lambda_{max} = 5.8961 \; CI = 0.2240 \; RI = 1.12$		

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo C.

Figura 3.1.3-6: Ponderación de alternativas vs C4: Directrices para la Implementación de Controles



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

Los resultados de la Tabla 3.1.3-5 indican que NIST SP 800-30 Rev. 1 obtuvo el vector de prioridad más alto (0.53), concentrando más de la mitad del peso total en este criterio. ISO/IEC 27005:2022 se situó en segundo lugar con 0.24, seguido por MAGERIT v3.0 con 0.14. Por otro lado, EBIOS Risk Manager y OCTAVE-S v1.0 presentaron los valores más bajos, con 0.05 y 0.04 respectivamente. Cabe señalar que OCTAVE-S, que lideró en el criterio de practicidad (C1), ocupa aquí la última posición al evaluarse la especificidad de sus directrices de control.

En lo que sigue, se integraron los vectores de prioridad locales de las alternativas (Tabla 3.1.3-2, Tabla 3.1.3-3, Tabla 3.1.3-4, Tabla 3.1.3-5) con los pesos globales de los criterios (Tabla 3.1.3-1). Ese procedimiento permitió obtener la matriz jerárquica, el peso global de cada referente internacional y establecer su jerarquización definitiva en función de su idoneidad para el contexto de las pymes.

La Tabla 3.1.3-6 presenta el ranking global obtenido del modelo AHP aplicado a los cinco referentes internacionales analizados. Este resultado corresponde a la matriz jerárquica. La Figura 3.1.3-7:

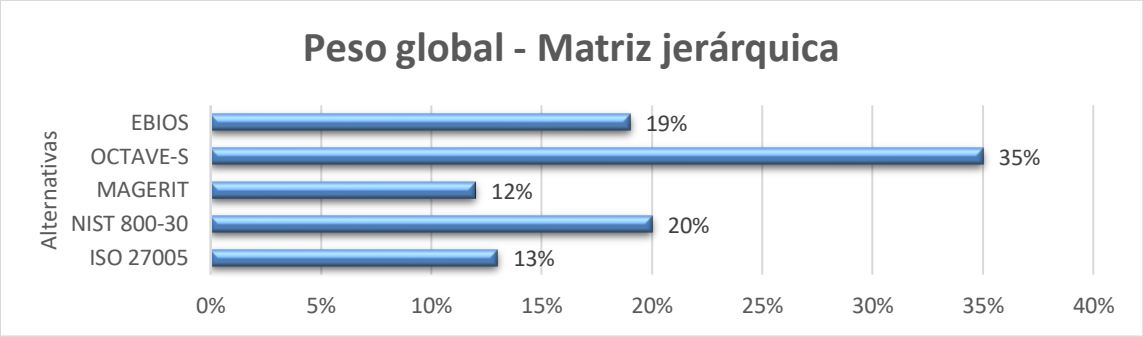
Ponderación de alternativas Fase I - Matriz jerárquica muestra su ponderación porcentual en una gráfica de barras.

Tabla 3.1.3-6: Matriz jerárquica - Ranking global de estándares, guías y metodologías internacionales para la gestión de riesgos

Alternativa	Peso global	Orden de ponderación
ISO/IEC 27005	0.13	4
NIST SP 800-30	0.20	2
MAGERIT	0.12	5
OCTAVE-S	0.35	1
EBIOS	0.19	3

Fuente: Elaboración propia a partir de la síntesis jerárquica del modelo AHP documentada en el Anexo C.

Figura 3.1.3-7: Ponderación de alternativas Fase I - Matriz jerárquica



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

Como se evidencia en la Tabla 3.1.3-6, la metodología OCTAVE-S v1.0 obtuvo la mayor ponderación global con un 35.40%, posicionándose como la alternativa más adecuada para sustentar la metodología propuesta. Este resultado es consecuencia directa de su alto desempeño en el criterio C1: Practicidad y simplicidad, el cual, al tener un peso del 57% en la decisión estratégica, actuó como el factor determinante del modelo.

En segundo lugar, se ubicó NIST SP 800-30 Rev. 1 con un 20.34%. Si bien esta alternativa lideró los criterios técnicos y de control (C2, C3 y C4), la menor ponderación asignada a estos factores en el contexto pyme limitó su puntaje global frente a OCTAVE-S. EBIOS Risk Manager ocupó la tercera posición con un 18.92%, presentando un perfil equilibrado pero sin dominar ningún criterio específico.

Por último, los marcos ISO/IEC 27005:2022 (13.10%) y MAGERIT v3.0 (12.24%) quedaron relegados a las posiciones 4 y 5 respectivamente. Los resultados sugieren que, a pesar de su robustez teórica y reconocimiento internacional, su exigencia en términos de estructura organizacional y carga documental penalizó su viabilidad al ser evaluados bajo las restricciones de recursos típicas de las pymes colombianas.

Análisis de sensibilidad

Con el propósito de evaluar la robustez del ranking obtenido, se realizó un análisis de sensibilidad variando los pesos de cada criterio en rangos de ±10% y ±15%, redistribuyendo proporcionalmente los pesos restantes. La Tabla 3.1.3-7 presenta el ranking resultante de cada alternativa en ocho escenarios de perturbación. La fila final indica si el primer lugar cambia respecto al escenario base. Como se observa, OCTAVE-S v1.0 mantiene el primer lugar en la totalidad de los ocho escenarios de perturbación evaluados, con una ventaja sobre el segundo clasificado que oscila entre 11.0 y 19.1 puntos porcentuales según el escenario. Este resultado confirma que la primacía de OCTAVE-S no es sensible a variaciones razonables en la ponderación de los criterios y que el ranking del primer lugar es robusto dentro del rango ±10–15% ensayado.

Tabla 3.1.3-7. Análisis de sensibilidad - Ranking bajo variaciones de ±10%-15% en pesos según criterios

Alternativa	Base	+10% C1	−10% C1	+15% C2	−15% C2	+10% C3	−10% C3	+15% C4
Pesos C1|C2|C3|C4	57.48%|23.52%|12.62%|6.38%	63.23%|20.34%|10.91%|5.52%	51.73%|26.70%|14.33%|7.24%	54.83%|27.05%|14.04%|6.09%	60.13%|19.99%|13.20%|6.67%	56.65%|23.18%|13.88%|6.29%	58.31%|23.86%|12.36%|6.47%	56.89%|23.28%|12.49%|7.34%
ISO 27005	#4	#5	#4	#4	#4	#4	#4	#4
NIST 800-30	#2	#3	#2	#2	#2	#2	#2	#2
MAGERIT	#5	#4	#5	#5	#5	#5	#5	#5
OCTAVE-S	#1	#1	#1	#1	#1	#1	#1	#1
EBIOS	#3	#2	#3	#3	#3	#3	#3	#3
P(OCTAVE-S)	0.3539	0.3767	0.3311	0.3451	0.3627	0.3503	0.3576	0.3507
Ventaja vs #2	15.1pp	19.1pp	11.0pp	13.5pp	16.6pp	14.5pp	15.6pp	14.4pp
¿Cambia el #1?	No	No	No	No	No	No	No	No
¿Cambia rango intermedio?	No	Sí *	No	No	No	No	No	No

Fuente: Elaboración propia a partir del Anexo C. Cálculos verificados mediante la fórmula $\boldsymbol{P'_i = \sum_j w'_j a_{ij}}$. (*) En el escenario +10% C1, EBIOS asciende al segundo lugar y NIST SP 800-30 desciende al tercero. El cambio en posiciones intermedias se debe al mayor peso local de EBIOS en el criterio C1 respecto a NIST SP 800-30 (0.2113 vs 0.0736).

3.1.4 Producto (d): Síntesis integradora de principios, directrices y requisitos aplicables al contexto pyme, utilizada para el diseño de la metodología propuesta.

Con base en (i) la caracterización comparativa homogénea de los marcos normativos (Producto a, apartado 3.1.1), (ii) los criterios de adaptabilidad definidos para pymes (Producto b, apartado 3.1.2) y (iii) la priorización obtenida mediante el modelo AHP (Producto c, apartado 3.1.3), se elaboró una síntesis integradora organizada en principios, directrices de flujo metodológico y requisitos mínimos aplicables al contexto pyme.

Como resultado de esta integración, el flujo metodológico se estructuró en tres fases tomando como base OCTAVE-S v1.0, incorporando componentes de ISO/IEC 27005:2022 para la definición de criterios de valoración, aceptación y tratamiento del riesgo. De manera complementaria, los marcos NIST SP 800-30 Rev. 1, MAGERIT v3.0 y EBIOS RM se integraron como insumos estructurales dentro de las fases del proceso, aportando taxonomías normalizadas, relaciones de dependencia y elementos para la construcción de escenarios, y como insumos de referencia para estandarizar el

levantamiento en pymes, junto con referenciales de controles (ISO/IEC 27001 Anexo A, ISO/IEC 27002 y NIST SP 800-53).

La Tabla 3.1.4-1, Tabla 3.1.4-2 y Tabla 3.1.4-3 presentan, respectivamente, los principios integrados, las directrices del flujo, y los requisitos mínimos (registros y documentación) derivados de esta síntesis.

Tabla 3.1.4-1: Principios integrados aplicables al contexto pyme

Principio integrado (síntesis)	Descripción operativa en la síntesis	Evidencia mínima asociada	Fundamento en los Marcos de Trabajo
Enfoque basado en activos críticos	El análisis se registró a partir de activos priorizados del negocio	Inventario priorizado de activos críticos	OCTAVE-S requiere seleccionar un límite de hasta cinco activos críticos para que la evaluación sea manejable en organizaciones pequeñas. MAGERIT también inicia identificando activos relevantes y esenciales según su valor para la misión.
Participación de equipo interno reducido	La identificación y validación se registró mediante sesiones con personal clave	Registro de participantes y acuerdos de sesión	OCTAVE-S se basa en el principio de autodirección, donde un equipo interdisciplinario interno de 3 a 5 personas lidera el proceso. EBIOS RM refuerza el uso de talleres estructurados para capturar conocimiento del ecosistema y del negocio.
Escalas cualitativas para valoración	La valoración se registró con escalas simples ajustadas al contexto pyme	Definición de escalas (impacto/probabilidad y/o vulnerabilidad)	OCTAVE-S privilegia valoración con escalas cualitativas (Alto, Medio, Bajo). ISO/IEC 27005 permite enfoques cualitativos y semicuantitativos, siempre que se definan criterios y consistencia.
Trazabilidad del riesgo	La relación activo–escenario–riesgo–decisión se registró en un hilo documental	Matriz de riesgos con campos de decisión, responsable, estado y evidencia.	NIST SP 800-30 Rev.1 estructura el riesgo desde escenarios/factores (fuente–evento–vulnerabilidad–impacto) para soportar decisiones; ISO/IEC 27005 exige trazabilidad hacia tratamiento y aceptación.
Iteración y revisión	La revisión del análisis se consignó como actividad recurrente	Fecha/frecuencia de revisión y control de versiones	La gestión de riesgos no es una actividad de una sola vez; ISO/IEC 27005 define ciclos estratégicos (largos) y operacionales (cortos) para revisiones periódicas. EBIOS RM también propone un enfoque iterativo basado en talleres y refinamiento progresivo de escenarios.

Fuente: Elaboración propia a partir de la caracterización comparativa de marcos normativos, los criterios de adaptabilidad para pymes y las fuentes primarias OCTAVE-S v1.0, ISO/IEC 27005:2022, NIST SP 800-30 Rev. 1, MAGERIT v3.0 y EBIOS RM.

Tabla 3.1.4-2: Síntesis integradora del flujo metodológico

Fase del proceso (OCTAVE-S)	Elementos base consignados (flujo principal)	Componentes incorporados (síntesis integrada)
Fase 1: Construcción de perfiles de amenazas basados en activos	Identificación de activos críticos con equipo interno; definición de requisitos de seguridad por activo; identificación de amenazas asociadas	ISO/IEC 27005: delimitación de contexto/alcance, criterios cualitativos de impacto y criterios de aceptación del riesgo para orientar la valoración. MAGERIT v3.0: apoyo a la determinación de criticidad mediante relaciones de dependencias (activo esencial ↔ activos de soporte) para evitar omisiones en activos habilitadores. NIST SP 800-30: estructuración de la caracterización de la amenaza en términos de fuente/evento y condiciones predisponentes para estandarizar el levantamiento. EBIOS RM: incorporación del enfoque de eventos temidos para vincular el impacto a la misión del negocio desde el inicio
Fase 2: Identificación de vulnerabilidades de infraestructura	Revisión de caminos de acceso y componentes tecnológicos clave; registro de debilidades y prácticas inseguras asociadas a los activos críticos	ISO/IEC 27005: guías de identificación y análisis de vulnerabilidades con apoyo de listas de verificación y fuentes de referencia técnica, manteniendo coherencia con criterios definidos. NIST SP 800-30: consolidación de la relación vulnerabilidad–condiciones predisponentes–probabilidad, como soporte para una estimación reproducible. MAGERIT v3.0: mapeo de vulnerabilidades sobre activos de soporte relevantes derivados del modelo de dependencias. EBIOS RM: enriquecimiento de rutas de ataque a partir del ecosistema (proveedores/terceros) cuando aplique al activo crítico
Fase 3: Desarrollo de estrategias y planes de mitigación	Valoración cualitativa de riesgos; priorización de riesgos críticos; definición de estrategia de protección y planes de acción	NIST SP 800-30: determinación del nivel de riesgo como función de probabilidad × impacto (matriz de priorización) para ordenar hallazgos de forma trazable. ISO/IEC 27005: selección de opción de tratamiento (evitar, mitigar/modificar, compartir/transferir, aceptar/retener) y formalización del plan de tratamiento con responsables y evidencias. Referenciales de controles: uso de ISO/IEC 27001 Anexo A, ISO/IEC 27002 y NIST SP 800-53 como base de selección de salvaguardas. EBIOS RM: validación de medidas frente a escenarios (coherencia entre evento temido–ruta de ataque–medida)

Fuente: Elaboración propia a partir de las directrices metodológicas de OCTAVE-S v1.0 y de la integración de componentes de ISO/IEC 27005:2022, NIST SP 800-30 Rev. 1, MAGERIT v3.0 y EBIOS RM, de acuerdo con la caracterización comparativa y la priorización AHP reportada en la Fase I.

Tabla 3.1.4-3: Requisitos mínimos integrados aplicables al contexto pyme

Requisito mínimo consignado	Registro / documento mínimo	Fuentes normativas consignadas en la síntesis
Definición de contexto, alcance y supuestos	Documento de alcance, supuestos y límites del análisis	ISO/IEC 27005 + OCTAVE-S
Criterios de impacto y aceptación del riesgo	Plantilla de criterios (impacto/aceptación) y reglas de uso	ISO/IEC 27005
Inventario de activos con requisitos de seguridad	Inventario de activos con C-I-D (y criticidad)	OCTAVE-S + ISO/IEC 27005 (+ MAGERIT como apoyo de dependencias)
Catálogo típico de activos para pyme	Lista consolidada de activos típicos (esenciales y de soporte)	MAGERIT / NIST SP 800-30 / EBIOS RM (transferencia taxonómica)
Catálogo típico de amenazas para pyme	Lista consolidada de amenazas típicas (fuentes/eventos)	NIST SP 800-30 / MAGERIT / EBIOS RM (transferencia taxonómica)
Catálogo típico de vulnerabilidades para pyme	Lista consolidada de vulnerabilidades típicas y condiciones predisponentes	NIST SP 800-30 / MAGERIT / EBIOS RM (transferencia taxonómica)
Registro de escenarios de riesgo por activo	Matriz de escenarios (amenaza–vulnerabilidad–consecuencia) y evento temido asociado	OCTAVE-S + ISO/IEC 27005 + EBIOS RM (enfoque de eventos temidos)
Registro de valoración del riesgo	Matriz de valoración cualitativa (reglas + evidencia de asignación)	OCTAVE-S + ISO/IEC 27005 + NIST SP 800-30 (estructuración probabilidad × impacto)
Decisión de tratamiento del riesgo	Campo/registro de decisión por riesgo (opción + justificación)	ISO/IEC 27005
Referencial de controles para selección de medidas	Tabla de controles aplicables y trazabilidad a riesgos	ISO/IEC 27001 Anexo A / ISO/IEC 27002 / NIST SP 800-53 (insumo normativo)
Plan de tratamiento mínimo	Plan de tratamiento (medida, responsable, fecha, evidencia, estado)	ISO/IEC 27005 + OCTAVE-S

Fuente: Elaboración propia a partir de la caracterización comparativa de marcos normativos, los criterios de adaptabilidad para pymes y la síntesis integradora derivada de OCTAVE-S v1.0, ISO/IEC 27005:2022, NIST SP 800-30 Rev. 1, MAGERIT v3.0 y EBIOS RM.

De manera complementaria, se consolidaron catálogos de referencia de activos, amenazas y vulnerabilidades a partir de NIST SP 800-30, MAGERIT v3.0 y EBIOS RM, registrándose su uso como

insumos taxonómicos para el levantamiento y la organización de información en pymes. Asimismo, se referenciaron repositorios de controles (ISO/IEC 27002 y NIST SP 800-53) como insumos para la selección de medidas durante el tratamiento del riesgo.

3.2 Resultados de la Fase II – OE2: Análisis y selección de herramientas y soluciones de software para la gestión de riesgos

En la Fase II se consolidaron cuatro productos metodológicos derivados de la triangulación entre (i) los requisitos funcionales definidos en la síntesis integradora de la Fase I (Producto d) y (ii) la revisión técnica de soluciones de software OpenSource y gratuitas disponibles en el mercado.

El desarrollo de esta fase respondió a la necesidad de instrumentar tecnológicamente el flujo metodológico híbrido diseñado, asegurando que la herramienta seleccionada no solo fuese viable técnicamente, sino que permitiese la personalización requerida por el contexto pyme.

Los productos se organizaron siguiendo la estructura lógica definida en la metodología: (a) caracterización comparativa técnica y funcional de las herramientas candidatas, (b) criterios de evaluación, (c) modelo AHP para la priorización de software, y (d) selección de la herramienta tecnológica.

3.2.1 Producto (a): Caracterización técnica y funcional de herramientas de software

A partir de la búsqueda en repositorios públicos, plataformas de evaluación técnica, sitios oficiales y literatura especializada, se realizó un análisis técnico-funcional basado en la documentación oficial de cada alternativa (manuales, guías técnicas, arquitectura, dependencias y funcionalidades relacionadas con el ciclo de gestión del riesgo). Esto permitió preseleccionar y consolidar una caracterización unificada bajo criterios de licenciamiento (OpenSource/GPL o modelos Freemium), vigencia (mantenimiento activo) y enfoque en gestión de riesgos (GRC).

La caracterización se sistematizó mediante fichas técnicas de análisis funcional, admitiendo variables críticas como el modelo de despliegue, la compatibilidad metodológica y los requisitos de infraestructura.

En cumplimiento del procedimiento metodológico, se desarrollaron dos instrumentos de análisis previos:

- Matriz de preselección: Donde se aplicaron los criterios de inclusión a diversas soluciones del mercado (Ver Anexo D).
- Fichas técnicas de análisis funcional: Donde se documentaron individualmente los requisitos y capacidades de las cinco herramientas finalistas (Ver Anexo E).

A partir de la consolidación de estos instrumentos, la Tabla 3.2.1-1 presenta la comparación técnico-funcional de las cinco herramientas analizadas en la Fase II (OE2). La información presentada es una síntesis derivada del análisis documental realizado. Para consultar el detalle de requisitos, módulos, evidencias consultadas y fuentes de verificación por campo, remítase al Anexo E.

Tabla 3.2.1-1: Síntesis comparativa técnico-funcional de herramientas analizadas para la gestión de riesgos de seguridad informática

Herramienta	Modelo de licenciamiento / disponibilidad	Enfoque funcional predominante	Cobertura funcional del ciclo de riesgo (síntesis)	Requisitos de infraestructura / despliegue (según documentación)	Rasgo relevante para pyme (descriptivo)
MONARC	OpenSource (GNU AGPL v3.0)	Modelado del riesgo basado en activos y dependencias; reutilización de conocimiento (catálogos/modelos).	Soporta el ciclo de riesgo mediante: contexto y modelado de activos, uso de catálogos (amenazas/medidas), valoración cualitativa (impacto–probabilidad), análisis y tratamiento conforme a la configuración del modelo.	Aplicación web on-premise tipo servidor; despliegue sobre stack LAMP o equivalente (servidor web, PHP, BD MySQL/MariaDB), con componentes auxiliares según el método de instalación.	Posibilita capitalización/reutilización de catálogos/modelos y aceleración del análisis al no partir desde cero.
SimpleRisk (Core / open-core)	Open-core / freemium: núcleo abierto y capacidades avanzadas/extendidas bajo licenciamiento comercial (según edición).	Operación GRC orientada a registro, mitigación y seguimiento del riesgo.	Cubre: registro de riesgos, asignación de atributos, planificación/seguimiento de mitigaciones, revisiones y salidas operativas (reportes/exports según edición/configuración).	Aplicación web on-premise; despliegue típico tipo servidor (stack equivalente a LAMP). Requisitos y dependencias específicas varían por versión/edición y configuración.	Curva de adopción operativa (enfoque tipo "risk register"), útil para transición progresiva desde esquemas tipo hoja de cálculo; validar alcance del núcleo vs. extensiones.
ERAMBA (Community Edition)	Community Edition (free/open version) bajo términos de licencia del proveedor (custom); modalidades/alcances diferenciados frente a ediciones comerciales.	GRC con énfasis en cumplimiento, controles y auditoría, incorporando revisiones periódicas y trazabilidad de evidencias.	Cubre el ciclo de riesgo mediante: registro/gestión de riesgos, gestión de controles, evidencias y reportes; incorpora revisiones/auditorías programadas y seguimiento por flujos (workflows) según configuración.	Aplicación web; despliegue documentado on-premise (frecuente vía contenedores/Docker o VM) y modalidad SaaS según oferta. Requiere recursos medios en escenarios de cumplimiento/auditoría por la carga modular.	Útil cuando se exige trazabilidad de cumplimiento y control; puede demandar mayor esfuerzo de parametrización y recursos de infraestructura que alternativas más ligeras.
PILAR (Basic / edición utilizada)	Propietaria: distribución bajo licencia de uso (incluye opción de evaluación). La edición de evaluación puede imponer limitaciones funcionales (p. ej., restricciones de informes/exportaciones) según condiciones del proveedor.	Herramienta de análisis de riesgos asociada a MAGERIT (benchmark metodológico).	Soporta análisis basado en activos y dependencias conforme a MAGERIT: modelado/valoración de activos, uso de bibliotecas (amenazas/salvaguardas), cálculo de impacto y riesgo; tratamiento y reportes/exportaciones dependen de la edición/licencia.	Aplicación de escritorio (entorno Java según requisitos del proveedor); uso local de proyectos/archivos y/o capacidades asociadas a la edición.	Aporta formalismo metodológico y bibliotecas estructuradas, con posible mayor carga operativa por curva de aprendizaje y restricciones por licenciamiento/edición.
Pirani Risk	Propietaria (SaaS): planes comerciales con versión gratuita limitada (según proveedor).	Gestión operativa de riesgos (plataforma SaaS) con módulos aplicables a riesgos e ISMS; usada como benchmark funcional por usabilidad.	Cubre: registro de riesgos, parametrización de matrices/heatmaps, priorización, planes de acción y seguimiento; tableros/reportes y automatizaciones dependen del plan.	SaaS (nube): acceso vía navegador web; no requiere instalación local; dependencias y mantenimiento gestionados por el proveedor.	Puesta en marcha rápida sin infraestructura propia; limitación: dependencia del modelo SaaS y restricciones del plan frente a escalamiento.

Fuente: Elaboración propia a partir del análisis documental técnico-funcional de las herramientas evaluadas en la Fase II, con base en los requisitos, módulos, evidencias consultadas y fuentes de verificación sistematizadas en el Anexo E.

3.2.2 Producto (b): Criterios evaluativos para el análisis multicriterio (AHP) de herramientas de gestión de riesgos en pymes

A partir del análisis conceptual desarrollado en el Marco Teórico y Estado del Arte (apartados 1.1.5 y 1.2.3), y con base en las restricciones típicas de las pymes descritas en el apartado 1.1.3, se definieron cuatro criterios evaluativos para valorar comparativamente las herramientas que

avanzaron al AHP luego de la preselección en la Fase II. Estos criterios Operacionalizan, en términos comparables, los atributos funcionales y operativos que se consideran determinantes para seleccionar una solución que soporte la metodología de gestión de riesgos propuesta.

La derivación de los criterios se fundamentó en la intersección entre: (i) los requisitos funcionales esperados para herramientas orientadas a la gestión de riesgos de seguridad de la información (gestión de activos, amenazas, vulnerabilidades, tratamiento y seguimiento), (ii) factores sociotécnicos de adopción (usabilidad, accesibilidad técnica y adaptabilidad), y (iii) limitaciones estructurales de pymes (recursos limitados, baja madurez, ausencia de personal especializado).

Los criterios definidos en la Tabla 3.2.2-1 sirvieron como base para estructurar el modelo jerárquico AHP de la Etapa 3 de la Fase II. A partir de ellos se construyeron: (a) la matriz de comparación por pares de criterios; (b) las matrices de evaluación de alternativas por criterio; y (c) la síntesis global para el ranking final de herramientas.

Tabla 3.2.2-1: Criterios evaluativos definidos para el análisis AHP de herramientas aplicables a la gestión de riesgos de seguridad informática

Criterio	Definición operativa	Evidencia/indicadores de análisis (síntesis)	Relación con restricciones típicas pyme (síntesis)
Gestión organizacional	Capacidad de la herramienta para soportar el componente organizacional y documental requerido en la gestión de riesgos: estructurar el inventario (activos/contexto), registrar información base y producir salidas documentales para trazabilidad y toma de decisiones.	Registro estructurado de activos/procesos/áreas; catálogos configurables; documentación y reportes (inventarios, matrices, estados); evidencias de trazabilidad (historial, responsables, estados).	Reduce dependencia de prácticas informales (p. ej., hojas de cálculo) y facilita institucionalizar la gestión del riesgo con trazabilidad mínima y carga documental controlada.
Análisis técnico	Capacidad para representar y analizar aspectos técnicos relevantes del entorno tecnológico que soporta los activos: infraestructura, componentes y (si aplica) registro/seguimiento de vulnerabilidades y hallazgos técnicos vinculables al riesgo.	Modelado/registro de componentes tecnológicos y relaciones; soporte para registrar hallazgos técnicos/vulnerabilidades (nativo o integrable); consolidación/priorización de hallazgos; capacidad de generar documentación técnica para tratamiento.	Permite gestionar riesgo con fundamento técnico incluso cuando la pyme carece de herramientas especializadas; si el criterio se soporta parcialmente, evidencia límites realistas de adopción.
Gestión de riesgos	Capacidad para soportar el ciclo de gestión del riesgo de seguridad: identificación, análisis/evaluación, tratamiento y seguimiento, manteniendo coherencia entre riesgo, controles/acciones y estado.	Registro de riesgos (amenaza–activo–vulnerabilidad o estructura equivalente); escalas y métodos de valoración (impacto/probabilidad u otros); planes de tratamiento (acciones/controles, responsables,	Prioriza herramientas que permitan “cerrar el ciclo” (de análisis a acción) con mecanismos de seguimiento, adecuados para recursos

Criterio	Definición operativa	Evidencia/indicadores de análisis (síntesis)	Relación con restricciones típicas pyme (síntesis)
		fechas); seguimiento (revisiones, tableros, alertas/estados).	limitados y ejecución operacional.
Viabilidad técnica y operativa	Factibilidad de implementación y uso en pymes considerando infraestructura requerida, facilidad de despliegue, sostenibilidad de soporte/mantenimiento y usabilidad para equipos no especializados.	Requisitos de instalación (servidor, SaaS, desktop), complejidad de despliegue (Docker/VM/LAMP), disponibilidad de documentación y soporte, modelo de licenciamiento/costos, usabilidad/curva de aprendizaje.	Minimiza fricción de adopción: selecciona alternativas implementables con recursos limitados, sin exigir capacidades avanzadas o costos que excedan el contexto pyme.

Fuente: Elaboración propia a partir del Marco Teórico y Estado del Arte, especialmente de los apartados sobre herramientas OpenSource, gestión de riesgos de seguridad informática y restricciones operativas de las pymes.

Para facilitar la lectura, a continuación se presenta una síntesis descriptiva de cada criterio:

- Gestión Organizacional

Se refiere a la capacidad para estructurar el contexto (activos/áreas/procesos) y producir trazabilidad documental mínima para soportar decisiones de riesgo en la pyme.

- Análisis Técnico

Se refiere a la capacidad para registrar/modelar elementos técnicos relevantes y vincular hallazgos técnicos (incluidas vulnerabilidades, nativas o integrables) con el análisis de riesgo.

- Gestión de Riesgos

Se refiere a la capacidad para soportar el ciclo completo de riesgo (identificación, análisis/evaluación, tratamiento y seguimiento) manteniendo coherencia entre riesgo–acciones/controles–estado.

- Viabilidad Técnica y Operativa

Se refiere a la factibilidad real de implementación y uso en pymes considerando infraestructura, despliegue, soporte/mantenimiento, licenciamiento/costos y usabilidad.

Estos criterios corresponden a los cuatro criterios evaluativos definidos en la Etapa 2 de la Fase II: gestión organizacional, análisis técnico, gestión de riesgos y viabilidad técnica y operativa.

3.2.3 Producto (c): Modelo jerárquico AHP y priorización de herramientas para gestión de riesgos (alternativas Open Source y benchmarks)

El tercer producto de la Fase II consistió en la estructuración y ejecución del modelo de decisión multicriterio AHP para priorizar comparativamente las herramientas mediadas por las TIC. Este modelo integró los insumos de los productos anteriores: las herramientas finalistas caracterizadas técnica y funcionalmente (Producto a) actuaron como alternativas, y los criterios evaluativos definidos (Producto b) operaron como criterios de decisión.

La aplicación del AHP permitió cuantificar la idoneidad relativa de cada herramienta en función de criterios homogéneos, obteniendo así vectores de prioridad locales y globales que sustentan la priorización final. En adición, la evidencia técnica reproducible del cálculo (matrices por pares, vectores, razón de consistencia y síntesis global) se consolida en el archivo electrónico del modelo AHP (Anexo F).

- Estructura jerárquica del modelo AHP

El modelo AHP se estructuró en tres niveles jerárquicos (Ver Figura 3.2.3-1):

3.2.3.1.1 Nivel 1 (Objetivo)

Seleccionar la herramienta de software más adecuada para soportar la metodología propuesta de gestión de riesgos de seguridad de la información en pymes.

3.2.3.1.2 Nivel 2 (Criterios)

Los cuatro criterios evaluativos definidos en el Producto (b):

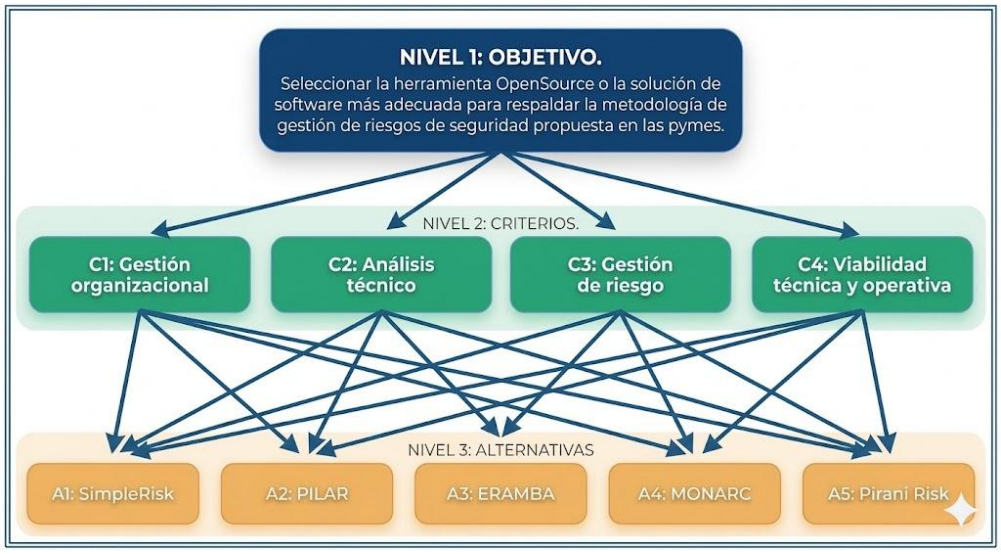
- C1: Gestión organizacional
- C2: Análisis técnico
- C3: Gestión de riesgo
- C4: Viabilidad técnica y operativa

3.2.3.1.3 Nivel 3 (Alternativas)

Las cinco herramientas finalistas caracterizadas en el Producto (a):

- A1: SimpleRisk
- A2: PILAR
- A3: ERAMBA
- A4: MONARC
- A5: Pirani Risk

Figura 3.2.3-1: Estructura jerárquica del modelo de decisión AHP para la selección de la herramienta de gestión de riesgos



Fuente: Elaboración propia a partir de los criterios evaluativos definidos en la Fase II y del análisis técnico-funcional de las herramientas. La representación gráfica fue apoyada mediante herramienta de inteligencia artificial generativa **[227]**.

A diferencia de la Fase I (donde se empleó consenso de expertos), en la Fase II las matrices de comparación por pares fueron diligenciadas por el investigador principal (Anexo F), con base en la evidencia documental consolidada en el Anexo D (preselección) y el Anexo E (fichas técnicas).

- Comparación por pares entre criterios

Tras aplicar el método AHP, se obtuvieron los vectores propios que representan la importancia relativa de cada criterio de evaluación definido en el Producto (b). En la Tabla 3.2.2-1 se observa que el criterio “Gestión de riesgos” obtuvo el mayor peso relativo (46%). Seguido por “Viabilidad

técnica y operativa" (30%). En tercer lugar, se ubicó "Gestión organizacional" (19%). Finalmente, el criterio "Análisis técnico" presentó el menor peso (5%).

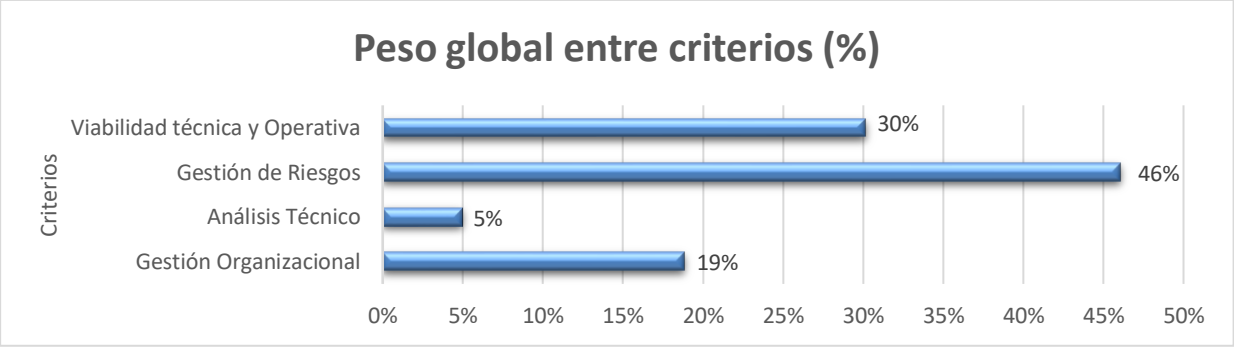
Tabla 3.2.3-1: Pesos globales para la selección de herramientas mediante AHP (Fase II)

Criterio	Peso global (vector promedio)
C1: Gestión organizacional	0.19
C2: Análisis técnico	0.05
C3: Gestión de riesgos	0.46
C4: Viabilidad técnica y operativa	0.30

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo F.

El detalle completo de la matriz de comparación pareada, los cálculos de normalización y la verificación de consistencia se encuentra disponible en el Anexo F. Una representación gráfica de la ponderación de criterios puede presentarse en la Figura 3.2.3-2.

Figura 3.2.3-2: Distribución de los pesos globales de los criterios de evaluación (Modelo AHP - Fase II)



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

- Comparación por pares de alternativas respecto a cada criterio

Para cada uno de los cuatro criterios, el investigador principal, sin panel de expertos comparó las cinco alternativas (herramientas) por pares. En las siguientes tablas, se presentan las matrices de comparación y los vectores de prioridad resultantes.

C1: Gestión organizacional

Se contrastaron las cinco herramientas mediante juicios del investigador principal, priorizando aquellas herramientas TIC con mayor capacidad para estructurar el contexto organizacional (activos/áreas/procesos), registrar información base y generar trazabilidad documental (responsables, estados, reportes) para soportar la toma de decisiones en la pyme. Los cálculos detallados de la matriz de comparación pareada y su verificación de consistencia se presentan en el Anexo F. La Tabla 3.2.3-2 resume los vectores de prioridad (pesos locales) obtenidos para este criterio. Una representación gráfica se presenta en la Figura 3.2.3-3: Ponderación de alternativas vs C1: Gestión organizacional.

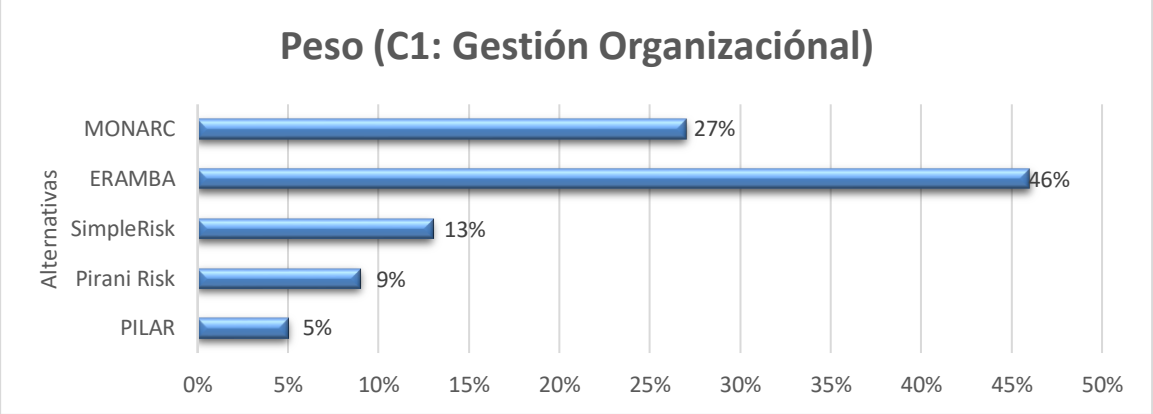
Tabla 3.2.3-2. Priorización de alternativas respecto al criterio C1: Gestión organizacional

Alternativa (herramienta)	Vector de prioridad (peso local)
PILAR	0.05
Pirani Risk	0.09
SimpleRisk	0.13
ERAMBA	0.46
MONARC	0.27

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo F.

Los datos de la Tabla 3.2.3-2 muestran que ERAMBA alcanzó el mayor vector de prioridad (0.46), seguido por MONARC (0.27). SimpleRisk ocupó la tercera posición con 0.13, mientras que Pirani Risk (0.09) y PILAR (0.05) registraron los valores más bajos. En términos comparativos, la diferencia entre la primera alternativa (ERAMBA) y la segunda (MONARC) fue de 0.19 puntos, y la suma de las tres alternativas con menor ponderación (SimpleRisk, Pirani Risk y PILAR) fue de 0.27.

Figura 3.2.3-3: Ponderación de alternativas vs C1: Gestión organizacional



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

C2: Análisis técnico

Se contrastaron las cinco herramientas mediante juicios del investigador principal, priorizando aquellas con mayor capacidad para registrar/modelar elementos técnicos relevantes (componentes y relaciones de infraestructura) y vincular hallazgos técnicos (incluidas vulnerabilidades, nativas o integrables) con el análisis de riesgo. Los cálculos detallados de la matriz de comparación pareada y su verificación de consistencia se presentan en el Anexo F. La Tabla 3.2.3-3 resume los vectores de prioridad (pesos locales) obtenidos para este criterio. Al igual, la Figura 3.2.3-4: Ponderación de alternativas vs C2: Análisis Técnico presenta los datos en porcentajes.

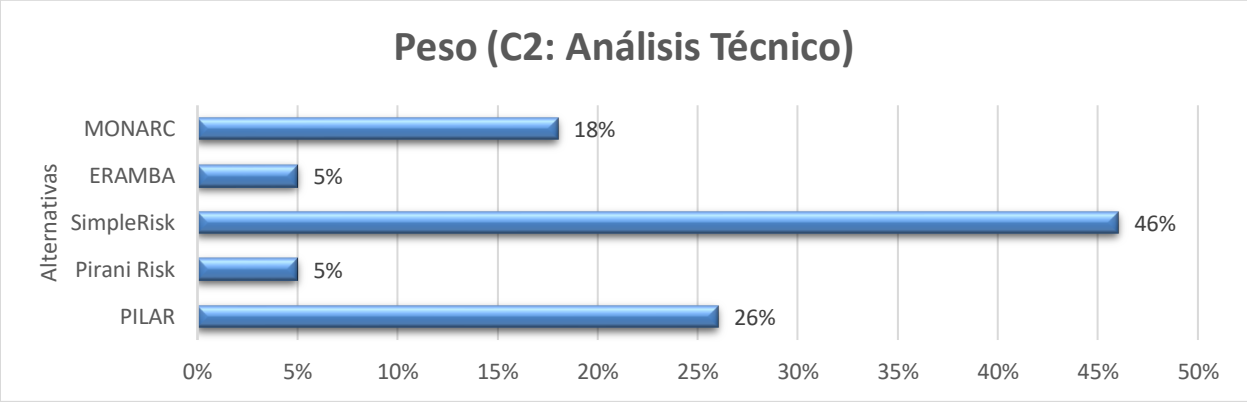
Tabla 3.2.3-3: Priorización de alternativas respecto al criterio C2: Análisis técnico

Alternativa (herramienta)	Vector de prioridad (peso local)
PILAR	0.26
Pirani Risk	0.05
SimpleRisk	0.46
ERAMBA	0.05
MONARC	0.18

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo F.

Los datos de la Tabla 3.2.3-3 muestran que SimpleRisk alcanzó el mayor vector de prioridad (0.46), seguido por PILAR (0.26) y MONARC (0.18). Pirani Risk y ERAMBA registraron los valores más bajos (0.05 cada una). En términos comparativos, la diferencia entre la primera alternativa (SimpleRisk) y la segunda (PILAR) fue de 0.20 puntos, y la suma de las dos alternativas con menor ponderación (Pirani Risk y ERAMBA) fue de 0.10.

Figura 3.2.3-4: Ponderación de alternativas vs C2: Análisis Técnico



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

C3: Gestión de riesgos

En relación con el criterio C3: Gestión de riesgos, el investigador principal comparó por pares las cinco alternativas considerando su capacidad para soportar el ciclo de gestión del riesgo de seguridad (identificación, análisis/evaluación, tratamiento y seguimiento) y mantener la coherencia entre riesgo–acciones/controles–estado, conforme a la definición operativa del criterio. Los cálculos detallados de la matriz de comparación pareada y su verificación de consistencia se encuentran documentados en el Anexo F.

La Tabla 3.2.3-4: Priorización de alternativas respecto al criterio C3: Gestión de Riesgos presentó los vectores de prioridad (pesos locales) resultantes para cada herramienta, los cuales se complementaron con la Figura 3.2.3-5 (representación porcentual de la ponderación local por alternativa). En los resultados se observó que MONARC alcanzó el mayor vector de prioridad (0.43). SimpleRisk y ERAMBA registraron valores equivalentes (0.22 cada una), mientras que Pirani Risk presentó un valor de 0.09 y PILAR el menor valor del conjunto (0.04). La diferencia entre la

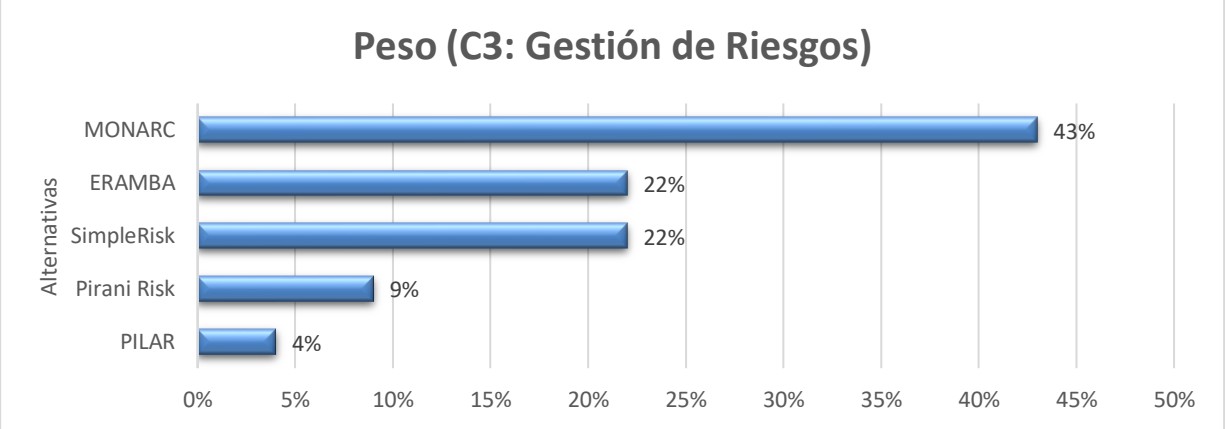
alternativa con mayor ponderación local (MONARC) y el siguiente nivel de alternativas (SimpleRisk/ERAMBA) fue de 0.21 puntos en este criterio.

Tabla 3.2.3-4: Priorización de alternativas respecto al criterio C3: Gestión de Riesgos

Alternativa (herramienta)	Vector de prioridad (peso local)
PILAR	0.04
Pirani Risk	0.09
SimpleRisk	0.22
ERAMBA	0.22
MONARC	0.43

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo F.

Figura 3.2.3-5: Ponderación de alternativas vs C3: Gestión de riesgos



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

C4: Viabilidad Técnica y Operativa.

En el criterio C4, el investigador principal comparó por pares las cinco alternativas considerando la factibilidad de implementación y uso en pymes (infraestructura requerida, facilidad de despliegue, sostenibilidad de soporte/mantenimiento, licenciamiento/costos y usabilidad). Los cálculos detallados y la verificación de consistencia de la matriz se consignaron en el Anexo F.

La Tabla 3.2.3-5: Priorización de alternativas respecto al criterio C4: Viabilidad Técnica y Operativa presentó los pesos locales obtenidos, y la Figura 3.2.3-6: Ponderación de alternativas vs C4: Viabilidad técnica y operativa mostró su distribución porcentual. En este criterio, Pirani Risk alcanzó el mayor peso local (0.57). En segundo lugar, se posicionó SimpleRisk (0.20). Posteriormente,

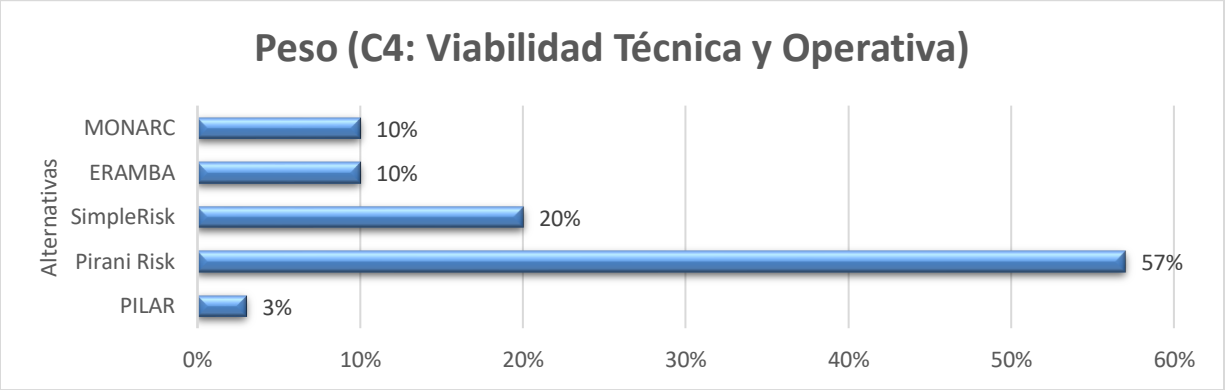
ERAMBA (0.10) y MONARC (0.10) registraron valores equivalentes, mientras que PILAR obtuvo el menor peso (0.03).

Tabla 3.2.3-5: Priorización de alternativas respecto al criterio C4: Viabilidad Técnica y Operativa

Alternativa (herramienta)	Vector de prioridad (peso local)
PILAR	0.03
Pirani Risk	0.57
SimpleRisk	0.20
ERAMBA	0.10
MONARC	0.10

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo F.

Figura 3.2.3-6: Ponderación de alternativas vs C4: Viabilidad técnica y operativa



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

En lo que sigue, se integraron los vectores de prioridad locales de las alternativas obtenidos para cada criterio (C1 a C4, presentados en las Tabla 3.2.3-2, Tabla 3.2.3-3, Tabla 3.2.3-4, Tabla 3.2.3-5) con los pesos globales de los criterios definidos previamente, con el fin de obtener el peso global de cada herramienta y su jerarquización definitiva dentro del modelo AHP. El detalle de las matrices de comparación, normalizaciones y verificación de consistencia se consolidó en el Anexo F.

La Tabla 3.2.3-6 presenta el ranking global obtenido del modelo AHP aplicado a las cinco herramientas evaluadas (matriz jerárquica). MONARC registró el mayor peso global (0.29), seguido por Pirani Risk (0.23), ERAMBA (0.22), SimpleRisk (0.21) y PILAR (0.05), estableciendo el orden de ponderación 1 a 5 en el mismo sentido.

De acuerdo con los valores reportados, la diferencia entre la alternativa ubicada en la primera posición (MONARC, 0.29) y la segunda (Pirani Risk, 0.23) fue de 0.06. Asimismo, entre las alternativas ubicadas en las posiciones segunda, tercera y cuarta se observó una cercanía en los pesos globales (0.23, 0.22 y 0.21, respectivamente), mientras que PILAR presentó el valor más bajo del conjunto (0.05).

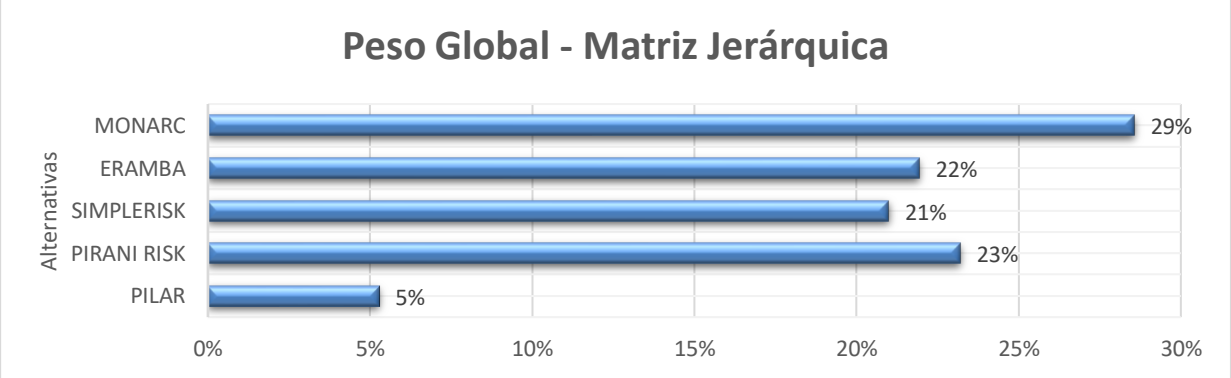
Tabla 3.2.3-6: Matriz jerárquica - Ranking global de herramientas para la gestión de riesgos de seguridad

Alternativa	Peso global	Orden de ponderación
PILAR	0.05	5
PIRANI RISK	0.23	2
SIMPLERISK	0.21	4
ERAMBA	0.22	3
MONARC	0.29	1

Fuente: Elaboración propia a partir de los cálculos de comparación pareada documentados en el Anexo F.

La Figura 3.2.3-7: Ponderación de alternativas Fase II - Matriz jerárquica complementa la tabla anterior al representar de forma porcentual la ponderación global de cada alternativa (29%, 23%, 22%, 21% y 5%), facilitando la visualización del ordenamiento final. La evidencia completa del cálculo del modelo (matrices por criterio, vectores de prioridad y síntesis global) se mantiene disponible en el Anexo F, como soporte técnico verificable del procedimiento. Las matrices de comparación por criterio (C1–C4) registraron CR ≤ 0.10; el detalle se documentó en el Anexo F.

Figura 3.2.3-7: Ponderación de alternativas Fase II - Matriz jerárquica



Fuente: Elaboración propia a partir de los resultados de la matriz AHP.

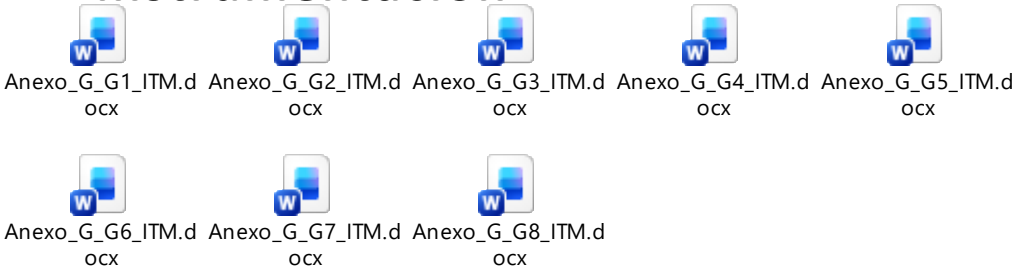
3.3 Resultados de la Fase III – OE3: Uso del software OpenSource seleccionado para la gestión de riesgos en seguridad informática en pymes

Los resultados de la Fase III se derivaron de la instrumentación técnico-operativa controlada de la herramienta OpenSource MONARC, previamente seleccionada en la Fase II.

La fase III se ejecutó en un entorno controlado para operacionalizar la metodología propuesta, asegurando la trazabilidad entre los requisitos normativos integrados en la Fase I (principios, directrices y requisitos mínimos) y su implementación en MONARC.

El procedimiento se estructuró en cinco etapas secuenciales, alineadas con el flujo operativo de MONARC y el ciclo metodológico definido en la síntesis integradora (ver Tabla 3.1.4-2).

A continuación se describen los resultados obtenidos en cada etapa junto con los productos verificables generados. Para mayor detalle técnico-metodológico, se remite al Anexo: Soporte técnico-metodológico de instrumentación



Se presenta una versión condensada del soporte técnico-metodológico para la instrumentación de MONARC en la Fase III (OE3).

G.1.2 Parámetros mínimos de despliegue y configuración base

Tabla G.1.2-1. Parámetros mínimos de despliegue y configuración base del entorno (VM VirtualBox + MONARC).

Parámetro	Valor adoptado	Propósito metodológico	Riesgo si se omite	Regla mínima de control
Plataforma de virtualización	Oracle VM VirtualBox (host de escritorio)	Proveer un entorno aislado, controlado y reproducible para la ejecución de MONARC, independiente del sistema operativo anfitrión.	Dependencia del entorno del host, imposibilidad de replicar el análisis en condiciones técnicas equivalentes.	Uso exclusivo de VirtualBox durante la Fase III, sin cambios de hipervisor.
Modo de despliegue	Máquina Virtual preconfigurada (imagen OVA)	Reducir la complejidad técnica del despliegue y garantizar homogeneidad en la instalación del stack de MONARC.	Errores de configuración manual en servicios, versiones inconsistentes del entorno base.	Importación directa de la imagen OVA sin modificación de componentes internos.
Versión de MONARC	MONARC v2.13.x (p3, commit 6d10eba)	Asegurar compatibilidad con las funciones de modelado, evaluación automática del riesgo y gestión del tratamiento.	Incompatibilidad funcional, variaciones en la lógica de cálculo o en la estructura de datos.	Congelación de versión durante toda la ejecución de OE3.
Sistema operativo invitado	Linux (incluido en la imagen VM oficial)	Soportar la ejecución estable de los servicios web, base de datos y componentes de MONARC.	Fallos de servicio, inestabilidad del entorno o pérdida de compatibilidad.	No alterar la distribución ni la configuración base del sistema operativo invitado.
Asignación de CPU	≥ 2 vCPU	Garantizar capacidad mínima para la ejecución fluida de la interfaz web y procesos internos.	Lentitud en la navegación y posibles bloqueos durante cálculos de riesgo.	Mantener la asignación mínima definida durante toda la fase.
Asignación de memoria RAM	≥ 4 GB	Permitir la operación simultánea de servicios web, base de datos y dashboard sin degradación funcional.	Interrupciones del servicio o cierres inesperados de la aplicación.	No reducir la memoria asignada una vez iniciado el análisis.
Almacenamiento virtual	Disco virtual persistente (≥ 40 GB)	Asegurar almacenamiento suficiente para análisis, catálogos, reportes y registros históricos.	Pérdida de información o imposibilidad de guardar avances del análisis.	Uso exclusivo de disco persistente; no ejecutar en modo "live" o temporal.
Configuración de red	NAT o Adaptador Puente (según escenario local)	Permitir acceso controlado al Front Office desde navegador web del host.	Inaccesibilidad a la interfaz de MONARC o conflictos de conectividad.	Definir y mantener un único modo de red durante toda la Fase III.
Acceso a la aplicación	URL local (IP/host de la VM) vía navegador web	Facilitar el acceso operativo al Front Office sin dependencias externas.	Interrupción del flujo metodológico por falta de acceso a la herramienta.	Verificación de acceso previo a cualquier parametrización o análisis.
Mecanismo de autenticación	Credenciales locales (usuario/contraseña)	Controlar el acceso a la instancia y la integridad del análisis.	Acceso no autorizado o alteración de la información registrada.	Cambio de credenciales por defecto antes de iniciar la instrumentación.
Idioma del análisis	Definido al crear el análisis y bloqueado	Garantizar coherencia lingüística en activos, catálogos y reportes generados.	Imposibilidad de reutilizar bibliotecas o inconsistencias semánticas en los datos.	No modificar el idioma tras la creación del análisis base.
Modelo de análisis inicial	Blank Model o Cases Model	Establecer la estructura base para el inventario de activos y riesgos.	Arrastre de configuraciones no controladas o incompatibles con la	Seleccionar el modelo antes de configurar escalas y catálogos.

Tabla G.1.6-1. Checklist metodológico de verificación del entorno (condición "listo para instrumentar").

Ítem de verificación	Criterio de aceptación	Método de verificación (cómo se comprueba, sin captura)	Responsable (rol)	Evidencia esperada en H.1
Acceso a Front Office	Autenticación exitosa y navegación operativa en la interfaz de análisis.	Inicio de sesión con credenciales válidas y carga completa de la interfaz.	Analista de riesgos	Registro de acceso y metadatos de sesión.
Acceso a Back Office	Disponibilidad del módulo de administración para gestión técnica.	Autenticación con rol autorizado y acceso al panel administrativo.	Administrador de sistemas	Registro de acceso administrativo.
Servicios de la aplicación activos	Servicios web y base de datos operativos.	Verificación de respuesta de la URL de la instancia y estabilidad de sesión.	Administrador de sistemas	Registro de estado de servicios.
Coherencia de versión de MONARC	MONARC v2.13.x con commit 6d10eba.	Revisión de la información de versión desde la interfaz o configuración del sistema.	Administrador de sistemas	Declaración técnica de versión.
Configuración de virtualización	VM ejecutándose en Oracle VM VirtualBox con recursos asignados según parámetros mínimos.	Revisión de la configuración de la VM en el gestor de VirtualBox.	Administrador de sistemas	Tabla de parámetros de la VM.
Configuración de red definida	Conectividad estable entre anfitrión y VM	Comprobación de resolución de la URL	Administrador de red	Registro de configuración de red.

	mediante el modo de red adoptado.	interna y estabilidad de conexión.		
Persistencia de datos	Capacidad de guardar y recuperar cambios del análisis.	Ejecución de operación de guardado y recarga de sesión.	Analista de riesgos	Registro de persistencia del análisis.
Idioma del análisis	Idioma definido antes de la creación del análisis y bloqueado posteriormente.	Verificación del campo de idioma en la creación del análisis.	Analista de riesgos	Metadatos del análisis base.
Disponibilidad de modelo base	Modelos "Blank" o "Cases" disponibles para inicialización.	Acceso al asistente de creación de análisis y selección de modelo.	Analista de riesgos	Registro de inicialización del análisis.
Snapshot base creado	Existencia de un punto de restauración previo a la instrumentación.	Revisión del historial de instantáneas de la VM en VirtualBox.	Administrador de sistemas	Registro del snapshot base.
Seguridad de acceso	Credenciales de prueba activas y control de sesión habilitado.	Ejecución del ciclo completo de autenticación y cierre de sesión.	Analista de riesgos	Registro de configuración de cuenta.
Integración MOSP (si aplica)	Conectividad configurada para descarga de objetos de seguridad.	Validación de credenciales de integración y prueba de conexión.	Analista de riesgos	Registro de configuración MOSP.

Con el fin de declarar el análisis "listo para instrumentar" antes de avanzar a la configuración de criterios de evaluación (G.3), se aplicó un checklist metodológico de consistencia como criterio de aceptación del análisis base. Este checklist verifica condiciones mínimas de coherencia y completitud (p. ej., idioma fijado, alcance definido, nomenclatura aplicada, metadatos mínimos

registrados y mapeo inicial de contexto establecido), de modo que la unidad de trabajo quede estable y preparada para el diligenciamiento y configuración posterior sin reprocesos.

Tabla G.2.5-1. Checklist metodológico de consistencia del análisis base (criterio de aceptación)

Ítem de verificación	Condición de cumplimiento	Evidencia esperada (tipo, no contenido)	Momento de verificación (Etapa 1 / previo a Etapa 2)	Observaciones
Fijación del idioma del análisis	Idioma seleccionado y bloqueado en la creación del análisis, independiente del idioma de la interfaz.	Metadato de configuración del análisis.	Etapa 1	Parámetro crítico para la compatibilidad de activos y catálogos.
Definición del alcance técnico	Síntesis del contexto registrada en el subpaso 1.1 del establecimiento del contexto.	Campo narrativo persistente vinculado al análisis.	Etapa 1	Delimita el análisis como unidad de instrumentación.
Aplicación de nomenclatura	Identificador único y representativo consignado en el campo "Name".	Identificador visible en la cabecera del análisis.	Etapa 1	Facilita la identificabilidad y búsqueda del artefacto.
Registro de metadatos mínimos	Nombre, descripción e idioma diligenciados conforme a las reglas definidas.	Formulario de metadatos del Front Office.	Etapa 1	Base para la trazabilidad institucional y documental.
Consistencia terminológica mínima	Coherencia lingüística entre el modelo base seleccionado (Blank/Cases) y el idioma del análisis.	Registro de creación del análisis.	Previo a Etapa 2	Evita incompatibilidades en la carga de activos.
Delimitación como unidad operativa	Activación de la barra de progreso con validación de los subpasos 1.1 a 1.3 mediante *tick boxes*.	Estado de validación de pasos en el Front Office.	Previo a Etapa 2	Condición necesaria para habilitar la configuración de criterios de evaluación en G.3.

G.8.1 Restricciones que afectan instrumentación (R#)

Se identificaron restricciones asociadas a decisiones de diseño de la herramienta y del entorno de despliegue que afectan la instrumentación del ciclo de gestión de riesgos. Para cada restricción se definieron: (i) el componente del flujo afectado, (ii) el instrumento compensatorio aplicable y (iii) el mecanismo de registro de trazabilidad.

Tabla G.8.1-1. Restricciones operativas (R#) y compensaciones metodológicas

R#	Restricción operativa	Impacto sobre la instrumentación (etapa/artefacto afectado)	Instrumento compensatorio	Registro de trazabilidad (dónde se deja constancia)	Observaciones
R1	Idioma del análisis no editable una vez creado.	Etapa 1 (creación del análisis) y consistencia terminológica en catálogos/reportes.	Regla previa de creación del análisis (G.2.2) y checklist de consistencia (G.2.5).	Metadatos del análisis (nombre, idioma) y registro de creación del análisis.	Si se requiere cambio de idioma, se creó un nuevo análisis y se migró la configuración aplicable.
R2	Cambios en escalas sin versionado histórico dentro de MONARC.	Etapa 2 (escalas/umbrales): un ajuste afecta retroactivamente la valoración.	Regla de congelamiento/versionado de criterios (G.3.6).	Tabla externa de versionado de criterios y anotación de versión en metadatos del análisis.	Se evitó modificar escalas tras iniciar el modelado y la evaluación.
R3	Herencia de impactos con flexibilidad limitada para excepciones granulares.	Etapa 3 (activos/dependencias): posible sobre/infra-valoración en activos secundarios específicos.	Regla de modelado de dependencias y criterio de justificación metodológica (G.4.3–G.4.4).	Notas de modelado (observaciones del activo) y criterios de consistencia C–I–D.	Cuando fue necesario, se separaron activos o se ajustó la relación de dependencia para

					preservar coherencia.
R4	El riesgo no se calcula si falta un parámetro obligatorio (p. ej., probabilidad, qualification o impacto heredado).	Etapas 2–4: bloquea evaluación, tratamiento o reportes.	Criterios de control por etapa (G.6.3) y checklist end-to-end (G.6.7).	Registro de verificación por etapa y checklist de cierre.	Se verificó completitud mínima antes de avanzar a la siguiente etapa.
R5	El tratamiento tipo *Reduce* exige recomendación vinculada y vulnerabilidad residual definida.	Etapa 4 (tratamiento): no permite cierre del riesgo reducido sin residual.	Catálogo mínimo de recomendaciones/controles (G.5.3) y regla de tratamiento (G.6.5).	Campos de tratamiento (tipo), recomendación asociada y residual en el riesgo.	Si no fue posible definir residual bajo *Reduce*, se aplicó el tipo de tratamiento correspondiente según la decisión metodológica.
R6	El valor residual se actualiza cuando se implementan todas las recomendaciones asociadas (lógica global).	Etapa 4 (seguimiento): avance parcial no refleja reducción numérica inmediata.	Regla de seguimiento (G.6.6) y matriz externa de avance (%).	Historial de implementación en MONARC y registro complementario de avance.	Se mantuvo trazabilidad del estado por recomendación para evitar interpretaciones erróneas del progreso.
R7	Gestión limitada de costos, plazos y dependencias complejas entre medidas.	Priorización y planeación fuera del motor de riesgo de MONARC.	Matriz externa de priorización/planeación (costo–esfuerzo–impacto).	Archivo complementario de priorización y referencia cruzada con el plan de tratamiento.	La priorización se documentó como complemento metodológico sin alterar el registro de riesgos en MONARC.

Anexo: ; las evidencias reproducibles mediante capturas, exportaciones y registros técnicos se consolidan en el Anexo: Evidencias técnicas y artefactos reproducibles de instrumentación, que incluye tablas completas, checklists diligenciados y archivos exportados.

3.3.1 Resultados de la Etapa 0: Despliegue técnico y condiciones mínimas de entorno

Se habilitó un entorno reproducible de MONARC utilizando una VM en VirtualBox, seleccionada por su viabilidad en contextos pyme con recursos limitados (sin necesidad de servidores dedicados). La VM se configuró con Ubuntu Server 22.04 LTS como sistema operativo base, cumpliendo los requisitos mínimos de MONARC (stack LAMP: Apache 2.4, MySQL 8.0, PHP 8.1). Se instaló MONARC versión 2.12.3 (última estable disponible al momento de la ejecución, descargada del repositorio oficial en GitHub).

Los parámetros técnicos mínimos documentados incluyeron:

- Recursos asignados: 2 GB RAM, 1 núcleo CPU, 20 GB disco (suficiente para análisis base sin escalamiento).
- Configuración de red: Modo NAT con reglas de reenvío de puertos para acceso desde el host local vía navegador (puerto 8080 → 80) y servicios adicionales (5000 → 5000, 2222 → 22).
- Dependencias instaladas: Composer, Node.js y paquetes PHP requeridos (detalle en Anexo H).

Se creó un snapshot inicial para restauración, y se verificó la estabilidad mediante pruebas de acceso y carga de interfaz. No se registraron fallos críticos durante el despliegue. La verificación del entorno se realizó mediante un checklist diligenciado (ver Tabla 3.3.1-1), confirmando accesos, servicios y persistencia de datos. Figura 3.3.1-1 muestra la configuración de red de la VM en modo NAT con reenvío de puertos del Front Office.

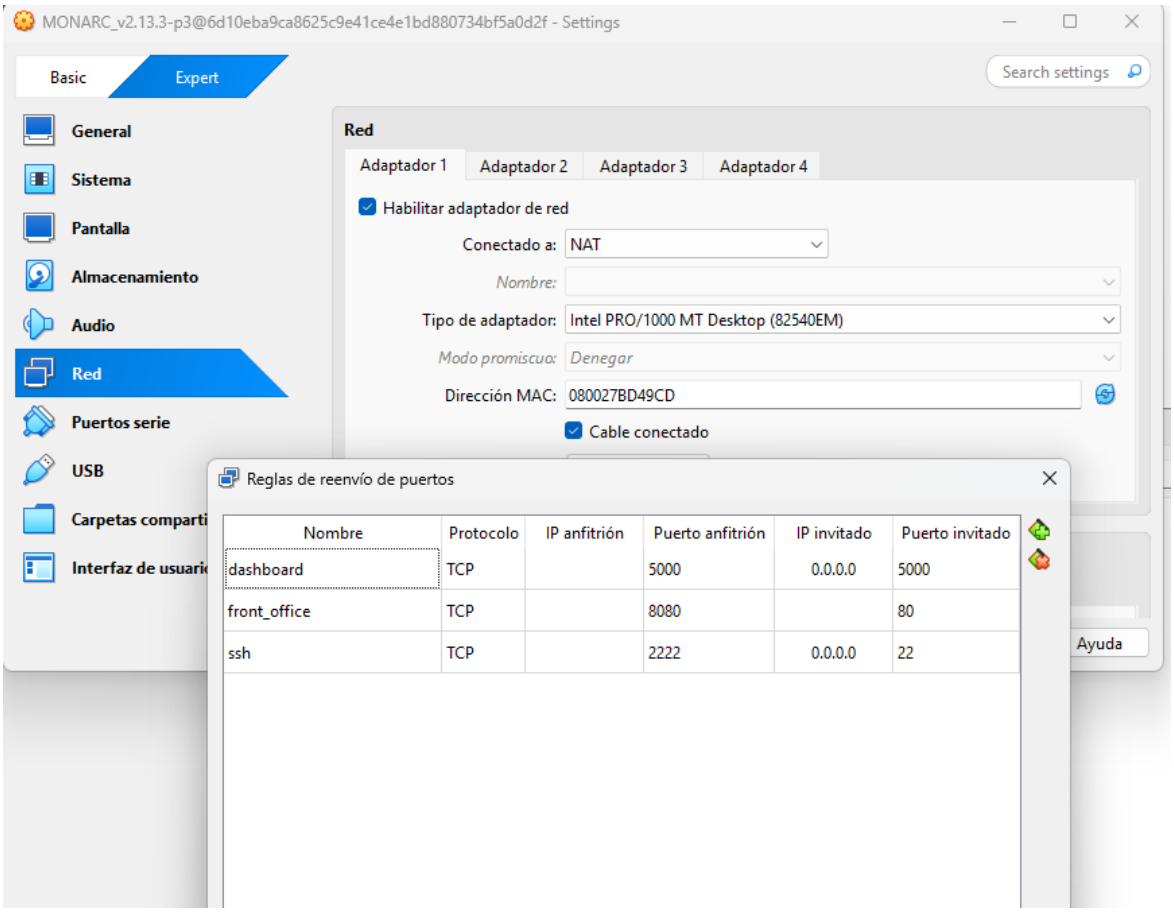
Tabla 3.3.1-1: Checklist diligenciado para la verificación del entorno de despliegue de MONARC

Ítem	Criterio	Estado	Evidencia (Anexo H)
Acceso Front Office	Autenticación exitosa	OK	H1_Acceso_Login.png
Coherencia versión	v2.13.x	OK	Tabla H.1.1-1

Ítem	Criterio	Estado	Evidencia (Anexo H)
Snapshot base	Punto de restauración	OK	H1_Snapshot_Base.png

Fuente: Elaboración propia a partir de la verificación técnica del entorno de despliegue de MONARC, con evidencias documentadas en el Anexo H.

Figura 3.3.1-1: Configuración de red de la VM de MONARC



Fuente: Captura de pantalla propia de la configuración NAT y reglas de reenvío de puertos de la máquina virtual de MONARC en VirtualBox.

3.3.2 Resultados de la Etapa 1: Creación del análisis base y parametrización inicial del contexto

Se creó un análisis base denominado "Análisis PyME Servicios Colombia" como unidad de trabajo en MONARC. Se parametrizó el contexto inicial del análisis, incluyendo:

a. Alcance: Análisis de riesgos de seguridad de la información para activos críticos de PyME del sector servicios (≤100 empleados, ingresos ≤$5000M COP/año).
b. Idioma: español (idioma de la interfaz) con la particularidad de controlar el idioma de los menús, botones y opciones del programa en sí, luego se dejó idioma inglés (idioma del análisis de riesgo) en función de determinar el idioma de los módulos básicos habilitados (activos, amenazas, vulnerabilidades, entre otros).
c. Metodología aplicada: Síntesis integradora OCTAVE-S + ISO 27005 + NIST 800-30 + MAGERIT + EBIOS RM (según Producto d, Fase I).

Se identificaron los módulos equivalentes en MONARC para representar los componentes del contexto metodológico definidos en la propuesta (ver Tabla 3.3.2-1).

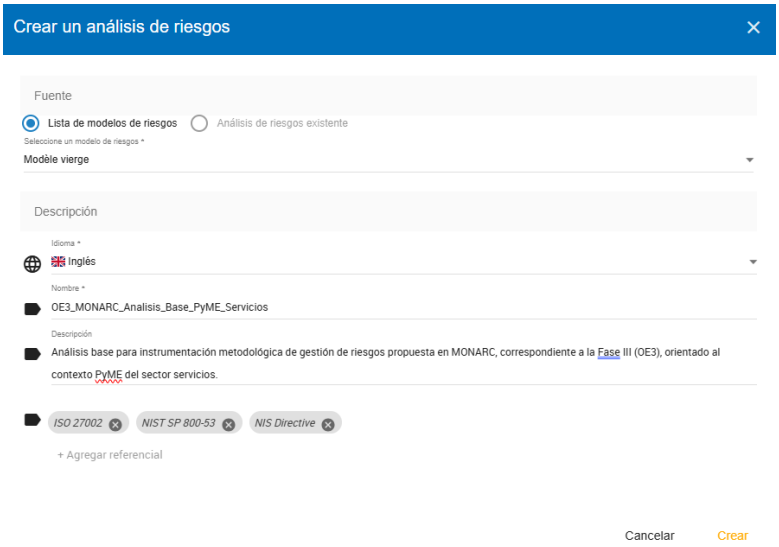
Tabla 3.3.2-1: Mapeo entre componentes metodológicos de la propuesta y módulos equivalentes de MONARC

Componente Metodológico (Fase I)	Módulo MONARC Equivalente	Observación Técnica
Definición de contexto y alcance (ISO 27005)	Step 0 → Context of Risk Analysis	Campo narrativo para alcance
Activos críticos (OCTAVE-S ≤5)	Step 1 → Primary Assets	Categoría "Primary" en MONARC
Activos de soporte (MAGERIT esencial↔soporte)	Step 1 → Secondary Assets	Jerarquía de dependencias
Amenazas (NIST 800-30 fuentes/eventos)	Knowledge Base → Threats	Catálogo importable/editable
Vulnerabilidades (NIST 800-30 condiciones predisponentes)	Knowledge Base → Vulnerabilities	Catálogo importable/editable
Controles (ISO 27001 Anexo A, NIST 800-53)	Knowledge Base → Referentials + Recommendation Sets	Referenciales + recomendaciones operativas

Fuente: elaboración propia a partir de la metodología propuesta y de la revisión funcional de MONARC documentada en el Anexo H.

La Figura 3.3.2-1 muestra la creación de la unidad de trabajo en MONARC. Se seleccionó la opción *Lista de modelos de riesgos* con el modelo *Modèle vierge*. El idioma elegido fue inglés. El nombre del análisis fue “OE3_MONARC_Analisis_Base_PyME_Servicios”. En la descripción se indicó que corresponde a la Fase III (OE3), orientado al sector servicios. Se asociaron los referenciales ISO 27002, NIST SP 800-53 y NIS Directive. La interfaz pertenece a la etapa inicial del análisis.

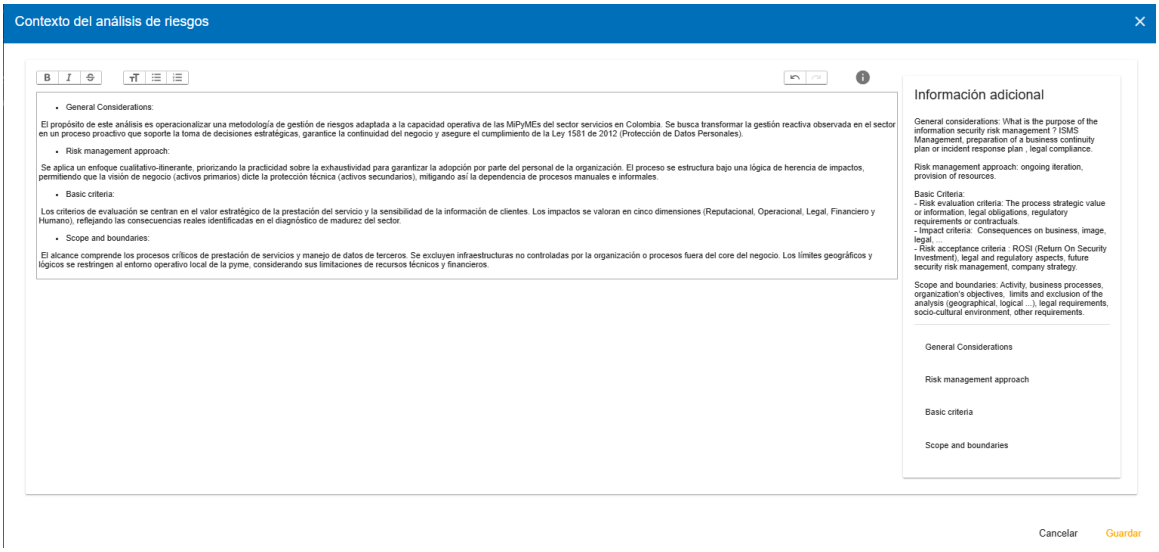
Figura 3.3.2-1: Creación del análisis de riesgos



Fuente: captura de pantalla propia de la creación del análisis base de riesgos en MONARC.

En esta fase, se parametrizó el contexto inicial del análisis para alinear MONARC con la metodología híbrida definida en la Fase I. La configuración se orientó en garantizar la trazabilidad entre los hallazgos del diagnóstico, la definición del alcance y la ejecución técnica del análisis de riesgos. Como se observa en la Figura 3.3.2-2, el alcance se delimitó a los activos críticos que sustentan la continuidad operativa y el cumplimiento legal en una pyme del sector servicios.

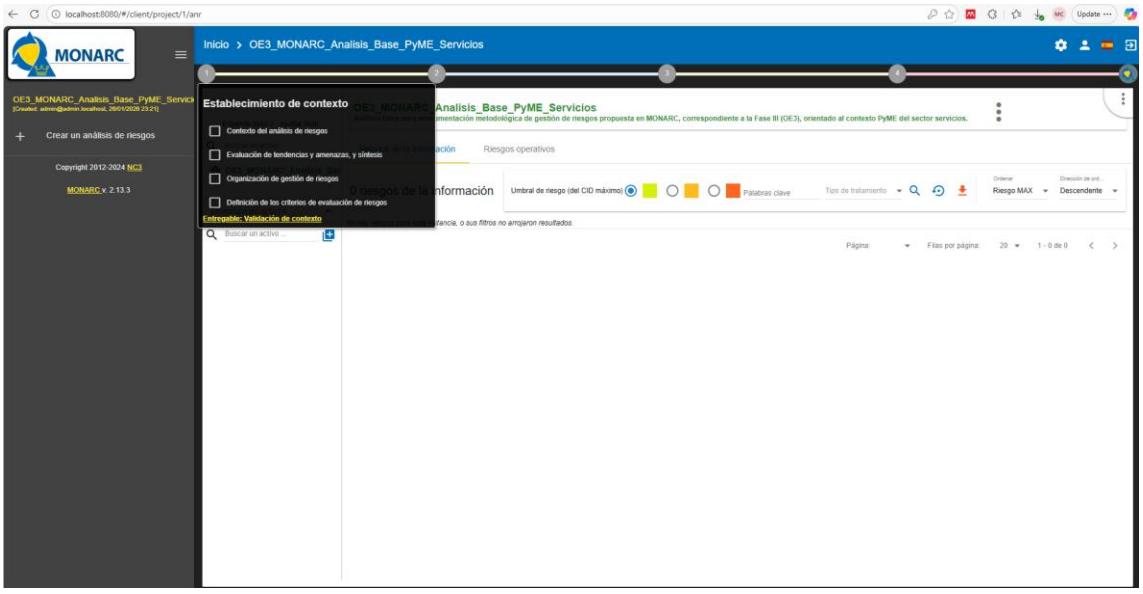
Figura 3.3.2-2: Parametrización del contexto inicial del análisis de riesgos en MONARC



Fuente: captura de pantalla propia de la parametrización del contexto inicial del análisis de riesgos en MONARC.

La Figura 3.3.2-3 muestra el panel principal de MONARC después de la creación del análisis base. En la interfaz se observa el nombre del análisis activo, y la ubicación del proceso en la etapa de **Establecimiento de contexto**. Esta pantalla permite verificar que el análisis fue creado correctamente y que la herramienta quedó lista para iniciar el registro de información, riesgos operativos y riesgos de la información asociados al caso de estudio.

Figura 3.3.2-3: Dashboard inicial del análisis base en la etapa de establecimiento de contexto



Fuente: captura de pantalla propia del panel inicial del análisis base creado en MONARC.

3.3.3 Resultados de la Etapa 2: Configuración de criterios de evaluación del riesgo

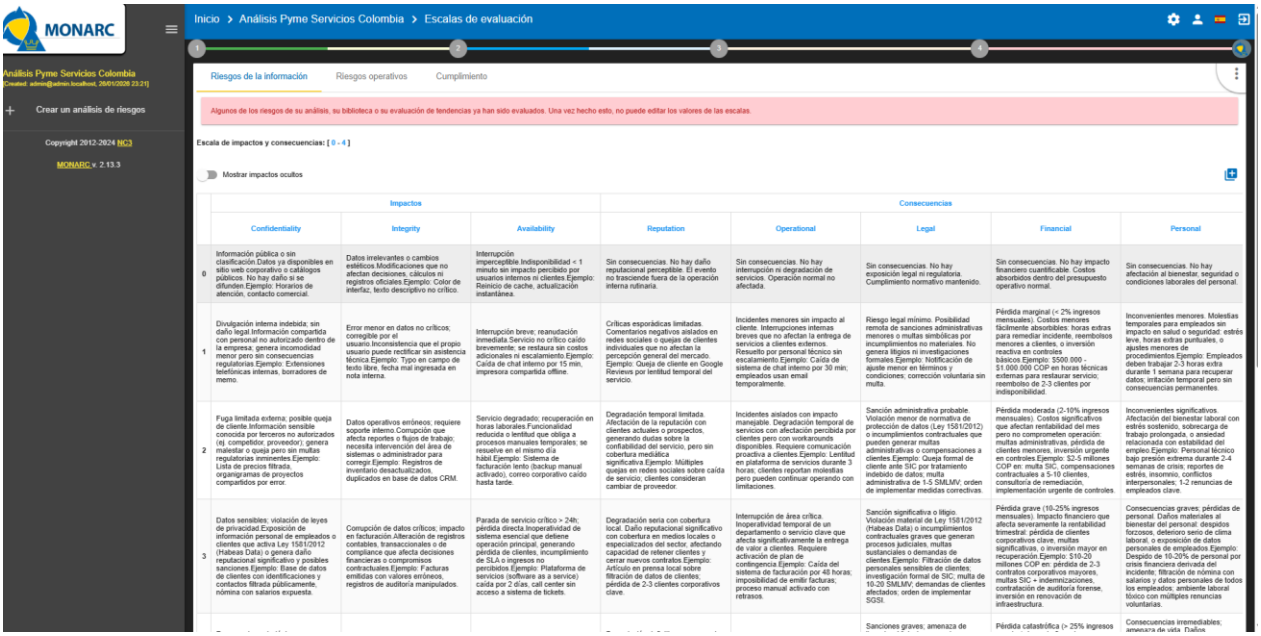
Se parametrizaron criterios mínimos para cálculo del riesgo, alineados con el enfoque híbrido definido en la metodología, principalmente a partir de OCTAVE-S e ISO/IEC 27005. Escalas implementadas: Impacto C-I-D (0-4 cualitativo), Probabilidad (0-4 basada en frecuencia), Vulnerabilidad (0-4 explotabilidad). Umbrales: Riesgo residual <2 aceptable, >3 prioritario.

Las Figura 3.3.3-1, Figura 3.3.3-2, Figura 3.3.3-3 corresponden al subpaso 1.4 “Definición de los criterios de evaluación de riesgos”. Se configuró una escala de impactos y consecuencias para riesgos de la información, que incluyó ocho dimensiones: confidencialidad, integridad, disponibilidad, reputación, operacional, legal, financiera y personal, cada una con niveles del 0 al 4.

Se definió una escala de probabilidad con cinco niveles (0 a 4) y una escala de vulnerabilidad con seis niveles (0 a 5), con descripciones para cada valor. También se estableció el umbral de aceptación de riesgos de la información, con un valor crítico de 30.

Para los riesgos operativos, se parametrizó una escala de impactos con cinco dimensiones: reputación, operacional, legal, financiera y personal, con niveles del 0 al 4. Se repitió la escala de probabilidad y se definió un umbral de aceptación más estricto, con valor crítico en 6. Estas Configuraciones permiten calcular automáticamente los niveles de riesgo de información ($R = I * A * V$), los niveles de riesgos operativos ($R = I * P$) y establecer qué escenarios son aceptables o requieren tratamiento.

Figura 3.3.3-1: Escala de impactos y consecuencias CID para riesgos de la información en MONARC

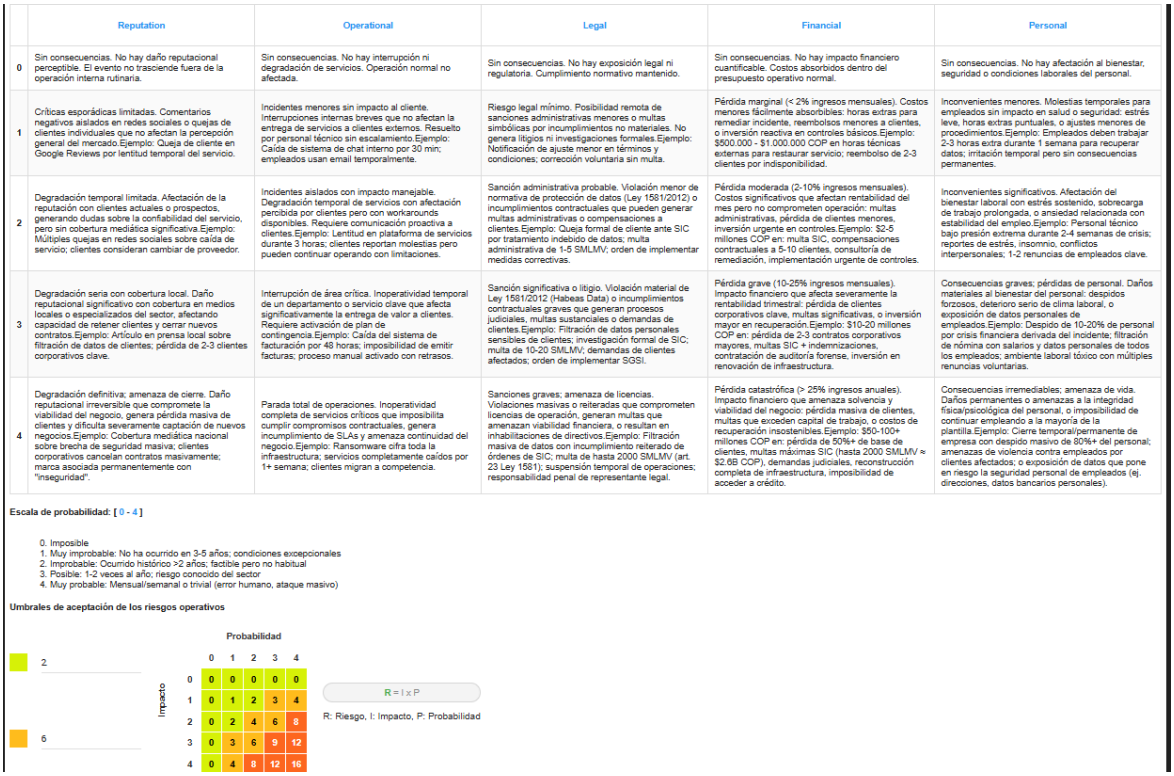


Fuente: captura de pantalla propia de la parametrización de escalas de impacto y consecuencias para riesgos de la información en MONARC.

Figura 3.3.3-2: Escala de probabilidad, vulnerabilidad y umbrales de aceptación para riesgos de la información en MONARC

Fuente: captura de pantalla propia de la parametrización de las escalas de probabilidad, vulnerabilidad y umbrales de aceptación para riesgos de la información en MONARC.

Figura 3.3.3-3: Escala de impactos y umbrales de aceptación para riesgos operativos en MONARC



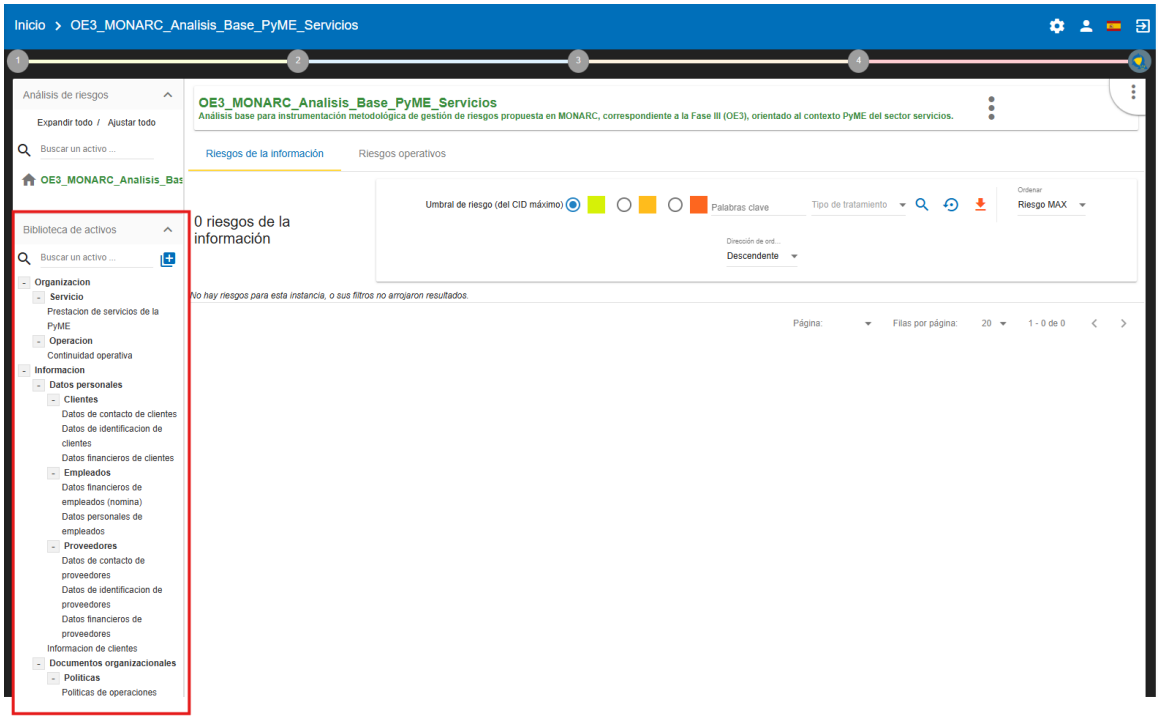
	Reputation	Operational	Legal	Financial	Personal
0	Sin consecuencias. No hay daño reputacional perceptible. El evento no trasciende fuera de la operación interna rutinaria.	Sin consecuencias. No hay interrupción ni degradación de servicios. Operación normal no afectada.	Sin consecuencias. No hay exposición legal ni regulatoria. Cumplimiento normativo mantenido.	Sin consecuencias. No hay impacto financiero cuantificable. Costos absorbidos dentro del presupuesto operativo normal.	Sin consecuencias. No hay afectación al bienestar, seguridad o condiciones laborales del personal.
1	Críticas esporádicas limitadas. Comentarios negativos aislados en redes sociales o quejas de clientes individuales que no afectan la percepción general del mercado.Ejemplo: Queja de cliente en Google Reviews por lentitud temporal del servicio.	Incidentes menores sin impacto al cliente. Interrupciones internas breves que no afectan la entrega de servicios a clientes externos. Resuelto por personal técnico sin escalamiento.Ejemplo: Caída de sistema de chat interno por 30 min; empleados usan email temporalmente.	Riesgo legal mínimo. Posibilidad remota de sanciones administrativas menores o multas simbólicas por incumplimientos no materiales. No genera litigios ni investigaciones formales.Ejemplo: Notificación de ajuste menor en términos y condiciones; corrección voluntaria sin multa.	Pérdida marginal (< 2% ingresos mensuales). Costos menores fácilmente absorbibles: horas extras para remediar incidente, reembolsos menores a clientes, o inversión reactiva en controles básicos.Ejemplo: $500.000 - $1.000.000 COP en horas técnicas externas para restaurar servicio; reembolso de 2-3 clientes por indisponibilidad.	Inconvenientes menores. Molestias temporales para empleados sin impacto en salud o seguridad: estrés leve, horas extras puntuales, o ajustes menores de procedimientos.Ejemplo: Empleados deben trabajar 2-3 horas extra durante 1 semana para recuperar datos; irritación temporal pero sin consecuencias permanentes.
2	Degradación temporal limitada. Afectación de la reputación con clientes actuales o prospectos, generando dudas sobre la confiabilidad del servicio, pero sin cobertura mediática significativa.Ejemplo: Múltiples quejas en redes sociales sobre caída de servicio; clientes consideran cambiar de proveedor.	Incidentes aislados con impacto manejable. Degradación temporal de servicios con afectación percibida por clientes pero con workarounds disponibles. Requiere comunicación proactiva a clientes.Ejemplo: Lentitud en plataforma de servicios durante 3 horas; clientes reportan molestias pero pueden continuar operando con limitaciones.	Sanción administrativa probable. Violación menor de normativa de protección de datos (Ley 1581/2012) o incumplimientos contractuales que pueden generar multas administrativas o compensaciones a clientes.Ejemplo: Queja formal de cliente ante SIC por tratamiento indebido de datos; multa administrativa de 1-5 SMLMV; orden de implementar medidas correctivas.	Pérdida moderada (2-10% ingresos mensuales). Costos significativos que afectan rentabilidad del mes pero no comprometen operación: multas administrativas, pérdida de clientes menores, inversión urgente en controles.Ejemplo: $2-5 millones COP en: multa SIC, compensaciones contractuales a 5-10 clientes, consultoría de remediación, implementación urgente de controles.	Inconvenientes significativos. Afectación del bienestar laboral con estrés sostenido, sobrecarga de trabajo prolongada, o ansiedad relacionada con estabilidad del empleo.Ejemplo: Personal técnico bajo presión extrema durante 2-4 semanas de crisis; reportes de estrés, insomnio, conflictos interpersonales; 1-2 renuncias de empleados clave.
3	Degradación seria con cobertura local. Daño reputacional significativo con cobertura en medios locales o especializados del sector, afectando capacidad de retener clientes y cerrar nuevos contratos.Ejemplo: Artículo en prensa local sobre filtración de datos de clientes; pérdida de 2-3 clientes corporativos clave.	Interrupción de área crítica. Inoperatividad temporal de un departamento o servicio clave que afecta significativamente la entrega de valor a clientes. Requiere activación de plan de contingencia.Ejemplo: Caída del sistema de facturación por 48 horas; imposibilidad de emitir facturas; proceso manual activado con retrasos.	Sanción significativa o litigio. Violación material de Ley 1581/2012 (Habeas Data) o incumplimientos contractuales graves que generan procesos judiciales, multas sustanciales o demandas de clientes.Ejemplo: Filtración de datos personales sensibles de clientes; investigación formal de SIC; multa de 10-20 SMLMV; demandas de clientes afectados; orden de implementar SGSI.	Pérdida grave (10-25% ingresos mensuales). Impacto financiero que afecta severamente la rentabilidad trimestral: pérdida de clientes corporativos clave, multas significativas, o inversión mayor en recuperación.Ejemplo: $10-20 millones COP en: pérdida de 2-3 contratos corporativos mayores, multas SIC + indemnizaciones, contratación de auditoría forense, inversión en renovación de infraestructura.	Consecuencias graves; pérdidas de personal. Daños materiales al bienestar del personal: despidos forzosos, deterioro serio de clima laboral, o exposición de datos personales de empleados.Ejemplo: Despido de 10-20% de personal por crisis financiera derivada del incidente; filtración de nómina con salarios y datos personales de todos los empleados; ambiente laboral tóxico con múltiples renuncias voluntarias.
4	Degradación definitiva; amenaza de cierre. Daño reputacional irreversible que compromete la viabilidad del negocio, genera pérdida masiva de clientes y dificulta severamente captación de nuevos negocios.Ejemplo: Cobertura mediática nacional sobre brecha de seguridad masiva; clientes corporativos cancelan contratos masivamente; marca asociada permanentemente con "inseguridad".	Parada total de operaciones. Inoperatividad completa de servicios críticos que imposibilita cumplir compromisos contractuales, genera incumplimiento de SLAs y amenaza continuidad del negocio.Ejemplo: Ransomware cifra toda la infraestructura; servicios completamente caídos por 1+ semana; clientes migran a competencia.	Sanciones graves; amenaza de licencias. Violaciones masivas o reiteradas que comprometen licencias de operación, generan multas que amenazan viabilidad financiera, o resultan en inhabilitaciones de directivos.Ejemplo: Filtración masiva de datos con incumplimiento reiterado de órdenes de SIC; multa de hasta 2000 SMLMV (art. 23 Ley 1581); suspensión temporal de operaciones; responsabilidad penal de representante legal.	Pérdida catastrófica (> 25% ingresos anuales). Impacto financiero que amenaza solvencia y viabilidad del negocio: pérdida masiva de clientes, multas que exceden capital de trabajo, o costos de recuperación insostenibles.Ejemplo: $50-100+ millones COP en: pérdida de 50%+ de base de clientes, multas máximas SIC (hasta 2000 SMLMV ≈ $2.6B COP), demandas judiciales, reconstrucción completa de infraestructura, imposibilidad de acceder a crédito.	Consecuencias irremediables; amenaza de vida. Daños permanentes o amenazas a la integridad física/psicológica del personal, o imposibilidad de continuar empleando a la mayoría de la plantilla.Ejemplo: Cierre temporal/permanente de empresa con despido masivo de 80%+ del personal; amenazas de violencia contra empleados por clientes afectados; o exposición de datos que pone en riesgo la seguridad personal de empleados (ej. direcciones, datos bancarios personales).

Fuente: captura de pantalla propia de la parametrización de la escala de impactos y umbrales de aceptación para riesgos operativos en MONARC.

3.3.4 Resultados de la Etapa 3: Modelado jerárquico de activos, dependencias y catálogos de análisis

La Figura 3.3.4-1 muestra la estructura jerárquica construida para el modelado de activos dentro de la herramienta. En el panel de navegación se observan categorías principales correspondientes a infraestructura tecnológica, aplicaciones y software, y recursos organizacionales. La biblioteca contiene activos secundarios organizados bajo clases reutilizables, cuyo detalle se presenta en el Anexo H. Asimismo, se evidencia la organización del árbol de activos en niveles primarios y secundarios, siguiendo la estructura requerida para el análisis de riesgos.

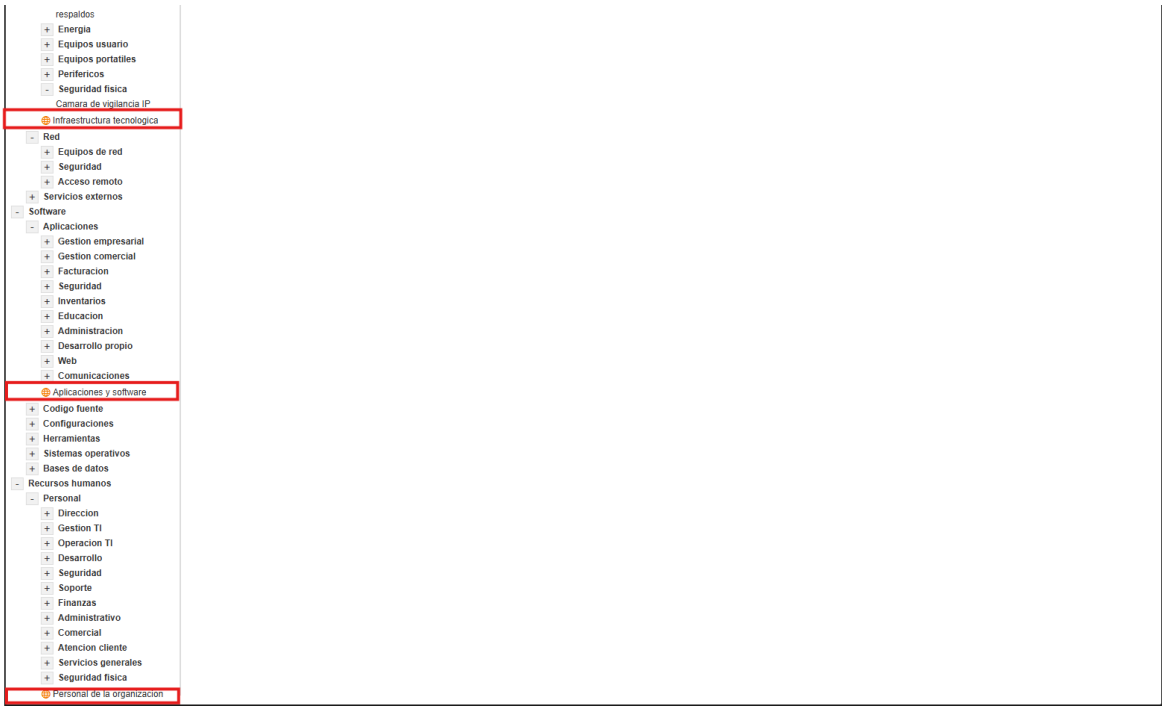
Figura 3.3.4-1: Biblioteca de activos de MONARC: Clasificación jerárquica de activos base disponibles para el análisis.



Fuente: captura de pantalla propia de la biblioteca de activos configurada en MONARC para el análisis de riesgos.

Posteriormente, la Figura 3.3.4-2 presenta el despliegue completo de las categorías y subcategorías reutilizadas disponibles en la biblioteca de activos de MONARC para el modelado técnico del análisis. En particular, se observan clases asociadas a hardware, software, red, código fuente y seguridad física. De este modo, se documenta la utilización de plantillas disponibles en la biblioteca interna de la herramienta para soportar la configuración del análisis.

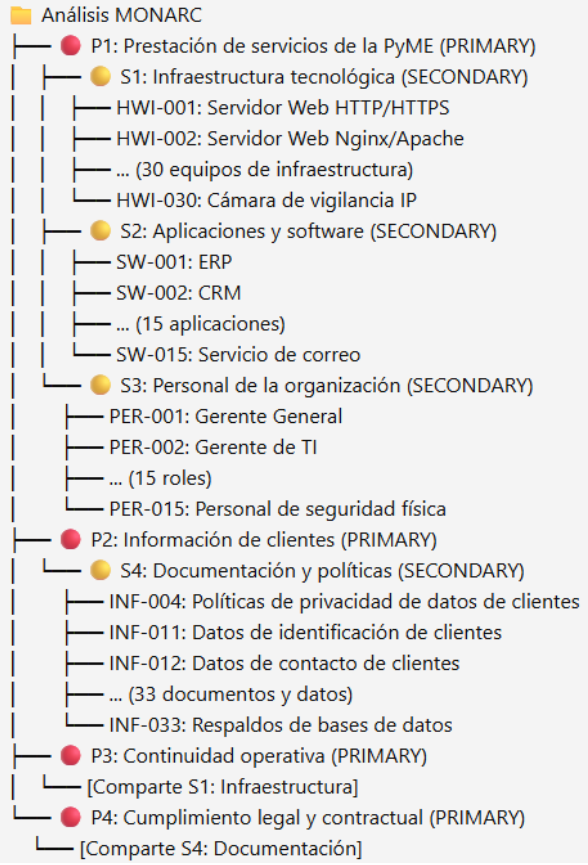
Figura 3.3.4-2: Despliegue completo de categorías en la biblioteca de activos: Recursos disponibles para modelado técnico.



Fuente: captura de pantalla propia de las categorías reutilizables disponibles en la biblioteca de activos de MONARC para el modelado técnico del análisis.

De igual manera, la Figura 3.3.4-3 respalda la vinculación entre activos primarios y secundarios configurada durante la etapa. Se identifican activos principales definidos como base del análisis, cada uno asociado a dependencias técnicas específicas. Esta estructura habilitó la propagación automática de impactos dentro del sistema de evaluación del riesgo.

Figura 3.3.4-3: Árbol de activos primarios y secundarios configurado en MONARC



Fuente: captura de pantalla propia del árbol de activos primarios y secundarios configurado en MONARC.

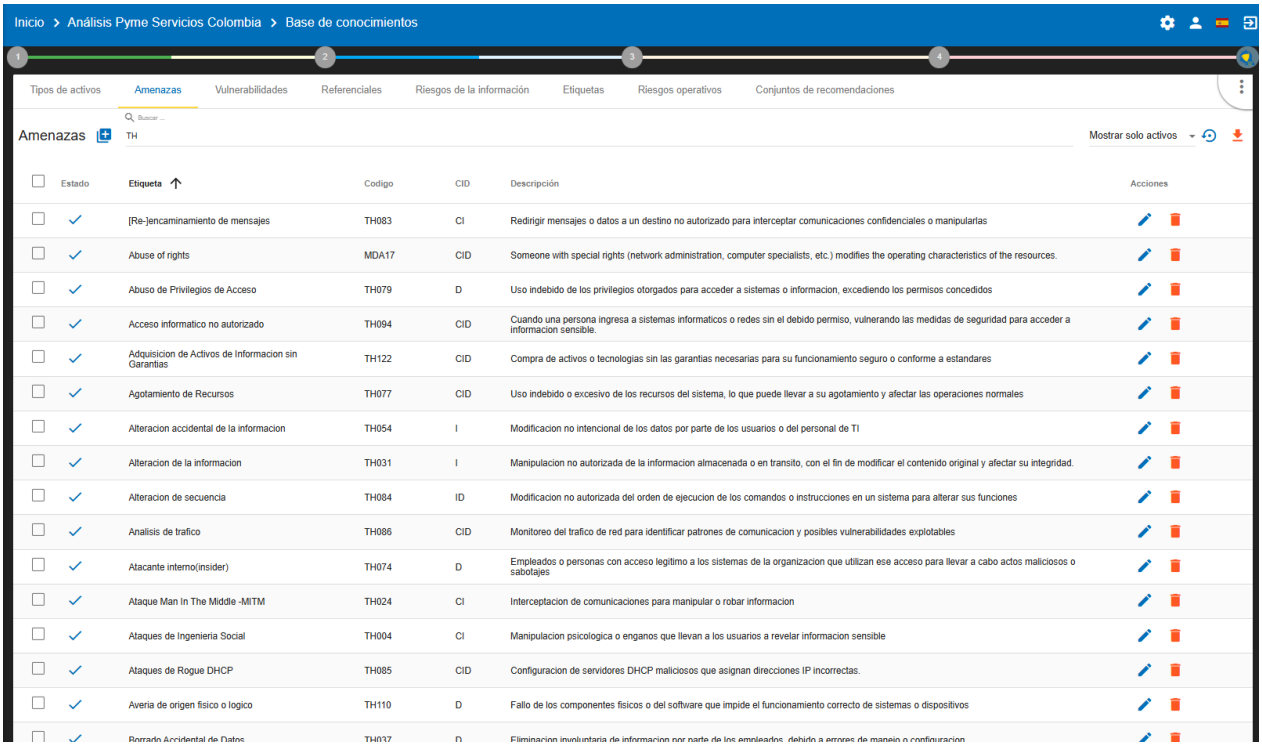
De manera complementaria, se configuraron catálogos funcionales de amenazas, vulnerabilidades y controles. Estos catálogos fueron adaptados al contexto de análisis mediante selección y activación de entradas disponibles en la herramienta. En consecuencia, se habilitó la generación de escenarios de riesgo durante la ejecución del flujo analítico.

Durante la configuración de la base de conocimientos para el análisis, se cargaron catálogos personalizados de amenazas, vulnerabilidades, controles y conjuntos de recomendaciones, adaptados al contexto pyme del sector servicios. Las Figura 3.3.4-4, Figura 3.3.4-5, Figura 3.3.4-6 presentadas, corresponden a una muestra representativa de cada uno de estos catálogos, ya integrados en MONARC.

En el caso de las amenazas, los registros se identifican mediante el prefijo TH###, como por ejemplo TH083 o TH079, lo que permite diferenciarlas de amenazas nativas del sistema. De igual forma, las

vulnerabilidades fueron organizadas bajo la nomenclatura VUL###, mientras que el referencial de controles se basó en el Anexo A de la ISO/IEC 27001. Cada conjunto de catálogos fue importado en formato CSV con nombres de archivo controlados para asegurar la trazabilidad. MONARC permite exportaciones que mezclan elementos nativos con los adaptados; sin embargo, el uso de códigos personalizados, etiquetas normalizadas y el registro sistemático de las acciones de importación/exportación documentadas en el Anexo H, garantizan la integridad del modelo y la replicabilidad del análisis.

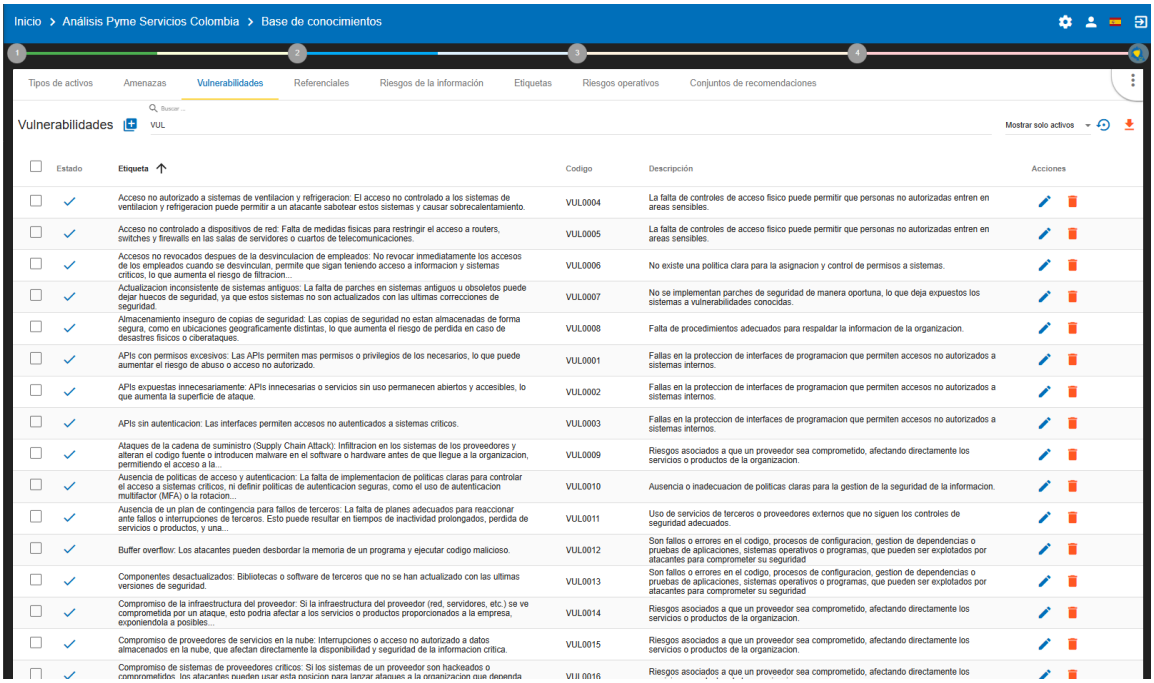
Figura 3.3.4-4: Catálogo personalizado de amenazas integrado en MONARC



Estado	Etiqueta	Codigo	CID	Descripción	Acciones
✓	[Re-]encaminamiento de mensajes	TH083	CI	Redirigir mensajes o datos a un destino no autorizado para interceptar comunicaciones confidenciales o manipularlas	
✓	Abuse of rights	MDA17	CID	Someone with special rights (network administration, computer specialists, etc.) modifies the operating characteristics of the resources.	
✓	Abuso de Privilegios de Acceso	TH079	D	Uso indebido de los privilegios otorgados para acceder a sistemas o informacion, excediendo los permisos concedidos	
✓	Acceso informatico no autorizado	TH094	CID	Cuando una persona ingresa a sistemas informaticos o redes sin el debido permiso, vulnerando las medidas de seguridad para acceder a informacion sensible.	
✓	Adquisicion de Activos de Informacion sin Garantias	TH122	CID	Compra de activos o tecnologias sin las garantias necesarias para su funcionamiento seguro o conforme a estandares	
✓	Agotamiento de Recursos	TH077	CID	Uso indebido o excesivo de los recursos del sistema, lo que puede llevar a su agotamiento y afectar las operaciones normales	
✓	Alteracion accidental de la informacion	TH054	I	Modificacion no intencional de los datos por parte de los usuarios o del personal de TI	
✓	Alteracion de la informacion	TH031	I	Manipulacion no autorizada de la informacion almacenada o en transito, con el fin de modificar el contenido original y afectar su integridad.	
✓	Alteracion de secuencia	TH084	ID	Modificacion no autorizada del orden de ejecucion de los comandos o instrucciones en un sistema para alterar sus funciones	
✓	Analisis de trafico	TH086	CID	Monitoreo del trafico de red para identificar patrones de comunicacion y posibles vulnerabilidades explotables	
✓	Atacante interno(insider)	TH074	D	Empleados o personas con acceso legitimo a los sistemas de la organizacion que utilizan ese acceso para llevar a cabo actos maliciosos o sabotajes	
✓	Ataque Man In The Middle -MITM	TH024	CI	Interceptacion de comunicaciones para manipular o robar informacion	
✓	Ataques de Ingenieria Social	TH004	CI	Manipulacion psicologica o enganos que llevan a los usuarios a revelar informacion sensible	
✓	Ataques de Rogue DHCP	TH085	CID	Configuracion de servidores DHCP maliciosos que asignan direcciones IP incorrectas.	
✓	Averia de origen fisico o logico	TH110	D	Fallo de los componentes fisicos o del software que impide el funcionamiento correcto de sistemas o dispositivos	
✓	Borrado Accidental de Datos	TH037	D	Eliminacion involuntaria de informacion por parte de los empleados, debido a errores de manejo o configuracion	

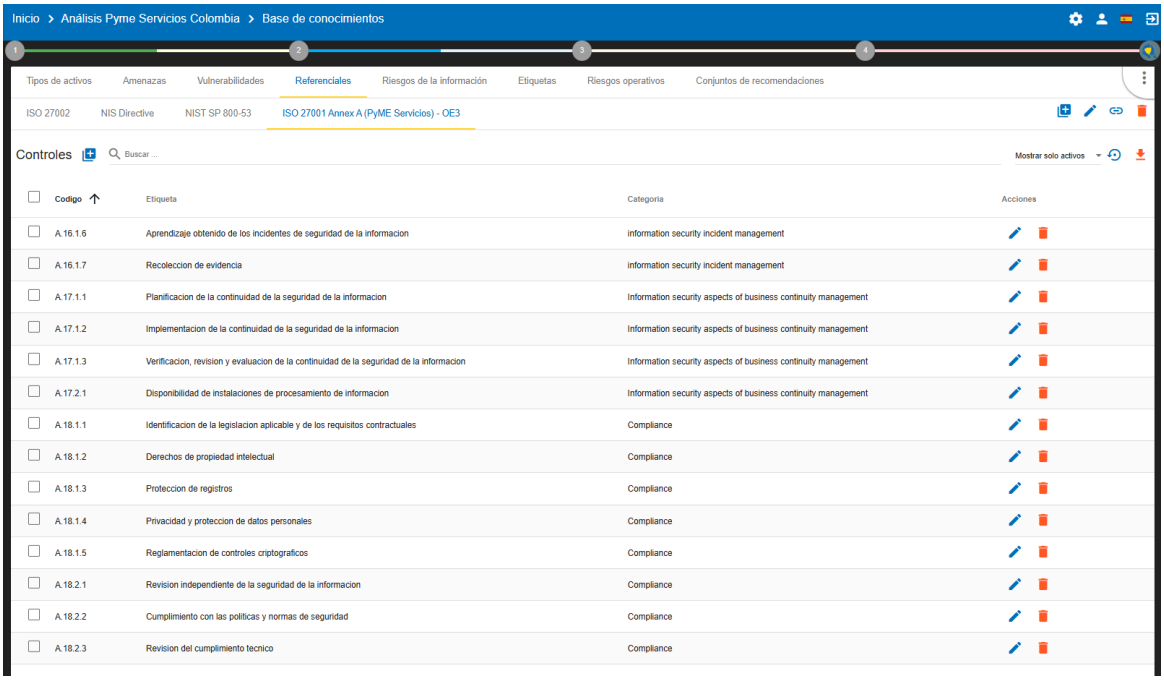
Fuente: captura de pantalla propia del catálogo personalizado de amenazas integrado en la base de conocimientos de MONARC.

Figura 3.3.4-5: Catálogo de vulnerabilidades personalizado en MONARC



Fuente: captura de pantalla propia del catálogo personalizado de vulnerabilidades integrado en la base de conocimientos de MONARC.

Figura 3.3.4-6: Referencial de controles ISO/IEC 27001 Anexo A cargado en MONARC

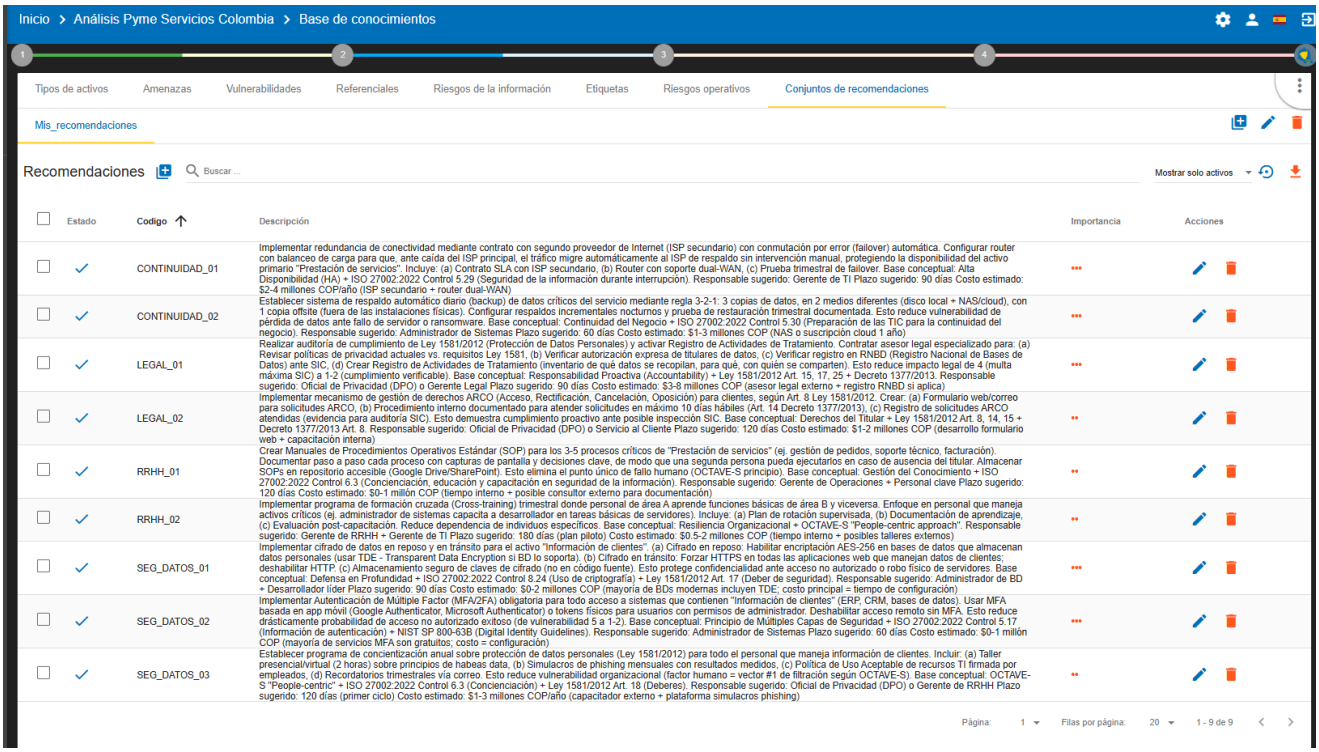


Fuente: captura de pantalla propia del catálogo personalizado de referencial de controles integrado en la base de conocimientos de MONARC.

Se presenta en la Figura 3.3.4-7 la vista del conjunto de recomendaciones gestionado en la Base de Conocimiento (Knowledge Base). Cada entrada cuenta con un código identificador único y una descripción detallada de las acciones para reducir la vulnerabilidad de los riesgos detectados. Estas recomendaciones fueron adaptadas al contexto de la pyme del sector servicios, integrando buenas prácticas y marcos normativos (como la ISO 27001) según el nivel de madurez identificado.

En ese sentido, la vinculación de este conjunto de recomendaciones mediante el proceso de tratamiento permite transformar los riesgos actuales en riesgos residuales, garantizando una trazabilidad total entre activos, amenazas, vulnerabilidades y futuros controles a identificar, adquirir e implementar.

Figura 3.3.4-7: Conjunto de recomendaciones personalizadas cargadas en MONARC



Fuente: captura de pantalla propia del catálogo personalizado de recomendaciones para el tratamiento de riesgos integrado en la base de conocimientos de MONARC.

3.3.5 Resultados de la Etapa 4: Verificación del flujo completo, tratamiento, seguimiento y salidas documentales

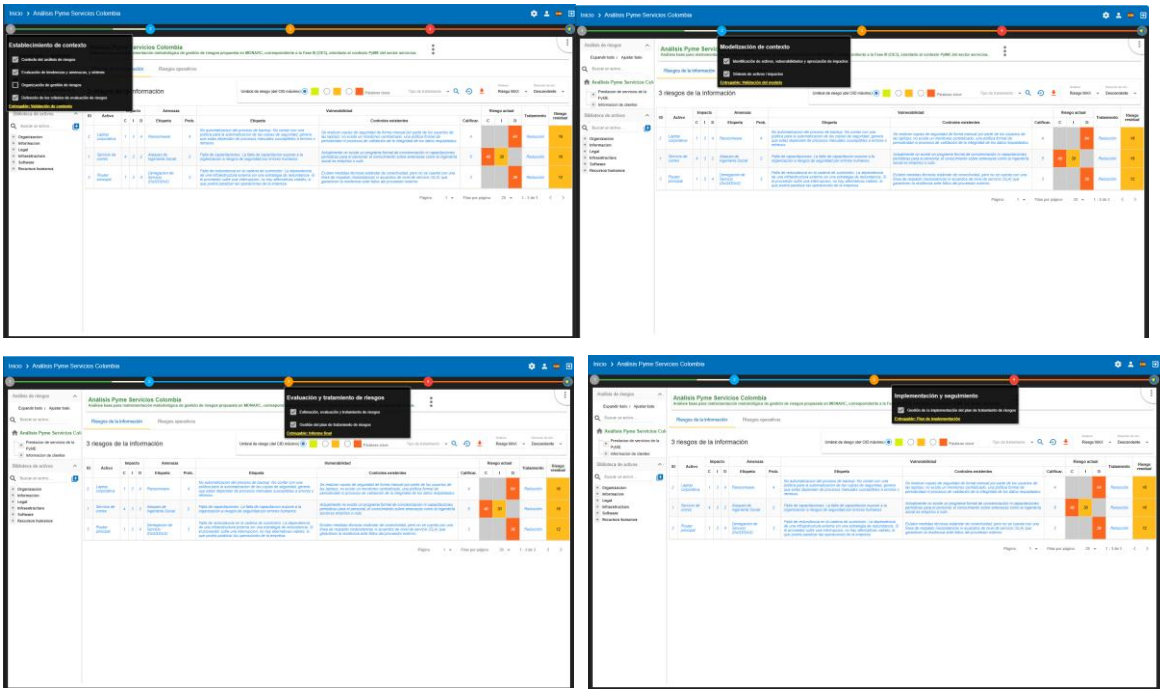
En esta etapa se verificó la operatividad integral del flujo de gestión de riesgos instrumentado en MONARC. Se recorrió de forma secuencial y controlada las funciones disponibles desde la evaluación hasta el tratamiento, el registro de seguimiento y la generación de salidas documentales.

La verificación se ejecutó sobre la configuración previamente establecida en las etapas 1 a 3 (contexto, criterios de evaluación, modelado de activos y base de conocimiento), la cual había habilitado el cálculo automático, la clasificación por umbrales y la disponibilidad de catálogos personalizados de amenazas, vulnerabilidades, referenciales y conjuntos de recomendaciones.

- Verificación del flujo completo del análisis (Etapas 0–4)

Esta verificación se realizó mediante la navegación y ejecución continua del análisis de riesgos a través de los módulos del sistema, sin interrupciones funcionales. La Figura 3.3.5-1 presentó la continuidad operativa del análisis desde el contexto y el modelado, hasta la evaluación y el tratamiento, evidenciando que el workflow permaneció habilitado conforme se completaron los subpasos del proceso.

Figura 3.3.5-1: Flujo operativo del análisis ejecutado en MONARC.



De igual forma, Figura 3.3.5-1 mostró los escenarios registrados durante la ejecución del análisis, donde se observaron asociaciones entre activos, amenazas y vulnerabilidades, así como la clasificación automática del nivel de exposición según los criterios y umbrales configurados.

- Tratamiento de riesgos de información

En el módulo de riesgos de información se observaron inicialmente los riesgos evaluados con estado *Not treated* o "No se ha tratado", lo cual permitió constatar la habilitación del flujo de tratamiento posterior a la etapa de evaluación. La Figura 3.3.5-2 presenta la consolidación de los riesgos de la información evaluados en vista de lista, con ordenamiento por score y clasificación automática por color, en coherencia con los umbrales configurados para riesgos de información.

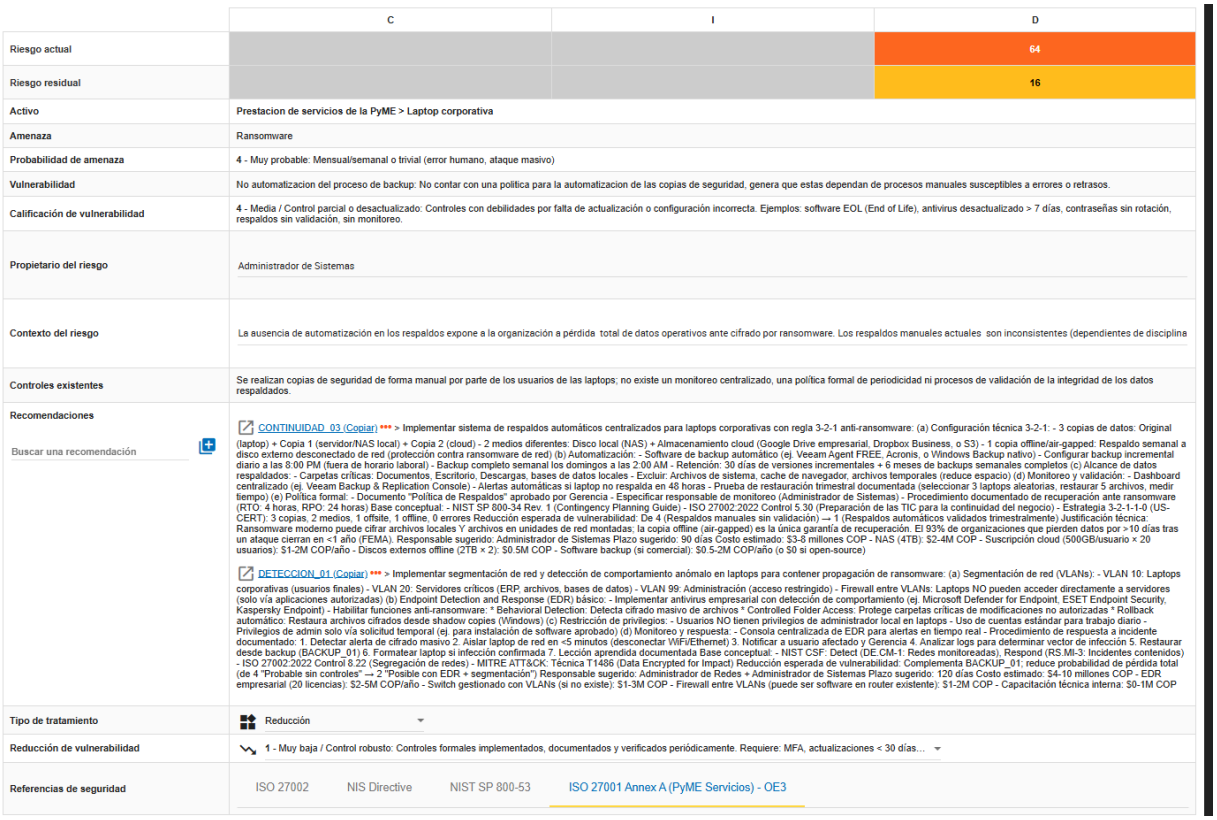
Figura 3.3.5-2: Lista de riesgos de información evaluados con estado inicial sin tratamiento

Fuente: captura de pantalla propia de la lista de riesgos de información evaluados y clasificados por umbral en MONARC.

Para cada riesgo se ingresó a la ventana de tratamiento mediante selección directa desde la lista. En dichas ventanas se observó que el sistema consolidó información contextual del escenario (activo, amenaza, vulnerabilidad, impactos y score), y habilitó campos para registrar propietario, estrategia de tratamiento, recomendaciones y parámetros de reducción.

La Figura 3.3.5-3 muestra un ejemplo de tratamiento diligenciado para un riesgo de información. En la ventana se registraron: (i) el propietario del riesgo, (ii) la estrategia seleccionada, (iii) la vinculación de recomendaciones desde el conjunto definido en la base de conocimiento, y (iv) el ajuste de reducción de vulnerabilidad, tras lo cual el sistema recalculó automáticamente el riesgo residual, pasando de un riesgo actual de 64 a un riesgo residual de 16.

Figura 3.3.5-3: Ventana de tratamiento de riesgo de información con recomendaciones vinculadas y cálculo automático de riesgo residual en MONARC



	C	I	D
Riesgo actual			64
Riesgo residual			16
Activo	Prestacion de servicios de la PyME > Laptop corporativa		
Amenaza	Ransomware		
Probabilidad de amenaza	4 - Muy probable: Mensual/semanal o trivial (error humano, ataque masivo)		
Vulnerabilidad	No automatizacion del proceso de backup: No contar con una politica para la automatizacion de las copias de seguridad, genera que estas dependan de procesos manuales susceptibles a errores o retrasos.		
Calificación de vulnerabilidad	4 - Media / Control parcial o desactualizado: Controles con debilidades por falta de actualización o configuración incorrecta. Ejemplos: software EOL (End of Life), antivirus desactualizado > 7 días, contraseñas sin rotación, respaldos sin validación, sin monitoreo.		
Propietario del riesgo	Administrador de Sistemas		
Contexto del riesgo	La ausencia de automatización en los respaldos expone a la organización a pérdida total de datos operativos ante cifrado por ransomware. Los respaldos manuales actuales son inconsistentes (dependientes de disciplina		
Controles existentes	Se realizan copias de seguridad de forma manual por parte de los usuarios de las laptops; no existe un monitoreo centralizado, una política formal de periodicidad ni procesos de validación de la integridad de los datos respaldados.		
Recomendaciones Buscar una recomendación	CONTINUIDAD_03 (Copiar) *** > Implementar sistema de respaldos automáticos centralizados para laptops corporativas con regla 3-2-1 anti-ransomware: (a) Configuración técnica 3-2-1: - 3 copias de datos: Original (laptop) + Copia 1 (servidor/NAS local) + Copia 2 (cloud) - 2 medios diferentes: Disco local (NAS) + Almacenamiento cloud (Google Drive empresarial, Dropbox Business, o S3) - 1 copia offline/air-gapped: Respaldo semanal a disco externo desconectado de red (protección contra ransomware de red) (b) Automatización: - Software de backup automático (ej. Veeam Agent FREE, Acronis, o Windows Backup nativo) - Configurar backup incremental diario a las 8:00 PM (fuera de horario laboral) - Backup completo semanal los domingos a las 2:00 AM - Retención: 30 días de versiones incrementales + 6 meses de backups semanales completos (c) Alcance de datos respaldados: - Carpetas críticas: Documentos, Escritorio, Descargas, bases de datos locales - Excluir: Archivos de sistema, cache de navegador, archivos temporales (reduce espacio) (d) Monitoreo y validación: - Dashboard centralizado (ej. Veeam Backup & Replication Console) - Alertas automáticas si laptop no respalda en 48 horas - Prueba de restauración trimestral documentada (seleccionar 3 laptops aleatorias, restaurar 5 archivos, medir tiempo) (e) Política formal: - Documento "Política de Respaldos" aprobado por Gerencia - Especificar responsable de monitoreo (Administrador de Sistemas) - Procedimiento documentado de recuperación ante ransomware (RTO: 4 horas, RPO: 24 horas) Base conceptual: - NIST SP 800-34 Rev. 1 (Contingency Planning Guide) - ISO 27002:2022 Control 5.30 (Preparación de las TIC para la continuidad del negocio) - Estrategia 3-2-1-1-0 (US-CERT): 3 copias, 2 medios, 1 offsite, 1 offline, 0 errores Reducción esperada de vulnerabilidad: De 4 (Respaldos manuales sin validación) → 1 (Respaldos automáticos validados trimestralmente) Justificación técnica: Ransomware moderno puede cifrar archivos locales Y archivos en unidades de red montadas; la copia offline (air-gapped) es la única garantía de recuperación. El 93% de organizaciones que pierden datos por >10 días tras un ataque cierran en <1 año (FEMA). Responsable sugerido: Administrador de Sistemas Plazo sugerido: 90 días Costo estimado: $3-8 millones COP - NAS (4TB): $2-4M COP - Suscripción cloud (500GB/usuario × 20 usuarios): $1-2M COP/año - Discos externos offline (2TB × 2): $0.5M COP - Software backup (si comercial): $0.5-2M COP/año (o $0 si open-source) DETECCION_01 (Copiar) *** > Implementar segmentación de red y detección de comportamiento anómalo en laptops para contener propagación de ransomware: (a) Segmentación de red (VLANs): - VLAN 10: Laptops corporativas (usuarios finales) - VLAN 20: Servidores críticos (ERP, archivos, bases de datos) - VLAN 99: Administración (acceso restringido) - Firewall entre VLANs: Laptops NO pueden acceder directamente a servidores (solo vía aplicaciones autorizadas) (b) Endpoint Detection and Response (EDR) básico: - Implementar antivirus empresarial con detección de comportamiento (ej. Microsoft Defender for Endpoint, ESET Endpoint Security, Kaspersky Endpoint) - Habilitar funciones anti-ransomware: * Behavioral Detection: Detecta cifrado masivo de archivos * Controlled Folder Access: Protege carpetas críticas de modificaciones no autorizadas * Rollback automático: Restaura archivos cifrados desde shadow copies (Windows) (c) Restricción de privilegios: - Usuarios NO tienen privilegios de administrador local en laptops - Uso de cuentas estándar para trabajo diario - Privilegios de admin solo vía solicitud temporal (ej. para instalación de software aprobado) (d) Monitoreo y respuesta: - Consola centralizada de EDR para alertas en tiempo real - Procedimiento de respuesta a incidente documentado: 1. Detectar alerta de cifrado masivo 2. Aislar laptop de red en <5 minutos (desconectar WiFi/Ethernet) 3. Notificar a usuario afectado y Gerencia 4. Analizar logs para determinar vector de infección 5. Restaurar desde backup (BACKUP_01) 6. Formatear laptop si infección confirmada 7. Lección aprendida documentada Base conceptual: - NIST CSF: Detect (DE.CM-1: Redes monitoreadas), Respond (RS.MI-3: Incidentes contenidos) - ISO 27002:2022 Control 8.22 (Segregación de redes) - MITRE ATT&CK: Técnica T1486 (Data Encrypted for Impact) Reducción esperada de vulnerabilidad: Complementa BACKUP_01; reduce probabilidad de pérdida total (de 4 "Probable sin controles" → 2 "Posible con EDR + segmentación") Responsable sugerido: Administrador de Redes + Administrador de Sistemas Plazo sugerido: 120 días Costo estimado: $4-10 millones COP - EDR empresarial (20 licencias): $2-5M COP/año - Switch gestionado con VLANs (si no existe): $1-3M COP - Firewall entre VLANs (puede ser software en router existente): $1-2M COP - Capacitación técnica interna: $0-1M COP		
Tipo de tratamiento	Reducción		
Reducción de vulnerabilidad	1 - Muy baja / Control robusto: Controles formales implementados, documentados y verificados periódicamente. Requiere: MFA, actualizaciones < 30 días...		
Referencias de seguridad	ISO 27002 NIS Directive NIST SP 800-53 ISO 27001 Annex A (PyME Servicios) - OE3		

Fuente: captura de pantalla propia del tratamiento de un riesgo de información con recomendaciones vinculadas y cálculo automático de riesgo residual en MONARC.

- Tratamiento de riesgos operativos

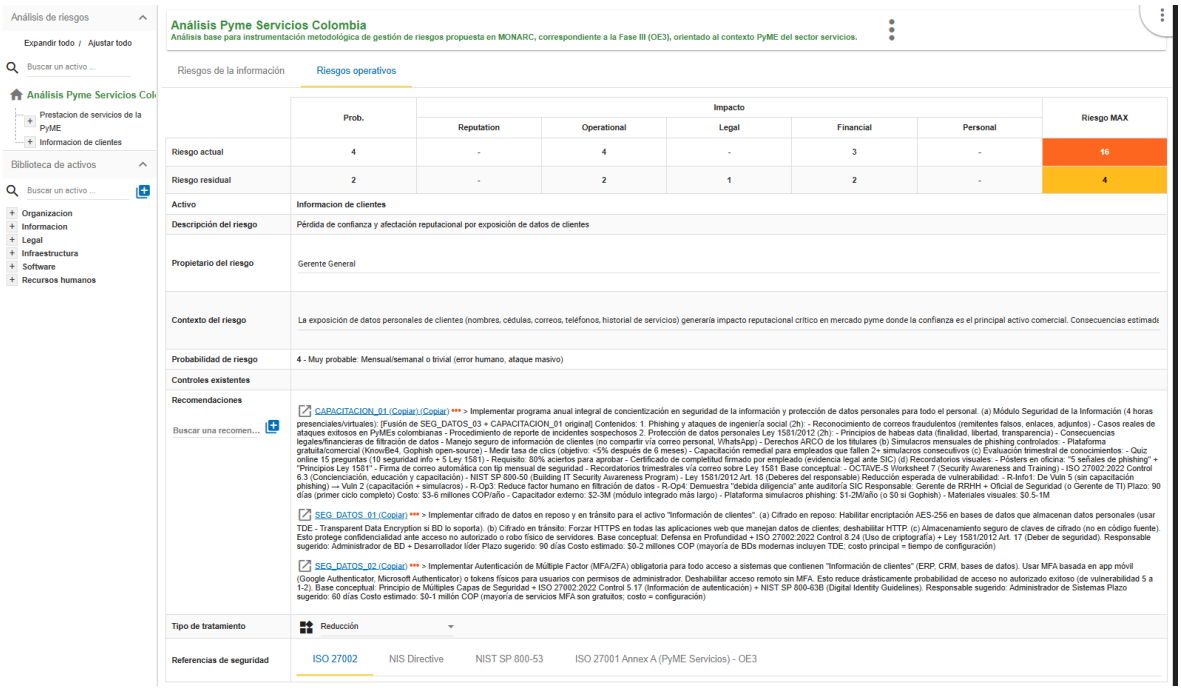
En el módulo de riesgos operativos se observa una vista diferenciada para la consolidación de escenarios evaluados. La Figura 3.3.5-4 muestra la lista de riesgos operativos con su clasificación automática por umbral, evidenciando que la estructura de impacto corresponde a dimensiones del negocio (reputacional, operacional, legal, financiera y personal), tal como fue parametrizado en la Etapa 2.

Figura 3.3.5-4: Lista de riesgos operativos evaluados con estado inicial Not treated y clasificación automática por umbral.

Fuente: captura de pantalla propia de la lista de riesgos operativos evaluados y clasificados por umbral en MONARC.

La Figura 3.3.5-5 evidencia un ejemplo de tratamiento diligenciado para un riesgo operativo, donde se observan los campos habilitados para registrar responsable, estrategia y recomendaciones, así como el ajuste de valores asociados a impactos (según el modelo operativo configurado). Tras el registro de cambios, el sistema recalculó el riesgo residual, el cual pasó de 16 a 4, presentando la actualización del estado del riesgo dentro del análisis operativo.

Figura 3.3.5-5: Ventana de tratamiento de riesgo operativo con recomendaciones vinculadas y actualización del riesgo residual en MONARC



Fuente: captura de pantalla propia del tratamiento de un riesgo operativo con recomendaciones vinculadas y actualización automática del riesgo residual en MONARC.

- Consistencia del tratamiento

Durante el tratamiento se observó la capacidad del sistema para reutilizar recomendaciones mediante su identificador, permitiendo su vinculación transversal en múltiples escenarios. Adicionalmente, la Tabla 3.3.5-1 consolidó, para los riesgos tratados, el score previo y posterior al tratamiento, el propietario registrado y la reducción aplicada (por reducción de vulnerabilidad en riesgos de información o por ajustes de impacto en riesgos operativos), según lo que se observó en las ventanas de tratamiento y en el estado final del flujo.

Tabla 3.3.5-1: Matriz consolidada de tratamiento (antes y después)

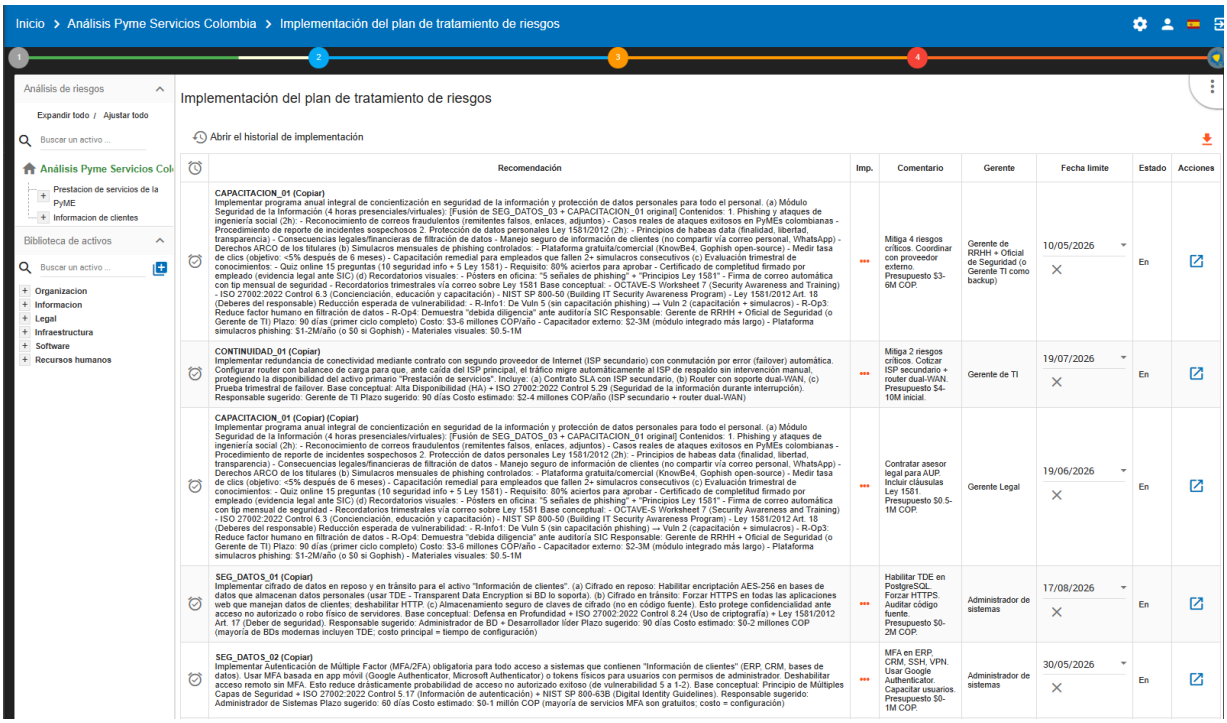
ID Riesgo	Activo	Score Actual	Propietario	Recomendaciones Vinculadas	Reducción	Score Residual	Resultado
INFO-2	Laptop corporativa	**64**	Admin Sistemas	CONTINUIDAD_03, DETECCION_01	Vuln 4→1	**16**	-75%
INFO-1	Servicio correo	**40**	Gerente RRHH	CAPACITACION_01, CAPACITACION_02	Vuln 5→2	**16**	-60%
INFO-3	Router principal	**36**	Gerente TI	CONTINUIDAD_01	Vuln 3→1	**12**	-67%
OP-5	Información clientes	**16**	Gerente General	SEG_DATOS_01, SEG_DATOS_02, CAPACITACION_01	Imp 4/3→2/2	**4**	-75%
OP-4	Información clientes	**12**	Oficial Privacidad	LEGAL_01, LEGAL_02, CAPACITACION_01	Imp 4→1	**3**	-75%
OP-1	Prestación servicios	**12**	Gerente General	CONTINUIDAD_01, CONTINUIDAD_02	Imp 4/4→2/2	**6**	-50%
OP-2	Prestación servicios	**6**	Gerente RRHH	RRHH_01, RRHH_02	Imp 3→1	**2**	-67%

Fuente: Elaboración propia. Los escenarios se construyeron variando el nivel de reducción de vulnerabilidad aplicado en MONARC para el activo de mayor score inicial (INFO-2, Laptop corporativa, score 64). El escenario base corresponde al tratamiento ejecutado en el caso simulado; los escenarios moderado y conservador representan implementaciones parciales de los controles recomendados y permiten dimensionar el efecto ante restricciones operativas típicas de una pyme real.

- Seguimiento del plan de tratamiento

La transición hacia el componente de implementación y seguimiento permitió verificar que el flujo soportó el registro de responsables y plazos asociados al plan de tratamiento. Como se observa en la Figura 3.3.5-6, las recomendaciones vinculadas a los riesgos tratados se consolidan en una lista de gestión (por ejemplo, *Manager* y *Deadline*), donde se registran campos como responsables, fecha límite por recomendación, estado y comentarios. Esta funcionalidad habilita el seguimiento del plan de tratamiento dentro del workflow.

Figura 3.3.5-6: Lista de gestión del plan de tratamiento de riesgos.



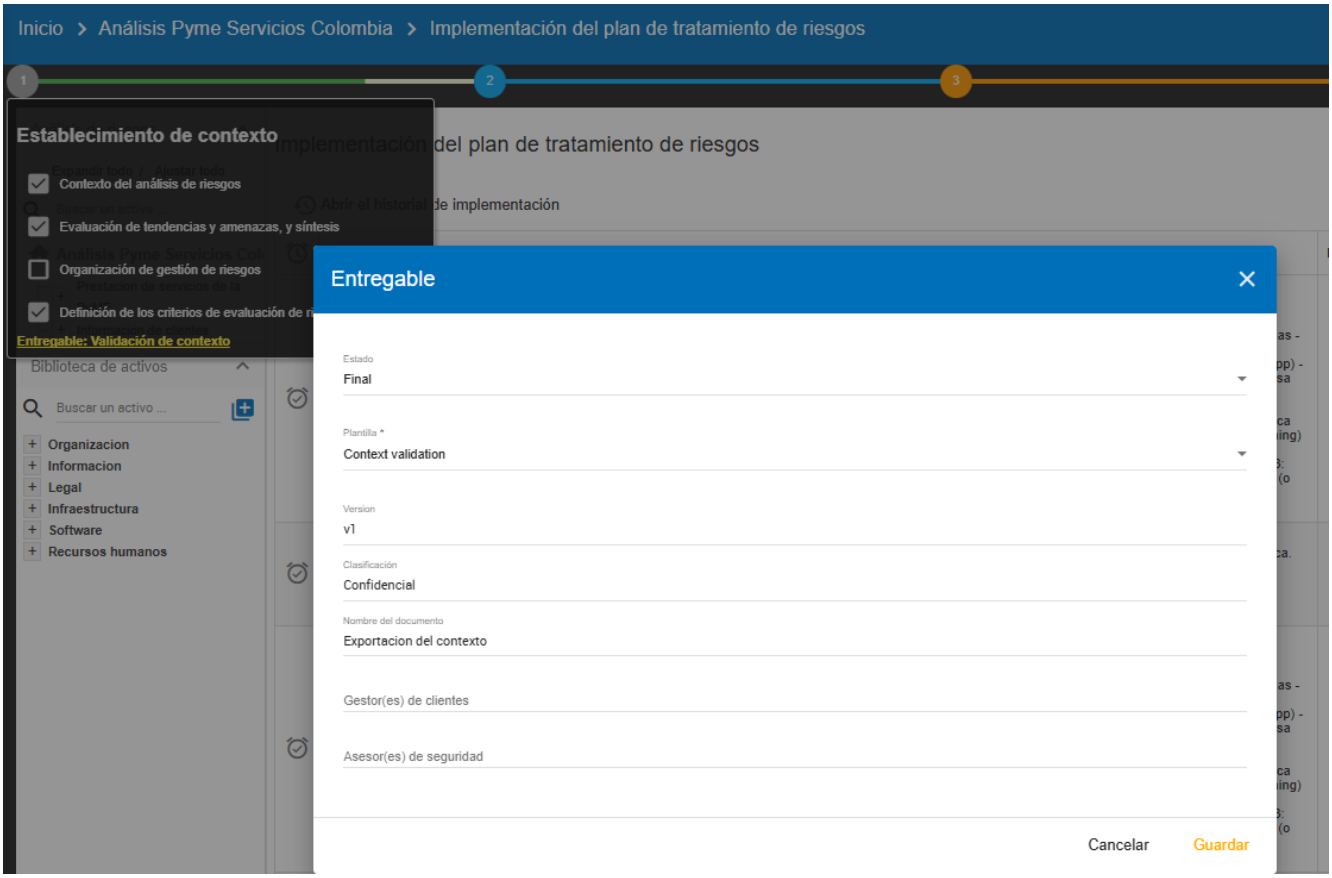
Fuente: captura de pantalla propia de la lista de seguimiento del plan de tratamiento de riesgos en MONARC.

- Generación de salidas documentales y exportación de artefactos

Finalmente, se verificó la disponibilidad de funciones de reporte y exportación posteriores a la ejecución del análisis. La Figura 3.3.5-1 mostró el módulo de reportes y exportaciones disponibles en cada una de las Etapas tras la ejecución del flujo, evidenciando opciones para generar artefactos documentales y formatos de intercambio del análisis.

La Figura 3.3.5-7 muestra la configuración del entregable asociado a la validación del contexto en MONARC, ubicado en la Etapa 1 del flujo de análisis. En esta ventana se registran campos como estado, plantilla, versión, clasificación y nombre del documento, lo que permite generar el reporte correspondiente en formato descargable.

Figura 3.3.5-7: Generación del reporte de contexto en MONARC

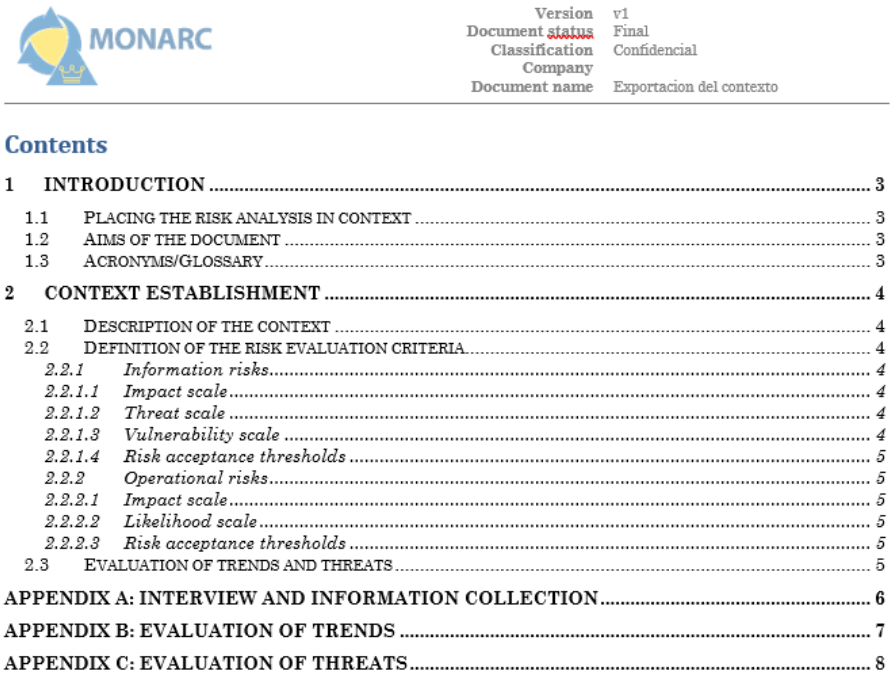


Fuente: captura de pantalla propia de la configuración del entregable para la generación del reporte de contexto en MONARC.

La Figura 3.3.5-8 presenta un fragmento del entregable de contexto generado automáticamente por MONARC en formato DOCX. El documento exportado consolida la información registrada durante la etapa de establecimiento del contexto, incluyendo la descripción del análisis, los criterios de evaluación del riesgo, las escalas de impacto, probabilidad y vulnerabilidad, los umbrales de aceptación y los anexos asociados a la evaluación de tendencias y amenazas. Este entregable evidencia la capacidad de la herramienta para generar documentación trazable del

proceso de análisis, aspecto relevante para respaldar la validación metodológica y conservar evidencia del caso aplicado.

Figura 3.3.5-8: Fragmento del entregable de contexto generado en formato DOCX por MONARC



MONARC

Version v1
Document status Final
Classification Confidencial
Company
Document name Exportacion del contexto

Contents

Fuente: captura de pantalla propia del entregable de contexto generado en formato DOCX por MONARC.

Los artefactos generados en la Fase III constituyeron la línea base técnica, y fueron reutilizados en la Fase IV mediante la duplicación del análisis para ejecutar una prueba de escritorio con parámetros realistas derivados del Instrumento de Diagnóstico, manteniendo consistencia metodológica y preservando la confidencialidad.

3.4 Resultados de las Fase IV – OE4: Validación de la metodología propuesta

La Fase IV validó la metodología propuesta mediante su aplicación en una pyme, construida como prueba de escritorio a partir del Instrumento de Recolección de Datos, con el fin de verificar ejecutabilidad, suficiencia de productos, desempeño metodológico y consolidar evidencia documental de validación como soporte del OE4 (cuarto objetivo específico de la investigación).

3.4.1 Caso de estudio simulado “Pyme Servicios Colombia” (prueba de escritorio)

La validación de la metodología propuesta se desarrolló mediante una prueba de escritorio, construyendo un caso simulado denominado “PyME Servicios Colombia”. La decisión de emplear un escenario demostrativo respondió a la necesidad de verificar la ejecutabilidad y trazabilidad del ciclo metodológico instrumentado en la herramienta, manteniendo condiciones realistas y, a la vez, evitando el uso de información identificable o sensible asociada a una organización específica.

El escenario simulado se fundamentó en los hallazgos empíricos del Instrumento de Diagnóstico sobre Gestión de Riesgos de Seguridad de la Información aplicado a 72 organizaciones (referenciado en el planteamiento del problema). Dichos resultados permitieron inferir patrones recurrentes en MiPyMEs, tales como: baja adopción de metodologías formales de gestión de riesgos, debilidades en la planificación de controles, tendencia reactiva ante incidentes de seguridad y una alta dependencia de herramientas ofimáticas para el registro y seguimiento. En consecuencia, el caso simulado se diseñó para representar una PyME del sector servicios con rasgos organizacionales compatibles con ese patrón, en términos de operación intensiva en información de terceros, recursos limitados y madurez heterogénea en prácticas de seguridad.

En términos de contexto, el escenario se configuró como una organización privada del sector servicios cuya operación depende de procesos digitales y de la gestión de información asociada a clientes y operación interna. Por consiguiente, permitió representar un escenario donde los impactos potenciales de un incidente se reflejan tanto en la tríada Confidencialidad–Integridad–Disponibilidad (C-I-D) como en consecuencias operativas y de cumplimiento, en coherencia con el enfoque adoptado en el análisis (riesgos de información y riesgos operacionales).

Acerca de las características organizacionales específicas del escenario, para efectos de la prueba de escritorio, el caso simulado se describió con parámetros realistas y acordes al contexto observado en el instrumento empírico:

- **Tamaño organizacional:** estructura pequeña con alrededor de 20 empleados, organización relativamente plana y roles multifuncionales (1 gerente general, 3 coordinadores, 16 operativos).

- **Operación y servicios:** prestación de servicios profesionales con componentes digitales (gestión de clientes, comunicaciones corporativas, documentación de procesos y soporte de la operación mediante aplicaciones).
- **Madurez tecnológica:** dependencia de servicios digitales de bajo costo y uso de herramientas de productividad comunes; infraestructura local limitada y equipos de usuario final como base Operacional; ausencia de un esquema robusto de administración centralizada.
- **Rol de seguridad:** inexistencia de un responsable dedicado de seguridad de la información; funciones asumidas parcialmente por un rol de TI no especializado y con disponibilidad limitada (medio tiempo).

Esta caracterización se utilizó exclusivamente para estructurar un caso plausible y representativo, sin asociarlo a ninguna organización real ni incorporar información identificable o sensible.

Respecto al alcance del análisis de riesgos simulado, la identificación y modelado de activos se orientó a representar un inventario típico de pymes del sector servicios, considerando:

Activos primarios (4) de negocio:

1. prestación de servicios (proceso crítico),
2. información de clientes (datos personales e historial de servicios),
3. continuidad operativa,
4. cumplimiento legal y normativo (incluyendo obligaciones asociadas al tratamiento de datos personales).

- **Activos secundarios de soporte (aprox. 95):** infraestructura TI, software/aplicaciones, personal/RRHH y documentación/procedimientos organizacionales.

La estructura de activos y dependencias se definió de forma que permitiera la trazabilidad entre procesos críticos, activos de soporte y escenarios de riesgo, manteniendo la coherencia con las capacidades de modelado jerárquico establecidas en la instrumentación previa.

Selección de escenarios de riesgo (amenazas y vulnerabilidades). La selección de escenarios priorizó amenazas consistentes con el contexto reportado por el instrumento empírico y con tendencias ampliamente documentadas en el panorama de incidentes, en especial aquellas asociadas a:

- **ingeniería social** (por ejemplo, campañas de suplantación y engaño dirigidas a usuarios),
- **malware con impacto en disponibilidad e integridad** (por ejemplo, cifrado de información y afectación de activos críticos),
- **interrupciones de conectividad y servicios** que afectan la continuidad operativa (dependencia ISP único),
- **debilidades de control de acceso** (credenciales débiles, gestión deficiente de permisos, ausencia de medidas reforzadas de autenticación MFA), y
- **prácticas manuales** que limitan trazabilidad (respaldos inconsistentes, registro de incidentes disperso y ausencia de bitácoras estructuradas).

Las vulnerabilidades asociadas se definieron en coherencia con las debilidades técnicas y organizacionales típicas de organizaciones con recursos limitados: ausencia de lineamientos documentados, baja capacitación, controles parciales y dependencia de procedimientos informales.

Tratamiento de riesgos simulado. El caso permitió estructurar un conjunto acotado de recomendaciones realistas (aprox. 11), alineadas con buenas prácticas y referenciales comúnmente reconocidos en el contexto (por ejemplo, familia ISO/IEC 27001/27002 como marco de controles), integrando medidas:

- **técnicas**, orientadas a mejorar continuidad, control de acceso, protección de información y reducción de superficie de ataque;
- **organizacionales**, orientadas a fortalecer cultura, capacitación, políticas internas y formalización mínima de procedimientos; y
- **de cumplimiento**, orientadas a soportar obligaciones asociadas al tratamiento de datos personales y a la gestión documental requerida para evidenciar acciones de seguridad.

La inclusión de medidas organizacionales se justificó por las barreras evidenciadas en el instrumento empírico, particularmente la falta de capacitación y la confusión conceptual en prácticas reales, reforzando así que la necesidad de controles no se limite a componentes tecnológicos.

Limitaciones metodológicas del caso simulado. Escenario simulado con valores de probabilidad, impacto y vulnerabilidad asignados mediante juicio experto del investigador, apoyado en la

evidencia agregada del instrumento y en supuestos controlados, y no mediante talleres participativos internos con una pyme real tal y como lo enfatiza OCTAVE-S. Esta condición reduce validez externa de estimaciones cuantitativas específicas; sin embargo, no afecta la validez de constructo de la validación metodológica, centrada en verificar la ejecutabilidad de etapas, la cobertura de elementos del proceso de gestión de riesgos y la utilidad de las salidas para toma de decisiones en un contexto pyme.

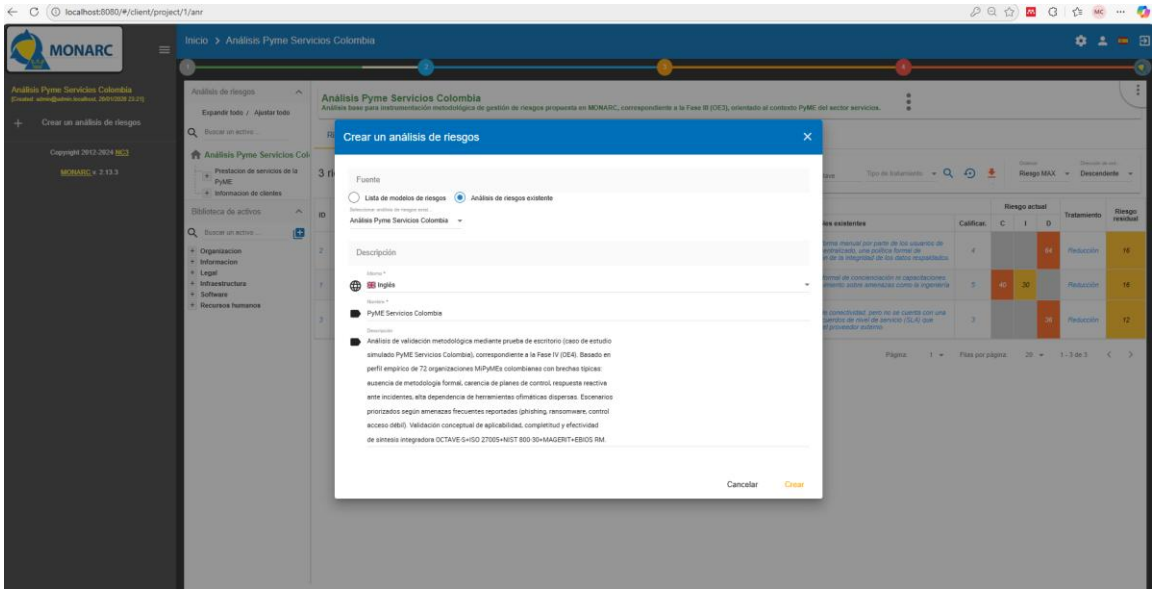
Nota de trazabilidad OE3→OE4. Dado que el caso simulado se construyó aprovechando la instrumentación previa, el análisis de validación se apoyó en la duplicación (clonación) del análisis base desarrollado en el OE3, así que se reutilizó la configuración metodológica (escalas, umbrales, catálogos y estructura jerárquica). Además, permitió concentrar la variación en la narrativa y el análisis por criterios de validación.

3.4.2 Ejecución del análisis de riesgos (OE4)

- Duplicación y contextualización

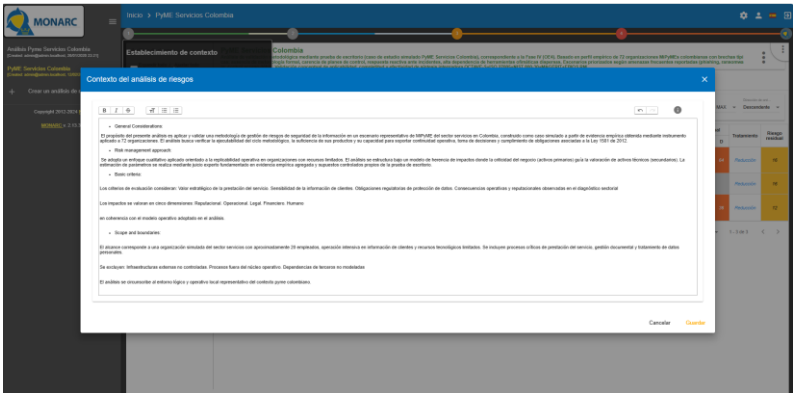
Se observa en Figura 3.4.2-1 la ventana de creación de análisis basada en uno existente, donde se seleccionó el análisis previamente instrumentado en el OE3. Esta funcionalidad nativa de clonación en MONARC generó un nuevo análisis de riesgos independiente que heredó la parametrización previamente establecida, incluyendo escalas de evaluación, umbrales de aceptación, estructura jerárquica de activos, catálogos configurados y conjuntos de recomendaciones. A partir de esta instancia se procedió a la ejecución del flujo metodológico orientado a la validación del caso simulado.

Figura 3.4.2-1: Clonación del análisis base OE3 para crear análisis de validación OE4.



Se observa el registro del contexto del análisis correspondiente al caso simulado “PyME Servicios Colombia”, donde se documentó el alcance organizacional, los criterios de evaluación y el enfoque aplicado. Esta información se integró como referencia base para la ejecución del análisis y para su inclusión automática en los artefactos documentales generados por la herramienta.

Figura 3.4.2-2: Contextualización del análisis clonado en el Step 0 de MONARC.



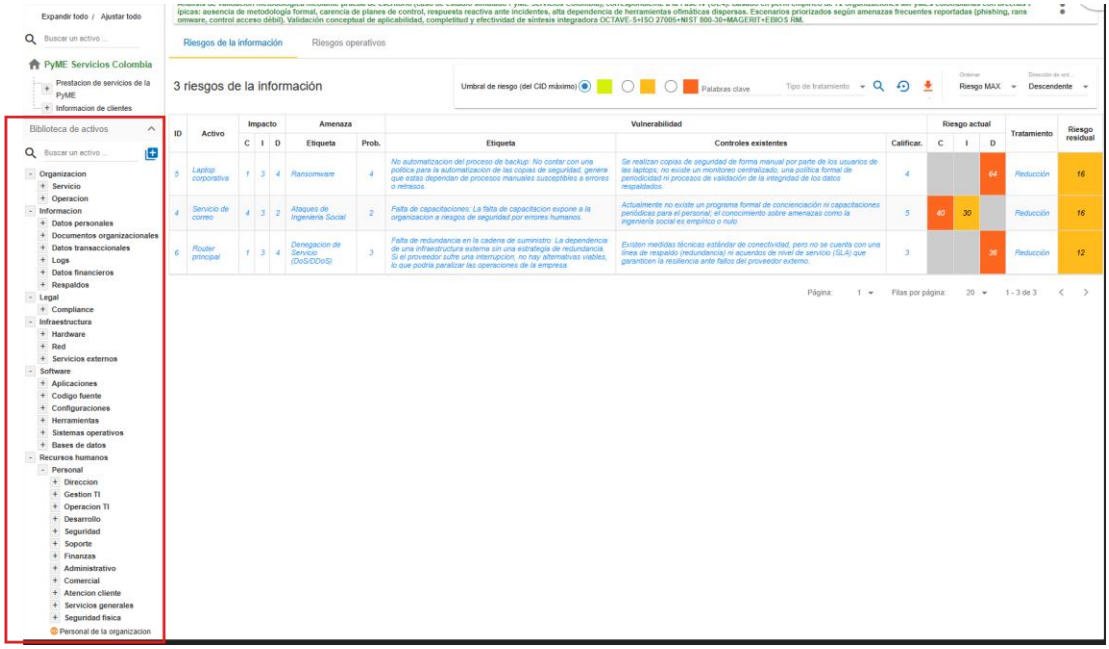
- Modelado de activos y escenarios

En la Figura 3.4.2-3 se presenta la verificación de la herencia de la estructura jerárquica de activos tras la clonación del análisis base. El inventario consolidado de 99 elementos (4 activos primarios y estratégicos y 91 activos operativos/secundarios) se visualiza en el panel de navegación,

manteniendo intactas las relaciones jerárquicas y dependencias definidas durante el modelado del OE3.

La interfaz evidencia la preservación de la taxonomía organizacional y tecnológica utilizada para clasificar activos (organización, información, infraestructura, software, recursos humanos, entre otros), así como la disponibilidad inmediata de dichos elementos para la generación de escenarios de riesgo en el análisis clonado.

Figura 3.4.2-3: Árbol de activos heredado (99 activos visibles).

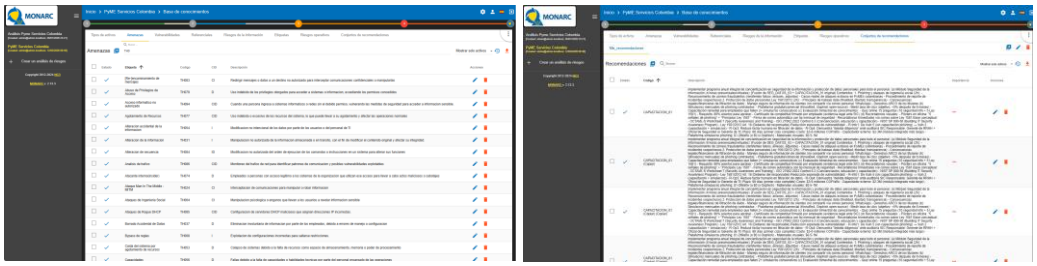


En la Figura 3.4.2-4 se observa la disponibilidad de los catálogos personalizados dentro de la Base de Conocimiento del análisis clonado. La interfaz muestra el conjunto de amenazas contextualizadas y el conjunto de recomendaciones previamente configurados durante la instrumentación metodológica del OE3, accesibles sin procesos adicionales de importación o configuración.

La persistencia de estos catálogos confirma que la funcionalidad de duplicación del sistema transfiere íntegramente los repositorios semánticos asociados al análisis base, incluyendo taxonomías de amenazas y conjuntos estructurados de medidas de tratamiento. En consecuencia, la instancia de validación conserva la misma base conceptual y operativa empleada en el diseño

metodológico, garantizando consistencia analítica entre fases y evitando la introducción de variabilidad configuracional.

Figura 3.4.2-4: Verificación de disponibilidad de catálogos heredados.

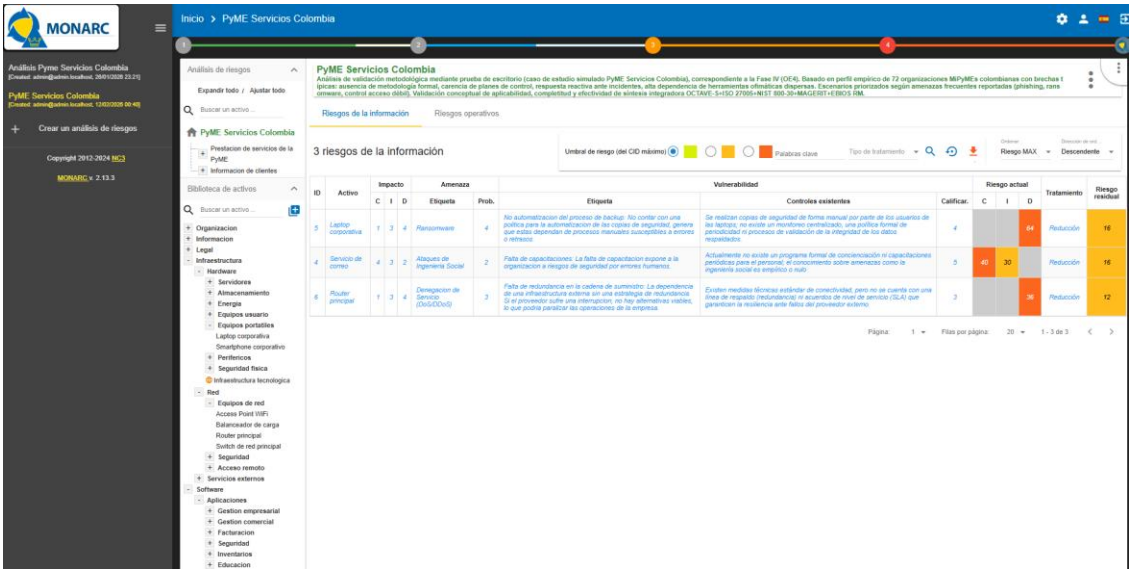


- Evaluación y tratamiento de riesgos

La Figura 3.4.2-5 presenta la ejecución del módulo de evaluación de riesgos de información correspondiente al Step 2 del flujo analítico. En la interfaz se visualiza la matriz de escenarios generados mediante la asociación entre activos secundarios, amenazas y vulnerabilidades, así como la consolidación automática de valores de impacto, probabilidad y calificación de controles existentes.

Se registraron tres escenarios técnicos evaluados, correspondientes a amenazas de ransomware, ingeniería social y denegación de servicio, vinculadas respectivamente a activos tecnológicos de usuario final, comunicaciones y red. Para cada escenario el sistema calculó automáticamente el valor del riesgo y lo clasificó conforme a los umbrales establecidos en la parametrización heredada del análisis base, evidenciándose la representación cromática del nivel de exposición en la matriz.

Figura 3.4.2-5: Evaluación de riesgos de información en caso simulado.



Se muestra en la Figura 3.4.2-6 la ejecución del módulo de evaluación de riesgos operativos correspondiente al Step 2 del flujo analítico. Se visualiza la consolidación de escenarios asociados a activos primarios, también, se muestra la valoración del impacto mediante dimensiones organizacionales configuradas previamente (reputacional, Operacional, legal, financiera y personal).

Se registraron cuatro escenarios de riesgo vinculados a procesos críticos del negocio, el cálculo de los valores fue automático por el sistema a partir de la combinación de probabilidad e impactos asignados. Se aprecia la clasificación resultante conforme a los umbrales definidos en la parametrización heredada del análisis base, evidenciándose la diferenciación cromática del nivel de exposición y el estado de tratamiento asociado a cada escenario.

Escenario 1

Activo: Información de clientes

Descripción: Pérdida de confianza y afectación reputacional por exposición de datos

- Probabilidad registrada: 4
- Impactos asignados:
  - Operacional: 4

  - Financiero: 3
  - Reputacional: —
  - Legal: —
  - Personal: —
- Riesgo actual calculado: 16
- Tratamiento registrado: Reducción
- Riesgo residual: 4

Este escenario refleja una valoración en la que se asignaron consecuencias operacionales y financieras, generando un nivel de exposición clasificado visualmente en el rango alto según los umbrales configurados.

Escenario 2

Activo: Información de clientes

Descripción: Exposición a sanciones regulatorias por incumplimiento en protección de datos

- Probabilidad registrada: 3
- Impactos asignados:
  - Legal: 4
  - Reputacional: —
  - Operacional: —
  - Financiero: —
  - Personal: —
- Riesgo actual calculado: 12
- Tratamiento registrado: Reducción
- Riesgo residual: 6

Se observa que la valoración se concentró exclusivamente en la dimensión legal, evidenciando la capacidad del modelo para focalizar consecuencias específicas dentro del análisis operativo.

Escenario 3

Activo: Prestación de servicios de la PyME

Descripción: Interrupción significativa de la capacidad de prestación del servicio

- Probabilidad registrada: 3
- Impactos asignados:
  - Operacional: 4
  - Reputacional: —
  - Legal: —
  - Financiero: —
  - Personal: —
- Riesgo actual calculado: 12
- Tratamiento registrado: Reducción
- Riesgo residual: 4

El impacto principal se configuró en la dimensión Operacional, reflejando la asociación directa entre el activo primario y la continuidad del proceso de negocio evaluado.

Escenario 4

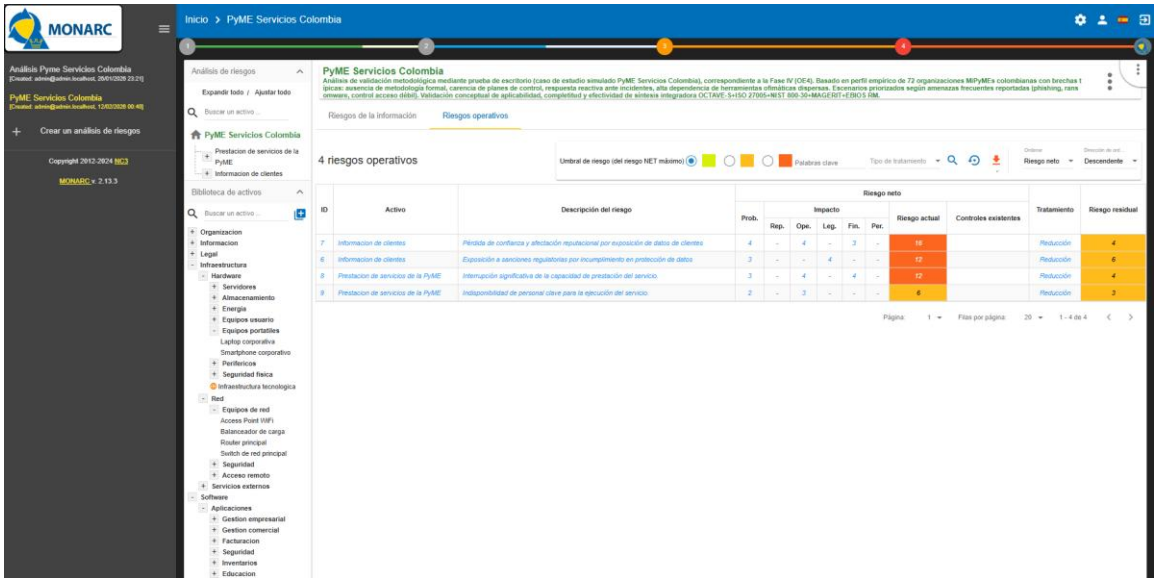
Activo: Prestación de servicios de la PyME

Descripción: Indisponibilidad de personal clave para la ejecución del servicio

- Probabilidad registrada: 2
- Impactos asignados:
  - Operacional: 3
  - Reputacional: —
  - Legal: —
  - Financiero: —
  - Personal: —
- Riesgo actual calculado: 6
- Tratamiento registrado: Reducción
- Riesgo residual: 3

Este escenario presenta el menor nivel de exposición dentro del conjunto evaluado, con valores inferiores tanto en probabilidad como en impacto Operacional.

Figura 3.4.2-6: Evaluación de riesgos operativos en caso simulado.



En la Figura 3.4.2-7 se muestra la ejecución del Step 3 — Gestión del plan de tratamiento, allí se evidencia la transición desde la evaluación hacia la mitigación de riesgos, se aprecia el uso vinculante de recomendaciones provenientes del catálogo previamente configurado.

La interfaz consolida información clave del escenario tratado, incluyendo:

- recomendación aplicada
- activo asociado
- controles existentes documentados
- score de riesgo actual
- score residual calculado automáticamente

confirmando el comportamiento del motor analítico de MONARC para proyectar la reducción de exposición antes de la implementación real de controles.

Escenario 1

Recomendación: CAPACITACION_01

Activo: Información de clientes / Servicio de correo

- Riesgo actual: 40

- Riesgo residual calculado: 16

Se observa que la vinculación de la recomendación orientada a concienciación y capacitación en ingeniería social produce una reducción cuantificable del nivel de riesgo, manteniendo la estrategia de tratamiento como Reducción.

Escenario 2

Recomendación: CONTINUIDAD_01

Activo: Prestación de servicios / Router principal

- Riesgo actual: 36
- Riesgo residual calculado: 12

La recomendación asociada a redundancia de conectividad y conmutación por error automático reduce el riesgo operativo del activo crítico de red, evidenciando el efecto proyectado de medidas de resiliencia tecnológica sobre la continuidad del negocio.

Escenario 3

Recomendación: CAPACITACION_01 (reutilizada)

Activo: Información de clientes

- Riesgo actual: 16
- Riesgo residual calculado: 4

Este escenario evidencia reutilización del catálogo de controles, donde la misma recomendación se vincula a múltiples riesgos, manteniendo consistencia metodológica y reduciendo duplicidad en la planificación de mitigaciones.

Escenario 4

Recomendación: SEG_DATOS_01

Activo: Información de clientes

- Riesgo actual: 16
- Riesgo residual calculado: 4

La recomendación orientada a cifrado de datos en reposo y tránsito genera una disminución proyectada del nivel de exposición mediante fortalecimiento de protección de la información sensible.

Escenario 5

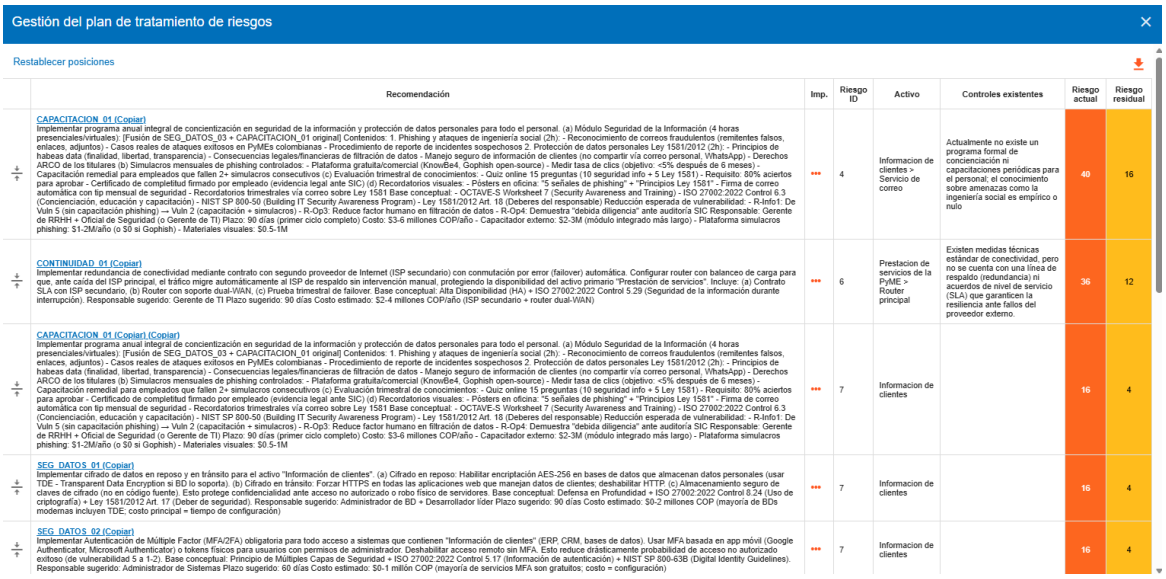
Recomendación: SEG_DATOS_02

Activo: Información de clientes

- Riesgo actual: 16
- Riesgo residual calculado: 4

La aplicación de autenticación multifactor (MFA) obligatoria muestra una reducción equivalente del riesgo, evidenciando consistencia en el comportamiento del cálculo residual frente a controles que reducen superficie de acceso no autorizado.

Figura 3.4.2-7: Tratamiento de riesgo con vinculación de recomendaciones y cálculo automático de riesgo residual.



La Figura 3.4.2-8 presenta la interfaz correspondiente al Step 4 — Implementación del plan de tratamiento, donde las recomendaciones definidas en la etapa anterior son Operacionalizadas mediante la asignación de responsables, plazos de ejecución y notas de seguimiento. Por consiguiente, esta matriz constituye el punto en el cual el análisis de riesgos se transforma en un

plan de acción organizacional ejecutable, a su vez, incorpora elementos de accountability otorgando insumo para la toma de decisiones y control de gestión.

La estructura de la interfaz permite observar las siguientes dimensiones:

- Recomendación aplicada
- Nivel de importancia
- Comentarios operativos
- Responsable asignado (Manager)
- Fecha límite de ejecución (Deadline)
- Estado de implementación
- Acciones de seguimiento

También se observan las acciones siguientes:

Acción 1 — Programa de capacitación integral

Recomendación: CAPACITACION_01

Responsable:

- Gerente de RRHH
- Oficial de Seguridad
- Gerente TI (backup)

Fecha límite: 10/05/2026

Comentario operativo:

- Mitiga 4 riesgos críticos
- Coordinación con proveedor externo
- Presupuesto estimado: 3–6M COP

Interpretación técnica:

La recomendación impacta múltiples escenarios de riesgo simultáneamente, evidenciando priorización estratégica de controles organizacionales transversales.

Acción 2 — Redundancia de conectividad

Recomendación: CONTINUIDAD_01

Responsable: Gerente de TI

Fecha límite: 19/07/2026

Comentario:

- Mitiga 2 riesgos críticos
- Cotización ISP secundario
- Implementación router dual-WAN
- Presupuesto inicial 4–10M COP

Interpretación: Control técnico orientado a resiliencia operativa que protege activo primario de prestación de servicios.

Acción 3 — Adecuación contractual y cumplimiento

Recomendación: CAPACITACION_01 (contexto legal)

Responsable: Gerente Legal

Fecha límite: 19/06/2026

Comentario:

- Ajuste contractual para AUP (adecuación de contratos estatales)
- Inclusión cláusulas Ley 1581
- Presupuesto 0.5–1M COP

Interpretación: Evidencia integración del tratamiento de riesgos con dimensión regulatoria.

Acción 4 — Cifrado de datos

Recomendación: SEG_DATOS_01

Responsable: Administrador de sistemas

Fecha límite: 17/08/2026

Comentario:

- Habilitar TDE en bases
- Forzar HTTPS
- Auditoría código fuente
- Presupuesto 0–2M COP

Interpretación: Medida técnica enfocada en confidencialidad y cumplimiento.

Acción 5 — Autenticación multifactor

Recomendación: SEG_DATOS_02

Responsable: Administrador de sistemas

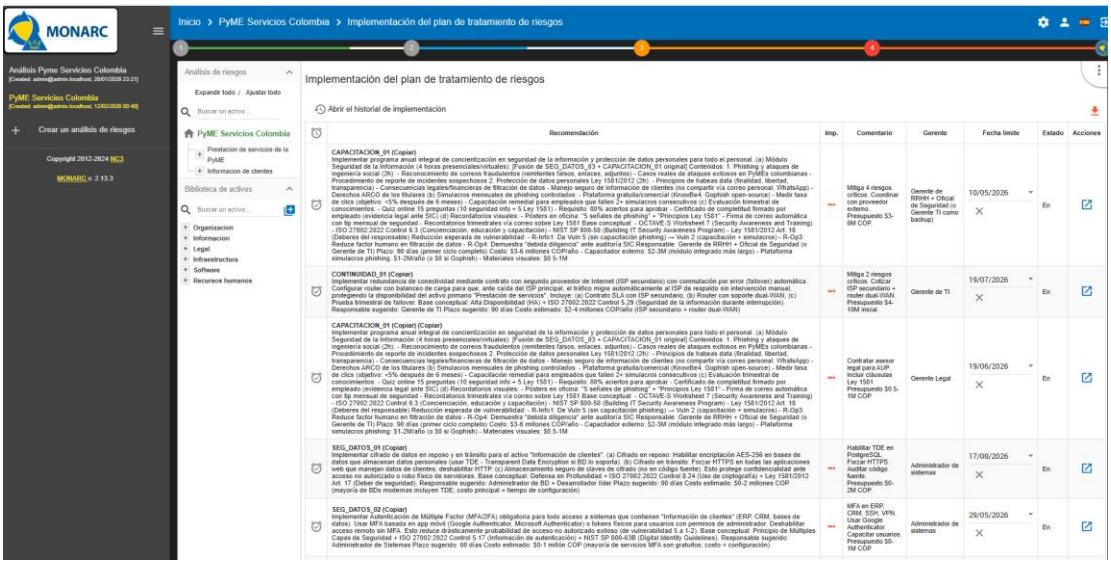
Fecha límite: 29/05/2026

Comentario:

- MFA en ERP / CRM / VPN / Correo
- Capacitación usuarios
- Presupuesto 0–1M COP

Interpretación: Control de acceso preventivo que reduce superficie de ataque.

Figura 3.4.2-8: Gestión de implementación del plan de tratamiento.



3.4.3 Generación de productos documentales

La ejecución del análisis de riesgos en el OE4 no concluyó únicamente en la obtención de valores de riesgo dentro de la herramienta, sino en la generación de productos documentales verificables, los cuales constituyeron la evidencia empírica de la aplicabilidad operativa de la metodología propuesta.

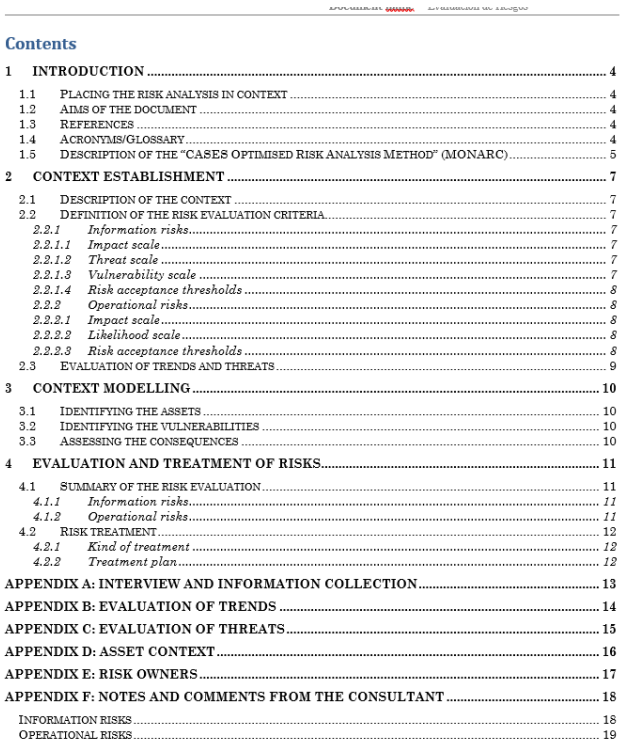
En este trabajo, la producción documental no se abordó como la descarga de un único reporte automático generado por el sistema, sino como una integración controlada de entregables derivados de cada etapa del proceso, permitiendo mantener trazabilidad metodológica y capacidad de revisión.

La Figura 3.4.3-1 evidencia la estructura automática del entregable documental producido por la herramienta, en la cual se organizan de forma jerárquica los componentes del análisis desarrollado: introducción del contexto, establecimiento de criterios de evaluación, modelado de activos, evaluación de riesgos de información y operativos, y definición del tratamiento de riesgos.

Se observa que el documento integra secciones asociadas a la definición de escalas de impacto, probabilidad y vulnerabilidad, así como umbrales de aceptación del riesgo, confirmando la incorporación acumulativa de la información registrada durante las etapas metodológicas previas. Asimismo, el índice incluye apéndices técnicos que documentan insumos del proceso analítico tales como entrevistas, evaluación de tendencias, caracterización de amenazas, contexto de activos y asignación de responsables, evidenciando la trazabilidad documental del análisis.

El documento completo del cual se extrae el fragmento se encuentra disponible para consulta en el Anexo I, donde se presenta la evaluación íntegra con sus matrices, mapas de riesgo y plan de tratamiento correspondiente.

Figura 3.4.3-1: Fragmento del índice del documento consolidado generado por MONARC correspondiente al caso simulado “PyME Servicios Colombia.



Contents

4. Conclusiones y recomendaciones

Este capítulo cierra la investigación mediante una lectura integrada de los resultados obtenidos y de las posibilidades de mejora derivadas del proceso desarrollado. En la primera parte se presentan las conclusiones, orientadas a valorar el cumplimiento del objetivo general y de los objetivos específicos gracias a los aportes alcanzados en cada fase. En la segunda parte se formulan recomendaciones, lecciones aprendidas y líneas de trabajo futuro, enfocadas en la actualización de referentes, el fortalecimiento metodológico, la adopción tecnológica, la validación en contextos reales y la transferencia de la metodología a pymes con recursos limitados.

4.1 Conclusiones

La investigación permitió construir una metodología de análisis y gestión de riesgos de seguridad informática para pymes del sector servicios en Colombia, con una orientación práctica, trazable y

ajustada a organizaciones con recursos limitados. El resultado no consistió en adoptar un único referente internacional ni en seleccionar una herramienta de forma aislada, sino en articular referentes, criterios de decisión, soporte tecnológico y validación aplicada dentro de un mismo proceso. De esta manera, el trabajo logró conectar la revisión conceptual con una propuesta operativa capaz de identificar activos críticos, valorar riesgos, definir tratamientos, asignar responsables y generar evidencias documentales para la toma de decisiones.

El aporte central de la investigación se expresa en la continuidad entre sus cuatro fases. La caracterización de referentes permitió construir una base metodológica híbrida; la selección de MONARC ofreció un soporte tecnológico coherente con esa base; la instrumentación demostró que la propuesta podía configurarse y ejecutarse dentro de la herramienta; y la prueba de escritorio permitió verificar su aplicabilidad en un escenario pyme controlado. Esta secuencia evidencia el cumplimiento del objetivo general, sin desconocer que la validación realizada demuestra ejecutabilidad y trazabilidad bajo condiciones controladas, pero no constituye una medición empírica generalizable del impacto en pymes reales. A partir de esta lectura global, las conclusiones siguientes desarrollan el aporte específico de cada fase, precisando los resultados obtenidos, su contribución al cumplimiento de los objetivos y las principales limitaciones que deben considerarse para futuras aplicaciones de la metodología.

4.1.1 Conclusiones de la fase I

El primer objetivo específico, orientado a caracterizar referentes internacionales para la gestión de riesgos de seguridad informática en pymes, se cumplió. La evidencia de este cumplimiento se encuentra en la sección 3.1, donde se documentan los cuatro productos metodológicos derivados de la Fase I: caracterización comparativa, criterios de adaptabilidad, modelo AHP y síntesis integradora. La caracterización comparativa homogénea de ISO/IEC 27005:2022, NIST SP 800-30 Rev. 1, MAGERIT v3.0, OCTAVE-S v1.0 y EBIOS Risk Manager permitió comparar referentes de distinta naturaleza —estándares, guías y metodologías— bajo enfoques con niveles diferentes de prescripción, profundidad técnica, carga documental y flexibilidad aplicativa, evitando tratarlos como equivalentes normativos y generando una base objetiva para su posterior evaluación. La evidencia se presenta en la Tabla 3.1.1-1.

El segundo aporte consistió en traducir las restricciones típicas de las pymes en criterios comparables de adaptabilidad. La definición de practicidad y simplicidad, consideraciones técnico-administrativas, recomendaciones para el tratamiento del riesgo y directrices para la implementación de controles convirtió limitaciones cualitativas —recursos reducidos, baja madurez, ausencia de personal especializado y necesidad de procesos simples— en atributos evaluables. Este resultado fortaleció la conexión entre el problema de investigación y el modelo de decisión multicriterio, como se evidencia en la Tabla 3.1.2-1.

Por su parte, la aplicación del AHP permitió priorizar los referentes analizados y reveló una tensión metodológica central: los enfoques con mayor solidez técnica no siempre son los más viables para pymes con baja capacidad operativa. OCTAVE-S v1.0 ocupó el primer lugar del ranking global por su orientación práctica y autodirigida, mientras que NIST SP 800-30 mostró fortalezas en criterios técnicos y de control. Esta lectura, respaldada en las Tablas 3.1.3-1 a 3.1.3-6 y en las Figuras 3.1.3-1 y 3.1.3-2, permitió direccionar la metodología hacia un equilibrio entre simplicidad, trazabilidad y suficiencia técnica, en lugar de privilegiar únicamente la profundidad documental.

El reporte de la Razón de Consistencia (CR) por matriz aportó transparencia al alcance del ejercicio AHP, además, respondió al criterio de rigor solicitado durante la evaluación. Aunque no todas las matrices se ubicaron por debajo del umbral convencional de 0,10, esta situación reconoció la complejidad de comparar referentes heterogéneos mediante consenso experto. La decisión no se sustentó únicamente en los valores iniciales del ranking, sino también en el análisis de sensibilidad presentado en la Tabla 3.1.3-7. Análisis de sensibilidad - Ranking bajo variaciones de ±10%-15% en pesos según criterios. La permanencia de OCTAVE-S v1.0 como primera alternativa en los escenarios de variación evaluados fortaleció la confianza en la selección y mostró que el resultado no dependía de una configuración puntual de pesos.

El producto de mayor alcance de la Fase I fue la síntesis integradora documentada en las Tablas 3.1.4-1, 3.1.4-2 y 3.1.4-3. Esta síntesis no adoptó un referente de manera excluyente, sino que articuló la estructura operativa de OCTAVE-S con componentes de ISO/IEC 27005, NIST SP 800-30, MAGERIT y EBIOS RM. Con ello, la fase aportó el fundamento metodológico central de la propuesta: una base híbrida, adaptable y trazable para gestionar riesgos de seguridad informática en pymes

del sector servicios. Como acierto principal, se logró vincular los referentes internacionales con restricciones reales de adopción; como limitación, se identificaron tensiones de consistencia en algunas matrices AHP y la antigüedad de OCTAVE-S v1.0 frente a amenazas digitales contemporáneas, mitigadas parcialmente mediante la integración de taxonomías y componentes de otros referentes.

4.1.2 Conclusiones de la fase II

El segundo objetivo específico, orientado a analizar herramientas y soluciones de software para la gestión de riesgos y seleccionar una alternativa de soporte para la metodología propuesta, se cumplió satisfactoriamente. La evidencia de este cumplimiento se encuentra en la sección 3.2, donde se documentan la caracterización técnico-funcional de herramientas, los criterios evaluativos, el modelo AHP y la selección final de MONARC como herramienta base para la instrumentación posterior. Esta fase permitió transitar de la definición metodológica construida en la Fase I a la identificación de una solución tecnológica capaz de soportar, de manera operativa, el ciclo de gestión de riesgos de seguridad informática en pymes.

El primer aporte de la fase fue la comparación técnico-funcional de cinco herramientas: MONARC, SimpleRisk, ERAMBA, PILAR y Pirani Risk. Esta comparación evidenció que las alternativas disponibles no poseen la misma naturaleza de licenciamiento, alcance funcional ni modelo de despliegue. Por ello, la fase no se limitó a identificar herramientas OpenSource, sino que incorporó soluciones open-core, comunitarias, propietarias y SaaS como referentes funcionales para establecer una evaluación más realista. La evidencia se presenta en la Tabla 3.2.1-1: Síntesis comparativa técnico-funcional de herramientas analizadas para la gestión de riesgos de seguridad informática y en los Anexos D y E, donde se documentan la matriz de preselección y las fichas técnicas de análisis funcional.

La definición de criterios evaluativos constituyó un segundo aporte relevante, porque tradujo las necesidades de instrumentación de la metodología en atributos comparables de software. Los criterios de gestión organizacional, análisis técnico, gestión de riesgos y viabilidad técnica y operativa permitieron valorar las herramientas no solo por sus funcionalidades aisladas, sino por su capacidad para estructurar información, soportar el ciclo de riesgo, generar trazabilidad y ser

implementadas en entornos con recursos limitados. A diferencia de los criterios de la Fase I, orientados a la simplicidad y practicidad del referente metodológico, estos criterios se enfocaron en la capacidad operativa de las herramientas, fortaleciendo la coherencia entre la síntesis integradora de la Fase I y la selección tecnológica de la Fase II.

La priorización mediante AHP mostró que la herramienta más adecuada no era necesariamente la más sencilla de desplegar ni la más sólida en una funcionalidad específica, sino aquella con mejor equilibrio frente al conjunto de criterios definidos. MONARC obtuvo la mayor ponderación global porque presentó una alineación más directa con la gestión de riesgos basada en activos, el uso de catálogos, la valoración del riesgo, el tratamiento y la reutilización de conocimiento. Aunque Pirani Risk, ERAMBA y SimpleRisk presentaron pesos globales cercanos, sus modelos de licenciamiento, restricciones funcionales o necesidades de parametrización limitaron su pertinencia como soporte principal de una metodología orientada a pymes y apoyada en soluciones abiertas. La evidencia se consolida en las Tablas 3.2.3-1 a 3.2.3-6 y en el Anexo F.

La trazabilidad del proceso de selección se sostuvo mediante la documentación de la matriz de preselección, las fichas técnicas de análisis funcional y el modelo AHP consignado en el Anexo F. No obstante, a diferencia de la Fase I, en esta fase no se incorporó un panel de expertos ni se desarrolló un análisis específico de consistencia mediante CR, por lo que la priorización debe interpretarse como una valoración estructurada del investigador principal, basada en evidencia documental. Esta condición no invalida la selección de MONARC, pero delimita su alcance metodológico y refuerza la necesidad de contrastar los juicios en futuras aplicaciones mediante panel experto, revisión por pares o análisis de sensibilidad.

Como acierto principal, la Fase II permitió seleccionar una herramienta coherente con la metodología propuesta y con las restricciones operativas del contexto pyme. La elección de MONARC no debe interpretarse como un veredicto universal frente a las demás alternativas, sino como el resultado de una ponderación específica orientada a instrumentar la metodología híbrida definida en la Fase I. Su limitación más relevante radica en que el análisis funcional se fundamentó principalmente en documentación oficial, repositorios y fichas técnicas, ante la escasez de estudios empíricos sobre estas herramientas en pymes latinoamericanas. Esta condición refuerza la necesidad de validar la herramienta seleccionada en escenarios aplicados y de contrastar, en

futuras investigaciones, los juicios del investigador con paneles expertos o pruebas comparativas en organizaciones reales.

4.1.3 Conclusiones de la fase III

El tercer objetivo específico se cumplió al usar MONARC como soporte técnico para operacionalizar la metodología propuesta de gestión de riesgos de seguridad informática en pymes. La sección 3.3 documenta este cumplimiento mediante el despliegue del entorno, la creación del análisis base, la parametrización del contexto, la configuración de escalas, el modelado de activos, la adaptación de catálogos, el tratamiento de riesgos y la generación de salidas documentales. Con esta fase, la investigación dejó de tener una metodología únicamente formulada en términos conceptuales y pasó a contar con un flujo técnico ejecutable dentro de una herramienta OpenSource.

La instrumentación mostró que MONARC puede operar en un entorno controlado y reproducible, sin exigir una infraestructura especializada. La máquina virtual configurada, el checklist de verificación del entorno y las evidencias de acceso y estabilidad permitieron comprobar que la herramienta puede instalarse y probarse bajo condiciones razonables para organizaciones con capacidades tecnológicas limitadas. Este resultado, respaldado en la Tabla 3.3.1-1 y en la Figura 3.3.1-1: Configuración de red de la VM de MONARC, es relevante porque confirma que la viabilidad técnica de la metodología no depende de plataformas propietarias ni de recursos de alto costo, sino de una configuración documentada y replicable.

Uno de los hallazgos más importantes de esta fase fue la correspondencia entre la metodología diseñada y los módulos funcionales de MONARC. El contexto, los activos críticos, los activos de soporte, las amenazas, las vulnerabilidades, los controles y las recomendaciones encontraron una representación operativa dentro de la herramienta. La Tabla 3.3.2-1 evidencia ese mapeo y permite concluir que MONARC no fue usado solo como repositorio de información, sino como medio para traducir los componentes metodológicos en registros, relaciones, catálogos, escalas y flujos de tratamiento.

La configuración de criterios de evaluación permitió ajustar la herramienta al enfoque híbrido construido en las fases anteriores. Las escalas de impacto, probabilidad, vulnerabilidad y umbrales de aceptación hicieron posible diferenciar el tratamiento de riesgos de información y riesgos

operativos, conservando la trazabilidad entre el modelo propuesto y el cálculo automatizado del riesgo. En términos metodológicos, esto demostró que MONARC puede representar tanto dimensiones de la tríada de la seguridad, como confidencialidad, integridad y disponibilidad, como impactos organizacionales asociados a reputación, operación, legalidad, finanzas y personas.

El modelado de activos y la adaptación de catálogos confirmaron la capacidad de reutilización y personalización de la herramienta. La estructura de activos primarios y secundarios permitió representar dependencias, mientras que los catálogos personalizados de amenazas, vulnerabilidades, controles y recomendaciones facilitaron la construcción de escenarios coherentes con una pyme del sector servicios. Este resultado es importante porque la metodología requiere partir de activos críticos y relaciones de dependencia, no de listas genéricas desconectadas del negocio. Las figuras de la sección 3.3 y el Anexo H respaldan la trazabilidad de esta configuración.

La verificación del flujo completo permitió comprobar que MONARC soporta la transición desde la evaluación hasta el tratamiento, seguimiento y generación de reportes. La herramienta calculó riesgos, clasificó escenarios por umbral, vinculó recomendaciones, registró responsables, recaculó riesgos residuales y generó artefactos documentales. La Tabla 3.3.5-1 muestra esta trazabilidad al consolidar valores antes y después del tratamiento, lo que permite concluir que la instrumentación no se limitó a configurar la herramienta, sino que logró ejecutar un ciclo funcional de gestión de riesgos.

El principal acierto de la Fase III fue convertir la propuesta metodológica en una base técnica reutilizable para la validación posterior. El análisis base, las escalas, los catálogos, el árbol de activos, las recomendaciones, los tratamientos y los reportes generados constituyeron la línea técnica que luego pudo ser reutilizada en la Fase IV. Con ello se demostró que la metodología propuesta en la Fase I podía ejecutarse mediante MONARC, no solo como registro documental, sino como flujo operativo de gestión de riesgos con contexto, valoración, tratamiento, seguimiento y generación de evidencias.

La experiencia de instrumentación también permitió reconocer que MONARC es una plataforma intuitiva y documentada, con repositorio en GitHub, página oficial, documentación técnica y videos educativos que facilitan desde la instalación hasta el uso general de sus funcionalidades. Los videos

se encuentran en inglés y pueden corresponder a versiones distintas, por ello, durante el uso de la versión más reciente se observaron diferencias en pantallas, rutas de navegación y disposición de ciertas funcionalidades. Esta situación no limita el uso de MONARC, sino que evidencia la evolución de la plataforma y las mejoras incorporadas en sus versiones actuales.

Aunque la herramienta puede ser utilizada por distintos perfiles, la calidad de la información registrada depende del conocimiento de quien realiza la parametrización y el análisis. Identificar activos, formular escenarios, asociar amenazas y vulnerabilidades, valorar impactos y definir tratamientos exige comprender el contexto y las particularidades organizacionales de la pyme. En el caso de los catálogos, el cargue exigió respetar la estructura de las plantillas para que MONARC interpretara correctamente los campos y dejara los elementos parametrizados, disponibles y seleccionables durante el análisis. Además, la herramienta permite marcar avances, identificar actividades completadas y reconocer elementos pendientes dentro del flujo de trabajo.

Respecto al idioma, los encabezados y nombres estructurales de algunos módulos permanecen fijos, pero las opciones, descripciones y contenidos parametrizados pueden registrarse en español, lo que facilita su adaptación a equipos locales. En consecuencia, la Fase III demostró que la metodología propuesta en la Fase I puede ejecutarse mediante MONARC, siempre que su adopción se acompañe de guías, plantillas y orientación metodológica para asegurar que la parametrización refleje adecuadamente las particularidades de la pyme.

4.1.4 Conclusiones de la fase IV

El cuarto objetivo específico, orientado a validar la metodología propuesta mediante su aplicación en un caso de estudio o prueba de escritorio en una pyme simulada, se cumplió satisfactoriamente. La evidencia de este cumplimiento se encuentra en la sección 3.4 y en el Anexo I, donde se documentan la construcción del caso simulado “PyME Servicios Colombia”, la ejecución del análisis de riesgos, el tratamiento propuesto, el plan de acción y los productos documentales generados. Esta fase permitió comprobar que la metodología no solo era conceptualmente coherente e instrumentalizable en MONARC, sino que podía ejecutarse de extremo a extremo sobre un escenario pyme plausible, construido a partir de patrones reales identificados en el instrumento de diagnóstico aplicado a 72 organizaciones.

La validación tuvo como punto de partida un escenario simulado diseñado para representar condiciones frecuentes en pymes del sector servicios: estructura pequeña, roles multifuncionales, dependencia de servicios digitales de bajo costo, madurez tecnológica limitada y ausencia de un responsable dedicado de seguridad de la información. Esta decisión permitió preservar la confidencialidad de organizaciones reales y, al mismo tiempo, mantener un contexto suficientemente representativo para probar el cumplimiento de la metodología. La utilidad del caso no radicó en reproducir una empresa específica, sino en construir un entorno controlado donde fuera posible verificar si las fases, productos y criterios definidos podían operar de forma articulada.

Un resultado especialmente significativo fue la reutilización del análisis base instrumentado en la Fase III. La funcionalidad de clonación de MONARC permitió transferir escalas, umbrales, catálogos, estructura jerárquica de activos y conjuntos de recomendaciones hacia una nueva instancia de validación, reduciendo el esfuerzo de preparación y conservando consistencia metodológica entre fases. Este hallazgo aporta valor práctico porque muestra que la metodología puede replicarse en ciclos sucesivos sin reconstruir desde cero toda la configuración, siempre que exista una base técnica previamente validada. Las figuras de clonación, contextualización y verificación de activos heredados respaldan esta trazabilidad en la sección 3.4.

La ejecución del caso permitió comprobar que el modelo soporta simultáneamente riesgos de información y riesgos operativos. Los escenarios evaluados incluyeron amenazas como ransomware, ingeniería social, denegación de servicio, exposición de datos, incumplimiento regulatorio, interrupción del servicio e indisponibilidad de personal clave. Más allá del número de escenarios, el aporte consistió en verificar que la metodología puede relacionar activos, amenazas, vulnerabilidades, impactos, probabilidad, tratamiento y riesgo residual dentro de un mismo flujo. De esta manera, la validación evidenció que la propuesta no se limita a una lectura técnica de amenazas digitales, sino que integra consecuencias organizacionales relevantes para la continuidad, el cumplimiento y la toma de decisiones en pymes.

El tratamiento de riesgos mostró que las recomendaciones vinculadas en MONARC pueden transformar el análisis en un plan de acción priorizado. Las medidas propuestas como capacitación, redundancia de conectividad, adecuación contractual, cifrado y autenticación multifactor fueron asociadas a responsables, fechas, presupuestos estimados y estados de seguimiento. Esta transición resulta clave para el cumplimiento del OE4, porque evidencia que la metodología no

termina en la identificación o valoración del riesgo, sino que produce insumos ejecutables para gestión, control y seguimiento. La gestión del plan de tratamiento, presentada en la sección 3.4, confirma la capacidad de convertir riesgos priorizados en acciones organizacionales auditables.

La generación automatizada del documento consolidado reforzó la trazabilidad del proceso completo. El entregable producido por MONARC integró contexto, criterios de evaluación, modelado de activos, evaluación de riesgos, tratamiento y apéndices técnicos, permitiendo conservar evidencia verificable de la validación. Este producto tiene importancia metodológica porque ofrece una salida documental revisable por terceros y útil para soportar decisiones del nivel directivo o ejercicios de auditoría. El Anexo I complementa esta evidencia al reunir la evaluación íntegra, las matrices, los mapas de riesgo y el plan de tratamiento del caso simulado.

El principal aporte de la Fase IV fue demostrar la ejecutabilidad, trazabilidad y suficiencia operativa de la metodología propuesta en un escenario pyme controlado. Los resultados permitieron verificar que los productos construidos en las fases previas tal como referente metodológico integrado, herramienta seleccionada, parametrización técnica y catálogos podían articularse en una validación funcional. Con esta fase, la investigación cerró el ciclo propositivo-aplicado: caracterizó referentes, seleccionó una herramienta, instrumentó el flujo metodológico y verificó su aplicación mediante una prueba de escritorio documentada. El alcance de esta validación debe interpretarse con prudencia. Al tratarse de un caso simulado, los valores de riesgo y las reducciones proyectadas no representan resultados empíricos generalizables ni reducciones garantizadas para cualquier pyme. Su valor se ubica en la validez de constructo: demostrar que la metodología puede ejecutarse, generar trazabilidad, producir salidas documentales y orientar decisiones de tratamiento bajo supuestos controlados. También se reconoce que la validación no incluyó medición sistemática de usabilidad con usuarios finales no especializados, por lo que sus resultados se circunscriben a la comprobación metodológica y técnica del flujo propuesto.

4.2 Recomendaciones, lecciones aprendidas y trabajo futuro

Las recomendaciones que se presentan surgen de las decisiones, aciertos y límites identificados durante el desarrollo de la investigación. Se orientan a aspectos concretos: actualización de referentes, mejora del uso de AHP, vigilancia tecnológica de herramientas GRC, adopción práctica de MONARC, validación en pymes reales, medición de usabilidad y construcción de materiales que

faciliten la apropiación por parte de equipos no especializados. También, recoge aprendizajes derivados de la ejecución técnica y metodológica de las cuatro fases. Estos aprendizajes permiten advertir qué conviene hacer y qué debe evitarse al aplicar una metodología de gestión de riesgos en contextos pyme: no adoptar referentes de forma cerrada, no seleccionar herramientas solo por costo o disponibilidad, no usar MONARC como si produjera el análisis por sí sola, no comunicar reducciones de riesgo simuladas como mejoras garantizadas y no generalizar resultados sin validaciones reales.

4.2.1 Recomendaciones, lecciones aprendidas y trabajo futuro de la fase I

A partir de los hallazgos y las limitaciones de la Fase I, se recomienda que futuras caracterizaciones de referentes internacionales para la gestión de riesgos incorporen revisiones periódicas de estándares, guías y metodologías, especialmente cuando el referente seleccionado tenga una versión oficial con varios años de antigüedad. En este caso, OCTAVE-S v1.0 demostró alta pertinencia para pymes por su practicidad y orientación a organizaciones pequeñas; sin embargo, su vigencia documental exige complementarlo con taxonomías, catálogos de amenazas y criterios de valoración provenientes de referentes más recientes. Por tanto, no se recomienda adoptar un único referente de manera aislada o cerrada, sino mantener una lógica integradora que permita actualizar activos, amenazas, vulnerabilidades y controles conforme evolucione el entorno tecnológico.

En futuras aplicaciones del AHP se recomienda fortalecer la trazabilidad del juicio experto desde el inicio del proceso. Para ello, conviene conservar las matrices individuales preliminares, documentar las razones de desacuerdo durante la deliberación, registrar la matriz consensuada final y reportar explícitamente los valores de Razón de Consistencia (CR) por cada matriz. Esta recomendación surge de la experiencia de la Fase I, donde algunas matrices superaron el umbral convencional de consistencia, situación asociada a la comparación de referentes heterogéneos mediante consenso experto. No se recomienda ocultar o generalizar los valores de CR bajo una afirmación global de

consistencia; por el contrario, se recomienda presentar de forma transparente, interpretarse metodológicamente y complementarse con análisis de sensibilidad.

También se recomienda que los estudios que utilicen AHP en contextos similares apliquen mecanismos complementarios para fortalecer la confiabilidad del proceso decisorio. Entre ellos se encuentran la revisión de transitividad para identificar comparaciones que generan mayor tensión, la contrastación de escalas alternativas a la escala lineal de Saaty, y cuando se disponga de matrices individuales, usar métodos de agregación de juicios o medidas de concordancia entre expertos. Se reconoce que estas acciones no sustituyen el criterio experto, pero ayudan a explicar mejor la estabilidad del ranking y a reducir el riesgo de que la selección final dependa de una configuración puntual de pesos o de consensos insuficientemente documentados.

Una lección aprendida relevante fue la importancia de operacionalizar los criterios de adaptabilidad antes de iniciar las comparaciones por pares. La definición clara de practicidad y simplicidad, consideraciones técnico-administrativas, recomendaciones para el tratamiento del riesgo y directrices para la implementación de controles permitió reducir ambigüedades y orientar la discusión del panel hacia condiciones reales de adopción en pymes. En consecuencia, no se recomienda iniciar un AHP únicamente con nombres generales de criterios; cada criterio debe contar con definición operativa, indicadores observables y relación explícita con las restricciones del contexto evaluado.

Como línea de trabajo futuro, se recomienda validar la síntesis integradora derivada de la Fase I en escenarios empresariales reales, no solo mediante pruebas de escritorio. Una aplicación en pymes del sector servicios permitiría contrastar si la combinación entre OCTAVE-S, ISO/IEC 27005, NIST SP 800-30, MAGERIT y EBIOS RM conserva su utilidad cuando intervienen restricciones organizacionales reales, disponibilidad limitada de personal, tiempos reducidos y datos incompletos. Esta validación ayudaría a ajustar los

catálogos de activos, amenazas, vulnerabilidades y controles, así como a determinar qué elementos de la metodología deben simplificarse, automatizarse o reforzarse.

Finalmente, se recomienda avanzar hacia enfoques de gestión dinámica del riesgo, incorporando ciclos de revisión más cortos, actualización periódica de catálogos, mecanismos de retroalimentación y, cuando la madurez organizacional lo permita, automatización parcial de la identificación y monitoreo de amenazas. La Fase I dejó una base metodológica adaptable, pero su evolución futura dependerá de la capacidad para mantener actualizados los insumos del análisis y reducir la dependencia de procesos manuales. En ese sentido, no se recomienda tratar la caracterización de referentes como un ejercicio único e inmutable, sino como una base revisable que debe ajustarse ante cambios tecnológicos, regulatorios y operativos.

4.2.2 Recomendaciones, lecciones aprendidas y trabajo futuro de la fase II

La Fase II dejó como principal aprendizaje que la selección de una herramienta para gestión de riesgos no debe basarse únicamente en su condición de gratuita, OpenSource o de fácil despliegue. En futuras investigaciones o implementaciones institucionales se recomienda evaluar las soluciones tecnológicas desde una perspectiva funcional, metodológica y operativa, considerando su capacidad para soportar el ciclo completo de gestión de riesgos, generar trazabilidad, permitir parametrización y ajustarse a las capacidades reales de las pymes. No se recomienda seleccionar una herramienta solo por disponibilidad o bajo costo, ya que una solución aparentemente accesible puede resultar insuficiente si no permite documentar activos, amenazas, vulnerabilidades, tratamientos, responsables, estados y evidencias.

La comparación realizada evidenció que el ecosistema de herramientas para gestión de riesgos es heterogéneo: algunas soluciones son OpenSource, otras open-core, comunitarias, propietarias, SaaS o freemium. Por ello, en trabajos posteriores se recomienda ampliar la vigilancia tecnológica hacia herramientas emergentes o no consideradas en esta investigación, entre ellas CISO Assistant, OpenGRC, Artica Forge u otras plataformas GRC ligeras adaptables a contextos pyme. En el caso

particular de CISO Assistant, su enfoque OpenSource, su orientación a GRC, evaluación de riesgos, auditoría, marcos de referencia y gestión de evidencias la convierten en una alternativa relevante para comparaciones futuras frente a MONARC, especialmente si se busca evaluar capacidades de cumplimiento, trazabilidad, reutilización de referentes y gestión integrada de programas de ciberseguridad.

También se recomienda diferenciar con precisión el modelo de licenciamiento, las restricciones funcionales y las condiciones de despliegue de cada herramienta antes de incluirla en un proceso de priorización. No se debe asumir que una versión gratuita equivale a una solución OpenSource plena, ni que una alternativa SaaS es automáticamente viable para pymes sin evaluar dependencia del proveedor, tratamiento de datos, costos futuros, posibilidades de exportación y sostenibilidad operativa. Esta precaución es especialmente importante cuando se comparan herramientas con ediciones comunitarias, planes comerciales, despliegue en nube, despliegue on-premise o modelos híbridos.

Para futuras aplicaciones del AHP en selección de herramientas tecnológicas, se recomienda fortalecer el proceso de juicio mediante revisión por pares o panel experto. La Fase II permitió estructurar una valoración documentada desde el investigador principal; sin embargo, una réplica con administradores de sistemas, responsables de seguridad informática, consultores y usuarios de pymes permitiría contrastar los pesos asignados y reducir el sesgo de una evaluación unipersonal. En ese escenario, podrían incorporarse mecanismos de concordancia como W de Kendall, siempre que existan varios evaluadores y matrices individuales que permitan calcular el grado de acuerdo. No se recomienda presentar métricas de concordancia si no fueron aplicadas ni existen los insumos necesarios para su cálculo.

Una lección práctica de esta fase fue que los criterios de evaluación deben formularse con suficiente detalle antes de iniciar cualquier comparación. Los criterios de gestión organizacional, análisis técnico, gestión de riesgos y viabilidad técnica y operativa permitieron orientar la selección porque fueron asociados con evidencias observables, tales como registro de activos, configuración de escalas, generación de reportes, requisitos de despliegue y capacidad de seguimiento. En futuras evaluaciones no conviene usar criterios genéricos como “facilidad de uso” o “mejor

herramienta" sin definición operativa, ya que esto aumenta la ambigüedad y debilita la trazabilidad del juicio.

Respecto a MONARC, se recomienda que las pymes del sector servicios lo adopten mediante una prueba piloto de alcance reducido antes de extenderlo a toda la organización. Una implementación inicial sobre un conjunto limitado de activos críticos permite validar la curva de aprendizaje, ajustar catálogos, revisar escalas de impacto y probabilidad, y determinar si el equipo interno puede sostener la operación de la herramienta. No se recomienda iniciar la adopción con un inventario amplio o con todos los procesos de la empresa, porque esto puede aumentar la carga documental y generar rechazo temprano frente a la metodología.

También se recomienda fortalecer los materiales de apropiación de MONARC en español y adaptarlos a pymes latinoamericanas. La herramienta ofrece capacidades relevantes para modelar riesgos basados en activos y reutilizar conocimiento; no obstante, su adopción puede verse limitada si los equipos no cuentan con guías simples, ejemplos sectoriales, catálogos contextualizados y rutas de configuración inicial. Esta recomendación puede ser asumida por comunidades OpenSource, instituciones académicas, programas de transformación digital o grupos de investigación interesados en cerrar la brecha entre herramientas especializadas y organizaciones con baja madurez en seguridad informática.

Como trabajo futuro, la selección de MONARC abre la posibilidad de avanzar hacia evaluaciones más empíricas y comparativas. Sería conveniente aplicar la herramienta en pymes reales del sector servicios, medir tiempos de parametrización, esfuerzo requerido por el equipo, comprensión de los usuarios, utilidad de los reportes y capacidad de seguimiento de los planes de tratamiento. No se debe considerar que el ranking obtenido en esta investigación sea universal o definitivo; su valor está en haber seleccionado la herramienta más coherente con los criterios definidos para esta metodología, pero otros contextos podrían modificar las ponderaciones y favorecer alternativas como ERAMBA, SimpleRisk, Pirani Risk o incluso herramientas emergentes como CISO Assistant.

Una línea adicional de desarrollo consiste en explorar la integración de MONARC con herramientas de escaneo de vulnerabilidades, fuentes de inteligencia de amenazas y mecanismos de actualización de catálogos. Esta evolución permitiría acercar la metodología a modelos de gestión dinámica del riesgo, reduciendo la dependencia de procesos manuales y facilitando revisiones más

frecuentes. No obstante, dicha integración debe realizarse de forma gradual, evitando sobrecargar a pymes con capacidades técnicas limitadas o convertir una metodología orientada a la practicidad en un esquema complejo difícil de sostener.

Finalmente, se recomienda que los programas de maestría en seguridad informática y los centros de investigación promuevan contribuciones aplicadas a herramientas OpenSource existentes. En lugar de limitar los trabajos de grado al análisis comparativo de software, existe una oportunidad para desarrollar guías, traducciones, plantillas, catálogos sectoriales, scripts de apoyo o extensiones funcionales que fortalezcan la adopción de herramientas como MONARC o permitan evaluar nuevas alternativas GRC abiertas. Esta orientación permitiría que la investigación académica produzca resultados reutilizables y contribuya de forma directa a mejorar las capacidades de gestión de riesgos en pymes.

4.2.3 Recomendaciones, lecciones aprendidas y trabajo futuro de la fase III

La experiencia de instrumentación realizada en la Fase III deja una recomendación central: MONARC debe adoptarse como una herramienta metodológica, no solo como una aplicación tecnológica. Su instalación y navegación pueden ser abordadas con apoyo de la documentación oficial, el repositorio GitHub y los videos educativos disponibles, pero la utilidad del análisis depende de preparar previamente el alcance, los criterios, los catálogos y los responsables. No se recomienda iniciar la implementación con la expectativa de que la herramienta “produzca” el análisis por sí misma; MONARC facilita el registro, cálculo, tratamiento y seguimiento, pero la calidad del resultado depende del criterio con el que se traduzca la realidad de la pyme en activos, amenazas, vulnerabilidades, impactos y controles.

Para una primera adopción en pymes del sector servicios, conviene trabajar con un alcance reducido y manejable. Una buena práctica consiste en seleccionar pocos activos críticos, parametrizar escalas simples, cargar catálogos mínimos y ejecutar un ciclo completo antes de ampliar el uso a más procesos o áreas. No se recomienda comenzar con inventarios extensos, catálogos demasiado amplios o múltiples unidades organizacionales en paralelo, porque esa

decisión puede convertir una metodología diseñada para ser práctica en una carga documental difícil de sostener.

La preparación de plantillas debe asumirse como una actividad previa obligatoria. El cargue de catálogos en MONARC requiere respetar la estructura definida por la herramienta para que los campos sean interpretados correctamente y queden disponibles durante el análisis. Por ello, se recomienda construir plantillas institucionales validadas de activos, amenazas, vulnerabilidades, controles y recomendaciones, preferiblemente con ejemplos en español y convenciones de codificación estables. No se debe modificar la estructura de los archivos de importación sin pruebas previas, ni cargar catálogos sin revisar consistencia semántica, duplicidades o correspondencia con el contexto organizacional.

La adopción de MONARC también requiere definir un perfil responsable que combine conocimiento del negocio y criterio técnico en seguridad informática. Aunque la herramienta puede ser usada por distintos perfiles, el análisis pierde valor si quien diligencia la información no comprende los procesos, activos críticos, amenazas plausibles, vulnerabilidades reales y consecuencias operativas para la pyme. No se recomienda delegar la parametrización únicamente a un operador técnico ni únicamente a un usuario funcional; el mejor resultado se obtiene cuando existe acompañamiento entre personal del negocio, responsable de TI y apoyo metodológico en gestión de riesgos.

Para fortalecer la sostenibilidad del uso, cada implementación debería dejar una bitácora técnica y metodológica. Esta bitácora debe registrar versión instalada, decisiones de parametrización, catálogos cargados, cambios realizados, responsables, evidencias generadas y criterios usados para aceptar o tratar riesgos. No se recomienda ejecutar análisis sucesivos sin control de versiones o sin documentar ajustes, porque se pierde trazabilidad y se dificulta explicar por qué un riesgo cambió, por qué se modificó un umbral o por qué se seleccionó una recomendación específica.

Como línea de mejora práctica, sería valioso construir un paquete de adopción de MONARC para pymes latinoamericanas. Este paquete podría incluir plantillas CSV validadas, catálogos mínimos por sector, guía rápida en español, ejemplos de activos críticos, recomendaciones típicas, glosario técnico y una ruta de implementación por semanas. No se recomienda que cada pyme construya

desde cero sus catálogos y guías, porque eso aumenta el esfuerzo inicial y produce resultados poco comparables entre organizaciones similares.

El trabajo futuro debería concentrarse en medir la adopción real de la herramienta, no solo su funcionamiento técnico. Sería útil evaluar tiempo de configuración, comprensión de usuarios, esfuerzo de mantenimiento, utilidad de los reportes, facilidad para hacer seguimiento al plan de tratamiento y capacidad de reutilizar catálogos en ciclos posteriores. No se debe asumir que una instrumentación exitosa en laboratorio garantiza apropiación organizacional; la validación en entornos reales debe incluir factores humanos, disponibilidad de tiempo, responsabilidades internas y cultura de gestión del riesgo.

Una evolución razonable consiste en desarrollar utilidades que faciliten la conversión de catálogos externos a formatos compatibles con MONARC. Esto podría reducir trabajo repetitivo y mejorar la actualización de amenazas, vulnerabilidades y recomendaciones. Aun así, cualquier automatización debe mantener revisión humana, porque los catálogos no son neutros: deben ajustarse al sector, tamaño, procesos, exposición tecnológica y restricciones de cada pyme. Automatizar sin contextualizar puede generar análisis genéricos, extensos y poco útiles.

Finalmente, las universidades, grupos de investigación y comunidades podrían aportar valor produciendo materiales reutilizables para la adopción de herramientas GRC abiertas. En lugar de limitarse a comparar software, futuros trabajos podrían desarrollar guías, traducciones, laboratorios, catálogos sectoriales, plantillas y extensiones funcionales para MONARC u otras plataformas similares. Esta línea permitiría que las tesis de profundización no solo evalúen herramientas, sino que dejen artefactos prácticos para reducir la brecha entre conocimiento de referentes para la gestión de riesgos de seguridad informática y aplicación real en pymes.

4.2.4 Recomendaciones, lecciones aprendidas y trabajo futuro de la fase IV

La principal recomendación derivada de la Fase IV es avanzar desde la prueba de escritorio hacia estudios de caso con pymes reales del sector servicios en Colombia. La validación simulada permitió comprobar ejecutabilidad, trazabilidad y suficiencia documental, pero todavía se requiere contrastar la metodología con información real de procesos, activos, responsables, controles

existentes y restricciones operativas. No se debe presentar el caso “PyME Servicios Colombia” como evidencia de efectividad empírica generalizable; su aporte fue demostrar que el flujo puede ejecutarse de manera coherente, no probar que las reducciones proyectadas ocurrirán en cualquier organización.

Una validación posterior debería incluir participación de actores internos de la pyme, no solo la ejecución técnica por parte del investigador. Conviene involucrar a gerencia, responsables de TI, líderes de proceso y personal administrativo para observar cómo entienden los activos, cómo interpretan los escenarios de riesgo, qué tan útil consideran el plan de tratamiento y qué dificultades encuentran al revisar los reportes. No basta con que la herramienta calcule valores y genere documentos; la metodología debe ser comprensible para quienes toman decisiones y para quienes tienen que ejecutar las acciones de tratamiento.

El plan de tratamiento requiere una validación gerencial más fuerte en futuras aplicaciones. Las acciones propuestas deben revisarse con criterios de viabilidad presupuestal, disponibilidad de responsables, urgencia operativa, dependencia entre controles y capacidad real de implementación. No se recomienda presentar las recomendaciones únicamente como una lista técnicamente correcta de controles; deben convertirse en una ruta de decisión para la pyme, con acciones priorizadas, costos estimados, responsables reconocidos por la organización y evidencias mínimas para demostrar avance.

Las reducciones de riesgo calculadas en la prueba de escritorio deben usarse con prudencia. En escenarios simulados, los valores de probabilidad, impacto, vulnerabilidad y reducción dependen del juicio experto y de supuestos controlados; por tanto, no deben comunicarse como porcentajes garantizados de mejora. Para validaciones reales, se recomienda acompañar los puntajes con una explicación ejecutiva de su alcance, indicando que sirven para priorizar decisiones y comparar escenarios, no para prometer resultados automáticos. No se debe convertir el cálculo residual en una afirmación de efectividad sin verificar la implementación real del control.

La alineación de las recomendaciones con controles de referencia debe mantenerse, pero evitando una adopción mecánica de estándares. En futuras validaciones, cada control debería justificar qué riesgo reduce, sobre qué activo actúa, qué responsable lo puede ejecutar y qué evidencia permitirá verificar su implementación. No se recomienda afirmar que una medida es pertinente solo porque

aparece en ISO/IEC 27001 o en otro referente; su pertinencia debe demostrarse frente al contexto de la pyme, el nivel de exposición identificado y la capacidad operativa disponible.

Para fortalecer la validez externa, resulta necesario replicar la metodología en pymes con distintos niveles de madurez digital, tamaños y subsectores de servicios. Una sola aplicación real permitiría ajustar el procedimiento; varias aplicaciones permitirían identificar patrones comunes, restricciones recurrentes y componentes reutilizables. No conviene generalizar la metodología a todo el universo pyme sin someterla a escenarios diversos, porque las prioridades de riesgo, los activos críticos y la capacidad de tratamiento cambian significativamente entre organizaciones.

También se recomienda incorporar una evaluación de usabilidad y apropiación de la metodología. Instrumentos como SUS (cuestionario utilizado para medir la usabilidad percibida de un sistema, producto o servicio), entrevistas breves, observación guiada podrían medir el esfuerzo requerido, la comprensión del flujo, la utilidad de los reportes y la facilidad para hacer seguimiento al plan de tratamiento. No se debe asumir que una metodología es adoptable solo porque fue ejecutable técnicamente; la adopción depende de que los usuarios comprendan el proceso, reconozcan su valor y puedan sostenerlo con los recursos disponibles.

La transferencia de la metodología exige productos menos académicos y más cercanos a la toma de decisiones. Sería útil elaborar una guía ejecutiva en español para propietarios, gerentes y responsables operativos de pymes, con ejemplos de activos, escenarios de riesgo, controles mínimos, evidencias esperadas y preguntas de decisión. No se recomienda comunicar la propuesta únicamente mediante lenguaje normativo o técnico, esto es una barrera de apropiación, su adopción depende de que la dirección entienda cómo la gestión de riesgos protege continuidad, información de clientes, cumplimiento legal y sostenibilidad operativa.

Como trabajo futuro, la metodología podría evolucionar hacia esquemas de revisión periódica y gestión dinámica del riesgo, pero sin perder su carácter práctico. La integración con fuentes de inteligencia de amenazas, catálogos sectoriales o herramientas de escaneo puede aportar valor cuando la pyme ya cuenta con inventario de activos y de riesgos, responsables, criterios de aceptación y disciplina mínima de seguimiento. No se recomienda incorporar automatización avanzada en organizaciones que aún no han consolidado lo básico, porque podría aumentar la

complejidad sin mejorar la capacidad real de decisión, la idea es hacer del ejercicio un proceso gradual y de mejora continua.

Finalmente, las instituciones académicas y centros de investigación pueden aportar valor mediante ejercicios de validación aplicada, no solo mediante nuevas revisiones documentales. Las tesis de profundización podrían replicar la metodología en sectores específicos, comparar resultados entre pymes, medir usabilidad, construir guías ejecutivas o desarrollar paquetes de evidencias para auditoría. No se trata de repetir la metodología como ejercicio académico, sino de probar su utilidad en condiciones organizacionales concretas y producir artefactos que faciliten su transferencia a empresas con recursos limitados.

B. Anexo: Matriz de Consistencia

Elemento	Descripción
1. Pregunta de investigación	¿Cómo, a partir de normas internacionales de seguridad de la información y herramientas OpenSource, se puede proponer una metodología que permita a las PyMEs del sector servicios en Colombia gestionar los riesgos de seguridad informática de manera efectiva durante el periodo de julio de 2023 a junio de 2024?
2. Enfoque y alcance de la investigación	**Enfoque:** Mixto (cualitativo y cuantitativo), con uso de encuestas estructuradas y análisis AHP para priorización de normas y herramientas de software open source. **Alcance:** Proponer una metodología basada en normas internacionales y herramientas OpenSource, adaptada a PyMEs del sector servicios en Colombia para el período julio 2023 – junio 2024. **Diseño metodológico:** Propositivo-aplicado, validada mediante un caso de estudio o prueba de escritorio en una PyME colombiana del sector servicios.
3. Problema de investigación	Muchas PyMEs colombianas del sector servicios carecen de metodologías integrales y sistemáticas que combinen normas internacionales de seguridad de la información y herramientas OpenSource accesibles para gestionar riesgos de seguridad informática de manera efectiva, afectando la protección de sus activos y operaciones, especialmente durante el periodo de julio de 2023 a junio de 2024.
4. Objetivos de la investigación	**Objetivo general:** Proponer una metodología para el análisis y gestión de riesgos de seguridad informática en PyMEs, basada en normas internacionales y software OpenSource disponibles, que fortalezca la seguridad y contribuya a la protección de sus activos y operaciones. **Objetivos específicos:** 1. Caracterizar normas internacionales para la gestión de riesgos comprendiendo los principios, directrices y requisitos que se puedan ajustar a la seguridad informática en las PyMEs. 2. Analizar herramientas y soluciones de software OpenSource que puedan ajustarse a la gestión de riesgos, seleccionando uno o varios softwares a utilizar. 3. Usar el (los) software OpenSource para la gestión de riesgos en seguridad informática en las PyMEs y que dé cumplimiento a la metodología propuesta. 4. Validar la metodología propuesta a través de su aplicación con un caso de estudio o prueba de escritorio en una PyME.
5. Variables de studio	**Variable independiente:** Aplicación de metodología basada en normas internacionales y software OpenSource. **Variable dependiente:** Nivel de gestión de riesgos de seguridad informática en la PyME.
6. Hipótesis	**Hipótesis general:** La integración de normas internacionales de seguridad de la información con herramientas OpenSource permitirá una gestión más efectiva de los riesgos en las PyMEs colombianas del sector servicios, contribuyendo al fortalecimiento de la protección de sus activos y operaciones.

Elemento	Descripción
	Hipótesis específicas: 1. La comprensión de principios, directrices y requisitos de normas internacionales facilita la selección de aquellas que son más adaptables a las PyMEs del sector servicios. 2. El uso de herramientas OpenSource para la gestión de riesgos se asocia positivamente con la percepción de facilidad y eficiencia en la gestión de riesgos de seguridad informática en PyMEs. 3. La integración de normas internacionales y herramientas OpenSource permite estructurar una metodología más ajustada a la identificación, evaluación y tratamiento de riesgos en PyMEs del sector servicios. 4. La validación de la metodología propuesta en un caso de estudio con MONARC evidenciará un fortalecimiento en la protección de activos y en la gestión de riesgos de seguridad informática en las PyMEs.

C. Anexo: Matriz de Operacionalización

Variable	Definición Conceptual	Definición Operacional	Dimensiones	Indicadores
Variable Independiente: Aplicación de metodología basada en normas internacionales y software Open Source	Es el uso integrado de referentes internacionales para la gestión de riesgos (ISO/IEC 27005, NIST SP 800-30, MAGERIT, OCTAVE-S, EBIOS RM) y herramientas Open Source (PILAR, MONARC, ERAMBA, SimpleRisk, Pirani Risk) para evaluar y mitigar riesgos de seguridad informática en PyMEs. Estas metodologías proporcionan estructuras sistemáticas para identificar, evaluar y tratar riesgos (Valencia Duque & Orozco, 2017; Crespo Martínez, 2017).	Se mide mediante: análisis documental de normas (ISO, NIST, etc.), evaluación de herramientas usando criterios definidos (funcionalidad, usabilidad, costo, compatibilidad), priorización con método AHP, y aplicación práctica simulada en PyME. Instrumentos: análisis documental, entrevistas a expertos y método AHP.	- Capacidad normativa (aplicabilidad a PyME) - Evaluación de herramientas - Aplicación práctica en entorno PyME	- Ranking de normas según aplicabilidad - Ranking de herramientas según criterios AHP - Informe de aplicación práctica de herramienta (MONARC)
Variable Dependiente: Nivel de gestión de riesgos de seguridad informática en la PyME	Se refiere a la capacidad organizacional para identificar, analizar, evaluar y tratar los riesgos asociados a la seguridad de la información en el contexto específico de las pequeñas y medianas empresas (PyMEs), considerando las amenazas, vulnerabilidades y consecuencias que puedan afectar la confidencialidad, integridad y disponibilidad de los activos. Según la ISO/IEC 27005:2022	Se medirá a través de la aplicación práctica de la metodología propuesta (con base en ISO/IEC 27005, MAGERIT, NIST 800-30, OCTAVE-S, EBIOS RM) y soportada por software Open Source (como MONARC). Se evaluarán las capacidades de la PyME para identificar, evaluar y tratar riesgos en un escenario simulado. Instrumento: Lista de verificación	1. Identificación de riesgos 2. Evaluación de riesgos 3. Tratamiento de riesgos	1. Número y claridad de los activos identificados y su valor 2. Cantidad de amenazas y vulnerabilidades asociadas por activo 3. Nivel de riesgo residual identificado 4. Número y pertinencia de los controles propuestos

y la guía ISO 73:2009, esta gestión debe ser sistemática, documentada y continuamente mejorada (ISO/IEC 27005:2022; ISO Guide 73:2009).	estructurada y análisis de reportes generados por el software MONARC, triangulado con entrevistas semiestructuradas a responsables del proceso.	5. Cobertura del plan de tratamiento sobre los riesgos prioritarios

D. Anexo: Modelo AHP para la Selección del referente internacional de trabajo

Matriz de comparación pareada									
	Practicidad y Simplicidad	Consideraciones Técnicas y Administrativas	Recomendaciones para el Tratamiento de Riesgos	Directrices para la Implementación de Controles	Matriz normalizada				Vector Promedio
Practicidad y Simplicidad	1.00	4.00	5.00	6.00	0.62	0.72	0.54	0.43	0.57
Consideraciones Técnicas y Administrativas	0.25	1.00	3.00	4.00	0.15	0.18	0.32	0.29	0.24
Recomendaciones para el Tratamiento de Riesgos	0.20	0.33	1.00	3.00	0.12	0.06	0.11	0.21	0.13
Directrices para la Implementación de Controles	0.17	0.25	0.33	1.00	0.10	0.04	0.04	0.07	0.06
Totales	1.62	5.58	9.33	14.00					

Ponderación de criterios vs. elementos											
	Practicidad y Simplicidad					Matriz normalizada					Vector promedio
	ISO 27005	NIST 800-30	MAGERIT	OCTAVE	EBIOS						
ISO 27005	1.00	0.33	0.20	0.13	0.20	0.05	0.02	0.02	0.07	0.03	0.04
NIST 800-30	3.00	1.00	0.25	0.14	0.33	0.14	0.07	0.03	0.08	0.06	0.07
MAGERIT	5.00	4.00	1.00	0.20	0.33	0.23	0.26	0.11	0.12	0.06	0.15
OCTAVE-S	8.00	7.00	5.00	1.00	4.00	0.36	0.46	0.53	0.58	0.68	0.52
EBIOS	5.00	3.00	3.00	0.25	1.00	0.23	0.20	0.32	0.15	0.17	0.21
Totales	22.00	15.33	9.45	1.72	5.87						

Ponderación de criterios vs. elementos											
	Consideraciones Técnicas y Administrativas					Matriz normalizada					Vector promedio
	ISO 27005	NIST 800-30	MAGERIT	OCTAVE	EBIOS						
ISO 27005	1.00	0.33	3.00	1.00	3.00	0.18	0.13	0.20	0.12	0.45	0.22
NIST 800-30	3.00	1.00	3.00	3.00	2.00	0.53	0.40	0.20	0.37	0.30	0.36
MAGERIT	0.33	0.33	1.00	0.20	0.33	0.06	0.13	0.07	0.02	0.05	0.07
OCTAVE-S	1.00	0.33	5.00	1.00	0.33	0.18	0.13	0.33	0.12	0.05	0.16
EBIOS	0.33	0.50	3.00	3.00	1.00	0.06	0.20	0.20	0.37	0.15	0.19
Totales	5.67	2.50	15.00	8.20	6.67						

Ponderación de criterios vs. elementos											
	Recomendaciones para el Tratamiento de Riesgo					Matriz normalizada					Vector promedio
	ISO 27005	NIST 800-30	MAGERIT	OCTAVE	EBIOS						
ISO 27005	1.00	1.00	3.00	5.00	3.00	0.35	0.35	0.23	0.38	0.38	0.34
NIST 800-30	1.00	1.00	3.00	5.00	3.00	0.35	0.35	0.23	0.38	0.38	0.34
MAGERIT	0.33	0.33	1.00	0.33	0.33	0.12	0.12	0.08	0.03	0.04	0.08
OCTAVE-S	0.20	0.20	3.00	1.00	0.50	0.07	0.07	0.23	0.08	0.06	0.10
EBIOS	0.33	0.33	3.00	2.00	1.00	0.12	0.12	0.23	0.15	0.13	0.15
Totales	2.87	2.87	13.00	13.33	7.83						

Ponderación de criterios vs. elementos											
	Directrices para la Implementación de Controles					Matriz normalizada					Vector promedio
	ISO 27005	NIST 800-30	MAGERIT	OCTAVE	EBIOS						
ISO 27005	1.00	0.17	3.00	7.00	7.00	0.13	0.10	0.32	0.30	0.33	0.24
NIST 800-30	6.00	1.00	5.00	8.00	8.00	0.80	0.62	0.53	0.35	0.37	0.53
MAGERIT	0.20	0.20	1.00	5.00	5.00	0.03	0.12	0.11	0.22	0.23	0.14
OCTAVE-S	0.14	0.13	0.20	1.00	0.50	0.02	0.08	0.02	0.04	0.02	0.04
EBIOS	0.14	0.13	0.20	2.00	1.00	0.02	0.08	0.02	0.09	0.05	0.05
Totales	7.49	1.62	9.40	23.00	21.50						

MATRIZ JERÁRQUICA						
	Practicidad y Simplicidad	Consideraciones Técnicas y Administrativas	Recomendaciones para el Tratamiento de Riesgos	Directrices para la Implementación de Controles	**Total**	Orden de ponderación
ISO 27005	0.04	0.22	0.34	0.24	13.10%	4
NIST 800-30	0.07	0.36	0.34	0.53	20.34%	2
MAGERIT	0.15	0.07	0.08	0.14	12.24%	5
OCTAVE-S	0.52	0.16	0.10	0.04	35.40%	1
EBIOS	0.21	0.19	0.15	0.05	18.92%	3
Ponderación	0.57	0.24	0.13	0.06		

E. Anexo: Matriz de preselección de herramientas para la gestión de riesgos

Campo	Qué registrar	Valores esperados
Tipo/Enfoque (Nivel 1)	Clasifica dominio/categoría. Si no es GRC-SI → descarte y resto N/A.	GRC - Seguridad de la Información; GRC - Riesgos Operativos (ERM); GRC - Riesgos Financieros; GRC - Riesgos Laborales (SST); Vulnerability Scanner; Project Management; SIEM / IDS; ITSM / CMDB / Activos; Security Assessment Tool; Por verificar
Licencia / Modelo	Etiqueta breve de licencia y modalidad.	AGPLv3; GPLv3; MPL2.0; Propietaria (SaaS); Community/source-available
OSS verificable (Nivel 2)	¿Código disponible bajo licencia libre? Benchmarks pueden ser No.	Sí / No / Parcial / N/A / Por verificar
Proyecto activo (Nivel 3)	Actividad a fecha de corte (releases/commits/updates).	Alta / Media / Baja / N/A / Por verificar
Funcionalidad Riesgos (Nivel 3)	Soporte al ciclo de riesgo SI.	Sí / Parcial / No / N/A
Docs técnica (Nivel 3)	Manual/guías/instalación/arquitectura oficiales.	Sí / Parcial / No / N/A
Uso reportado (Nivel 3)	Uso en organizaciones o estudios/casos.	Sí / Parcial / No / N/A
Decisión (Nivel 4)	Resultado del tamizado.	Pasa a AHP / Benchmark / Descartada
Motivo principal	1 frase técnica (máx. 20–25 palabras).	Ej.: 'Filtro Nivel 1: no GRC-SI'
Fuentes consultadas	Links a sitio oficial, repo, licencia, docs, release; marketplaces solo apoyo.	URL(s)

ANEXO D – Matriz de Preselección de Herramientas (Fase II)

Nota metodológica: Se aplicó desarte en cascada. Si una herramienta falla en Nivel 1 (Tipo/Enfoque) o Nivel 2 (OSS verificable, salvo Benchmark), los criterios de Nivel 3 se registran como 'N/A'. Fecha de corte sugerida: 2024-06-30.

ID	Herramienta	Tipo/Enfoque (Nivel 1)	Licencia / Modelo	OSS verificable (Nivel 2)	Proyecto activo	Funcionalidad Riesgos (Nivel 3)	Docs técnica	Uso reportado	Decisión (Nivel 4)	Motivo principal	Fuentes consultadas (links)
1	MONARC	GRC - Seguridad de la Información	AGPLv3 (OSS)	Sí	Alta	Sí	Sí	Sí	Pasa a AHP	Aprueba los filtros.	https://www.monarc.lu/ ; https://github.com/monarc-project/
2	ERAMBA	GRC - Seguridad de la Información	Community (source-available) / Enterprise	Parcial	Alta	Sí	Sí	Sí	Pasa a AHP	Cumple criterios mínimos con licencia/edición comunitaria (limitaciones conocidas).	https://www.eramba.org/ ; https://github.com/eramba ; https://www.eramba.org/community-edition ; https://www.eramba.org/documentation
3	SimpleRisk	GRC - Seguridad de la Información	Core OSS (MPL 2.0) + extras de pago	Parcial	Alta	Sí	Sí	Sí	Pasa a AHP	Cumple criterios mínimos con núcleo abierto; alta viabilidad PyME.	https://www.simplerisk.com/ ; https://github.com/simplerisk
4	PILAR (MAGERIT)	GRC - Seguridad de la Información	Propietaria (CCN-CERT) / Basic disponible	No	Alta	Sí	Sí	Sí	Benchmark	Benchmark: herramienta de referencia MAGERIT/ENS (no OSS).	https://www.pilar-tools.com/
5	Pirani Risk	GRC - Seguridad de la Información	Propietaria (SaaS) / plan Free	No	Alta	Sí	Sí	Sí	Benchmark	Benchmark: alta usabilidad y viabilidad operativa PyME sin infraestructura (no OSS).	https://www.piranirisk.com/
6	verinice	GRC - Seguridad de la Información	GPLv3 (OSS)	Sí	Alta	Sí	Sí	Sí	Descartada	Descartada por cronología/alcance del estudio (priorización de alternativas usadas en AHP).	https://verinice.com/ ; https://github.com/sernet/verinice
7	GLPI	ITSM / CMDB / Activos	GPL (OSS)	Sí	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: ITSM/CMDB (no gestiona ciclo GRC de riesgo SI).	https://glpi-project.org/ ; https://github.com/glpi-project/glpi
8	OpenVAS / Greenbone	Vulnerability Scanner	Mixto (OSS + comercial)	Parcial	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: escáner de vulnerabilidades (no GRC).	https://www.greenbone.net/ ; https://github.com/greenbone
9	6clicks	GRC - Seguridad de la Información	Propietaria (SaaS)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 2: no cumple licenciamiento OSS (sin excepción).	https://www.6clicks.io/
10	AuditBoard	GRC - Seguridad de la Información	Propietaria (Enterprise)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 2: no OSS; orientada a grandes organizaciones (costo/escala).	https://www.auditboard.com/
11	Wrike	Project Management	Propietaria (SaaS)	N/A	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: gestión de proyectos (no GRC).	https://www.wrike.com/
12	isms.online	GRC - Seguridad de la Información	Propietaria (SaaS)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 2: no OSS; referencia de mercado.	https://www.isms.online/
13	openGRC	GRC - Seguridad de la Información	Community/source (Creative Commons Attribution Non Commercial Share Alike 4.0 International)	Parcial	Media	Parcial	Sí	No	Descartada	Licencia restrictiva y madurez muy baja (versión alpha); sin casos de uso aplicados.	https://github.com/LeeMangold/OpenGRC ; https://docs.opengrc.com
14	CISO Assitant	GRC - Seguridad de la Información	AGPLv3 (OSS)	Sí	Alta	Parcial	Parcial	No	Descartada	Licencia OSS válida pero funcionalidad de riesgo limitada y documentación parcial.	https://github.com/intuitem/ciso-assistant-community ; https://www.wikidata.org/wiki/Q135450643
15	ArcherySec	Vulnerability Scanner	BSD/GPL (OSS)	Sí	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: gestión de vulnerabilidades AppSec (no GRC).	https://github.com/archerysec/archerysec
16	OpenRMF	GRC - Seguridad de la Información	MIT / comercial	Parcial	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 3: enfoque nicho (RMF/FedRAMP) o verificación incompleta para PyME general.	https://openrmf.io/ ; https://github.com/SoteriaSoftware
17	Ralph	ITSM / CMDB / Activos	Apache 2.0 (OSS)	Sí	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: ITAM/DCIM (no ciclo GRC de riesgo SI).	https://ralph.allegro.tech/ ; https://github.com/allegro/ralph
18	RiskLens	GRC - Riesgos Financieros	Propietaria (SaaS)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1/2: FAIR cuantitativo comercial fuera de alcance PyME típica.	https://www.risklens.com/
19	MSRA (Microsoft)	Security Assessment Tool	Propietaria (gratuita)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1/2: assessment (no GRC integral) y no OSS.	https://www.microsoft.com/
20	HSI Donesafe	GRC - Riesgos Laborales (SST)	Propietaria (SaaS)	N/A	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: SST/HSE (fuera de alcance).	https://www.donesafe.com/ (por verificar)
21	GlobalSuite	GRC - Seguridad de la Información	Propietaria (Enterprise)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 2: no OSS; plataforma comercial.	https://www.globalsuite.es/ (por verificar)
22	GPSecure	Por verificar	Por verificar	Por verificar	N/A	N/A	N/A	N/A	Descartada	No verificable con evidencia primaria a fecha de corte.	Por verificar
23	grcbit	GRC - Seguridad de la Información	Licencia propietaria gratuita (custom license, sin libertades OSS)	No	N/A	N/A	N/A	N/A	Descartada	Licencia restrictiva: no permite modificar ni crear derivados (no cumple definición OSS)	https://github.com/grcbit/grc ; https://github.com/OWASP/www-project-it-grc ; http://dev.grcbit.cloud:8000/demo
24	Optial SmartStart	GRC - Riesgos Operativos (ERM)	Propietaria (SaaS)	N/A	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: ERM (fuera de alcance).	https://www.optial.com/ (por verificar)
25	SecurityScorecard	GRC - Seguridad de la Información	Propietaria (SaaS)	No	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 2: no OSS; ratings/TPRM comercial.	https://securityscorecard.com/ (por verificar)
26	Project Risk Management Software	Project Management	N/A	N/A	N/A	N/A	N/A	N/A	Descartada	Filtro Nivel 1: categoría genérica (no herramienta específica evaluable).	N/A
27	Open Source Risk Engine	GRC - Riesgos Financieros	N/A	N/A	N/A	N/A	N/A	N/A	Descartada	Riesgos financieros	https://github.com/OpenSourceRisk/Engine ; https://www.opensourcerisk.org/
28	RA Risk Coverage	GRC - Riesgos Operativos (ERM)	N/A	N/A	N/A	N/A	N/A	N/A	Descartada	No verificable con evidencia primaria a fecha de corte.	https://github.com/amrFHamza/ra-risk-coverage
29	PTA Professional	Por verificar	Por verificar	Por verificar	N/A	N/A	N/A	N/A	Descartada	No verificable.	Por verificar

F. Anexo: Ficha técnica de análisis funcional de las herramientas

Este anexo consolida cinco fichas técnicas (una por herramienta) elaboradas a partir de la revisión de documentación oficial, repositorios públicos y material técnico disponible. Las fichas actúan como soporte verificable de la síntesis comparativa presentada en la Tabla 3.2.1-1 del Capítulo 3.

Nota metodológica: La información aquí registrada corresponde al análisis técnico-funcional (Etapa 2) solo de las herramientas finalistas derivadas de la matriz de preselección de herramientas (Etapa 1) y sirve de insumo para la evaluación multicriterio mediante AHP (Etapa 3). No se realizaron despliegues de prueba para todas las herramientas debido a restricciones de tiempo/recursos; por tanto, las evidencias se sustentan en fuentes primarias verificables (manuales, guías, arquitectura, requisitos y licenciamiento). La evaluación comparativa se basó en atributos funcionales declarados y documentados, consistentes con el enfoque sociotécnico y los criterios definidos para el modelo AHP.

Ficha 1. MONARC

1. Identificación y disponibilidad

Herramienta	MONARC
Tipo / enfoque	GRC – Gestión de riesgos de seguridad de la información (enfoque basado en activos; alineación ISO/IEC 27005).
URL oficial	https://www.monarc.lu
Repositorio / descarga	https://github.com/monarc-project (repositorio principal del proyecto MONARC)
Licencia / modelo	Open Source (GNU AGPL v3.0).

2. Requisitos técnicos y despliegue

Modelo de despliegue	Aplicación web on-premise (servidor).
Requisitos mínimos (síntesis)	Stack tipo LAMP o equivalente (servidor web + PHP + base de datos MySQL/MariaDB).
Dependencias relevantes	PHP (framework y extensiones), motor de base de datos (MySQL/MariaDB). Componentes auxiliares según instalación (p. ej., scripts de despliegue).
Notas de instalación	Instalación recomendada mediante procedimiento oficial (manual o automatizado). Se sugiere despliegue en VM para aislar dependencias y facilitar evidencia reproducible.

3. Cobertura funcional del ciclo de gestión del riesgo

Elemento del ciclo	Evidencia funcional (según documentación)
Contexto e inventario de activos	Modelado de activos en estructura jerárquica; permite asociar dependencias y herencia de impacto según el modelo.
Identificación de amenazas/vulnerabilidades	Uso de librerías/catálogos (importables/editables) para amenazas y medidas; asociación al modelo de activos.
Análisis y evaluación	Valoración cualitativa configurable (impacto/probabilidad), cálculo de niveles de riesgo según configuración del modelo.
Tratamiento	Gestión de medidas/controles y planificación de tratamiento según configuración; generación de plan o listado de acciones.
Monitoreo/seguimiento	Seguimiento del estado del análisis y de medidas; reportes/tableros según roles.

4. Módulos / componentes relevantes

- Modelado de activos y dependencias (árbol jerárquico).
- Bibliotecas (catálogos) y reutilización de conocimiento (p. ej., modelos sectoriales descargables).
- Módulo de análisis de riesgos y tableros de visualización.
- Soporte de exportación/impresión de resultados (según configuración).

5. Observaciones para contexto PyME

Destaca por la posibilidad de capitalizar modelos/catálogos reutilizables para no iniciar el análisis desde cero; requiere capacidades mínimas de administración de servidor para el despliegue on-premise.

6. Fuentes oficiales (URLs base)

- Sitio oficial del proyecto: https://www.monarc.lu
- Repositorio oficial: https://github.com/monarc-project

7. Evidencias consultadas (trazabilidad documental por campo)

- A) Licenciamiento / OpenSource verificable
- Repositorio oficial (archivo LICENSE / información de licencia del proyecto). Verificación de que el modelo es GNU AGPL v3.0 (consulta directa del repositorio).
- MONARC – Technical Guide (PDF): referencias al carácter OpenSource del proyecto y componentes (secciones introductorias / overview). (p. 1–2)
- B) Requisitos técnicos / arquitectura / dependencias
- MONARC – Technical Guide (PDF): requisitos de despliegue y componentes (stack tipo servidor web + base de datos; dependencias por componente/servicio). (p. 3–9)
- Download – MONARC (PDF): rutas de instalación/paquetes y componentes asociados (Ansible, guía de despliegue, plataforma de objetos). (p. 1–3)
- C) Soporte al ciclo de gestión del riesgo (alineación metodológica)
- MONARC – Method Guide (PDF): alineación explícita con ISO/IEC 27005 y descomposición por etapas del ciclo (identificación, análisis, evaluación, tratamiento, monitoreo/revisión). (menciones a ISO/IEC 27005 en p. 2, 4–5, 12, 23, 25; desarrollo del método en p. 2–5, 10–16, 18–24)
- User Guide – MONARC (PDF): evidencia operativa de funcionalidades relacionadas con activos, librerías/catálogos y gestión del análisis. (gestión de assets/libraries y objetos reutilizables: p. 44–50; análisis/gestión del riesgo en la herramienta: p. 59–60 y p. 133–138)
- D) Tratamiento del riesgo / plan / seguimiento
- User Guide – MONARC (PDF): funcionalidades asociadas a plan de tratamiento, acciones/medidas y seguimiento en el sistema. (p. 59, 62–64; y seguimiento/reportes vinculados al análisis: p. 133–138)
- MONARC – Method Guide (PDF): definición conceptual del tratamiento y su relación con las decisiones del método. (p. 18–24)
- E) Rasgo relevante para PyME (reutilización / aceleración del análisis)
- User Guide – MONARC (PDF): reutilización de modelos/catálogos y publicación/compartición de análisis (capitalización de conocimiento). (p. 45–47)
- Download – MONARC (PDF): referencia a Objects Sharing Platform (plataforma de objetos/modelos reutilizables). (p. 3)

Ficha 2. ERAMBA (Community Edition)

1. Identificación y disponibilidad

Herramienta	ERAMBA (Community Edition)
Tipo / enfoque	GRC – Cumplimiento, controles y auditoría (gestión de riesgos y controles con orientación a revisiones periódicas).
URL oficial	https://www.eramba.org
Repositorio / descarga	Descarga oficial Community Edition: https://www.eramba.org/get-community Página de producto (Community/Enterprise): https://www.eramba.org/eramba-software Repositorios asociados (proyecto): https://github.com/eramba
Licencia / modelo	Community Edition (código disponible bajo términos de la edición; condiciones específicas según proveedor).

2. Requisitos técnicos y despliegue

Modelo de despliegue	Aplicación web on-premise; despliegue frecuente mediante contenedores (Docker) o VM.
Requisitos mínimos (síntesis)	Servidor web + runtime (según stack del proveedor) + base de datos; recursos medios por módulos de cumplimiento/auditoría.
Dependencias relevantes	Contenedores (Docker/Compose) cuando se use método recomendado; base de datos y componentes del stack web.
Notas de instalación	La instalación y el despliegue se documentaron mediante fuentes oficiales consultadas (guías/cursos de la plataforma de aprendizaje y repositorios de soporte). No se realizaron pruebas de instalación en el marco del estudio; el análisis se sustentó en trazabilidad documental.

3. Cobertura funcional del ciclo de gestión del riesgo

Elemento del ciclo	Evidencia funcional (según documentación)
Contexto y activos	Inventarios/estructuras de activos y contexto de cumplimiento (según configuración).
Identificación	Registro de riesgos y/o issues; asociación a activos y controles.
Análisis y evaluación	Metodología configurable para evaluar riesgos; soporta revisiones periódicas.
Tratamiento	Gestión de controles, planes y evidencias; mapeo a marcos normativos.
Monitoreo/seguimiento	Workflows de auditoría/revisión y notificaciones; evidencias y reportes.

4. Módulos / componentes relevantes

- Gestión de riesgos (basada en activos y/o procesos, según configuración).
- Gestión de controles de seguridad y evidencias.
- Cumplimiento/auditoría (plantillas y mapeo a marcos).
- Revisiones periódicas y seguimiento por workflows.

5. Observaciones para contexto PyME

Útil cuando se requiere trazabilidad de cumplimiento y auditoría. Puede demandar mayor esfuerzo de parametrización y recursos de infraestructura que herramientas más ligeras.

6. Fuentes oficiales (URLs base)

- Sitio oficial: https://www.eramba.org
- Documentación (sección oficial): https://www.eramba.org/learning/

7. Evidencias consultadas (trazabilidad documental por campo)

- Licencia / modelo (Community vs Enterprise; precio fijo anual; "open/free version") → https://www.eramba.org/eramba-software → eramba Free GRC software.pdf.
- Modelo de despliegue (On-premise y SaaS; "Where it sits? Your Premises / Our Premises") → eramba Free GRC software.pdf, comparación de planes con modalidad On premises y SaaS.
- Descarga/obtención de la Community Edition (mecanismo oficial de acceso a la edición Community) → https://www.eramba.org/get-community
- Repositorio (artefactos y repositorios asociados al proyecto: docker/automation/templates, etc.) → https://github.com/eramba
- Base de conocimiento y guías (instalación/actualización, guías de implementación, módulos de soporte, "common features", quick guides) → https://www.eramba.org/learning
- Módulos/cobertura funcional (Compliance; Risk Mgmt & Reviews; Data Flows & GDPR; Controls & Audits; Policies; Incidents; Projects; BCP) → eramba Free GRC software.pdf, lista de "Core GRC Modules".
- Funcionalidades transversales (Filters, CSV Imports, Notifications, Dynamic Statuses, Custom Fields, REST APIs, WebHooks, Reports) → eramba Free GRC software.pdf, bloque "Common Module Features". Soporte de aprendizaje/documentación (free learning platform) → eramba Free GRC software.pdf, donde se menciona explícitamente la "Free learning platform" para los planes.
- Evidencia de instalación en entorno virtualizado (VMware install) → https://www.eramba.org/learning/courses/13/episodes/278

Ficha 3. SimpleRisk (Core / Open-core)

1. Identificación y disponibilidad

Herramienta	SimpleRisk (Core / Open-core)
Tipo / enfoque	GRC – Operación de riesgos y mitigación (enfoque orientado a registro, seguimiento y reportes operativos).
URL oficial	https://www.simplerisk.com
Repositorio / descarga	https://github.com/simplerisk (código del núcleo y recursos asociados)
Licencia / modelo	Open-core / freemium (núcleo abierto; extensiones o módulos avanzados bajo licenciamiento comercial, según edición).

2. Requisitos técnicos y despliegue

Modelo de despliegue	Aplicación web autoalojada (self-hosted) en entorno on-premise (servidor/VM). La documentación oficial contempla instalación en Linux y Windows Server, y también una opción de despliegue por appliance/VM.
Requisitos mínimos (síntesis)	Stack tipo LAMP o equivalente (servidor web + PHP + base de datos MySQL/MariaDB).
Dependencias relevantes	PHP, motor MySQL/MariaDB, servidor web (Apache/Nginx). Dependencias adicionales según módulos/edición.
Notas de instalación	La instalación y actualización están documentadas en la base de conocimiento oficial (guías por sistema operativo y método). No se realizaron pruebas de instalación en el marco del estudio; por tanto, este bloque se fundamenta en verificación documental (manuales/KB) y no en evidencias de ejecución (capturas de despliegue).

3. Cobertura funcional del ciclo de gestión del riesgo

Elemento del ciclo	Evidencia funcional (según documentación)
Contexto e inventario base	Estructuras para registrar activos/áreas/procesos (según configuración) y asociar riesgos a dichos elementos.
Identificación	Registro de riesgos y atributos; importación o carga según capacidades de la edición.
Análisis y evaluación	Matrices o fórmulas de valoración (impacto/probabilidad), parametrizables según la edición/configuración.
Tratamiento	Planificación y seguimiento de mitigaciones/acciones con responsables y fechas.
Monitoreo/seguimiento	Estados de riesgo, revisiones, reportes

4. Módulos / componentes relevantes

- Registro y mantenimiento de riesgos (risk register).
- Gestión de acciones/mitigaciones y seguimiento de estados.
- Reportes y exportaciones (según edición).
- Módulos complementarios (según licenciamiento) para integraciones o capacidades avanzadas.

5. Observaciones para contexto PyME

Adecuada para adopción progresiva por su orientación operativa y curva de aprendizaje moderada; el modelo open-core implica revisar alcance de funciones disponibles en el núcleo frente a extensiones.

6. Fuentes oficiales (URLs base)

- Sitio oficial: https://www.simplerisk.com
- Repositorio: https://github.com/simplerisk

7. Evidencias consultadas (trazabilidad documental por campo)

- Requisitos técnicos / despliegue (stack tipo LAMP; guías de instalación; opción VM/VirtualBox): La base de conocimiento lista guías específicas para instalación en Ubuntu 18.04 (Apache/MySQL/PHP), CentOS 7 (Apache/MySQL/PHP), Windows Server (WAMP) y VirtualBox Appliance, confirmando el enfoque de despliegue web on-premise y el stack requerido.
- Ciclo de riesgo – Tratamiento (planificación de mitigaciones; acceso a riesgos sin mitigación; vínculo con revisión): “Plan Mitigation” describe la pantalla para gestionar riesgos sin plan de mitigación, con acceso directo a planificar mitigaciones y a iniciar revisiones desde la misma vista.
- Ciclo de riesgo – Tratamiento (detalle de la mitigación; responsable, costo/esfuerzo, % mitigación, residual risk; documentación soporte; auditoría): “Mitigation Details” documenta que la mitigación define el quién/qué/cuándo y cómo el Residual Risk disminuye según el % de mitigación; además, registra campos y trazabilidad (incluye evidencia/documentos de soporte y audit trail).
- Gestión de controles (asociación de controles a mitigaciones; conexión GRC control–riesgo): La guía “How to Attach Controls to Mitigations…” explica el procedimiento para adjuntar controles (desde la sección de “governance”) a las mitigaciones, y cómo esos controles impactan el cálculo/mitigación del riesgo.
- Ciclo de riesgo – Monitoreo/seguimiento (revisiones; resultado; próximo paso; fecha próxima; audit trail): “Review Details” define la página de revisión del riesgo, incluyendo resultado (approve/reject), next step, próxima fecha de revisión y audit trail de acciones/cambios.
- Ciclo de riesgo – Monitoreo/seguimiento (identificación de pendientes; priorización por score; acceso directo): “Perform Reviews” describe la vista que lista riesgos sin revisión previa, permite filtrar/ordenar y acceder de forma directa a la revisión/mitigación (enfocado en priorización operativa).
- Gestión operativa por agrupación (proyectos; batch-close; soporte a planificación): “Plan Projects” documenta la función de agrupar riesgos, gestionar proyectos por

Ficha 4. PILAR (Basic / edición utilizada)

1. Identificación y disponibilidad

Herramienta	PILAR (Basic / edición utilizada)
Tipo / enfoque	Herramienta de análisis de riesgos asociada a MAGERIT (benchmark metodológico) y está orientada al análisis de riesgos en CIS (sistemas de información y comunicaciones).
URL oficial	https://www.pilar-tools.com
Repositorio / descarga	No aplica (software propietario; el código fuente no se distribuye públicamente). Descarga disponible para Windows/Linux (con firma) y Mac (instrucciones), según portal oficial.
Licencia / modelo	Propietaria (disponibilidad según edición; existen ediciones de uso gratuito/restringido según proveedor). Requiere licencia de uso. La herramienta permite licencia de evaluación (30 días), solicitud de evaluación, compra o solicitud institucional (sector público español) según condiciones del proveedor.

2. Requisitos técnicos y despliegue

Modelo de despliegue	Aplicación de escritorio (entorno Java, según edición).
Requisitos mínimos (síntesis)	Sistema operativo compatible + runtime Java (según requisitos del proveedor). Almacenamiento local para proyectos.
Dependencias relevantes	Java Runtime Environment (según versión recomendada).
Notas de instalación	El proveedor indica que además de la descarga se requiere licencia de uso. Se documentan opciones de licencia de evaluación (30 días) y limitaciones funcionales del modo evaluación. No se realizaron pruebas de instalación en el estudio; el análisis se sustentó en trazabilidad documental.

3. Cobertura funcional del ciclo de gestión del riesgo

Elemento del ciclo	Evidencia funcional (según documentación)
Contexto y activos	Modelado de activos y dependencias con valoración de impacto en dimensiones (según MAGERIT).
Identificación	Uso de catálogos/bibliotecas de amenazas y salvaguardas asociadas a MAGERIT.
Análisis y evaluación	Cálculo de impacto y riesgo (cuantitativo/cualitativo) con dependencias y agregación (según configuración).
Tratamiento	Planificación de salvaguardas/controles y análisis de reducción de riesgo (según módulos disponibles).
Monitoreo/seguimiento	Soporte a mantenimiento del análisis y

4. Módulos / componentes relevantes

- Modelado y valoración de activos (enfoque MAGERIT).
- Bibliotecas de amenazas y salvaguardas (controles).
- Cálculo de riesgo con dependencias y análisis de impacto.
- Generación de informes/exportaciones (según edición).

5. Observaciones para contexto PyME

Aporta rigor formal como referencia metodológica (benchmark), aunque su naturaleza propietaria y curva de aprendizaje pueden incrementar la carga operativa en entornos PyME.

6. Fuentes oficiales (URLs base)

- Sitio oficial del producto: https://www.pilar-tools.com
- Referencias institucionales sobre MAGERIT/ENS (según bibliografía del trabajo).

7. Evidencias consultadas (trazabilidad documental por campo)

- Disponibilidad / Descarga (multiplataforma; versiones; firmas) → Página de descarga PILAR Basic 2025.1.4 (31.10.2025), sección "Descarga" (Windows/Linux con "firma"; Mac con "instrucciones"; variantes ES/ENS, EN, IT). Respalda: disponibilidad de binarios por SO, control de integridad (firmas) y versiones/fecha.
- Licencia/modelo (no OSS): Portal de descarga, nota "se requiere licencia de uso".
- Opciones de licencia: Portal de descarga, bloque "Licencia de uso – Opciones" (evaluación 30 días / solicitar / adquirir / canal institucional).
- Limitaciones de la evaluación → Página de descarga, bloque "Licencias de evaluación - limitaciones" (sin informes, sin exportación CSV/XML, límites de activos/riesgos/salvaguardas). Respalda: restricciones operativas que afectan evidencia por instalación, reportes y exportaciones.
- Descarga/edición/fecha: Portal de descarga PILAR Basic 2025.1.4 (31.10.2025), sección "Descarga" (binarios por SO y firmas).

Ficha 5. Pirani Risk (SaaS / plan utilizado)

1. Identificación y disponibilidad

Herramienta	Pirani Risk
Tipo / enfoque	Plataforma SaaS para gestión de riesgos “no financieros” con sistemas (módulos) como ISMS (seguridad de la información), Compliance, etc.; usada como benchmark funcional por usabilidad y rapidez de adopción.
URL oficial	https://www.piranirisk.com/
Repositorio / descarga	No aplica (administrado por el proveedor).
Licencia / modelo	Propietaria (SaaS). Existe Plan Free (indefinido) y planes de pago. El Plan Free contempla límites de uso (usuarios/registros/almacenamiento).

2. Requisitos técnicos y despliegue

Modelo de despliegue	SaaS (nube), acceso vía navegador web.
Requisitos mínimos (síntesis)	Navegador web + conectividad; no requiere instalación local. (Derivado del esquema de alta/uso del software vía cuenta y dashboard.)
Dependencias relevantes	No aplica (administrado por el proveedor).
Notas de instalación	No se realizaron pruebas de instalación ni capturas propias en el marco del estudio; el análisis se sustentó en trazabilidad documental (guías/ebooks del proveedor). Se agendó una demo.

3. Cobertura funcional del ciclo de gestión del riesgo

Elemento del ciclo	Evidencia funcional (según documentación)
Contexto y catálogo base	Creación de organización, estructura de procesos y “factores/fuentes” según sistema (p. ej., ISMS), con posibilidad de asociar activos cuando se trata de ISMS.
Identificación	Identificación/registro de riesgos; soporte guiado y sugerencias (integración con IA) según material del proveedor.
Análisis y evaluación	Priorización/visualización mediante mapas de calor y análisis de perfil de riesgo inherente/residual.
Tratamiento	Definición y parametrización de controles y evaluación de efectividad; planes de acción asociados.
Monitoreo/seguimiento	Monitoreo continuo, reporte de eventos y uso de dashboard/heatmap para seguimiento de riesgos.

4. Módulos / componentes relevantes

- Sistemas/módulos: ORM, AML, ISMS, Compliance, Auditoría (según material comercial).
- Funciones transversales reportadas: gestión de controles, reportes (mapa de calor), importación desde Excel, asignación de responsables, etc.

5. Observaciones para contexto PyME

Fortaleza: adopción rápida sin infraestructura propia; adecuada como benchmark de usabilidad.
Limitación: dependencia del modelo SaaS y restricciones del Plan Free (usuarios/registros/almacenamiento y selección de un sistema de gestión).

6. Fuentes oficiales (URLs base)

- Sitio oficial del proveedor: https://www.piranirisk.com
- Secciones de planes/funcionalidades según plan consultado (según bibliografía y evidencias del trabajo).

7. Evidencias consultadas (trazabilidad documental por campo)

- Tipo/enfoque (módulos disponibles, incluido ISMS): Documento donde se listan los sistemas de gestión (ORM/AML/ISMS/Compliance/Auditoría) y se enfatiza la interfaz intuitiva/fácil de usar.
- Licencia/modelo (Plan Free + límites): Descripción del Plan Free (indefinido), y límites de hasta 5 usuarios, 200 registros y 2GB.
- Modelo de despliegue SaaS (sin instalación local): Guía que evidencia el uso mediante creación de cuenta, verificación por correo y acceso al “software”/dashboard (indicador práctico de modelo SaaS).
- Contexto (procesos, roles/grupos, control de acceso): Guía donde se describe la creación de roles y grupos de responsables para controlar acceso a información por áreas.
- ISMS (activos de información y criterios tipo C-I-D): Guía donde, para ISMS, se describen datos del activo y calificación basada en confidencialidad, integridad y disponibilidad.
- Tratamiento (controles) y monitoreo (heatmap/dashboard): Documento que describe controles/mitigación y el monitoreo con mapa de calor (ubicación inherente y residual).
- Evidencias adjuntas y exportación: Guía que menciona adjuntar evidencias y exportar información, además de descargar reporte básico del mapa de calor.

G. Anexo: Modelo AHP para la Selección de herramienta de gestión de riesgos

Matriz de comparación pareada									
	Gestión Organizacional	Análisis Técnico	Gestión de Riesgos	Viabilidad técnica y Operativa	Matriz normalizada				Vector Promedio
Gestión Organizacional	1.00	7.00	0.33	0.33	0.14	0.35	0.17	0.09	0.19
Análisis Técnico	0.14	1.00	0.14	0.20	0.02	0.05	0.07	0.06	0.05
Gestión de Riesgos	3.00	7.00	1.00	2.00	0.42	0.35	0.51	0.57	0.46
Viabilidad técnica y Operativa	3.00	5.00	0.50	1.00	0.42	0.25	0.25	0.28	0.30
Totales	7.14	20.00	1.98	3.53					

Ponderación de criterios vs. elementos											
	Gestión Organizacional					Matriz normalizada					Vector promedio
	PILAR	PIRANI RISK	SIMPLERISK	ERAMBA	MONARC						
PILAR	1.00	0.33	0.33	0.20	0.20	0.06	0.02	0.03	0.10	0.04	0.05
PIRANI RISK	3.00	1.00	0.33	0.20	0.20	0.18	0.07	0.03	0.10	0.04	0.09
SIMPLERISK	3.00	3.00	1.00	0.20	0.33	0.18	0.21	0.10	0.10	0.07	0.13
ERAMBA	5.00	5.00	5.00	1.00	3.00	0.29	0.35	0.52	0.52	0.63	0.46
MONARC	5.00	5.00	3.00	0.33	1.00	0.29	0.35	0.31	0.17	0.21	0.27
Totales	17.00	14.33	9.67	1.93	4.73						

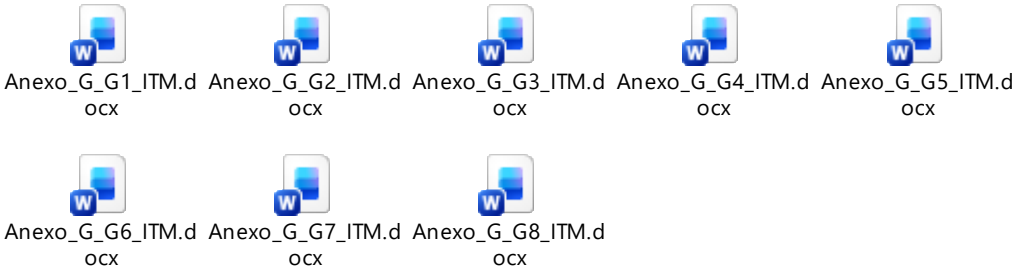
Ponderación de criterios vs. elementos											
	Análisis Técnico					Matriz normalizada					Vector promedio
	PILAR	PIRANI RISK	SIMPLERISK	ERAMBA	MONARC						
PILAR	1.00	5.00	0.33	5.00	3.00	0.21	0.26	0.17	0.26	0.41	0.26
PIRANI RISK	0.20	1.00	0.14	1.00	0.20	0.04	0.05	0.07	0.05	0.03	0.05
SIMPLERISK	3.00	7.00	1.00	7.00	3.00	0.63	0.37	0.51	0.37	0.41	0.46
ERAMBA	0.20	1.00	0.14	1.00	0.20	0.04	0.05	0.07	0.05	0.03	0.05
MONARC	0.33	5.00	0.33	5.00	1.00	0.07	0.26	0.17	0.26	0.14	0.18
Totales	4.73	19.00	1.95	19.00	7.40						

Ponderación de criterios vs. elementos											
	Gestión de Riesgos					Matriz normalizada					Vector promedio
	PILAR	PIRANI RISK	SIMPLERISK	ERAMBA	MONARC						
PILAR	1.00	0.33	0.14	0.14	0.20	0.04	0.03	0.03	0.03	0.09	0.04
PIRANI RISK	3.00	1.00	0.33	0.33	0.25	0.13	0.09	0.06	0.06	0.12	0.09
SIMPLERISK	7.00	3.00	1.00	1.00	0.33	0.30	0.26	0.18	0.18	0.16	0.22
ERAMBA	7.00	3.00	1.00	1.00	0.33	0.30	0.26	0.18	0.18	0.16	0.22
MONARC	5.00	4.00	3.00	3.00	1.00	0.22	0.35	0.55	0.55	0.47	0.43
Totales	23.00	11.33	5.48	5.48	2.12						

Ponderación de criterios vs. elementos											
	Viabilidad técnica y Operativa					Matriz normalizada					Vector promedio
	PILAR	PIRANI RISK	SIMPLERISK	ERAMBA	MONARC						
PILAR	1.00	0.11	0.14	0.20	0.20	0.04	0.07	0.02	0.02	0.02	0.03
PIRANI RISK	9.00	1.00	5.00	7.00	7.00	0.33	0.63	0.73	0.57	0.57	0.57
SIMPLERISK	7.00	0.20	1.00	3.00	3.00	0.26	0.13	0.15	0.25	0.25	0.20
ERAMBA	5.00	0.14	0.33	1.00	1.00	0.19	0.09	0.05	0.08	0.08	0.10
MONARC	5.00	0.14	0.33	1.00	1.00	0.19	0.09	0.05	0.08	0.08	0.10
Totales	27.00	1.60	6.81	12.20	12.20						

MATRIZ JERÁRQUICA						
	Gestión Organizacional	Análisis Técnico	Gestión de Riesgos	Viabilidad técnica y Operativa	**Total**	Orden de ponderación
PILAR	0.05	0.26	0.04	0.03	5.28%	5
PIRANI RISK	0.09	0.05	0.09	0.57	23.21%	2
SIMPLERISK	0.13	0.46	0.22	0.20	21.00%	4
ERAMBA	0.46	0.05	0.22	0.10	21.94%	3
MONARC	0.27	0.18	0.43	0.10	28.57%	1
Ponderación	0.19	0.05	0.46	0.30		

H. Anexo: Soporte técnico-metodológico de instrumentación



Se presenta una versión condensada del soporte técnico-metodológico para la instrumentación de MONARC en la Fase III (OE3).

G.1.2 Parámetros mínimos de despliegue y configuración base

Tabla G.1.2-1. Parámetros mínimos de despliegue y configuración base del entorno (VM VirtualBox + MONARC).

Parámetro	Valor adoptado	Propósito metodológico	Riesgo si se omite	Regla mínima de control
Plataforma de virtualización	Oracle VM VirtualBox (host de escritorio)	Proveer un entorno aislado, controlado y reproducible para la ejecución de MONARC, independiente del sistema operativo anfitrión.	Dependencia del entorno del host, imposibilidad de replicar el análisis en condiciones técnicas equivalentes.	Uso exclusivo de VirtualBox durante la Fase III, sin cambios de hipervisor.
Modo de despliegue	Máquina Virtual preconfigurada (imagen OVA)	Reducir la complejidad técnica del despliegue y garantizar homogeneidad en la instalación del stack de MONARC.	Errores de configuración manual en servicios, versiones inconsistentes del entorno base.	Importación directa de la imagen OVA sin modificación de componentes internos.
Versión de MONARC	MONARC v2.13.x (p3, commit 6d10eba)	Asegurar compatibilidad con las funciones de modelado, evaluación automática del riesgo y gestión del tratamiento.	Incompatibilidad funcional, variaciones en la lógica de cálculo o en la estructura de datos.	Congelación de versión durante toda la ejecución de OE3.
Sistema operativo invitado	Linux (incluido en la imagen VM oficial)	Soportar la ejecución estable de los servicios web, base de datos y componentes de MONARC.	Fallos de servicio, inestabilidad del entorno o pérdida de compatibilidad.	No alterar la distribución ni la configuración base del sistema operativo invitado.
Asignación de CPU	≥ 2 vCPU	Garantizar capacidad mínima para la ejecución fluida de la interfaz web y procesos internos.	Lentitud en la navegación y posibles bloqueos durante cálculos de riesgo.	Mantener la asignación mínima definida durante toda la fase.
Asignación de memoria RAM	≥ 4 GB	Permitir la operación simultánea de servicios web, base de datos y dashboard sin degradación funcional.	Interrupciones del servicio o cierres inesperados de la aplicación.	No reducir la memoria asignada una vez iniciado el análisis.
Almacenamiento virtual	Disco virtual persistente (≥ 40 GB)	Asegurar almacenamiento suficiente para análisis, catálogos, reportes y registros históricos.	Pérdida de información o imposibilidad de guardar avances del análisis.	Uso exclusivo de disco persistente; no ejecutar en modo "live" o temporal.
Configuración de red	NAT o Adaptador Puente (según escenario local)	Permitir acceso controlado al Front Office desde navegador web del host.	Inaccesibilidad a la interfaz de MONARC o conflictos de conectividad.	Definir y mantener un único modo de red durante toda la Fase III.
Acceso a la aplicación	URL local (IP/host de la VM) vía navegador web	Facilitar el acceso operativo al Front Office sin dependencias externas.	Interrupción del flujo metodológico por falta de acceso a la herramienta.	Verificación de acceso previo a cualquier parametrización o análisis.
Mecanismo de autenticación	Credenciales locales (usuario/contraseña)	Controlar el acceso a la instancia y la integridad del análisis.	Acceso no autorizado o alteración de la información registrada.	Cambio de credenciales por defecto antes de iniciar la instrumentación.
Idioma del análisis	Definido al crear el análisis y bloqueado	Garantizar coherencia lingüística en activos, catálogos y reportes generados.	Imposibilidad de reutilizar bibliotecas o inconsistencias semánticas en los datos.	No modificar el idioma tras la creación del análisis base.
Modelo de análisis inicial	Blank Model o Cases Model	Establecer la estructura base para el inventario de activos y riesgos.	Arrastre de configuraciones no controladas o incompatibles con la	Seleccionar el modelo antes de configurar escalas y catálogos.

Tabla G.1.6-1. Checklist metodológico de verificación del entorno (condición "listo para instrumentar").

Ítem de verificación	Criterio de aceptación	Método de verificación (cómo se comprueba, sin captura)	Responsable (rol)	Evidencia esperada en H.1
Acceso a Front Office	Autenticación exitosa y navegación operativa en la interfaz de análisis.	Inicio de sesión con credenciales válidas y carga completa de la interfaz.	Analista de riesgos	Registro de acceso y metadatos de sesión.
Acceso a Back Office	Disponibilidad del módulo de administración para gestión técnica.	Autenticación con rol autorizado y acceso al panel administrativo.	Administrador de sistemas	Registro de acceso administrativo.
Servicios de la aplicación activos	Servicios web y base de datos operativos.	Verificación de respuesta de la URL de la instancia y estabilidad de sesión.	Administrador de sistemas	Registro de estado de servicios.
Coherencia de versión de MONARC	MONARC v2.13.x con commit 6d10eba.	Revisión de la información de versión desde la interfaz o configuración del sistema.	Administrador de sistemas	Declaración técnica de versión.
Configuración de virtualización	VM ejecutándose en Oracle VM VirtualBox con recursos asignados según parámetros mínimos.	Revisión de la configuración de la VM en el gestor de VirtualBox.	Administrador de sistemas	Tabla de parámetros de la VM.
Configuración de red definida	Conectividad estable entre anfitrión y VM	Comprobación de resolución de la URL	Administrador de red	Registro de configuración de red.

	mediante el modo de red adoptado.	interna y estabilidad de conexión.		
Persistencia de datos	Capacidad de guardar y recuperar cambios del análisis.	Ejecución de operación de guardado y recarga de sesión.	Analista de riesgos	Registro de persistencia del análisis.
Idioma del análisis	Idioma definido antes de la creación del análisis y bloqueado posteriormente.	Verificación del campo de idioma en la creación del análisis.	Analista de riesgos	Metadatos del análisis base.
Disponibilidad de modelo base	Modelos "Blank" o "Cases" disponibles para inicialización.	Acceso al asistente de creación de análisis y selección de modelo.	Analista de riesgos	Registro de inicialización del análisis.
Snapshot base creado	Existencia de un punto de restauración previo a la instrumentación.	Revisión del historial de instantáneas de la VM en VirtualBox.	Administrador de sistemas	Registro del snapshot base.
Seguridad de acceso	Credenciales de prueba activas y control de sesión habilitado.	Ejecución del ciclo completo de autenticación y cierre de sesión.	Analista de riesgos	Registro de configuración de cuenta.
Integración MOSP (si aplica)	Conectividad configurada para descarga de objetos de seguridad.	Validación de credenciales de integración y prueba de conexión.	Analista de riesgos	Registro de configuración MOSP.

Con el fin de declarar el análisis "listo para instrumentar" antes de avanzar a la configuración de criterios de evaluación (G.3), se aplicó un checklist metodológico de consistencia como criterio de aceptación del análisis base. Este checklist verifica condiciones mínimas de coherencia y completitud (p. ej., idioma fijado, alcance definido, nomenclatura aplicada, metadatos mínimos

registrados y mapeo inicial de contexto establecido), de modo que la unidad de trabajo quede estable y preparada para el diligenciamiento y configuración posterior sin reprocesos.

Tabla G.2.5-1. Checklist metodológico de consistencia del análisis base (criterio de aceptación)

Ítem de verificación	Condición de cumplimiento	Evidencia esperada (tipo, no contenido)	Momento de verificación (Etapa 1 / previo a Etapa 2)	Observaciones
Fijación del idioma del análisis	Idioma seleccionado y bloqueado en la creación del análisis, independiente del idioma de la interfaz.	Metadato de configuración del análisis.	Etapa 1	Parámetro crítico para la compatibilidad de activos y catálogos.
Definición del alcance técnico	Síntesis del contexto registrada en el subpaso 1.1 del establecimiento del contexto.	Campo narrativo persistente vinculado al análisis.	Etapa 1	Delimita el análisis como unidad de instrumentación.
Aplicación de nomenclatura	Identificador único y representativo consignado en el campo "Name".	Identificador visible en la cabecera del análisis.	Etapa 1	Facilita la identificabilidad y búsqueda del artefacto.
Registro de metadatos mínimos	Nombre, descripción e idioma diligenciados conforme a las reglas definidas.	Formulario de metadatos del Front Office.	Etapa 1	Base para la trazabilidad institucional y documental.
Consistencia terminológica mínima	Coherencia lingüística entre el modelo base seleccionado (Blank/Cases) y el idioma del análisis.	Registro de creación del análisis.	Previo a Etapa 2	Evita incompatibilidades en la carga de activos.
Delimitación como unidad operativa	Activación de la barra de progreso con validación de los subpasos 1.1 a 1.3 mediante *tick boxes*.	Estado de validación de pasos en el Front Office.	Previo a Etapa 2	Condición necesaria para habilitar la configuración de criterios de evaluación en G.3.

G.8.1 Restricciones que afectan instrumentación (R#)

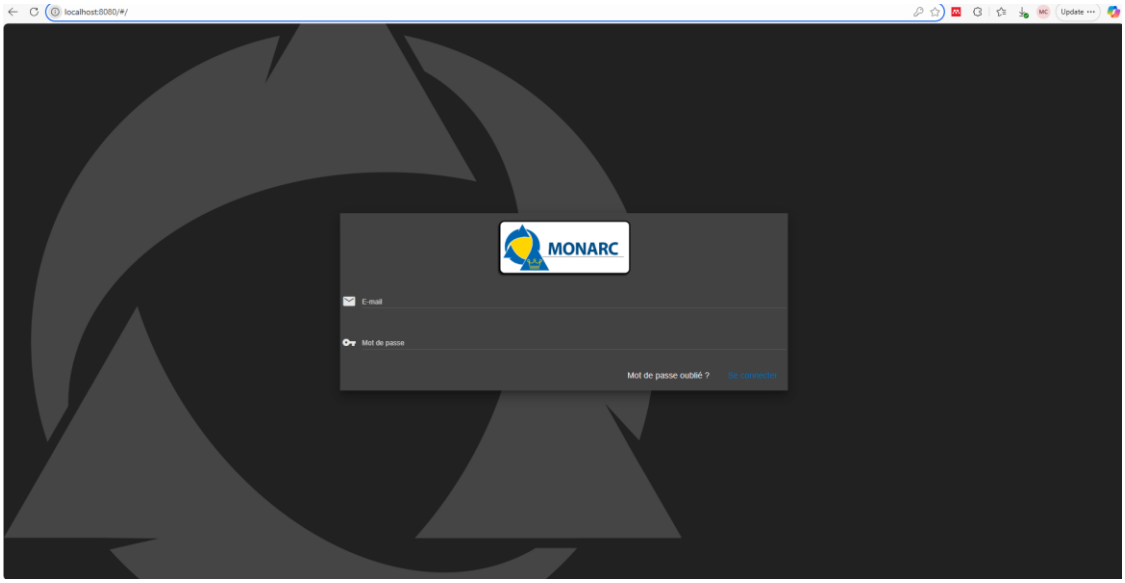
Se identificaron restricciones asociadas a decisiones de diseño de la herramienta y del entorno de despliegue que afectan la instrumentación del ciclo de gestión de riesgos. Para cada restricción se definieron: (i) el componente del flujo afectado, (ii) el instrumento compensatorio aplicable y (iii) el mecanismo de registro de trazabilidad.

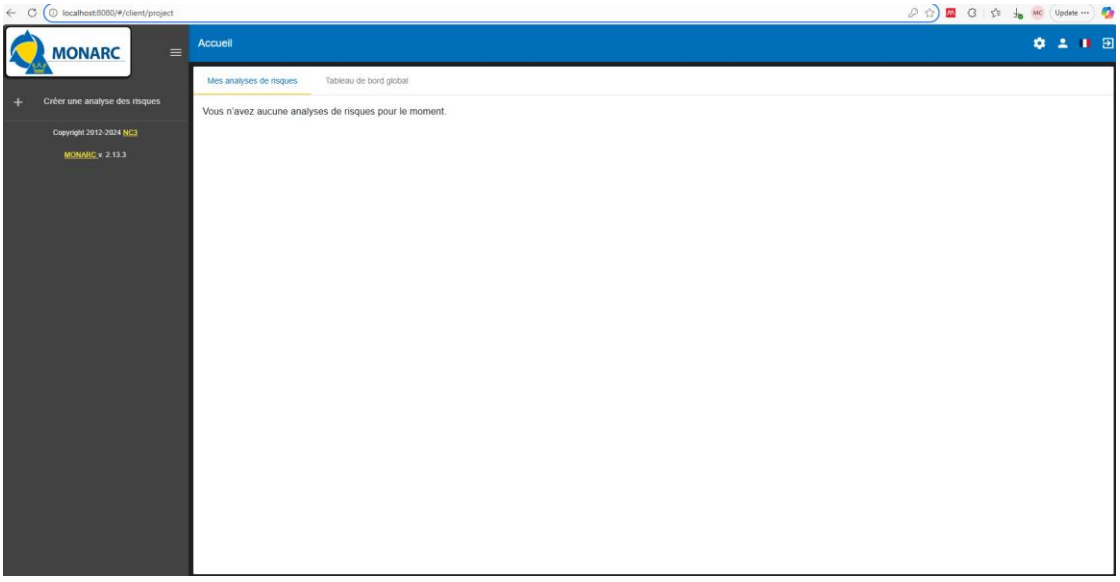
Tabla G.8.1-1. Restricciones operativas (R#) y compensaciones metodológicas

R#	Restricción operativa	Impacto sobre la instrumentación (etapa/artefacto afectado)	Instrumento compensatorio	Registro de trazabilidad (dónde se deja constancia)	Observaciones
R1	Idioma del análisis no editable una vez creado.	Etapa 1 (creación del análisis) y consistencia terminológica en catálogos/reportes.	Regla previa de creación del análisis (G.2.2) y checklist de consistencia (G.2.5).	Metadatos del análisis (nombre, idioma) y registro de creación del análisis.	Si se requiere cambio de idioma, se creó un nuevo análisis y se migró la configuración aplicable.
R2	Cambios en escalas sin versionado histórico dentro de MONARC.	Etapa 2 (escalas/umbrales): un ajuste afecta retroactivamente la valoración.	Regla de congelamiento/versionado de criterios (G.3.6).	Tabla externa de versionado de criterios y anotación de versión en metadatos del análisis.	Se evitó modificar escalas tras iniciar el modelado y la evaluación.
R3	Herencia de impactos con flexibilidad limitada para excepciones granulares.	Etapa 3 (activos/dependencias): posible sobre/infra-valoración en activos secundarios específicos.	Regla de modelado de dependencias y criterio de justificación metodológica (G.4.3–G.4.4).	Notas de modelado (observaciones del activo) y criterios de consistencia C–I–D.	Cuando fue necesario, se separaron activos o se ajustó la relación de dependencia para

					preservar coherencia.
R4	El riesgo no se calcula si falta un parámetro obligatorio (p. ej., probabilidad, qualification o impacto heredado).	Etapas 2–4: bloquea evaluación, tratamiento o reportes.	Criterios de control por etapa (G.6.3) y checklist end-to-end (G.6.7).	Registro de verificación por etapa y checklist de cierre.	Se verificó completitud mínima antes de avanzar a la siguiente etapa.
R5	El tratamiento tipo *Reduce* exige recomendación vinculada y vulnerabilidad residual definida.	Etapa 4 (tratamiento): no permite cierre del riesgo reducido sin residual.	Catálogo mínimo de recomendaciones/controles (G.5.3) y regla de tratamiento (G.6.5).	Campos de tratamiento (tipo), recomendación asociada y residual en el riesgo.	Si no fue posible definir residual bajo *Reduce*, se aplicó el tipo de tratamiento correspondiente según la decisión metodológica.
R6	El valor residual se actualiza cuando se implementan todas las recomendaciones asociadas (lógica global).	Etapa 4 (seguimiento): avance parcial no refleja reducción numérica inmediata.	Regla de seguimiento (G.6.6) y matriz externa de avance (%).	Historial de implementación en MONARC y registro complementario de avance.	Se mantuvo trazabilidad del estado por recomendación para evitar interpretaciones erróneas del progreso.
R7	Gestión limitada de costos, plazos y dependencias complejas entre medidas.	Priorización y planeación fuera del motor de riesgo de MONARC.	Matriz externa de priorización/planeación (costo–esfuerzo–impacto).	Archivo complementario de priorización y referencia cruzada con el plan de tratamiento.	La priorización se documentó como complemento metodológico sin alterar el registro de riesgos en MONARC.

I. Anexo: Evidencias técnicas y artefactos reproducibles de instrumentación

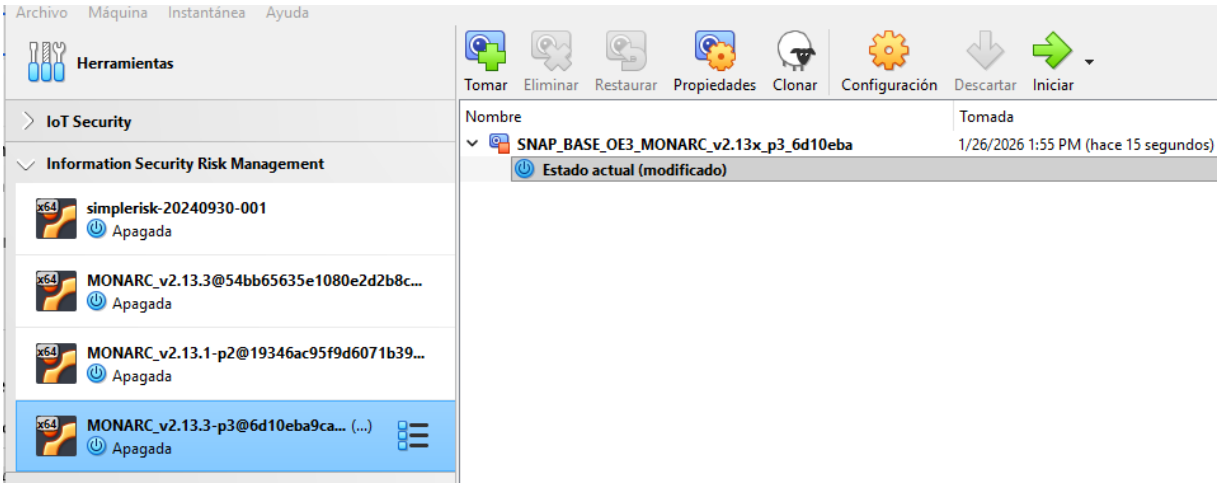

localhost:8080/#/
MONARC
E-mail
Mot de passe
Mot de passe oublié ?
Se connecter


localhost:8080/#/client/project
MONARC
Accueil
Mes analyses de risques
Tableau de bord global
Vous n'avez aucune analyses de risques pour le moment.
Créer une analyse des risques
Copyright 2012-2024 NC3
MONARC v. 2.13.3

H.1.1 Tabla completa de parámetros del entorno (VM y configuración base)

Tabla H.1.1-1. Parámetros técnicos del entorno reproducible

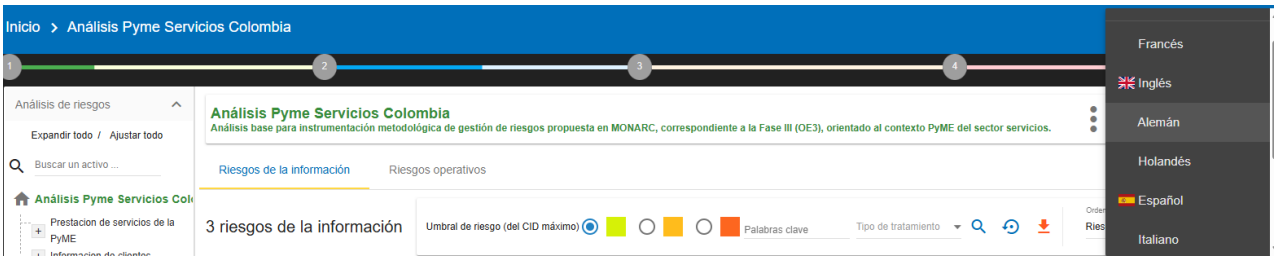
Campo	Valor
Sistema de virtualización	VirtualBox
Tipo de despliegue	VM
Host (SO y versión)	Windows 11 Home Single Language, versión 25H2 (OS Build 26200.7462)
CPU asignada (núcleos)	4
RAM asignada (GB)	4 GB (4096 MB)
Disco asignado (GB)	97.66 GB
Tipo de disco	VDI
Adaptador(es) de red (modo)	Adaptador 1 – NAT (Intel PRO/1000 MT Desktop (NAT))
IP de la VM	10.0.2.15
Puertos expuestos/forwarding (si aplica)	8080→80 (Front Office), 5000→5000 (API), 2222→22 (SSH)
URL de acceso (Front Office)	http://localhost:8080
Usuario de acceso	admin@admin.localhost / admin
Fecha/hora de despliegue	2025-08-13 20:07
MONARC versión	v2.13.x (p3, commit 6d10eba)
Fecha última modificación (según imagen)	2025-07-03 17:24
Componentes (stack) (si se registra)	Apache2, MySQL, PHP (LAMP stack); servicios activos vía systemctl
Observaciones técnicas	SO invitado: Ubuntu 22.04.2 (64-bit); Controlador gráfico: VMSVGA; Memoria de video: 64 MB; Paravirtualización: KVM; Audio y USB: deshabilitados; Carpetas compartidas: Ninguna



H.2.1 Registro de metadatos del análisis

Tabla H.2.1-1. Metadatos del análisis (unidad de instrumentación)

Campo	Valor
Nombre del análisis	OE3_MONARC_Analisis_Base_PyME_Servicios
Alcance (texto breve)	Instrumentación metodológica OE3 en MONARC para contexto PyME del sector servicios (análisis base; sin resultados).
Idioma configurado	Inglés (EN) [idioma del análisis]
Descripción	Análisis base para instrumentación metodológica de gestión de riesgos propuesta en MONARC, correspondiente a la Fase III (OE3), orientado al contexto PyME del sector servicios.
Fecha/hora de creación	26-01-2026 23:21
Identificador interno (si aparece)	N/A (no visible en interfaz)
Usuario/rol que creó	Admin
Versión MONARC	V 2.13.3
Observaciones	Front Office en español; idioma del análisis definido por opciones disponibles en el formulario (FR/EN/DE/NL)



H.3.1 Tabla completa de escalas (impacto C–I–D, probabilidad, vulnerabilidad)

Tabla H.3.1-1. Escala de impacto (C-I-D)

Nivel	Confidencialidad (descripción)	Integridad (descripción)	Disponibilidad (descripción)
0 - Sin Impacto	**Información pública o sin clasificación.** Datos ya disponibles en sitio web corporativo o catálogos públicos. No hay daño si se difunden. *Ejemplo*: Horarios de atención, contacto comercial.	**Datos irrelevantes o cambios estéticos.** Modificaciones que no afectan decisiones, cálculos ni registros oficiales. *Ejemplo*: Color de interfaz, texto descriptivo no crítico.	**Interrupción imperceptible.** Indisponibilidad < 1 minuto sin impacto percibido por usuarios internos ni clientes. *Ejemplo*: Reinicio de cache, actualización instantánea.
1 - Bajo	**Divulgación interna indebida; sin daño legal.** Información compartida con personal no autorizado dentro de la empresa; genera incomodidad menor pero sin consecuencias regulatorias. *Ejemplo*: Extensiones telefónicas internas, borradores de memo.	**Error menor en datos no críticos; corregible por el usuario.** Inconsistencia que el propio usuario puede rectificar sin asistencia técnica. *Ejemplo*: Typo en campo de texto libre, fecha mal ingresada en nota interna.	**Interrupción breve; reanudación inmediata.** Servicio no crítico caído brevemente; se restaura sin costos adicionales ni escalamiento. *Ejemplo*: Caída de chat interno por 15 min, impresora compartida offline.
2 - Medio	**Fuga limitada externa; posible queja de cliente.** Información sensible conocida por terceros no autorizados (ej. competidor, proveedor); genera malestar o queja pero sin multas regulatorias inminentes. *Ejemplo*: Lista de precios filtrada, organigramas de proyectos compartidos por error.	**Datos operativos erróneos; requiere soporte interno.** Corrupción que afecta reportes o flujos de trabajo; necesita intervención del área de sistemas o administrador para corregir. *Ejemplo*: Registros de inventario desactualizados, duplicados en base de datos CRM.	**Servicio degradado; recuperación en horas laborales.** Funcionalidad reducida o lentitud que obliga a procesos manuales temporales; se resuelve en el mismo día hábil. *Ejemplo*: Sistema de facturación lento (backup manual activado), correo corporativo caído hasta tarde.
3 - Alto	**Datos sensibles; violación de leyes de privacidad.** Exposición de información	**Corrupción de datos críticos; impacto en facturación.**	**Parada de servicio crítico > 24h; pérdida directa.** Inoperatividad de sistema

	personal de empleados o clientes que activa Ley 1581/2012 (Habeas Data) o genera daño reputacional significativo y posibles sanciones. *Ejemplo*: Base de datos de clientes con identificaciones y contactos filtrada públicamente, nómina con salarios expuesta.	Alteración de registros contables, transaccionales o de compliance que afecta decisiones financieras o compromisos contractuales. *Ejemplo*: Facturas emitidas con valores erróneos, registros de auditoría manipulados.	esencial que detiene operación principal, generando pérdida de clientes, incumplimiento de SLA o ingresos no percibidos. *Ejemplo*: Plataforma de servicios (software as a service) caída por 2 días, call center sin acceso a sistema de tickets.
4 - Crítico	**Fuga masiva estratégica; amenaza de cierre.** Divulgación de secretos comerciales, estrategias, contratos clave o información estratégica que compromete la viabilidad del negocio y puede derivar en demandas judiciales graves o pérdida de licencias. *Ejemplo*: Propiedad intelectual del modelo de negocio publicada, acuerdos de confidencialidad con grandes clientes violados irreversiblemente.	**Pérdida total de bases de datos; fraude mayor.** Destrucción o corrupción irreversible de información esencial sin respaldo recuperable, o manipulación fraudulenta que implica responsabilidad penal. *Ejemplo*: Borrado completo de base de datos de 5 años de operación sin backup, alteración maliciosa de registros financieros para desvío de fondos.	**Inoperatividad total permanente; quiebra.** Caída catastrófica sin plan de recuperación efectivo que imposibilita cumplir contratos vigentes, atender clientes o mantener operaciones básicas durante días/semanas. *Ejemplo*: Ransomware que cifra toda la infraestructura sin respaldo, incendio del datacenter único sin DR plan.

H.3.2 Tabla completa de escala de probabilidad

Tabla H.3.2-1. Escala de probabilidad

Nivel	Descripción	Criterio operativo
0 - Imposible	**Técnicamente imposible** bajo la configuración actual o sin conexión lógica. El evento no puede ocurrir con los controles y arquitectura existentes, o no existe vector de ataque plausible. *Ejemplo*: Explotación de protocolo no implementado en la red, acceso físico a servidor ubicado en datacenter con controles biométricos cuando el atacante está en otro país.	El evento no puede ocurrir con los controles y arquitectura existentes, o no existe vector de ataque plausible (p. ej., protocolo no implementado; acceso físico no viable).
1 - Muy improbable	**Rara vez / Excepcional**. No ha ocurrido en los últimos 3-5 años. Requiere condiciones muy inusuales o un atacante muy sofisticado. El evento no tiene precedentes en la organización y requeriría una combinación improbable de factores (ej. vulnerabilidad 0-day + conocimiento interno privilegiado + timing perfecto). *Ejemplo*: Ataque APT dirigido específicamente a esta PyME, exfiltración mediante manipulación física del hardware sin detección.	El evento no tiene precedentes en la organización y requeriría una combinación improbable de factores (vulnerabilidad 0-day + conocimiento interno privilegiado + timing perfecto).
2 - Improbable	**Poco frecuente / Histórico remoto**. Ha ocurrido alguna vez en la historia de la empresa (>2 años atrás) o es posible teóricamente pero no habitual. El evento es técnicamente factible y se tiene conocimiento de casos similares en el sector, pero no es una amenaza recurrente para esta organización específica. *Ejemplo*: Ransomware en 2019 (antes de controles actuales), phishing exitoso documentado hace 3 años, falla de proveedor cloud que causó caída prolongada en el pasado.	El evento es técnicamente factible y se tiene conocimiento de casos similares en el sector, pero no es una amenaza recurrente para esta organización específica (p. ej., ransomware histórico; phishing exitoso antiguo; falla de proveedor cloud en el pasado).
3 – Probable	**Ocasional / Recurrente**. Ocurre periódicamente (ej. 1-2 veces al año). Es un riesgo conocido y factible sin requerir grandes recursos del atacante. El evento se materializa con cierta regularidad en esta organización o en pares del sector; existe evidencia de intentos o incidentes menores documentados. *Ejemplo*: Intentos de phishing bloqueados por filtro mensualmente (con 1-2 clicks de empleados al año), caídas de servicio de proveedor por mantenimientos no coordinados, errores de configuración detectados en auditorías anuales.	El evento se materializa con cierta regularidad en esta organización o en pares del sector; existe evidencia de intentos o incidentes menores documentados (p. ej., phishing bloqueado con 1–2 clics/año; caídas de proveedor; hallazgos en auditorías).
4 – Muy probable	**Frecuente / Inminente**. Ocurre varias veces al año (mensual/semanal) o es trivial de ejecutar (ej. error humano común, ataque automatizado masivo). El evento es parte de la realidad operativa cotidiana; puede materializarse sin acción maliciosa intencional (error humano) o mediante ataques automatizados no dirigidos. *Ejemplo*: Escaneos de puertos automatizados detectados semanalmente, empleados que olvidan cerrar sesión en equipos compartidos, errores de configuración en actualizaciones	El evento es parte de la realidad operativa cotidiana; puede materializarse sin acción maliciosa intencional (error humano) o mediante ataques automatizados no dirigidos (p. ej., escaneos semanales; sesiones abiertas; errores en actualizaciones mensuales; phishing masivo diario).

H.3.3 Tabla completa de escala de vulnerabilidad

Tabla H.3.3-1. Escala de vulnerabilidad

Nivel	Descripción	Criterio operativo
0 - Nula	Sin vulnerabilidad / Control total. El activo no está expuesto o cuenta con controles redundantes y verificados.	El activo está completamente aislado (no conectado) o protegido por múltiples capas de controles técnicos y organizacionales verificados por auditoría. **Evidencia requerida:** • Controles de cifrado extremo a extremo implementados • Segmentación de red validada (VLAN/Firewall) • Auditoría de seguridad reciente (< 6 meses) sin hallazgos críticos • Respaldos cifrados offsite con pruebas de recuperación exitosas **Ejemplo:** Servidor de base de datos crítica en DMZ con WAF, IDS/IPS, cifrado en reposo (AES-256), acceso solo vía VPN con MFA, logs centralizados en SIEM, respaldos automáticos diarios con recuperación probada mensualmente.
1 - Muy baja	**Muy baja / Control robusto.** Controles formales implementados, documentados y verificados periódicamente.	Existen controles preventivos y detectivos formalizados en políticas, implementados técnicamente y sujetos a revisión periódica. **Evidencia requerida:** • Política de seguridad documentada y aprobada por dirección • Actualizaciones de seguridad automáticas o gestionadas (parches críticos < 30 días) • Autenticación multifactor (MFA) implementada • Segregación de funciones (principio de menor privilegio) • Capacitación de personal en últimos 12 meses **Ejemplo:** Sistema ERP con autenticación LDAP + MFA (Google Authenticator), actualizaciones de seguridad aplicadas mensualmente, acceso basado en roles (RBAC) revisado trimestralmente, backups incrementales diarios con retención de 30 días, personal capacitado en manejo de incidentes.
2 - Baja	**Baja / Control estándar.** Controles básicos implementados pero sin verificación regular de efectividad.	Existen controles fundamentales pero sin procesos formales de mantenimiento o auditoría. La efectividad no se mide sistemáticamente. **Evidencia requerida:** • Antivirus/EDR instalado (puede ser versión gratuita) • Políticas de contraseñas definidas (complejidad mínima) • Firewall básico configurado • Respaldos configurados (no necesariamente probados) • Conciencia informal de seguridad (sin capacitación formal) **Ejemplo:** Servidor de archivos con Windows Defender actualizado, contraseñas con requisito de 8 caracteres alfanuméricos, firewall de Windows habilitado con reglas básicas, backup semanal en disco externo sin pruebas de recuperación, usuarios saben "no abrir adjuntos sospechosos" pero sin entrenamiento anti-phishing.
3 - Media	**Media / Control parcial o desactualizado.** Controles implementados parcialmente,	Los controles existen pero presentan debilidades significativas por falta de actualización, configuración incorrecta o cobertura incompleta. **Evidencia requerida:** • Software con versión no soportada pero aún funcional (ej. Windows Server 2012) • Antivirus desactualizado (definiciones > 7 días) • Contraseñas no rotadas periódicamente

	desactualizados o con configuraciones débiles.	• Respaldos irregulares o sin validación • Falta de monitoreo/logs de eventos de seguridad **Ejemplo:** Aplicación web en PHP 7.2 (EOL desde 2020), certificado SSL autofirmado, usuarios con contraseñas complejas pero sin cambio en 2+ años, backup mensual sin cifrar en NAS local accesible por toda la red interna, sin registros de acceso o auditoría.
4 - Alta	**Alta / Debilidad conocida.** Controles inefectivos, mal configurados o con fallas evidentes que facilitan explotación.	Existen controles nominales pero su implementación deficiente los hace inoperantes ante amenazas comunes. Vulnerabilidades conocidas sin remediar. **Evidencia requerida:** • Software sin actualizaciones críticas (> 6 meses de retraso) • Configuraciones por defecto sin cambiar • Uso de contraseñas compartidas entre usuarios • Ausencia de respaldos recientes (> 3 meses) • Servicios innecesarios expuestos a internet • Falta de segregación de red (todos los dispositivos en misma subred) **Ejemplo:** Sistema de gestión con contraseña de administrador compartida por email, accesible desde internet sin VPN, puerto RDP (3389) abierto con intentos de fuerza bruta diarios no monitoreados, último respaldo exitoso hace 4 meses, parches de seguridad pendientes desde hace 8 meses, logs no revisados nunca.
5 - Crítica	**Crítica / Ausencia de control.** Sin controles implementados o con exposición total. Explotación inmediata posible.	El activo carece completamente de medidas de protección, mantiene configuraciones de fábrica o está expuesto sin restricciones. Cualquier actor puede comprometer el activo. **Evidencia requerida:** • Credenciales por defecto sin cambiar (admin/admin, root/root) • Sin firewall o firewall completamente abierto (regla ANY/ANY) • Sin antivirus/EDR • Sin respaldos configurados • Sin políticas de seguridad • Personal sin conocimiento básico de amenazas • Servicios críticos accesibles públicamente sin autenticación **Ejemplo:** Router con contraseña admin/admin, cámara IP con interfaz web accesible desde internet sin contraseña, servidor NAS con SMB v1 habilitado y carpetas compartidas sin autenticación, estación de trabajo sin antivirus con software pirata desactualizado, datos sensibles sin cifrar en laptops sin bloqueo de pantalla.

H.3.4 Tabla completa de umbrales de aceptabilidad del riesgo

Tabla H.3.4-1. Umbrales de aceptación de riesgos de información (R=I*A*V)

Rango / Umbral	Clasificación	Representación (color/etiqueta)	Observación
0-10	Bajo (Aceptable)	Verde lima	**SE ACEPTA**. El costo de implementar controles adicionales supera el beneficio esperado. Riesgos triviales que no afectan activos críticos o cuyo impacto es fácilmente absorbible por la organización. No requiere acción adicional más allá del mantenimiento de controles actuales. **Ejemplo**: Pérdida de confidencialidad de información pública (Impacto 1), phishing bloqueado efectivamente (Amenaza 2, Vulnerabilidad 2).
11-30	Medio (Tolerable)	Ámbar	**SE MONITOREA**. Riesgo latente que requiere vigilancia y planificación de tratamiento a **mediano plazo** (6-18 meses) o cuando el presupuesto lo permita. Se acepta temporalmente bajo las siguientes condiciones: • Registro formal del riesgo en matriz de seguimiento • Revisión trimestral de evolución (probabilidad/impacto) • Asignación de responsable de monitoreo • Plan de contingencia documentado **Racionalidad**: PyMEs operan con riesgos medios controlados; eliminar todos sería prohibitivamente costoso y no necesariamente incrementaría la seguridad de manera proporcional. **Ejemplo**: Datos operativos con respaldos desactualizados (Impacto 2, Amenaza 3, Vulnerabilidad 3 = 18).
>30	Alto (Crítico)	Naranja intenso / Bermellón	**SE TRATA CON PRIORIDAD**. Inaceptable para la continuidad del negocio. Requiere acción correctiva **inmediata** (< 90 días) mediante una de las cuatro opciones de tratamiento: 1. **Mitigar**: Implementar controles para reducir probabilidad o impacto 2. **Transferir**: Contratar seguro cibernético, externalizar servicio 3. **Evitar**: Discontinuar actividad o activo asociado 4. **Aceptar formalmente**: Solo si existe justificación aprobada por alta dirección **Gatillo de escalamiento**: Cualquier riesgo > 30 debe ser presentado a gerencia dentro de 15 días hábiles de su identificación. **Ejemplo**: Base de datos de clientes sin MFA ni respaldos cifrados (Impacto 4, Amenaza 3, Vulnerabilidad 3 = 36).

Tabla H.3.4-2. Umbrales de aceptación de riesgos operacionales (R=I*P)

Rango / Umbral	Clasificación	Representación (color/etiqueta)	Observación
0-3	Bajo (Aceptable)	Verde lima	**SE ACEPTA**. Eventos con bajo impacto o probabilidad muy remota. El seguimiento rutinario mediante operaciones normales es suficiente. No requiere inversión adicional en controles. **Ejemplo**: Caída de servicio no crítico (chat interno) por mantenimiento (Impacto 1, Probabilidad 3 = 3).
4-8	Medio (Tolerable)	Ámbar	**E MONITOREA**. Riesgo gestionable con controles compensatorios o planes de contingencia. Tratamiento diferido hasta disponibilidad de recursos. Requiere: • Inclusión en registro de riesgos con revisión mensual • Procedimiento documentado de respuesta ante materialización • Métricas de seguimiento (KRIs - Key Risk Indicators) **Ejemplo**: Sistema ERP con parches retrasados pero con respaldos verificados (Impacto 3, Probabilidad 2 = 6).
>8	Alto (Crítico)	Naranja intenso / Bermellón	**SE TRATA CON PRIORIDAD**. Combinación de alto impacto y probabilidad significativa que amenaza objetivos del negocio. Requiere plan de tratamiento aprobado y recursos asignados dentro del trimestre actual. **Criterio de priorización interna** (dentro de rojos): • **Nivel 1 (Urgente)**: R ≥ 12 → Acción en 30 días • **Nivel 2 (Prioritario)**: R = 9-11 → Acción en 90 días **Ejemplo**: Servidor crítico sin respaldos funcionales con incidentes recurrentes (Impacto 4, Probabilidad 3 = 12).

CATALOGO DE ACTIVOS

H4_Activos_Consolidado_MONARC_v03

El siguiente modelado permite la producción de trazabilidad documental e informes estructurados para la toma de decisiones, reduciendo la dependencia de hojas de cálculo manuales y asegurando la reproducibilidad del análisis de riesgos en el contexto de la pyme.

- **SÍNTESIS DE ACTIVOS E IMPACTOS - INFORMACIÓN ADICIONAL**
- **¿Activos primarios identificados?**

Sí. Se identificaron cuatro (4) activos primarios siguiendo la metodología OCTAVE-S (límite ≤5 activos críticos para organizaciones pequeñas):

- **P1: Prestación de servicios de la PyME (Service Delivery)**
    - Proceso de negocio crítico que representa la capacidad operativa central.
    - Dimensiones de impacto: C=1, I=3, D=4 (centrado en la disponibilidad).
- **P2: Información de clientes (Customer Information)**
    - Datos personales sujetos a la Ley 1581/2012 (Ley de Protección de Datos de Colombia).
    - Dimensiones de impacto: C=4, I=3, D=3 (centrado en la confidencialidad).
- **P3: Continuidad operativa (Operational Continuity)**
    - Resiliencia empresarial y capacidad de recuperación ante desastres.
    - Dimensiones de impacto: C=1, I=2, D=4 (centrado en la disponibilidad).
- **P4: Cumplimiento legal y normativo (Legal and Regulatory Compliance)**
    - Obligaciones regulatorias (SIC, legislación laboral, legislación tributaria).
    - Dimensiones de impacto: C=2, I=3, D=2 (centrado en la integridad).
- **¿Criterios de seguridad?**

Sí. Evaluación de impacto basada en la tríada CIA de la norma ISO/IEC 27005:2022 (Confidencialidad, Integridad, Disponibilidad) utilizando una escala cualitativa 0-4:

- **0:** Ninguno.
- **1:** Bajo (inconveniente menor, impacto <$5M COP).
- **2:** Moderado (degradación temporal, impacto entre $5-25M COP).
- **3:** Significativo (interrupción operativa, impacto entre $25-100M COP).
- **4:** Crítico (impacto severo en el negocio, >$100M COP o sanciones regulatorias).

Nota: Criterios alineados con el contexto de la PyME (ingresos ~$500M COP/año, 20 empleados).

- **¿Principales activos de soporte?**

Sí. 95 activos de soporte organizados en 4 categorías estratégicas siguiendo el modelo de dependencia de MAGERIT v3.0 (esencial ↔ soporte):

- **S1: Infraestructura TI (IT Infrastructure) - 30 activos operativos**
    - Ejemplos: Servidor de aplicaciones, enrutador principal, portátiles corporativos, equipos de red.
- **S2: Software y aplicaciones (Software and Applications) - 25 activos operativos**
    - Ejemplos: Sistema ERP, servicio de correo electrónico, software de respaldo, herramientas de productividad.

- **S3: Personal y RRHH (Personnel and Human Resources) - 20 activos operativos**
    - Ejemplos: Administrador de sistemas, desarrolladores clave, gerente de operaciones.
- **S4: Documentación y procedimientos (Documentation and Procedures) - 20 activos operativos**
    - Ejemplos: SOPs (Procedimientos Operativos Estándar), políticas de seguridad, planes de continuidad de negocio, contratos.

Total: 99 activos (4 primarios + 4 estratégicos + 91 operativos) con herencia de impacto habilitada (primario → estratégico → operativo).

- **¿Características del modelado?**

El modelado de activos implementado en MONARC presenta:

1. **Estructura jerárquica (3 niveles):**
    - Los activos primarios definen los impactos a nivel de negocio (valores CIA).
    - Los activos estratégicos heredan y propagan los impactos.
    - Los activos operativos reciben impactos transitivos automáticamente.
2. **Mecanismo de herencia de impacto:**
    - Funcionalidad nativa de MONARC utilizada para transmitir en cascada los valores CIA desde los activos primarios.
    - Habilita la trazabilidad: riesgo operativo → activo de soporte → activo primario → impacto en el negocio.
3. **Catálogos integrados de amenazas y vulnerabilidades:**
    - 132 amenazas contextualizadas (sintetizadas de NIST 800-30 + MAGERIT + EBIOS RM).
    - Evaluación de vulnerabilidades basada en la madurez de controles (Hoja de trabajo 4 de OCTAVE-S).
    - Conjunto de recomendaciones personalizadas (11 controles adaptados al contexto de la PyME colombiana).
4. **Trazabilidad documental e informes estructurados:**
    - Vinculación activo-escenario-riesgo-decisión mantenida durante todo el flujo de trabajo.

- Generación automática de informes de inventario, matrices de riesgo y planes de tratamiento.
- Formatos de exportación (PDF, JSON, CSV) que habilitan la auditabilidad y reducen la dependencia de hojas de cálculo.

5. **Alineación con metodología híbrida (Síntesis Fase I):**
   - **OCTAVE-S:** Enfoque autodirigido, ≤5 activos críticos, enfoque en riesgo operativo.
   - **ISO 27005:** Criterios de aceptación de riesgos, opciones de tratamiento (reducir/transferir/aceptar/evitar).
   - **NIST 800-30:** Caracterización de amenazas (fuente/evento), escalas de probabilidad.
   - **MAGERIT:** Dependencias de activos (esencial ↔ soporte), propagación de impacto.
   - **EBIOS RM:** Eventos temidos (consecuencias operativas: dimensiones R/O/L/F/P).

CATALOGO DE AMENAZAS

Código	Etiqueta	Descripción	C	I	D	Theme
TH001	Phishing	Engaños a usuarios a través de correos maliciosos	1	0	0	Compromise of information
TH002	Ransomware	Secuestro de información mediante cifrado malicioso	0	0	1	Compromise of information
TH003	Denegación de Servicio (DoS/DDoS)	Ataques que inundan un servidor o red con tráfico, dejándolos inoperativos	0	0	1	Compromise of information
TH004	Ataques de Ingenieria Social	Manipulación psicológica o engaños que llevan a los usuarios a revelar información sensible	1	1	0	Compromise of information
TH005	Pharming	Manipulación de las direcciones DNS que utilizan los usuarios y los llevan a páginas web falsas, que simulan ser las de entidades bancarias o de portales de ventas online, entre otras. Una vez allí, el usuario digita sus datos, los cuales son capturados y utilizados para la ejecución de fraudes.	0	1	1	Compromise of information
TH006	Malware	Software malicioso diseñado para dañar, interrumpir o comprometer sistemas informáticos: Keylogger: Captura de pulsaciones del teclado para obtener información sensible Gusanos: Programas auto-replicantes que se propagan a través de redes y sistemas Troyanos: Software malicioso que se oculta en aplicaciones legitimas Adware: Software publicitario intrusivo que se instala sin consentimiento Rootkit: Herramienta maliciosa que permite acceso persistente a un sistema comprometido	0	1	0	Compromise of information
TH007	Spoofing	Robo de información simulando un sitio web oficial, en donde el usuario confiado digita su información personal, como usuario, contraseñas, números de cuenta, entre otros.	1	0	0	Compromise of information
TH008	Bypass de reglas	Explotación de Configuraciones incorrectas para saltarse restricciones.	0	1	0	Compromise of information
TH009	Ping Flood	Ataques DoS mediante el envío masivo de solicitudes ICMP (ping).	0	0	1	Compromise of information
TH010	Fragment Flood y Jumbo Frame	Ataque que explota la fragmentación de paquetes de red o el uso de marcos de gran tamaño (jumbo frames) para saturar el ancho de banda y provocar interrupciones en el servicio.	0	0	1	Compromise of information
TH011	VLAN Hopping	Explotación de Configuraciones incorrectas para acceder a otras VLANs.	1	1	1	Compromise of information

Código	Etiqueta	Descripción	C	I	D	Theme
TH012	MAC Flooding	Ataques que saturan la tabla CAM del switch.	0	0	1	Compromise of information
TH013	NTP Reflexion	Ataque de amplificación que utiliza servidores NTP mal configurados para inundar una red objetivo con tráfico, aprovechando el protocolo de tiempo de red.	0	0	1	Compromise of information
TH014	Cross-Site request Forgery (CSRF)	Aprovechamiento de la sesión autenticada del usuario para ejecutar acciones no autorizadas.	0	1	0	Compromise of information
TH015	Wormhole, Sinkhole	Ataque en el que un nodo malicioso intercepta y redirige el tráfico de red, o crea un "hueco" en la red para controlar el flujo de datos y manipular rutas.	1	1	0	Compromise of information
TH016	Slowloris	Ataque de denegación de servicio que envía solicitudes HTTP parciales y lentas para mantener las conexiones abiertas, agotando los recursos del servidor sin necesidad de alto volumen de tráfico.	0	0	1	Compromise of information
TH017	Dumpster Diving	Técnica de ingeniería social que implica buscar información sensible en la basura, como documentos desechados, que pueda ser utilizada para acceder a sistemas o realizar fraudes.	1	0	1	Compromise of information
TH018	Rogue APs	Creación de puntos de acceso falsos para interceptar el tráfico.	1	0	0	Compromise of information
TH019	Password Cracking	Método de ataque que busca descifrar contraseñas utilizando técnicas como fuerza bruta, diccionarios o ataques de relleno de credenciales.	1	0	0	Compromise of information
TH020	Inyecciones de comandos FTP	Inyección de comandos maliciosos en las transferencias.	0	0	1	Compromise of information
TH021	TCP Syn Attack	Ataque que explota el proceso de establecimiento de conexión TCP enviando múltiples solicitudes SYN sin completar la conexión, agotando los recursos del servidor.	1	1	1	Compromise of information
TH022	DHCP Starvation	Saturación de direcciones IP disponibles por dispositivos maliciosos.	0	0	1	Compromise of information
TH023	Envenenamiento de cache DNS	Alteración de respuestas DNS para redirigir a los usuarios a sitios maliciosos.	0	1	0	Compromise of information
TH024	Ataque Man In The Middle -MITM	Interceptación de comunicaciones para manipular o robar información	1	1	0	Compromise of information
TH025	Compromiso de Credenciales	Acceso no autorizado a sistemas mediante la captura de credenciales legitimas	1	0	0	Compromise of information
TH026	Intercepción de Comunicaciones	Interceptar las comunicaciones electrónicas para acceder a información confidencial	1	0	0	Compromise of information

Código	Etiqueta	Descripción	C	I	D	Theme
TH027	SQL Injection	Inyección de comandos SQL en formularios para acceder a bases de datos	0	1	1	Compromise of information
TH028	Sniffing de tráfico SNMP	Captura de trafico de red para extraer datos de dispositivos de red.	1	0	0	Compromise of information
TH029	Cross-Site-Scripting (XSS)	Ejecución de scripts maliciosos en páginas web vulnerables	0	1	0	Compromise of information
TH030	Difusión de software dañino	Propagación de software malicioso, como malware, virus o ransomware, que busca comprometer los sistemas y datos de la organización.	0	1	1	Technical failures
TH031	Alteración de la Información	Manipulación no autorizada de la Información almacenada o en tránsito, con el fin de modificar el contenido original y afectar su integridad.	0	1	0	Compromise of information
TH032	Reencaminamiento de mensajes	Intercepción y redirección de mensajes o datos a destinos no autorizados, comprometiendo la seguridad de las comunicaciones y la confidencialidad de la Información.	1	0	1	Compromise of information
TH033	Fallo de Servidor	Fallos técnicos en el servidor que afectan los datos almacenados	0	0	1	Technical failures
TH034	Fallo de Disco Duro	Fallo en el almacenamiento físico de discos duros que resulta en perdida de datos	0	0	1	Technical failures
TH035	Repudio por fallos técnicos de registro y auditoría	Incapacidad de demostrar que un usuario o entidad realizó una acción determinada en un sistema, debido a fallas en los mecanismos de registro, trazabilidad o auditoría, lo que impide atribuir responsabilidades de forma verificable.	0	1	1	Technical failures
TH036	Parche de Seguridad No Aplicado	Fallo en la aplicación de parches de seguridad	0	0	1	Technical failures
TH037	Borrado Accidental de Datos	Eliminación involuntaria de Información por parte de los empleados, debido a errores de manejo o configuración	0	0	1	Compromise of functions
TH038	Errores de los usuarios	Falta de conocimientos o habilidades que llevan a tomar decisiones incorrectas o a ejecutar acciones no deseadas	1	1	1	Compromise of functions
TH039	Errores en Instalación	Problemas causados por una instalación incorrecta de sistemas, hardware o software que puede afectar su funcionamiento	0	0	1	Compromise of functions
TH040	Errores en Mantenimiento	Fallas durante el proceso de mantenimiento, como la falta de aplicación de parches o Actualizaciones de seguridad	0	0	1	Compromise of functions
TH041	Errores en Actualización	Errores cometidos durante la actualización de software, hardware o sistemas, que pueden causar problemas operativos	0	0	1	Compromise of functions

Código	Etiqueta	Descripción	C	I	D	Theme
TH042	Errores en Configuración	Mala configuración de sistemas que deja vulnerabilidades abiertas o impide el funcionamiento adecuado de los mismos	1	1	1	Compromise of functions
TH043	Errores de Administracion	Fallas en la gestión administrativa de los sistemas, que pueden afectar la integridad o la disponibilidad de los datos	0	1	1	Compromise of functions
TH044	Errores en Secuencia	Modificación no autorizada o incorrecta del orden de los comandos en sistemas. Ya está en el archivo, pero podría reforzarse.	0	1	1	Compromise of functions
TH045	Errores en Uso	Empleados que usan incorrectamente sistemas o aplicaciones, generando problemas en su funcionamiento o seguridad	0	0	1	Compromise of functions
TH046	Errores en Monitorizacion	Fallas en el monitoreo de sistemas o redes, lo que puede impedir la detección temprana de incidentes de seguridad	0	0	1	Compromise of functions
TH047	Errores en la planificación del proyecto	Fallos en la definición o programación de las actividades, recursos o tiempos del proyecto, que pueden resultar en retrasos, costos imprevistos o incumplimientos de objetivos.	0	0	1	Compromise of functions
TH048	Errores en el cálculo del presupuesto	Inexactitudes en la estimación de los costos o en la asignación de recursos financieros que llevan a insuficiencias presupuestarias o desperdicio de fondos.	0	0	1	Compromise of functions
TH049	Fallos en la segregación de funciones	Asignación incorrecta de responsabilidades o funciones críticas, que puede generar conflictos de interés o debilitar los controles internos de seguridad.	0	0	1	Compromise of functions
TH050	Errores en Comunicaciones	Problemas en la comunicación interna o externa que afectan la operatividad de la organización o causan malentendidos	0	0	1	Compromise of functions
TH051	Indisponibilidad del personal	Ausencia o falta de personal clave para llevar a cabo operaciones criticas o para atender emergencias	1	0	1	Compromise of functions
TH052	Vulnerabilidades no controladas	Vulnerabilidades conocidas en los sistemas que no han sido gestiónadas ni corregidas a tiempo	1	1	1	Compromise of functions
TH053	Caída del sistema por agotamiento de recursos	Colapso de sistemas debido a la falta de recursos como espacio de almacenamiento, memoria o poder de procesamiento	0	0	1	Compromise of functions
TH054	Alteración accidental de la Información	Modificación no intencional de los datos por parte de los usuarios o del personal de TI	0	1	0	Compromise of functions
TH055	Destrucción de Información	Perdida irrecuperable de Información debido a fallos accidentales en los sistemas o por error humano	0	0	1	Compromise of functions
TH056	Capacidades	Fallas debido a la falta de capacidades o habilidades técnicas por parte del personal encargado de las operaciones	0	0	1	Compromise of functions

Código	Etiqueta	Descripción	C	I	D	Theme
TH057	Deficiencias en la organización	Problemas estructurales en la organización que impiden la ejecución correcta de táreas y operaciones	1	1	1	Compromise of functions
TH058	Configuración Errónea de Seguridad	Configuración incorrecta de medidas de seguridad que deja sistemas vulnerables a ataques o accesos no autorizados	0	0	1	Compromise of functions
TH059	Peculado	Apropiación indebida o uso fraudulento de recursos o bienes públicos o privados por parte de un funcionario o empleado con acceso a dichos activos.	0	0	1	Unauthorized actions
TH060	Soborno	Ofrecimiento o recepción de dinero, bienes o favores a cambio de influir en las decisiones o acciones de una persona en una posición de poder o autoridad.	1	1	1	Unauthorized actions
TH061	Extorsion	Obtención de dinero, bienes o servicios mediante amenazas o coerción, forzando a la víctima a cumplir con las demandas del extorsionador.	1	1	1	Unauthorized actions
TH062	Cohecho	Acto de ofrecer o recibir beneficios económicos a cambio de la realización o no de un acto dentro de las funciones de un funcionario público.	1	1	1	Unauthorized actions
TH063	Falsificación de documentos	Alteración, creación o Modificación fraudulenta de documentos con la intención de engañar o cometer un fraude para obtener beneficios financieros o influir en decisiones.	0	1	0	Unauthorized actions
TH064	Ciberextorsion	Amenaza en la que se exige un pago a cambio de no realizar un ataque o liberar Información robada	1	1	1	Compromise of information
TH065	Ciberterrorismo	Uso de la tecnología para llevar a cabo actos terroristas, como ataques a infraestructuras criticas o sistemas	1	1	1	Compromise of information
TH066	Ciberdelincuencia	Actividades ilegales realizadas a través de medios digitales, como fraudes, robos de identidad, y estafas	1	0	0	Compromise of information
TH067	Ciberataques	Acciones deliberadas para comprometer la seguridad de sistemas informáticos o redes	1	1	1	Compromise of information
TH068	Cibersecuestro	Secuestro de Información o sistemas mediante software malicioso que bloquea el acceso, generalmente para pedir un rescate (similar al ransomware)	0	0	1	Compromise of information
TH069	Ciberespionaje	Actividades de espionaje realizadas a través de sistemas informáticos, generalmente para robar Información confidencial o estratégica	1	0	0	Compromise of information
TH070	Operadores de Botnets	Grupos que controlan una red de dispositivos comprometidos (botnets) para realizar actividades maliciosas, como ataques DDoS o envío de spam	0	0	1	Compromise of information
TH071	Grupos criminales	Organizaciones dedicadas a actividades delictivas a través de medios tecnológicos,	1	0	0	Compromise of information

Código	Etiqueta	Descripción	C	I	D	Theme
		como robos de identidad, fraudes, o estafas en línea				
TH072	Servicios de inteligencia extranjeros	Entidades gubernamentales extranjeras que buscan infiltrarse en sistemas informáticos para robar Información sensible o realizar ciberespionaje	1	0	0	Loss of essential services
TH073	Hackers	Individuos o grupos que buscan vulnerabilidades en sistemas y redes para explotarlas con diversos fines, desde el reconocimiento hasta el robo de datos o ataques	1	0	0	Compromise of information
TH074	Atacante interno(insider)	Empleados o personas con acceso legitimo a los sistemas de la organización que utilizan ese acceso para llevar a cabo actos maliciosos o sabotajes	0	0	1	Compromise of information
TH075	Información Interna	Uso o filtración indebida de Información confidencial por parte de empleados con acceso autorizado a los sistemas internos	1	0	1	Unauthorised actions
TH076	Divulgación, Fuga, Modificación o de Información	Actos deliberados que implican la divulgación no autorizada, Modificación o destrucción de Información sensible	1	1	1	Unauthorised actions
TH077	Agotamiento de Recursos	Uso indebido o excesivo de los recursos del sistema, lo que puede llevar a su agotamiento y afectar las operaciones normales	1	1	1	Unauthorised actions
TH078	Manipulación de los Sistemas (HW,SF,TC)	Cambios no autorizados en los sistemas de hardware, software o telecomunicaciones que comprometen su funcionamiento	0	1	1	Unauthorised actions
TH079	Abuso de Privilegios de Acceso	Uso indebido de los privilegios otorgados para acceder a sistemas o Información, excediendo los permisos concedidos	0	0	1	Unauthorised actions
TH080	Manipulación de la configuración	Alteración deliberada de la configuración de sistemas críticos para causar fallos o abrir brechas de seguridad	0	1	1	Unauthorised actions
TH081	Suplantación de la identidad del usuario	Acto de hacerse pasar por otro usuario autorizado para obtener acceso a Información o sistemas que normalmente no se permitirían	1	1	1	Unauthorised actions
TH082	Manipulación de los registros de actividad (log)	Alteración o Eliminación de los registros de actividad de sistemas (logs) para ocultar acciones maliciosas o actividades ilegales	0	1	0	Unauthorised actions
TH083	[Re-]encaminamiento de mensajes	Redirigir mensajes o datos a un destino no autorizado para interceptar comunicaciones confidenciales o manipularlas	1	1	0	Unauthorised actions
TH084	Alteración de Secuencia	Modificación no autorizada del orden de ejecución de los comandos o instrucciones en un sistema para alterar sus funciones	0	1	1	Unauthorised actions
TH085	Ataques de Rogue DHCP	Configuración de servidores DHCP maliciosos que asignan direcciones IP incorrectas.	1	1	1	Compromise of information
TH086	Análisis de tráfico	Monitoreo del tráfico de red para identificar patrones de comunicación y posibles vulnerabilidades explotables	1	1	1	Unauthorised actions

Código	Etiqueta	Descripción	C	I	D	Theme
TH087	Repudio como acción no autorizada o conducta del usuario	Negación por parte de un usuario o entidad de haber realizado una acción específica dentro de un sistema, como enviar un mensaje, aprobar un trámite, modificar un registro o ejecutar una transacción, generando incertidumbre sobre la autoría de la acción.	0	1	0	Unauthorized actions
TH088	Difusión de software dañino	Instalación o propagación intencional de software malicioso dentro de la organización para comprometer sistemas	1	1	1	Technical failures
TH089	Uso No Previsto	Uso de los sistemas o la Información de manera que no estaba prevista ni autorizada, lo que puede resultar en fallos o riesgos	0	0	1	Unauthorized actions
TH090	Sabotaje Interno	Actos deliberados para causar daño a la organización desde dentro, utilizando acceso autorizado a sistemas críticos	0	0	1	Unauthorized actions
TH091	Piggybacking	Cuando una persona no autorizada accede a un área restringida aprovechando que otra persona con acceso permitido le permite el ingreso, generalmente sin darse cuenta.	1	1	1	Compromise of information
TH092	Shoulder Surfing	Técnica de observación en la que un atacante mira sobre el hombro de una persona para obtener Información confidencial, como contraseñas o datos en una pantalla.	1	0	0	Compromise of information
TH093	Suplantación	Acto en el que una persona se hace pasar por otra, ya sea físicamente o a través de documentos falsificados, para obtener acceso a áreas o sistemas restringidos.	0	1	1	Compromise of information
TH094	Acceso informático no autorizado	Cuando una persona ingresa a sistemas informáticos o redes sin el debido permiso, vulnerando las medidas de seguridad para acceder a Información sensible.	1	1	1	Compromise of information
TH095	Intrusion en Data Center	Entrada no autorizada a las instalaciones del Data Center, lo que puede comprometer la seguridad física de los servidores y sistemas	1	1	1	Compromise of information
TH096	Robo de Equipos	Perdida o sustracción de equipos que contienen Información sensible y que son esenciales para la operación de la organización, como servidores, discos duros, o dispositivos de red, exponiendo al riesgo de filtración de datos o mal uso de la Información.	1	0	0	Physical damage
TH097	Vandalismo	Daños deliberados a la infraestructura física de la organización, como romper equipos, sistemas o instalaciones	0	0	1	Compromise of information
TH098	Daño Deliberado a Servidores	Actos intencionales para destruir o dañar los servidores u otros equipos críticos, lo que puede interrumpir las operaciones	0	0	1	Compromise of information

Código	Etiqueta	Descripción	C	I	D	Theme
TH099	Inundación	Desborde de agua o fallas en los sistemas de drenaje causando daños a las instalaciones o equipos	0	0	1	Physical damage
TH100	Huracanes	Tormentas con fuertes vientos y lluvias que pueden causar destrucción en infraestructuras	0	0	1	Physical damage
TH101	Tormentas eléctricas	Fenómenos meteorológicos que incluyen rayos y fuertes lluvias, con potencial de dañar sistemas eléctricos y electrónicos	1	1	1	Physical damage
TH102	Terremoto	Movimiento sísmico de la tierra que puede causar colapso de edificios, daños en infraestructuras y equipos	1	1	1	Physical damage
TH103	Incendio	Fuego que puede dañar o destruir edificios, sistemas y equipos críticos, comprometiendo la operatividad de la organización	0	0	1	Physical damage
TH104	Condiciones inadecuadas de temperatura o humedad	Exposición de los sistemas críticos a temperaturas extremas o niveles de humedad inadecuados, lo que puede afectar su funcionamiento o causar daños irreversibles	1	0	1	Compromise of information
TH105	Desastres industriales	Fallos graves en procesos industriales, como derrames químicos, explosiones o emisiones toxicas, que impactan directamente la infraestructura y los sistemas de la organización	0	0	1	Physical damage
TH106	Degradación de los soportes de almacenamiento de la Información	Deterioro físico o lógico de los medios de almacenamiento que afecta la disponibilidad y confiabilidad de los datos	0	0	1	Compromise of information
TH107	Emanaciones electromagnéticas	Interferencias electromagnéticas que afectan el funcionamiento de equipos electrónicos y sistemas de comunicación	1	1	1	Compromise of information
TH108	Contaminación mecánica	Contaminación en entornos operativos que puede dañar equipos físicos y afectar la eficiencia de las operaciones	1	1	1	Physical damage
TH109	Contaminación electromagnética	Perturbaciones en los equipos electrónicos debido a radiaciones electromagnéticas externas o internas	1	1	1	Compromise of information
TH110	Avería de origen físico o lógico	Fallo de los componentes físicos o del software que impide el funcionamiento correcto de sistemas o dispositivos	0	0	1	Compromise of information
TH111	Fallo de servicios de comunicaciones	Interrupciones en los servicios de comunicación que impiden la transmisión de datos o el acceso a redes	0	0	1	Loss of essential services
TH112	Interrupción de otros servicios y suministros esenciales	Corte en los suministros esenciales (agua, gas, internet) que afectan la operatividad de la empresa	0	0	1	Loss of essential services
TH113	Corte de Suministro de Energía	Interrupciones en el suministro eléctrico que afectan la operatividad de los sistemas y equipos	0	0	1	Compromise of information
TH114	Fallo de Sistema UPS	Fallo en los sistemas de alimentación ininterrumpida (UPS) que resultan en la perdida de energía critica	0	0	1	Compromise of information

Código	Etiqueta	Descripción	C	I	D	Theme
TH115	Sobrecarga de Energia	Exceso de consumo eléctrico que puede dañar equipos o causar cortes imprevistos en la red eléctrica	0	0	1	Compromise of information
TH116	Sanciones por incumplimiento de normativas de protección de datos	Multas o sanciones impuestas por organismos reguladores debido al incumplimiento de las leyes de protección de datos personales	1	1	1	Compromise of functions
TH117	Multas por Incumplimiento de auditorías de Seguridad	Penalizaciones derivadas de auditorías fallidas en seguridad de la Información	0	0	1	Compromise of functions
TH118	Cambio de legislación	Modificaciones en las leyes o regulaciones que pueden afectar las operaciones de la organización, obligando a realizar ajustes en procedimientos o cumplimiento normativo.	0	1	0	Compromise of functions
TH119	Cambio de política monetaria	Variaciones en la política económica del gobierno, como ajustes en tasas de interés o medidas inflacionarias, que impactan el costo de financiación y la estabilidad financiera de la empresa.	1	1	1	Compromise of functions
TH120	Cambio de hábitos de compra del consumidor	Alteraciones en las preferencias o comportamientos de los consumidores que pueden reducir la demanda de productos o servicios de la organización, afectando sus ingresos.	0	1	0	Compromise of functions
TH121	Fluctuaciones de tasas de interés, tasas de cambio, precios	Variaciones en los tipos de interés, divisas o precios de materias primas que pueden aumentar los costos operativos o disminuir los márgenes de ganancia de la empresa.	1	1	1	Compromise of functions
TH122	Adquisición de Activos de Información sin Garantías	Compra de activos o tecnologías sin las garantías necesarias para su funcionamiento seguro o conforme a estándares	1	1	1	Compromise of functions
TH123	Contratación de Personal sin Cumplimiento de Requisitos	Contratación de empleados que no cumplen con los requisitos o competencias necesarias para gestionar activos de Información	0	0	1	Compromise of functions
TH124	Escape de Información	Perdida o filtración de Información debido a cambios mal planificados o ejecutados en la organización	0	0	1	Compromise of functions
TH125	Perdida de Activos de Información	Desaparición o deterioro de activos de información durante la implementación de cambios organizacionales	0	0	1	Compromise of functions
TH126	Modificaciones no autorizadas	Cambios realizados en los sistemas o procesos sin la debida autorización, lo que puede comprometer la seguridad	0	1	1	Compromise of functions
TH127	Indisponibilidad del Talento Humano	Ausencia de personal clave para la operación, lo que afecta la continuidad del negocio	1	0	1	Compromise of functions

Código	Etiqueta	Descripción	C	I	D	Theme
TH128	Indisponibilidad Financiera	Falta de recursos financieros para realizar cambios o mantener la operación ante imprevistos organizacionales	0	0	1	Compromise of functions
TH129	Contratación de Proveedores sin Cumplimiento de Requisitos	Riesgo derivado de subcontratar proveedores que no cumplen con los estándares o requisitos de seguridad de la organización	1	1	1	Loss of essential services
TH130	Contratación de Servicios sin cumplimiento de requisitos	Subcontratación de servicios críticos sin revisar las garantías de calidad o seguridad, lo que expone a la organización a riesgos	1	1	1	Loss of essential services
TH131	Riesgos por outsourcing	Dependencia excesiva de terceros para la operación, lo que puede generar vulnerabilidades o exposición a riesgos externos	1	0	0	Loss of essential services
TH132	Compromiso de Proveedor Crítico	Fallo o compromiso de un proveedor esencial que afecta directamente la operatividad o la continuidad del negocio	0	0	1	Loss of essential services
TH133	Interrupción en la Cadena de Suministro de TI	Falta de entrega o retraso en los suministros críticos de tecnología o servicios de TI, impactando en la capacidad operativa	0	0	1	Loss of essential services

CATALOGO DE VULNERABILIDADES

Código	Etiqueta	Descripción
VUL0001	APIs con permisos excesivos: Las APIs permiten más permisos o privilegios de los necesarios, lo que puede aumentar el riesgo de abuso o acceso no autorizado.	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0002	APIs expuestas innecesariamente: APIs innecesarias o servicios sin uso permanecen abiertos y accesibles, lo que aumenta la superficie de ataque.	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0003	APIs sin autenticación: Las interfaces permiten accesos no autenticados a sistemas críticos.	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0004	Acceso no autorizado a sistemas de ventilación y refrigeración: El acceso no controlado a los sistemas de ventilación y refrigeración puede permitir a un atacante sabotear estos sistemas y causar sobrecalentamiento.	La falta de controles de acceso físico puede permitir que personas no autorizadas entren en áreas sensibles.
VUL0005	Acceso no controlado a dispositivos de red: Falta de medidas físicas para restringir el acceso a routers, switches y firewalls en las salas de servidores o cuartos de telecomunicaciones.	La falta de controles de acceso físico puede permitir que personas no autorizadas entren en áreas sensibles.

Código	Etiqueta	Descripción
VUL0006	Accesos no revocados después de la desvinculacion de empleados: No revocar inmediatamente los accesos de los empleados cuando se desvinculan, permite que sigan teniendo acceso a información y sistemas críticos, lo que aumenta el riesgo de filtracion...	No existe una política clara para la asignación y control de permisos a sistemas.
VUL0007	Actualización inconsistente de sistemas antiguos: La falta de parches en sistemas antiguos u obsoletos puede dejar huecos de seguridad, ya que estos sistemas no son actualizados con las ultimas correcciones de seguridad.	No se implementan parches de seguridad de manera oportuna, lo que deja expuestos los sistemas a vulnerabilidades conocidas.
VUL0008	Almacenamiento inseguro de copias de seguridad: Las copias de seguridad no estan almacenadas de forma segura, como en ubicaciones geograficamente distintas, lo que aumenta el riesgo de perdida en caso de desastres físicos o ciberataques.	Falta de procedimientos adecuados para respaldar la información de la organización.
VUL0009	Ataques de la cadena de suministro (Supply Chain Attack): Infiltracion en los sistemas de los proveedores y alteran el código fuente o introducen malware en el software o hardware antes de que llegue a la organización, permitiendo el acceso a la...	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0010	Ausencia de políticas de acceso y autenticación: La falta de implementacion de políticas claras para controlar el acceso a sistemas críticos, ni definir políticas de autenticación seguras, como el uso de autenticación multifactor (MFA) o la rotacion...	Ausencia o inadecuación de políticas claras para la gestión de la seguridad de la información.
VUL0011	Ausencia de un plan de contingencia para fallos de terceros: La falta de planes adecuados para reaccionar ante fallos o interrupciones de terceros. Esto puede resultar en tiempos de inactividad prolongados, perdida de servicios o productos, y una...	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.
VUL0012	Buffer overflow: Los atacantes pueden desbordar la memoria de un programa y ejecutar código malicioso.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0013	Componentes desactualizados: Bibliotecas o software de terceros que no se han actualizado con las ultimas versiones de seguridad.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos

Código	Etiqueta	Descripción
		o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0014	Compromiso de la infraestructura del proveedor: Si la infraestructura del proveedor (red, servidores, etc.) se ve comprometida por un ataque, esto podría afectar a los servicios o productos proporcionados a la empresa, exponiendola a posibles...	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0015	Compromiso de proveedores de servicios en la nube: Interrupciones o acceso no autorizado a datos almacenados en la nube, que afectan directamente la disponibilidad y seguridad de la información critica.	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0016	Compromiso de sistemas de proveedores críticos: Si los sistemas de un proveedor son hackeados o comprometidos, los atacantes pueden usar esta posicion para lanzar ataques a la organización que dependa de dichos servicios o productos, aprovechandose de...	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0017	Configuración de puertos inseguros: Puertos no seguros o innecesarios estan abiertos, lo que aumenta el riesgo de ataques.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0018	Configuración inadecuada de módulos de seguridad: Módulos de seguridad no configurados correctamente o deshabilitados, lo que aumenta las vulnerabilidades.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0019	Configuración incorrecta de NAT/PAT: Configuraciones incorrectas de NAT/PAT que permiten el redireccionamiento inadecuado del trafico, exponiendo la red interna a ataques.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0020	Configuración incorrecta de VLANs: Segmentacion de redes mal implementada que permite el acceso no autorizado a diferentes segmentos de red.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0021	Configuración incorrecta de permisos de archivo: Permisos de archivo mal configurados, exponiendo archivos sensibles.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0022	Contraseñas débiles o reutilizadas: El uso de contraseñas faciles de adivinar o que son reutilizadas en multiples sistemas facilita los ataques de fuerza bruta y de relleno de credenciales.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.

Código	Etiqueta	Descripción
VUL0023	Contraseñas predeterminadas no modificadas: El uso de contraseñas predeterminadas en aplicaciones o sistemas que no han sido modificadas representa un riesgo elevado, ya que estas contraseñas suelen ser conocidas por atacantes y fácilmente explotables.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0024	Contraseñas predeterminadas no modificadas: Uso de contraseñas por defecto en dispositivos o sistemas que no han sido modificadas, permite accesos no autorizados fácilmente.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0025	Danos físicos en hardware: Golpes, caidas u otros danos físicos que comprometen el funcionamiento del hardware.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0026	Dependencia de parches manuales: La dependencia de la aplicacion manual de parches, genera retrasos en la implementacion de Actualizaciones. Este proceso es propenso a errores humanos y puede causar que algunos sistemas queden desprotegidos durante...	No se implementan parches de seguridad de manera oportuna, lo que deja expuestos los sistemas a vulnerabilidades conocidas.
VUL0027	Dependencia excesiva de un unico proveedor: La falta de proveedores alternativos aumenta este riesgo cuando la empresa depende en gran medida de un solo proveedor para productos o servicios clave.	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.
VUL0028	Dependencias inseguras: Cuando el software depende de bibliotecas o componentes de terceros que contienen vulnerabilidades.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0029	Desconfiguración accidental: Modificacion incorrecta de parametros críticos durante operaciones regulares.	Los usuarios o administradores pueden cometer errores que comprometan la seguridad.
VUL0030	Desconocimiento sobre seguridad: Los empleados no estan al tanto de las mejores practicas, lo que les impide detectar y reaccionar ante amenazas como correos de phishing, contraseñas débiles o uso inseguro de sistemas.	Los empleados no tienen el conocimiento necesario para operar de manera segura dentro de los sistemas de la organización.
VUL0031	Deserializacion insegura: Ocurre cuando un software acepta datos serializados sin validacion adecuada,	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o

Código	Etiqueta	Descripción
	permitiendo que se ejecuten comandos maliciosos cuando los datos se deserializan.	pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0032	Desgaste por uso prolongado: El uso prolongado o continuo de dispositivos de hardware sin mantenimiento puede provocar desgaste de componentes mecanicos o electronicos. Esto incluye dispositivos de almacenamiento, ventiladores y cables.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0033	Desprotección en equipos moviles: Falta de medidas de seguridad físicas para proteger dispositivos moviles, como laptops o smartphones, exponiendolos a danos o robos.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0034	Empleados desmotivados: La desmotivacion de los empleados puede llevar a errores accidentales, baja productividad o, en casos extremos, comportamientos negligentes que comprometen la seguridad de la información, como no seguir las políticas de...	Los usuarios o administradores pueden cometer errores que comprometan la seguridad.
VUL0035	Errores de control de acceso (IDOR): Los errores de control de acceso ocurren cuando el software permite a un usuario acceder a recursos sin una validacion adecuada de permisos.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0036	Errores de ingreso manual de datos: Ingresar datos incorrectos en sistemas críticos puede generar errores que afecten la funcionalidad de los sistemas o exponerlos a vulnerabilidades.	Los usuarios o administradores pueden cometer errores que comprometan la seguridad.
VUL0037	Exposicion a interferencias electromagneticas (EMI): La exposicion a interferencias electromagneticas puede afectar el rendimiento y la integridad de los dispositivos de hardware. Las senales electromagneticas pueden generar errores en la transmision...	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0038	Exposicion a variaciones de voltaje: Equipos expuestos a variaciones repentinas en el suministro de energia, como picos o bajadas de voltaje, pueden dañarse o funcionar de manera erratica.	La falta de sistemas de alimentacion ininterrumpida (UPS) o fallos en los sistemas de refrigeración puede causar danos a los equipos.

Código	Etiqueta	Descripción
VUL0039	Exposicion de directorios compartidos no seguros: Permitir acceso no controlado a directorios compartidos, lo que expone los datos a usuarios no autorizados.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0040	Exposicion de servicios innecesarios: Servidores con servicios habilitados que no son necesarios, pero accesibles publicamente.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0041	Exposicion innecesaria de servicios de red: Servicios habilitados en la red sin necesidad, lo que aumenta la superficie de ataque.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0042	FTP no cifrado habilitado: El uso de FTP sin cifrado permite la interceptacion de datos durante la transferencia.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0043	Fallas en el sistema de ventilación y refrigeración: Sistemas de ventilación y refrigeración inadecuados que provocan sobrecalentamiento y apagones en los dispositivos.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0044	Fallas en el sistema de ventilación: El fallo en los sistemas de ventilación puede permitir que los equipos se sobrecalienten, lo que podría causar apagones, ralentizacion de los sistemas o danos físicos.	La falta de sistemas de alimentacion ininterrumpida (UPS) o fallos en los sistemas de refrigeración puede causar danos a los equipos.
VUL0045	Fallas en la alimentacion electrica: Dispositivos afectados por cortes de energia o falta de un suministro adecuado.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0046	Fallas en la gestión de energia: Hardware que no gestióna adecuadamente la energia puede ser susceptible a sobrecalentamientos o apagones, lo que puede resultar en perdida de datos o danos físicos.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0047	Fallos en dispositivos de almacenamiento: Dispositivos de almacenamiento que fallan o sufren danos físicos, comprometiendo la integridad de los datos.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.

Código	Etiqueta	Descripción
VUL0048	Falta de Certificaciones de Seguridad (ISO 27001): No certificarse a pesar de la no obligatoriedad en Colombia, expone a la organización a posibles brechas de seguridad y perdida de confianza de clientes.	Falta de cumplimiento con normativas legales o regulaciones especificas del sector.
VUL0049	Falta de Controles de Cumplimiento: La falta de revisión regular de los controles implementados para asegurar el cumplimiento de normativas y políticas de seguridad. Esto puede provocar vulnerabilidades que queden sin detectar.	No se realizan auditorias de seguridad regulares para identificar vulnerabilidades.
VUL0050	Falta de acuerdos de nivel de servicio (SLA) claros: Los proveedores no tienen SLAs detallados o estos no cubren tiempos de respuesta y recuperacion adecuados. Esto expone a la organización a riesgos operacionales si los proveedores no cumplen con las...	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.
VUL0051	Falta de auditoria de accesos a información critica: No se realizan auditorias periodicas para monitorear quien accede a que información, lo que facilita el acceso no autorizado sin deteccion.	No existe una política clara para la asignación y control de permisos a sistemas.
VUL0052	Falta de autenticación en la concesion de direcciones IP (DHCP): Permitir que dispositivos no autorizados reciban direcciones IP sin control.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0053	Falta de autenticación multifactor (MFA): No habilitar autenticación multifactor (MFA) en conexiones sensibles como SSH o RDP.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0054	Falta de automatizacion en la aplicacion de parches: La falta de automatizacion de parcheos, conlleva retrasos en la protección de sistemas frente a vulnerabilidades conocidas.	No se implementan parches de seguridad de manera oportuna, lo que deja expuestos los sistemas a vulnerabilidades conocidas.
VUL0055	Falta de capacitaciones: La falta de capacitacion expone a la organización a riesgos de seguridad por errores humanos.	Los empleados no tienen el conocimiento necesario para operar de manera segura dentro de los sistemas de la organización.
VUL0056	Falta de cierre seguro en áreas de almacenamiento de datos: Los lugares donde se almacenan los datos físicos o los equipos que contienen datos (como discos duros) no estan debidamente asegurados, permitiendo accesos no autorizados.	La falta de controles de acceso físico puede permitir que personas no autorizadas entren en áreas sensibles.

Código	Etiqueta	Descripción
VUL0057	Falta de cifrado en APIs: La comunicacion no cifrada entre las APIs y los sistemas permite ataques de intermediario (MITM).	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0058	Falta de configuración de SSL/TLS adecuada: Configuración incorrecta del cifrado SSL/TLS, lo que permite la interceptacion de datos sensibles.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0059	Falta de control de acceso a documentos físicos sensibles: No asegurar debidamente en gabinetes con llave o zonas restringidas.los documentos físicos importantes, como contratos, registros financieros o secretos comerciales,	No existe una política clara para la asignación y control de permisos a sistemas.
VUL0060	Falta de control de acceso biometrico: No contar con sistemas avanzados de acceso biometrico, como huellas dactilares o reconocimiento facial, para áreas criticas, permite que personas no autorizadas accedan fisicamente a equipos importantes.	La falta de controles de acceso físico puede permitir que personas no autorizadas entren en áreas sensibles.
VUL0061	Falta de control de versiones en APIs: Las versiones antiguas o no seguras de APIs pueden seguir expuestas y permitir ataques debido a la falta de Actualización de la API.	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0062	Falta de controles de seguridad en los proveedores: La falta de controles de seguridad implementados por el provedor aumenta el riesgo de que las vulnerabilidades en sus sistemas o procesos afecten directamente a la organización que depende de ellos.	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0063	Falta de ejercicios y simulacros de respuesta a incidentes: No se realizan pruebas periodicas o simulacros para entrenar al personal en la respuesta a ciberincidentes.	Falta de un procedimiento adecuado para responder a incidentes de seguridad, lo que prolonga el tiempo de recuperacion.
VUL0064	Falta de gestión del ciclo de vida de parches: No contar con un proceso claro para gestionar el ciclo de vida de los parches, desde la Identificación de vulnerabilidades hasta la aplicacion de parches y Actualizaciones.	No se implementan parches de seguridad de manera oportuna, lo que deja expuestos los sistemas a vulnerabilidades conocidas.
VUL0065	Falta de hardening del servidor: No se han aplicado las mejores practicas de seguridad en la configuración del servidor, dejando Configuraciones por defecto vulnerables.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.

Código	Etiqueta	Descripción
VUL0066	Falta de monitoreo adecuado para detectar incidentes: No implementar soluciones de monitoreo adecuadas para detectar incidentes de seguridad en tiempo real. Esto incluye la falta de sistemas de deteccion de intrusiones, alertas automatizadas y...	Falta de un procedimiento adecuado para responder a incidentes de seguridad, lo que prolonga el tiempo de recuperacion.
VUL0067	Falta de políticas de gestión de Actualizaciones y parches: La ausencia de una política clara sobre la aplicacion de parches y Actualizaciones a los sistemas deja los dispositivos vulnerables a ataques que aprovechan fallos conocidos.	Ausencia o inadecuación de políticas claras para la gestión de la seguridad de la información.
VUL0068	Falta de políticas de monitoreo y auditoria: La organización carece de políticas que obliguen a realizar auditorias regulares y monitoreo de accesos a sistemas, lo que permite que las actividades no autorizadas pasen desapercibidas.	Ausencia o inadecuación de políticas claras para la gestión de la seguridad de la información.
VUL0069	Falta de políticas de protección de datos: No existen políticas que regulen como se protegen los datos críticos, como los datos de Identificación de clientes, datos financieros o secretos comerciales. Esto puede llevar a la exposicion de datos sensibles.	Ausencia o inadecuación de políticas claras para la gestión de la seguridad de la información.
VUL0070	Falta de políticas de retencion y restauracion de datos: No existen políticas claras que regulen cuanto tiempo se deben almacenar las copias de seguridad, ni como deben restaurarse en caso de incidentes.	Falta de procedimientos adecuados para respaldar la información de la organización.
VUL0071	Falta de políticas de uso de dispositivos personales (BYOD): No existen políticas que regulen el uso de dispositivos personales (como smartphones o laptops) dentro de la red corporativa, lo que permite el acceso no controlado y aumenta el riesgo de...	Ausencia o inadecuación de políticas claras para la gestión de la seguridad de la información.
VUL0072	Falta de procedimientos para eliminar los derechos de acceso a la terminacion del empleo: La falta de procedimientos adecuados para revocar o eliminar los derechos de acceso a los sistemas cuando un empleado es despedido o termina su relacion laboral...	Los usuarios o administradores pueden cometer errores que comprometan la seguridad.
VUL0073	Falta de procedimientos para la notificacion de incidentes: Carecer de un procedimiento formal para notificar internamente y externamente los incidentes de seguridad.	Falta de un procedimiento adecuado para responder a incidentes de seguridad, lo que prolonga el tiempo de recuperacion.

Código	Etiqueta	Descripción
VUL0074	Falta de redundancia en la cadena de suministro: La dependencia de una infraestructura externa sin una estrategia de redundancia. Si el proveedor sufre una interrupcion, no hay alternativas viables, lo que podría paralizar las operaciones de la empresa.	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.
VUL0075	Falta de respuesta rapida ante incidentes de seguridad del proveedor: Incapacidad para responder ante incidentes de seguridad, al no tener un plan adecuado de respuesta y mitigacion.	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0076	Falta de segmentacion de accesos según roles: Los empleados tienen acceso a información y sistemas mas alla de los necesarios para cumplir con sus funciones, puede exponer información a un mayor riesgo de filtracion o mal uso.	No existe una política clara para la asignación y control de permisos a sistemas.
VUL0077	Falta de segmentacion de red: Redes internas no segmentadas adecuadamente, lo que permite a los atacantes moverse lateralmente, acceso innecesario o no autorizado.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0078	Falta de supervision del estado de los parches: No llevar registro o monitoreo adecuado del estado de los parches aplicados, puede dar lugar a sistemas desprotegidos.	No se implementan parches de seguridad de manera oportuna, lo que deja expuestos los sistemas a vulnerabilidades conocidas.
VUL0079	Falta de un equipo de respuesta a incidentes: No contar con un equipo designado para gestionar y mitigar incidentes de seguridad limita la capacidad de la empresa para controlar y reducir los impactos de los ataques.	Falta de un procedimiento adecuado para responder a incidentes de seguridad, lo que prolonga el tiempo de recuperacion.
VUL0080	Falta de un plan de respuesta a incidentes: No existe un plan estructurado para abordar ciberincidentes, lo que deja a la organización sin una guia clara sobre los pasos a seguir en caso de un ataque.	Falta de un procedimiento adecuado para responder a incidentes de seguridad, lo que prolonga el tiempo de recuperacion.
VUL0081	Falta de validacion de entradas: Permite ataques como la inyeccion SQL o el Cross-Site Scripting (XSS)	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0082	Falta de visibilidad en las operaciones del proveedor: La falta de visibilidad suficiente sobre como el	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.

Código	Etiqueta	Descripción
	proveedor maneja la seguridad, el almacenamiento de datos o las operaciones criticas.	
VUL0083	Firmware desactualizado: Falta de Actualización en el firmware de dispositivos, lo que los deja expuestos a vulnerabilidades conocidas.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0084	Gestión inadecuada de autenticación en servidores de correo: Configuraciones débiles de autenticación que permiten accesos no autorizados a servidores de correo.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0085	Gestión inadecuada de permisos de usuario: Permisos de usuario no gestiónados correctamente, permite a usuarios con privilegios innecesarios acceder a información sensible.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0086	ICMP habilitado innecesariamente: Permitir el uso del protocolo ICMP sin control adecuado permite a los atacantes realizar escaneos y ataques como el "ping flood".	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0087	Inadecuada gestión y protección de contraseñas: La falta de una correcta gestión y protección de contraseñas, incluyendo la ausencia de políticas solidas, reutilizacion de contraseñas o la falta de cifrado, expone los sistemas a ataques.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0088	Incumplimiento de la Ley de Protección de Datos: El incumplimiento con las normativas vigentes en cuanto a la recoleccion, almacenamiento y manejo de datos personales, puede llevar a sanciones legales y perdidas de confianza.	Falta de cumplimiento con normativas legales o regulaciones especificas del sector.
VUL0089	Interrupcion en la cadena de suministro de componentes: La dependencia de componentes de hardware que se vuelven escasos o inaccesibles debido a problemas en la cadena de suministro puede afectar la capacidad de reparar o reemplazar componentes danados.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0090	Interrupcion en la cadena de suministro: Cualquier interrupcion debido a problemas logisticos, fallos del proveedor, desastres naturales, etc. puede afectar directamente las operaciones de la organización.	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.

Código	Etiqueta	Descripción
VUL0091	Inyecciones en APIs: Permite que un atacante envie comandos maliciosos que el sistema procesa erroneamente.	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0092	Manipulacion fisica de dispositivos moviles: Dispositivos moviles como laptops, smartphones o tablets pueden ser robados o manipulados si no estan fisicamente protegidos.	La falta de controles de acceso físico puede permitir que personas no autorizadas entren en áreas sensibles.
VUL0093	Manipulacion fisica no autorizada: La manipulacion no autorizada del hardware puede exponerlo a danos físicos o a la alteracion de componentes sensibles.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0094	No automatizacion del proceso de backup: No contar con una política para la automatizacion de las copias de seguridad, genera que estas dependan de procesos manuales susceptibles a errores o retrasos.	Falta de procedimientos adecuados para respaldar la información de la organización.
VUL0095	No cifrado de las copias de seguridad: Las copias de seguridad no estan cifradas, lo que facilita el acceso no autorizado en caso de que las copias sean robadas o comprometidas.	Falta de procedimientos adecuados para respaldar la información de la organización.
VUL0096	No se Realizan Auditorias Internas: La ausencia de auditorias periodicas dentro de la organización impide detectar desviaciones de las políticas de seguridad, el cumplimiento normativo, y posibles brechas en la seguridad.	No se realizan auditorias de seguridad regulares para identificar vulnerabilidades.
VUL0097	No validacion de los datos procesados: No verificar la precision o integridad de los datos procesados puede llevar a errores en el sistema, lo que afecta la confiabilidad de la información y aumenta el riesgo de decisiones basadas en datos incorrectos.	Los usuarios o administradores pueden cometer errores que comprometan la seguridad.
VUL0098	Obsolescencia de hardware: Dispositivos que ya no reciben soporte o Actualizaciones de seguridad.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0099	Permisos de acceso inadecuados: Usuarios con permisos excesivos o incorrectos, lo que puede llevar a accesos no autorizados.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.

Código	Etiqueta	Descripción
VUL0100	Permitir acceso root sin restricciones (SSH): El acceso root permitido sin una protección adecuada, facilita el control total del sistema a traves de accesos no autorizados.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0101	Permitir almacenamiento de contraseñas en texto plano: Contraseñas no cifradas, exponen las credenciales al robo durante accesos no autorizados.	Uso de contraseñas débiles o reutilizacion de las mismas para distintos sistemas críticos.
VUL0102	Phishing dirigido (Spear Phishing): Tecnica de engano a traves del correo electronico para comprometer la seguridad.	Tecnicas utilizadas por atacantes para enganar a las personas y obtener acceso no autorizado a sistemas o información.
VUL0103	Problemas de conexion y cableado defectuoso: Los cables danados, mal instalados o desconectados pueden causar fallos de comunicacion entre componentes de hardware, como servidores, estaciones de trabajo y dispositivos de red.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0104	Proveedores sin políticas claras de seguridad de la información: El proveedor no tiene políticas solidas para proteger los datos o gestionar la seguridad de la información, lo que puede llevar a filtraciones, manipulaciones o accesos no autorizados a...	Riesgos asociados a que un proveedor sea comprometido, afectando directamente los servicios o productos de la organización.
VUL0105	Pruebas de software insuficientes: Si el software no pasa por suficientes pruebas de seguridad o calidad, pueden pasar por alto vulnerabilidades criticas.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0106	Puertos abiertos innecesarios: Permite el acceso no autorizado o ataques de red.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0107	RDP habilitado en redes inseguras: El protocolo RDP se permite en redes no protegidas, lo que expone el acceso remoto a ataques y secuestro de sesion.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0108	Red Wi-Fi sin cifrado adecuado: Configurar la red wifi sin cifrado WPA2 o WPA3, permite que los atacantes intercepten las comunicaciones.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0109	Relaying abierto: El relaying no controlado permite que el servidor sea utilizado para enviar correos no deseados (spam).	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.

Código	Etiqueta	Descripción
VUL0110	Respuesta ICMP mal configurada: Configuración incorrecta de las respuestas ICMP permite que los atacantes exploren la red en busca de vulnerabilidades.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0111	Retrasos en la entrega de Actualizaciones o parches por parte de terceros: La falta de Actualizaciones de seguridad o parches a tiempo por parte de proveedores hacia la organización, quedaria expuesta a vulnerabilidades de seguridad conocidas que no...	Uso de servicios de terceros o proveedores externos que no siguen los controles de seguridad adecuados.
VUL0112	Routers con Configuraciones inseguras de seguridad: Configuraciones predeterminadas o el no uso de políticas de seguridad adecuadas.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0113	SNMP v1/v2 sin cifrado: Uso de versiones vulnerables del protocolo SNMP que no cifran las comunicaciones.	Configuración insegura de equipos de red, como routers, switches, firewalls o puntos de acceso.
VUL0114	Sensibilidad a condiciones ambientales (temperatura, humedad): Equipos electronicos sensibles a cambios en temperatura o humedad pueden fallar o sufrir danos físicos si las condiciones no se controlan adecuadamente.	La falta de sistemas de alimentacion ininterrumpida (UPS) o fallos en los sistemas de refrigeración puede causar danos a los equipos.
VUL0115	Sensibilidad a condiciones ambientales (temperatura, humedad, contaminantes): Dispositivos vulnerables a danos por exposicion a condiciones ambientales adversas., lo que puede provocar fallos en su funcionamiento.	Problemas físicos o de gestión en los dispositivos y equipos que soportan los sistemas de la organización, incluyendo fallos físicos, incompatibilidades, y falta de Actualizaciones criticas.
VUL0116	Sistemas de monitoreo inadecuados: No contar con suficientes camaras de vigilancia o sensores en áreas criticas, lo que facilita que personas no autorizadas puedan acceder a esas zonas sin ser detectadas.	La falta de controles de acceso físico puede permitir que personas no autorizadas entren en áreas sensibles.
VUL0117	Smishing (SMS Phishing): Tecnica de manipulacion a traves de mensajes de texto.	Tecnicas utilizadas por atacantes para enganar a las personas y obtener acceso no autorizado a sistemas o información.
VUL0118	Sobrecarga de servidores: La falta de refrigeración adecuada provoca sobrecalentamiento de los servidores, lo que puede llevar a fallos de hardware, perdida de datos, o incluso danos permanentes en los dispositivos.	La falta de sistemas de alimentacion ininterrumpida (UPS) o fallos en los sistemas de refrigeración puede causar danos a los equipos.

Código	Etiqueta	Descripción
VUL0119	Software no licenciado: El uso de software sin licencia puede representar un riesgo porque no se actualiza ni se reciben parches oficiales del proveedor.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad
VUL0120	Tasa de limitacion inadecuada (Rate limiting): Las APIs no implementan controles adecuados sobre la frecuencia de las solicitudes, permitiendo ataques de denegacion de servicio (DoS).	Fallas en la protección de interfaces de programación que permiten accesos no autorizados a sistemas internos.
VUL0121	Transferencia de zona DNS no segura: Permitir la transferencia de zonas DNS sin autenticación, exponiendo información critica.	Los sistemas no estan configurados según las mejores practicas de seguridad, lo que deja brechas que los atacantes pueden explotar.
VUL0122	UPS defectuosos o insuficientes: Los sistemas de alimentacion ininterrumpida (UPS) no son suficientes o estan defectuosos, lo que deja los equipos críticos vulnerables a cortes de energia prolongados, provocando la perdida de datos o danos en el hardware.	La falta de sistemas de alimentacion ininterrumpida (UPS) o fallos en los sistemas de refrigeración puede causar danos a los equipos.
VUL0123	Uso indebido de sistemas compartidos: Los sistemas compartidos entre diferentes departamentos o usuarios no cuentan con un control estricto de accesos, permite que usuarios sin privilegios acceder a información sensible.	No existe una política clara para la asignación y control de permisos a sistemas.
VUL0124	Uso indebido de sistemas: La falta de conocimiento sobre las políticas de uso seguro de sistemas abre puertas a ataques o mal uso de los recursos.	Los empleados no tienen el conocimiento necesario para operar de manera segura dentro de los sistemas de la organización.
VUL0125	Vishing: Manipulacion psicologica a traves de llamadas telefonicas para obtener datos o acceso a sistemas.	Tecnicas utilizadas por atacantes para enganar a las personas y obtener acceso no autorizado a sistemas o información.
VUL0126	Vulnerabilidades de dia cero: Software con fallos aun no descubiertos o no parcheados por el proveedor.	Son fallos o errores en el código, procesos de configuración, gestión de dependencias o pruebas de aplicaciones, sistemas operativos o programas, que pueden ser explotados por atacantes para comprometer su seguridad

CATALOGO DE CONTROLES

Referencial aplicado para la metodología propuesta: ISO/IEC 27001 – Anexo A (controles).

Código	Control (label)	Categoría MONARC
A.5.1.1	Políticas para la seguridad de la información	Information security policies
A.5.1.2	Revisión de las Políticas para seguridad de la información	Information security policies
A.6.1.1	Roles y responsabilidades para la seguridad de información	Organization of information security
A.6.1.2	Separacion de deberes	Organization of information security
A.6.1.3	Contacto con las autoridades	Organization of information security
A.6.1.4	Contacto con grupos de interes especial	Organization of information security
A.6.1.5	Seguridad de la información en la gestion de proyectos	Organization of information security
A.6.2.1	Política para dispositivos moviles	Organization of information security
A.6.2.2	Teletrabajo	Organization of information security
A.7.1.1	Seleccion	Human resource security
A.7.1.2	Terminos y condiciones del empleo	Human resource security
A.7.2.1	Responsabilidades de la direccion	Human resource security
A.7.2.2	Toma de conciencia, educacion y formacion en la seguridad de la información	Human resource security
A.7.2.3	Proceso disciplinario	Human resource security
A.7.3.1	Terminacion o cambio de responsabilidades de empleo	Human resource security
A.8.1.1	Inventario de activos	Asset management
A.8.1.2	Propiedad de los activos	Asset management
A.8.1.3	Uso aceptable de los activos	Asset management
A.8.1.4	Devolucion de activos	Asset management
A.8.2.1	Clasificacion de la información	Asset management
A.8.2.2	Etiquetado de la información	Asset management
A.8.2.3	Manejo de activos	Asset management
A.8.3.1	Gestion de medios removibles	Asset management
A.8.3.2	Disposicion de los medios	Asset management
A.8.3.3	Transferencia de medios fisicos	Asset management
A.9.1.1	Política de control de acceso	Access control
A.9.1.2	Política sobre el uso de los servicios de red	Access control
A.9.2.1	Registro y cancelacion del registro de usuarios	Access control
A.9.2.2	Suministro de acceso de usuarios	Access control
A.9.2.3	Gestion de derechos de acceso privilegiado	Access control
A.9.2.4	Gestion de información de autenticacion secreta de usuarios	Access control
A.9.2.5	Revisión de los derechos de acceso de usuarios	Access control
A.9.2.6	Retiro o ajuste de los derechos de acceso	Access control

A.9.3.1	Uso de la información de autenticacion secreta	Access control
A.9.4.1	Restriccion de acceso a la información	Access control
A.9.4.2	Procedimiento de ingreso seguro	Access control
A.9.4.3	Sistema de gestion de contrasenas	Access control
A.9.4.4	Uso de programas utilitarios privilegiados	Access control
A.9.4.5	Control de acceso a codigos fuente de programas	Access control
A.10.1.1	Política sobre el uso de controles criptograficos	Cryptography
A.10.1.2	Gestion de llaves	Cryptography
A.11.1.1	Perimetro de seguridad fisica	Physical and environmental security
A.11.1.2	Controles fisicos de entrada	Physical and environmental security
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Physical and environmental security
A.11.1.4	Protección contra amenazas externas y ambientales	Physical and environmental security
A.11.1.5	Trabajo en areas seguras	Physical and environmental security
A.11.1.6	Areas de despacho y carga	Physical and environmental security
A.11.2.1	Ubicacion y protección de los equipos	Physical and environmental security
A.11.2.2	Servicios de suministro	Physical and environmental security
A.11.2.3	Seguridad del cableado	Physical and environmental security
A.11.2.4	Mantenimiento de equipos	Physical and environmental security
A.11.2.5	Retiro de activos	Physical and environmental security
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Physical and environmental security
A.11.2.7	Disposicion segura o reutilizacion de equipos	Physical and environmental security
A.11.2.8	Equipos de usuario desatendidos	Physical and environmental security
A.11.2.9	Política de escritorio limpio y pantalla limpia	Physical and environmental security
A.12.1.1	Procedimientos de operacion documentados	Operations security
A.12.1.2	Gestion de cambios	Operations security
A.12.1.3	Gestion de capacidad	Operations security
A.12.1.4	Separacion de los ambientes de desarrollo, pruebas y operacion	Operations security
A.12.2.1	Controles contra codigos maliciosos	Operations security
A.12.3.1	Respaldo de información	Operations security
A.12.4.1	Registro de eventos	Operations security
A.12.4.2	Protección de la información de registro	Operations security
A.12.4.3	Registros del administrador y del operador	Operations security
A.12.4.4	Sincronizacion de relojes	Operations security
A.12.5.1	Instalacion de software en sistemas operativos	Operations security
A.12.6.1	Gestion de las vulnerabilidades tecnicas	Operations security
A.12.6.2	Restricciones sobre la instalacion de software	Operations security

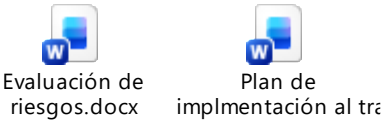
A.12.7.1	Información controles de auditoría de sistemas	Operations security
A.13.1.1	Controles de redes	Communications security
A.13.1.2	Seguridad de los servicios de red	Communications security
A.13.1.3	Separación en las redes	Communications security
A.13.2.1	Políticas y procedimientos de transferencia de información	Communications security
A.13.2.2	Acuerdos sobre transferencia de información	Communications security
A.13.2.3	Mensajería electrónica	Communications security
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	Communications security
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	System acquisition, development and maintenance
A.14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	System acquisition, development and maintenance
A.14.1.3	Protección de transacciones de los servicios de las aplicaciones	System acquisition, development and maintenance
A.14.2.1	Política de desarrollo seguro	System acquisition, development and maintenance
A.14.2.2	Procedimientos de control de cambios en sistemas	System acquisition, development and maintenance
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	System acquisition, development and maintenance
A.14.2.4	Restricciones en los cambios a los paquetes de software	System acquisition, development and maintenance
A.14.2.5	Principios de construcción de sistemas seguros	System acquisition, development and maintenance
A.14.2.6	Ambiente de desarrollo seguro	System acquisition, development and maintenance
A.14.2.7	Desarrollo contratado externamente	System acquisition, development and maintenance
A.14.2.8	Pruebas de seguridad de sistemas	System acquisition, development and maintenance
A.14.2.9	Prueba de aceptación de sistemas	System acquisition, development and maintenance
A.14.3.1	Protección de datos de prueba	System acquisition, development and maintenance
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Supplier relationships
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Supplier relationships
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	Supplier relationships
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	Supplier relationships
A.15.2.2	Gestión de cambios en los servicios de proveedores	Supplier relationships
A.16.1.1	Responsabilidad y procedimientos	Information security incident management

A.16.1.2	Reporte de eventos de seguridad de la información	Information security incident management
A.16.1.3	Reporte de debilidades de seguridad de la información	Information security incident management
A.16.1.4	Evaluacion de eventos de seguridad de la información y decisiones sobre ellos	Information security incident management
A.16.1.5	Respuesta a incidentes de seguridad de la información	Information security incident management
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Information security incident management
A.16.1.7	Recoleccion de evidencia	Information security incident management
A.17.1.1	Planificacion de la continuidad de la seguridad de la información	Information security aspects of business continuity management
A.17.1.2	Implementacion de la continuidad de la seguridad de la información	Information security aspects of business continuity management
A.17.1.3	Verificacion, revisión y evaluacion de la continuidad de la seguridad de la información	Information security aspects of business continuity management
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Information security aspects of business continuity management
A.18.1.1	Identificación de la legislacion aplicable y de los requisitos contractuales	Compliance
A.18.1.2	Derechos de propiedad intelectual	Compliance
A.18.1.3	Protección de registros	Compliance
A.18.1.4	Privacidad y protección de datos personales	Compliance
A.18.1.5	Reglamentacion de controles criptograficos	Compliance
A.18.2.1	Revisión independiente de la seguridad de la información	Compliance
A.18.2.2	Cumplimiento con las Políticas y normas de seguridad	Compliance
A.18.2.3	Revisión del cumplimiento técnico	Compliance

CHECKLIST DE CONSISTENCIA DE CATÁLOGOS FUNCIONALES

Catálogo	Regla	Criterio	Estado	Observación
Amenazas	Campos obligatorios completos	code/label/theme presentes en todas las filas	Cumple	Faltantes: 0
Amenazas	Códigos únicos	code sin duplicados	Cumple	Duplicados: 0
Amenazas	Themes válidos	theme ∈ {6 themes MONARC}	Cumple	Themes usados: Compromise of functions, Compromise of information, Loss of essential services, Physical damage, Technical failures, Unauthorised actions
Amenazas	CID binario	c/i/a en {0,1}	Cumple	Valores inválidos: 0
Vulnerabilidades	Campos obligatorios completos	code/label presentes en todas las filas	Cumple	Faltantes: 0
Vulnerabilidades	Códigos únicos	code sin duplicados	Cumple	Duplicados: 0
Vulnerabilidades	Límite label (255)	label ≤ 255 caracteres	Cumple	Máximo observado: 255
Controles	Campos obligatorios completos	code/label/category presentes en todas las filas	Cumple	Faltantes: 0
Controles	Códigos únicos	code sin duplicados	Cumple	Duplicados: 0
Controles	Categorías definidas	category usada para organización y filtro	Cumple	Categorías distintas: 14

J. Anexo: Soporte entregables validación caso de uso



5. Bibliografía

[1] R. Adriko and J. R. C. Nurse, "Cybersecurity, cyber insurance and small-to-medium-sized enterprises: a systematic Review," *Inf. Comput. Secur.*, vol. 32, no. 5, pp. 691–710, Nov. 2024, doi: 10.1108/ICS-01-2024-0025.

[2] Equipo Editorial Py+, "¿Por qué es importante la ciberseguridad en las pymes?," Pymas. Accessed: May 17, 2025. [Online]. Available: https://www.pymas.com.co/ideas-para-crecer/ayuda-legal/ciberseguridad-pymes-colombia

[3] QBE Singapore, "Less than half of SMEs fully aware of cyber risks, while the number without protection grows, finds QBE Singapore annual SME survey | QBE Singapore," QBE Singapore. Accessed: May 16, 2025. [Online]. Available: https://www.qbe.com/sg/newsroom/press-releases/less-than-half-of-smes-fully-aware-of-cyber-risks

[4] European Union Agency for Cybersecurity., *Cybersecurity for SMEs: challenges and recommendations.* LU: Publications Office, 2021. doi: 10.2824/770352.

[5] A. K. Tetteh, "Cybersecurity needs for SMEs," *Issues in Information Systems*, vol. 25, no. 1, pp. 235–246, 2024, doi: 10.48009/1_iis_2024_120.

[6] INCIBE, "Pasado, presente y futuro de la seguridad de la información," Dec. 05, 2023. Accessed: Dec. 02, 2024. [Online]. Available: https://www.incibe.es/empresas/blog/pasado-presente-y-futuro-de-la-seguridad-de-la-informacion

[7] L. C. Piñón, A. L. Sapién, and M. del C. Gutiérrez, "Capacitación en ciberseguridad en una empresa mexicana," *Inf. Tecnológica*, vol. 34, no. 6, pp. 43–52, Dec. 2023, doi: 10.4067/S0718-07642023000600043.

[8] M. Antunes, M. Maximiano, R. Gomes, and D. Pinto, "Information Security and Cybersecurity Management: A Case Study with SMEs in Portugal," *J. Cybersecurity Priv.*, vol. 1, no. 2, pp. 219–238, Jun. 2021, doi: 10.3390/jcp1020012.

[9] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, Gaithersburg, MD, USA, Cybersecurity White Paper NIST CSWP 29, Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[10] A. Papathanasiou, G. Liontos, A. Katsouras, V. Liagkou, and E. Glavas, "Cybersecurity Guide for SMEs: Protecting Small and Medium-Sized Enterprises in the Digital Era," *J. Inf. Secur.*, vol. 16, no. 01, pp. 1–43, 2025, doi: 10.4236/jis.2025.161001.

[11] "Cybersecurity Standards Scorecard (2023 Edition)," SANS Institute. Accessed: Feb. 25, 2026. [Online]. Available: https://www.sans.org/webcasts/cybersecurity-standards-scorecard-2023-edition

[12] M. Roddie-Fonseca and T. Williams, "2023 Survey: Incident Response," SANS Institute, White paper / Survey report, Sep. 2023. Accessed: May 06, 2026. [Online]. Available: https://www.sans.org/white-papers/2023-survey-event-incident-response

[13] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLoS ONE*, vol. 19, no. 3 March, Mar. 2024, doi: 10.1371/journal.pone.0301183.

[14] "América Latina enfrenta más de 3.1 millones de ataques de malware por día, alerta Kaspersky," /. Accessed: Feb. 25, 2026. [Online]. Available: https://latam.kaspersky.com/about/press-releases/america-latina-enfrenta-mas-de-31-millones-de-ataques-de-malware-por-dia-alerta-kaspersky

[15] Comunicación CCIT, *Evaluación, retos y amenazas a la ciberseguridad*, (Jun. 30, 2021). Accessed: Feb. 25, 2026. [Online Video]. Available: https://www.youtube.com/watch?v=w-facvItbuE

[16] V. Díaz, “Fortaleciendo la Ciberseguridad en Colombia: Educación y Protección Empresarial - CCIT - Cámara Colombiana de Informática y Telecomunicaciones,” *CCIT*, Jun. 28, 2024. Accessed: Aug. 13, 2025. [Online]. Available: https://www.ccit.org.co/articulos-tictac/fortaleciendo-la-ciberseguridad-en-colombia-educacion-y-proteccion-empresarial/?utm_source=chatgpt.com

[17] Cámara Colombiana de Informática y Telecomunicaciones, “Balance de Ciberseguridad 2024: Desafíos y prevención para un entorno digital seguro,” CCIT. Accessed: May 03, 2026. [Online]. Available: https://www.ccit.org.co/noticias/balance-de-ciberseguridad-2024-desafios-y-prevencion-para-un-entorno-digital-seguro/

[18] Cámara Colombiana de Informática y Telecomunicaciones and Policía Nacional de Colombia, “Balance Anual CECIP 2024,” Policía Nacional de Colombia, Balance anual, 2025. Accessed: May 03, 2026. [Online]. Available: https://caivirtual.policia.gov.co/sites/default/files/observatorio/BALANCE%20ANUAL%20CECIP%202024.pdf

[19] TicTac, Cámara Colombiana de Informática y Telecomunicaciones, and Policía Nacional de Colombia, “Tendencias del Cibercrimen en Colombia 2019-2020.” Accessed: May 17, 2025. [Online]. Available: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen-2019-2020.pdf

[20] Lucky Bamidele Benjamin, Ayodeji Enoch Adegbola, Prisca Amajuoyi, Mayokun Daniel Adegbola, and Kudirat Bukola Adeusi, “Digital transformation in SMEs: Identifying cybersecurity risks and developing effective mitigation strategies,” *Glob. J. Eng. Technol. Adv.*, vol. 19, no. 2, pp. 134–153, May 2024, doi: 10.30574/gjeta.2024.19.2.0084.

[21] V. R. Ávila Velásquez, A. S. Velásquez Rodriguez, and E. G. Núñez Barahona, “Factores económicos que inciden en las PYMES de Comayagua, Honduras por apertura del Aeropuerto Internacional Palmerola,” *Econ. Adm. EA*, vol. 15, no. 2, pp. 5–27, Dec. 2023, doi: 10.5377/eya.v15i2.17203.

[22] Instituto Tecnológico Metropolitano (ITM), “Microempresas en Colombia tienen riesgo a la quiebra antes de cumplir cinco años de vida,” ITM. Accessed: Feb. 25, 2026. [Online]. Available: https://www.itm.edu.co/noticias-principales/microempresas-en-colombia-tienen-riesgo-a-la-quiebra-antes-de-cumplir-cinco-anos-de-vida/

[23] J. C. Barrios, “Colombia registró 36.000 millones de intentos de ciberataques en 2024: pymes son las más vulnerables,” Forbes Colombia. Accessed: Feb. 25, 2026. [Online]. Available: https://forbes.co/2025/07/15/negocios/pymes-son-las-mas-vulnerables-en-ciberseguridad/

[24] FortiGuard Labs, “Informe global del panorama de amenazas de Fortinet 2025,” Fortinet, Threat report / Informe de amenazas, 2025. Accessed: Feb. 25, 2026. [Online]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/es_la/threat-landscape-report-2025.pdf

[25] Grupo Nex and Instituto Tecnológico Metropolitano, “Instrumento de recolección de datos del cliente: Diseño, construcción y análisis de resultados de la encuesta para la recolección de los datos del cliente.” Instituto Tecnológico Metropolitano, Medellín, Colombia, 2024.

[26] S. N. Matheu-García, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, “Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices,” *Comput. Stand. Interfaces*, vol. 62, pp. 64–83, Feb. 2019, doi: 10.1016/j.csi.2018.08.003.

[27] A. Alahmari and B. Duncan, “Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence,” in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Dublin, Ireland: IEEE, 2020, pp. 1–5. doi: 10.1109/CyberSA49311.2020.9139638.

[28] K. AL-Dosari and N. Fetais, “Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach,” *Electron. Switz.*, vol. 12, no. 17, Sep. 2023, doi: 10.3390/electronics12173629.

[29] M. Wilson and S. McDonald, “One size does not fit all: exploring the cybersecurity perspectives and engagement preferences of UK-Based small businesses,” *Inf. Secur. J.*, vol. 34, no. 1, pp. 15–49, 2025, doi: 10.1080/19393555.2024.2357310.

[30] Z. Wang, “Digital Transformation and Risk Management for SMEs: A Systematic Review on Available Evidence,” *Adv. Econ. Manag. Polit. Sci.*, vol. 65, no. 1, pp. 209–218, Dec. 2023, doi: 10.54254/2754-1169/65/20231639.

[31] D. R. Calvo and I. Briceño Álvarez, “Metodología didáctica para la enseñanza de creación de catálogos de autoridad de autor en los cursos de catalogación de la Escuela de Bibliotecología y Ciencias de la Información de la Universidad de Costa Rica,” *E-Cienc. Inf.*, vol. 12, no. 2, pp. 59–81, Jul. 2022, doi: 10.15517/eci.v12i2.49440.

[32] M. Durán Acosta, “El impacto de la crisis sanitaria generada por COVID-19 en la finanzas de las Pequeñas y medianas empresas (Pymes) de Hermosillo, Sonora,” *Rev. Investig. Académica Sin Front. Div. Cienc. Económicas Soc.*, no. 34, pp. 1–21, Jan. 2021, doi: 10.46589/RDIASF.VI34.357.

[33] J. Guaña-Moya, “La importancia de la seguridad informática en la educación digital: retos y soluciones,” *RECIMUNDO*, vol. 7, no. 1, pp. 609–616, Feb. 2023, doi: 10.26820/recimundo/7.(1).enero.2023.609-616.

[34] G. R. D. L. C. Rodríguez, R. A. M. Fernández, and A. C. M. D. L. Santos, “Information security in e-commerce based on ISO 27001: A systematic review,” *Innov. Softw.*, vol. 4, no. 1, pp. 219–236, Mar. 2023, doi: 10.48168/innosoft.s11.a79.

[35] W. A. Arpi-Saquipay and O. A. Cajamarca-Criollo, “Análisis de riesgos de seguridad de la información en el proceso de contratación de personal en una Institución de Educación Superior en Ecuador, basado en la Norma ISO 27002 Anexo A dominio 7.,” *MQRInvestigar*, vol. 7, no. 3, pp. 2793–2808, Aug. 2023, doi: 10.56048/mqr20225.7.3.2023.2793-2808.

[36] A. Iliana and C. Gonzaga, “Análisis documental: impacto de la seguridad jurídica antes los delitos informáticos: Documentary analysis: impact of legal security in computer crime,” *LATAM Rev. Latinoam. Cienc. Soc. Humanidades*, vol. 5, no. 4, pp. 2541–2551, Jul. 2024, doi: 10.56712/LATAM.V5I4.2437.

[37] E. A. Nantes, “El método Analytic Hierarchy Process para la toma de decisiones: repaso de la metodología y aplicaciones,” *Investig. Oper.*, vol. 27, no. 46, pp. 54–73, Nov. 2019, doi: 10.13140/RG.2.2.29822.54086.

[38] O. S. B. Pinargote, J. A. A. Chóez, C. D. C. Manrique, and C. R. C. Plúa, “Políticas de seguridad en la infraestructura tecnológica de instituciones de salud mediante un appliance fortinet 80e: Estudio de caso Hospital Básico Jipijapa,” *Rev. Científica Salud BIOSANA*, vol. 4, no. 1, pp. 115–138, Mar. 2024, doi: 10.62305/BIOSANA.V4I1.102.

[39] P. Solana-González, K. H. S. Fontana, and A. A. Vanti, “Prácticas de seguridad de la información contable y su contribución al cumplimiento de requerimientos de gobierno corporativo,” *Rev.*

Gest. Tecnol., vol. 19, no. 2, pp. 149–174, Apr. 2019, doi: 10.20397/2177-6652/2019.v19i2.1531.

[40] R. E. T. Correa, E. A. G. Mori, J. V. Valderrama, and A. C. M. de los Santos, "Implementation of access controls for a professional practice management system," *Innov. Softw.*, vol. 4, no. 1, pp. 37–51, Mar. 2023, doi: 10.48168/innosoft.s11.a80.

[41] Norma Técnica Colombiana, Ed., *Gestión del riesgo. Principios y directrices*, NTC-ISO 31000, Bogotá, Colombia., Feb. 16, 2011. [Online]. Available: https://www.contaduria.gov.co/documents/115223/5709447/NTC-ISO+31000+2018.pdf

[42] G. Purdy, "ISO 31000:2009—Setting a new standard for risk management," *Risk Anal.*, vol. 30, no. 6, pp. 881–886, Jun. 2010, doi: 10.1111/j.1539-6924.2010.01442.x.

[43] International Organization for Standardization, *Risk management -- Guidelines*, ISO 31000:2018, Geneva, Switzerland., 2018.

[44] Instituto Nacional de Ciberseguridad, "Gestión de riesgos. Una guía de aproximación para el empresario," Instituto Nacional de Ciberseguridad, España, Guía, Apr. 2025. Accessed: May 06, 2026. [Online]. Available: https://www.incibe.es/empresas/materiales/gestion-de-riesgos-una-guia-de-aproximacion-para-el-empresario-actualizacion

[45] F. Settembrino, "Riesgos puros frente a riesgos especulativos," *Gerenc. Riesgos Seguros*, no. 46, pp. 9–19, 1994, [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=5596493

[46] The Committee of Sponsoring Organizations of the Treadway Commission (COSO) and World Business Council for Sustainable Development (WBCSD), *Enterprise Risk Management - Applying enterprise risk management toenvironmental, social and governance-related risks*, 2018. Accessed: Nov. 28, 2025. [Online]. Available: https://www.coso.org/_files/ugd/3059fc_671ed4466c0e423b93a9ef3d2e30b786.pdf

[47] ISO, *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*, 2022. [Online]. Available: https://www.iso.org/es/contents/data/standard/08/05/80585.html

[48] International Organization for Standardization and International Electrotechnical Commission, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*, ISO/IEC 27000:2018, Geneva, Switzerland., Feb. 2018. [Online]. Available: https://www.iso.org/standard/73906.html

[49] Centro Criptológico Nacional, "Guía de Seguridad CCN-STIC-401: Glosario y abreviaturas," Centro Criptológico Nacional, Madrid, España, Guía de seguridad CCN-STIC-401, Aug. 2015. [Online]. Available: https://www.ccn-cert.cni.es/comunicacion-eventos/comunicados-ccn-cert/2362-actualizada-la-guia-401-de-glosario-y-abreviaturas-con-1-069-terminos.html

[50] M. N. Aleksandrov, V. A. Vasiliev, and S. V. Aleksandrova, "Implementation of the Risk-based Approach Methodology in Information Security Management Systems," in *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)*, Yaroslavl, Russian Federation: IEEE, Sep. 2021, pp. 137–139. doi: 10.1109/ITQMIS53292.2021.9642767.

[51] National Institute of Standards and Technology, "NIST Special Publication 800-30: Guide for Conducting Risk Assessments," National Institute of Standards and Technology, Gaithersburg, MD, 2012. doi: 10.6028/NIST.SP.800-30r1.

[52] A. S. Cerqueira Junior and C. H. Arima, “Cyber risk management and ISO 27005 applied in organizations: a systematic literature review,” *Rev. Foco*, vol. 16, no. 2, p. e1188, Feb. 2023, doi: 10.54751/revistafoco.v16n2-215.

[53] J. C. Giraldo Mejía, F. A. Vargas Agudelo, M. Mena Rivas, and I. A. Delgado, “Method to Manage the Security of Information Assets,” *RISTI - Rev. Ibérica Sist. E Tecnol. Informação*, vol. E°62, pp. 252–266, 2023.

[54] J. V. Barraza de la Paz, L. A. Rodríguez-Picón, V. Morales-Rocha, and S. V. Torres-Argüelles, “A Systematic Review of Risk Management Methodologies for Complex Organizations in Industry 4.0 and 5.0,” *Systems*, vol. 11, no. 5, May 2023, doi: 10.3390/systems11050218.

[55] NIST, “Managing information security risk :,” National Institute of Standards and Technology, Gaithersburg, MD, 2011. doi: 10.6028/NIST.SP.800-39.

[56] L. A. Giraldo Ríos, “Impacto de la ciberseguridad en los modelos de negocio de las organizaciones,” in *Ciberseguridad en la Frontera Digital: desafíos y oportunidades en los nuevos ecosistemas tecnológicos empresariales*, M. E. Realpe Díaz and G. A. Gómez Rodríguez, Eds., Escuela Superior de Guerra, 2025, pp. 15–42. doi: 10.25062/9786287818002.01.

[57] M. A. Fikri, F. A. Putra, Y. Suryanto, and K. Ramli, “Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency,” *Procedia Comput. Sci.*, Jan. 2019, doi: 10.1016/j.procs.2019.11.234.

[58] S. A. Abdymanapov, M. Muratbekov, S. Altynbek, and A. Barlybayev, “Fuzzy expert system of information security risk assessment on the example of analysis learning management systems,” *IEEE Access*, vol. 9, pp. 156556–156565, 2021, doi: 10.1109/access.2021.3129488.

[59] A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, “Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors,” *Risk Anal.*, vol. 43, no. 10, pp. 2082–2098, Oct. 2023, doi: 10.1111/risa.14092.

[60] S. Armenia, M. Angelini, F. Nonino, G. Palombi, and M. F. Schlitzer, “A dynamic simulation approach to support the evaluation of cyber risks and security investments in SMEs,” *Decis. Support Syst.*, vol. 147, p. 113580, Aug. 2021, doi: 10.1016/J.DSS.2021.113580.

[61] M. Benz and D. Chatterjee, “Calculated risk? A cybersecurity evaluation tool for SMEs,” *Bus. Horiz.*, vol. 63, no. 4, pp. 531–540, Jul. 2020, doi: 10.1016/j.bushor.2020.03.010.

[62] M. Brunner, C. Sauerwein, M. Felderer, and R. Breu, “Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region,” *Comput Secur*, vol. 92, p. 101776, Mar. 2020, doi: 10.1016/j.cose.2020.101776.

[63] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, “Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations,” *Sensors*, vol. 23, no. 15, p. 6666, Jul. 2023, doi: 10.3390/s23156666.

[64] R. Riesco and V. Villagrá, “Leveraging cyber threat intelligence for a dynamic risk framework,” *Int. J. Inf. Secur.*, vol. 18, pp. 715–739, Apr. 2019, doi: 10.1007/s10207-019-00433-2.

[65] M. Antunes, M. Maximiano, and R. Gomes, “A client-centered information security and cybersecurity auditing framework,” *Appl. Sci.*, vol. 12, no. 9, p. 4102, Apr. 2022, doi: 10.3390/app12094102.

[66] I. Lee, “Cybersecurity: Risk management framework and investment cost analysis,” *Bus. Horiz.*, vol. 64, no. 5, pp. 659–671, Sep. 2021, doi: 10.1016/j.bushor.2021.02.022.

[67] S. Saeed, S. Suayyid, M. S. Al-Ghamdi, H. Al-Muhaisen, and A. M. Almuhaideb, “A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience,” *Sensors*, vol. 23, no. 16, p. 7273, Aug. 2023, doi: 10.3390/s23167273.

[68] A. Ghadge, M. Weib, N. Caldwell, and R. L. Wilding, “Managing cyber risk in supply chains: A review and research agenda,” *Supply Chain Manag. Int. J.*, vol. 25, no. 2, pp. 223–240, 2020, doi: 10.2139/ssrn.3426030.

[69] M. van Haastrecht *et al.*, “A shared cyber threat intelligence solution for smes,” *Electron. Switz.*, vol. 10, no. 23, Dec. 2021, doi: 10.3390/electronics10232913.

[70] P. Tubío Figueira, C. López Bravo, and J. L. Rivas López, “Improving information security risk analysis by including threat-occurrence predictive models,” *Comput. Secur.*, vol. 88, Jan. 2020, doi: 10.1016/j.cose.2019.101609.

[71] G. Culot, G. Nassimbeni, M. Podrecca, and M. Sartor, “The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda,” *TQM J.*, vol. 33, no. 7, pp. 76–105, 2021, doi: 10.1108/tqm-09-2020-0202.

[72] E. K. Parsons, E. Panaousis, G. Loukas, and G. Sakellari, “A survey on cyber risk management for the Internet of Things,” *Appl. Sci.*, vol. 13, no. 15, p. 9032, Aug. 2023, doi: 10.3390/app13159032.

[73] S. Andersson, E. Bergström, M. Lundgren, K. Bernsmed, and G. Bour, “Information security risk management tools in the air traffic management domain: what are practitioners’ needs?,” *Inf. Secur. J. Glob. Perspect.*, vol. 34, no. 6, pp. 561–578, 2025, doi: 10.1080/19393555.2025.2498472.

[74] S. Phillips, S. Taylor, M. Boniface, S. Modafferi, and M. Surridge, “Automated Knowledge-Based Cybersecurity Risk Assessment of Cyber-Physical Systems,” *IEEE Access*, vol. 12, pp. 82482–82505, 2024, doi: 10.1109/access.2024.3404264.

[75] T. Tam, A. Rao, and J. Hall, “The good, the bad and the missing: A narrative review of cyber-security implications for Australian small businesses,” *Comput. Secur.*, vol. 109, Oct. 2021, doi: 10.1016/j.cose.2021.102385.

[76] R. Alonso, R. Haber, F. Castaño, and D. R. Recupero, “Interoperable software platforms for introducing artificial intelligence components in manufacturing: A meta-framework for security and privacy,” *Heliyon*, vol. 10, Feb. 2024, doi: 10.1016/j.heliyon.2024.e26446.

[77] M. Beyrouti, A. Lounis, B. Lussier, A. Bouabdallah, and A. Samhat, “Vulnerability-oriented risk identification framework for IoT risk assessment,” *Internet Things*, vol. 27, p. 101333, Oct. 2024, doi: 10.1016/j.iot.2024.101333.

[78] M. Al-Abdullah, A. Yayla, and M. S. Al-Atoum, “Teaching case combining standards to conduct risk assessment at SecureEnd Solutions,” *J. Inf. Syst. Educ.*, vol. 35, no. 4, pp. 461–466, Nov. 2024, doi: 10.62273/swqx4831.

[79] F. Kitsios, E. Chatzidimitriou, and M. Kamariotou, “The ISO/IEC 27001 information security management standard: How to extract value from data in the IT sector,” *Sustainability*, vol. 15, no. 7, p. 5828, Mar. 2023, doi: 10.3390/su15075828.

[80] N. A. Chandra, K. Ramli, A. A. P. Ratna, and T. S. Gunawan, “Information security risk assessment using situational awareness frameworks and application tools,” *Risks*, vol. 10, no. 8, p. 165, Aug. 2022, doi: 10.3390/risks10080165.

[81] I. Sánchez-García, T. Feliu, and J. Calvo-Manzano, “Building a cyber risk treatment taxonomy,” *Clust Comput*, vol. 28, p. 205, Jan. 2025, doi: 10.1007/s10586-024-04899-1.

[82] L. Gordon, M. Loeb, and L. Zhou, “Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model,” *J. Cybersecurity*, vol. 6, no. 1, Mar. 2020, doi: 10.1093/cybsec/tyaa005.

[83] T. D. Le, T. Le-Dinh, and S. Uwizeyemungu, “Search engine optimization poisoning: A cybersecurity threat analysis and mitigation strategies for small and medium-sized enterprises,” *Technol. Soc.*, vol. 76, p. 102470, Mar. 2024, doi: 10.1016/j.techsoc.2024.102470.

[84] S. M. Toapanta Toapanta, Y. J. T. Terán Terranova, B. A. Naranjo Sánchez, and L. E. Mafla Gallegos, “Security and privacy in information management in a distributed environment for public organizations,” in *Fuzzy Systems and Data Mining VI*, in Frontiers in Artificial Intelligence and Applications, vol. 331. Virtual, Online, China: IOS Press BV, 2020, pp. 378–389. doi: 10.3233/faia200716.

[85] L. Villafuerte Clavijo and B. Oviedo Bayas, “Vulnerability of the technological infrastructure of the Salinas Fire Department, year 2023,” *Rev. Tecnológica Cienc. Educ. Edw. Deming*, vol. 8, no. 2, pp. 10–31, Jun. 2024, doi: 10.37957/rfd.v8i2.131.

[86] D. L. Andrade Talero, “Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en magerit v3.,” Monografía de especialización, Universidad Nacional Abierta y A Distancia - UNAD, Colombia, 2021. Accessed: Dec. 16, 2024. [Online]. Available: https://repository.unad.edu.co/handle/10596/43373

[87] P. Impulso de la Administración Electrónica, “Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método,” Madrid, España, 2012. [Online]. Available: https://administracionelectronica.gob.es/pae_Home/dam/jcr:fb373672-f804-4d05-8567-2d44b3020387/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf

[88] I. Mugarza, I. Yarza, I. Agirre, F. Lussiana, and S. Botta, “Safety and Security Concept for Software Updates on Mixed-criticality Systems,” in *2021 5th International Conference on System Reliability and Safety (ICSRS)*, Nov. 2021, pp. 171–180. doi: 10.1109/icsrs53853.2021.9660658.

[89] A. Brezavšček and A. Baggia, “Recent trends in information and cyber security maturity assessment: A systematic literature review,” *Systems*, vol. 13, no. 1, p. 52, Jan. 2025, doi: 10.3390/systems13010052.

[90] R. A. Caralli, J. F. Stevens, L. R. Young, and W. R. Wilson, “Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process,” 2007. [Online]. Available: http://www.sei.cmu.edu/publications/pubweb.html

[91] C. Woody, “Applying OCTAVE: Practitioners Report,” Carnegie Mellon University, May 2006. [Online]. Available: https://www.sei.cmu.edu/documents/2102/2006_004_001_14675.pdf

[92] A. Awad, M. Shokry, A. Khalaf, and M. Abd-Ellah, “Assessment of potential security risks in advanced metering infrastructure using the OCTAVE Allegro approach,” *Comput Electr Eng*, vol. 108, p. 108667, May 2023, doi: 10.1016/j.compeleceng.2023.108667.

[93] C. R. Junior, I. Becker, and S. Johnson, “Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity,” Sep. 2023, [Online]. Available: http://arxiv.org/abs/2309.17186

[94] Y. Valdés-Rodríguez, J. Hochstetter-Diez, M. Diéguez-Rebolledo, A. Bustamante-Mora, and R. Cadena-Martínez, "Analysis of Strategies for the Integration of Security Practices in Agile Software Development: A Sustainable SME Approach," *IEEE Access*, vol. 12, pp. 35204–35230, 2024, doi: 10.1109/access.2024.3372385.

[95] T. R. Mcintosh *et al.*, "From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models," *Comput. Secur.*, vol. 144, p. 103964, Sep. 2024, doi: 10.1016/j.cose.2024.103964.

[96] M. Van Haastrecht, B. Y. Ozkan, M. Brinkhuis, and M. Spruit, "Respite for smes: A systematic review of socio-technical cybersecurity metrics," *Appl. Sci. Switz.*, vol. 11, no. 15, Aug. 2021, doi: 10.3390/app11156909.

[97] H. J. Hadi, N. Ahmad, K. Aziz, Y. Cao, and M. Alshara, "Cost-Effective Resilience: A Comprehensive Survey and Tutorial on Assessing Open-Source Cybersecurity Tools for Multi-Tiered Defense," *IEEE Access*, vol. 12, pp. 194053–194076, 2024, doi: 10.1109/access.2024.3510533.

[98] S. A. Akhavani, B. Ousat, and A. Kharraz, "Open Source, Open Threats? Investigating Security Challenges in Open-Source Software," *ArXiv*, vol. abs/2506.12995, Jun. 2025, doi: 10.48550/arxiv.2506.12995.

[99] A. Agbeyangi and H. Suleman, "Advances and challenges in low-resource-environment software systems: A survey," *Informatics*, vol. 11, no. 4, p. 90, Nov. 2024, doi: 10.3390/informatics11040090.

[100] D. A. Almeida, G. C. Murphy, G. Wilson, and M. Hoye, "Investigating whether and how software developers understand open source software licensing," *Empir. Softw. Eng.*, vol. 24, no. 1, pp. 211–239, Feb. 2019, doi: 10.1007/s10664-018-9614-9.

[101] D. Cruz, J. R. Almeida, and J. Oliveira, "Open Source Solutions for Vulnerability Assessment: A Comparative Analysis," *IEEE Access*, vol. 11, pp. 100234–100255, 2023, doi: 10.1109/access.2023.3315595.

[102] J. Rodriguez, "The 7 Best Free and Open Source Risk Management Software," The 7 Best Free and Open Source Risk Management Software. Accessed: May 24, 2024. [Online]. Available: https://www.goodfirms.co/risk-management-software/blog/best-free-open-source-risk-management-software

[103] P. Pritika, B. Shanmugam, and S. Azam, "Risk assessment of heterogeneous IoMT devices: A review," *Technologies*, vol. 11, no. 1, p. 31, Feb. 2023, doi: 10.3390/technologies11010031.

[104] M. El-Hajj and Z. A. Mirza, "Protecting Small and Medium Enterprises: A Specialized Cybersecurity Risk Assessment Framework and Tool," *Electronics*, vol. 13, no. 19, p. 3910, Oct. 2024, doi: 10.3390/electronics13193910.

[105] A. Setiawan, A. Mufti, F. A. Mau, A. Purkoni, and A. Setiawan, "Bridging cybersecurity and enterprise risk management in the digital era," *TechComp Innov. J. Comput. Sci. Technol.*, vol. 2, no. 1, pp. 28–38, 2025, doi: 10.70063/techcompinnovations.v2i1.66.

[106] M. I. Khan, S. Tanwar, and A. Rana, "The need for information security management for SMEs," in *Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020*, Institute of Electrical and Electronics Engineers Inc., Dec. 2020, pp. 328–332. doi: 10.1109/SMART50582.2020.9337108.

[107] R. A. Khan, S. Khan, H. U. Khan, and M. Ilyas, "Systematic Literature Review on Security Risks and its Practices in Secure Software Development," *IEEE Access*, vol. 10, pp. 5456–5481, 2022, doi: 10.1109/access.2022.3140181.

[108] S. A. Ahmad and P.-C. Teo, “The implementation of enterprise risk management (ERM) frameworks in small and medium enterprises (SMEs): A literature review,” *Int. J. Acad. Res. Bus. Soc. Sci.*, vol. 14, no. 9, pp. 290–307, Sep. 2024, doi: 10.6007/ijarbss/v14-i9/22353.

[109] A. A. Alahmari and R. A. Duncan, “Investigating potential barriers to cybersecurity risk management investment in SMEs,” in *2021 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Pitesti, Romania: IEEE, Jul. 2021, pp. 1–6. doi: 10.1109/ECAI52376.2021.9515166.

[110] A. A. Alahmari and R. A. Duncan, “Towards Cybersecurity Risk Management Investment: A Proposed Encouragement Factors Framework for SMEs,” in *2021 IEEE International Conference on Computing, ICOCO 2021*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 115–121. doi: 10.1109/ICOCO53166.2021.9673554.

[111] J. A. Calvo-Manzano, T. San Feliu, Á. Herranz, J. Mariño, L. Fredlund, and A. M. Moreno, “CyberESP: An Integrated Cybersecurity Framework for SMEs,” *J. Softw. Evol. Process*, vol. 37, no. 9, p. e70050, Sep. 2025, doi: 10.1002/smr.70050.

[112] H. Kure, S. Islam, and H. Mouratidis, “An integrated cyber security risk management framework and risk predication for the critical infrastructure protection,” *Neural Comput. Appl.*, vol. 34, pp. 15241–15271, Feb. 2022, doi: 10.1007/s00521-022-06959-2.

[113] T. Herath, H. Herath, and D. Cullum, “An Information Security Performance Measurement Tool for Senior Managers: Balanced Scorecard Integration for Security Governance and Control Frameworks,” *Inf. Syst. Front.*, vol. 25, pp. 681–721, Feb. 2022, doi: 10.1007/s10796-022-10246-9.

[114] D. Dhinakaran, S. Edwin Raja, A. Ramathilagam, G. Vennila, and A. Alagulakshmi, “Ethical and legal challenges with IoT in home digital twins,” *MethodsX*, vol. 14, p. 103409, Jun. 2025, doi: 10.1016/j.mex.2025.103409.

[115] M. M. Kshetri, N. A. Sayeed, and S. A. Rana, “AssessITS: Integrating Procedural Guidelines and Practical Evaluation Metrics for Organizational IT and Cybersecurity Risk Assessment AssessITS: Integrating Procedural Guidelines and Practical Evaluation Metrics for Organizational IT and Cybersecurity Risk,” *J. Inf. Secur.*, vol. 15, pp. 564–588, 2024, doi: 10.4236/jis.2024.154032.

[116] A. Ključnikov, L. Mura, and D. Sklenár, “Information security management in smes: Factors of success,” *Entrep. Sustain. Issues*, vol. 6, no. 4, pp. 2081–2094, Jun. 2019, doi: 10.9770/jesi.2019.6.4(37).

[117] Yu. V. Trifonov and E. A. Fomina, “Development of Risk Assessment Tools for Enterprises,” *Issues Risk Anal.*, vol. 18, no. 5, pp. 38–47, Oct. 2021, doi: 10.32686/1812-5220-2021-18-5-38-47.

[118] S. M. Ali, A. Razzaque, M. Yousaf, and R. Shan, “An Automated Compliance Framework for Critical Infrastructure Security Through Artificial Intelligence,” *IEEE Access*, vol. 13, pp. 4436–4459, 2025, doi: 10.1109/access.2024.3524496.

[119] A. Alfaadhel, I. Almomani, and M. Ahmed, “Risk-Based Cybersecurity Compliance Assessment System (RC2AS),” *Appl. Sci.*, vol. 13, no. 10, p. 6145, 2023, doi: 10.3390/app13106145.

[120] Š. Grigaliūnas, M. Schmidt, R. Brūzgienė, P. Smyrli, S. Andreou, and A. Lopata, “Holistic Information Security Management and Compliance Framework,” *Electron. Switz.*, vol. 13, no. 19, Oct. 2024, doi: 10.3390/electronics13193955.

[121] R. S. Putrus, “A risk-based management approach to third-party data security, risk and compliance,” *ISACA J.*, vol. 6, pp. 36–41, 2017, [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/a-riskbased-management-approach-to-thirdparty-data-security-risk-and-compliance

[122] B. Valkenburg and I. Bongiovanni, “Unravelling the three lines model in cybersecurity: a systematic literature review,” *Comput Secur*, vol. 139, p. 103708, Apr. 2024, doi: 10.1016/j.cose.2024.103708.

[123] P. Cheimonidis and K. Rantos, “Dynamic Risk Assessment in Cybersecurity: A Systematic Literature Review,” *Future Internet*, vol. 15, p. 324, Sep. 2023, doi: 10.3390/fi15100324.

[124] T. E. Belay, S. Gupta, and E. Burisa, “Perform scanning and comparison of open source web application testing tools: Using strategic holistic approach,” *J. Posthumanism*, vol. 5, no. 2, pp. 1377–1402, Apr. 2025, doi: 10.63332/joph.v5i2.512.

[125] J. Ruohonen, G. Choudhary, and A. Alami, “An Overview of Cyber Security Funding for Open Source Software,” *ArXiv*, vol. abs/2412.05887, Dec. 2024, doi: 10.48550/arxiv.2412.05887.

[126] J. Ayala, Y.-J. Tung, and J. Garcia, “A Mixed-Methods Study of Open-Source Software Maintainers On Vulnerability Management and Platform Security Features,” *ArXiv*, vol. abs/2409.07669, Sep. 2024, doi: 10.48550/arxiv.2409.07669.

[127] R. N. Rajapakse, M. Zahedi, M. A. Babar, and H. Shen, “Challenges and solutions when adopting DevSecOps: A systematic review,” *Inf. Softw. Technol.*, vol. 141, p. 106700, Jan. 2022, doi: 10.1016/j.infsof.2021.106700.

[128] S. Elder *et al.*, “Do I really need all this work to find vulnerabilities?,” *Empir. Softw. Eng.*, vol. 27, no. 6, p. 154, Aug. 2022, doi: 10.1007/s10664-022-10179-6.

[129] CCN-CERT, “Nuevo portal de PILAR, la solución de análisis y getión de riesgos del CCN,” Comunicados CCN-CERT. Accessed: Jul. 01, 2024. [Online]. Available: https://www.ccn-cert.cni.es/es/comunicacion-eventos/comunicados-ccn-cert/10388-nuevo-portal-de-pilar-la-solucion-de-analisis-y-gestion-de-riesgos-del-ccn.html

[130] SimpleRisk, “SimpleRisk.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.simplerisk.com/solutions/risk-management

[131] Á. Moreno Ontoria, “Estudio de herramientas de análisis y gestión de riesgos y propuesta de mejora de la herramienta PILAR,” Trabajo Fin de Grado, Universidad de Valladolid, Valladolid, España, 2019. [Online]. Available: http://uvadoc.uva.es/handle/10324/41310

[132] Centro Criptológico Nacional, “PILAR - Análisis y Gestión de Riesgos - Ayuda,” Centro Criptológico Nacional, Madrid, España, Manual de usuario / Ayuda, 2024. [Online]. Available: https://www.pilar-tools.com/doc/help_basic_es_e_20241.pdf

[133] MAGERIT, “Metodología de PILAR.” Accessed: Dec. 20, 2024. [Online]. Available: https://pilar.ccn-cert.cni.es/metodologia/implementacion

[134] Eramba, “Risk Management.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.eramba.org/learning/courses/8/episodes/109

[135] NC3-LU, “MONARC - Documentation.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.monarc.lu/documentation/

[136] MONARC - Method for an Optimised aNAlysis of Risks by @NC3-LU, “MonarcAppFO,” github. Accessed: Jan. 05, 2025. [Online]. Available: https://github.com/monarc-project/MonarcAppFO

[137] J. Sokol, “Documentation - SimpleRisk.” Accessed: Jan. 05, 2025. [Online]. Available: https://github.com/simplerisk/documentation

[138] "Simplerisk Core – Software Panama." Accessed: Feb. 24, 2026. [Online]. Available: https://software.com.pa/produto/simplerisk-core/
[139] "SimpleRisk Pricing," SimpleRisk GRC Software. Accessed: Feb. 24, 2026. [Online]. Available: https://www.simplerisk.com/pricing
[140] "Risk Assessment Extra," SimpleRisk GRC Software. Accessed: Feb. 24, 2026. [Online]. Available: https://www.simplerisk.com/products/extras/risk-assessment
[141] SimpleRisk, "SimpleRisk Company Overview," 2026. [Online]. Available: https://simplerisk-downloads.s3.amazonaws.com/public/overview/simplerisk-overview.pdf
[142] J. Sokol, "How to use SimpleRisk as your foundation for NIST cybersecurity compliance," SimpleRisk. Accessed: May 06, 2026. [Online]. Available: https://www.simplerisk.com/blog/simplerisk-nist-cybersecurity-framework-mapping
[143] SimpleRisk, "How to Conduct a Proper Cybersecurity Risk Analysis," SimpleRisk. Accessed: May 06, 2026. [Online]. Available: https://www.simplerisk.com/blog/proper-cybersecurity-risk-analysis
[144] SimpleRisk, "Mitigation Details - SimpleRisk Support," SimpleRisk Support. Accessed: May 02, 2026. [Online]. Available: https://simplerisk.freshdesk.com/support/login
[145] SimpleRisk, "Review Regularly - SimpleRisk Support," SimpleRisk Support. Accessed: May 03, 2026. [Online]. Available: https://simplerisk.freshdesk.com/support/login
[146] SimpleRisk, "Review Details - SimpleRisk Support," SimpleRisk Support. Accessed: May 02, 2026. [Online]. Available: https://simplerisk.freshdesk.com/support/login
[147] Pirani, "Gestión de Seguridad de la Información," Pirani. Accessed: May 06, 2026. [Online]. Available: https://www.piranirisk.com/es/producto/pirani-isms
[148] N. Molina, "¿Qué es Pirani?" Accessed: Feb. 24, 2026. [Online]. Available: https://www.piranirisk.com/es/blog/que-es-pirani
[149] Pirani Risk, "Guía básica para usar un software de gestión de riesgos." Accessed: Feb. 24, 2026. [Online]. Available: https://www.piranirisk.com/es/academia/especiales/guia-para-usar-un-software-de-gestion-de-riesgos
[150] M. M. Jiménez, "10 métodos de análisis de riesgos," piranirisk. Accessed: Dec. 15, 2024. [Online]. Available: https://www.piranirisk.com/es/blog/10-metodos-de-analisis-de-riesgos
[151] D. R. Chittibala, "Advancements in automated code scanning techniques for detecting security vulnerabilities in open source software," *Int. J. Comput. Eng.*, vol. 5, no. 2, pp. 16–25, Mar. 2024, doi: 10.47941/ijce.1737.
[152] J. P. Seara and C. Serrão, "Automation of system security vulnerabilities detection using open-source software," *Electronics*, vol. 13, no. 5, p. 873, Feb. 2024, doi: 10.3390/electronics13050873.
[153] S. Islam, N. Basheer, S. Papastergiou, M. Ciampi, and S. Silvestri, "Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure," *J. Reliab. Intell. Environ.*, vol. 11, Jul. 2025, doi: 10.1007/s40860-025-00253-3.
[154] M. A. Hussein and E. K. Hamza, "Secure mechanism applied to big data for IIoT by using Security Event and Information Management System (SIEM)," *Int. J. Intell. Eng. Syst.*, vol. 15, no. 6, pp. 667–681, Dec. 2022, doi: 10.22266/ijies2022.1231.59.

[155] X. Li, S. Moreschini, Z. Zhang, and D. Taibi, “Exploring factors and metrics to select open source software components for integration: An empirical study,” *J Syst Softw*, vol. 188, p. 111255, Feb. 2021, doi: 10.1016/j.jss.2022.111255.
[156] C. Crovini, G. Ossola, and B. Britzelmaier, “How to reconsider risk management in SMEs? An advanced, reasoned and organised literature review,” *Eur. Manag. J.*, vol. 39, no. 1, pp. 118–134, 2021, doi: 10.1016/j.emj.2020.11.002.
[157] S. Xu, Y. Gao, L. Fan, Z. Liu, Y. Liu, and H. Ji, “LiDetector: License Incompatibility Detection for Open Source Software,” Apr. 22, 2022, *arXiv*: arXiv:2204.10502. doi: 10.48550/arXiv.2204.10502.
[158] “GNU Affero General Public License - GNU Project - Free Software Foundation.” Accessed: Dec. 25, 2025. [Online]. Available: https://www.gnu.org/licenses/agpl-3.0.html
[159] “Mozilla Public License 2.0,” Open Source Initiative. Accessed: Dec. 25, 2025. [Online]. Available: https://opensource.org/license/MPL-2.0/
[160] “Mozilla Public License, version 2.0.” Accessed: Dec. 25, 2025. [Online]. Available: https://www.mozilla.org/en-US/MPL/2.0/
[161] “Licenses,” Open Source Initiative. Accessed: Dec. 25, 2025. [Online]. Available: https://opensource.org/licenses/
[162] T. Maryka, D. M. German, and G. Poo-Caamaño, “On the Variability of the BSD and MIT Licenses,” in *Open Source Systems: Adoption and Impact*, E. Damiani, F. Frati, D. Riehle, and A. I. Wasserman, Eds., Cham: Springer International Publishing, 2015, pp. 146–156. doi: 10.1007/978-3-319-17837-0_14.
[163] “Apache License, Version 2.0 | Apache Software Foundations.” Accessed: Dec. 25, 2025. [Online]. Available: https://www.apache.org/licenses/LICENSE-2.0
[164] “SPDX License List | Software Package Data Exchange (SPDX).” Accessed: Dec. 25, 2025. [Online]. Available: https://spdx.org/licenses/
[165] G. Gonzalez Granadillo *et al.*, “Automated Cyber and Privacy Risk Management Toolkit,” *Sensors*, vol. 21, no. 16, p. 5493, Aug. 2021, doi: 10.3390/s21165493.
[166] N. A. Krüger and N. Meyer, “The Development of a Small and Medium-Sized Business Risk Management Intervention Tool,” *J. Risk Financ. Manag.*, vol. 14, no. 7, Jul. 2021, doi: 10.3390/jrfm14070310.
[167] E. Ratter, M. Kalbarczyk, and K. Pietrzyk-Wiszowaty, “The utilization of lean management tools in the application of risk management methods according to ISO 31000:2018,” *Eur. Res. Stud. J.*, vol. 27, no. 1, pp. 65–81, Feb. 2024, doi: 10.35808/ersj/3349.
[168] W. G. Alheadary, “Towards Development of a Security Risk Assessment Model for Saudi Arabian Business Environment Based on the ISO/IEC 27005 ISRM Standard,” *J. Inf. Secur.*, vol. 14, no. 03, pp. 195–211, 2023, doi: 10.4236/jis.2023.143012.
[169] B. Barafort, A. L. Mesquida, and A. Mas, “ISO 31000-based integrated risk management process assessment model for IT organizations,” *J. Softw. Evol. Process*, vol. 31, no. 1, p. e1984, 2019, doi: 10.1002/smr.1984.
[170] A. A. Ganin *et al.*, “Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management,” *Risk Anal.*, vol. 40, no. 1, pp. 183–199, Jan. 2020, doi: 10.1111/risa.12891.
[171] G. Cascavilla, D. Tamburri, and W. Heuvel, “Cybercrime threat intelligence: A systematic multi-vocal literature review,” *Comput Secur*, vol. 105, p. 102258, Jun. 2021, doi: 10.1016/j.cose.2021.102258.

[172] R. W. Saaty, “The analytic hierarchy process-what it is and how it is used,” *Math. Model.*, vol. 9, no. 3–5, pp. 161–176, 1987, doi: /10.1016/0270-0255(87)90473-8.
[173] K. J. Aladayleh and M. J. Aladaileh, “Applying Analytical Hierarchy Process (AHP) to BIM-Based Risk Management for Optimal Performance in Construction Projects,” *Buildings*, vol. 14, no. 11, p. 3632, Nov. 2024, doi: 10.3390/buildings14113632.
[174] M. T. Arévalo Cuadrado, “Aplicación del método multicriterio proceso de análisis jerárquico (AHP) para la priorización de la inversión en los proyectos de la Escuela Superior Politécnica de Chimborazo,” Project investigation, Escuela Superior Politécnica de Chimborazo, Riobamba, Ecuador, 2021. [Online]. Available: https://dspace.espoch.edu.ec/items/5a4a9cdb-2b20-4fa5-bb44-51a3422661a6
[175] “7 SMB Cybersecurity Statistics for 2025 | NinjaOne.” Accessed: May 17, 2025. [Online]. Available: https://www.ninjaone.com/blog/smb-cybersecurity-statistics/
[176] A. Abdelmagid and R. Diaz, “Zero Trust Architecture as a risk countermeasure in small–medium enterprises and advanced technology systems,” *Risk Anal.*, vol. 45, no. 8, p. 2390, 2025, doi: 10.1111/risa.70026.
[177] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, “Cost benefits of using machine learning features in NIDS for cyber security in UK small medium enterprises (SME),” *Future Internet*, vol. 13, no. 8, Aug. 2021, doi: 10.3390/fi13080186.
[178] F. Alzahrani, “Evaluating the Usable-Security of Healthcare Software Through Unified Technique of Fuzzy Logic, ANP and TOPSIS,” *IEEE Access*, vol. 8, pp. 109905–109916, Jan. 2020, doi: 10.1109/access.2020.3001996.
[179] A. Afrasiabi, M. Tavana, and D. Di Caprio, “An extended hybrid fuzzy multi-criteria decision model for sustainable and resilient supplier selection,” *Environ. Sci. Pollut. Res. Int.*, vol. 29, pp. 37291–37314, Jan. 2022, doi: 10.1007/s11356-021-17851-2.
[180] J. A. Alarcon, “Risk management model for information security,” *Decis. Rev.*, vol. 3, pp. 1–6, May 2023, doi: 10.47909/dtr.05.
[181] A. Darko, A. Chan, E. Ameyaw, E. Owusu, E. Pärn, and D. Edwards, “Review of application of analytic hierarchy process (AHP) in construction,” *Int. J. Constr. Manag.*, vol. 19, pp. 436–452, Sep. 2019, doi: 10.1080/15623599.2018.1452098.
[182] A. Petrillo, V. A. P. Salomon, and C. L. Tramarico, “State-of-the-art review on the Analytic Hierarchy Process with benefits, opportunities, costs, and risks,” *J. Risk Financ. Manag.*, vol. 16, no. 8, p. 372, Aug. 2023, doi: 10.3390/jrfm16080372.
[183] B. S. Arunnima, D. Bijulal, and R. Sudhir Kumar, “Open Innovation Intellectual Property Risk Maturity Model: An Approach to Measure Intellectual Property Risks of Software Firms Engaged in Open Innovation,” *Sustainability*, vol. 15, no. 14, p. 11036, Jul. 2023, doi: 10.3390/su151411036.
[184] S. Moslem, M. K. Saraji, A. Mardani, A. Alkharabsheh, S. Duleba, and D. Esztergár-Kiss, “A Systematic Review of Analytic Hierarchy Process Applications to Solve Transportation Problems: From 2003 to 2022,” *IEEE Access*, vol. 11, pp. 11973–11990, 2023, doi: 10.1109/access.2023.3234298.
[185] K. Rashidi, A. Noorizadeh, D. Kannan, and K. Cullinane, “Applying the triple bottom line in sustainable supplier selection: A meta-review of the state-of-the-art,” *J. Clean. Prod.*, vol. 269, p. 122001, Oct. 2020, doi: 10.1016/j.jclepro.2020.122001.

[186] R. Salehzadeh and M. Ziaeian, “Decision making in human resource management: a systematic review of the applications of analytic hierarchy process,” *Front. Psychol.*, vol. 15, Aug. 2024, doi: 10.3389/fpsyg.2024.1400772.

[187] S. Kumar, W. M. Lim, R. Sureka, C. J. C. Jabbour, and U. Bamel, “Balanced scorecard: trends, developments, and future directions,” *Rev. Manag. Sci.*, vol. 18, no. 8, pp. 2397–2439, Aug. 2024, doi: 10.1007/s11846-023-00700-6.

[188] P. Madzík and L. Falát, “State-of-the-art on analytic hierarchy process in the last 40 years: Literature review based on Latent Dirichlet Allocation topic modelling,” *PLoS ONE*, vol. 17, May 2022, doi: 10.1371/journal.pone.0268777.

[189] M. Alrawad *et al.*, “Managers’ perception and attitude toward financial risks associated with SMEs: Analytic Hierarchy Process approach,” *J. Risk Financ. Manag.*, vol. 16, no. 2, p. 86, Feb. 2023, doi: 10.3390/jrfm16020086.

[190] M. Mariani and M. Borghi, “Industry 4.0: A bibliometric review of its managerial intellectual structure and potential evolution in the service industries,” *Technol. Forecast. Soc. Change*, vol. 149, p. 119752, Dec. 2019, doi: 10.1016/j.techfore.2019.119752.

[191] H. R. Mahyar, M. Mojtahedi, and M. J. Ostwald, “Industry 4.0, Disaster Risk Management and Infrastructure Resilience: A Systematic Review and Bibliometric Analysis,” *Buildings*, vol. 11, no. 9, p. 411, Sep. 2021, doi: 10.3390/buildings11090411.

[192] S. Chaube *et al.*, “An Overview of Multi-Criteria Decision Analysis and the Applications of AHP and TOPSIS Methods,” *Int. J. Math. Eng. Manag. Sci.*, vol. 9, no. 3, pp. 581–615, Jun. 2024, doi: 10.33889/ijmems.2024.9.3.030.

[193] R. A. Khan, I. Keshta, H. A. Hashimi, A. Almagrabi, H. Alwageed, and M. Alzahrani, “A Fuzzy-AHP Decision-Making Framework for Optimizing Software Maintenance and Deployment in Information Security Systems,” *J. Softw. Evol. Process*, vol. 37, Jan. 2025, doi: 10.1002/smr.2758.

[194] M. Siavvas, D. Kehagias, D. Tzovaras, and E. Gelenbe, “A hierarchical model for quantifying software security based on static analysis alerts and software metrics,” *Softw. Qual. J.*, vol. 29, pp. 431–507, May 2021, doi: 10.1007/s11219-021-09555-0.

[195] M. H. Hersyah, Md. D. Hossain, Y. Taenaka, and Y. Kadobayashi, “Fuzzyfortify: a multi-attribute risk assessment for multi-factor authentication and cloud container orchestration,” *Front. Comput. Sci.*, vol. 7, no. 1557918, p. 1557918, Jul. 2025, doi: 10.3389/fcomp.2025.1557918.

[196] H. Setiawan, F. A. Putra, and A. R. Pradana, “Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute,” in *2017 International Conference on Information Technology Systems and Innovation (ICITSI)*, Bandung, Indonesia: IEEE, Oct. 2017, pp. 251–256. doi: 10.1109/ICITSI.2017.8267952.

[197] A. Santos-Olmo, L. E. Sánchez, E. Álvarez, D. G. Rosado, and E. Fernandez-Medina, “Revisión Sistemática de Análisis de Riesgos Asociativos y Jerárquicos. Periodo 2014 – 2019,” in *Seguridad Informática. X Congreso Iberoamericano, CIBSI 2020*, Universidad del Rosario, 2020. doi: 10.12804/si9789587844337.13.

[198] S. Mubarak, H. Heyasat, and S. Wibowo, “Information Security Models are a Solution or Puzzle for SMEs? A Systematic Literature Review,” in *ACIS 2019 Proceedings*, Perth, Australia, 2019. [Online]. Available: https://aisel.aisnet.org/acis2019/15/

[199] P. F. de A. Lima, C. Verbano, P. F. de A. Lima, and C. Verbano, “Project Risk Management Implementation in SMEs: A Case Study from Italy,” *J. Technol. Manag. Amp Innov.*, vol. 14, no. 1, pp. 3–10, 2019, doi: 10.4067/S0718-27242019000100003.

[200] A. P. Putra and B. Soewito, “Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 4, 2023, doi: 10.14569/ijacsa.2023.0140468.

[201] C. Garcia-Porras, S. Huamani-Pastor, and J. Armas-Aguirre, “Information Security Risk Management Model for Peruvian SMEs,” in *2018 IEEE Sciences and Humanities International Research Conference (SHIRCON)*, Lima: IEEE, Nov. 2018, pp. 1–5. doi: 10.1109/SHIRCON.2018.8592994.

[202] D. Espinosa T., J. Martínez P., and S. Amador D., “Gestión del riesgo en la seguridad de la información con base en la Norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la Metodología OCTAVE-S. Caso de estudio: proceso de inscripciones y admisiones en la división de admisión registro y control AC,” *Rev. Ing. USBMed*, vol. 5, no. 2, pp. 33–43, 2014, Accessed: May 27, 2025. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=6833266&info=resumen&idioma=SPA

[203] B. M. Paredes, J. Harold, B. V. Sosa, and J. Augusto, “Implementación de un modelo de procesos de seguridad de la información para una pyme peruana basada en la norma ISO/IEC 27005 y metodología Octave-S,” Universidad Señor de Sipán, Pimentel, 2024. Accessed: May 27, 2025. [Online]. Available: https://repositorio.uss.edu.pe/handle/20.500.12802/12739

[204] P. Huaman, L. S. Raymunda, R. Novoa, and F. Elías, “Evaluación de riesgos en activos de tecnologías de información en una MIPYME,” *Rev. Cienc. Tecnol.*, vol. 18, no. 3, pp. 71–78, Sep. 2022, doi: 10.17268/rev.cyt.2022.03.07.

[205] C. Montenegro and D. Moncayo, “Information security risk in SMEs: A hybrid model compatible with IFRS: Evaluation in two Ecuadorian SMEs of automotive sector,” in *Proceedings of the 6th International Conference on Information Communication and Management, ICICM 2016*, Institute of Electrical and Electronics Engineers Inc., Dec. 2016, pp. 115–120. doi: 10.1109/INFOCOMAN.2016.7784226.

[206] L. S. Blanco Marín and B. D. Cabrera Rincón, “Implementación de un software basado en herramientas de software libre para la gestión del riesgo de la Universidad Libre,” Trabajo de grado, Universidad Libre, Bogotá, Colombia, 2018. [Online]. Available: https://repository.unilibre.edu.co/handle/10901/11154

[207] I. Mayo Martínez, “Herramientas para la gestión de riesgos de la seguridad de la información. Aplicación de GlobalSUITE al método Magerit,” Final Project, E.T.S.I. de Sistemas Informáticos (UPM), España, 2018. [Online]. Available: https://oa.upm.es/54266/

[208] E. Silva, “Propuesta de seguridad informática en los aspectos organizativos de un sistema informático, aplicando ISO 27002 y CSF,” *Rev. Ing. E Innov. Futuro*, vol. 2, no. 1, May 2023, doi: 10.62465/riif.v2n1.2023.9.

[209] G. C. Dias, U. R. De Oliveira, G. Lima, and V. Fernandes, “Risk Management in the Import/Export Process of an Automobile Company: A Contribution for Supply Chain Sustainability,” *Sustainability*, vol. 13, p. 6049, May 2021, doi: 10.3390/su13116049.

[210] P. F. Blin, T. Aditya, P. B. Santosa, and C. Claramunt, “A Methodological Approach towards Cyber Risk Management in Land Administrations Systems,” *Land*, vol. 13, no. 1, Jan. 2024, doi: 10.3390/land13010019.

[211] S. X. Romo Sañicela and M. I. Vásquez Castro, “Análisis comparativo de metodologías de análisis de riesgos (MAGERIT vs. NIST SP 800-30),” Tesis de maestría, Universidad Politécnica Salesiana, Cuenca, Ecuador, 2023. [Online]. Available: https://dspace.ups.edu.ec/handle/123456789/26674

[212] Y. Z. Giraldo Montes, “Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad,” Tesis de maestría, Instituto Tecnológico Metropolitano, Medellín, Colombia, 2021. [Online]. Available: https://hdl.handle.net/20.500.12622/5550

[213] D. F. C. Garay, M. A. Carbajal Ramos, J. Armas-Aguirre, and J. M. M. Molina, “Information security risk management model for mitigating the impact on SMEs in Peru,” in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, Sevilla, Spain: IEEE, Jun. 2020, pp. 1–7. doi: 10.23919/CISTI49556.2020.9140980.

[214] A. Santos Olmo Parra, L. E. Sanchez Crespo, E. Alvarez, M. Huerta, and E. Fernandez Medina Paton, “Methodology for dynamic analysis and risk management on ISO27001,” *IEEE Lat. Am. Trans.*, vol. 14, no. 6, pp. 2897–2911, Jun. 2016, doi: 10.1109/TLA.2016.7555273.

[215] J. A. Tamayo Reinel, “Adaptación de una metodología para el análisis y gestión de riesgos informáticos para organizaciones del sector salud en Colombia.,” Proyecto aplicado, Universidad Nacional Abierta y a Distancia, Colombia, 2020. [Online]. Available: https://repository.unad.edu.co/handle/10596/35868

[216] J. F. Carias, S. Arrizabalaga, L. Labaka, and J. Hernantes, “Cyber Resilience Self-Assessment Tool (CR-SAT) for SMEs,” *IEEE Access*, vol. 9, pp. 80741–80762, 2021, doi: 10.1109/ACCESS.2021.3085530.

[217] T. A. Chandrinos and S. Gritzalis, “Analysis of frameworks / methods for information security risk management,” Master thesis, University of Piraeus, Piraeus, Greece, 2023. doi: 10.26267/unipi_dione/2903.

[218] W. Ruiz Gómez, “Implementación de herramientas en software libre para la gestión de servicios de red en las PYMES, caso: ASFEP,” tesis de maestría, Universidad Cesar Vallejo, 2019. [Online]. Available: https://hdl.handle.net/20.500.12692/38870

[219] S. Matheu, J. Martínez-Gil, I. Bicchierai, J. Marchel, R. Piliszek, and A. Skarmeta, “A Flexible Risk-Based Security Evaluation Methodology for Information Communication Technology System Certification,” *Appl. Sci.*, Feb. 2025, doi: 10.3390/app15031600.

[220] M. Güler and G. Büyüközkan, “Cybersecurity maturity assessment using an incomplete hesitant fuzzy AHP method and Bonferroni means operator,” *Expert Syst. Appl.*, p. 127268, Mar. 2025, doi: 10.1016/j.eswa.2025.127268.

[221] Y. S. Chen, J. C. L. Chou, Y. S. Lin, Y. H. Hung, and X. H. Chen, “Identification of SMEs in the Critical Factors of an IS Backup System Using a Three-Stage Advanced Hybrid MDM–AHP Model,” *Sustain. Switz.*, vol. 15, no. 4, Feb. 2023, doi: 10.3390/su15043516.

[222] C. A. Villegas Rivera, “Modelo de gestión de riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas,” tesis de maestría, Universidad Católica Santo Toribio de Mogrovejo, USAT-Tesis, 2022. [Online]. Available: http://hdl.handle.net/20.500.12423/4551

[223] R. Scholz, R. Czichos, P. Parycek, and T. Lampoltshammer, “Organizational vulnerability of digital threats: A first validation of an assessment method,” *Eur J Oper Res*, vol. 282, pp. 627–643, Sep. 2019, doi: 10.1016/j.ejor.2019.09.020.

[224] R. B. Johnson, A. J. Onwuegbuzie, and L. A. Turner, “Toward a Definition of Mixed Methods Research,” *J. Mix. Methods Res.*, vol. 1, no. 2, pp. 112–133, Apr. 2007, doi: 10.1177/1558689806298224.

[225] M. Neri, F. Niccolini, and L. Martino, “Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment,” *Inf Comput Secur*, vol. 32, pp. 38–52, Jul. 2023, doi: 10.1108/ics-05-2023-0084.

[226] M. Rajadurai and P. Kaliyaperumal, “Optimizing Multimodal Transportation: A Novel Decision-Making Approach With Fuzzy Risk Assessment,” *IEEE Access*, vol. 13, pp. 14584–14610, 2025, doi: 10.1109/access.2025.3528037.

[227] “Google Gemini,” Gemini. Accessed: Feb. 25, 2026. [Online]. Available: https://gemini.google.com