Universidad Tecnológica Nacional
MAYO - AGOSTO 2026 / Año 24 - Nº 56

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

M-SCORE: An Explainable and Quantitative Cybersecurity Maturity Scoring Model for SMEs

M-SCORE: Un Modelo Cuantitativo y Explicable de Scoring de Madurez en Ciberseguridad para PyMEs

Presentado: 16/04/2026

Aprobado: 26/06/2026

Publicado: 20/07/2026

Diego Angelo Bolatti
https://orcid.org/0000-0002-8275-4476
Universidad Tecnológica Nacional, Argentina.
dbolatti@gfe.frre.utn.edu.ar

Javier Diaz
https://orcid.org/0000-0002-4225-3829
Universidad Nacional de La Plata, Argentina.
jdiaz@unlp.edu.ar

Verónica Bollati
https://orcid.org/0000-0003-4008-9903
Universidad Tecnológica Nacional, Argentina.
vbollati@ca.frre.utn.edu.ar

Abstract

Small and medium-sized enterprises (SMEs) face persistent cybersecurity exposure while often lacking the resources, expertise, and governance structures required to adopt comprehensive assessment frameworks. Existing cybersecurity maturity models provide useful guidance, yet they frequently remain fragmented across domains, weakly operationalized for SME realities, and insufficiently explicit in how maturity scores are computed and prioritized. This paper proposes **M-SCORE**, a quantitative and multi-dimensional cybersecurity maturity evaluation model specifically designed for SMEs. The model integrates core cybersecurity dimensions—governance, protection of data and assets, continuity and resilience, third-party risk, awareness, and detection and response, with optional coverage of AI governance—into a structured scoring approach based on measurable indicators, verifiable evidence, weighted sub-dimensions, and auditable implementation levels.

To improve practical applicability without compromising reproducibility, M-SCORE adopts

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

a hybrid architecture in which deterministic rule-based scoring is complemented by agent-assisted semantic support for evidence interpretation, document classification, and recommendation generation. In this design, AI agents do not determine the score; instead, they enhance the efficiency and usability of the assessment workflow while preserving transparency and traceability. The paper follows a Design Science Research approach and formalizes the model, its scoring logic, and its conceptual automation architecture. A preliminary application scenario is also outlined to illustrate how M-SCORE can support maturity profiling, gap identification, and roadmap prioritization in resource-constrained SME environments.

Keywords: cybersecurity maturity model; SMEs; quantitative assessment; maturity scoring; agent-assisted assessment; rule-based evaluation; cybersecurity governance; third-party risk; resilience; Design Science Research.

Resumen

Las pequeñas y medianas empresas (PyMEs) enfrentan una exposición persistente a riesgos de ciberseguridad, al tiempo que frecuentemente carecen de los recursos, la experiencia y las estructuras de gobernanza necesarias para adoptar marcos de evaluación integrales. Los modelos de madurez en ciberseguridad existentes ofrecen orientación útil, aunque suelen presentar fragmentación entre dominios, una operacionalización débil para la realidad de las PyMEs y escasa transparencia respecto de cómo se calculan y priorizan los puntajes de madurez. Este artículo propone **M-SCORE**, un modelo de evaluación de madurez en ciberseguridad cuantitativo y multidimensional, diseñado específicamente para PyMEs. El modelo integra dimensiones esenciales de ciberseguridad —gobernanza, protección de datos y activos, continuidad y resiliencia, riesgo de terceros, concientización, y detección y respuesta, con cobertura opcional de gobernanza de inteligencia artificial— en un enfoque de scoring estructurado basado en indicadores medibles, evidencia verificable, sub-dimensiones ponderadas y niveles de implementación auditables. Para mejorar la aplicabilidad práctica sin comprometer la reproducibilidad, M-SCORE adopta una arquitectura híbrida en la que el scoring determinista basado en reglas se complementa con soporte semántico asistido por agentes para la interpretación de evidencia, la clasificación documental y la generación de recomendaciones. En este diseño, los agentes de inteligencia artificial no determinan el puntaje; en cambio, mejoran la eficiencia y la usabilidad del flujo de evaluación, preservando la transparencia y la trazabilidad. El artículo sigue un enfoque de Design Science Research y formaliza el modelo, su lógica de scoring y su arquitectura conceptual de automatización. Se presenta también un escenario de aplicación preliminar para ilustrar cómo M-SCORE puede apoyar la elaboración de perfiles de madurez, la identificación de brechas y la priorización de hojas de ruta en entornos PyME con recursos limitados.

Palabras claves: modelo de madurez en ciberseguridad; PyMEs; evaluación cuantitativa; scoring de madurez; evaluación asistida por agentes; evaluación basada en reglas; gobernanza de ciberseguridad; riesgo de terceros; resiliencia; Design Science Research.

Introduction

Small and medium-sized enterprises (SMEs) are increasingly exposed to cybersecurity risks as a result of their growing dependence on digital infrastructures, cloud services, and

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

interconnected supply chains. However, their ability to manage such risks remains constrained by structural limitations, including restricted budgets, limited availability of specialized personnel, and low levels of formalization in governance processes. This imbalance between exposure and capability positions SMEs as a critical vulnerability within broader digital ecosystems.

A wide range of frameworks and standards has been developed to structure cybersecurity risk management, including the NIST Cybersecurity Framework (CSF 2.0; NIST, 2024), NIST Special Publications (e.g., SP 800-53, NIST, 2020; SP 800-37, NIST, 2018; and SP 800-161, Boyens et al., 2022), CIS Controls v8.1, and ISO/IEC 27001–27002. These frameworks provide comprehensive guidance for organizing cybersecurity practices across governance, protection, detection, response, and recovery domains. However, they are primarily defined as reference models and do not inherently provide mechanisms for quantitative, reproducible, and operational maturity evaluation, particularly in resource-constrained environments such as SMEs.

The increasing use of artificial intelligence in cybersecurity assessment further reinforces the need for structured and controlled evaluation approaches, as highlighted by frameworks such as the NIST Artificial Intelligence Risk Management Framework (NIST, 2023). In parallel, academic literature has proposed multiple cybersecurity maturity models and assessment approaches intended to support the evaluation of organizational capabilities and the prioritization of improvement actions. While these approaches provide valuable conceptual structures, they tend to exhibit persistent limitations.

Existing models frequently remain fragmented across domains, addressing governance, controls, awareness, resilience, or supply chain risk as separate assessment areas — a separation that limits the ability to obtain a coherent view of cybersecurity maturity. Many of these approaches also lack formalized scoring mechanisms, relying instead on qualitative interpretations or loosely defined maturity levels. Compounding both problems, they seldom reflect the operational realities of SMEs, where simplicity, cost-efficiency, and incremental implementation are not optional features but basic requirements.

Recent advances in automation and artificial intelligence introduce new possibilities for supporting cybersecurity assessment processes, particularly in areas such as document analysis, compliance evaluation, and evidence interpretation. However, approaches that rely heavily on AI-driven decision-making may compromise explainability, auditability, and reproducibility when evaluation logic becomes opaque. In cybersecurity governance contexts, these properties are essential to ensure trust in assessment outcomes and to support informed decision-making.

Another recent work on explainable artificial intelligence (XAI) emphasizes the importance of transparency and interpretability in automated decision-support systems, particularly in cybersecurity and governance contexts (Tjoa & Guan, 2021; Samek et al., 2021). These studies reinforce the need for approaches in which evaluation logic remains explicit, verifiable, and traceable.

In response to these limitations, this paper proposes M-SCORE, a quantitative and multi-dimensional cybersecurity maturity evaluation model specifically designed for SMEs. The model is defined as a conceptual, maturity-oriented framework intended to support structured cybersecurity assessment through the integration of key domains, including governance, protection of data and assets, continuity and resilience, third-party risk, awareness, and detection and response.

The core of M-SCORE is a deterministic and rule-based scoring mechanism grounded in

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

measurable indicators, verifiable evidence, weighted sub-dimensions, and explicitly defined implementation levels. This design is intended to ensure transparency, reproducibility, and auditability of the evaluation process. At the same time, the model incorporates a hybrid agent-assisted architecture that is intended to support evidence interpretation, document classification, and recommendation generation, while preserving a strict separation between semantic processing and scoring logic.

This work extends previous research efforts focused on cybersecurity governance in SMEs, particularly the M-GAP model presented at a previous conference (Bolatti et al., 2025). While prior work addressed governance as a standalone assessment dimension, the present study advances toward an integrated and quantitative maturity evaluation framework that consolidates multiple cybersecurity domains into a unified scoring structure.

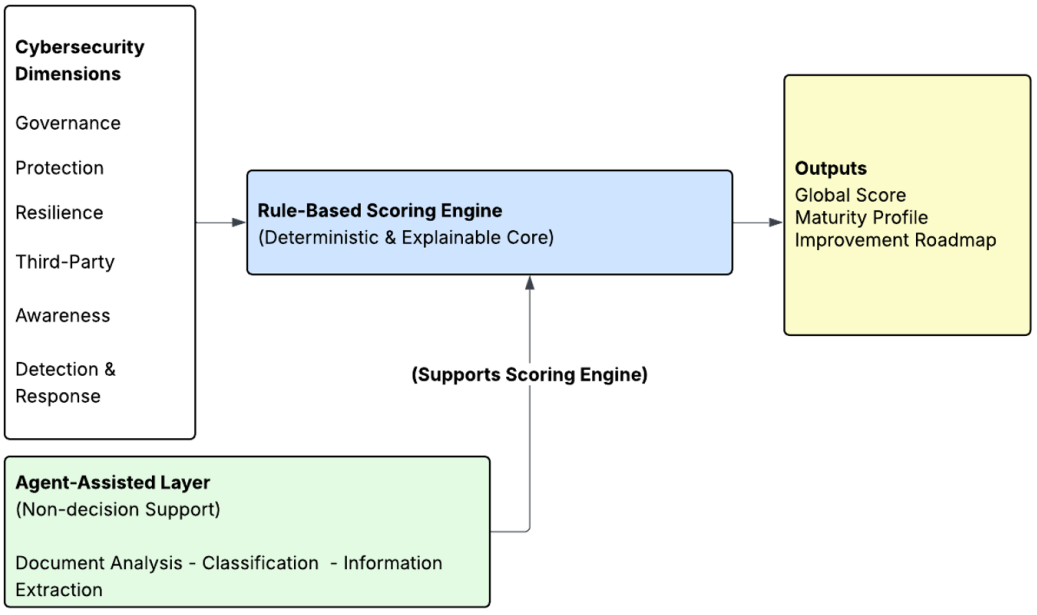

Fig 1: Conceptual overview of the M-SCORE model

Figure 1 provides a conceptual overview of the M-SCORE model, illustrating the relationship between cybersecurity dimensions, the rule-based scoring engine, and the agent-assisted support layer. The figure is intended to introduce the structure of the model prior to its formal definition, emphasizing its hybrid and multi-dimensional nature.

This research follows a Design Science Research (DSR) approach, focusing on the design and formalization of an artifact intended to address a relevant and practical problem. The paper presents the conceptual foundations of the model, its structural components, and its scoring logic, along with a conceptual architecture for its implementation. A preliminary application scenario is included to illustrate how the model can be applied to generate maturity profiles, identify gaps, and support the prioritization of improvement actions in SME environments.

The remainder of the paper is structured as follows. Section 2 reviews the relevant literature on cybersecurity frameworks, maturity models, and quantitative assessment approaches.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

Section 3 defines the problem addressed by this research. Section 4 presents the M-SCORE model. Section 5 introduces the agent-assisted architecture. Section 6 outlines an application scenario. Section 7 discusses implications and limitations, and Section 8 concludes the paper.

Literature Review

This literature review adopts a structured narrative approach, focusing on widely recognized cybersecurity frameworks, maturity models, and recent research contributions related to quantitative assessment and automation. Sources were selected based on their relevance to SME environments, their influence on cybersecurity practice, and their contribution to the conceptual and methodological foundations of maturity evaluation.

Cybersecurity risk management has been extensively addressed through international standards and frameworks that provide structured guidance for organizing security practices. Among the most influential are the NIST Cybersecurity Framework (CSF 2.0; NIST, 2024), NIST Special Publications such as SP 800-53 (NIST, 2020) and SP 800-37 (NIST, 2018), ISO/IEC 27001–27002, and the CIS Controls v8.1. These frameworks define comprehensive sets of functions, controls, and processes intended to support governance, protection, detection, response, and recovery activities. Their widespread adoption has contributed to the establishment of a common language for cybersecurity management across organizations and sectors (Azmi et al., 2018). Comparative studies have further explored the integration of multiple frameworks to support structured assessment approaches (Sulistyowati et al., 2020).

Earlier studies on information security governance frameworks have explored structured approaches to evaluating organizational security practices, although often without formalized quantitative mechanisms (Rebollo et al., 2015).

Despite their relevance, these frameworks are primarily defined as reference models rather than evaluation mechanisms. They specify what organizations are expected to implement but provide limited guidance on how to quantify implementation levels or compare maturity across different contexts. As a result, organizations—particularly SMEs—face challenges when attempting to translate these frameworks into measurable and operational assessments.

To address this limitation, a growing body of research has focused on cybersecurity maturity models, which are intended to support the evaluation of organizational capabilities and to guide improvement processes. These models typically define maturity levels associated with the implementation of controls or practices. Some approaches align maturity levels with established frameworks such as NIST CSF or ISO/IEC 27002, enabling organizations to evaluate their posture relative to recognized standards (Almuhammadi & Alsaleh, 2017). Recent work has also explored the development of structured cybersecurity capability models tailored to organizational contexts, including SMEs, emphasizing the need for systematic and scalable evaluation approaches.

However, existing maturity models present important limitations. A recurrent issue is the reliance on qualitative or semi-quantitative assessment methods, where maturity levels are conceptually defined but lack formalized and reproducible scoring mechanisms. This limitation restricts the ability to perform consistent comparisons across time and between organizations. In addition, many models adopt a control-centric perspective, focusing on the presence or absence of specific practices without sufficiently capturing their effectiveness, integration, or contextual relevance.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

Another significant limitation relates to domain fragmentation. Cybersecurity capabilities are frequently evaluated in isolation—such as governance, technical controls, awareness, or supply chain security—without providing an integrated perspective. This separation limits the ability to capture systemic interdependencies and to produce coherent maturity profiles, particularly in SME environments where resource allocation decisions require a holistic view.

Prior research has also emphasized the importance of organizational capabilities as a foundation for cybersecurity resilience, highlighting the need for structured and measurable capability development approaches (Malatji et al., 2022).

Human factors also represent a critical dimension of cybersecurity maturity. Awareness initiatives are often insufficient when not integrated into structured governance and evaluation processes, resulting in limited behavioral impact (Bada et al., 2019). Workforce capability frameworks further highlight the importance of skills development and organizational competencies in shaping cybersecurity maturity (Petersen et al., 2020).

From a methodological perspective, recent work in cybersecurity risk analysis has emphasized the limitations of traditional qualitative approaches and highlighted the need for more structured and quantitative evaluation mechanisms. Approaches such as adversarial risk analysis propose more rigorous decision-making frameworks that account for uncertainty and strategic interactions (Ríos Insua et al., 2021). These contributions reinforce the need for models capable of supporting prioritization and resource allocation based on measurable criteria.

In parallel, the increasing adoption of digital platforms and cloud-based infrastructures has stimulated research on automated and semi-automated cybersecurity assessment approaches. These approaches explore the use of rule-based systems and machine learning techniques to support compliance evaluation, configuration analysis, and security posture assessment. While such approaches demonstrate potential for improving scalability and reducing manual effort, they also introduce challenges related to interpretability and trust.

The use of artificial intelligence in cybersecurity assessment remains an evolving area. While AI can support tasks such as document classification, anomaly detection, and evidence interpretation, its integration into evaluation processes requires careful design to preserve verifiable results, traceable outcomes, and reproducibility. This requirement is particularly relevant in maturity assessment contexts, where evaluation outcomes must be justifiable and subject to validation.

Within this context, SMEs present specific challenges that are not fully addressed by existing approaches. Limited resources, simplified organizational structures, and dependence on external service providers require models that are not only rigorous but also practically implementable. Although prior work has highlighted the need for simplified and tailored frameworks for SMEs, these efforts often remain either too high-level or insufficiently formalized in terms of measurement and scoring.

In summary, the literature reveals a persistent gap between existing cybersecurity frameworks, maturity models, and automated assessment approaches. Frameworks provide structured guidance but lack quantification mechanisms. Maturity models introduce evaluation structures but often remain qualitative or fragmented. Automated approaches improve efficiency but may compromise transparency. These limitations motivate the development of a conceptual, maturity-oriented framework that integrates quantitative rigor, multi-dimensional structure, SME applicability, and controlled use of automation.

The M-SCORE model is proposed in this context as an approach intended to address these limitations, as detailed in the following sections.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

Problem Statement

The increasing exposure of small and medium-sized enterprises (SMEs) to cybersecurity threats has not been matched by a proportional evolution in their ability to assess and manage cybersecurity maturity in a structured and measurable way. While existing frameworks provide comprehensive guidance and maturity models offer conceptual evaluation structures, there remains a fundamental disconnect between **what should be implemented** and **how implementation can be objectively measured and operationalized in practice.**

This disconnect becomes particularly evident in SME environments, where cybersecurity decisions must be made under constraints of limited resources, reduced technical specialization, and high dependency on external service providers. In such contexts, assessment approaches that rely on qualitative judgments or loosely defined maturity levels are insufficient to support prioritization and resource allocation. Conversely, highly complex or data-intensive models are often impractical to implement. As a result, SMEs frequently operate without a clear, consistent, and reproducible understanding of their cybersecurity maturity.

A key limitation identified in the literature is the absence of **formalized quantitative mechanisms** capable of translating cybersecurity practices into measurable outcomes. Although some approaches introduce scoring schemes, these are often implicit, non-transparent, or inconsistently applied, limiting their reproducibility and comparability. Without a well-defined scoring logic grounded in observable evidence, maturity assessments risk becoming subjective and difficult to validate.

At the same time, cybersecurity capabilities are inherently **multi-dimensional and interdependent**, spanning governance, technical protection, resilience, human factors, and third-party dependencies. Existing approaches frequently evaluate these dimensions independently, which restricts the ability to capture systemic relationships and to produce a coherent maturity profile. For SMEs, where resource allocation decisions must consider trade-offs across domains, the lack of integrated evaluation mechanisms represents a significant limitation.

The growing availability of automation and artificial intelligence introduces additional complexity. These technologies enable more efficient data processing, evidence analysis, and scalability of assessments. At the same time, approaches that embed AI directly into evaluation or scoring processes may compromise verifiable results and evaluation consistency, particularly when decision logic becomes opaque. This creates a tension between **automation and explainability**, which must be carefully balanced in cybersecurity maturity assessment.

The problem addressed in this research can be formulated as follows:

How can a cybersecurity maturity evaluation model for SMEs be designed to be simultaneously quantitative, multi-dimensional, operationally feasible, and compatible with automated support mechanisms, while preserving transparency, reproducibility, and auditability?

Addressing this problem requires reconciling several competing requirements. The model must provide a **formal and deterministic scoring mechanism** capable of producing consistent and comparable results across different contexts. At the same time, it must remain sufficiently **simple and adaptable** to be implemented in SMEs without requiring extensive resources or specialized expertise. Furthermore, the model must integrate multiple cybersecurity domains into a unified structure, enabling holistic assessment and prioritization.

In addition, the model must support the use of automation in a controlled manner. Rather

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

than delegating evaluation decisions to artificial intelligence, automation should be designed to assist in tasks such as evidence interpretation, document analysis, and recommendation generation, while preserving a **rule-based and explainable core evaluation process.** This separation is essential to ensure that maturity assessments remain auditable and defensible.

From a Design Science Research perspective, these requirements define the characteristics of the artifact to be developed. The proposed solution must therefore combine **quantitative rigor, structural integration, SME-oriented design, and controlled automation support** into a coherent evaluation model.

The following section presents the M-SCORE model as a response to this problem, detailing its dimensions, components, and scoring methodology.

The M-SCORE Model

The M-SCORE model is defined as a conceptual, maturity-oriented framework intended to support structured cybersecurity evaluation in SME environments.

Figure 2 presents a conceptual representation of the M-SCORE model, illustrating its multi-dimensional structure, the hierarchical relationship between indicators and scoring components, and the integration of the rule-based evaluation core with supporting evidence inputs. The figure is intended to provide an introductory view of how cybersecurity capabilities are structured and aggregated within the model prior to its formal definition.

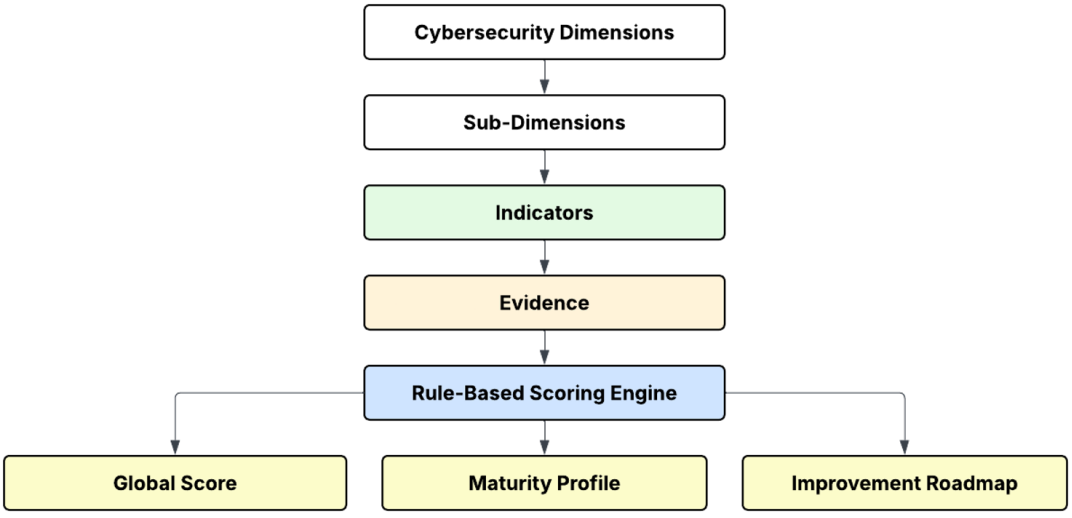

Fig 2: Internal structure of the M-SCORE model and scoring logic.

The M-SCORE model is defined as a conceptual, maturity-oriented framework intended to support structured cybersecurity evaluation in small and medium-sized enterprises. Its primary objective is to provide a formal mechanism for translating cybersecurity practices into measurable and comparable outcomes through a deterministic and evidence-based scoring approach.

Table 1 summarizes the main dimensions of the M-SCORE model, along with representative indicators and typical evidence types used during the evaluation process.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

Dimension	Description	Example Indicators	Evidence Type
Governance	**Security governance and risk management**	**Security policy, risk assessment**	**Policies, reports**
Protection of Data & Assets	**Protection of information and systems**	**Backups, patching, access control**	**Configurations, logs**
Continuity & Resilience	**Business continuity capabilities**	**DR plans, RTO/RPO**	**Procedures, test results**
Third-Party Risk	**Supplier and service risk management**	**Contracts, SLA clauses**	**Agreements**
Awareness	**Human factor security**	**Training programs**	**Training records**
Detection & Response	**Incident management capabilities**	**Logs, playbooks**	**Logs, incident reports**

Table 1: M-SCORE dimensions, example indicators, and evidence types.

At its core, the model is organized around a set of interrelated cybersecurity dimensions that represent essential organizational capabilities for managing cyber risk. These dimensions include governance, protection of data and assets, continuity and resilience, third-party risk management, awareness, and detection and response. Each dimension captures a specific aspect of cybersecurity maturity while remaining interconnected with the others through operational dependencies and shared organizational processes.

Within each dimension, the model defines sub-dimensions and associated indicators that represent specific practices or capabilities. These indicators are explicitly designed to be observable and verifiable, ensuring that the evaluation process is grounded in concrete evidence rather than subjective interpretation. Typical forms of evidence include documented policies, system configurations, operational logs, contractual agreements, training records, and incident management artifacts.

Each indicator is evaluated according to predefined criteria and mapped to discrete implementation levels that reflect the degree of adoption within the organization. These levels are structured progressively, providing a pathway for incremental maturity development, and their bounded number is deliberate: the model is designed around artifacts that organizations operating under resource constraints can realistically produce and maintain.

The model defines five discrete implementation levels (L0–L4) for each indicator, mapped to a normalized numerical score on a [0, 1] scale. The assignment of a level is governed by explicit evaluation rules that specify the observable conditions required for each level to be granted. These rules operate on verifiable evidence such as documented policies, configuration artifacts, operational logs, and contractual records. Table 2 presents the formal

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

definition of the implementation levels, their associated scoring values, and the evaluation criteria applied to determine whether a given level has been reached. The use of discrete levels with explicit assignment criteria ensures that the scoring process remains reproducible and independent of evaluator subjectivity. When a particular piece of evidence satisfies the conditions for multiple levels, the highest applicable level is assigned.

Level	Label	Score (I)	Evaluation Criteria (Assignment Rules)	Example Evidence
L0	**Not implemented**	**0.00**	**No verifiable evidence of the practice exists. The control is absent or entirely undocumented.**	**No policy document; no configuration record; no log artifact.**
L1	**Informal / Ad hoc**	**0.25**	**Practice exists in an ad hoc or informal manner. No formal documentation, procedure, or approval is in place, but some observable evidence of the activity is verifiable.**	**Informal backup routine without written procedure; email-based security communication without approved policy.**
L2	**Defined / Documented**	**0.50**	**Practice is formally documented and approved. A written procedure or policy exists and is accessible to responsible personnel, but evidence of consistent execution or monitoring is not yet verifiable.**	**Approved information security policy; documented backup procedure without execution logs.**
L3	**Implemented / Monitored**	**0.75**	**Practice is actively implemented and supported by verifiable execution evidence. Monitoring or periodic review is in place, but the process has not yet been formally optimized or subjected to continuous improvement cycles.**	**Backup logs with timestamps; completed training attendance records; active patch management registry.**
L4	**Optimized / Continuous**	**1.00**	**Practice is fully implemented, monitored, and subject to periodic review and continuous improvement. Evidence includes periodic audits, improvement cycles, or formal performance metrics demonstrating ongoing effectiveness.**	**Audit results; incident response metrics; tested and validated DR plan with documented RTO/RPO measurements.**

Table 2: M-SCORE implementation levels, scoring values, evaluation criteria, and representative evidence types.

The quantitative nature of the model is achieved through a hierarchical weighted aggregation process, which provides a structured pathway for combining individual observations into higher-level maturity scores. This aggregation is performed in three stages: indicator-level evaluation, sub-dimension aggregation, and dimension-level aggregation, culminating in a global maturity score.

The aggregation at the sub-dimension level is defined as:

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

$$S_{d,s} = \sum_{i=1}^{N_{d,s}} w_{d,s,i} \cdot I_{d,s,i} \quad (1)$$

Where $I_{d,s,i}$ denotes the score assigned to indicator i within sub-dimension s of dimension *d*, and $w_{d,s,i}$ represents the corresponding weight associated with that indicator.

The aggregation at the dimension level is defined as:

$$S_d = \sum_{s=1}^{S_d} W_{d,s} \cdot S_{d,s} \quad (2)$$

Where $S_{d,s}$ is the score of sub-dimension s, and $W_{d,s}$ represents the weight of that sub-dimension within dimension d.

Finally, the global maturity score is computed as:

$$S_{global} = \sum_{d=1}^{D} W_d \cdot S_d \quad (3)$$

where Sd is the score of dimension d, and Wd represents the weight assigned to that dimension. This formulation is intended to provide a unified measure of organizational cybersecurity maturity while preserving traceability to lower-level components.

The scoring model follows a hierarchical weighted aggregation approach, commonly used in multi-criteria decision analysis, enabling transparent and interpretable evaluation across multiple dimensions. The weights applied at each level are defined such that resulting scores remain within a normalized and comparable range, facilitating consistent interpretation across different organizational contexts.

A fundamental characteristic of M-SCORE is that all scoring operations are deterministic and rule-based. Each indicator is evaluated through explicitly defined rules that map observable evidence to specific implementation levels, ensuring that identical input conditions produce identical outputs. This property — reproducibility — is what makes the model auditable: every score can be traced back through evaluation criteria to the evidence that produced it, without relying on probabilistic inference or opaque interpretation.

In addition to numerical outputs, the model provides a multi-dimensional maturity profile that reflects the relative strengths and weaknesses of the organization across different cybersecurity domains. This profile enables a more granular interpretation than a single aggregate score and is intended to support the identification of critical gaps and the prioritization of improvement actions.

Based on the comparison between current and target maturity levels, the model is also intended to support the definition of structured improvement pathways. These pathways provide guidance for progressive enhancement of cybersecurity capabilities, aligned with organizational constraints and priorities.

To ensure applicability in SME environments, the model incorporates design principles focused on simplicity, scalability, and feasibility. The number of indicators per dimension is intentionally bounded, and the required evidence is aligned with artifacts that organizations can realistically produce or obtain. The model also supports partial assessments, allowing incremental adoption without requiring comprehensive implementation from the outset.

Another key characteristic of M-SCORE is its interpretability. The structure of dimensions, indicators, and scoring rules is explicitly defined and communicable to both technical and

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

non-technical stakeholders. This makes the model usable as a governance support mechanism — not just as an evaluation instrument — facilitating decision-making and strategic alignment without requiring specialist interpretation.

Finally, the model is defined in a manner that anticipates its integration into an automated evaluation environment. The explicit specification of indicators, evidence types, and scoring rules provides a foundation for the implementation of a rule-based evaluation engine. This design is intended to support consistent and scalable application of the model, while maintaining the verifiable results and control required for cybersecurity maturity assessment.

Agent-Assisted Architecture

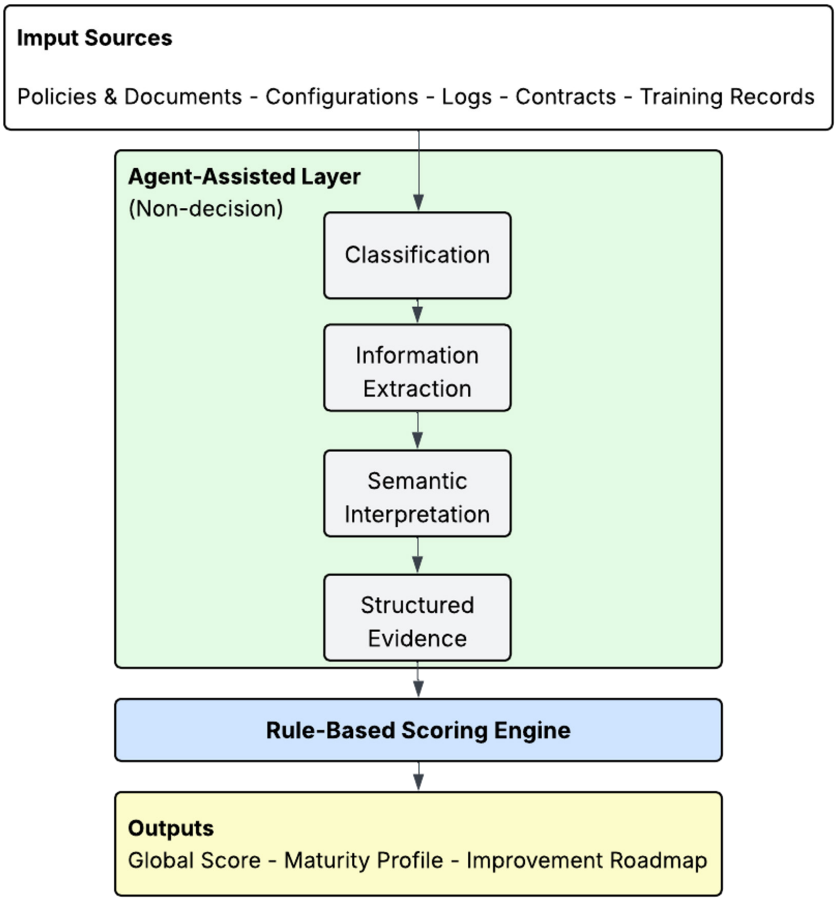

Fig 3: Agent-assisted architecture supporting the M-SCORE model.

Figure 3 presents the conceptual architecture that supports the implementation of the M-SCORE model, illustrating the interaction between data inputs, the rule-based scoring engine, and the agent-assisted processing layer. The figure provides a high-level view of how automation can enhance the assessment process without altering the deterministic nature

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

of the scoring mechanism.

The architecture is conceptualized as a hybrid system in which quantitative evaluation and semantic processing are explicitly separated. At its core, the M-SCORE model relies on a rule-based evaluation engine responsible for computing maturity scores based on predefined indicators, weights, and implementation levels. This component operates deterministically, ensuring that identical inputs always produce identical outputs.

Complementing this core component, the architecture incorporates an agent-assisted layer that supports the processing and interpretation of input data. This layer is intended to support the usability and scalability of the model, particularly in contexts where evidence is heterogeneous, unstructured, or distributed across multiple sources. Rather than replacing the evaluation logic, the agent-assisted layer acts as an intermediary that facilitates the transformation of raw inputs into structured evidence suitable for scoring.

The input layer of the architecture includes multiple sources of information relevant to cybersecurity assessment, such as policy documents, configuration files, system logs, training records, and contractual agreements with third-party providers. In SME environments, these inputs are often incomplete, inconsistently formatted, or maintained outside centralized systems. The agent-assisted layer addresses this challenge by enabling automated or semi-automated processing of such data.

Within this layer, intelligent agents perform tasks such as document classification, information extraction, and semantic interpretation of evidence. For example, agents can analyze policy documents to identify the presence of required controls, extract relevant clauses from supplier contracts, or interpret logs and configuration data to determine whether specific practices are implemented. These tasks reduce the manual effort required during the assessment process and improve consistency in evidence interpretation.

A key design principle of this architecture is that agents do not assign scores nor modify evaluation rules. Instead, they produce structured outputs—such as labeled evidence, extracted attributes, or binary indicators—that serve as inputs to the rule-based scoring engine. The final evaluation remains entirely governed by deterministic rules defined within the M-SCORE model. This separation ensures that the use of artificial intelligence does not compromise the explainability or reproducibility of the assessment results.

The interaction between components can be understood as a pipeline in which raw data is first processed by agents, transformed into structured evidence, and then evaluated by the scoring engine. This pipeline allows organizations to benefit from automation while maintaining full control over the evaluation logic. Furthermore, it enables traceability, as each score can be linked back not only to a specific indicator but also to the evidence extracted or interpreted by the agents.

Another important characteristic of the architecture is its modularity. The agent-assisted layer can be implemented using different technologies depending on the context, ranging from simple rule-based parsers to more advanced natural language processing models. This flexibility allows the architecture to be adapted to different levels of technological maturity, making it suitable for a wide range of SME environments.

From an implementation perspective, the architecture supports both centralized and distributed deployment models. In simpler scenarios, the entire system can be implemented as a single application that processes uploaded evidence and generates maturity reports. In more advanced settings, the architecture can be decomposed into services, where agents operate as independent components responsible for specific types of data processing, and the scoring engine is exposed as a separate evaluation service.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

The outputs of the system include not only the quantitative maturity scores defined by M-SCORE but also enriched information derived from the agent-assisted processing layer. This includes structured evidence repositories, traceability links between indicators and supporting artifacts, and contextualized recommendations based on identified gaps. These outputs enhance the practical value of the model, enabling organizations to move from assessment to action more efficiently.

The separation between scoring logic and semantic processing is what allows the architecture to exploit automation without sacrificing the core requirements of maturity evaluation. Complex and heterogeneous input data can be processed efficiently through the agent layer, while the deterministic scoring engine ensures that the resulting maturity scores remain verifiable, comparable, and independent of variation in AI model behavior.

From an implementation perspective, the agent-assisted layer can leverage existing open-source or commercial security tooling capable of collecting and analyzing system and security data, such as log aggregation systems, endpoint monitoring platforms, configuration assessment tools, and vulnerability scanning solutions. These technologies enable the automated collection of evidence required by the model, including logs, configurations, and security events. In this context, the role of the agent-assisted layer is to normalize and interpret this information, transforming heterogeneous technical data into structured evidence aligned with the model's indicators.

Recent advances in large language models (LLMs) have demonstrated their capability to process and interpret heterogeneous data sources, supporting tasks such as document analysis and evidence extraction in cybersecurity contexts. However, these approaches also highlight the importance of maintaining human-interpretable and controlled evaluation mechanisms (Pearce et al., 2022).

The following section illustrates the application of the model and architecture through a representative scenario.

Application Scenario

To illustrate the applicability of the M-SCORE model and its supporting architecture, this section presents a representative application scenario based on a typical small and medium-sized enterprise operating in a digitally dependent environment. The objective is not to provide a full empirical validation, but to demonstrate how the model can be applied in practice to generate measurable results, identify gaps, and support decision-making.

The scenario considers an SME with approximately 25 employees, operating in the commercial sector and relying on a combination of on-premise systems and cloud-based services for its daily operations. The organization manages customer data, financial records, and supplier information, and depends on external service providers for accounting software, cloud storage, and connectivity. Cybersecurity responsibilities are handled by a single IT generalist, without a formally established governance structure.

The assessment process begins with the collection of evidence across the dimensions defined by M-SCORE. This includes existing policies (if any), system configurations, backup procedures, user management practices, supplier contracts, and records of training or awareness activities. Given the heterogeneous and partially unstructured nature of these inputs, the agent-assisted layer supports the identification and classification of relevant information, enabling the transformation of raw data into structured evidence aligned with the model's indicators.

In practical implementations, this evidence collection process can be supported by existing operational tools commonly deployed in SME environments. These include centralized

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

logging systems, endpoint monitoring agents, backup management solutions, and cloud service dashboards. Such components facilitate the continuous generation of technical and organizational evidence, which can be automatically processed and mapped to the model's indicators. This approach reduces manual effort and enables a more consistent and scalable assessment process.

Once the evidence is structured, the rule-based evaluation engine assigns scores to each indicator according to predefined criteria. For example, in the governance dimension, the absence of a formally approved security policy results in a low implementation level, while the presence of informal practices without documentation may correspond to an intermediate level. In the protection dimension, partial implementation of backup mechanisms without regular validation leads to a moderate score, reflecting the existence of controls with limited effectiveness.

To illustrate the indicator-level evaluation process and the application of the assignment rules defined in Table 2, Table 3 presents a representative set of five indicators drawn from three dimensions of this scenario. For each indicator, the table specifies the observed evidence, the implementation level assigned according to the evaluation criteria, the corresponding numerical score, and the indicator weight within its sub-dimension. The sub-dimension score S_0,s for the governance sub-dimension "Policy and Risk Management" is computed as S_0,s = (0.5 × 0.25) + (0.3 × 0.00) + (0.2 × 0.00) = 0.125, confirming that indicator weights sum to 1.0 within each sub-dimension and that the resulting score directly feeds the dimension aggregation in Equation (2).

Dimension	Indicator	Observed Evidence	Level	Score (I)	Weight (w) in sub-dimension
Governance	**Information Security Policy**	**No written policy document found; IT staff reports informal verbal guidelines communicated to employees.**	**L1**	**0.25**	**0.50**
Governance	**Risk Assessment Process**	**No documented risk assessment or risk register found; no evidence of any formal identification of information assets or threats.**	**L0**	**0.00**	**0.30**
Governance	**Role and Responsibility Assignment**	**No formal assignment of cybersecurity roles or responsibilities documented; no designated security owner identified.**	**L0**	**0.00**	**0.20**
Protection of Data & Assets	**Data Backup**	**Weekly backup to external drive confirmed via IT staff interview; no automated backup log or restoration test record available.**	**L1**	**0.25**	**0.40**
Awareness	**Security Awareness Training**	**No training program, schedule, or attendance records exist; no evidence of any awareness activity in the past 12 months.**	**L0**	**0.00**	**0.60**

Table 3: Representative indicator-level evaluation results for the application scenario, illustrating evidence-to-score mapping and sub-dimension aggregation inputs.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

At the sub-dimension and dimension levels, scores are aggregated using the weighted mechanism defined in Section 4. The resulting maturity profile reveals an uneven distribution of capabilities. Governance and third-party risk management exhibit low maturity levels due to the absence of formal processes and structured supplier evaluation. Protection of data and assets shows moderate maturity, supported by basic technical controls. Awareness and training present minimal development, as no formal program exists. Detection and response capabilities are limited to reactive actions without defined procedures, while continuity and resilience are partially addressed through ad hoc backup practices.

The global maturity score derived from this assessment reflects an early-stage maturity level, consistent with the organizational characteristics of the SME. More importantly, the multi-dimensional profile provides actionable insights by highlighting the most critical gaps. In this scenario, the lack of governance mechanisms and supplier risk management emerges as a priority, followed by the need to formalize incident response procedures and implement structured awareness initiatives.

Table 4 presents a representative example of the maturity assessment results, illustrating how the model provides both dimension-level insights and an overall maturity score.

Dimension	Score	Maturity Level
Governance	**0.25**	**Initial**
Protection of Data & Assets	**0.55**	**Developing**
Continuity & Resilience	**0.40**	**Basic**
Third-Party Risk	**0.20**	**Initial**
Awareness	**0.15**	**Initial**
Detection & Response	**0.30**	**Basic**
Global Score	**0.31**	**Initial**

Table 4: Example maturity assessment results for the representative SME scenario.

Based on these results, the model is intended to support the definition of a prioritized improvement roadmap. Initial actions focus on low-cost, high-impact measures, such as the formalization of a basic security policy, the establishment of a simple risk assessment process, and the implementation of structured backup validation procedures. Subsequent steps include the introduction of supplier evaluation criteria, the development of incident response playbooks, and the implementation of periodic awareness training. This staged approach aligns with the incremental maturity progression supported by M-SCORE.

The role of the agent-assisted architecture in this scenario is particularly relevant during the evidence processing phase. By automating the classification and extraction of relevant information, agents reduce the effort required from the organization and improve the consistency of the assessment. At the same time, the deterministic scoring engine ensures that all evaluation results remain transparent and reproducible.

This application scenario demonstrates that M-SCORE can be effectively applied in SME environments characterized by limited resources and low formalization. The model not only

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

provides a quantitative assessment of cybersecurity maturity but also supports the transition from evaluation to action through structured and prioritized recommendations.

Discussion and Implications

This study proposes M-SCORE as a response to the persistent gap between high-level cybersecurity frameworks and the practical need for structured, measurable, and operational maturity evaluation in SMEs. The model is intended to contribute to the field by introducing a quantitative and multi-dimensional approach that remains aligned with established standards while addressing their limitations in terms of operationalization and assessment.

From a conceptual perspective, M-SCORE advances existing maturity assessment approaches by shifting from predominantly qualitative or loosely defined evaluation schemes toward a formalized and deterministic scoring model. This shift is particularly consequential in cybersecurity contexts, where decision-making requires not only identification of gaps but also the ability to prioritize actions based on measurable criteria. Grounding evaluation in observable evidence and explicit scoring rules strengthens both the rigor and the reproducibility of assessments.

Another important contribution lies in the integration of multiple cybersecurity domains into a unified evaluation structure. Rather than treating governance, technical controls, awareness, resilience, and third-party risk as independent assessment areas, M-SCORE captures their interdependencies within a single model. This integrated perspective reflects the systemic nature of cybersecurity and enables more coherent prioritization of improvement efforts, especially in environments where resources must be carefully allocated.

The model also is intended to contribute to responding to the identified gap between theoretical frameworks and practical implementation. While widely adopted standards provide valuable guidance, their direct application often requires interpretation and adaptation. M-SCORE operationalizes these frameworks by translating their principles into measurable indicators, structured evidence requirements, and weighted scoring mechanisms. In doing so, it provides a practical pathway for SMEs to align with recognized standards without incurring the complexity typically associated with their full implementation.

In addition, research on organizational cybersecurity strategies highlights the importance of aligning security capabilities with broader organizational structures and decision-making processes (Ahmad et al., 2014).

The introduction of a hybrid agent-assisted architecture represents an additional contribution, particularly in the context of increasing interest in the use of artificial intelligence in cybersecurity. Unlike approaches that embed AI directly into decision-making processes, this work explicitly separates semantic processing from evaluation logic. This design intends to preserve the transparency and auditability of the scoring process while enabling automation to improve efficiency and scalability. The result is a balanced approach that leverages the strengths of AI without compromising the core requirements of maturity assessment.

From a practical standpoint, M-SCORE offers a structured mechanism for SMEs to assess their cybersecurity posture and define improvement strategies. The model's emphasis on simplicity, scalability, and evidence-based evaluation makes it suitable for organizations with limited resources and low levels of formalization. The ability to generate both quantitative scores and multi-dimensional maturity profiles enables organizations to identify critical gaps and prioritize actions in a systematic manner.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

However, several limitations must be acknowledged. First, while the model is defined to be broadly applicable, the definition of indicators, weights, and implementation levels may require adaptation to specific sectors or regulatory contexts. Second, the validation presented in this study is limited to a representative application scenario, and further empirical evaluation is necessary to assess the model's performance across diverse organizational settings. Third, the effectiveness of the agent-assisted layer depends on the quality and availability of input data, which may vary significantly across SMEs.

These limitations open several avenues for future research. Empirical validation through multiple case studies or longitudinal assessments would strengthen the evidence supporting the model. Additionally, the integration of decision-support techniques, such as multi-criteria decision analysis, could enhance the weighting mechanisms and support more advanced prioritization strategies. Further exploration of agent-based processing capabilities may also improve the automation of evidence interpretation while maintaining transparency.

Overall, the findings suggest that it is possible to design cybersecurity maturity evaluation models that combine quantitative rigor, multi-dimensional integration, and practical applicability, while incorporating automation in a controlled and explainable manner. This is intended to contribute to advancing both the academic understanding and the practical implementation of cybersecurity maturity assessment in SME environments.

This also suggests that the model can be incrementally integrated with existing cybersecurity tooling ecosystems, allowing organizations to leverage already available data sources without requiring significant additional investments.

Conclusions

This paper introduced M-SCORE, a quantitative and multi-dimensional cybersecurity maturity evaluation model specifically designed for small and medium-sized enterprises. The model addresses key limitations identified in existing approaches, including the lack of formalized scoring mechanisms, the fragmentation of cybersecurity domains, and the limited operational applicability of current frameworks in SME environments.

A structured set of dimensions, combined with a deterministic rule-based scoring methodology, enables M-SCORE to transform cybersecurity practices into measurable, reproducible, and auditable outcomes. Organizations can use these outcomes to assess their current maturity levels, identify critical gaps, and prioritize improvement actions based on objective criteria rather than qualitative judgment.

A distinguishing feature of the model is the integration of a hybrid agent-assisted architecture that enhances the assessment process without compromising transparency. Separating semantic processing from evaluation logic allows the model to leverage automation for efficiency gains while preserving the explainability and traceability required for cybersecurity governance.

The application scenario presented in this study demonstrates the practical feasibility of M-SCORE in SME contexts, highlighting its ability to operate under conditions of limited resources and low formalization. The model's emphasis on simplicity, scalability, and evidence-based evaluation makes it a suitable foundation for both manual and automated assessment processes.

From a research perspective, this work is intended to contribute to advancing cybersecurity maturity assessment by providing a model that integrates quantitative rigor,

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

multi-dimensional analysis, and controlled use of automation. Future work will focus on the implementation and validation of the proposed architecture through the development of a functional prototype, integrating the rule-based scoring engine with agent-assisted components. In particular, ongoing research will explore the application of the model in real SME environments, enabling empirical validation using local organizations and sector-specific scenarios. This includes the deployment of pilot implementations, the collection of real-world evidence, and the evaluation of the model's effectiveness in supporting decision-making and maturity improvement processes.

Use of Generative AI and AI Tools in the Preparation of the Article

The author(s) declare the use of the AI tool ChatGPT for generating the document structure, searching for references, and proposing the architecture of the proposed solution. The authors confirm that after its use, the resulting content was reviewed, verified, and edited, and they assume full responsibility for the content presented in this article.

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

Referencias

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357–370. https://doi.org/10.1007/s10845-012-0683-0

Almuhammadi, S., & Alsaleh, M. (2017). Information security maturity model for NIST cybersecurity framework. *Computer Science & Information Technology (CS & IT), 7*(3), 51–62. https://doi.org/10.5121/csit.2017.70305

Azmi, R., Tibben, W., & Win, K. T. (2018). Review of cybersecurity frameworks: Context and shared concepts. *Journal of Cyber Policy*, 3(2), 258–283. https://doi.org/10.1080/23738871.2018.1520271

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv preprint. (Original work presented at CSSS 2015) https://doi.org/10.48550/arXiv.1901.02672.

Bolatti, D., Díaz, J., & Bollati, V. A. (2025). Strategic cybersecurity governance for SMEs: An adaptive and progressive governance model. In *Proceedings of the XXXI Congreso Argentino de Ciencias de la Computación (CACIC 2025)* (pp. 893–902). Red de Universidades con Carreras en Informática. http://sedici.unlp.edu.ar/handle/10915/189846

Boyens, J., Smith, A., Bartol, N., Winkler, K., Holbrook, A., & Fallon, M. (2022). Cybersecurity supply chain risk management practices for systems and organizations (NIST SP 800-161 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1

Malatji, M., Marnewick, A. L., & Von Solms, S. (2022). Cybersecurity capabilities for critical infrastructure resilience. *Information & Computer Security, 30*(2), 255–279. https://doi.org/10.1108/ICS-06-2021-0091

National Institute of Standards and Technology (NIST). (2023). Artificial Intelligence Risk Management Framework (AI RMF 1.0). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.100-1

National Institute of Standards and Technology. (2024). The NIST cybersecurity framework (CSF) 2.0. https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations (NIST SP 800-53 Rev. 5). https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2018). Risk management framework for information systems and organizations (NIST SP 800-37 Rev. 2). https://doi.org/10.6028/NIST.SP.800-37r2

Pearce, H., Ahmad, B., Tan, B., Dolan-Gavitt, B., & Karri, R. (2022). Asleep at the keyboard? Assessing the security of GitHub Copilot's code contributions. *2022 IEEE Symposium on Security and Privacy (SP)*, 754–768. https://doi.org/10.1109/SP46214.2022.9833571

Petersen, R., Santos, D., Smith, M. C., Wetzel, K. A., & Witte, G. (2020). *Workforce framework for cybersecurity (NICE framework)* (NIST SP 800-181 Rev. 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181r1

Rebollo, O., Mellado, D., Fernández-Medina, E., & Mouratidis, H. (2015). Empirical evaluation of a cloud computing information security governance framework. *Information and Software Technology, 58*, 44–57. https://doi.org/10.1016/j.infsof.2014.10.003

Ríos Insua, D., Couce-Vieira, A., Rubio, J. A., Pieters, W., Labunets, K., & Rasines, D. G. (2021). An Adversarial risk analysis for cybersecurity. *Risk Analysis*, 41(1), 16–36. https://doi.org/10.1111/risa.13331

Revista Tecnología y Ciencia
DOI: https://doi.org/10.33414/rtyc.56.99-119.2026 - ISSN 1666-6933

Samek, W., Montavon, G., Lapuschkin, S., Anders, C. J., & Müller, K.-R. (2021). Explaining deep neural networks and beyond: A review of methods and applications. Proceedings of the IEEE, 109(3), 247–278. https://doi.org/10.1109/JPROC.2021.3060483

Sulistyowati, D., Handayani, F., & Suryanto, Y. (2020). Comparative analysis and design of cybersecurity maturity assessment methodology using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV: International Journal on Informatics Visualization*, 4(4), 225–230. https://doi.org/10.30630/joiv.4.4.482

Tjoa, E., & Guan, C. (2021). A survey on explainable artificial intelligence (XAI): Toward medical XAI. *IEEE Transactions on Neural Networks and Learning Systems*, 32(11), 4793–4813. https://doi.org/10.1109/TNNLS.2020.3027314

Authors‘ Contribution

	Academic Collaboration													
Author’s First and Last Name	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Diego A. Bolatti	x	x	x	x	x	x	x	x	x	x	x		x	x
Javier Diaz	x		x			x						x		
Verónica Bollati	x		x	x	x	x				x		x	x	x

1-Administración del proyecto, 2-Adquisición de fondos, 3-Análisis formal, 4-Conceptualización, 5-Curaduría de datos, 6-Escritura - revisión y edición, 7-Investigación, 8-Metodología, 9-Recursos, 10-Redacción - borrador original, 11-Software, 12-Supervisión, 13-Validación, 14-Visualización.