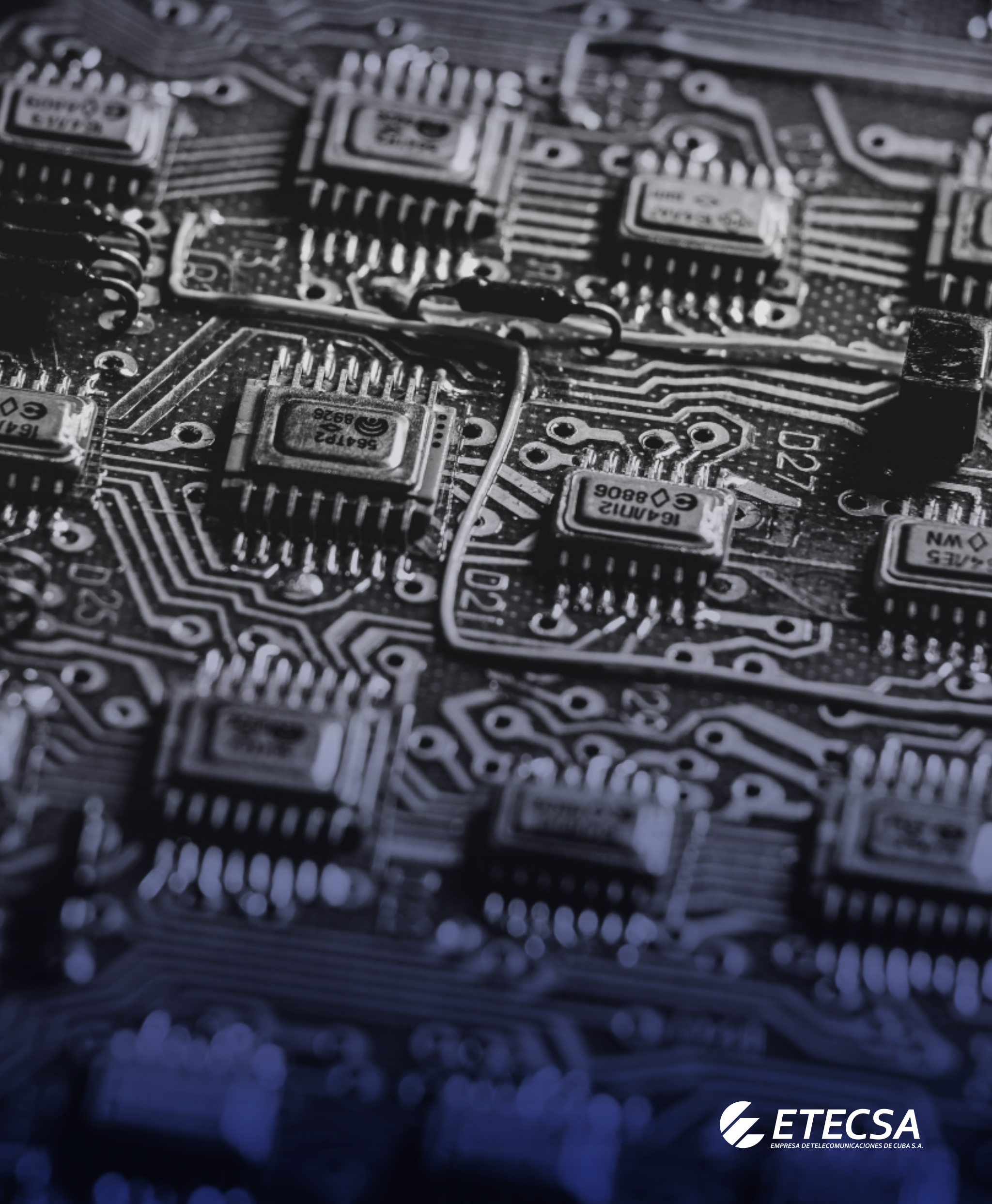
RNPS: 0514 ISSN: 2224-6274 VOL.23 - NO. 1 **JANUARY / JULY 2026**

tono

Scientific-Technical Journal of the Telecommunications Company of Cuba S.A.



ETECSA
EMPRESA DE TELECOMUNICACIONES DE CUBA S.A.

tono
Scientific-Technical Journal

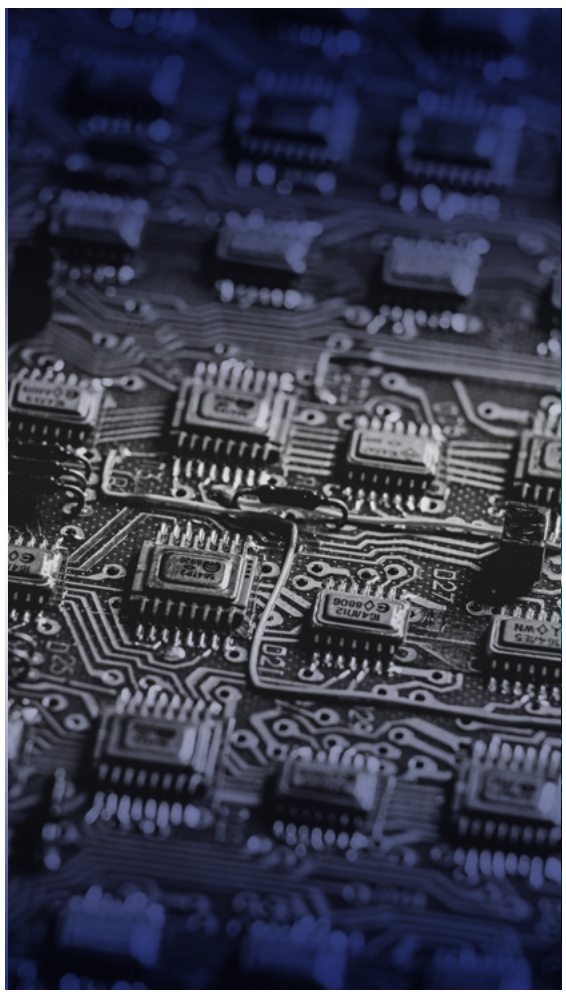
ETECSA
EMPRESA DE TELECOMUNICACIONES DE CUBA S.A.

Biannual Publication Vol.23 – No. 1 - 2026
RNPS: 0514 ISSN: 2224-6274

Tono, Scientific-Technical Journal of the Telecommunications Company of Cuba S.A.

The opinions expressed by the authors in the articles reflect their own points of view and do not necessarily coincide with the criteria of the editorial board.

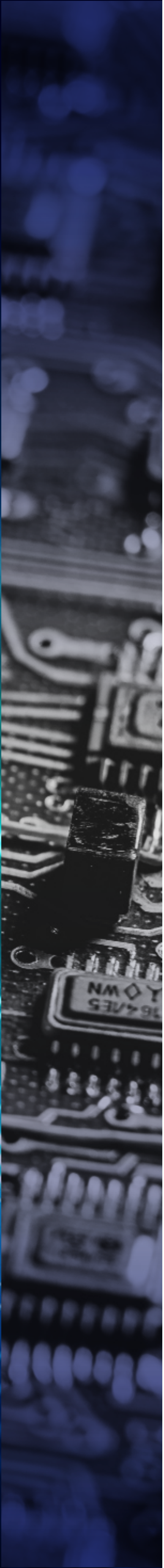
All research articles in this publication have undergone a rigorous double-blind peer review.



Cover:
Internet

Contact us

Scientific and Technical Surveillance and Information Division, ETECSA
Adress: Centro de Negocios Miramar, calle 3ra, e/ 76 y 78, Edificio Beijing, 4to Piso, oficina 404. Playa, C.P.: 11300. La Habana, Cuba.
Phone : (53) 7266-8453
Email: tono@etecsa.cu
Website: www.revistatonoetecsa.cu



Scientific Advisory Committee

Melissa Saltiel Delgado, M.Sc.
Mirta Julieta García García, M.Sc.
María del Pilar Caso Álvarez, M.Sc.
Alberto García García, M.Sc.
Fidel Mirabal Puig, M.Sc.

Editorial Board

Journal Director

Grisel Ojeda Amador, M.Sc.

Executive Editor

Inés María León Martínez, B.A.

Section Editor

Mirta Ulloa Ferreiro, B.A.

Translation

Armando Camejo Hernández, B.A.
Lena María cué Morales, B.A.
Frans Carlos Castellano Caballero, B.A.
Odalys Ojeda Fuentes, B.A.
Idalmis María Barbería Espinosa, B.A.
Alejandro Daniel Fadragas Robaina, B.A.

Original Design

Marcel Mazorra Martínez, B.A.

Layout

Isabel Canales Calvo, B.A.

Technical support and programming

Maritza de la C. Menéndez Figueredo, Eng.

Data review

Elisa María Alfaro Díaz, B.A.
Darian Díaz García, Eng.

Referees

Caridad Anías Calderón, Ph.D. (CUJAE)
Félix Álvarez Paliza, Ph.D. (UCLV)
Glauco Antonio Guillén Nieto, Ph.D. (LACETEL[1])
José Raúl Vento Álvarez, Ph.D. (UPR[2])
Osvaldo Andrés Pérez García, Ph.D. (CENATAV[3])
Lindsay Alonso Gómez Beltrán, Ph.D. (Univ. Camagüey[4])
Gregory Randall, Ph.D. (Univ. de la República, Uruguay[5])
María Matilde García Lorenzo, Ph.D. (UCLV)
Jorge Gulin González, Ph.D. (UCI)
Omar Correa Madrigal, Ph.D. (UCI)
Arelys Emiliana Ramos Fleites, MSc. (UCLV[6])
Alberto Javier García García, M.Sc. (ETECSA)
Raúl E. Rodriguez Doncel, Eng. (CONAS)
Fidel Mirabal Puig, M.Sc. (ETECAS)
Armando Tito Bernot, M.Sc. (ETECSA)
Pablo Domínguez Vázquez, M.Sc. (ETECSA)
Maydel Vázquez Fernández, M.Sc. (ETECSA)
Karina Leonor Fernández Sánchez, M.Sc. (ETECSA)

[1]* LACETEL: Instituto de Investigación y Desarrollo de las Telecomunicaciones (Telecommunications Research and Development Institute)

[2] UPR: Universidad de Pinar del Río “Hermanos Saíz Montes” (University of Pinar del Río “Hermanos Saíz Montes”)

[3] CENATAV: Centro Nacional de Aplicaciones Tecnológicas Avanzadas (Advanced Technologies Application Center)

[4] Universidad de Camagüey: (University of Camagüey)

[5] Universidad de la República de Uruguay: University of Uruguay

[6] UCLV: Universidad Central “Marta Abreu” de Las Villas (Central University "Marta Abreu" of Las Villas)

EDITOR'S LETTER

We are pleased to present this issue of Tono journal, which compiles notable contributions in the fields of science and technology. This selection provides an up-to-date overview of the advances and challenges in digital security, technology management, and process transformation—priority areas for the country's sovereign development and efficiency.

Digital security and infrastructure modernization are key comprehensive themes in today's context. The studies included in this compilation range from an analysis of vulnerabilities in TM Forum's Open API to the protection of mobile devices, confirming the need for holistic strategies to address increasingly sophisticated threats. Likewise, in this compilation, experiences with technological integration in strategic sectors such as Cuba's biopharmaceutical supply chain, where the shift toward Inventory 4.0 models shows the impact of digitization on operational strength, are examined.

Technology management practices in the national context are characterized by a systemic and applied approach. The documented proposals present solutions that balance innovation with practical sustainability, such as extending the Tier model from the data center to the service, conducting digital security maturity assessments for consulting services, and developing IT systems to evaluate the impact of information technologies on organizations. Notable progress has been made in areas such as infrastructure standardization, the measurement of organizational development, and the creation of management tools tailored to the country's specific conditions.

EDITOR'S LETTER

The findings of the event confirm the need to maintain an approach that combines technical improvement with institutional capacity building. It is evident that the effectiveness of digital transformation strategies requires both advanced technological solutions and professionals well-prepared to implement them in accordance with criteria of efficiency and technological sovereignty, as reflected in initiatives such as Girasol Tecnológico, which contribute to the visibility and strengthening of the national digital ecosystem.

A new feature in this issue of Tono journal is the paper "The Artificial Intelligence Revolution in Telecommunications," presented at the 2025 Scientific Conference organized by the “Vladimir Ilich Lenin” Pre-University Vocational Institute of Exact Sciences and Empresa de Telecomunicaciones de Cuba S.A. (ETECSA, in Spanish). This work shows not only the vast knowledge of Cuban young people but also their interest in exploring new topics such as the use of AI.

This compilation proves the level of specialization and maturity achieved by this knowledge community in Cuba. We appreciate the collective contribution of researchers and professionals whose work helps strengthen the foundations for secure, efficient, and reliable national digital development.

Sincerely,

Publishing Team
Tono Scientific-Technical Journal

TABLE OF CONTENTS

VOL.23 NO. 1
JANUARY / JULY 2026

RESEARCH

Threats and Vulnerabilities in TM Forum Open APIs 7
Clayret Echenique Quintana, Eng. and Jorge Manuel Sotolongo Piedra, Eng.

From Data Center to service: extending the Tier Model 26
Ernesto Carrazana Ruiz, Eng., Irisleidis Lázara Casi Estevanell, Eng., and Héctor Manuel Jacas Joa, Eng.

Technological sunflower 40
Lázaro Santana Linares, Eng., Maikol Ismael Mirabal Hidalgo, Eng., and Raydel García Mesa, M. Sc.

Towards Inventory Management 4.0: Integration of Digital Technologies in Cuba's Biopharmaceutical Supply Chain 56
Zuleyka Calzado Mesa, M. Sc., Gabriela Ojeda de la Paz, Eng., and Damián Aldait García Pérez, Eng.

Digital Security Maturity Assessment for Consulting Services 67
Noel Emilio Rojas Martos, M. Sc., and Liban de Armas Granado, M. Sc.

The AI Revolution in Telecommunications: A Journey from the Past to the Future 83
Rafael Alberto Noa Yanes, and Ivette García Montero, Eng.

Computer system for evaluating the impact of Information Technologies in organizations 93
Ernesto Elias Elzaurdín Valdés, Eng., Meliza Leon Bencomo, Ts., and Marynelsa Bonne Cuza, M. Sc.

RESEARCH

Threats and Vulnerabilities in TM Forum Open APIs

Clayret Echenique Quintana, Eng.[1*]
Jorge Manuel Sotolongo Piedra, Eng.[2]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

Telecommunications sector faces distinctive cybersecurity challenges arising from its migration to cloud-native architectures and its role as a central axis of the digital environment. In this context, TM Forum's Open APIs, which materialize the ODA architecture principles, constitute a significant attack surface by enabling interoperability between decoupled systems. This research aimed to identify and analyze the main threats and vulnerabilities affecting these interfaces, in order to contribute to the design of future security frameworks. A systematic literature review methodology based on the PRISMA protocol was employed, with searches conducted across six databases: IEEE Xplore, Scopus, Web of Science, Google Scholar, ResearchGate, and ScienceDirect and additional official sources. From the identified records, 7 studies were included after applying inclusion and exclusion criteria. As the main contribution, a correlation taxonomy was constructed integrating STRIDE+P categories, OWASP API Top 10 2023 vulnerabilities, and ODA architecture components, identifying 17 significant correlations. The results reveal that 47% present Critical

[1*] University of Computer Sciences. Carretera a San Antonio de los Baños, Km 2 ½, reparto Torrens, municipio Boyeros, La Habana, Cuba. cechenique@uci.cu

[2] University of Computer Sciences. Carretera a San Antonio de los Baños, Km 2 ½, reparto Torrens, municipio Boyeros, La Habana, Cuba. jorgemsp@uci.cu

severity, concentrated in the API Gateway, customer management, and access control. It is concluded that the security of these APIs requires granular authorization controls and field-level schema validation, providing an empirical foundation for specific security frameworks in ODA ecosystems.

Keywords: Threats in Open API, ODA, Open API, TM Forum Open APIs, Open API Security

Introduction

Telecommunications sector faces distinctive cybersecurity challenges due to its role as a central axis of the digital environment. Service providers are particularly vulnerable to cyber threats arising from geopolitical tensions, including espionage and other malicious activities. They also face technological risks inherent to their migration to cloud-native architectures, which are less well known and represent a threat to both new and legacy network services (Donegan, 2023). In this context, standardization and the adoption of open architectures emerge as fundamental pillars for innovation and interoperability. TM Forum has been a pioneer in developing reference frameworks and best practices to guide this evolution (TM Forum, 2025a).

Among its most significant contributions is the Open Digital Architecture (ODA) reference framework, conceived as an architectural model based on decoupled and reusable components for building agile business ecosystems. To complement this vision, TM Forum's Open APIs materialize the principles of the ODA implementation layer by providing a standardized set of technical specifications that enable seamless, secure, and scalable integration between systems, platforms, and partners across the digital ecosystem.

The growing use of APIs (Application Programming Interfaces) in the telecommunications sector has facilitated the creation of new products, especially with the rise of cloud services and mobile applications. However, this openness introduces significant vulnerabilities that can be exploited by malicious actors.

According to the State of API Security H2 report in 2025, the main API security problems are due to the fact that 80% of security leaders

lack continuous real-time monitoring; 33% of organizations suffered a security incident due to APIs in the last year; only 19% are confident in the accuracy of their API inventory; and 51% of organizations are still in planning stages or at basic levels in their API security maturity (Salt, 2025).

In this context, TM Forum Open APIs emerge as a fundamental standard driving integration and the creation of an interconnected service ecosystem in the telecommunications sector. These programming interfaces not only facilitate connectivity and interoperability between complex services, but also enable comprehensive lifecycle management, even in environments where multiple partners collaborate in service delivery.

Based on the REST design principles and being technologically independent, TM Forum Open APIs have become the basis for simple and consistent service management. But this standardization, while essential for innovation, also extends the reach of the aforementioned vulnerabilities; therefore, the security of these APIs becomes a critical pillar for the reliability and sustainability of the digital ecosystem.

For this reason, this research aims to systematize the main threats and vulnerabilities to which TM Forum Open APIs are exposed, in order to contribute to future research on the conception of security frameworks that integrate best practices and security standards for TM Forum Open APIs.

Materials and Methods

This research is based on a systematic literature review aimed at identifying, analyzing, and synthesizing the current state of threats and vulnerabilities in TM Forum Open APIs. To ensure methodological rigor in the document selection and analysis process, the PRISMA protocol was adopted. A search was conducted in six scientific databases and academic repositories, selected for their coverage in computer engineering, telecommunications, and cybersecurity: IEEE Xplore, Scopus, Web of Science, Google Scholar, ResearchGate, and ScienceDirect.

The search strategy was structured by combining controlled and free terms in English and Spanish, using Boolean operators (AND, OR, NOT) and truncations. Three thematic blocks were designed:

1. API and security: "API security" OR "API vulnerability" OR "API threat" OR "Open API security" OR "API risk"
2. TM Forum / ODA: "TM Forum" OR "Open Digital Architecture" OR "ODA" OR "Open API TM Forum" OR "TMF Open API"
3. Threats and vulnerabilities: "threat modeling" OR "STRIDE" OR "OWASP API Top 10" OR "cybersecurity" OR "vulnerability assessment" OR "risk assessment"

Table 1 establishes the inclusion and exclusion criteria for study selection:

Table 1. Inclusion and exclusion criteria for study selection

Inclusion Criteria	Exclusion Criteria
• Documents addressing API security in telecommunications contexts or open architectures. • Documents making explicit reference to TM Forum, ODA, or their Open APIs. • Documents analyzing threats, vulnerabilities, or security risks in RESTful APIs. • Documents proposing security frameworks, standards, or policies applicable to APIs. • Publications between 2020 and 2025, to ensure technological relevance. • Full-text or complete document access available.	• Documents not addressing API security topics. • Documents focused exclusively on APIs from other sectors without connection to telecommunications. • Commercial or promotional presentations or documents without academic or technical support. • Duplicates across databases. • Documents prior to 2020, except for essential historical normative references. • Articles in languages other than English or Spanish, unless they had a verifiable translation.

The document selection was conducted in three phases, following the PRISMA flow (see Figure 1):

Phase 1 – Identification: Searches were executed in the six databases, recording the number of results per source and removing duplicates using the Zotero reference manager and manual cross-checking.

Phase 2 – Screening: Titles and abstracts were evaluated against inclusion/exclusion criteria.

Phase 3 – Inclusion: Full texts of pre-selected documents were retrieved. The inclusion/exclusion criteria were reapplied to the full content, recording reasons for exclusion. The finally included documents were subjected to data extraction.

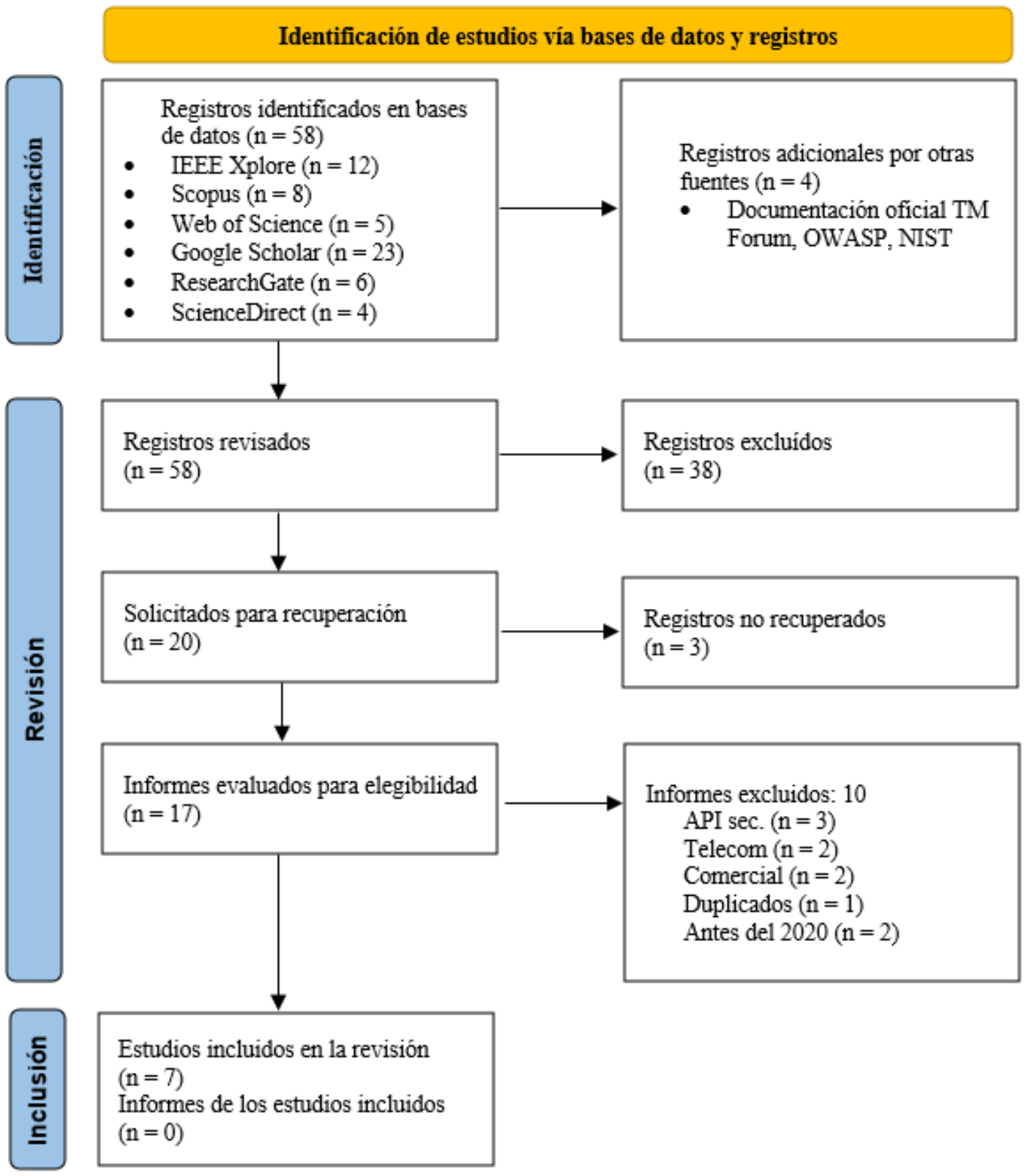


Figure 1. PRISMA Flow Diagram for Document Selection

Then, the following analytical methods were applied:

- Document analysis: Review of official TM Forum documentation, OWASP standards, NIST SP 800-53/63/228, and selected academic literature.
- Analysis and synthesis: Interpretation, processing, and categorization of extracted information, establishing relationships between threats, OWASP API Top 10 vulnerabilities, and recommended security controls.

Discussion and Results

An API is a set of rules and definitions that dictate how one software can interact with another. It acts as an intermediary that facilitates different software systems to communicate and exchange data seamlessly and in a standardized manner (Akintoye, 2025). For example, from a more technical and functional perspective, especially in

the context of the web, APIs are the mechanism that enables multiple applications to share data and interact through structured HTTP requests (Akintoye, 2025). During the evolution of web services, APIs emerged to meet the demands of seamless connectivity and rapid data exchange (Jaiswal, 2025).

Among the essential functions of an API in modern software architecture are (Akintoye, 2025; Garimilla, 2024):

- Promoting efficiency: Allow developers to integrate existing systems rather than building everything from scratch, saving time and resources.
- Enabling connectivity: Make it possible for systems built with completely different technologies and platforms to work together.
- Driving innovation and modularity: Offer tools to build creative solutions and compartmentalize functionalities, making software more flexible, scalable, and maintainable.
- Accelerating development: By simplifying integration, they reduce complexity and development cycles.

APIs use the Simple Object Access Protocol (SOAP) for its robustness, security, and standardization, especially in complex business environments. This is the oldest and most rigid protocol, based on XML messaging. It is characterized by strict communication standards, formalized contracts, and robust security features, being common in enterprise-level applications. However, its complexity often slowed down development (Akintoye, 2025; Jaiwal, 2025).

SOAP is largely considered a legacy technology, and the digital ecosystem has experienced a clear evolution from SOAP toward REST architectures. This transition was driven by the need for more agile, lightweight, and scalable solutions, especially with the rise of mobile applications and cloud services. Its key principles are the use of standard HTTP methods (GET, POST, PUT, DELETE); stateless communication, where each request contains all the necessary information to be processed; the use of lightweight data formats, particularly JSON; and it is highly scalable and simpler to implement (Akintoye, 2025; Jaiswal, 2025).

Currently, GraphQL is cited as an emerging trend and as an alternative to REST, since its main advantage is flexibility: it allows clients to request only the data they need, avoiding information overload (Jaiswal, 2025). To obtain and handle data, RESTful APIs are organized around two fundamental concepts (Akintoye, 2025):

1. Resource: It is the central object. A resource represents any data or object that can be accessed or manipulated, such as a user, a product, a post, or a book. Each resource is identified by a unique URI, which is the address to access it.
2. Endpoint: It is the specific URL where a resource can be accessed to perform an operation. An endpoint combines the server's base URL, the resource path, and an HTTP method to define an action.

Interaction occurs when a client sends a request to an endpoint, and the server returns a representation of the resource, commonly in JSON format.

Today, the role of APIs in web, mobile, and Software as a Service (SaaS) applications is to be the backbone that sustains modern applications. The evolution toward microservices architectures and cloud-native applications was driven by RESTful APIs. APIs allow decoupling system components, making it easier for different teams to develop and deploy them independently. In the cloud environment, RESTful APIs are ideal because they consume fewer computational resources and simplify horizontal scaling on platforms like Kubernetes. In contrast, mobile applications require fast and efficient data exchange to offer a good user experience. RESTful APIs, with their lightweight data (JSON) and lower latency, are much more suitable for this purpose (Jaiswal, 2025).

TM Forum Application Programming Interfaces

TM Forum Open APIs are the mechanism that allows all ODA blocks and components to connect and function as a unified and stable system (Hou et al., 2024; TM Forum, 2021a).

ODA is TM Forum's reference architecture framework, designed to replace monolithic systems with a collection of decoupled software

components. Its main objective is to enable Internet service providers to operate as agile digital enterprises, similar to large technology companies (Hou et al., 2024; TM Forum, 2021a).

TM Forum Open APIs have a RESTful API architectural style in JSON format defined with OpenAPI Specifications (OAS) and are used for the orchestration and management of services and resources between Business Support Systems and Operations Support Systems (BSS/OSS) (TM Forum, 2025b). These fulfill two essential functions within the ODA (TM Forum, 2021a):

- Standardized component interfaces: They define the reference interfaces through which ODA components (residing in functional blocks) expose their functionalities externally and communicate with each other. This API exposure approach is what allows the architecture to be platform-based and encourages agile evolution.
- Interoperability enabler: By being standardized, the APIs allow components from different providers or internal, proprietary, or legacy systems to connect and work together, drastically reducing integration complexity and cost.

The success of Open APIs lies in the fact that they are not just technical interfaces, but are anchored to TM Forum reference frameworks. Each Open API is based on a business information object defined in TM Forum's Information Framework (SID). This common semantic foundation ensures that, regardless of the provider, the business concept exchanged is consistent and universal. Furthermore, they map the functions of ODA blocks to business processes defined in eTOM, ensuring that the interfaces support end-to-end business workflows (V. P. Mochalov et al., 2019; TM Forum, 2021).

In practice, Open APIs are essential for digital transformation, especially in the areas of orchestration, automation, and virtualization. In the context of an ODA implementation, the APIs are used to interconnect the business management level with the network production level, for example, to automate the provisioning of a connectivity service.

Threats Exposing TM Forum Open APIs

The document IG1187 ODA Enterprise Risk Assessment v2.0 identifies a set of relevant security threats by adopting the STRIDE+P model, which encompasses the categories of spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege, and privacy risks. Each of these threats constitutes a critical axis in the risk management of open platforms, as they compromise the confidentiality, integrity, and availability of services, in addition to regulatory compliance regarding personal data protection (TM Forum, 2021b).

In particular, spoofing relates to attacks where a malicious actor impersonates a legitimate user or system; tampering involves the alteration of information in transit or at rest; repudiation reflects the absence of traceability and logging that allows denying performed actions; and information disclosure corresponds to the exposure of sensitive user or company data. Likewise, denial of service seeks to interrupt resource availability through overload, elevation of privilege allows an attacker to obtain unauthorized access, and the privacy category emphasizes the risks of regulatory non-compliance, particularly in relation to the General Data Protection Regulation (TM Forum, 2021b).

More specifically for the context of TM Forum Open APIs, the document highlights that programming interfaces constitute the main attack surface and recommends adopting as a reference the threats described in the OWASP API Top 10 (2019). These include broken object-level authorization, broken authentication, excessive data exposure, lack of resource or consumption control, broken function-level authorization, uncontrolled attribute mass assignment, insecure configurations, injection vulnerabilities, improper asset and version management, and lack of effective logging and monitoring (TM Forum, 2021b).

Within this set, the most critical threats for TM Forum Open APIs are those that directly impact authentication, authorization, and data protection. In particular, excessive data exposure constitutes a central risk by potentially revealing personal or confidential information

beyond what is strictly necessary. Deficient authentication and authorization facilitate improper access to sensitive objects or functions, while the absence of consumption controls and version management increases vulnerability to denial-of-service attacks. In this sense, TM Forum's risk assessment framework shows that the security of Open APIs depends on the combination of a structured threat analysis under STRIDE+P and the systematic adoption of the best practices proposed by OWASP for open APIs (Ariami *et al.*, 2024; Nikolov & Aleksieva-Petrova, 2025; TM Forum, 2021b).

Vulnerabilities of TM Forum Open APIs

The most common vulnerabilities in TM Forum Open APIs coincide with those described in the OWASP API Top 10 from 2019, according to IG1187 ODA Enterprise Risk Assessment v2.0; although this guide references the 2019 list, the author will adopt the 2023 list, which is the latest stable version (Mazzei *et al.*, 2025; OWASP, 2023; Sharma, 2025):

1. Broken Object Level Authorization (BOLA): APIs often expose object identifiers that can be manipulated by an attacker.
2. Broken Authentication: It occurs when authentication mechanisms are not implemented securely.
3. Broken Object Property Level Authorization: When an API returns or allows modification of more fields than necessary, or lacks per-field controls, it can expose or alter sensitive data.
4. Unrestricted Resource Consumption: If the API does not limit the number, size, or frequency of requests, system performance can be exhausted, leading to denial-of-service (DoS) or cost overruns.
5. Broken Function Level Authorization: It appears when administrative or high-privilege functions are not properly restricted. Attackers can execute actions that should be reserved only for certain roles.
6. Unrestricted Access to Sensitive Business Flows: Even if there are no technical vulnerabilities, attackers can abuse the business logic exposed by the API.

7. Server-Side Request Forgery (SSRF): It occurs when an API allows the user to indicate external or internal URLs without validation, causing the server to make malicious requests.
8. Security Misconfiguration: It includes errors in HTTP headers, permissions, CORS policies, insecure versions, enabled debug endpoints, or exposed keys.
9. Improper Inventory Management of APIs: Organizations often lose control of how many APIs have active, their versions, and what data they access.
10. Unsafe Consumption of APIs: When an application consumes external APIs without verifying their authenticity, without validating responses, or without controlling dependencies, it can become a victim of attacks.

Many TM Forum APIs operate complex business flows, interoperability with third parties, multiple versions, and varied consumption scenarios. Vulnerabilities such as unrestricted access to sensitive business flows and unsafe consumption are especially pertinent. In this case, there is no specific information indicating which of the aforementioned vulnerabilities affect TM Forum Open APIs, so this research will attribute these same vulnerabilities as expressed in the OWASP Top 10 (Friman *et al*., 2023; V. Mochalov *et al*., 2019; V. P. Mochalov *et al*., 2020; Smidovych & Davydovskyi, 2022).

Security and Management Policies for TM Forum Open APIs

Security in Open API implementation must be addressed under a comprehensive approach that contemplates both design principles and technical and management mechanisms. It is assumed that the environment is hostile, so no request should be considered trustworthy by default. For this purpose, every design, protocol, or API must undergo a formal threat modeling and risk assessment process, which allows identifying the attack surface and defining appropriate mitigation measures (Ohtani *et al*., 2021; Ranjan *et al*., 2022; TM Forum, 2017).

A key aspect is the delimitation of trust boundaries, with minimization of interface exposure only to those necessary for the

business, and applying a granular authorization model after robust authentication. Such authentication must be protected through cryptography, mandatory for all accesses, cannot be disabled, and must be recorded in immutable logs. Likewise, authorization must be applied after authenticating, ensuring that each user, system, or platform only accesses the services and data that correspond to them (Christian Chukwuemeka Ike *et al*., 2021; Jangam *et al*., 2022; Lafarga Poyo, 2025; TM Forum, 2017).

Data protection is a comprehensive concept and its application must be ensured both in transit and at rest, as well as during processing, avoiding insecure channels and using encryption at all times. Similarly, it is recommended to segment services into multiple defense layers to contain potential breaches, design platforms free of single points of failure, and apply secure configurations by default (Babu, 2025; Gambo & Almulhem, 2025; Horbenko, 2025; Micheal, 2025; Gambo & Almulhem, 2025).

In multi-user or multi-company environments, it is essential to ensure isolation between tenants through physical, virtual, or logical mechanisms, so that a compromise does not affect others. The design must also provide for maintainability, allowing updates and coexistence of API versions without compromising security, in addition to guaranteeing the integrity and provenance of components through protected inventories and cryptographic trust chains (TM Forum, 2017).

Likewise, privacy protection, especially of personally identifiable information, must be integrated from the start in compliance with regulations such as the General Data Protection Regulation (GDPR), incorporating data minimization, access control, consent management, and traceability practices (Sun *et al*., 2022; TM Forum, 2017).

Regarding security policy management, each platform defines its own domain and trust boundary, with the exposed APIs being the attack surface to protect. This requires the implementation of federated access control mechanisms, multi-factor authentication —at least two factors for sensitive data—, assignment of policies to roles and users,

as well as the distribution and execution of said policies at decision and enforcement points within the platform (Fernández-Martínez *et al*., 2024; Lefebvre *et al*., 2021; TM Forum, 2017).

As a technological reference, the Software-Defined Perimeter (SDP) model is proposed as an exemplary mechanism by allowing services to be hidden, establishing end-to-end encrypted connections, and simplifying the management of authentication, authorization, and access control. This model is based on three main components: the SDP client, responsible for verifying identity and device; the SDP controller, acting as a trusted intermediary configuring access in real-time; and the SDP gateway, ensuring encrypted termination close to the protected services (Fernández-Martínez *et al*., 2024; Lefebvre *et al*., 2021; TM Forum, 2017).

In this way, Open APIs are not only protected against common attacks such as DDoS, Man-in-the-Middle, OWASP Top 10, or advanced persistent threats, but also align with a systematic security framework that includes the definition of trust boundaries, threat identification, assessment and quantification of residual risks, and establishment of access policies adapted to each domain (Christian Chukwuemeka Ike *et al*., 2021; Min *et al*., 2022; Sun *et al*., 2022; TM Forum, 2017).

Taxonomy of Threats and Vulnerabilities in TM Forum Open APIs

Based on the document analysis described in the PRISMA methodology, a gap was identified in the specialized literature: the absence of a correlation model that integrates the threat categories of the STRIDE+P model, the vulnerabilities of the OWASP API Security Top 10, and the specific components of the ODA architecture. To fill this gap, a proprietary taxonomy of threats and vulnerabilities was designed through a manual cross-correlation process.

The construction of the taxonomy followed four methodological steps:

- Disaggregation of sources. The 7 categories of the STRIDE+P model were extracted from IG1187 ODA Enterprise Risk Assessment

v2.0.0 (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Privacy Risks) and the 10 vulnerabilities of the OWASP API Security Top 10 2023.

- Logical correlation. Links were established between each STRIDE+P category and the OWASP vulnerabilities susceptible to materializing that threat in a RESTful API context. Only correlations with explicit technical foundation in the analyzed documentation were recorded.
- Mapping to ODA components. Each validated correlation was assigned to the functional component of the ODA architecture where the vulnerability would have the greatest impact.
- Severity ranking. Own evaluation criteria were applied: impact on telecom service continuity, exposure of personal or financial data, detection complexity, and alignment with regulatory requirements. Severity was classified as Critical, High, Medium, and Low.

The resulting taxonomy, presented in Table 2, identifies 17 significant correlations between the 7 STRIDE+P categories and 9 of the 10 OWASP 2023 vulnerabilities. The vulnerability identifiers correspond to the numerical value assigned in the vulnerabilities section of this paper.

Table 2. Taxonomy of Threats and Vulnerabilities of TM Forum Open APIs

STRIDE+P Category	OWASP 2023 Vulnerability	Affected ODA Component	Severity	Justification
Spoofing	VUL_API2	API *Gateway*	Critical	Identity compromise at the main entry point of the ecosystem.
	VUL_API8	Identity management	High	Incorrect configuration of federated identity providers.
Tampering	VUL_API1	Resource Inventory	Critical	Manipulation of network resource inventory identifiers.
	VUL_API3	Product Catalog	High	Alteration of cataloged product and service properties.
	VUL_API7	Orchestration Services	High	Modification of internal orchestration flows through forced requests.
Repudiation	VUL_API8	Monitoring and Logging	Medium	Lack of traceability of critical actions due to deficient configuration.
	VUL_API9	API Inventory	Medium	Lack of record of exposed APIs prevents forensic auditing.
Information Disclosure	VUL_API1	Customer Management	Critical	Exposure of customer data due to broken object-level authorization.
	VUL_API3	Group Management	Critical	Filtering of personal data due to over-exposure of properties.
	VUL_API6	Billing and Revenue	High	Revelation of sensitive financial information through unprotected

STRIDE+P Category	OWASP 2023 Vulnerability	Affected ODA Component	Severity	Justification
				flows.
Denial of Service	VUL_API4	API *Gateway*	Critical	Gateway overload due to massive resource consumption without control.
	VUL_API7	Network Exposure	High	Attack on internal infrastructure from externally exposed API.
Elevation of Privilege	VUL_API1	Access Control	Critical	Horizontal privilege elevation between objects of the same level.
	VUL_API5	Administrative APIs	Critical	Access to administrative functions without role authorization.
	VUL_API6	Partner Ecosystems	High	Abuse of business flows to obtain elevated access in multi-partner ecosystem.
Privacy Risks	VUL_API3	Customer Profile	Critical	Exposure of PII violating GDPR and PCI-DSS standards.
	VUL_API9	Consent Management	High	Loss of traceability of user consent for data processing.

The analysis reveals that 47% of the correlations present Critical severity, concentrated in three axes: information disclosure, elevation of privilege, and denial of service. The taxonomy allows identifying the components with the highest number of Critical or High severity correlations. In this case, the API Gateway emerges as the most critical component. This finding justifies TM Forum's recommendation to implement SDP and Zero Trust mechanisms at the access perimeter.

Unlike the original STRIDE model, the STRIDE+P extension explicitly incorporates privacy risks. The taxonomy demonstrates that the Privacy category does not operate in isolation, but rather manifests itself mainly through the API3 vulnerability in the Customer Profile and Consent Management components. This suggests that the protection of personal data in TM Forum Open APIs cannot be addressed solely with access controls, but requires field-level data schema validation and data minimization mechanisms from its design.

Two methodological limitations are recognized: the correlation is based on document analysis, without empirical validation through penetration testing in real implementations of TM Forum Open APIs; and the assigned severity is relative to the telecommunications context and may vary in specific implementations. These limitations define the future work proposed in the conclusions.

Conclusions

The study of the security of TM Forum Open APIs evidences the growing need to address the vulnerabilities inherent to this type of

architecture. The study revealed the existence of significant threats that expose these programming interfaces. Particularly, the vulnerability analysis highlighted the criticality of the risks associated with these interfaces. The open nature of these APIs, designed to foster interoperability and innovation in the telecommunications sector, simultaneously introduces exposure points that can be exploited by malicious agents.

That is why, within TM Forum's security recommendations and also those from OWASP, they mainly indicate that every API must undergo a formal threat modeling and risk assessment process, which allows identifying the attack surface and defining appropriate mitigation measures. The method proposed for threat modeling in security frameworks is STRIDE+P according to IG1186, IG1187, and IG1195, and the systematic adoption of the best practices proposed by OWASP for Open APIs.

Part of these good practices are taken into account in projects and regulations such as the OWASP API Security Project, the OWASP Application Security Verification Standard (ASVS), and the NIST SP 800-228, 800-63, and 800-53 Rev 5 series. These resources provide a comprehensive framework for designing and implementing security controls that address the most common and critical vulnerabilities in environments such as those where TM Forum Open APIs converge. Therefore, they must be taken into account when selecting security controls for this type of API.

This taxonomy constitutes an empirical foundation for the development of future specific security frameworks for TM Forum Open APIs. This correlation model allows locating specific architectural threats, prioritizing controls by component, and sizing the regulatory impact based on the type of exposed data.

Bibliographic References

Akintoye, A. (2025). *API Development with Laravel: A Quick Start Guide*. Apress. https://doi.org/10.1007/979-8-8688-1576-8

Ariami, D., Windarta, S., Priambodo, D. F., & Amiruddin, A. (2024). Combining STRIDE and Penetration Testing for Improved Web Application Security: A Case Study on Stored XSS Vulnerabilities. 2024 *Beyond Technology Summit on Informatics International Conference* (BTS-I2C), 332-337. https://doi.org/10.1109/BTS-I2C63534.2024.10942270

Babu, M. (2025). *Enhancing Cloud Security: Implementing and Evaluating the Zero Trust Architecture with Firebase Services and Advanced Encryption Algorithms* [Masters, Dublin, National College of Ireland]. https://norma.ncirl.ie/7426/

Christian Chukwuemeka Ike, Adebimpe Bolatito Ige, Sunday Adeola Oladosu, Peter Adeyemo Adepoju, Olukunle Oladipupo Amoo, & Adeoye Idowu Afolabi. (2021). Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. *Magna Scientia Advanced Research and Reviews*, 2(1), 074-086. https://doi.org/10.30574/msarr.2021.2.1.0032

Csoma, M.-I., Koné, B., Botez, R., Ivanciu, I.-A., Kora, A., & Dobrota, V. (2020). *Management and Orchestration for Network Function Virtualization: An Open Source MANO Approach*. 2020 19th RoEduNet Conference: Networking in Education and Research (RoEduNet), 1-6. https://doi.org/10.1109/RoEduNet51892.2020.9324847

Donegan, P. (2023). *Cybersecurity strategies: Risk management moves firmly into the telco spotlight*. https://inform.tmforum.org/research-and-analysis/reports/cybersecurity-strategies-risk-management-moves-firmly-into-the-telco-spotlight

Fernández-Martínez, C., Bikos, A., Verikoukis, C., & Siddiqui, S. (2024). *Trusted Access to 6G Testbeds Through a Security Intent-Driven Software-Defined Perimeter Framework*. 2024 IEEE 29th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 1-6. https://doi.org/10.1109/CAMAD62243.2024.10942785

Gambo, M. L., & Almulhem, A. (2025). Zero Trust Architecture: A Systematic Literature Review. *Journal of Network and Systems Management*, *34*(1), 25. https://doi.org/10.1007/s10922-025-09998-x

Garimilla, M. (2024). THE ART OF API DESIGN: BEST PRACTICES FOR MODERN SOFTWARE DEVELOPMENT. *International Journal of Engineering and Technology Research (IJETR)*, *9*(2), 229-239. https://doi.org/10.5281/ZENODO.13772395

Horbenko, Y. (2025). Secure Front-End Automation Framework: A Novel Approach to Client-Side Data Encryption and Zero Trust API Interaction. *Asian Journal of Research in Computer Science*, *18*(6), 177-193. https://doi.org/10.9734/ajrcos/2025/v18i6690

Hou, X., Zhao, Y., & Wang, H. (2024). *Voices from the Frontier: A Comprehensive Analysis of the OpenAI Developer Forum*. arXiv. https://doi.org/10.48550/arXiv.2408.01687

Jaiswal, I. A. (2025). *THE EVOLUTION OF WEB SERVICES AND APIS: FROM SOAP TO RESTFUL DESIGN*. 14.

Jangam, S. K., Karri, N., & Muntala, P. S. R. P. (2022). Advanced API Security Techniques and Service Management. *International Journal of Emerging Research in Engineering and Technology*, *3*(4), 63-74. https://doi.org/10.63282/3050-922X.IJERET-V3I4P108

Lafarga Poyo, F. (2025). *Zero trust framework for microservices security: Analysis, design, and implementation*. https://hdl.handle.net/20.500.14468/29428

Lefebvre, M., Nair, S., Engels, D. W., & Horne, D. (2021). *Building a Software Defined Perimeter (SDP) for Network Introspection*. 2021 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), 91-95. https://doi.org/10.1109/NFV-SDN53031.2021.9665152

Mazzei, C., Firoamant, D., Quagliarini, A., Salatino, C., Reale, A., & Brunetti, F. (2025). *The Open Chain Framework for the "Management by Projects" in Fiber-only Network Wholesale Telcos*.

Micheal, D. (2025). *Digital Identity and Privacy in API-Driven Environments: Combining Blockchain, Cryptography, and Forensic Techniques*.

Min, N. M., Visoottiviseth, V., Teerakanok, S., & Yamai, N. (2022). OWASP IoT Top 10 based Attack Dataset for Machine Learning. 2022 24th *International Conference on Advanced Communication Technology (ICACT)*, 317-322. https://doi.org/10.23919/ICACT53585.2022.9728969

Mochalov, V. P., Bratchenko, N. Yu., & Yakovlev, S. V. (2019). Process-Oriented Management System for Infocommunication Networks and Services Based on TM Forum Frameworx. 2019 International Russian Automation Conference (RusAutoCon), 1-6. https://doi.org/10.1109/RUSAUTOCON.2019.8867619

Nikolov, L., & Aleksieva-Petrova, A. (2025). *Threat modeling based on STRIDE framework for web application*. AIP Conference Proceedings, 3308(1), 030007. https://doi.org/10.1063/5.0272341

Ohtani, M., Omata, S., & Kanishima, K. (2021). Development of Reference Model for Enterprise Architecture Leveraging TM Forum Assets. 2021 22nd Asia-*Pacific Network Operations and Management Symposium (APNOMS)*, 210-213. https://doi.org/10.23919/APNOMS52696.2021.9562626

OWASP. (2023). *OWASP API Security Project* | OWASP Foundation. https://owasp.org/www-project-api-security/

Ranjan, P., Khunger, A., Veera, C., Satya, V., & Dahiya, S. (2022). *Threat Modeling and Risk Assessment of APIs in Fintech Applications*. 2, 44-61. https://doi.org/10.56472/25832646/JETA-V2I2P108

Salt. (2025). Salt Security: *State of API Security Report*. https://content.salt.security/Gartner-Voice-of-the-Customer.html

Sharma, A. (2025). *5G APIs security and privacy threat analysis within 5G technology domain*. https://urn.kb.se/resolve?urn=urn:nbn:se:his:diva-25387

Sun, R., Wang, Q., & Guo, L. (2022). *Research Towards Key Issues of API Security*. En W. Lu, Y. Zhang, W. Wen, H. Yan, & C. Li (Eds.), Cyber Security (pp. 179-192). Springer Nature. https://doi.org/10.1007/978-981-16-9229-1_11

TM Forum. (2017). *Platform Security and Policy Management R17.0.1* (TR263D) – TM Forum. https://www.tmforum.org/resources/technical-report/tr263d-platform-security-and-policy-management-r17-0-1/

TM Forum. (2021a). IG1167 ODA Functional Architecture Exploratory Report v5.1.0. *TM Forum*. https://www.tmforum.org/resources/exploratory-report/ig1167-oda-functional-architecture-exploratory-report-v5-1-0/

TM Forum. (2021b). IG1187 ODA Enterprise Risk Assessment v2.0.0. *TM Forum*. https://www.tmforum.org/resources/standard/ig1187-oda-enterprise-risk-assessment-v2-0-0/

TM Forum. (2025a). About TM Forum | *TM Forum*. https://www.tmforum.org/about/

TM Forum. (2025b). *OpenAPI Directory*. https://www.tmforum.org/oda/open-apis/directory

RESEARCH

From the Data Center to the Service: Extending the Tier Model

Ernesto Carrazana Ruiz, Eng. [1*],
Irisleidis Lázara Casi Estevanell, Eng [2],
Héctor Manuel Jacas Joa, Eng.[3]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

The guidelines for the design and implementation of data centers are extensively documented, providing a high level of detail in every aspect to consider for infrastructure deployment. However, this is not the case regarding the design of redundancy for IT services. Therefore, this article proposes an adaptation of the Uptime Institute's Tier model for IT services, supported by the best design practices. As case studies, ETECSA's Web Hosting platforms were employed as examples of optimization, high availability, and security. In any IT service, resource optimization and digital security represent two essential pillars in the pursuit of achieving 100% availability. This article may be of interest to those seeking guidance in the design of resilient and secure IT services.

Keywords: Threats in Open API, ODA, Open API, TM Forum Open APIs, Open API Security

[1*] Engineer. Empresa de Telecomunicaciones de Cuba S.A (ETECSA). Postal address: 11300. ernesto.carrazana@etecsa.cu

[2] . Engineer. Empresa de Telecomunicaciones de Cuba S.A (ETECSA). Postal address: 11300. irisleidis.casi@etecsa.cu

[3] Engineer. Empresa de Telecomunicaciones de Cuba S.A (ETECSA). Postal address: 11300. hector.jacas@etecsa.cu

Introduction

Cuba regulates Information and Communication Technologies (ICTs) in Decree-Law No. 370/2017 (Gaceta Oficial No 45 Ordinaria de 4 de julio de 2019 [1]), specifically defining them in Article 3 of Chapter 1: "Information and Communication Technologies, hereinafter ICTs, are defined as the set of resources, tools, equipment, computer programs and applications, networks, and media that allow the compilation, processing, storage, and reception of information in any format: voice, data, text, video, and images." ICTs security is regulated in Decree-Law No. 360/2019. (Gaceta Oficial No 45 Ordinaria de 4 de julio de 2019). Both decrees outline in great detail the use and security of ICTs in Cuban society; however, they do not include any standard, requirement, or regulation for the design and implementation of redundancy and the consequent level of availability of computer services generated with ICTs.

Internationally, the Uptime Institute, creator and certifier of the Tier model, lists on its website the Tiers (levels) according to the scope and characteristics of data centers, reflected in the annual availability level in percentage (Tier Certification, Uptime Institute, 2025). Each tier reflects a set of requirements associated with a specific maximum allowable service disruption time. The following is a summary of some of the main requirements of this model:

- Tier I: the lowest level, it includes small backup systems for office work. It requires backup power, climate control, and a designated location.
- Tier II: it includes all the parameters of Tier I in addition to greater redundancy and electrical generation capacity.
- Tier III: it includes all the parameters of Tier II in addition to high tolerance to faults and interruptions.
- Tier IV: it includes all the parameters of Tier III in addition to several independent systems, so that the effects are always partial.

ETECSA's Public Data Centers meet Tier III standards, meaning that any Virtual Data Center client benefits from high security and availability by default. However, this does not guarantee that the services

[1] Official Gazette No. 45, Ordinary Edition, July 4, 2019

deployed on the infrastructure will have the same fault tolerance. This article proposes an extension of the Tier model by extrapolating concepts from the physical environment to the realm of IT services, aiming to provide a classification for redundancy and availability levels, as well as establish how to improve these parameters.

Materials and Methods

The extension of the Uptime Institute Tier model which is being proposed in this article takes into account, among other aspects, energy backup and climate control, as these fall under a lower level of responsibility. Therefore, the Tier model can be extended as follows:

- Tier I: Low-resource IT services intended for redundancy and backup. The servers are neither specialized nor segmented. Indefinite outages and permanent data loss are possible due to system corruption or failure.
- Tier II: Medium-resource IT services designed for redundancy and backup. Multi-node designs with specialized, segmented, and redundant servers. Deployed operating systems and applications must be maintained and updated. Indefinite outages and permanent data loss are possible in the event of destruction or corruption of the physical systems.
- Tier III: It includes all the parameters of Tier II in addition to the performance of geographically cross-referenced protection operations (backups), so that in the event of physical destruction of the data center or corruption of the systems, information is not lost and a total restoration is possible, although in this scenario there will be a prolonged service interruption.
- Tier IV: Increases the replication capacity and high geographic availability (or geo-redundancy) of Tier III, creating a multi-site service where each site is a complete service operating in active-active or active-passive configurations. This requires a high consumption of redundancy resources. Implementing this scheme results in a low probability of data loss and service interruptions.

Overview

Just as designing a data center requires analyzing the characteristics of the intended space and the types of servers to be acquired, a similar analysis is equally useful for deploying an IT service. It is essential to understand the types of CPUs, storage, the presence or absence of GPUs, and the technology that orchestrates virtualization, if it is a virtualized infrastructure. The presence of GPUs is a prime example that influences decision-making in today's world, given their significant impact on artificial intelligence systems; in their absence, it becomes crucial to analyze the feasibility of replacing them with CPUs.

Once the environment and type of service to be deployed are understood, the next step is to determine the desired level of redundancy within the extended Tier model proposed in this article, based on the system's criticality. The aspects to consider can be summarized as follows:

- CPU: CPU speed and allocation type. In virtualized environments, this generally refers to virtualized CPUs, which do not necessarily have to be a 1:1 representation of the physical CPU speed.
- Storage: This refers to the type of physical hard drive (HDD, SSD, or any other designation). This way, it is possible to make plans—for example, to reserve SSD storage for applications with high read and write demands, such as a database.
- GPU: The presence of a GPU is fundamental when attempting to deploy an artificial intelligence system.
- Technology that orchestrates virtualization: It is important to know the technology used to manage the environment (if it is virtualized), as these technologies differ in their characteristics despite sharing the same design principles. Examples: OpenStack, Proxmox, and VMware vCloud Director.
- Redundancy: it is important to estimate the consumption of resources allocated to backups and the resources allocated to replicating the different nodes of the system.

- Network interfaces: it is necessary to know the bandwidth of the network interfaces, as high network consumption can cause bottlenecks.

Connectivity

A good network design and a robust firewall policy simplify administration and reduce the likelihood of errors. Even minor changes to connectivity can lead to significant service disruptions. Virtualization services provide firewall and router mechanisms, as well as a virtualized networking system overall.

The three main measures in terms of connectivity are network segmentation, the implementation of a standardized, easily understood nomenclature in the management environment, and the restriction of access to only those that are necessary.

Segmenting traffic by network interfaces serves two purposes. The first, and most important, is security. Using different networks that support different protocols makes it harder for a security breach to occur and limits an attacker's ability to cause damage. The second is the potential for bottlenecks if the network interfaces have low bandwidth. To avoid them, traffic types need to be isolated, allowing them to run in parallel. Examples of network segmentation are presented below:

- Administration Network: This network is provided to each server and it is intended to allow remote access by system administrators. Accessing this network via a VPN is recommended. Under normal circumstances, it has low bandwidth consumption.
- Containment Network: In environments where a firewall or router is required, service providers sometimes do not offer all the required functionalities; this network layer is implemented to isolate the Management Network, and can be orchestrated by different applications, for example pfSense (pfSense, 2025).
- Service Network: This layer is recommended for providing public services, ensuring that only edge servers are directly exposed to the internet. Under normal circumstances, it has moderate bandwidth consumption.

- Data Network: This layer handles the highest traffic volume; therefore, isolation from external access is recommended. If necessary, it could be segmented into specific networks, such as the database network or storage network.
- Public Network: Internet access network. With a single IP address, it's possible to use NAT to segment and isolate published services. For example, only allowing ports 80 and 443 for access to a website.
- Multi-Site Replication Network: If the goal is to achieve Extended Tier IV and the infrastructure lacks a native replication method, this network must be implemented at each site and linked via a VPN for enhanced security. This ensures secure an efficient data replication, as it avoids competing with other protocols for bandwidth.

Redundancy and Availability

Achieving maximum availability requires high levels of redundancy. A service with low redundancy is more susceptible to reduced uptime due to minor issues. Therefore, the following best practices are outlined for achieving high redundancy while optimizing resources:

- Multiple servers: Deploying each application on at least two independent servers allows for hot deployment of changes and provides fault tolerance.
- Data applications: Some applications, such as storage or database applications, require at least three servers to function correctly, as they must avoid split-brain mode. In this state, with an even number of servers, the cluster is unable to determine the correct data if 50% of the servers contain one piece of data and the other 50% contain another. Therefore, it is recommended to scale these types of services horizontally to ensure an odd number of servers.
- Load balancing: Presenting multiple paths in the flow requires implementing load balancers. When properly implemented and optimized, they are a powerful tool, as they allow for traffic moderation and the full utilization of the resources being balanced.

- Multi-node system challenge: Implementing a multi-node system with load balancing can cause undesirable behavior in some applications, requiring an additional layer to address this issue. For example, multiple PHP nodes can lead to session loss if a caching system like Redis or Memcached is not in place.
- Data replication: It can become complex and resource-intensive. For example, if the static content of a website were stored on five web servers, with all nodes active, it would be necessary to store this static content five times and, in addition, implement a multi-node replication system. The solution to this problem is a centralized storage system, accessible via the network, for example, using the NFS protocol.
- Network replication: This process can become challenging if the network parameters required by the replication application are not available. Therefore, the system design must consider the feasibility of synchronous replication (data must be correctly replicated across all nodes before proceeding) or asynchronous replication (data is replicated according to a planned schedule).
- Infrastructure replication: replication can be guaranteed by the infrastructure itself with native equipment replication systems.
- Global load balancing: In an Extended Tier IV scenario, load balancing between regions poses a challenge. Choosing a solution that is appropriate to the environment in which the platform is deployed is vital for the proper functioning of this complex design.
- Backup system: both data and the servers themselves must be protected. It is advisable to treat these two schemes differently, as it is not always appropriate to restore an entire server if restoring the data can resolve the service disruption. Likewise, it is advisable to plan different backup retention and execution periods for different servers; for example, a database should be protected more frequently than a web server.

Servers and Applications

Server specialization is desirable for many reasons, but the main one is application isolation, which facilitates system maintenance

and updates and adds an extra layer of security. The following sections will discuss factors that must be taken into account when designing and deploying some of the most widely used systems and applications:

- Load balancers: Among the many options, NGINX, Apache, and HAProxy stand out. Their respective documentation can be found in the references (nginx, 2025), (Apache HTTP Server Project, 2025), and (HAProxy, 2025). HAProxy excels over the competition thanks to its robustness, speed, versatility, and features. Generally speaking, HAProxy can be the solution for any load balancing need.
- Storage: The need for distributed storage increases in redundant environments. Solutions like GlusterFS and Ceph (GlusterFS, 2025; Ceph, 2025) allow for storage in the form of NFS or another protocol required by the applications being implemented. In the examples presented, the choice between one over the other depends on the size of the system. GlusterFS has a shorter learning curve but fewer features; conversely, Ceph offers a highly complex and versatile implementation.
- Web servers: NGINX and Apache are currently the most popular options for this purpose. Both are similar in performance and functionality; choosing one or the other will depend on small details such as the existence of the ".htaccess" file in Apache, which allows for hot deployment of changes.
- Memory caching: Redis and Memcached (Redis The Real-time Data Platform, 2025; Memcached—a distributed memory object caching system, 2025) are among the most widely used solutions today to enhance system performance. Both are easy to deploy, but only Redis offers replication capabilities in high-availability environments; however, these solutions consume significant resources.
- Firewall, router, VPN: The ideal solution is pfSense (pfSense, 2025) when all these functionalities are needed. It is a comprehensive tool, easy to deploy, with the possibility of being implemented in a high availability environment, even with facilities for multi-site environments.

- Databases such as MariaDB (MariaDB Foundation - MariaDB.org, 2025), PostgreSQL (PostgreSQL: The World's Most Advanced Open Source Relational Database, 2025), and many others are feasible options for deployment in the virtual realm; however, the determining factor is performance when it comes to forming a cluster, since the difficulty in deployment and network characteristics can cause a considerable deterioration in response time.
- Security mechanisms: Operating systems like Windows and Linux have built-in security mechanisms, such as firewalls and security policies. In the case of Linux, proper configuration of SELinux is crucial. This native security policy mechanism, if not configured correctly, can lead to undesirable situations in administration and service delivery. Additionally, if you intend to offer internet-facing services, it is advisable to implement a specialized web application security application, such as ModSecurity (ModSecurity Project, 2025).
- Server protection: Server protection should be automated, ideally using the tools provided by the infrastructure hosting the platform. If this isn't possible, at a minimum, virtual machines should be periodically downloaded and stored in a different location.
- Data protection: Data can be replicated using tools such as Rsync (rsync(1) - Linux man page, 2025) or Lsync (lsyncd, 2025), which allow data to be sent remotely to secure environments. For databases, periodical dumps can be run.
- Identity and access service: applications such as FreeIPA (FreeIPA - Identity, Policy, Audit - FreeIPA Documentation, 2025) or OpenLdap (OpenLdap, Main Page, 2025) are essential in environments with multiple administrators and/or users, as they enable centralized control of users and their roles across all systems.

Results and Discussion

Following the methodology outlined in this article, a design for a shared hosting platform will be presented below. This platform would be implemented using ETECSA's Virtual Data Center service.

The platform's overall vision is to offer a web hosting service to multiple clients, so that all websites share the same resources but in an isolated manner. The design was intended to place it at the Extended Tier III level, with technological decisions made with the goal of subsequently upgrading the platform to Extended Tier IV.

Five different networks are used in this design:

- Management network via VPN
- Public Network
- Service Network
- Data Network
- Authentication Network to isolate traffic from the identity service

The platform distributes its functionalities across the servers:

1. Firewall: I tis a service provided by the infrastructure. It constitutes the platform's first firewall, where IP and port control, as well as routing, are performed.
2. Load balancers: These constitute the platform's entry point and are implemented in active-passive mode. Their main function is carried out using the HAProxy service, which distributes traffic according to the type of connection established by clients (FTP, HTTP, HTTPS) and balances the load between servers that operate in active-active mode, such as balancing HTTP and HTTPS requests between the two web servers. Additionally, they provide a second layer of security due to the use of the Fail2Ban tool, designed to mitigate spam and DDoS attacks.
3. WAF (Web Access Firewall): As a third line of defense, the robust synergy between the NGINX service and the ModSecurity module is leveraged to process and detect malicious content in URLs that could lead to SQL injections or brute-force attacks. It also detects sensitive content and a number of minor vulnerabilities, providing the platform with high security and reliability.
4. Web servers: These are the platform's main servers, where the web page services run, using the Apache service in conjunction with multiple versions of PHP. Their design and implementation

allow the two servers dedicated to this function to work together to process all requests.

5. Maxscale: They take their name from the service they implement, a MariaDB-specific load balancing solution. They operate in active-passive mode and incorporate a caching service for database queries, which reduces response time and the load on the database cluster.
6. Database: These servers run MariaDB in a master-slave configuration for writes and an active-active configuration for reads. This dual standard reduces the possibility of data corruption and increases query speed.
7. FTP: FTP service implemented with vsftp, which can be used by the clients to manage the content of their sites.
8. IDM (Identity Manager): It is the platform's authentication service, which collects customer data and uses it on the web servers to restrict customers to their own directories, thereby preventing them from accessing other customers' content.
9. Centralized NFS service: It is provided by the Data Center, crucial to reducing the platform's disk space consumption, as it reduces the need to redundancy static site content and also handles generating backups.

Figure 1 shows a deployment diagram that brings together the servers, their components, and the interaction between them:

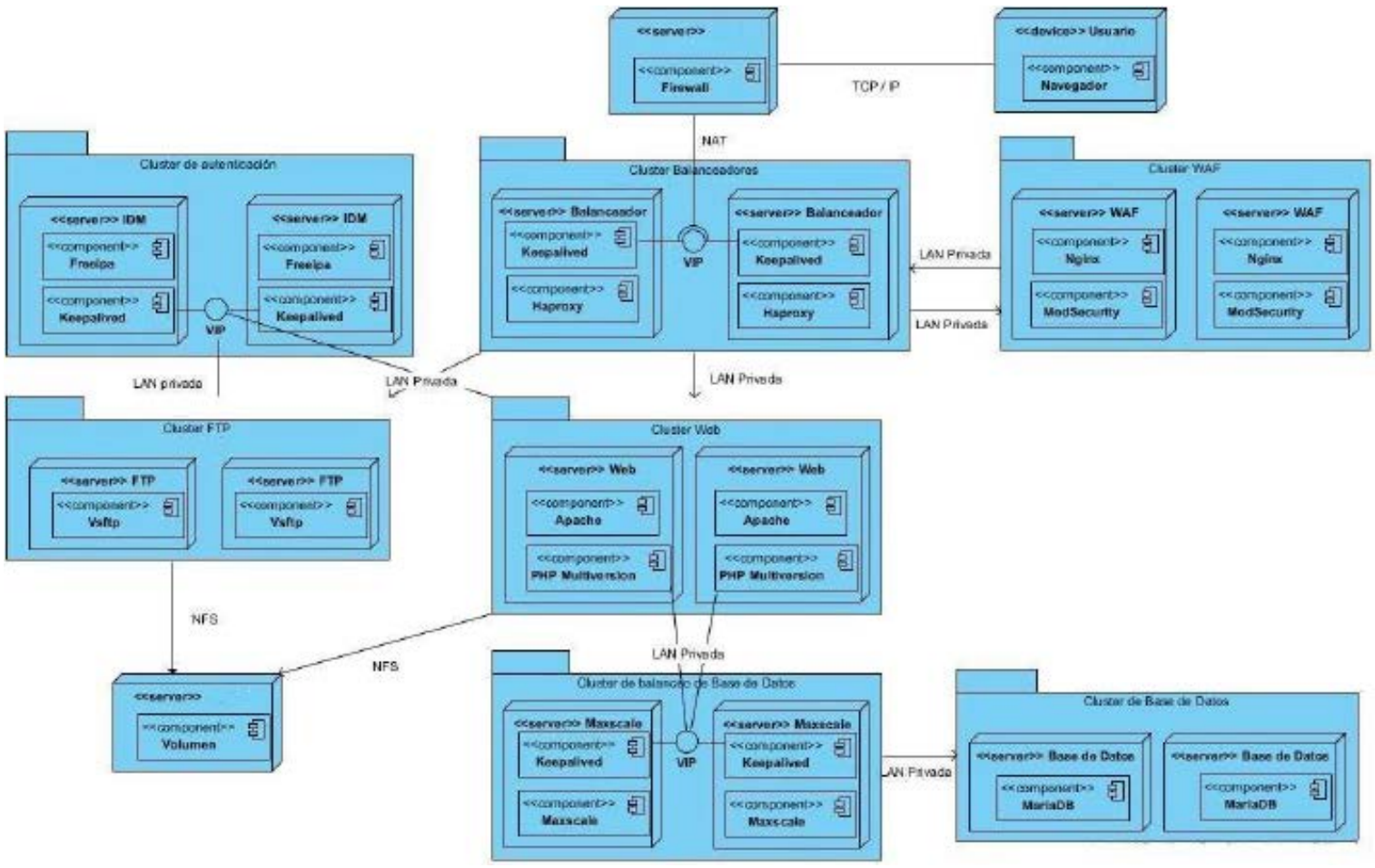


Figure 1. Deployment Diagram

After analyzing the graph in Figure 2, "Availability of ETECSA's Web Hosting Platforms in 2025 (%)," it is possible to demonstrates the effectiveness of the design and implementation of ETECSA's four web hosting platforms: Business Web Hosting (serving state clients), Individual Web Hosting (serving individuals and SMEs), GOB.CU (serving national priority websites), and the Press Information Center (CIP, designed to serve national digital newspapers). Their design closely resembles that described in this section. The availability times for CIP and GOB.CU are excellent, noting that CIP, due to its characteristics, belongs to the Extended Tier IV, while the other three platforms belong to the Extended Tier III.

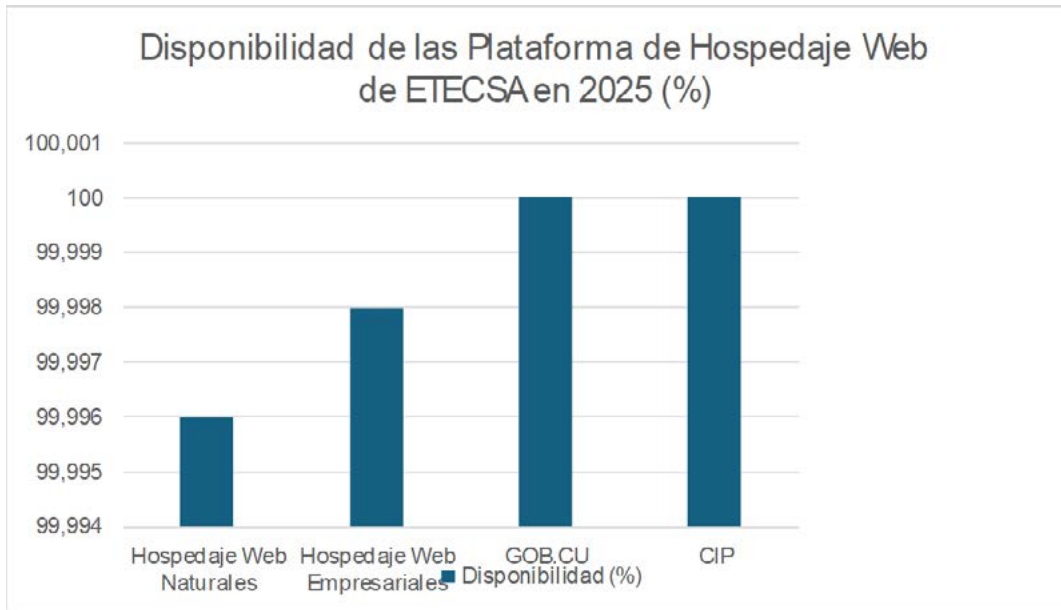


Figure 3. ETECSA's web hosting platform cybersecurity incidents during 2025 (%)

The graph of the Figure 3, "Cybersecurity Incidents of ETECSA's Web Hosting Platforms in 2025 (%)," demonstrates two facts: a security-focused design, when properly implemented, will provide satisfactory results over time. Only two cybersecurity incidents were recorded across the four platforms hosting more than 500 websites in 2025. However, even the most secure systems are not immune to vulnerabilities, as both incidents were caused by malicious agents obtaining administrator passwords.

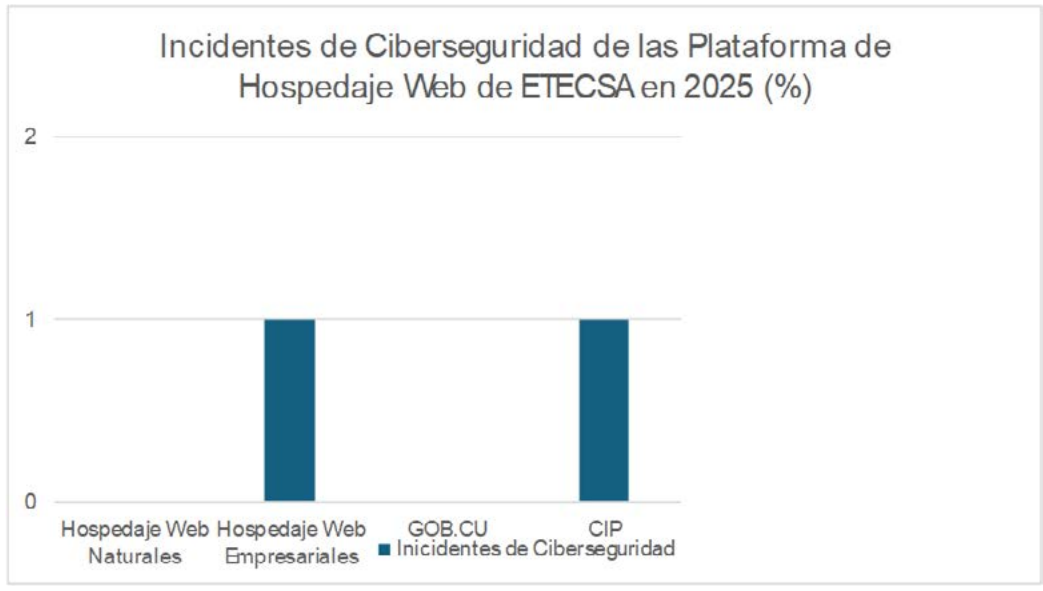


Figura 3. Incidentes de ciberseguridad de las plataforma de hospedaje web de ETECSA en 2025 (%)

Conclusions

The Extended Tier Model version presented in this article:

- It offers a clear and simple guide on the guidelines to follow in the design of redundancy for computer services.
- It facilitates the setup of an IT service and the identification of areas for improvement in optimization and availability.
- It provides good practices for redundancy of computer services.
- It is not a straitjacket, but rather another tool to support design and decision-making.

Bibliographic References

Apache HTTP *Server Project*. (October 5, 2025). Obtenido de Apache: https://httpd.apache.org

ceph. (October 5, 2025). Obtenido de ceph: https://www.ceph.io

FreeIPA - Identity, Policy, Audit - FreeIPA Documentation. (October 5, 2025). Obtenido de FreeIPA: https://www.freeipa.org

Gaceta Oficial No 45 Ordinaria de 4 de julio de 2019. (October 5, 2025). Obtenido de Gaceta Oficial de La República de Cuba: https://www.gacetaoficial.gob.cu/sites/default/files/goc-2019-045.pdf

GlusterFS. (October 5, 2025). Obtenido de Gluster: https://www.gluster.org

Haproxy The Reliable, High Performance TCP/HTTP Load Balancer. (October 5, 2025). Obtenido de Haproxy: https://www.haproxy.org

lsyncd. (October 5, 2025). Obtenido de github: https://github.com/lsyncd/lsyncd

MariaDB Foundation - MariaDB.org. (October 5, 2025). Obtenido de MariaDB: https://mariadb.org

memcached - a distributed memory object caching system. (October 5, 2025). Obtenido de memcached: https://memcached.org

Modsecurity Project. (October 5, 2025). Obtenido de Modsecurity: https://modsecurity.org

nginx. (October 5, 2025). Obtenido de nginx: https://www.nginx.org

OpenLdap, Main Page. (October 5, 2025). Obtenido de OpenLdap: https://www.openldap.org

pfsense. (October 5, 2025). Obtenido de pfsense: https://www.pfsense.org

PostgreSQL: The World s Most Advanced Open-Source Relational Database. (October 5, 2025). Obtenido de PostgreSQL: https://postgresql.org

Redis The Real-time Data Plarform. (October 5, 2025). Obtenido de Redis: https://redis.io

rsync(1) - Linux man page. (October 5, 2025). Obtenido de linux.die.net: https://linux.die.net/man/1/rsync

Tier Certification, Uptime Institute. (October 5, 2025). Obtenido de Uptime Institute: https://www.uptimeinstitute.com/Tier Certification

RESEARCH

Technological Sunflower

Lázaro Santana Linares, Eng [1*],
Maikol Ismael Mirabal Hidalgo, Eng [2],
Raydel García Mesa, M. Sc. [3]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

Currently, the rational use of energy is a fundamental aspect for humanity. To achieve the optimization of the solar energy obtained by a photovoltaic installation, there are two methodologies: the first consists of improving the internal components of a photovoltaic panel so that its performance increases, and the second consists of increasing the amount of solar radiation received by the panel. This article focuses on the second methodology. To this end, the goal is to keep the photovoltaic panel's surface area perpendicular to the light radiation from the light source. With this objective in mind, this paper presents the development and implementation of a dual-axis solar tracker prototype, to be applied to various photovoltaic and solar collection systems. This application allows the photovoltaic system to increase its production from 20 to 40 %. A low-cost device was designed and built, with simple construction, with a flexible structure

[1*] "José Antonio Echeverría" Technological University of Havana (CUJAE, for its acronym in Spanish). Calle 9naB /282 y 284, Santa Fe, Playa, La Habana. lazarosantana9627@gmail.com

[2] "José Antonio Echeverría" Technological University of Havana (CUJAE, for its acronym in Spanish). Calle 9naB /282 y 284, Santa Fe, Playa, La Habana. maikolmirabal@nauta.cu. Afiliación institucional completa. Postal address. maikolmirabal@nauta.cu

[3] "José Antonio Echeverría" Technological University of Havana (CUJAE, for its acronym in Spanish). Calle 9naB /282 y 284, Santa Fe, Playa, La Habana. raydel.gm@cime.cujae.edu.cu

and adaptable to other solar modules, with automatic and continuous operation, low electrical current consumption, and which can be used in other applications that require an activity of solar tracking. An Arduino Nano board, stepper motors with their controller, LDR (Light Dependent Resistor) sensors, i.e., photoresist; and a Bluetooth module were used for wireless communication with Android devices. Additionally, an application was developed to facilitate its use by the user, along with a battery and an electronic board for connecting all components.

Keywords: Threats in Open API, ODA, Open API, TM Forum Open APIs, Open API Security

Introduction

The demands of modern life are causing humanity to become more dependent on energy resources used for lighting, cooling, heating, and transportation. This has led to high consumption of fossil fuels, causing their depletion, an acceleration of global warming, and a rise in ocean levels (Anusha, 2017). Pollution problems, risk, and environmental degradation are the reasons why it is important to seek alternative energy sources to nuclear power and fossil fuels.

Addressing energy needs in a sustainable manner will greatly contribute to solving early-century challenges such as poverty, climate change, food security, among others (Casimiro *et al*., 2018). The current convergence of various crises (economic, along with continued oil and food price volatility) creates a suitable scenario for proposing a new formulation of policies, as well as for directing greater investments toward a safer and more sustainable development process.

The amount of solar energy annually received by the Earth is 1,5x18 KWh, which represents 10 000 times the energy consumption in that same period. In other words, the Sun is the main actor in biological processes on Earth and can be considered an inexhaustible source of energy that can be harnessed through an appropriate collection and conversion system to electrical and/or thermal energy, to mention just a few (Echenique et al., 2018). Solar energy systems harness the solar radiation incident on Earth to generate electricity or heating. The use

of solar energy presents certain difficulties that are currently being researched in order to achieve its proper utilization (Anusha, 2017).

In the case of Cuba, the Sun daily provides the national territory with the energy equivalent to 0,5 liters of oil per square meter of the Island. If we calculate this amount for the 110 000 km2 that Cuba has, we arrive at the surprising conclusion that the country daily receives, in solar energy, the equivalent of 55 million of tons of oil (Ecured, 2020). However, of all this amount of energy, only a modest percentage is utilized compared to other fuels, due to several factors, among which the high costs of solar energy collection technologies and the utilization of these systems stand out.

Among the various types of solar collection systems, photovoltaics stands out, which converts radiation from the Sun into electrical energy. There are two ways to achieve better utilization of the solar energy obtained: (a) improving the internal components of photovoltaic cells (manufacturing materials and methods) so that their performance increases (*El Porvenir*, 2020), and (b) increasing the amount of solar radiation received, by keeping the panel's surface area in a perpendicular position to the solar radiation (Onudi, 2009).

With the use of photovoltaic installations, electricity can be obtained and used in homes or for industrial purposes. The electricity obtained can be directly used or stored in accumulators for later use at night or on days without sunlight. In recent years, the use of this energy source has expanded from common uses, such as street lighting; powering traffic lights, calculators and other electronic devices; to surprising applications in air, maritime, and land transportation.

In solar energy utilization systems, it is of great importance to have the ability to perform adequate solar tracking, in order to capture the maximum amount of radiation at all times of the day [Panati (2015); Plesz, *et al*., (2009)]. For this purpose, so-called solar trackers are used, which are electromechanical devices that orient the collecting surface during the apparent path of the Sun. The objective of this project is to present the development and implementation of a prototype that enables solar trajectory tracking, thereby increasing

the radiation captured by the solar module through the continuous movement of the panel, to improve the performance of a photovoltaic installation, with low-cost construction.

Materials and Methods

In this research, the following materials and methods were used: observation of works related to the subject matter, use of the Internet, work with available online articles on the topic, interviews with specialists in solar panels, study of Arduino servomotors, and bibliographic consultations in libraries.

Solar Tracker

A solar tracker is a device composed of a fixed part and a movable one, whose purpose is to increase the capture of solar radiation. To this end, it has a collecting surface that must remain perpendicular to the Sun's rays throughout the day and within its range of motion. These are used in all solar tracking technologies: conventional photovoltaic solar energy, concentrated photovoltaic solar energy and, and concentrated solar thermal energy (Echenique *et al*., 2018).

A solar tracking system maximizes the electricity production of its solar system by moving its panels to follow the Sun throughout the day, optimizing the angle at which the panels receive solar radiation. Solar trackers are generally used for ground-mounted solar panels and large standalone solar installations such as solar trees.

When solar panels are exposed to sunlight, the angle at which the sun's rays meet the surface of the solar panel (known as the angle of incidence) determines how well the panel can convert incoming light into electricity. The narrower the angle of incidence, the more energy a photovoltaic panel can produce. Solar trackers help minimize this angle by working to orient the panels so that light strikes them perpendicular to their surface (Plesz, et al., 2009).

Solar trackers can be classified according to the type of movement they perform and the tracking algorithm.

Solar tracker by type of movement

Single-axis tracker

Rotation of the collecting surface occurs on a single axis, which can be horizontal, vertical, or oblique. This type of tracking represents

a minimum degree of complexity and its cost is lower compared to other types of trackers. The limitation of this type of tracker is that it cannot perform complete solar tracking, as it can follow either the azimuth or the solar inclination, but not both (Plesz, *et al*., 2009).

Dual-axis tracker

This type of tracker has two degrees of freedom and is capable of performing full solar tracking, both in inclination and azimuth. Although the installation performance may be higher compared to single-axis trackers, it is important to mention that the dual-axis tracker is more costly (Plesz, *et al*., 2009). Figure 1 illustrates the solar trackers according to their type of movement.

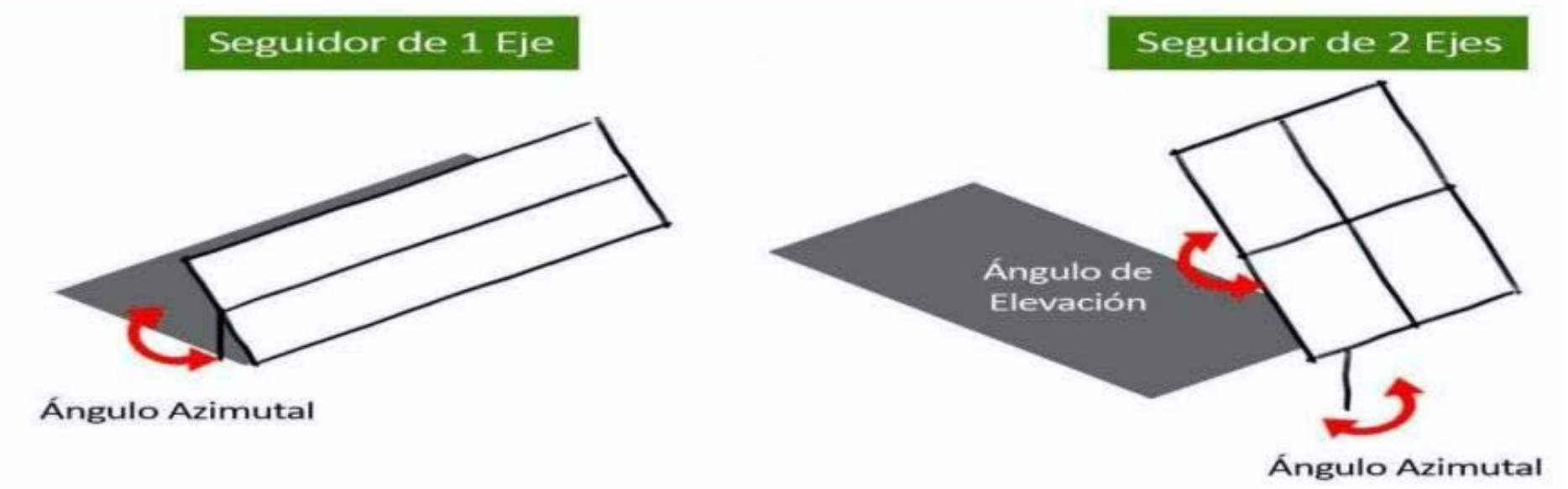


Figure 1. Solar tracking scheme

Solar tracker by tracking algorithm type

Solar clock tracking

This type is subject to the a 24 hour-clock and varies its position with respect to the cycle of this clock, with effective tracking of 12 hours. It moves at an angle of 120º. To achieve this, a Real-Time Clock (RTC) is incorporated into the device / the device is fitted with a Real-Time Clock (RTC), which consists of a microcontroller that accurately counts time and also incorporates / is equipped with a sensor to compensate for temperature changes that alter the electrons of the silicon crystal (Lakeou *et al*., 2006).

Luminosity-based tracking

The algorithm for this type of tracker is based on the signal provided by one or more sensors. Depending on this signal, a control command is sent to one or more motors to position them at the most suitable luminosity point. This type of tracking is easy to implement (Plesz, *et al*., 2009).

Astronomical programming tracking

This type of tracker is completely independent of weather conditions, since its algorithm does not require sensors to indicate the brightest point. Tracking in this case depends on a series of equations that predict the Sun's position at any given time. Although this model is highly accurate, it should be noted that implementing the algorithm involves a high degree of complexity (Sierra *et al*., 2008)

For this project, a solar tracker prototype was chosen that moves on two axes and uses a luminosity-based tracking algorithm. An economical device, with low-cost and recycled components. For its construction, an Arduino Nano board was selected because it offers great compatibility with all modules available on the market focused on Arduino is low-cost and has simple and flexible programming. Once configured, it can perform unattended and automatic solar tracking.

General design

The new solar tracker prototype now consists of three main stages: electronic system, electromechanical system, and software. Before manufacturing the device, a simulation was performed in Proteus (Proteus Design Suite), as shown in Figure 2. In this simulation, its correct operation was verified.

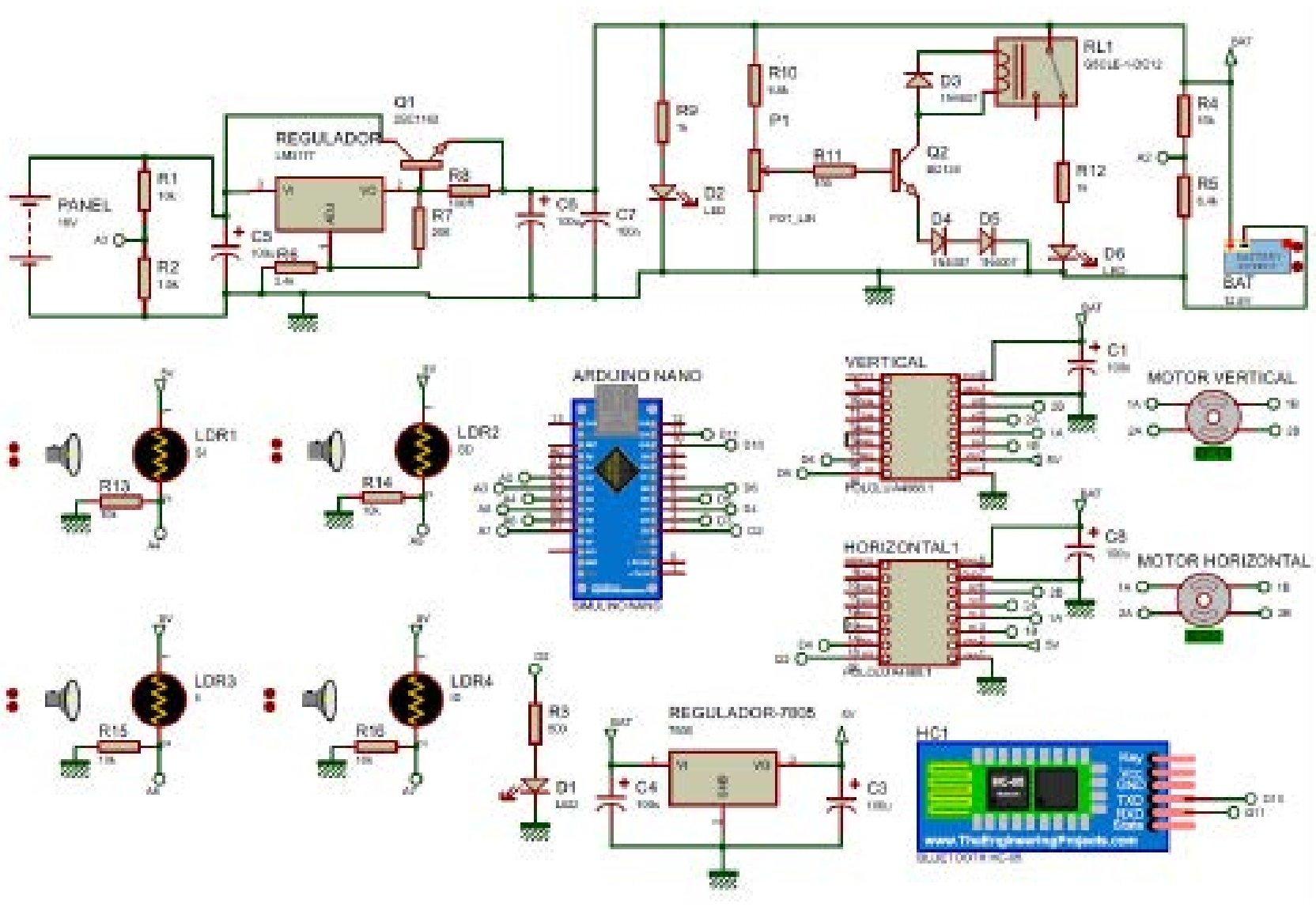


Figure 2. Prototype simulation in Proteus

Electronic system

Figure 3 illustrates the electronic schematic of the prototype.

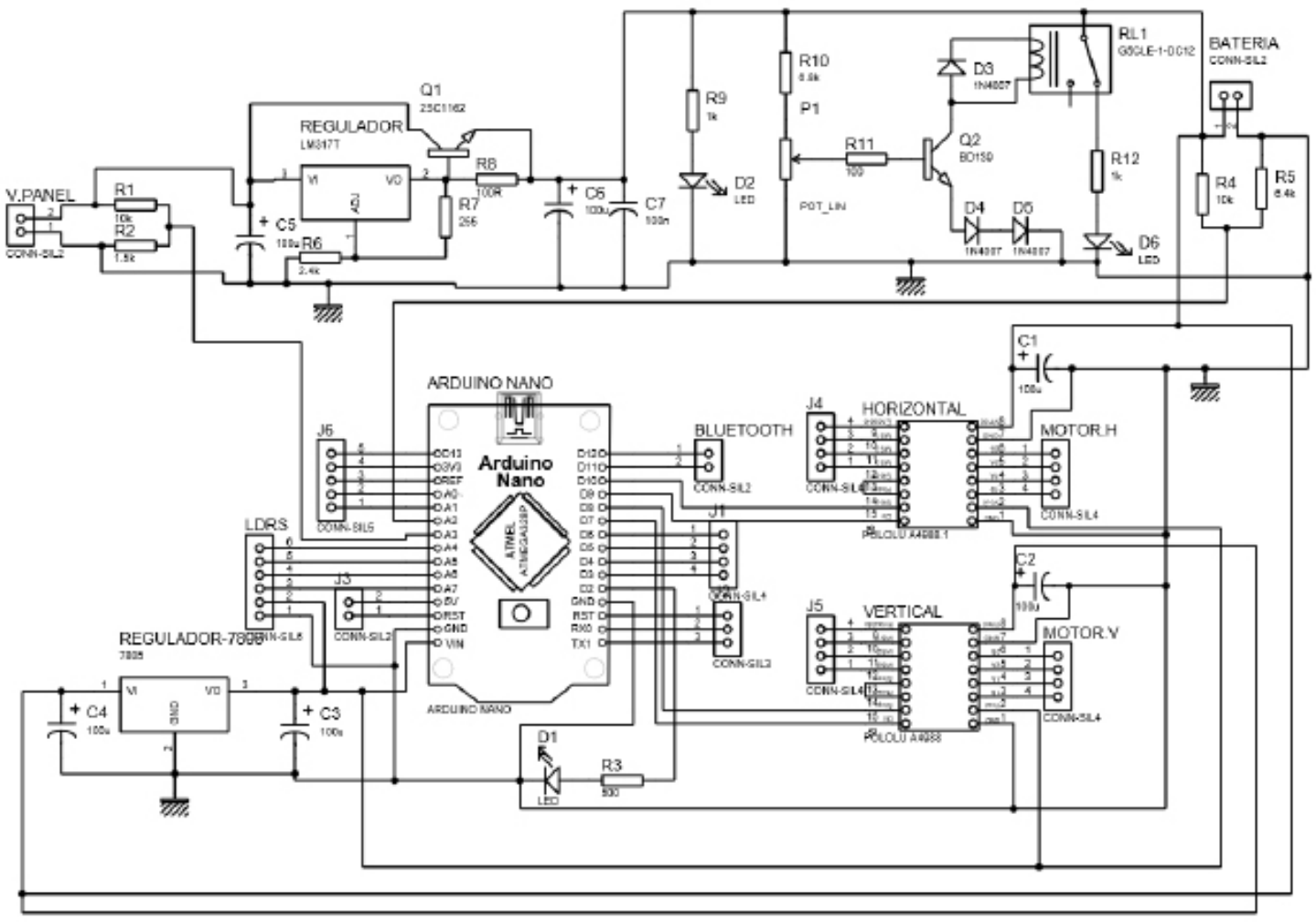


Figure 3. Electronic schematic of the prototype

Microcontroller

Arduino is an open-source electronic platform for creating microcontroller-based prototypes and applications, where both software and hardware are free, flexible, and easy to use. It can capture information from its surroundings through its input pins, to which a wide range of sensors and transducers can be connected. Similarly, it can act upon its surroundings through its output pins or lines. With these lines, it is possible to control lights, motors, relays, speakers, and all types of actuators (Sitiosolar, 2020).

The microcontroller on the Arduino board is programmed using the Arduino programming language. It is a high-level language with statements and syntax very similar to those of the C language. It also has a development environment based on Processing, which allows editing a program with the Arduino language, verifying it, compiling it, and writing it to the controller (Sitiosolar, 2020).

The tracking system uses the Arduino board (Figure 4) as the main controller. This board will be used to control the motors through four digital outputs connected to two drivers, as well as to read information from the four radiation sensors through four analog inputs. Table 1 shows the technical specifications of the Arduino Nano board.



Figure 4. Arduino Nano

Table 1. Technical specifications of the Arduino Nano board

Microcontroller	ATmega 328
Input voltage	7-12V
Operating voltage	5V
E/S Digital I/O pins	22 (6 outputs PWM)
E/S Analog input pins	8
E/S Current per I/O pin	40 mA
Flash memory	32 KB with 2 KB for the bootloader
SRAM	2 KB
EEPROM	1 KB
Clock speed	16 MHz

A4988 stepper motor control

The A4988 board, or A4988 driver "Pololu" (Figure 5), controls a stepper motor of up to 2A. A. It has five different resolutions: full step, half step, quarter step, eighth step, and sixteenth step. Control is performed so that each step input pulse corresponds to one micro-step of the stepper motor in the direction selected by the DIR pin (Lakeou *et al.*, 2006). Two drivers were used to control the two stepper motors used, configured for full-step operation at 1A.



Figure 5. A4988 Driver

Solar position sensors

For positioning, LDR sensors, or photoresistors, were used. These are variable resistors depending on the light incident on their surface. The greater the intensity of light incident on the LDR's surface, the lower its resistance, and the less light incident, the greater its resistance (Sitiosolar, 2020). For this project, four sensors were arranged, one for each quadrant of the panel or solar module (top right and left, bottom right and left), as shown in Figure 6.

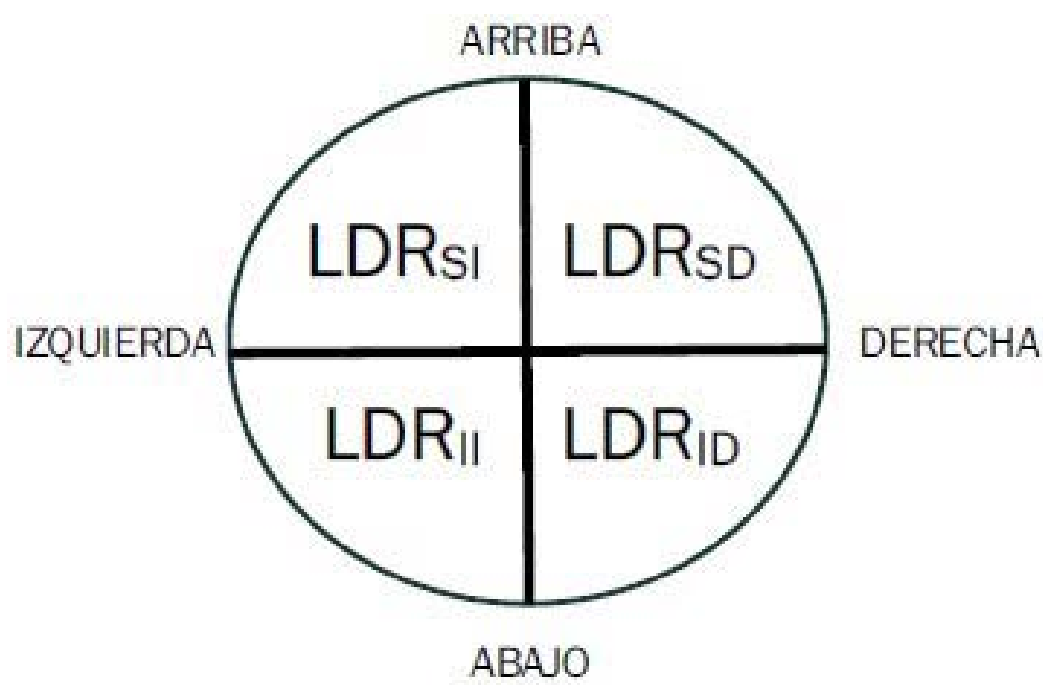


Figure 6. Distribution of the LDR

The system always drives the four sensors to have the same light intensity, indicating that the panel is oriented toward the Sun. The conditioned signals from each LDR are read on independent inputs of the Arduino Nano, which performs calibration and calculation, and executes the corresponding movements of the stepper motors. A Light Emitting Diode (LED) was incorporated to display the calibration time of the LDR.

Bluetooth module

The Bluetooth HC-05 Module (Figure 7) was incorporated into the system. This connects Arduino with a device wirelessly (Bluetooth), with the ease of operation of a serial port. All module parameters can be configured using AT commands. Bluetooth communication occurs between two types of devices: a master and a slave. Bluetooth is the name given to the communication protocol specially designed for low-power devices requiring short-range transmission and based on low-cost transceivers.



Figure 7. Bluetooth module

Battery

For storing the electrical charge generated by the photovoltaic system, a battery was developed using 18650 lithium cells recycled from laptops and electric vehicle batteries. This is also used as a power source for the electronic circuit and the devices used, enabling a self-powered and continuously operating system.

A total of 12 cells were used, connected in three columns and four rows. The result was a 12,6V y 10A lithium battery, similar to the one shown in Figure 8.



Figure 8. Battery

Electronic board

A printed circuit board (PCB) was developed for connecting the prototype's electronic devices: Arduino Nano board, A4988 drivers,

LDR sensors, and Bluetooth module. Additionally, a circuit was implemented for regulating the voltage delivered by the photovoltaic system and for automatic battery disconnection, facilitating proper battery charging. The following components were used: resistors of 100Ω 3W, 100Ω, 255Ω, 1KΩ, 1,5KΩ, 2,4KΩ, 6,4KΩ, 10KΩ and a potentiometer; electrolytic capacitors of 100uF 50V and 100uF 25V; 1N4007 diodes; 5mm 3,6V LEDs; a 2SC1162 transistor and a BD139, a 12V relay, and a LM317T voltage regulator.

Electronic components for display, device protection, and supply voltage regulation were added to this circuit. These components are: 7805 voltage regulator, 100uF 50V and 100uF 16V electrolytic capacitors, 500Ω and 10KΩ resistors, and a 5mm 3,6V LED.

Figure 9 shows the two sides of the PCB developed in Proteus. Its dimensions are: 97,3 mm wide and 121,5 mm long.

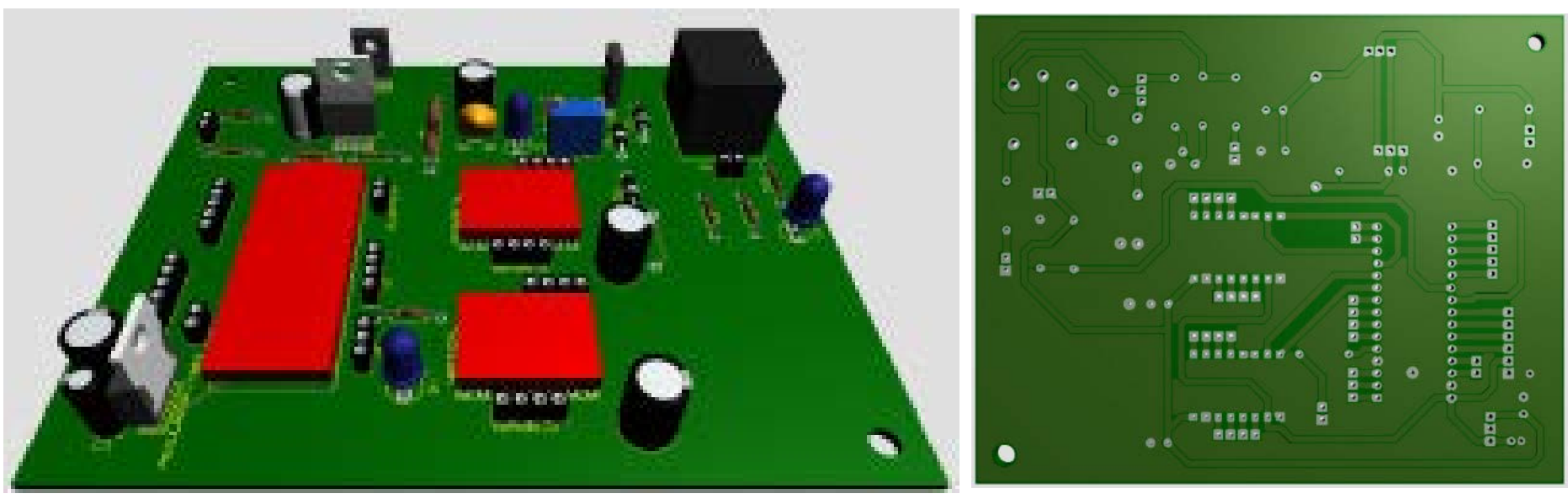


Figure 9. Prototype PCB

Electromechanical system

Metal structure

To support the solar panel, a metal piece in the shape of a U will be used, on which the photovoltaic module will rest. This piece will rest on a cubic metal base. For this prototype, a recycled chassis from a computer power supply was used. Inside this base, the printed circuit board will be placed. Recycled gearboxes from disused printers were also used to improve system mobility.

It is important to reiterate that the entire assembly described will be very lightweight to avoid the use of large motors, which would increase system cost and complexity.

Stepper motors

The stepper motor, also known as a step motor, is an electro-mechanical device that converts a series of electrical pulses into discrete angular displacements, meaning it is capable of rotating a certain number of degrees depending on its control inputs (Lakeou *et al*., 2006). In this prototype, two EM-323 stepper motors recycled from an EPSOM LX-300+ printer were used. These have a step angle of 3,75º (96 steps per revolution). Table 2 shows the technical specifications of this motor.

Table 2. Technical specifications of the EM-323 stepper motor

Item	Specification
Motor type	2-phase, 96-pole hybrid stepper motor
Coil resistance	16.0 Ω ±10% (25°C)
Control method	Bi-polar rated current drive
Phase drive	1-2 phase, W1-2 phase
Drive voltage	36.75 ±1.75 VDC
Drive current	0.1 to 0.9A
Paper feed pitch	Minimum Resolution: 0.059 mm (1/432") (1-2 phase, 2 pass)

Software

Arduino IDE

Since Arduino is a board that executes a series of previously uploaded codes, a program called IDE (Integrated Development Environment) is needed to load those codes. This IDE, installed on a PC, is a very simple environment to use, and the program to be executed by Arduino is written in it. Once written, it is loaded via the USB port, and Arduino will begin working autonomously (Sitiosolar, 2020). In broad terms, the operation of the developed software can be appreciated through the flowchart in Figure 10.

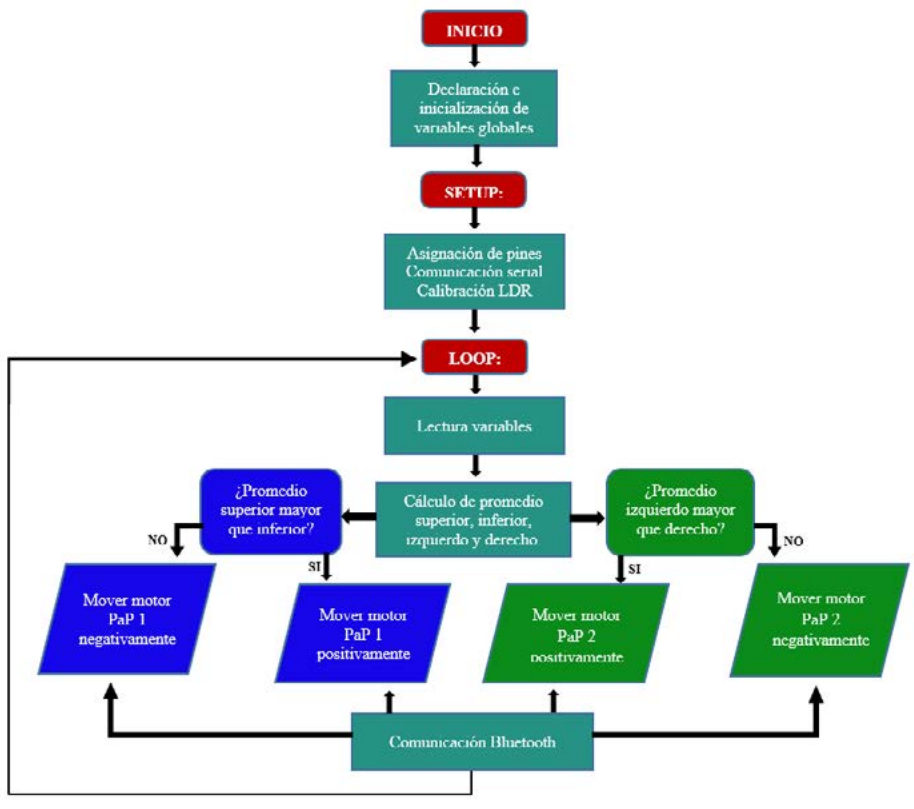


Figure 10. Basic flowchart

App inventor

App inventor is a software development environment created by Google Labs for developing applications for the Android operating system. The system is free and can be easily downloaded from the web. A custom / customized application was developed on this platform for this system, compatible with devices running the Android operating system. This application has a pleasant, simple, and easy-to-use visual interface. It allows for improved ease of control of the solar panel by users, as well as displaying readings of the following values: Solar Panel Voltage, Battery Voltage, and Battery Charge Percentage. This is shown in Figure 11.

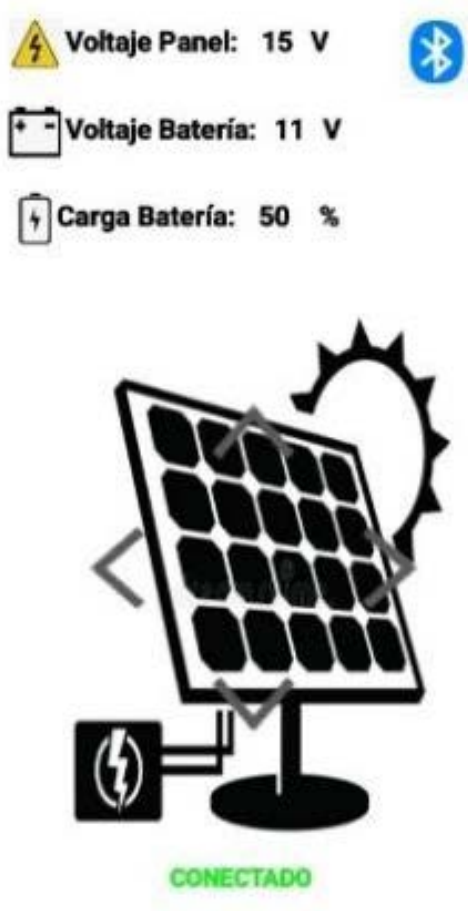


Figure 11. Prototype application

The final construction of the device is shown in Figure 12. This prototype was developed to demonstrate the functionality of the proposed solar tracking system. It serves as a basis for the development of other tracking systems with the same features, but with characteristics adapted to the photovoltaic module used.



Figure 12. Solar tracker prototype

Results and discussion

Operation

The LDR (photoresistors) help determine where there is more brightness during the day. These were placed at the vertices of the panel. To achieve greater accuracy in brightness measurement, the photoresistors should be covered around them to avoid capturing diffuse solar radiation, in other words, the propagation of light (electromagnetic waves) that is scattered and reflected in the atmosphere.

The LDR readings are calibrated and compared by the Arduino, which sends signals to the stepper motor drivers to execute the necessary movements. For example, the groups of LDR called left and right are compared, and if there is a difference greater or less than the determined sensitivity range, then a corresponding movement must be executed. The same applies to the top and bottom sensor groups, except that these determine the movement of the other axis. In this way, sunlight strikes the panel surface perpendicularly.

The photovoltaic module transforms the captured solar energy into electrical energy. This is regulated to charge the battery that powers the entire system. A disconnection system was developed for it when fully charged.

The Bluetooth module enables wireless communication between the prototype and the device running the developed Android application. It allows the user to control system movement and view the following values: Solar Panel Voltage, Battery Voltage, and Battery Charge Percentage. Figure 13 illustrates the operating schematic of the developed prototype.

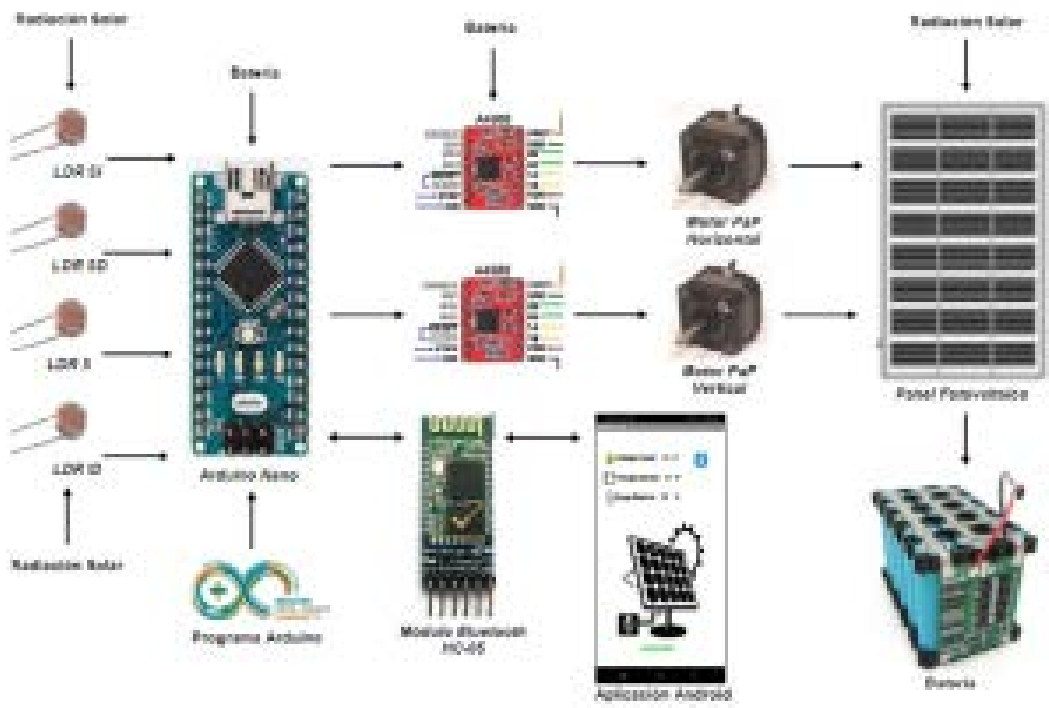


Figure 13.
Prototype operating schematic

Tests performed and results obtained

Tests to validate the operation of the solar tracker device and the algorithm were carried out using a natural light source, on a scale prototype of a photovoltaic installation. Using the prototype without the tracker function initially and subsequently with the tracker device activated, several values were recorded for different angular positions.

When comparing the results (shown in Figure 14), the performance increase of the installation with tracker compared to the static installation is 33,5 %.

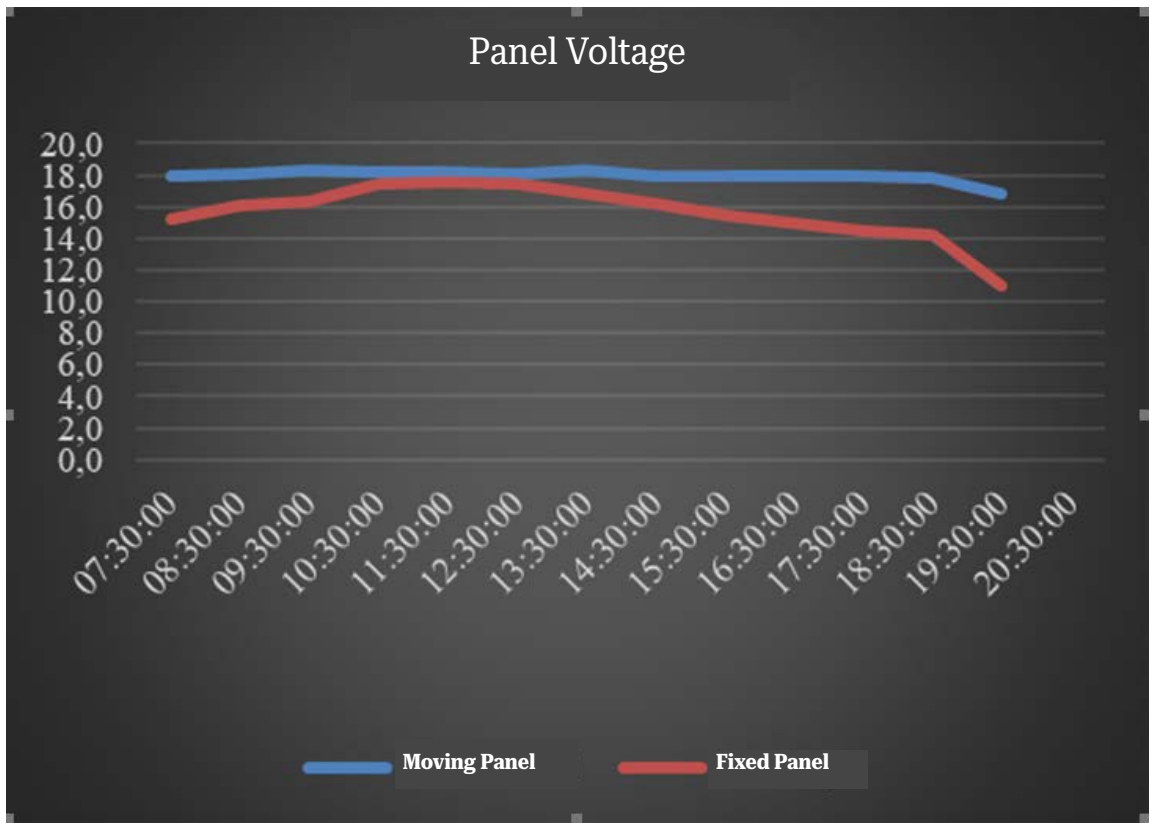


Figure 14. Comparison of voltage measured in a fixed panel with voltage in a panel using a solar tracker

Conclusions

The constructed prototype meets the required dual-axis tracking characteristics, performing solar tracking. This increases the radiation captured by the module by up to 33,5% and therefore improves the performance of the photovoltaic installation. The results obtained support that the developed dual-axis solar tracker achieves better energy performance compared to a photovoltaic system with fixed panels. A low-cost device with low electrical current consumption was achieved, with simple construction, a flexible structure adaptable to other solar modules, and automatic and continuous operation. The constructed prototype can be used in other applications requiring solar tracking activity, such as solar collectors, solar furnaces, among others.

Bibliographic References

ANUSHA, K.; CHANDRA, S. (2017). Design and development of real time clock based efficient solar tracking system. *International Journal of Engineering Research and Applications*. Retrieved from www.ijera.com

CASIMIRO, R.; GEA, M.; HOYOS, D; PLACCO C. (2018, septiembre). *SEGUIDOR SOLAR DE DOS EJES PARA HELIÓSTATO*. Instituto de Investigación en Energías No Convencionales (INENCO).

ECHENIQUE, R.; PERINO, E.; ODICINO, L.; PARELLÓ, D.; MURDOCCA, R. (2018, septiembre). *SISTEMA DE SEGUIMIENTO SOLAR PARA PANELES FOTOVOLTAICOS*. Laboratorio de Electrónica, Investigación y Servicios (L.E.I.S.) - Laboratorio de Energía Solar y Medio Ambiente - Facultad de Ciencias Físico Matemáticas y Naturales -U.N.S.L.

EcuRed, R. (2020, mayo 10). *Energía Solar en Cuba*. Retrieved from http://www.ecured.cu/ Energ%C3%Ada_solar_en_Cuba

ELPORVENIR. (2020, abril 16). *Seguidores Solares, una Optimización de la Energía Solar*. Retrieved from http://www.elporvenir.com.mx/notas.asp?nota_id=2 53973.

ONUDI, N. C. (2009, junio). *Hacia una Agenda Energética Integrada más allá de 2020*. Hofburg, Viena, Austria: Conferencia Internacional de Energía.

PANAIT, M.A; TUDAROSHE, T. (2015). *A simple neural networks solar tracker for optimizing conversion efficiency in off-grind solar generators*. Santander: ICREPQ.

PLESZ B.; SÁGI P.; TIMÁR-HORVATH, V. (2009). *Enhancement of solar panels power generation by the usage of solar tracking*. 3, 1. Proceedings of ECOpole,.

S. LAKEOU; S., OSOSANYA; E. LATIGO, O. MAHAMOUD; W. KARANGA; G. OSHUMARE; W. (2006). *Design of a low-cost digital controller for a solar tracking photo-voltaic (PV) module and wind turbine combination system*. Dresden, Germany: 21st European Photovoltaic Solar Energy Conference.

SIERRA, F.; CARO, E.; MEJÍA, F. (2008.). *Tecnologías para el aprovechamiento de la energía solar*. Bogotá: Universidad Nacional de Colombia.

SITIOSOLAR. (2020, mayo 27). *Los Paneles Solares Fotovoltaicos*. Retrieved from http://www.sitiosolar.com/paneles%20fotovoltaicas

RESEARCH

Towards Inventory Management 4.0: Integration of Digital Technologies in Cuba's Biopharmaceutical Supply Chain

Zuleyka Calzado Mesa, M. Sc. [1*], Gabriela Ojeda de la Paz, Eng [2], Damián Aldait García Pérez, Eng.[3]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

Inventory management ensures order within the warehouse and streamlines operational workflows. Through proper control of this management model, companies can efficiently satisfy customer demand. Biocubafarma is the holding company responsible for manufacturing medicines, equipment, and high-tech services aimed at improving the health of the Cuban population and geared toward generating exportable goods and services. Although a large portion of its processes is computerized—thereby optimizing many of its operations—the development of technological solutions remains necessary to drive the Company's advancement toward digital transformation and the evolution into Industry 4.0. This article addresses the outcomes of a sectoral innovation project carried out at the Information Technology Company (ETI, for its Spanish acronym). The project aimed to introduce smart tags into the supply inventory management system utilized

[1*] Empresa de Tecnología de la Información. Calle 18 #4310 e/ 43 y 47. Miramar, Playa La Habana, Cuba.zuleykacalzado@gmail.com

[2] Empresa de Tecnología de la Información. Calle 18 #4310 e/ 43 y 47. Miramar, Playa La Habana, Cuba.gabriela@eti.biocubafarma.cu

[3]Empresa de Tecnología de la Información. Calle 18 #4310 e/ 43 y 47. Miramar, Playa La Habana, Cuba.damian@eti.biocubafarma.cu

by the Biocubafarma Holding Company; modify said system by incorporating batch and location levels; and develop an Android-based application that enables operators to optimize warehouse operations and communicate in real time with the inventory system. All of this results in a 40% reduction in data capture times, the elimination of manual logging errors, and the achievement of real-time operational synchronization, ultimately maximizing supply chain efficiency.

Keywords: smart labels; inventory management; industry 4.0; batch; digital transformation

Introduction

"Inventory represents a strategic reserve of materials, raw materials, work-in-process, or finished goods that, although not used systematically, guarantees the continuity of customer service" (Cespón Castro, 2012). According to Schroeder (cited in Alemán Rodríguez, 2013), inventory is a stored quantity of materials intended to facilitate production or satisfy consumer demand. The aforementioned approaches highlight that inventory is composed of physical resources, whose rigorous control, is vital to avoid stockouts and ensure the proper functioning of any company or business.

Inventory management, defined by Cespón Castro (2012) as "the process that seeks to minimize the stored quantity without affecting customer service," has become an essential process for maximizing business efficiency and profitability. Logistics, for its part, integrates the planning and management of operations linked to the flow of raw materials, semi-finished, and finished products from their origin to the final consumer.

With the advent of Industry 4.0 and digitalization, inventory management has undergone a profound transformation through automation and the use of smart technologies. The implementation of smart labels, due to their ability to store data, enables wireless communication, remote identification, traceability, and real-time management, improving accuracy and agility in the supply chain.

Biocubafarma, a leading biotechnology and pharmaceutical company, has strengthened its logistic process in accordance with strict

regulations and has achieved comprehensive production tracking from the reception of raw materials to the delivery of finished products to the Ministry of Public Health (MINSAP, for its Spanish acronym). However, challenges persist in controlling products within the supplies area at the batch and location levels, as well as in tracking expiration dates for food products, which hinders optimal management.

Faced with this problem, ETI undertook the development of a sectoral innovation project to modernize the «Insumo» (Supply) inventory management system at the batch and location levels. Likewise, it developed an application that manages warehouse operations and communicates in real time with the inventory software. Additionally, for the products, smart labels were incorporated. This novel project is a clear example of how digitalization and Industry 4.0 can contribute to optimizing traceability, efficiency, and competitiveness in the Cuban biotechnology and pharmaceutical industry.

Materials and methods

Among the materials and methods used in the development of this project are:

Documentary Analysis

- **Concept:** Scientific research method involving the selection, consultation, critical review, and deconstruction of relevant information sources to identify the state of the art of a study object, evaluate its theoretical-methodological bases, and analyze regulatory or normative frameworks.
- **Application in the project:** Study of the international, national, and sectoral regulatory framework applicable to the inventory management system.

Observation

- **Concept:** Data collection method consisting of the direct, systematic, and deliberate perception of phenomena in their natural environment. In its non-participant modality, the researcher acts as an external and neutral agent to record objective data and behaviors (including extra-verbal information) without intervening in the dynamics.

- **Application in the project:** Diagnosis of current workflows and requirements gathering with the end-users of the organization.

Project Management Framework (Scrum)

- **Concept:** Agile and adaptive framework designed for the management and development of complex projects. It is based on empirical process control, iterative and incremental development, and continuous feedback to maximize the timely delivery of value.
- **Application in the project:** Management of the software lifecycle through the definition of sprints, ensuring information flow, risk mitigation, and effective communication between the technical team and stakeholders.

Computer Resources and Tools

Computer resources: A set of technological assets, hardware components, development environments, and software applications that enable data processing, storage, automation, and management within a project.

The technological ecosystem, standards, and tools applied in the design, development, deployment, and quality assurance of the inventory management system and the mobile application are broken down below:

Category	Tool / Technology	Conceptual Definition	Practical Application in the Project
Standards and Processes	DSI-P-F1-01 Procedure	Institutional methodological guide regulating the software development lifecycle.	Strict regulation of the sequence of operations and phases of the project in the Information Systems Division.
Integration and Middleware	Mule ESB (*Mule ESB, n.d.*)	Enterprise Service Bus (ESB) oriented to the integration of distributed applications.	Orchestration and integration of web services and communication between the organization's systems.
Mobile Development	Flutter (*Android Developers, n.d.*)	Open-source Software Development Kit (SDK) for a multiplatform user interface.	Development of the new native mobile application for Android devices from a single codebase.

Category	Tool / Technology	Conceptual Definition	Practical Application in the Project
Infrastructure (Servers)	Windows Server 2019 *(Axarnet, n.d.)*	Multiprocessing and multiuser server operating system with advanced support for virtualization and active security.	Hosting and deployment of the inventory management system in high-availability corporate environments.
Infrastructure (Servers)	Linux (Debian 10) *(Debian, n.d.)*	Free, stable, and multiuser operating system optimized for network server architectures.	Secondary server environment dedicated to the execution and deployment of lightweight services and containers.
Development Environment	.NET 7 *(Dotnet, n.d.)*	Modern, open-source, and multiplatform development platform for application execution.	Framework for developing the components and services of the desktop ecosystem.
Programming Language	C# *(Microsoft Learn, n.d.)*	Modern, synchronous, and object-oriented programming language with type safety.	Secure and robust coding of the internal logic for components integrated into .NET.
User Interface	Windows Presentation Foundation (WPF) *(Programarfacil, n.d.)*	Graphical presentation subsystem for creating user interfaces (UI) in desktop applications.	Design and implementation of the user interface (UI) for the desktop inventory management system.
Quality Assurance (QA)	Systems Documentation	Structured compilation of technical software artifacts and operational user guides.	Preparation of requirements specifications, user manuals, and system validation (QA) artifacts.

Discussion and outcomes

The sectoral innovation project developed for the integration of digital technologies in Biocubafarma's inventory management showed positive results that contributed to the modernization of the logistics system in the Cuban biopharmaceutical supply chain.

The introduction of smart labels allowed for the automatic and real-time identification of stored supplies, significantly improving product traceability from reception to warehouse output. The capacity of these labels to contain specific information on batch, location, and expiration dates facilitated rigorous control and the reduction of human

errors in inventory management. This project was framed within the improvement of the "Insumos" (Supplies) inventory management process, through the introduction of innovative technologies and passive optical networks with Gigabit Passive Optical Network (GPON) technology, to contribute to the digital transformation of the Cuban biotechnology and pharmaceutical industry. The execution of each of the defined results is detailed below.

1-) Result 1: "*Insumo*" inventory management system at the batch level was modified.

The main result of this work was the reengineering of the inventory management system (Mistral) to operate at the batch level, a fundamental advancement for Biocubafarma where traceability and expiry control are quality and safety imperatives.

Modified and Implemented Functionalities

Product entry and exit operations were modified to incorporate the "batch" level. The affected operations include:

- **Entry:** receiving report and claim report.
- **Exit:** delivery note, request and return note, exit note for Work Order (WO), other exits, exit transfers, and transfers between areas.

Additionally, new functionalities were developed for warehouse management at this new level:

- **Batch Relocation:** allows moving specific batches between locations, optimizing space and prioritizing products based on their expiration date.
- **Label Printing:** the generation and printing of DataMatrix labels for products and batches, as well as barcodes for location identification, was implemented. This constitutes the physical basis for traceability.

2-) Result 2: Develop an application for the Android system with functionalities that intervene in the inventory management process, linked to the "Insumos" inventory management system.

To provide operators with an agile, real-time tool, an Android application was developed. This application communicates with the Mistral system and allows for the immediate capture of information by reading DataMatrix labels and barcodes.

The application replicates and allows for the remote, guided execution of all warehouse operations modified in the central system, guaranteeing data integrity from the point of operation. The functionalities implemented in the app include: receiving report, delivery note, return note, exit note to WO, other exits, transfers, transfers between areas, batch relocation, and management of locations by product or by entry.

The set of results presented describes the digitalization of business processes: logistics and inventory management. The introduction of batch-level traceability and real-time data capture through mobile devices not only optimizes space and prioritizes products but is also a quality and safety imperative, particularly critical in a sector like pharmaceuticals (BioCubafarma). The Android app acts as a crucial bridge between the physical world (DataMatrix labels) and the central system (Mistral), eliminating delays and reducing errors.

Similarly, it is important to highlight that these results are at the forefront of technological and logistics management trends, aligning with the principles of Industry 4.0. The solution is not mere digitalization, but a deep integration that employs key contemporary technologies:

- **Real-time and batch-level traceability:** is the gold standard in regulated industries like pharmaceuticals and food.
- **Integrated systems architecture (Mistral + Android App + Mule ESB):** reflects the paradigm of systems of systems, where different software components seamlessly communicate to offer a unified solution.
- **Use of mobile technologies (Android) and automatic identification (DataMatrix):** accessible and high-impact technologies that modernize human-system interaction on the warehouse floor.
- **Automation of logistics processes:** the reengineering of processes such as transfers and automated relocation places the organization at an advanced level of digital maturity.

Scope and characteristics of the contribution achieved

The sectoral innovation project developed for inventory management

in a supplies warehouse at BioCubaFarma represents a high-impact intervention at the national level with a solid potential for international repercussion in contexts of similar regulatory and logistical complexity.

1. Scope of the Contribution and Strategic Significance

- Technological Sovereignty and National Repercussion: For the BioCubaFarma company, this development constitutes an own, sovereign, and sustainable solution, eliminating dependence on external applications.
- Alignment with Industry 4.0: The solution achieves an advanced level of digital maturity for the Business Group by automating operations in a supplies warehouse. It is not limited to recording data, but profoundly transforms the operational flow through process reengineering that places the company at the forefront of contemporary management trends.
- Critical Impact on Quality and Safety: By ensuring total traceability in real-time at the batch level, the project rigorously complies with the high regulatory demands of the global pharmaceutical industry, guaranteeing strict control over biosafety / biosecurity, expiration, and quality assurance.

2. Technical and Operational Characteristics of the Contribution

- The viability and solidity of this impact are based on a robust technological architecture and profound functional integration, divided into four fundamental axes:
- Robust Batch-Level Traceability: Through the reengineering of the central system (Mistral), the entry (receiving and claim reports) and exit (delivery notes, returns, exits to Work Order, transfers, and stock transfers) operations were comprehensively modified to operate under strict batch control. This also allows for the intelligent relocation of supplies in the warehouse, optimizing physical space and prioritizing products based on their expiration date.
- Automatic Identification and Mitigation of Human Error: The physical basis for traceability was implemented through the generation and printing of DataMatrix smart labels for products and

barcodes for location coding. This ecosystem automatically captures information, eliminating delays and drastically reducing human errors associated with manual records.

- Mobility and Ubiquity on the Ground: The development of a native mobile application for Android provides operators with an agile tool that remotely and in a guided manner replicates all the operations of the central system. The app acts as a crucial and immediate bridge between the physical world (warehouse labels) and the management system, directly guaranteeing data integrity at the point of operation.
- "System of Systems" Architecture and Advanced Infrastructure: The connectivity support was designed over passive optical networks with GPON (Gigabit Passive Optical Network) technology. On this basis, a fluid software ecosystem was structured where different components (Mistral + Android App + Mule ESB) transparently communicate and in an integrated manner, achieving perfect synchronization of logistics information.

Conclusions

The project achieved the technological modernization and digital transformation of logistics management in supply warehouses through three interconnected fundamental pillars: the reengineering of the central Mistral system, the deployment of a native Android mobile application, and the support of an advanced network infrastructure with GPON technology. The reengineering of the central system to operate at the batch level, together with the introduction of DataMatrix smart labels, allowed for the establishment of rigorous, real-time traceability control over supplies. This advancement is critical for drastically mitigating human error in manual records, optimizing physical storage space, and guaranteeing the strict biosafety regulations, expiry control, and quality assurance required in the international pharmaceutical sector.

Despite the positive results in operational efficiency, the study presents limitations associated with its initial scope, having been implemented as a validation in the ETI warehouse. The success of this initial

phase raises the immediate need to scale the solution to the rest of the units and laboratories of BioCubaFarma company, which will require the homogenization of the network infrastructure and the continuous training of operational personnel on the warehouse floor.

As future work, the expansion of the digital ecosystem is projected through the integration of distributed ledger technologies (blockchain) to strengthen the immutability of the drug custody chain. Likewise, the incorporation of predictive intelligence models aimed at anticipating supply demand curves and proactively optimizing batch expiration alerts is planned, thus consolidating the organization's definitive transition towards the paradigms of Industry 4.0.

References

Al-Sartawi, M., & Hassanzadeh, A. (2023). Digitalization enhancement in the pharmaceutical supply network using a supply chain risk management approach. *Scientific Reports*, 13(1), Artículo 22314. https://doi.org/10.1038/s41598-023-49216-7

Alemán Rodríguez, A. (2013). *Procedimiento para la clasificación y propuesta de métodos de inventario para los productos de la Sucursal Emprestur SA Villa Clara* (Tesis de maestría). Universidad Central “Marta Abreu” de Las Villas, Santa Clara, Cuba.

Android Developers. (2026). *Android API guidelines and core framework architecture*. Google Developer Documentation. https://developer.android.com/

Cespón Castro, R. (2012). *Administración de la Cadena de Suministro*. Editorial Feijóo, Universidad Central “Marta Abreu” de Las Villas.

Charles, V., & Tasnim, N. (2025). The integration of blockchain and predictive analytics for secure and transparent batch traceability in pharma supply chains. *International Journal of Production Research, 63*(2), 401-419. https://doi.org/10.1080/00207543.2024.2389104

Colectivo de autores. (2018). *La gestión de stock* (Cap. 5). McGraw-Hill Interamericana de España. https://www.mheducation.es/bcv/guide/capitulo/8448612124.pdf

Colectivo de autores. (2019a). Diseño de una metodología para la estandarización de los sistemas de codificación y clasificación de productos en empresas cubanas. *Ingeniería Industrial, 40*(2), 114-124. https://www.redalyc.org/jatsRepo/4096/40965950005/html/index.html

Colectivo de autores. (2019b). *La Gestión de Inventario como proceso clave en el sistema empresarial*. Contraloría General de la República de Cuba. https://www.contraloria.gob.cu/sites/default/files/articulos/2019-12/La%20Gestion%20de%20Inventario%20como%20proceso%20clave.pdf

Jagtheesan, S., & Shashi, K. (2023). Digital transformation in pharmaceutical supply chains: A qualitative study of strategic implementation approaches for enhanced efficiency. *Journal of Pharmaceutical Innovation*, 18(4), 512-526. https://doi.org/10.1007/s12247-023-09743-4

Lewandowska, M., & Koliński, A. (2023). Intelligent Warehouse in Industry 4.0—Systematic Literature Review. *Sensors*, *23*(8), Artículo 4105. https://doi.org/10.3390/s23084105

Microsoft Corporation. (2025). *C# Language Specification and .NET Framework architecture documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/dotnet/csharp/

Microsoft Corporation. (2026). SQL Server technical documentation: Relational database engine. Microsoft Learn. https://learn.microsoft.com/en-us/sql/sql-server/

MuleSoft. (2024). Anypoint Platform and Mule Enterprise Service Bus solutions architecture guide. Salesforce. https://www.mulesoft.com/

Nathan, I. (2022). Windows Presentation Foundation Development: Architecture and patterns for desktop applications (2da ed.). Apress.

Schildt, H. (2022). Java: The Complete Reference (12da ed.). McGraw-Hill Education.

Schroeder, R. (1992). Administración de operaciones: Toma de decisiones en la función de operaciones (3ra ed.). McGraw-Hill Interamericana.

Sharma, R., & Singh, S. (2023). A comprehensive study on Industry 4.0 in the pharmaceutical industry for sustainable development. Environmental Science and Pollution Research, 30(22), 61205-61218. https://doi.org/10.1007/s11356-023-26853-x

Stallings, W. (2021). Operating Systems: Internals and Design Principles (9na ed.). Pearson. [Sustenta el uso de plataformas tipo Debian/Windows Server a nivel de infraestructura].

RESEARCH

Methodology for the Digital Security Maturity Assessment Test for Consulting Services

Noel Emilio Rojas Martos, M. Sc. [1*], Liban de Armas Granado, M. Sc. [2]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

This study presented a methodological model for diagnosing digital security maturity, geared towards institutions with diverse organizational structures. The objective was to develop a tool capable of identifying gaps, prioritizing actions, and aligning digital security with institutional objectives and those of the Policy for Digital Transformation, the Cuban Digital Agenda, and the Artificial Intelligence Strategy. The approach combined a modular assessment matrix, strategic interviews, and a customized roadmap. The proposal was structured around nine dimensions: digital leadership, digital workplace, technologies, information and communication, digital security policies and strategies, digital operations, digital culture and climate, cloud migration, legal and regulatory frameworks, and digital skills. Qualitative techniques and ordinal scales were applied to construct contextualized maturity profiles, which activated processes of internal reflection and strategic planning. The results obtained from its application can reveal vulnerability patterns such as the absence of formal

[1*] Master degree, Commercial Specialist, Project Department, Consulting Directorate. DCCH. noel.rojas@etecsa.cu

[2] Master degree, Head of Project Department, Consulting Directorate. DCCH. liban.dearmas@etecsa.cu

policies, a weak reporting culture, and dependence on individual actors. At the same time, sustainable improvement opportunities were identified, achievable without complex technical requirements. The roadmap outlined phased actions, adaptable to each institutional context. The model demonstrated the capacity not only to diagnose but also to enable organizational transformation processes. Its application can foster institutional strengthening, prepare for external audits, and integrate digital security as a strategic component. Its incorporation as a foundational phase in continuous improvement and digital transformation processes is proposed.

Keywords: diagnosis; dimensions; model; transformation; security

Introduction

This study developed a methodological model for diagnosing digital security maturity geared towards institutions with diverse organizational structures. Its objective is to facilitate the identification of gaps, prioritize improvement actions based on the institutional level, support secure digital transformation processes, facilitate alignment with regulatory frameworks and international standards, and align digital security with institutional objectives, in line with the Policy for Digital Transformation, the Cuban Digital Agenda, and the Artificial Intelligence Strategy.

The evolution of information protection at the international level has given rise to a series of key concepts that transcend the technical defense of systems and data, and which today constitute pillars for assessing institutional maturity (Von Solms & Van Niekerk, 2013). Among these concepts, we highlight those most relevant to the design and application of assessment models:

1. **Cyber resilience:** the ability of an organization to anticipate, withstand, recover from, and adapt to cyber incidents (ITU, ENISA, NIST). Application in the model: Incorporated through indicators of operational continuity, crisis management, organizational learning, and adaptive flexibility.

2. **Digital security as a national capability:** digital security is a strategic capability involving legislation, infrastructure, education, cooperation, and governance (Global Cybersecurity Index [ITU]). Application in the model: It enables mapping institutional alignment with national policies, sectoral strategies, and regulatory frameworks.
3. **Socio-technical approach:** digital security is a phenomenon combining technology, people, processes, and culture (Von Solms & Van Niekerk). Application in the model: Justifies the inclusion of dimensions such as leadership, organizational culture, risk perception, and internal communication.
4. **Multi-level governance:** digital security requires coordination among local, national, and international actors, both public and private (UN Convention on Cybercrime [2024], EU and Latin American Cybersecurity Strategies). Application in the model: Evaluates institutional participation in collaborative networks, regulatory interoperability, and inter-institutional coordination capacity.
5. **Digital maturity and security by design:** digital security must be integrated from the design phase of processes, systems, and policies (ISO/IEC 27001, NIST Cybersecurity Framework). Application in the model: Diagnoses whether digital security is structurally incorporated or responds to a reactive logic.

The incorporation of these concepts allows the assessment model to transcend a technical audit and become a strategic tool for institutional transformation. By evaluating the nine dimensions covered by the assessment under study (digital leadership, digital workplace, technologies, information and communication, digital security policies and strategies, digital operations, digital culture and climate, cloud migration, legal and regulatory frameworks, and digital skills), it positions itself as an instrument aligned with international best practices and adaptable to national contexts.

The research was based on theoretical and methodological contributions from authors such as Von Solms and Van Niekerk (2013), who expanded the concept of digital security beyond technical aspects;

Siponen and Pahnila (2018), who addressed organizational compliance with security policies; Cuban regulations including Decree-Law 78/2023 "On the security and protection of classified and restricted information", Decree 104/2024 "Regulations for the security and protection of classified and restricted information", Decree 360/2019 "On ICT security and the defense of national cyberspace", Resolution 128/2019 "ICT Security Regulations", Resolution 105/2021 "Regulations on the national action model for cyber incident response"; and international frameworks such as the NIST Cybersecurity Framework (National Institute of Standards and Technology [NIST], 2018), ISO/IEC 27001 and 27002, and CIS Controls. The proposed assessment also enabled organizational transformation processes through a phased, adaptable, and action-oriented roadmap.

Materials and Methods

This research paper proposes a digital security maturity assessment for consulting services focused on digital transformation. To this end, it was necessary to conduct an approach to the theoretical framework and the state of the art of the main concepts and models associated with cybersecurity, as well as an analysis of regulations, standards, and publication recommendations from the ITU, cybersecurity companies, Cuban regulations related to the research topic, and identified trends and best practices. The research was supported by bibliographical sources from a broad range of stakeholders (regulators, operators, consultants, academics).

Through the assessment , the aim is to facilitate the identification of vulnerabilities associated with digital security and other intangible capabilities across budgeted and enterprise sectors, as well as other economic players interested in the digital transformation process. It offers the possibility of diagnosing the level of digital security maturity, drawing a strategic roadmap for the qualitative and quantitative improvement of its management, and increasing its outcomes. The assessment has practical implications because it constitutes one of the pillars of the project for the design and implementation of consulting services at the Telecommunications Company of Cuba

(ETECSA, in Spanish), making a contribution to Cuban society based on implemented best practices; it can also have a positive impact on the country's digital transformation process. The economic benefit is estimated based on savings from import substitution, derived from the company's in-house design and the intrinsic value of information, without the need for external consulting services.

This research combined theoretical and statistical-mathematical methods. From a theoretical perspective, the search, identification, and review of relevant literature were conducted to gather key information. Analysis and synthesis were applied to all consulted specialized literature from subject matter experts, cybersecurity companies, consulting firms, and international organizations, among others.

Systemic approaches were employed to ensure the integration, interrelation, interdependence, and synergy of the dimensions that contribute to the overall assessment. The method of moving from what is abstract to what is complex was implemented, and a system of conceptual abstractions was developed for each dimension, along with levels of analysis that enabled a study progressing from general to specific aspects in order to obtain a comprehensive picture of the process.

With the historical-logical method, it was possible to contextualize the subject of study within history and its evolution, from the emergence of cybersecurity as a science to the present day. Empirical methods such as literature review were used, through which a broad bibliography related to the proposed objective was accumulated, followed by selection, critical review, and summary to draw conclusions. Scientific observation was used to study the practical experience of various cybersecurity assessments and the results of their implementation, enabling the formulation of the problem, hypothesis testing, and projecting the social impact of the solution based on the widespread application of the assessment.

The research led to the development of a specific test (checklist) as an instrument to measure the level of digital security maturity, serving as a tool to diagnose the current state of agencies, enterprises, and organizations.

Results and Discussion

The digital security maturity assessment is based on the best practices of the Global Cybersecurity Index (GCI), published by the International Telecommunication Union (ITU). Furthermore, it is part of the TETR4DIG technology (Organizational Change Management Model Focused on Digital Transformation [De Armas Granado & Díaz Monjiotti, V2: 2022]) (Figure 1).

This assessment evaluates organizational commitment to digital security according to the five pillars of the Global Cybersecurity Agenda: legal, technical, and organizational measures, as well as capacity building and cooperation (Center for Internet Security [CIS], 2021). In addition, it corresponds with the eight strategic axes of the Policy for Digital Transformation, the Cuban Digital Agenda, and the Artificial Intelligence Strategy. Regarding its methodology, it is designed in the form of a test (checklist-style survey) for each of the dimensions.

Its objectives are to identify strengths and weaknesses in the organization's infrastructure; to identify risks and vulnerabilities; to create an action plan to improve digital security maturity, including short-, medium-, and long-term goals; to foster awareness and a culture of digital security; and to prepare the organization for compliance with approved national standards and policies.

To carry out the assessment , nine dimensions were identified that form part of the Digital Security Model (see Figure 2) presented during

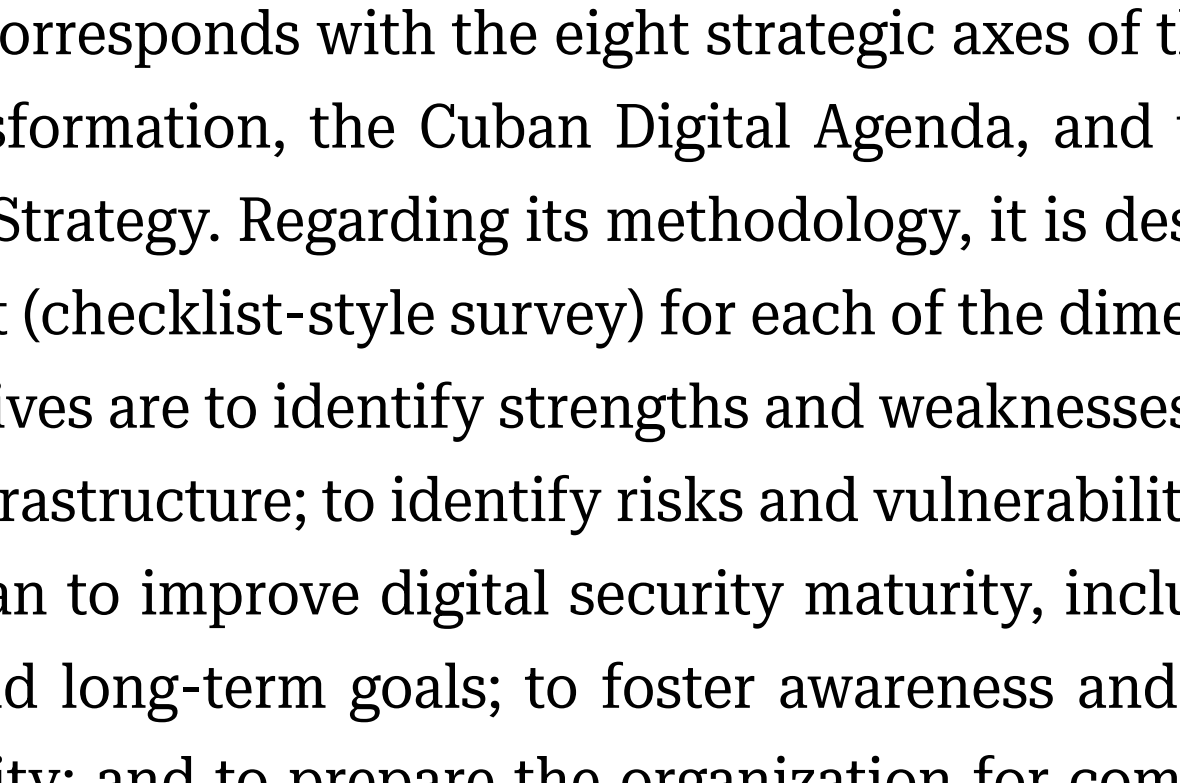


Figure 1. TETR4DIG: Organizational Change Management Model Focused on Digital Transformation (de Armas Granado, Liban; Díaz Monjiotti, Ela. 2022)



Figure 2. Digital Security Model Based on TETR4DIG Technology. (Rojas Martos, Noel E. 2024)

the events "Cybersecurity in Telecommunications 2023" and "XVI Ibero-American Seminar on Information Technology Security 2024".

Model Structure and Definition of Dimensions

Based on the rationale of the assessment, a review of Cuban regulations, international frameworks, and the conceptualization of TETR4DIG technology, an assessment tool was designed to evaluate the degree of advancement, integration, and sustainability of digital security in institutional environments.

These dimensions are not conceived as isolated elements, but as interdependent components forming a secure, resilient, and development-oriented digital ecosystem. The graphic representation of the model (centered on the concept of 'Digital Security' as an articulating core) visualizes the systemic relationship among leadership, policies, technology, culture, skills, and regulatory frameworks.

Each dimension responds to specific evaluation criteria and directly links to the strategic axes of the Cuban Policy for Digital Transformation, ensuring the contextual relevance of the instrument and its capability to guide continuous improvement processes, strategic planning, and regulatory compliance. The evolution of all dimensions represents a strategic component contributing to the strengthening of institutional digital security, and their evaluation identifies the level of maturity, integration, and alignment with policy axes. The meaning and scope of each evaluated dimension in the test is described below:

Digital leadership: It assesses senior management's commitment to cybersecurity as a key driver of institutional transformation. It includes the existence of clear policies, assignment of responsibilities, and strategic decision-making capability. Mature leadership drives digital governance and promotes an organizational culture oriented toward resilience.

Digital security policies and strategies: it analyzes the presence, updating, and application of institutional policies related to cybersecurity, data protection, and risk management. It determines whether these policies are aligned with national and international regulatory frameworks and integrated into organizational strategic planning.

Digital workplace: It assesses the degree of work environments digitalization. It includes the use of technological tools, process automation, and secure access to digital platforms. It also includes training for staff on the responsible and safe use of digital resources.

Information and Communication Technologies (ICTs): It examines available technological infrastructure, its level of interoperability, connectivity, and capacity to enable secure digital services. It includes technological asset management, system updates, and implementation of innovative solutions.

Culture and digital climate: It measures the level of awareness, participation, and trust of institutional actors in the digital environment. It evaluates the existence of awareness campaigns, inclusive practices, and mechanisms to foster digital values such as responsibility, ethics, and collaboration.

Legal and regulatory frameworks: It determines the organization's degree of compliance with current regulations on data protection, digital identity, cybersecurity, and artificial intelligence. It includes the existence of audit mechanisms, legal control, and regulatory adaptation.

Cloud migration: It explores the use of emerging technologies, particularly cloud computing, as a strategy to improve efficiency, scalability, and security of digital services. It addresses issues such as supplier management, data protection in virtual environments, and business continuity.

Digital operations: It evaluates the transformation of internal processes and public services through digital platforms, online procedures, and one-stop shops. It measures operational efficiency, user experience, and institutional responsiveness in digital environments.

Digital skills: It analyzes training, updating, and development of digital competencies among institutional staff. It includes knowledge in ICT, cybersecurity, artificial intelligence, and data management, as well as the existence of continuous training programs.

The analysis obtained through the digital security maturity assessment test reveals an institutional structure that, while having advanced in adopting technologies and digital policies, still faces challenges in the systemic integration of security as a cross-cutting axis. The analytical matrix and dimensional model make it possible to identify strengths in areas such as ICT infrastructure and digital operations, as well as gaps in strategic leadership, organizational culture, and digital skills.

The correspondence between the evaluated dimensions and the strategic axes of the Cuban Policy for Digital Transformation validates the contextual relevance of the model. This makes it possible to position it as a methodological tool capable of guiding continuous improvement processes, institutional planning, and regulatory compliance. Furthermore, by incorporating socio-technical approaches and digital governance principles, the assessment transcends technical auditing and it becomes an instrument for organizational transformation. This analysis not only helps characterize the current state of digital security in the institutions evaluated, but also provides practical input for strategy development, decision-making, and capacity building, with a view toward a secure, inclusive, and sustainable digital transformation.

Articulation of the Assessment Model With the Cuban Policy for Digital Transformation

The results of the digital security maturity assessment were organized into a matrix linking each evaluated dimension to the strategic axes defined in the “Cuban Policy...” This articulation validates the model's relevance in the national context and demonstrates its capacity to operationalize the public policy's guiding principles. The matrix

reveals a direct correspondence between the model's dimensions and the policy's strategic components, as shown below (Table 1):

Table 1. Linkage of dimensions with the Policy for Digital Transformation, the Cuban Digital Agenda, and the Artificial Intelligence Strategy and its Eight Strategic Axes.
Source: Authors' elaboration

No.	Digital Security Assessment Dimension	Connection to Cuban Policy	Strategic Axes	Factual Basis
1	Digital Leadership	The policy establishes that the State leads digital transformation as a "comprehensive, strategic, and urgent process" (p. 6), with a digital governance approach and multisectoral participation.	Regulatory Framework, Digital Government	Leadership drives the adoption of legal frameworks, public policies, and digital governance within the organization.
2	Digital Workplace	It promotes the digitalization of work processes, automation, and the use of digital tools in sectors such as health, education, and public administration (p. 12).	Digital Economy, Education and Digital Culture	It modernizes work environments, fosters digital productivity, and promotes technological literacy among staff.
3	Information and Communication Technologies (ICTs)	It prioritizes the development of digital infrastructure, connectivity, system interoperability, and accessible digital services (p. 9).	Digital Economy, Digital Government, Innovation	Technologies enable digital services, interoperability, automation, and the development of new business models.
4	Digital Security Policies and Strategies	It recognizes the need for a National Cybersecurity Strategy, personal data protection, and resilience against digital threats (p. 10).	Cybersecurity, Regulatory Framework	It reinforces data protection, risk management, and regulatory compliance in digital environments
5	Digital Operations	It drives the transformation of public services, online procedures, e-government platforms, and digital single windows (p. 13).	Digital Government, Digital Economy	It digitalizes internal processes and public services, improving efficiency and user experience.
6	Culture and Digital Climate	It promotes an inclusive digital culture, with emphasis on digital literacy, citizen participation, and trust in the digital environment (p. 11).	Education and Digital Culture, Digital Content	It promotes digital values, citizen participation, and the creation of inclusive digital content.
7	Cloud Migration	It refers to the adoption of emerging technologies such as cloud computing to improve the efficiency and security of digital services (p. 14).	Innovation, Cybersecurity	It facilitates scalability, flexibility, and security of digital services through emerging technologies.
8	Legal and Regulatory Frameworks	It proposes updating the legal framework to regulate data protection, digital identity, cybersecurity, and artificial intelligence (p. 15).	Regulatory Framework, Cybersecurity	It ensures that the organization complies with laws on data protection, digital identity, and AI.
9	Digital Competencies	Priority is given to developing digital talent and providing training in AI, ICT, and digital skills for all sectors (p. 16).	Education and Digital Culture, Innovation	It develops capabilities in ICTs, AI, and cybersecurity, aligned with continuous learning and innovation.

The correlation between the model's dimensions and the strategic pillars of Cuban policy confirms that the assessment not only evaluates the current state of institutional cybersecurity but also guides its alignment with national objectives. This contextual validation reinforces the model's utility as a tool for strategic planning, continuous improvement, and accountability.

Furthermore, the matrix shows that digital security is not limited to technical aspects, but spans leadership, culture, skills, regulations, and processes, in alignment with multi-level governance and socio-technical approaches promoted internationally. In this sense, the model contributes to positioning digital security as a comprehensive axis of institutional transformation.

Requirements Measured by the Test for Each Dimension

In order to implement the digital security maturity assessment model, a set of 160 items was designed across the nine strategic dimensions. Each item represents a specific requirement evaluating the degree of compliance, integration, and sustainability of institutional practices, policies, and capabilities in digital security. These requirements were formulated based on a critical review of Cuban regulations and international frameworks described earlier, as well as digital governance principles and guidelines of the "Cuban Policy..." Likewise, socio-technical, organizational, and regulatory criteria were incorporated to capture the complexity of the institutional digital environment.

The test structure follows a modular logic, where each dimension groups requirements ranging from technical and regulatory aspects to cultural, operational, and strategic factors. This organization facilitates the application of the instrument across different institutional types, enables the identification of specific gaps, and guides the formulation of contextualized improvement plans. Table 2 presents the requirements evaluated for each dimension along with a brief description justifying their inclusion and assessment relevance:

Table 2. Requirements Evaluated for Each Dimension, Accompanied by a Brief Description Justifying Their Inclusion and Assessment Relevance. Source: Authors' elaboration

No.	Dimension	Item objective	Evaluated Criteria (Summary)
1	Digital Leadership	To identify leadership structures, assignment of responsibilities, and institutional vision.	Approved policies, designated leaders, strategic planning, security culture, allocated resources.
2	Digital Security Policies and Strategies	To verify regulatory coherence, updating, and effectiveness of policies.	Existence, legal alignment, dissemination, auditing, response protocols, institutional participation.
3	Digital Workplace	To determine technical conditions, safe use of technologies, and staff training.	Digital tools, device protection, automation, access management, backup.
4	Information and Communication Technologies (ICTs)	To evaluate robustness, interoperability, and system updates.	Infrastructure, interoperability, monitoring, scalability, external integration.
5	Digital Culture and Climate	To identify values, practices, and perceptions supporting digital security.	Awareness building, risk perception, digital ethics, participation, feedback.
6	Legal and Regulatory Frameworks	To verify legal alignment, auditing, and regulatory adaptation.	Current legislation, international standards, auditing, legal training.
7	Cloud Migration	To evaluate planning, vendor management, and cloud data protection.	Adoption strategy, virtual security, operational continuity, authentication.
8	Digital Operations	To determine operational efficiency and user experience.	Digitalization, automation, interoperability, monitoring, citizen feedback.
9	Digital Competencies	To identify technical readiness, training programs, and institutional alignment.	Competency assessment, continuous training, certifications, learning networks.

Table 3 summarizes the main components of the test, where each dimension groups a set of items evaluating practices, capabilities, and institutional policies linked to digital security. In addition to the number of evaluated items, key recommendations are included to guide the interpretation of results and the formulation of improvement actions according to the identified maturity level.

Table 3. Summary table synthesizing the nine dimensions of the digital security maturity assessment test, the number of evaluated items in each, and key recommendations according to expected results. Source: Authors' elaboration

No.	Dimension	Evaluated Items	Key Recommendations According to Expected Results
1	Digital Leadership	24	To strengthen executive commitment, assign leaders, integrate security into strategic planning.
2	Digital Security Policies and Strategies	26	To formalize and update policies, to align them with regulatory frameworks, to ensure effective dissemination and application.
3	Digital Workplace	13	To digitalize work processes, protect devices, train staff in safe technology usage.
4	Information and Communication Technologies (ICTs)	20	To modernize infrastructure, to ensure interoperability, to implement monitoring and technology update mechanisms.
5	Culture and Digital Climate	12	To promote awareness campaigns, to foster digital values, to measure institutional perception and participation.
6	Legal and Regulatory Frameworks	20	To ensure regulatory compliance, to train on current legislation, to participate in regulatory processes.
7	Cloud Migration	19	To design adoption strategies, to select secure vendors, to protect data, and to guarantee operational continuity.
8	Digital Operations	14	To automate procedures, to improve user experience, to integrate platforms, and to evaluate operational performance.
9	Digital Competencies	21	To implement continuous training programs, to diagnose competencies, to encourage professional development.

Application and Interpretation of the Test

The digital security maturity assessment test can be applied through a combination of semi-structured interviews, document review, and direct observation, adapted to the organizational characteristics of each evaluated institution. The 160 items distributed across the nine dimensions allow for a modular, flexible, and contextualized assessment, facilitating the identification of strengths, gaps, and improvement opportunities.

Each item is evaluated on an ordinal scale reflecting the degree of institutional compliance, allowing results to be classified into four maturity levels using the assessment system proposed by TETR4DIG technology as a reference:

Basic: Undocumented digital security processes, in constant change, arranged ad hoc in a reactive manner.

Initial: Digital security processes executed uniformly with consistent results; implementation of digital security measures has begun in some areas of the entity.

Strategic: Strategically integrated digital security processes. Implementing a digital security roadmap holistically and integrally, oriented toward company resources and clients, with standardized, defined, and documented processes undergoing periodic review.

Innovative-disruptive: Digital security processes for data and information protection at the forefront; consolidated digital leadership; continuous improvement of effectiveness through technological change and innovation; and agile, innovative, flexible, connected, collaborative, open processes using relevant data protected across multiple technological mediums. Continuously adapting to changes.

This classification enables the construction of maturity profiles per dimension, identification of common patterns among institutions, and guidance for formulating specific improvement plans. In addition, it facilitates longitudinal comparison and assessment of the impact of strategic digital security interventions.

Conclusions

This article has proposed a digital security maturity assessment model specifically designed for institutional consulting services. Grounded in a socio-technical and interdisciplinary approach, the model allows evaluating the degree of integration, sustainability, and strategic alignment of digital security in public and private organizations, aligned with the strategic axes of the Cuban Policy for Digital Transformation and international reference frameworks (ISO/IEC 27001, NIST, ITU).

The modular structure of the assessment (composed of nine strategic dimensions and 160 evaluative items) facilitates a comprehensive characterization of the institutional digital environment, ranging from leadership and organizational culture to technological infrastructure, regulatory policies, and staff skills. This breadth makes it possible to identify specific gaps, guide improvement plans, and strengthen organizational capabilities toward a secure, inclusive, and resilient digital transformation.

The results obtained demonstrate that digital security cannot be approached as an isolated technical component, but rather as an integral process requiring committed leadership, effective governance, continuous training, and regulatory articulation. In this regard, the model positions itself as a valuable methodological tool for consultants, managers, and institutional leaders seeking to integrate digital security into their planning, evaluation, and decision-making processes.

Its application does not replace cybersecurity services currently in the portfolio of the Consulting Directorate; rather, it identifies weaknesses and opportunities so that these services can be contracted by those conducting the assessment . In conclusion, the potential of the assessment as a longitudinal monitoring instrument, adaptable to diverse sectoral contexts and scalable according to technological and regulatory advances, is highlighted. Its systematic application can contribute to strengthening security culture, improving institutional quality, and achieving strategic digital transformation objectives in Cuba and similar environments.

It is recommended to conduct an analysis of the indicators for each dimension comprising the digital security model, so that the assessment can be contracted by international organizations as part of consulting services.

References

De Armas Granado, L., Díaz Monjiotti, E., & Tito Bertor, A. (2021). *De la ciberseguridad a la seguridad digital en los servicios de consultoría de la Empresa de Telecomunicaciones de Cuba S.A*. En III Taller de Ciberseguridad “Bienestar para todos”. La Habana: ETECSA.

D’Antonio, G., & Olías de Lima, P. M. (2019). *Digital security en la nueva era de transformación digital*. Madrid: Real Instituto Elcano.

Decreto 104/2024. (2024). *Reglamento de la seguridad y protección de la información clasificada y limitada*. Gaceta Oficial de la República de Cuba.

Decreto 360/2019. (2019). *Sobre la seguridad de las TIC y la defensa del Ciberespacio Nacional*. Gaceta Oficial de la República de Cuba.

Decreto-Ley 78/2023. (2023). *Sobre la seguridad y protección de la información clasificada y limitada*. Gaceta Oficial de la República de Cuba.

ISO/IEC 27001. (2013). *Information technology – Security techniques – Information security management systems* – Requirements. Geneva: International Organization for Standardization.

ISO/IEC 27002. (2013). *Information technology – Security techniques – Code of practice for information security controls*. Geneva: International Organization for Standardization.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). Gaithersburg, MD: U.S. Department of Commerce.

Observatorio de la Ciberseguridad. (s. f.). *Indicador de madurez en ciberseguridad*. Recuperado de https://observatoriociberseguridad.org

Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia de Inteligencia Artificial. Ministerio de Comunicaciones, 2024.

Resolución 105/2021. (2021). *Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad*. Gaceta Oficial de la República de Cuba.

Resolución 128/2019. (2019). *Reglamento de Seguridad de las TIC*. Gaceta Oficial de la República de Cuba.

Rojas Martos, Noel E. *Modelo de Seguridad Digital basado en la tecnología TETR4DIG*. III Taller de Ciberseguridad. La Habana: ETECSA. XVI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información" (Palacio de las Convenciones. Cuba. 2024).

Siponen, M., & Pahnila, S. (2018). Hacia un modelo unificado de cumplimiento de la política de seguridad de la información. *Revista de Seguridad Informática*. 34 (2), 45–62.

Solms, B. von, & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38, 97–102.

RESEARCH

The AI Revolution in Telecommunications: A Journey from the Past to the Future

Rafael Alberto Noa Yanes [1*], Ivette García Montero, Eng. [2]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

This article, derived from the research seminar developed within the framework of the scientific exchange between the "Vladimir Ilich Lenin" Pre-University Vocational Institute of Exact Sciences and ETECSA, analyzes the transformative impact of artificial intelligence (AI) on the telecommunications sector. Through a documentary review and a multiple case study, four structural challenges of the pre-AI era were identified: manual management of exponential data traffic, saturation of customer service, reactive infrastructure maintenance, and static signature-based cybersecurity.

AI-enabled solutions are presented, such as self-optimizing networks, chatbots and virtual assistants, predictive maintenance, and real-time anomaly detection systems, documented with success stories from Google, Telefónica, Nokia, IBM, Movistar, Vodafone, among others. The discussion compares the previous reactive model with the current proactive and autonomous model, evidencing quantifiable reductions. It is concluded that AI has moved from being a futuristic promise to a decisive competitiveness factor, and its strategic adoption

[1*] Vladimir Ilich Lenin High School Vocational Institute of Exact Sciences

[2] Empresa de Telecomunicaciones de Cuba. VPEM. ivette.garcia@etecsa.cu

is recommended, along with investment in research, development, and academia-industry partnerships to prepare young talent for the future of telecommunications.

Keywords: Artificial Intelligence; telecommunications; predictive maintenance; cybersecurity; network automation

Introduction

Telecommunications have come a long way since the earliest long-distance communication systems: smoke signals, drums, the 4th century BC hydraulic telegraph, and the optical telegraph, considered the first modern system. In the 19th century, electric telegraphy and, later, telephony laid the foundations of today's industry, with milestones such as the first transatlantic cable (1858) and the founding of iconic companies like the Electric Telegraph Company (1846) and AT&T (1885). Figure 1 visually summarizes these key moments and their connection to the arrival of Artificial Intelligence (AI). Today, however, the challenge is no longer just overcoming physical distance, but managing the torrent of data flowing through networks.

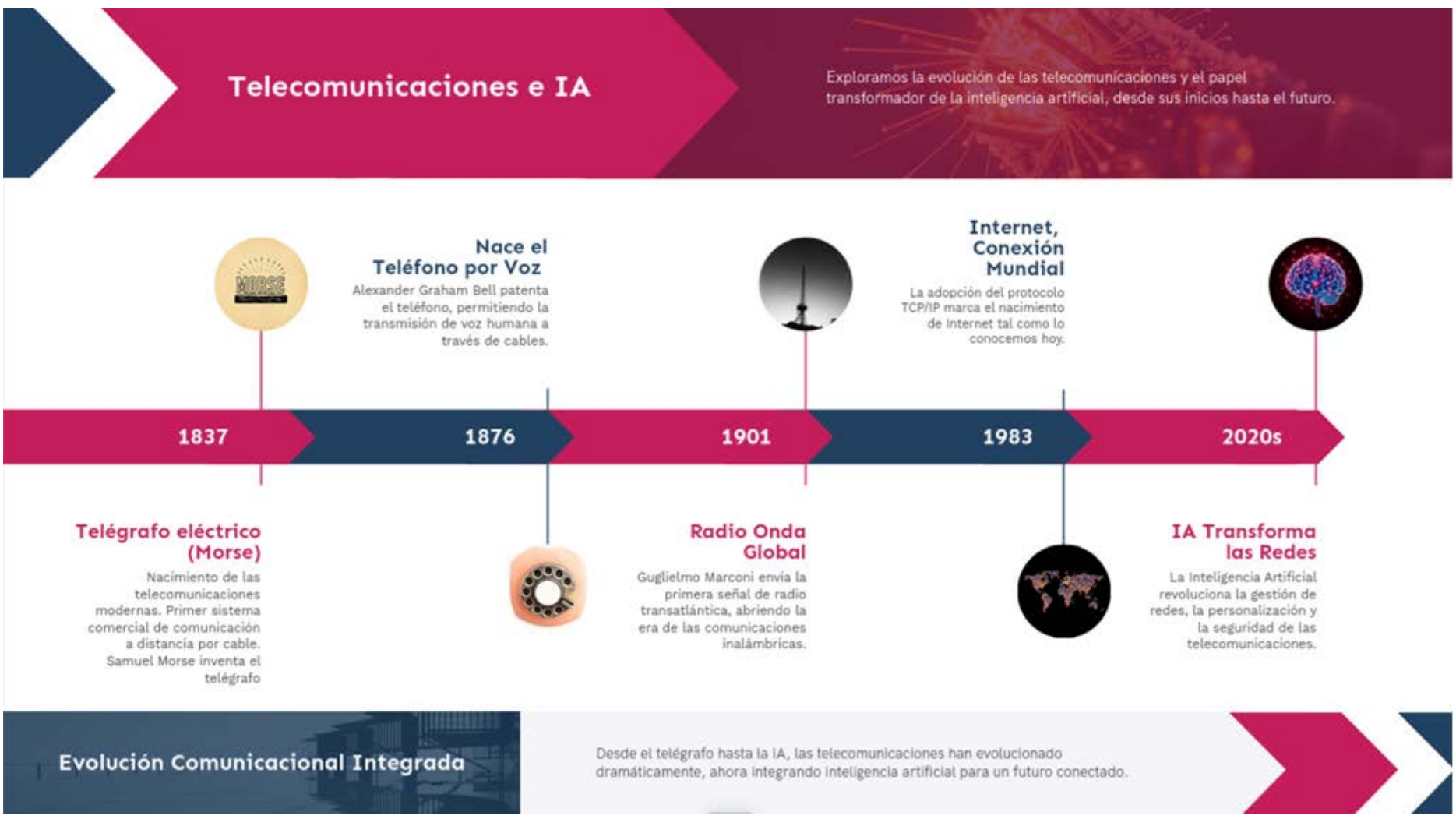


Figure 1. A Journey from the Past to the Future

This article aims to analyze the transformative impact of Artificial Intelligence (AI) on the telecommunications sector, identifying the main problems the industry faced before its implementation and showing how AI has helped to overcome them. The work is framed within the

scientific exchange between the "Vladimir Ilich Lenin" Pre-University Vocational Institute of Exact Sciences and ETECSA, with the aim of fostering collaborative innovation and preparing young talent for the challenges of the digital future.

The specialized literature and reports from leading companies (Cisco, Google, Telefónica, Nokia, IBM) have documented significant advances in areas such as network self-optimization, customer service through virtual assistants, predictive maintenance, and proactive cybersecurity. However, this article does not merely compile these contributions; it organizes them into an analytical framework that helps understand the evolution from a reactive model to an autonomous, intelligent one. The novelty lies in the systematization of these case studies and their application to the context of telecom cariers such as ETECSA, where collaboration with educational institutions drives knowledge transfer and the adoption of advanced technologies.

Materials and Methods

The research was carried out using a qualitative approach, based on the review and documentary analysis of specialized sources. A multiple case study methodology was employed, selecting representative companies from the telecommunications sector that have implemented AI solutions with publicly documented results.

Sources of Information

- Technical reports and press releases from leading companies: Cisco, Google, AT&T, Telefónica, Nokia, Ericsson, Movistar, Vodafone, Orange, and Verizon.
- Publications from international organizations and academic institutions, including IBM, the Luca de Tena Journalism Laboratory, and the Spanish Association of Telecommunications Engineers.
- Specialized articles in industry journals and technology platforms (Metaverso, Minsait, Aunoa).
- General reference materials (Google Cloud) to establish definitions and historical context.

Procedure

Identification of pre AI challenges: Recurring problems documented in the literature prior to the massive adoption of AI were analyzed,

classifying them into four categories: data traffic management, customer service, infrastructure maintenance, and cybersecurity.

- **Selection of success stories:** Companies with mature AI implementations were selected in each of the four areas, prioritizing those that reported quantitative metrics (reduction in outages, percentage of automated inquiries, decrease in false alarms, etc.).
- **Comparative analysis:** The “before” and “after” situations of AI were contrasted for each challenge, extracting the elements that demonstrate substantial improvement.
- **Contextualization:** The findings were integrated within the framework of the scientific exchange between the "Vladimir Ilich Lenin" Pre-Universitary Vocational Institute and ETECSA, highlighting how academia industry collaboration can accelerate the adoption of these technologies.

Results and Discussion

The Four Challenges of the Pre AI Era: an Analysis of the Structural Limitations

The documentary analysis conducted made it possible to identify four recurring problems that characterized the operation of telecommunications networks before the massive incorporation of artificial intelligence. These challenges did not act in isolation; rather, they feed back on each other: manual traffic management worsened bottlenecks, unforeseen failures overwhelmed customer service centers, and reactive security left exposure windows that widened with the exponential growth of data. Understanding this interrelation is key to appreciating the transformative impact that AI has had in addressing them comprehensively.

1. Exponential Data Growth and Manual Network Management

The rise of mobile phones and the Internet caused an unprecedented increase in data demand. Every second, demand grows; traffic increases progressively, placing unsustainable pressure on infrastructure not designed for such volume. In regions where AI is not used, operators monitor network performance manually, employ basic automation systems for device configuration, and perform limited data analysis. This leads

to so-called “bottlenecks,” which disrupt production and degrade the user experience. An emblematic case is Verizon, which experienced this problem in its Customer Service during peak demand periods, resulting in prolonged wait times and a less satisfactory experience.

2. Saturation of Customer Service

Customer dissatisfaction caused by bottlenecks is funneled into call centers, which constantly receive requests, complaints, and questions. Demand for this service also grows exponentially, but the quality of attention depends entirely on the experience and knowledge of the human operator, which requires ongoing training and generates long wait times. The IBM report cited in the literature notes that, before the adoption of chatbots, more than 60% of calls corresponded to routine inquiries, consuming a significant portion of operational resources.

3. Reactive Maintenance and Delayed Response to Failures

In the pre-AI era, infrastructure problems were only detected through user reports or manual monitoring. This meant technicians intervened only after receiving complaints or noticing a drop in performance. A paradigmatic example is AT&T, which between 2007 and 2010 faced severe network congestion following the launch of Apple's iPhone. The infrastructure was not prepared to handle the sudden increase in traffic, and the lack of predictive capabilities caused recurring outages during high-demand events.

4. Static Cybersecurity and Limited Threat Detection

Telecommunications companies built their protection systems on static firewalls and signature databases. These systems compare network traffic against known patterns of malicious activity, but they only identify previously recorded attacks and require constant manual updating. As traffic grows progressively, monitoring becomes unsustainable, generating “false positives” (unnecessary alarms) and “false negatives” (overlooked threats). This methodology was especially vulnerable to zero-day attacks, such as those experienced during the 2017 WannaCry ransomware outbreak, in which several companies relying exclusively on signature-based systems suffered infections.

Below, in Figure 2, the four systematized challenges are presented, accompanied by concrete documented examples:



Figure 2. The Four Major Telecommunications Challenges Before AI

These results show that the traditional model operated reactively, with human intervention as a bottleneck and structural limitations in adapting to the rapid growth in demand.

Solutions Enabled by AI

In a context dominated by human intervention, rigid systems, and the inability to anticipate problems, artificial intelligence has emerged as a technological enabler that radically transforms telecommunications operations. AI-based solutions are not limited to automating repetitive tasks; they introduce learning capabilities, real-time adaptation, and autonomous decision-making. The following table presents the main results documented in the literature and in reports from pioneering companies, organized according to the four previously identified challenges (Table 1).

Table 1. AI-Enabled Solutions for Each in the Telecommunications Sector

Challenge	AI-Based Solution	Documented Success Stories and Metrics
Traffic Management	Networks that self-optimize in real time through analysis of large volumes of data. AI makes it possible to dynamically adjust parameters, redistribute bandwidth, and anticipate congestion.	**Google** implemented the B4 system in its Software-Defined Networks (SDN), optimizing bandwidth usage between global data centers. **Cisco** has developed autonomous networks that self-configure, self-protect, and self-repair, drastically reducing the need for human intervention. **Huawei** integrated AI into its 5G networks, achieving energy efficiency.
Customer Service	Chatbots and virtual assistants with natural language processing, available 24/7, capable of handling repetitive inquiries and offering personalized responses based on user history.	According to an **IBM** report, companies that use chatbots can handle up to **80% of routine inquiries**, representing significant savings in operating costs. **Movistar** developed **Aura**, a virtual assistant that manages services, billing inquiries, and personalized recommendations. **Vodafone** uses **TOBi**, **Orange** has **Djingo** and **Verizon** has its own chatbot for technical support and billing assistance.

Maintenance	Predictive maintenance based on sensors connected to the infrastructure and **Machine Learning** algorithms that process large volumes of data to identify patterns, anomalies, and subtle deviations that indicate a possible future failure.	**Telefónica** implemented a Predictive Network Maintenance project that reduced **unplanned outages by 30%**. **Nokia**, with its **Nokia Predictive Care** platform, achieved **50% fewer false alarms** and improved network availability. **Ericsson** provides the **Ericsson Operations Engine** platform, used by operators such as **Telia Company** in Sweden, achieving a **25% reduction in service outages**.
Cybersecurity	Real-time anomaly detection systems, based on machine learning, that analyze behavior rather than relying solely on known signatures. They enable automatic responses (isolating compromised systems, blocking malicious IPs, applying patches) and continuously adapt to new cybercriminal tactics.	Documented benefits include **fast detection**, reduced exposure time to vulnerabilities; **decreased false positives and false negatives**; and **threat prediction capability** based on historical patterns and behavioral analysis. All of this translates into greater security, convenience, and trust for customers.

Discussion: Before and After, a Structural Transformation

The comparison between the pre AI and post AI scenarios reveals a transformation that goes beyond a mere incremental improvement. This represents a paradigm shift in the way telecommunications operate, affecting network architecture, customer relationships, and the ability to respond to contingencies.

This comparison shows that AI not only solves existing problems but redefines the very nature of operations. It marks a shift from a reactive model, where technology acted as passive support to human intervention, to a proactive and autonomous model, where AI is a central component that anticipates, decides, and executes. The novelty lies not only in the individual technologies (chatbots, SDN, sensors), but in their integration into unified management platforms that enable a closed automation loop: the network detects an anomalous condition, AI makes a decision, and executes the correction without human intervention.

Furthermore, the cases analyzed demonstrate that this transformation is scalable and quantifiable. The documented percentage reductions (30% in outages, 50% in false alarms, 80% in routine inquiries) are not anecdotal; they reflect sustained improvements that directly impact user satisfaction, operational efficiency, and profitability. Companies such as Telefónica, Nokia, and Ericsson have turned these capabilities into service offerings already used by operators in multiple countries, validating the technology's maturity.

Taken together, the gathered evidence confirms that AI has moved from being a futuristic promise to a decisive competitiveness factor in the telecommunications sector. Its adoption does not simply mean incorporating new tools, but reimagining processes and operational culture to make the most of the capabilities for anticipation, automation, and continuous learning (Figure 3).



Figure 3. AI Impact on Telecommunications: From the Reactive Model to the Proactive/Autonomous Model

Conclusions

This work has achieved the following objectives:

1. To identify and characterize the four fundamental challenges that telecommunications faced before the adoption of AI: manual management of exponential traffic, saturation of customer service, reactive maintenance, and static cybersecurity.
2. To demonstrate through documented success stories (Google, Telefónica, Nokia, IBM, etc.) that AI offers effective solutions, with quantifiable reductions in outages, false alarms, and operating costs, as well as substantial improvements in user experience.
3. To show the shift from a reactive model to a proactive, autonomous one, where artificial intelligence makes it possible to anticipate problems, automate responses, and free up human talent for higher-value strategic tasks.

Contributions

Beyond compiling information, this article systematizes the findings into an analytical framework that can serve as a reference for operators still in the early stages of AI adoption. It also highlights the importance of partnerships between operators and educational institutions to train new generations in emerging technologies, such as those described here.

Future Work

It is suggested to further explore AI applied to 5G and 6G networks, the Internet of Things (IoT), and the hyperautomation of network operations centers. It is also recommended to explore the ethical and governance challenges associated with intensive AI use, as well as to develop specific indicators to measure return on investment (ROI) on AI implementations in contexts such as Cuba, where ETECSA can act as a catalyst for digital transformation.

References

Asociación Española de Ingenieros de Telecomunicación. (n.d.). *Foro Histórico de las Telecomunicaciones*. Retrieved from https://www.aeit.es/soyteleco/grupos-de-trabajo/foro-historico-de-las-telecomunicaciones

Aunoa. (n.d.). *Desafíos y Soluciones en el uso de Chatbots en Telecomunicaciones*. Retrieved from https://aunoa.ai/blog/desafios-y-soluciones-en-el-uso-de-chatbots-en-telecomunicaciones

Google Cloud. (n.d.). *¿Qué es una Inteligencia Artificial o IA?* Retrieved from https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419

International Business Machines Corporation (IBM). (n.d.). *Chatbots*. Retrieved from https://www.ibm.com/think/topics/chatbots

Laboratorio de Periodismo Luca de Tena. (n.d.). *Cinco lecciones sobre la evolución de los medios en 40 años: de la maquetación en papel a la Inteligencia Artificial*. Retrieved from https://laboratoriodeperiodismo.org/cinco-lecciones-sobre-la-evolucion-de-los-medios-en-40-anos-de-la-maquetacion-en-papel-a-la-inteligencia-artificial

Metaverso. (n.d.). *La Revolución de la IA en la Gestión del Tráfico de Red: Soluciones, Casos de Uso y Retos Éticos*. Retrieved from https://metaverso.pro/blog/la-revolucion-de-la-ia-en-la-gestion-del-trafico-de-red-soluciones-casos-de-uso-y-retos-eticos

Metaverso. (n.d.). *La Revolución de la IA en el Mantenimiento Predictivo de Infraestructuras de Telecomunicaciones*. Retrieved from https://metaverso.pro/blog/la-revolucion-de-la-ia-en-el-mantenimiento-predictivo-de-infraestructuras-de-telecomunicaciones

Minsait. (n.d.). *IA Aplicada a las Telecomunicaciones*. Retrieved from https://www.minsait.com/es/insights/ia-aplicada-las-redes-de-telecomunicaciones

Telefónica. (n.d.). *Programa de investigación sobre IA en Telecomunicaciones*. Retrieved from https://www.telefonica.com/es/sala-comunicacion/blog/programa-investigacion-ia-industria-telecomunicaciones

RESEARCH

Computer system for evaluating the InformationTechnologies impact on organizations

Ernesto Elias Elzaurdín Valdés, Eng.[1*], Meliza Leon Bencomo, Ts.[2], Mary Nelsa Bonne Cuza, M. Sc.[3]

Received: 01/2026 | Accepted: 03/2026 | Published: 07/2026

Abstract

Digital transformation has been essential for achieving success in organizations, but it goes beyond merely implementing technology. This needs a cultural and organizational change. The Information Technologies (IT) impact is measured according to their alignment with business objectives and their value to organizations. In Cuba specifically, technological dependence on suppliers complicates the renewal of information technology infrastructures, making impact assessment crucial. This research aims to develop a computer system to reduce the complexity in the process of evaluating the information technologies impact on organizations. To this end, the Extreme Programming (XP) agile software development methodology, the Django framework, the Python programming language for the backend, and HTML5, CSS3, and JavaScript for the frontend were applied. This solution should assist IT. specialists, workers, and managers in addressing multiple information security risks and protecting the most important assets for their organization.

[1*] University of Computer Sciences, Cuba, Carretera San Antonio de los Baños km 2 ½ La Lisa, ernestoeev@uci.cu

[2] University of Computer Sciences, Cuba, Carretera San Antonio de los Baños km 2 ½ La Lisa, mleonb@uci.cu

[3] University of Computer Sciences, Cuba, Carretera San Antonio de los Baños km 2 ½ La Lisa, mary@uci.cu

Keywords: risk management, impact measurement, computer system, Information Technologies

Introduction

In recent years, organizations have been committing themselves to digital transformation due to the evident advantages it brings to business. It is important to highlight that this transformation aims to achieve benefits in terms of information management, processes, resources, and even the reduction of human errors. However, it is not merely about implementing new technologies, but about achieving a cultural and organizational change that guarantees success within organizations (Liendo Afonso, 2023). It is evident that, once investments in technological infrastructure are made, their security must be ensured, as cyber threats are increasingly prevalent and represent a vulnerability for organizations. Therefore, it is necessary to focus efforts on implementing adequate security measures to reduce the levels of risk to which information is exposed (Martínez Landrove, 2019).

The growth of Information Technology (IT) infrastructures has led to a surge in research on their impact on the organizations (Casanova, Calderón, 2020). The results of various research have identified that the greater the alignment between IT and business objectives, the broader the added value that IT infrastructures represent for an organization (Pérez Lorences, 2014). Impact is measured according to the entity's mission, making it vital to understand all IT assets.

Each asset holds a specific value, and many are key components supporting the critical services provided to users. These assets also directly influence on the capital and organization valuation, and IT risks can have a direct impact on the budget. For every organization, it is vital and challenging to determine the conditions that truly impact on the mission. It is very important to continuously analyze and understand the resources that meet objectives and may be compromised by Cybersecurity risks (Quinn et al., 2022). An exploratory study conducted by Casanova (2020) describes the state of IT infrastructure management in Cuba. This study revealed that within organizations, the highest average impacts "correspond to

slowness in responding to the organization's needs, which implies a serious alignment problem" (Casanova, 2020, p. 41). Furthermore, it highlights "the problems of implementing new systems, due to the increased management complexity" (Casanova, 2020, p. 41). Cuban organizations are technologically dependent on their suppliers, which hinders the periodic and pertinent renewal of IT infrastructures.

Consequently, awareness has arisen regarding the importance of evaluating the impact on infrastructure. Cuba, as a developing country, does not produce technology and must therefore import it. This latter aspect represents a challenge due to the economic blockade. Hence, impact assessment is of particular importance (Casanova, Calderón, 2020). To this end, there are reference frameworks that generally describe how to measure the information security impact. However, these are very generic and must be adapted to the objectives of the organizations, and there are no tools to help document this analysis. Therefore, this research focuses on seeking to reduce the complexity in evaluating the IT impact on organizations through the development of a computer system. The study is based on the process of evaluating the IT impact on organizations within the field of action of computer systems that carry out this management.

Materials and Methods

The research theoretical design was developed from an analysis of the main terms and definitions related to impact assessment. Likewise, a state-of-the-art study was conducted, taking into account analogous systems. Extreme Programming (XP) was selected as the methodology due to the characteristics of the software development process. It was decided to develop the application using the Python v3.9.2 programming language for the backend and HTML5, CSS3, and JavaScript for the frontend, with the Django v4.1.3 framework and the PostgreSQL v11.0.2 database management system.

The theoretical methods used were:

1. **Analytical-synthetic:** for processing information related to impact assessment in / on organizations and reaching the conclusions of the research.

2. **Inductive-deductive:** for the development of the theoretical framework of the research.
3. **Systemic-structural-functional:** for setting of the methodological strategy design and the implementation of the impact assessment computer system.

As an empirical method, the interview was used to learn about impact assessment in / on organizations from the client and to clarify the current state of the IT impact assessment process in / on Cuba. The research is based on the concept of 'impact on Information Security management Systems' from ISO 27001. Good practices for risk management and impact measurement defined by NIST (National Institute of Standards and Technology Cybersecurity Framework), the ISO 27000 series, COBIT (Control Objectives for Information and related Technology), and MAGERIT (Methodology for Information Systems Risk Analysis and Management) were studied and considered for the development of the application.

Discussion and Outcomes

To measure the IT impact on organizations, an assessment of IT assets must first be conducted according to their criticality and importance to the organization. This requires considering the replacement asset value or the business consequences of the loss or compromise of those assets. Subsequently, threats are identified, and the probability of occurrence (risk) is estimated (Figure 1). This information can be obtained from the asset owners or users, human resources personnel, facility managers, information security specialists, and other relevant sources. The performers involved in the IT impact assessment process on organizations are IT specialists, managers, and business workers.



Figure 1. Description of the impact measurement process

For the design and implementation of the computer system aimed at evaluating the IT impact on organizations, a web application is proposed, which will be integrated into the company Intranet. This tool allows to run an IT assets inventory and subsequently estimates the importance of each asset to the organization through the processing of a set of criteria entered by the user. Additionally, it will include an inventory of threats that could affect the organization's assets. It will have a functionality to estimate the risk for each asset inside the organization by calculating the total risk each asset faces. It will have a function to estimate the impact on the company of the possibility that assets are affected by the threats to which they are exposed. Finally, the organization's workers will have the possibility to access the system to assess their level of satisfaction with the company's assets (Figure 2).

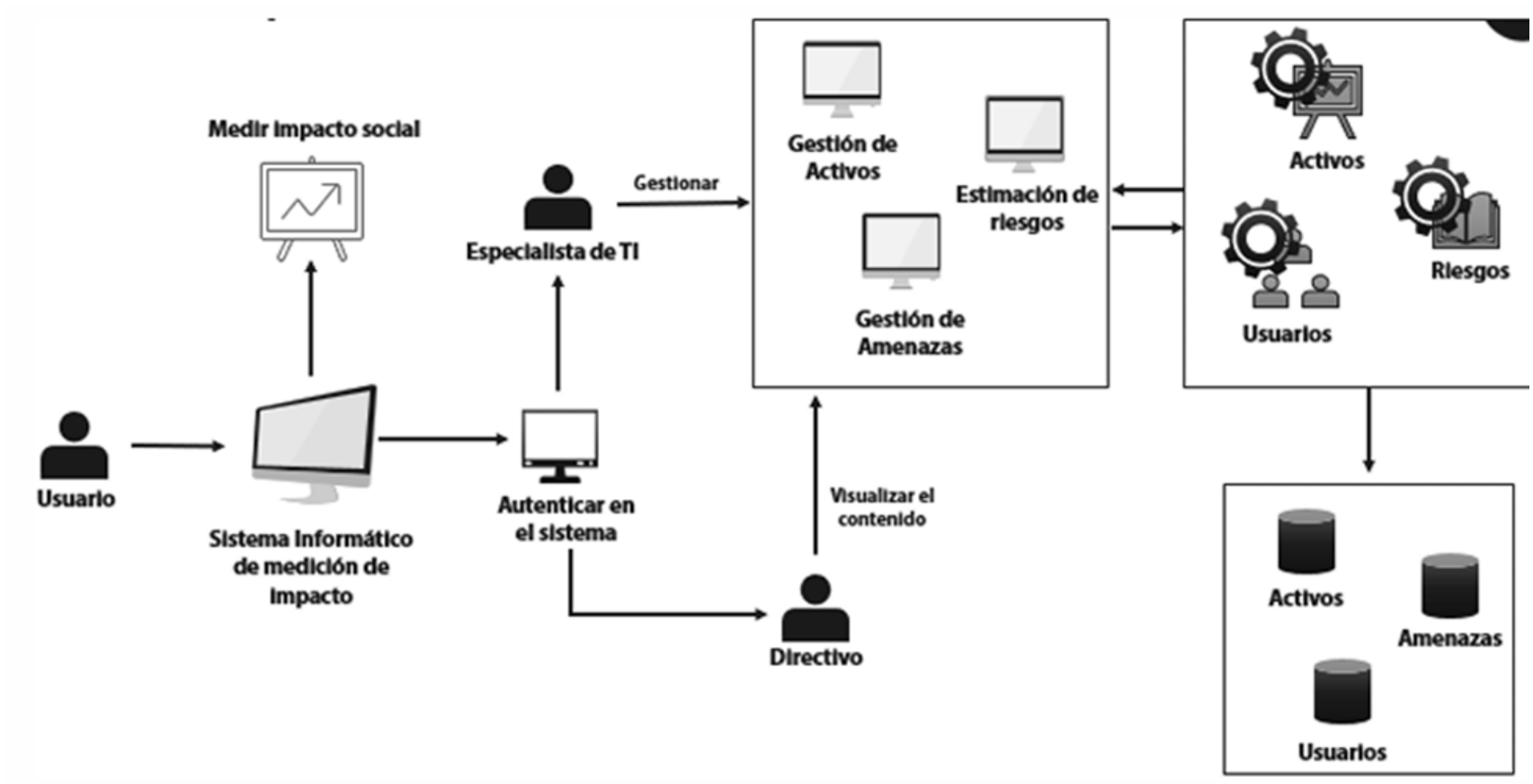


Figure 2. Description of the proposed solution

Fourteen functional requirements, fourteen user stories, and three CRC (Class, Responsibility, Collaboration) cards were defined, which describe how to authenticate users in the system, manage assets, manage threats, calculate importance, estimate risks, assess services, and measure social impact. Figure 3 shows, as part of the development process planning, the number of iterations into which the project is divided. Non-functional requirements for appearance, software, hardware, security, portability, performance, usability, and maintainability were also defined.

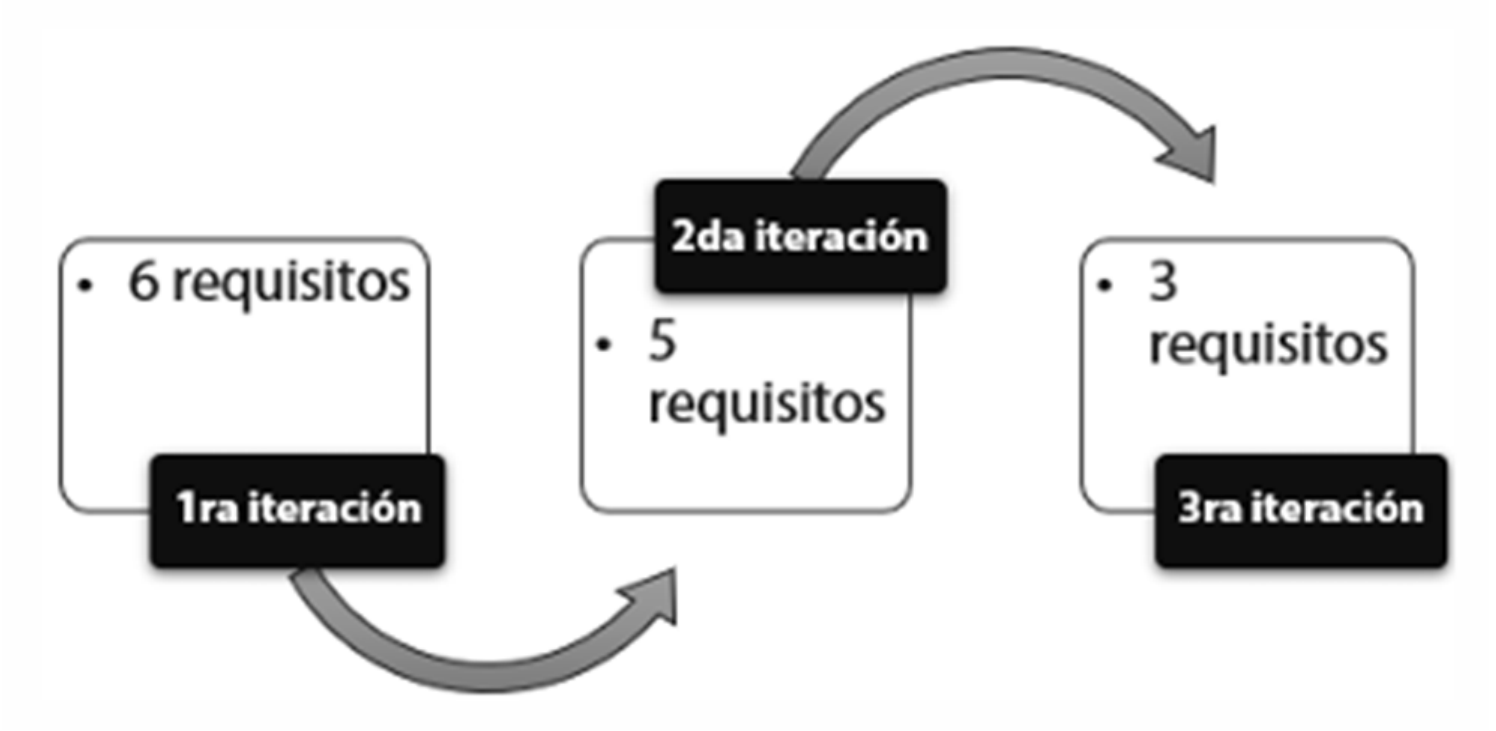


Figure 3. Development process planning

The system development is based on the Model-View-Controller (MVC) architectural pattern. In the case of the Django framework, it redefines this as Model-View-Template: the view acts as the controller and the templates act as the views. Regarding design, the following GRASP patterns were employed: Expert, Creator, Low Coupling, Controller, and High Cohesion. These describe the essential principles of object design and responsibility assignment, expressed in the form of patterns. As a data model, the entities Asset, User, and Threat were proposed. The relationship established between assets and threats is many-to-many, which gives rise to an additional entity that allows determining the probability of occurrence of certain threats on an asset (risk) (Figure 4).

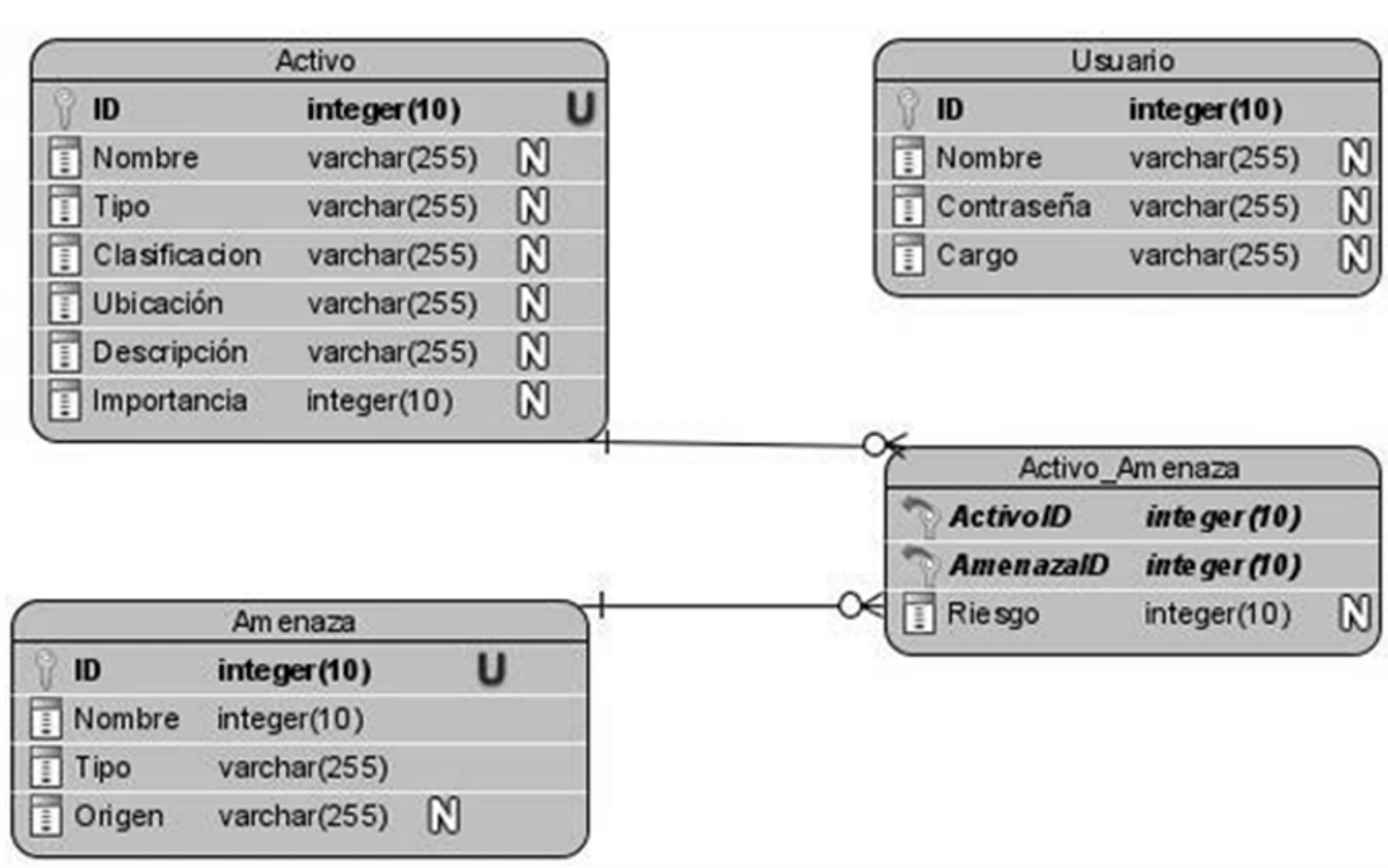


Figure 4. Data model of the solution proposal

As a web app, it is based on the customer-server architecture. This requires a dedicated server to host the information managed by the system. Customer should access through a navigator. As a web server, Apache is proposed and connection should be establish through HTTPS protocol using 443 port. Transport protocol is required to ensure the reliable and secure TCP information provision. Figure 5 shows necessary components and specifications for the solution deployment / implementation.

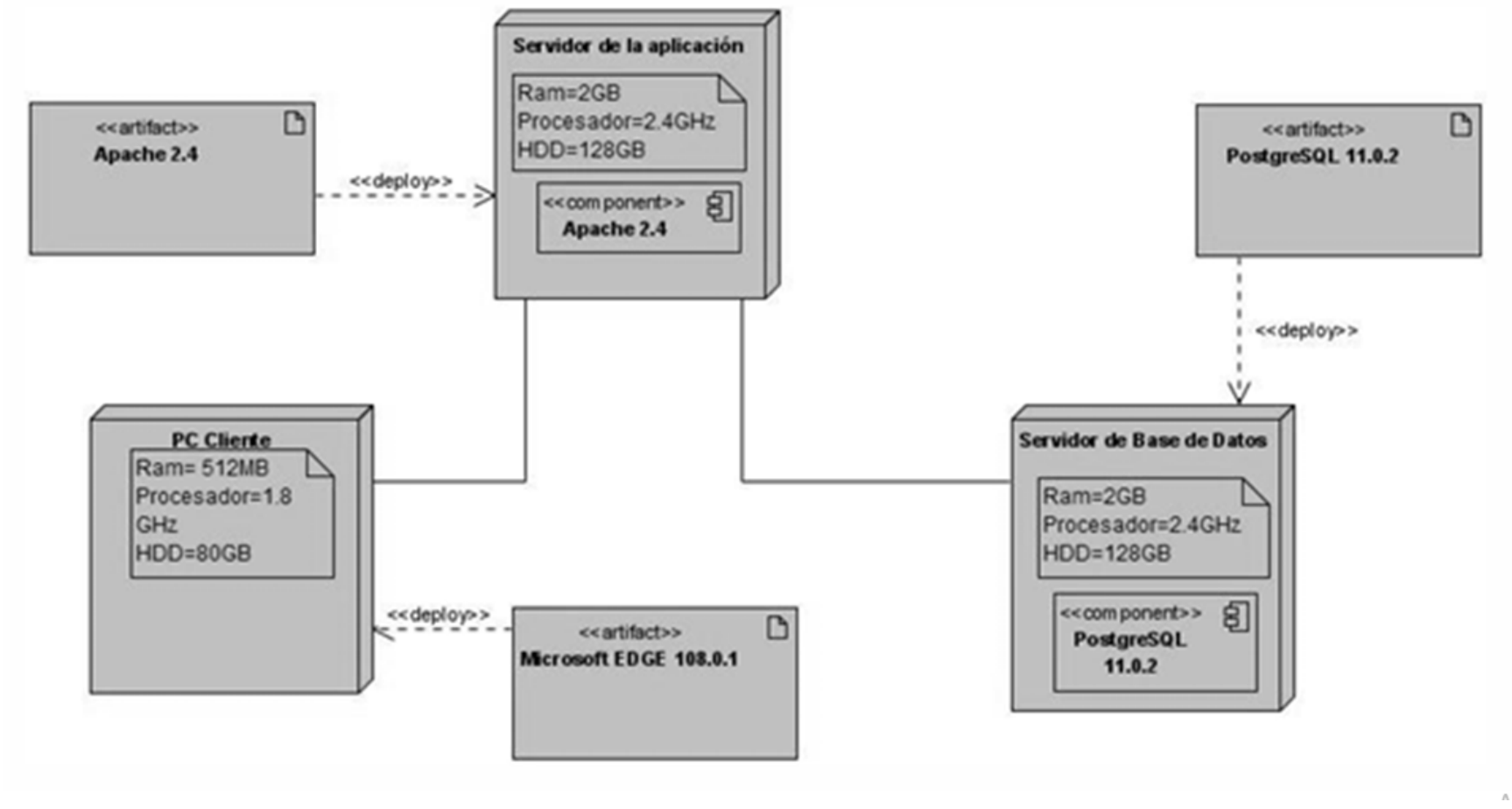


Figure 5. Solution deployment proposal

Conclusions

Having conducted the research and developed the computer system for evaluating the IT impact on organizations, the following conclusions can be drawn:

- The systematization of the theoretical-methodological foundations for measuring the IT impact on organizations helped clarify the process and thus implement a solution more in line with risk management and impact measurement standards.
- The planning and design of the system allowed for the organization of the development process and provided a guide for the implementation of the requirements.
- A computer system was implemented that should assist IT specialists, workers, and managers of organizations in reducing the complexity in the risk management and impact measurement process.

References

Casanova, M. P., & Calderón, C. A. (2020). Modelo para la gestión de infraestructuras de tecnologías de la información. *Tecnológicas*, *23*(48), 32-54. http://www.scielo.org.co/scielo.php?pid=S0123-77992020000200032&script=sci_arttext

Liendo Afonso, L. C. (2023). *Optimización del proceso de reporting del análisis de impacto en el negocio en una consultora de ciberseguridad* [Trabajo fin de grado/master, Universidad Europea]. Repositorio institucional. http://titula.universidadeuropea.com/handle/20.500.12880/5414

Martínez Landrove, N. (2019). *Ciberseguridad y riesgo operacional en las organizaciones* [Tesis de pregrado o máster, Universidad Pontificia Comillas]. Repositorio Comillas. https://repositorio.comillas.edu/xmlui/handle/11531/42317

Pérez Lorences, P. (2014). *Procedimiento para mejorar la gestión de tecnologías de la información en el sector empresarial cubano* [Tesis doctoral, Universidad Central “Marta Abreu” de Las Villas].

Quinn, S., et al. (2022). *Using business impact analysis to inform risk prioritization and response* (NIST IR 8286D). National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.IR.8286D