

tono

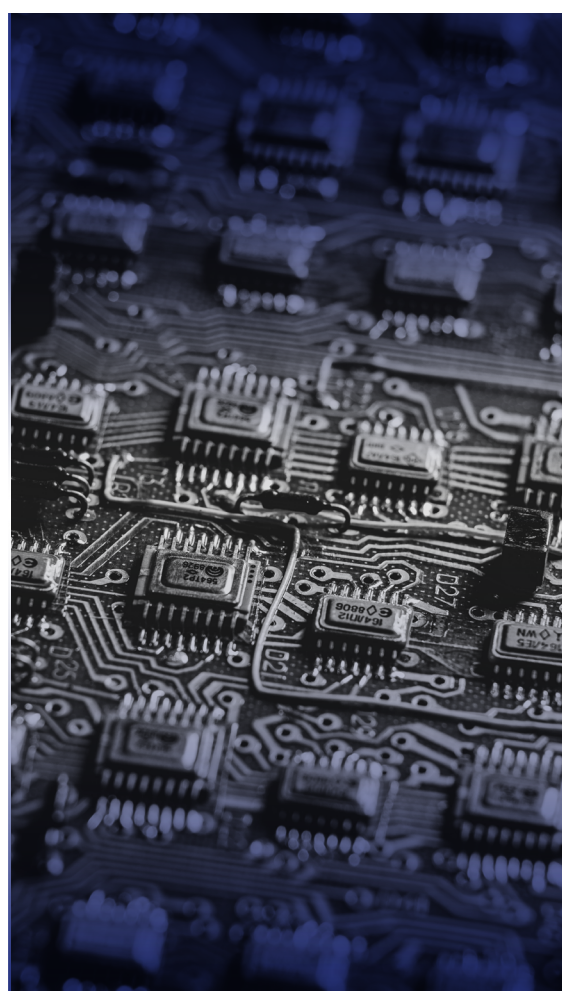
Revista Científico-Técnica de la Empresa
de Telecomunicaciones de Cuba S.A.

Publicación Semestral Vol.23 - No. 1 - 2026
RNPS: 0514 ISSN: 2224-6274

Tono, Revista Científico-Técnica de la Empresa de Telecomunicaciones de Cuba S.A.

Las opiniones de los autores expresadas en los artículos reflejan sus puntos de vista, pero no necesariamente coinciden con los criterios del consejo editorial.

Los artículos en esta publicación han sido sometidos a revisión por pares a doble ciego.



Portada:
Internet

Contáctenos

Dirección de Vigilancia e Información Científico-Técnica de ETECSA

Dirección: Centro de Negocios Miramar, calle 3ra, e/ 76 y 78, Edificio Beijing, 4to Piso, oficina 404. Playa, C.P.: 11300. La Habana, Cuba.

Teléfono : (53) 7266-8453

Correo electrónico: tono@etecsa.cu

Sitio web: www.revistatono.etecsa.cu

Comité científico asesor

M. Sc. Melissa Saltiel Delgado

M. Sc. Mirta Julieta García García

M. Sc. María del Pilar Caso Álvarez

M. Sc. Alberto Javier García García

M. Sc. Fidel Mirabal Puig

Consejo Editorial

Director/a de la revista

M. Sc. Grisel Ojeda Amador

Editor(a) ejecutivo

Lic. Inés María León Martínez

Editor(a) de sección

Lic. Mirta Ulloa Ferreiro

Traducción

Lic. Armando Camejo Hernández

Lic. Lena María Cué Morales

Lic. Frans Carlos Castellano Caballero

Lic. Odalys Ojeda Fuentes

Lic. Idalmis María Barbería Espinosa

Lic. Alejandro Daniel Fadrugas Robaina

Diseño original

Di. Marcel Mazorra Martínez

Maquetación

Di. Isabel Canales Calvo

Asistencia técnica y programación

Ing. Maritza de la C. Menéndez Figueredo

Revisión de datos

Lic. Elisa Alfaro Díaz

Ing. Darian Diaz García

Árbitros

Dra. Caridad Anías Calderón (CUJAE)

Dr. Félix Álvarez Paliza (UCLV)

Dr. Glauco Antonio Guillén Nieto (LACETEL)

Dr. José Raúl Vento Álvarez (UPR)

Dr. Osvaldo Andrés Pérez García (CENAIIV)

Dra. Lindsay Alonso Gómez Beltrán (Univ. Camagüey)

Dr. Gregory Randall (Univ. de la República, Uruguay)

Dra. C. María Matilde García Lorenzo (UCLV)

Dr. C. Jorge Gulin González (UCI)

Dr.C. Omar Mar Cornelio (UCI)

M. Sc. Arelys Emiliana Ramos Fleites (UCLV)

M. Sc. Alberto Javier García García (ETECSA)

Ing. Raúl E. Rodríguez Doncel (CONAS)

Ing. Fidel Mirahal Puig (ETECSA)

M. Sc. Armando Tito Bernot (ETECSA)

M. Sc. Pablo Domínguez Vázquez (ETECSA)

M. Sc. Maydel Vázquez Fernández (ETECSA)

M. Sc. Karina Leonor Fernández Sánchez (ETECSA)



Se ofrece en esta oportunidad una edición de la revista *Tono* que compila aportes destacados dentro del ámbito de las ciencias y la técnica. Esta selección representa un balance actualizado de los avances y desafíos en materia de seguridad digital, gestión tecnológica y transformación de procesos, áreas prioritarias para el desarrollo soberano y la eficiencia del país.

La seguridad digital y la modernización de infraestructuras se posicionan como ejes transversales en el contexto actual. Los estudios incluidos en esta compilación abordan desde el análisis de vulnerabilidades en Open API de TM Forum hasta la protección de dispositivos móviles, lo que confirma la necesidad de estrategias integrales ante amenazas de creciente sofisticación. Asimismo, se abordan experiencias de integración tecnológica en sectores estratégicos como la cadena de suministro biofarmacéutica cubana, donde la convergencia hacia modelos de Inventarios 4.0 demuestra el impacto de la digitalización en la fortaleza operativa.

La práctica de la gestión tecnológica en el contexto nacional se distingue por su enfoque sistémico y aplicado. Las propuestas documentadas muestran soluciones que equilibran innovación con sostenibilidad práctica, como la extensión del modelo Tier desde el centro de datos hacia el servicio, el diagnóstico de madurez en seguridad digital para servicios de consultoría, y el desarrollo de sistemas informáticos para la evaluación de impacto de las tecnologías de la información en las organizaciones. Resulta notable el progreso alcanzado en dominios como la estandarización de infraestructuras, la medición de madurez organizacional y la creación de herramientas de gestión adaptadas a las condiciones específicas del país.



CARTA DEL EDITOR

Los hallazgos del encuentro ratifican la necesidad de mantener un enfoque que combine perfeccionamiento técnico con desarrollo de capacidades institucionales. Se constata que la eficacia de las estrategias de transformación digital requiere de manera simultánea de soluciones tecnológicas avanzadas y de profesionales preparados para implementarlas con criterios de eficiencia y soberanía tecnológica, tal como se refleja en iniciativas como Girasol tecnológico, que aportan a la visualización y fortalecimiento del ecosistema digital nacional.

Como novedad en este número de la revista *Tono*, se presenta el artículo «La revolución de la inteligencia artificial en las telecomunicaciones», correspondiente a la Jornada Científica 2025 de la escuela vocacional Vladimir Ilich Lenin y la Empresa de Telecomunicaciones de Cuba S.A. (ETECSA). Este trabajo demuestra no solo el vasto conocimiento de la juventud cubana, sino también el interés de los jóvenes por acercarse a temáticas tan novedosas como el uso de la IA.

Esta compilación certifica el nivel de especialización y madurez alcanzado por esta comunidad de conocimiento en Cuba. Se valora el aporte colectivo de investigadores y profesionales cuyos trabajos contribuyen a fortalecer las bases para un desarrollo digital nacional seguro, eficiente y confiable.

Cordialmente,

**Grupo Editorial
Revista Científico-Técnica Tono**

INVESTIGACIÓN

Amenazas y vulnerabilidades en las Open API de TM Forum

Threats and Vulnerabilities in TM Forum Open APIs

Ing. Clayret Echenique Quintana, Ing. Jorge Manuel Sotolongo Piedra

7

Del Centro de Datos al servicio: extendiendo el Modelo Tier

From Data Center to service: extending the Tier Model

Ing. Ernesto Carrazana Ruiz, Ing. Irisleidis Lázara Casi Estevanell,

Esp. Héctor Manuel Jacas Joa

28

Girasol tecnológico

Technological sunflower

Ing. Lázaro Santana Linares,

Maikol Ismael Mirabal Hidalgo, M. Sc. Raydel García Mesa

43

Hacia una gestión de inventarios 4.0: Integración de tecnologías digitales en la cadena de suministro biofarmacéutica de Cuba

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

M. Sc. Zuleyka Calzado Mesa, Ing. Gabriela Ojeda de la Paz,

Ing. Damián Aldait García Pérez

61

Diagnóstico de Madurez en Seguridad Digital para servicios de consultoría

Digital Security Maturity Assessment for Consulting Services

M. Sc. Noel Emilio Rojas Martos, M. Sc. Liban de Armas Granado

70

La Revolución de la IA en las Telecomunicaciones: Un Viaje del Pasado al Futuro

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

Rafael Alberto Noa Yanes, Ing. Ivette García Montero

88

Sistema informático para la evaluación de impacto de las Tecnologías de la Información en las organizaciones

Computer system for evaluating the impact of Information Technologies in organizations

Ing. Ernesto Elias Elzaurdín Valdés, Ts. Meliza Leon Bencomo,

M. Sc. Mary Nelsa Bonne Cuza

99

Amenazas y vulnerabilidades en las Open API de TM Forum

Threats and Vulnerabilities in TM Forum Open APIs

Ing. Clayret Echenique Quintana^{1*},
Ing. Jorge Manuel Sotolongo Piedra ²

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

El sector de las telecomunicaciones enfrenta desafíos de ciberseguridad distintivos derivados de su migración a arquitecturas nativas de la nube y su rol como eje central del entorno digital. En este contexto, las Open API de TM Forum, que materializan los principios de la arquitectura ODA, constituyen una superficie de ataque significativa al facilitar la interoperabilidad entre sistemas desacoplados. El presente estudio tuvo como objetivo identificar y analizar las principales amenazas y vulnerabilidades que afectan a estas interfaces, con el fin de contribuir a la concepción de futuros marcos de seguridad. Se empleó una metodología de revisión sistemática de literatura basada en el protocolo PRISMA, con búsquedas en seis bases de datos: IEEE Xplore, Scopus, Web of

^{1*} Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños, Km 2 ½, reparto Torrens, municipio Boyeros, La Habana, Cuba. cechenique@uci.cu

² Universidad de las Ciencias Informáticas. Carretera a San Antonio de los Baños, Km 2 ½, reparto Torrens, municipio Boyeros, La Habana, Cuba. jorgemsp@uci.cu

Science, Google Scholar, ResearchGate y ScienceDirect y fuentes adicionales oficiales. De los registros identificados se incluyeron siete estudios tras aplicar criterios de inclusión y exclusión. Como principal aporte se construyó una taxonomía de correlación que integra las categorías STRIDE+P, las vulnerabilidades del OWASP API Top 10 2023 y los componentes de la arquitectura ODA, identificando 17 correlaciones significativas. Los resultados revelan que el 47 % presentan severidad crítica, concentradas en el API Gateway, la gestión de clientes y el control de acceso. Se concluye que la seguridad de estas APIs requiere controles de autorización granular y validación de esquemas a nivel de campo, constituyendo un fundamento empírico para marcos de seguridad específicos en ecosistemas ODA

Palabras clave: amenazas en las Open API, ODA, Open API, Open API de TM Forum, seguridad en las Open API

Abstract

The 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 principles of the ODA architecture, constitute a significant attack surface by enabling interoperability among decoupled systems. This study 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 records identified, 7 studies were included after applying inclusion and exclusion criteria. As the main original contribution, a three-dimensional 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 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*

Introducción

El sector de las telecomunicaciones enfrenta desafíos de ciberseguridad distintivos debido a su rol como eje central del entorno digital. Los proveedores de servicios son particularmente vulnerables a ciberamenazas derivadas de tensiones geopolíticas, incluyendo el espionaje y otras actividades maliciosas. También se enfrentan a riesgos tecnológicos propios de su migración a arquitecturas nativas de la nube, las cuales son menos conocidas y representan una amenaza para los servicios de red tanto nuevos como antiguos (Donegan, 2023). En este contexto, la estandarización y la adopción de arquitecturas abiertas surgen como pilares fundamentales para la innovación y la interoperabilidad. TM Forum ha sido pionero en el desarrollo de marcos de referencia y mejores prácticas para guiar esta evolución (TM Forum, 2025a).

Entre sus contribuciones más importantes se destaca el marco de referencia de Operaciones Digitales Abiertas (ODA, por sus siglas en inglés), concebido como un modelo arquitectónico basado en componentes desacoplados y reutilizables para construir ecosistemas de negocio ágiles. Para complementar esta visión, las Open API de TM Forum materializan los principios de la capa de implementación de ODA al proveer un conjunto estandarizado de especificaciones técnicas que permiten la integración fluida, segura y escalable entre sistemas, plataformas y socios en todo el ecosistema digital.

El creciente uso de las API (Interfaz de Programación de Aplicaciones, por sus siglas en inglés) en el sector de las telecomunicaciones ha facilitado la creación de nuevos productos, especialmente con el auge de los servicios en la nube y las aplicaciones móviles. Sin embargo, esta apertura introduce vulnerabilidades significativas que pueden ser explotadas por actores maliciosos.

Según el reporte *State of API Security* H2 en 2025, los principales problemas de seguridad de las API se deben a que el 80 % de los líderes de seguridad carecen de monitoreo continuo en tiempo real; el 33 % de las organizaciones sufrieron un incidente de seguridad debido a las API el último año, solo el 19 % están seguros de la precisión de su inventario de API y el 51 % de las organizaciones se encuentran todavía en etapas de planificación o en niveles básicos en su madurez de seguridad de API (Salt, 2025).

En este contexto, las Open API de TM Forum emergen como un estándar fundamental que impulsa la integración y la creación de un ecosistema de servicios interconectados en el sector de las telecomunicaciones. Estas interfaces de programación no solo facilitan la conectividad y la interoperabilidad entre servicios complejos, sino que también permiten una gestión integral de su ciclo de vida, incluso en entornos donde múltiples socios colaboran en la prestación del servicio.

Basadas en los principios del diseño REST y al ser tecnológicamente independientes, las Open API de TM Forum se han convertido en la base para una gestión de servicios sencilla y coherente. Pero esta estandarización, aunque esencial para la innovación, también extiende el alcance de las vulnerabilidades mencionadas; por ello, la seguridad de estas API se convierte en un pilar crítico para la fiabilidad y sostenibilidad del ecosistema digital.

Por este motivo, la presente investigación tiene como objetivo sistematizar las principales amenazas y vulnerabilidades a las que se exponen las Open API de TM Forum para contribuir a futuros trabajos de concepción de marcos de seguridad que integren las mejores prácticas y estándares de seguridad para las Open API de TM Forum.

Materiales y métodos

El presente estudio se fundamenta en una revisión sistemática de literatura orientada a identificar, analizar y sintetizar el estado actual de las amenazas y vulnerabilidades en las Open API de TM Forum. Para garantizar la rigurosidad metodológica del proceso de selección y análisis documental, se adoptó el protocolo PRISMA. Se realizó una

búsqueda en seis bases de datos científicas y repositorios académicos seleccionados por su cobertura en ingeniería informática, telecomunicaciones y ciberseguridad: IEEE Xplore, Scopus, Web of Science, Google Scholar, ResearchGate y ScienceDirect.

La estrategia de búsqueda se estructuró mediante la combinación de términos controlados y libres en inglés y español, utilizando operadores booleanos (AND, OR, NOT) y truncamientos. Se diseñaron tres bloques temáticos:

1. API y seguridad: «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. Amenazas y vulnerabilidades: «threat modeling» OR «STRIDE» OR «OWASP API Top 10» OR «cybersecurity» OR «vulnerability assessment» OR «risk assessment»

Se establecieron en la Tabla 1, los criterios de inclusión y exclusión para la selección de estudios:

Tabla 1. Criterios de inclusión y exclusión de la selección de estudios

Criterios de inclusión	Criterios de exclusión
• Documentos que aborden la seguridad de APIs en contextos de telecomunicaciones o arquitecturas abiertas. • Documentos que hagan referencia explícita a TM Forum, ODA o sus Open API. • Documentos que analicen amenazas, vulnerabilidades o riesgos de seguridad en APIs RESTful. • Documentos que propongan marcos, estándares o políticas de seguridad aplicables a APIs. • Publicaciones entre 2020 y 2025, para garantizar vigencia tecnológica. • Documentos de acceso completo o texto completo disponible.	• Documentos que no traten temas de seguridad en APIs. • Documentos centrados exclusivamente en APIs de otros sectores sin vinculación con telecomunicaciones. • Presentaciones comerciales, promocionales o documentos sin respaldo académico o técnico. • Duplicados entre bases de datos. • Documentos anteriores a 2020, salvo referencias normativas históricas esenciales. • Artículos en idiomas distintos al inglés o español, salvo que tuvieran traducción verificable.

La selección de documentos se realizó en tres fases, siguiendo el flujo PRISMA (Figura 1):

Fase 1 — Identificación: Se ejecutaron las búsquedas en las seis bases de datos, registrando el número de resultados por fuente y eliminando duplicados mediante el gestor bibliográfico Zotero y revisión manual cruzada.

Fase 2 — Revisión: Se evaluaron títulos y resúmenes contra los criterios inclusión/exclusión.

Fase 3 — Inclusión: Se recuperaron los textos completos de los documentos preseleccionados. Se aplicó nuevamente los criterios inclusión/exclusión al contenido completo, registrando las razones de exclusión. Los documentos finalmente incluidos fueron sometidos a extracción de datos.

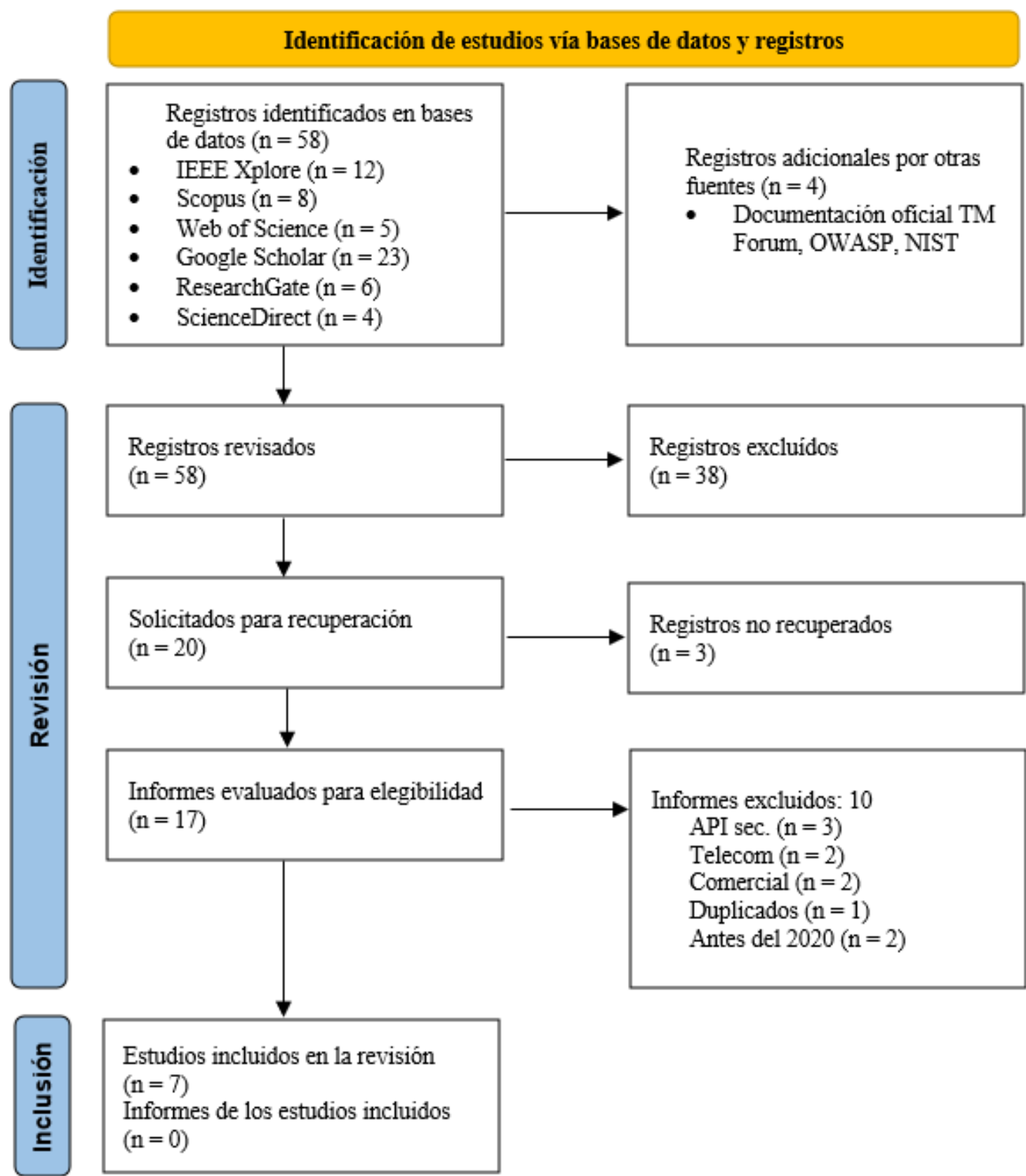


Figura 1. Flujo PRISMA para la selección de documentos

- Luego, se aplicaron los siguientes métodos analíticos:
- Análisis documental: Revisión de la documentación oficial de TM Forum, estándares OWASP, NIST SP 800-53/63/228, y literatura académica seleccionada.
 - Análisis y síntesis: Interpretación, procesamiento y categorización de la información extraída, estableciendo relaciones entre amenazas, vulnerabilidades de OWASP API Top 10 y controles de seguridad recomendados.

Resultados y discusión

Una API es un conjunto de reglas y definiciones que dictan cómo un *software* puede interactuar con otro. Actúa como un intermediario que facilita a diferentes sistemas de software comunicarse e intercambiar datos de manera fluida y estandarizada (Akintoye, 2025). Por ejemplo, desde una perspectiva más técnica y funcional, de forma especial en el contexto de la web, las API son el mecanismo que posibilita a varias aplicaciones compartir datos e interactuar mediante peticiones HTTP estructuradas (Akintoye, 2025). Durante la evolución de los servicios web, las API surgieron para satisfacer las demandas de conectividad fluida y rápido intercambio de datos (Jaiswal, 2025).

Dentro de las funciones esenciales de una API en la arquitectura de *software* moderna se encuentran (Akintoye, 2025; Garimilla, 2024):

- Promover la eficiencia: permiten a los desarrolladores integrar sistemas existentes en lugar de construir todo desde cero, lo que ahorra tiempo y recursos.
- Habilitar la conectividad: hacen posible que sistemas contruidos con tecnologías y plataformas completamente diferentes puedan trabajar juntos.
- Impulsar la innovación y la modularidad: ofrecen herramientas para construir soluciones creativas y compartimentar funcionalidades, lo que hace que el *software* sea más flexible, escalable y fácil de mantener.
- Acelerar el desarrollo: al facilitar la integración, reducen la complejidad y los ciclos de desarrollo.

Las API utilizan el Protocolo de Acceso a Objetos Simples (SOAP, por sus siglas en inglés), por su robustez, seguridad y estandarización, sobre todo en entornos empresariales complejos. Este es el protocolo más antiguo y rígido que se basa en mensajería XML. Se caracteriza por sus estrictos estándares de comunicación, contratos formalizados y robustas características de seguridad, siendo común en aplicaciones a nivel empresarial. Sin embargo, su complejidad a menudo ralentizaba el desarrollo (Akintoye, 2025; Jaiwal, 2025).

SOAP se considera, en gran medida, una tecnología heredada y el ecosistema digital ha experimentado una clara evolución desde SOAP

hacia arquitecturas REST. Esta transición fue impulsada por la necesidad de soluciones más ágiles, ligeras y escalables, en especial con el auge de las aplicaciones móviles y los servicios en la nube. Sus principios claves son el uso de métodos HTTP estándar (GET, POST, PUT, DELETE). La comunicación sin estado, donde cada petición contiene toda la información necesaria para ser procesada; el uso de formatos de datos ligeros, en particular JSON, y es altamente escalable y más sencillo de implementar (Akintoye, 2025; Jaiswal, 2025).

En la actualidad, GraphQL se menciona como una tendencia emergente y como una alternativa a REST, ya que su principal ventaja es la flexibilidad: permite a los clientes solicitar únicamente los datos que necesitan, evitando la sobrecarga de información (Jaiswal, 2025). Para obtener y manejar los datos, las APIs RESTful se organizan en torno a dos conceptos fundamentales (Akintoye, 2025):

1. **Recurso:** es el objeto central. Un recurso representa cualquier dato u objeto que puede ser accedido o manipulado como un usuario, un producto, una publicación o un libro. Cada recurso es identificado por una URI única que es la dirección para acceder a él.
2. **Endpoint:** es la URL específica donde un recurso puede ser accedido para realizar una operación. Un endpoint combina la URL base del servidor, la ruta del recurso y un método HTTP para definir una acción.

La interacción se produce cuando un cliente envía una petición a un endpoint y el servidor devuelve una representación del recurso, comúnmente en formato JSON.

Hoy en día, el rol de las API en aplicaciones web, móviles y en el Software como Servicio (SaaS, por sus siglas en inglés) es la columna vertebral que sostiene las aplicaciones modernas. La evolución hacia arquitecturas de microservicios y aplicaciones nativas de la nube fue impulsada por las API RESTful. Las API permiten desacoplar los componentes de un sistema, lo que facilita que diferentes equipos los desarrollen y desplieguen de forma independiente. En el entorno de la nube, las API RESTful son ideales porque consumen menos recursos computacionales y simplifican la escalabilidad horizontal en plataformas como Kubernetes. En cambio, en las aplicaciones móviles se

requiere un intercambio de datos rápido y eficiente para ofrecer una buena experiencia de usuario. Las API RESTful, con sus datos ligeros (JSON) y su menor latencia, son mucho más adecuadas para este propósito (Jaiswal, 2025).

Interface de Programación de Aplicaciones de TM Forum

Las Open API de TM Forum son el mecanismo que permite que todos los bloques y componentes de (ODA se conecten y funcionen como un sistema unificado y estable (Hou *et al.*, 2024; TM Forum, 2021a).

ODA es el marco de arquitectura de referencia de TM Forum, diseñado para reemplazar a los sistemas monolíticos con una colección de componentes de *software* desacoplados. Su objetivo principal es permitir a los proveedores de servicios de Internet operar como empresas digitales ágiles, similares a las grandes empresas de tecnología (Hou *et al.*, 2024; TM Forum, 2021a).

Las Open API de TM Forum tienen un estilo arquitectónico de API RESTful en formato JSON definidas con Especificaciones Open API (OAS, por sus siglas en inglés), y se utilizan para la orquestación y gestión de servicios y recursos entre Sistemas de Soporte al Negocio y Operaciones (BSS/OSS) (TM Forum, 2025b). Estas cumplen dos funciones esenciales dentro de la ODA (TM Forum, 2021a):

- Interfaces estandarizadas de componente: definen las interfaces de referencia mediante las cuales los componentes ODA (que residen en los bloques funcionales) exponen sus funcionalidades al exterior y se comunican entre sí. Este enfoque de exposición de API es lo que permite que la arquitectura sea platform-based y fomenta la evolución ágil.

Habilitador de interoperabilidad: al estar estandarizadas, las API permiten que componentes de diferentes proveedores o sistemas internos, propios o heredados, se conecten y trabajen juntos, lo que reduce de manera drástica la complejidad y el coste de la integración. El éxito de las Open API radica en que no son solo interfaces técnicas, sino que están ancladas a los marcos de referencia de TM Forum. Cada Open API se basa en un objeto de información de negocio definido en el Information Framework (SID) de TM Forum. Esta base semántica común asegura que, sin importar el proveedor,

el concepto de negocio intercambiado es consistente y universal. Por otra parte, mapean las funciones de los bloques ODA con los procesos de negocio definidos en el eTOM y esto asegura que las interfaces soportan flujos de trabajo de negocio de extremo a extremo (V. P. Mochalov *et al.*, 2019; TM Forum, 2021).

En la práctica, las Open API son fundamentales para la transformación digital, de manera especial en las áreas de orquestación, automatización y virtualización. En el contexto de una implementación de ODA, las APIs se utilizan para interconectar el nivel de gestión comercial con el nivel de producción de la red, por ejemplo, para automatizar la provisión de un servicio de conectividad.

Amenazas que exponen las Open API de TM Forum

En el documento IG1187 ODA Enterprise Risk Assessment v2.0 se identifican un conjunto de amenazas de seguridad relevantes mediante la adopción del modelo STRIDE+P, que abarcan las categorías de suplantación de identidad, manipulación de datos, repudio, divulgación de información, denegación de servicio, escalamiento de privilegios y riesgos de privacidad. Cada una de estas amenazas constituye un eje crítico en la gestión de riesgos de plataformas abiertas, pues comprometen la confidencialidad, integridad y disponibilidad de los servicios, además de la conformidad regulatoria en materia de protección de datos personales (TM Forum, 2021b).

En particular, la suplantación de identidad se relaciona con ataques donde un actor malicioso se hace pasar por un usuario o sistema legítimo; la manipulación de datos implica la alteración de información en tránsito o en reposo; el repudio refleja la ausencia de trazabilidad y registro que permita negar acciones realizadas; y la divulgación indebida de información corresponde a la exposición de datos sensibles de usuarios o empresas. Asimismo, la denegación de servicio busca interrumpir la disponibilidad de recursos mediante sobrecarga, el escalamiento de privilegios permite a un atacante obtener accesos no autorizados, y la categoría de privacidad enfatiza los riesgos de incumplimiento normativo, particularmente en relación con el Reglamento General de Protección de Datos (TM Forum, 2021b).

De manera más específica para el contexto de las Open API de TM Forum, el documento destaca que las interfaces de programación constituyen la principal superficie de ataque y recomienda adoptar como referencia las amenazas descritas en el OWASP API Top 10 (2019). Estas incluyen problemas de autorización a nivel de objeto, fallas en la autenticación, exposición excesiva de datos, ausencia de limitación de recursos o control de consumo, deficiencias en la autorización de funciones críticas, asignación masiva de atributos no controlados, configuraciones inseguras, vulnerabilidades de inyección, gestión inadecuada de activos y versiones y ausencia de registros y monitoreo efectivos (TM Forum, 2021b).

Dentro de este conjunto, las amenazas más críticas para las Open API de TM Forum son aquellas que impactan de manera directa en la autenticación, autorización y protección de datos. En particular, la exposición excesiva de datos constituye un riesgo central al poder revelar información personal o confidencial más allá de lo estrictamente necesario. La autenticación y autorización deficientes facilitan accesos indebidos a objetos o funciones sensibles, mientras que la ausencia de controles de consumo y gestión de versiones incrementa la vulnerabilidad frente a ataques de denegación de servicio. En este sentido, el marco de evaluación de riesgos de TM Forum evidencia que la seguridad de las Open API depende de la combinación de un análisis de amenazas estructurado bajo STRIDE+P y la adopción sistemática de las mejores prácticas propuestas por OWASP para API abiertas (Ariami *et al.*, 2024; Nikolov & Aleksieva-Petrova, 2025; TM Forum, 2021b).

Vulnerabilidades de las Open API de TM Forum

Las vulnerabilidades más comunes en las Open API de TM Forum coinciden con las descritas en el OWASP API Top 10 del 2019, según *IG1187 ODA Enterprise Risk Assessment* v2.0; aunque en esta guía referencian la lista del 2019, la autora adoptará las del 2023 que son la última versión estable: (Mazzei *et al.*, 2025; OWASP, 2023; Sharma, 2025):

1. Autorización rota a nivel de objeto (BOLA, por sus siglas en inglés): Las APIs a menudo exponen identificadores de objetos que pueden ser manipulados por un atacante.

2. Autenticación rota: Ocurre cuando los mecanismos de autenticación no se implementan de forma segura.
3. Autorización rota a nivel de propiedades del objeto: Cuando una API devuelve o permite modificar más campos de los necesarios o carece de controles por campo, puede exponer o alterar datos sensibles.
4. Consumo de recursos sin restricciones: Si la API no limita el número, tamaño o frecuencia de las solicitudes puede agotarse el rendimiento del sistema, generando denegaciones de servicio (DoS) o sobrecostos.
5. Autorización rota a nivel de función: Aparece cuando las funciones administrativas o de alto privilegio no están correctamente restringidas. Los atacantes pueden ejecutar acciones que deberían estar reservadas solo para ciertos roles.
6. Acceso sin restricciones a flujos de negocio sensibles: Incluso si no hay vulnerabilidades técnicas, los atacantes pueden abusar de la lógica de negocio expuesta por la API.
7. Falsificación de solicitudes del lado del servidor (SSRF): Ocurre cuando una API permite al usuario indicar direcciones URL externas o internas sin validación, haciendo que el servidor realice peticiones maliciosas.
8. Configuración de seguridad incorrecta: Incluye errores en cabeceras HTTP, permisos, políticas CORS, versiones inseguras, *endpoints* de depuración habilitados o claves expuestas.
9. Gestión inadecuada del inventario de APIs: Las organizaciones suelen perder el control de cuántas APIs tienen activas, sus versiones y a qué datos acceden.
10. Consumo inseguro de APIs: Cuando una aplicación consume APIs externas sin verificar su autenticidad, sin validar respuestas o sin controlar dependencias, puede convertirse en víctima de ataques.

Muchas APIs de TM Forum operan flujos de negocio complejos, interoperabilidad con terceros, versiones múltiples y escenarios de

consumo variado. Las vulnerabilidades como acceso sin restricciones a flujos de negocio sensibles y las de consumo inseguro son especialmente pertinentes. En este caso se carece de información que especifique que vulnerabilidades de las antes mencionadas afectan las Open API de TM Forum, por lo que se atribuirán en la investigación estas mismas vulnerabilidades expresadas en el Top 10 de OWASP (Friman *et al.*, 2023; V. Mochalov *et al.*, 2019; V. P. Mochalov *et al.*, 2020; Smidovych & Davydovskyi, 2022).

Seguridad y políticas de gestión de las Open API de TM Forum

La seguridad en la implementación de Open API debe abordarse bajo un enfoque integral que contemple tanto principios de diseño como mecanismos técnicos y de gestión. Se parte del supuesto de que el entorno es hostil, por lo que ninguna petición debe ser considerada confiable por defecto. Para ello, todo diseño, protocolo o API debe someterse a un proceso formal de modelado de amenazas y evaluación de riesgos, lo cual permite identificar la superficie de ataque y definir medidas de mitigación adecuadas (Ohtani *et al.*, 2021; Ranjan *et al.*, 2022; TM Forum, 2017).

Un aspecto clave es la delimitación de fronteras de confianza, con la minimización de la exposición de interfaces únicamente a las necesarias para el negocio, y aplicando un modelo de autorización granular tras una autenticación robusta. Dicha autenticación debe estar protegida mediante el uso de criptografía, ser obligatoria en todos los accesos, no poder deshabilitarse y quedar registrada en bitácoras inalterables. Asimismo, la autorización debe aplicarse después de autenticar, lo que asegura que cada usuario, sistema o plataforma solo acceda a los servicios y datos que le corresponden (Christian Chukwuemeka Ike *et al.*, 2021; Jangam *et al.*, 2022; Lafarga Poyo, 2025; TM Forum, 2017).

La protección de datos es transversal y debe garantizarse tanto en tránsito como en reposo y durante el procesamiento, evitando canales inseguros y empleando cifrado en todo momento. De igual forma, se recomienda segmentar los servicios en múltiples capas de defensa para contener posibles brechas, diseñar plataformas

libres de puntos únicos de fallo y aplicar configuraciones seguras por defecto (Babu, 2025; Gambo & Almulhem, 2025; Horbenko, 2025; Micheal, 2025; Gambo & Almulhem, 2025).

En entornos multiusuario o multiempresa es esencial asegurar el aislamiento entre inquilinos mediante mecanismos físicos, virtuales o lógicos, de forma que un compromiso no afecte a otros. El diseño también debe prever mantenibilidad, así como permitir actualizaciones y coexistencia de versiones de API sin comprometer la seguridad, además de garantizar la integridad y procedencia de los componentes a través inventarios protegidos y cadenas de confianza criptográficas (TM Forum, 2017).

De igual manera, la protección de la privacidad, especialmente de datos personales identificables, debe integrarse desde el inicio en cumplimiento con regulaciones como el Reglamento General de Protección de los Datos (GDPR), incorporando prácticas de minimización de datos, control de acceso, gestión de consentimiento y trazabilidad (Sun *et al.*, 2022; TM Forum, 2017).

En cuanto a la gestión de políticas de seguridad, cada plataforma define su propio dominio y frontera de confianza, siendo las API expuestas la superficie de ataque a proteger. Esto exige la implementación de mecanismos de control de acceso federado, autenticación multifactor —al menos de dos factores para datos sensibles—, asignación de políticas a roles y usuarios, así como la distribución y ejecución de dichas políticas en puntos de decisión y de cumplimiento dentro de la plataforma (Fernández-Martínez *et al.*, 2024; Lefebvre *et al.*, 2021; TM Forum, 2017).

Como referente tecnológico, el modelo de Perímetro Definido por Software (SDP) se plantea como un mecanismo ejemplar al permitir ocultar servicios, establecer conexiones cifradas de extremo a extremo y simplificar la gestión de autenticación, autorización y control de acceso. Este modelo se basa en tres componentes principales: el cliente SDP, encargado de verificar identidad y dispositivo; el controlador SDP, que actúa como intermediario de confianza configurando accesos en tiempo real; y el *gateway* SDP, que asegura la terminación

cifrada cercana a los servicios protegidos (Fernández-Martínez *et al.*, 2024; Lefebvre *et al.*, 2021; TM Forum, 2017).

De esta manera, las Open API no solo se protegen frente a ataques comunes como DDoS, *Man-in-the-middle*, OWASP Top 10 o amenazas persistentes avanzadas, sino que también se alinean con un marco sistemático de seguridad que incluye la definición de fronteras de confianza, identificación de amenazas, evaluación y cuantificación de riesgos residuales y establecimiento de políticas de acceso adaptadas a cada dominio (Christian Chukwuemeka Ike *et al.*, 2021; Min *et al.*, 2022; Sun *et al.*, 2022; TM Forum, 2017).

Taxonomía de amenazas y vulnerabilidades en Open API de TM Forum

A partir del análisis documental descrito en la metodología PRISMA, se identificó una carencia en la literatura especializada: la ausencia de un modelo de correlación que integre las categorías de amenazas del modelo STRIDE+P, las vulnerabilidades del OWASP API Security Top 10 y los componentes específicos de la arquitectura ODA. Para cubrir esta brecha, se diseñó una taxonomía propia de amenazas y vulnerabilidades mediante un proceso de correlación cruzada manual.

La construcción de la taxonomía siguió cuatro pasos metodológicos:

- Desagregación de fuentes. Se extrajeron las 7 categorías del modelo STRIDE+P del IG1187 ODA Enterprise Risk Assessment v2.0.0 (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege, Privacy Risks) y las 10 vulnerabilidades del OWASP API Security Top 10 2023.
- Correlación lógica. Se establecieron vínculos entre cada categoría STRIDE+P y las vulnerabilidades OWASP susceptibles de materializar dicha amenaza en un contexto de APIs RESTful. Se registraron únicamente las correlaciones con fundamento técnico explícito en la documentación analizada.
- Mapeo a componentes ODA. Cada correlación validada fue asignada al componente funcional de la arquitectura ODA donde la vulnerabilidad tendría mayor impacto.

• Jerarquización por severidad. Se aplicaron criterios propios de evaluación: impacto en continuidad del servicio telecom, exposición de datos personales o financieros, complejidad de detección y alineación con requisitos regulatorios. La severidad se clasificó en Crítica, Alta, Media y Baja.

La taxonomía resultante, presentada en la Tabla 2, identifica 17 correlaciones significativas entre las siete categorías STRIDE+P y 9 de las diez vulnerabilidades OWASP 2023. El identificador de las vulnerabilidades se corresponde con el valor numérico asignado en el apartado de vulnerabilidades de las APIs del presente artículo.

Tabla 2. Taxonomíade las amenazas y vulnerabilidades de las Open APIs de TM Forum

Categoría STRIDE+P	Vulnerabilidad OWASP 2023	Componente ODA Afectado	Severidad	Justificación
<i>Spoofing</i>	VUL_API2	API Gateway	Crítica	Compromiso de identidad en punto de entrada principal del ecosistema
	VUL_API8	Gestión de identidades	Alta	Configuración incorrecta de proveedores de identidad federada
<i>Tampering</i>	VUL_API1	Inventario de recursos	Crítica	Manipulación de identificadores de recursos de inventario de red
	VUL_API3	Catálogo del producto	Alta	Alteración de propiedades de productos y servicios catalogados
	VUL_API7	Servicios de orquestación	Alta	Modificación de flujos de orquestación internos mediante solicitudes forzadas
<i>Repudiation</i>	VUL_API8	Monitoreo y registro	Media	Ausencia de trazabilidad de acciones críticas por configuración deficiente
	VUL_API9	Inventario de APIs	Media	Falta de registro de <u>APIs</u> expuestas impide auditoría forense
<i>Information Disclosure</i>	VUL_API1	Gestión de clientes	Crítica	Exposición de datos de clientes por falla en autorización a nivel de objeto
	VUL_API3	Gestión de grupos	Crítica	Filtración de datos personales por sobreexposición de propiedades
	VUL_API6	Facturación e ingresos	Alta	Revelación de información financiera sensible por flujos desprotegidos
<i>Denial of Service</i>	VUL_API4	API Gateway	Crítica	Sobrecarga del <u>gateway</u> por consumo masivo de recursos sin control
	VUL_API7	Exposición de la red	Alta	Ataque a infraestructura interna desde API expuesta al exterior
<i>Elevation of Privilege</i>	VUL_API1	Control de acceso	Crítica	Escalamiento horizontal de privilegios entre objetos del mismo nivel
	VUL_API5	APIs administrativas	Crítica	Acceso a funciones administrativas sin autorización de rol
	VUL_API6	Ecosistemas de socios	Alta	Abuso de flujos de negocio para obtener accesos elevados en ecosistema multi-socios
<i>Privacy Risks</i>	VUL_API3	Perfil de clientes	Crítica	Exposición de PII violando GDPR y estándares PCI-DSS
	VUL_API9	Gestión de consentimiento	Alta	Pérdida de trazabilidad del consentimiento del usuario para tratamiento de datos

El análisis revela que el 47 % de las correlaciones presentan severidad Crítica, concentradas en tres ejes: divulgación de información, elevación de privilegios y denegación de servicios. La taxonomía permite identificar los componentes con mayor número de correlaciones

de severidad Crítica o Alta. En este caso, el API Gateway emerge como el componente más crítico. Este hallazgo justifica la recomendación de TM Forum de implementar mecanismos de SDP y Zero Trust en el perímetro de acceso.

A diferencia del modelo STRIDE original, la extensión STRIDE+P incorpora explícitamente los riesgos de privacidad. La taxonomía demuestra que la categoría: Privacidad no opera de forma aislada, sino que se manifiesta principalmente a través de la vulnerabilidad API3 en los componentes: Perfil de clientes y Gestión de consentimiento. Esto sugiere que la protección de datos personales en las Open API de TM Forum no puede abordarse únicamente con controles de acceso, sino que requiere validación de esquemas de datos a nivel de campo y mecanismos de minimización de datos desde el diseño.

Se reconocen dos limitaciones metodológicas: la correlación se basa en análisis documental, sin validación empírica mediante pruebas de penetración en implementaciones reales de Open API TM Forum; y la severidad asignada es relativa al contexto de telecomunicaciones y puede variar en implementaciones específicas. Estas limitaciones definen el trabajo futuro propuesto en las conclusiones.

Conclusiones

El estudio de la seguridad de las Open API de TM Forum, evidencian la creciente necesidad de abordar las vulnerabilidades inherentes a este tipo de arquitecturas. El estudio reveló la existencia de amenazas significativas que exponen estas interfaces de programación. Particularmente, en el análisis de las vulnerabilidades se destacó la criticidad de los riesgos asociados a estas interfaces. La naturaleza abierta de estas APIs, diseñada para fomentar la interoperabilidad y la innovación en el sector de las telecomunicaciones, introduce simultáneamente puntos de exposición que pueden ser explotados por agentes maliciosos.

Es por ello que, dentro de las recomendaciones de seguridad de TM Forum y por otra parte las de OWASP principalmente indican que toda API debe someterse a un proceso formal de modelado de amenazas y evaluación de riesgos, lo cual permite identificar la superficie de ataque y definir medidas de mitigación adecuadas. El método

que se plantea para modelar amenazas en los marcos de seguridad es STRIDE+P según IG1186, IG1187 e IG1195, y la adopción sistemática de las mejores prácticas propuestas por OWASP para Open APIs.

Parte de esas buenas prácticas, se consideran en los proyectos y normativas como *OWASP API Security Project*, *OWASP Application Security Verification Standard (ASVS)*, y las series *NIST SP 800-228*, *800-63* y *800-53 Rev 5*. Estos recursos proporcionan un marco integral para diseñar e implementar controles de seguridad que aborden las vulnerabilidades más comunes y críticas en entornos como en los que convergen las Open API de TM Forum. Es por ello que se deben tener en cuenta a la hora de seleccionar los controles de seguridad para este tipo de API.

La taxonomía presentada constituye un fundamento empírico para el desarrollo de futuros marcos de seguridad específicos para las Open API de TM Forum. Este modelo de correlación permite localizar amenazas arquitectónicas concretas, priorizar controles por componente y dimensionar el impacto regulatorio en función del tipo de datos expuestos.

Referencias bibliográficas

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 Framework*. 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>



Del Centro de Datos al servicio: extendiendo el Modelo Tier

From Data Center to service: extending the Tier Model

Ing. Ernesto Carrazana Ruiz ^{1*}, Ing. Irisleidis Lázara Casi Estevanell ²,
Esp. Héctor Manuel Jacas Joa³

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

Las pautas para el diseño e implementación de un Centro de Datos se encuentran ampliamente documentadas, con un alto nivel de detalle en cada aspecto a considerar para el despliegue de una infraestructura. Sin embargo, este no es el caso para el diseño de la redundancia de un servicio informático. Por tanto, el presente artículo propone una adaptación del modelo Tier de Uptime Institute, para servicios informáticos, apoyado por las mejores prácticas de diseño. Se emplean, como casos de uso, las plataformas de hospedaje web de ETECSA como ejemplos de optimización, alta disponibilidad y seguridad. En cualquier servicio informático, la optimización de los recursos y la seguridad digital son esenciales en la búsqueda del 100 % de disponibilidad. Este artículo puede ser de interés en caso de necesitar un apoyo para el diseño de servicios informáticos resilientes y seguros.

^{1*} Empresa de Telecomunicaciones de Cuba S.A (ETECSA). Dirección postal: 11300. ernesto.carrazana@etecsa.cu

² Empresa de Telecomunicaciones de Cuba S.A (ETECSA). Dirección postal: 11300. irisleidis.casi@etecsa.cu

³ Empresa de Telecomunicaciones de Cuba S.A (ETECSA). Dirección postal: 11300. hector.jacas@etecsa.cu

Palabras clave: servicios informáticos, modelo Tier, modelo Tier extendido, redundancia

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 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: IT Services, Tier model, Tier Model Extended, Redundancy

Introducción

Cuba regula las Tecnologías de la Información y las Comunicaciones (TIC) en el Decreto-Ley No 370/2017 (Gaceta Oficial n.º 45 Ordinaria de 4 de julio de 2019), específicamente las define en el artículo 3 del Capítulo 1: «Se denominan Tecnologías de la Información y la Comunicación, en lo adelante TIC al conjunto de recursos, herramientas, equipos, programas y aplicaciones informáticas, redes y medios, que permiten la compilación, procesamiento, almacenamiento y recepción de la información en cualquier formato: voz, datos, texto, video e imágenes». Mientras que la seguridad de las TIC se regula en el Decreto-Ley n.º 360/2019 (Gaceta Oficial n.º 45 Ordinaria de 4 de julio de 2019). Ambos decretos enmarcan con alto grado de detalle el uso y seguridad de las TIC en la sociedad cubana, sin embargo, no se recoge un estándar, requisito o norma para el diseño e implementación de la redundancia y consecuente grado de disponibilidad de los servicios informáticos generados con las TIC.

A nivel internacional, Uptime Institute, creador y certificador del modelo Tier, recoge en su web los Tiers (niveles) según el alcance y las características de los centros de datos, reflejadas en el nivel de

disponibilidad anual en porcentaje (Tier Certification, Uptime Institute, 2025). Cada Tier refleja un conjunto de requisitos asociados a un determinado tiempo de afectación de servicio máximo que se puede permitir. A continuación, se resumen algunos de los principales requisitos de este modelo:

- Tier I: nivel más bajo, aquí se encuentran pequeños sistemas de respaldo al trabajo de oficina. Necesita de respaldo energético, climático y un local designado.
- Tier II: presenta todos los parámetros de Tier I, con la capacidad adicional de tener una mayor redundancia y capacidad de generación eléctrica.
- Tier III: presenta todos los parámetros de Tier II, con la capacidad de tener alta tolerancia a fallas e interrupciones.
- Tier IV: presenta todos los parámetros de Tier III, con el añadido de presentar varios sistemas independientes, de forma tal que las afectaciones sean siempre parciales.

Los Centros de Datos Públicos de ETECSA cumplen con las características de Tier III, por lo que cualquier cliente de Centro de Datos Virtual cuenta con una alta seguridad y disponibilidad por defecto, pero esto no significa que los servicios que se implementen sobre la infraestructura cuenten con la misma tolerancia a fallos. El presente artículo propone una extensión del modelo Tier al extrapolar los conceptos del entorno físico al ámbito de los servicios informáticos, con el objetivo de brindar una clasificación para los niveles de redundancia y disponibilidad, así como establecer cómo incrementar estos parámetros.

Materiales y métodos

La extensión del modelo Tier de Uptime Institute propuesto en este artículo tiene en cuenta, entre varios aspectos, el respaldo energético y climatización, pues quedan en una capa inferior de responsabilidad. Entonces se puede extender el modelo Tier de la siguiente manera:

- Tier I: servicios informáticos de bajo consumo de recursos destinados a redundancia y salva. Los servidores no se encuentran

especializados ni segmentados. Es posible presentar interrupciones indefinidas y pérdida permanente de información ante corrupción o caída de los sistemas.

- Tier II: servicios informáticos de consumo medio de recursos destinados a redundancia y salva. Diseños multinodos, con servidores especializados, segmentados y redundantes. Los sistemas operativos y aplicativos desplegados deben ser mantenidos y actualizados. Es posible presentar interrupciones indefinidas y pérdida permanente de información ante destrucción o corrupción de los sistemas físicos.

- Tier III: presenta todos los parámetros de Tier II, con la capacidad añadida de realizar operaciones de protección (respaldos) cruzadas geográficamente, de forma tal que, ante la destrucción física del Centro de Datos o corrupción de los sistemas, no se pierda la información y sea posible un restablecimiento total, aunque en este escenario se presentará interrupción de servicio prolongada.

- Tier IV: incrementa la capacidad de replicación y alta disponibilidad geográfica (o geo-redundancia) del Tier III, de manera tal que constituya un servicio multisitio, en el que cada sitio constituya un servicio integro, que actúe en esquemas activo-activo o activo-pasivo. Supone un alto consumo de recurso de redundancia. Implementar este esquema supone bajas probabilidades de pérdida de información e interrupciones de servicio.

Visión general

Así como para el diseño de un Centro de Datos es necesario analizar las características del local que se pretende emplear y los tipos de servidores a adquirir, es igualmente útil realizar un análisis similar para el despliegue de un servicio informático. Es fundamental informarse sobre los tipos de CPU, el tipo de almacenamiento, de la presencia o no GPU y el tipo de tecnología que orquesta la virtualización, en caso de ser una infraestructura virtualizada. La presencia de GPU es un ejemplo tajante que condiciona la toma de decisiones en el mundo actual, dado su notable impacto en los sistemas de inteligencia artificial; ante su ausencia, resulta imprescindible analizar la viabilidad de sustituirla por CPU.

Al ser consciente del entorno y tipo de servicio que se desea desplegar, el siguiente paso es ubicar en el modelo Tier extendido propuesto en este artículo el nivel de redundancia que se desea según la criticidad que supone el sistema. Se pueden resumir los aspectos a tener en cuenta de la siguiente manera:

- CPU: velocidad de CPU y tipo de asignación. En caso de entornos virtualizados, de forma general se hace referencia a CPU virtualizados, los cuales no tienen que ser necesariamente una representación 1-1 de la velocidad del CPU físico.
- Almacenamiento: tipo de disco duro físico HDD, SSD o cualquier otra denominación. De esta manera, se puede planificar, por ejemplo, reservar el almacenamiento SSD para aplicativos de alto consumo de lectura y escritura como sería una base de datos.
- GPU: la presencia de GPU es fundamental cuando se pretende desplegar sistema de inteligencia artificial.
- Tecnología que orquesta la virtualización: es importante conocer la tecnología a emplear para la gestión del entorno (si es virtualizado), ya que estas tecnologías difieren en sus características a pesar de presentar los mismos principios de diseño. Ejemplo: OpenStack, Proxmox y VCloud director de VMware.
- Redundancia: es importante estimar el consumo de recursos destinados a salvaguardar y los recursos destinados a replicar los diferentes nodos del sistema.
- Interfaces de redes: es necesario conocer el ancho de banda de las interfaces de redes, pues un alto consumo de red puede provocar cuellos de botellas.

Conectividad

Un buen esquema de red y una buena política de *firewall* facilitan la administración y disminuyen la posibilidad de errores. Una pequeña manipulación en la conectividad puede desencadenar una gran afectación de servicio. Los servicios de virtualización brindan mecanismos de *firewall* y *routers*, así como un sistema de redes virtualizadas en general.

Las tres principales medidas en el plano de la conectividad son la segmentación de redes, la implementación de una nomenclatura

estandarizada de fácil comprensión en el entorno de administración y la restricción de los accesos solo a los necesarios.

Segmentar el tráfico por interfaces de redes tiene dos fines. El primero, y más importante, es la seguridad: emplear redes diferentes en las que se permiten protocolos diferentes dificulta una brecha de seguridad y mitiga la capacidad de un atacante de causar estragos. El segundo punto es la posibilidad de cuellos de botellas si las interfaces de redes son de bajo ancho de banda. Para evitarlos, se aíslan los tipos de tráfico, permitiendo que se ejecuten en paralelo. A continuación, se presenta ejemplos de segmentación de redes:

- Red de Administración: se le presenta a cada servidor y su objetivo es que los administradores de sistema puedan acceder remotamente. Se recomienda acceder a esta red desde una VPN. En circunstancias normales, presenta bajo consumo de ancho de banda.
- Red de Contención: en entornos en los que se requieran de un *firewall* o *router*, en ocasiones los proveedores de servicio no ofrecen todas las funcionalidades requeridas; se implementa esta capa de red para aislar la Red Administración, pudiendo ser orquestada por diferentes aplicativos, por ejemplo pfSense (pfSense, 2025).
- Red de Servicio: capa recomendada si se pretende ofrecer servicios públicos, de forma tal que solo los servidores de borde se encuentren directamente expuestos a Internet. En circunstancias normales presenta consumo medio de ancho de banda.
- Red de Datos: capa en la que se reúne el mayor tráfico; por ello, es recomendable su aislamiento, sin acceso directo desde el exterior. De ser necesario, podría segmentar en redes específicas, como la red de base de datos o red de almacenamiento.
- Red Pública: red de acceso a Internet. Con una sola IP es posible emplear el sistema NAT para segmentar y aislar los servicios publicados. Por ejemplo, solo permitir los puertos 80 y 443 para el acceso a una página web.
- Red de Replicación Multisitio: en el caso de aspirar al Tier IV Extendido y si no se cuenta con un método de replicación nativo de la infraestructura, es necesario implementar esta red en cada uno

de los sitios y enlazarlos a través de una VPN para mayor seguridad. De esta forma, se asegura que los datos sean replicados de forma segura y eficiente, al no competir con otros protocolos por el ancho de banda.

Redundancia y disponibilidad

Poder alcanzar los niveles máximos de disponibilidad implica alcanzar altos niveles de redundancia. Pues un servicio con baja redundancia incurre en la posibilidad de disminuir su tiempo de disponibilidad ante pequeños problemas. Por lo que a continuación se expondrán las mejores prácticas para obtener alta redundancia mientras se optimizan los recursos:

- Múltiples servidores: desplegar cada aplicativo en al menos dos servidores independientes, brinda la posibilidad de ejecutar cambios en caliente y tolerancia a fallas.
- Aplicativos de datos: algunos aplicativos, como los de almacenamiento o base de datos, requieren de al menos tres servidores para su correcto funcionamiento, ya que deben evitar el estado de cerebro dividido (*split brain*). En este estado, cuando se tiene un número par de servidores, el clúster no es capaz de determinar cuál es el dato correcto si el 50 % presenta un dato y el 50 % restante otro dato. Por ello, se sugiere escalar horizontalmente este tipo de servicios de forma tal que se cuente con un número impar de servidores.
- Balanceo de carga: presentar múltiples caminos en el flujo requiere implementar balanceadores de carga. Bien implementados y optimizados, constituyen una poderosa herramienta, pues permiten moderar el tráfico y aprovechar la totalidad de los recursos que balancean.
- Desafío del sistema multinodo: la implementación de un sistema de múltiples nodos con balanceo de carga provoca funcionamientos indeseados en algunos aplicativos, por lo que se requiere de una capa adicional para afrontar este detalle. Por ejemplo, múltiples nodos de PHP provocan la pérdida de sesión, si no se cuenta con un sistema de caché, como *redis* o *memcached*.
- Replicación de la información: se puede tornar complejo y alto consumidor de recursos. Por ejemplo, si se tuviese el contenido

estático de una página web en cinco servidores web, con todos los nodos activos, sería necesario almacenar este contenido estático cinco veces y, además, implementar un sistema de replicación multinodo. La solución a este inconveniente es un sistema de almacenamiento centralizado, al que se puede acceder mediante la red, por ejemplo, empleando el protocolo NFS.

- Replicación por la red: este proceso puede convertirse en un desafío si no se cuenta con los parámetros de red que exige el aplicativo de replicación. Por esta razón, en el diseño del sistema se debe tener presente la factibilidad de la replicación sincrónica (el dato debe replicarse correctamente en todos los nodos antes de proceder) o asincrónica (el dato se replica según un esquema planificado).

- Replicación de la infraestructura: la replicación la puede garantizar la propia infraestructura con sistemas de replicación nativos del equipamiento.

- Balanceo global: en un escenario de Tier IV Extendido, se presenta como desafío el balanceo de carga entre regiones. Elegir una solución adecuada al entorno en que se encuentra desplegado la plataforma es vital para el correcto funcionamiento de este complejo diseño.

- Sistema de salvallas: tanto los datos como los servidores en sí deben ser sujeto de protección. Es recomendable tratar estos dos esquemas de formas diferentes, pues no siempre será recomendable restaurar un servidor en su totalidad, si con restaurar los datos se puede solucionar la afectación de servicio. Asimismo, es conveniente planificar diferentes períodos de retención y ejecución de salva para diferentes servidores; por ejemplo, una base de datos debería de protegerse con mayor frecuencia que un servidor web.

Servidores y aplicativos

La especialización de los servidores es deseable por muchas razones, pero la principal es el aislamiento de los aplicativos, lo cual facilita el mantenimiento y actualización de los sistemas y añade una capa más de seguridad. A continuación, se expondrán factores a

tener en cuenta en el diseño y despliegue de alguno de los sistemas y aplicativos de mayor uso:

- **Balanceadores de carga:** entre las muchas opciones destacan NGINX, Apache y HAProxy. Sus respectivas documentaciones pueden consultarse en las referencias (nginx, 2025), (Apache HTTP Server Project, 2025) y (HAProxy, 2025). HAProxy sobresale por encima de la competencia gracias a su robustez, velocidad, versatilidad y funcionalidades. En términos generales, HAProxy puede ser la solución para cualquier necesidad de balanceo.

- **Almacenamiento:** las necesidades de almacenamiento distribuido aumentan en entornos redundantes. Soluciones como GlusterFS y Ceph (*GlusterFS*, 2025; Ceph, 2025) permiten brindar almacenamiento en forma de NFS u otro protocolo que necesite los aplicativos a implementar. En el caso de los ejemplos expuestos, la selección de uno sobre el otro se encuentra sujeta a la magnitud del sistema, GlusterFS presenta una menor curva de aprendizaje, pero menos funcionalidades; todo lo contrario, con Ceph, una implementación altamente compleja y versátil.

- **Servidores web:** NGINX y Apache son las opciones más populares en la actualidad para esta finalidad. Ambos se asemejan en desempeño y funcionalidades, decantarse por una o el otra dependerá de los pequeños detalles como la existencia del fichero «*htaccess*» en Apache que permite realizar cambios en caliente.

- **Cache de memoria:** Redis y Memcached (Redis The Real time Data Plataform, 225; Memcached-a distributed memory object caching system, 2025) son de las más empleadas en la actualidad para potenciar el desempeño de sistemas. Ambos son fáciles de desplegar, pero solo Redis presenta la posibilidad de replicación en entorno de alta disponibilidad, sin embargo, estas soluciones consumen grandes cantidades de recurso.

- **Firewall, router, VPN:** pfSense (pfSense, 2025) es la solución idónea cuando se necesita de todas estas funcionalidades, una herramienta integral, de fácil despliegue, con la posibilidad de implementarse en entorno de alta disponibilidad, incluso con facilidades para entornos multisitio.

- Base de datos: MariaDB (MariaDB Foundation - MariaDB.org, 2025), PostgreSQL (PostgreSQL: The World's Most Advanced Open Source Relational Database, 2025), y muchas otras son opciones factibles para el despliegue en el plano virtual, sin embargo, el factor determinante es el desempeño cuando de formar un clúster se trata, pues la dificultad en el despliegue y las características de red pueden provocar un considerable deterioro en el tiempo de respuesta.

- Mecanismos de seguridad: sistemas operativos como Windows o Linux presentan mecanismos nativos de seguridad, como *firewalls* o políticas de seguridad. En el caso de Linux es importante la correcta configuración de SELinux, un mecanismo nativo de políticas de seguridad que, si no se ajusta de forma adecuada, puede provocar situaciones indeseadas en la administración y en el servicio brindado. Adicionalmente, si se pretende ofrecer servicios de cara a Internet es recomendable implementar algún aplicativo especializado en la protección de aplicaciones web, como ModSecurity (Modsecurity Project, 2025).

- Protección de servidores: la protección de los servidores debería ocurrir como una tarea automatizada, de preferencia con las herramientas que brinda la infraestructura en la que se encuentra la plataforma. De no ser posible, mínimo se debería descargar con periodicidad las máquinas virtuales y almacenarlas en un sitio diferente.

- Protección de datos: los datos pueden ser replicados con herramientas como Rsync (rsync(1) - *Linux man page*, 2025) o Lsync (lsyncd, 2025), los cuales permiten enviar los datos de manera remota a entornos seguros. En el caso de las bases de datos se pueden ejecutar *dumps* periódicamente.

- Servicio de identidad y acceso: aplicativos como FreeIpa (FreeIPA - Identity, Policy, Audit - FreeIPA Documentation, 2025) o OpenLdap (OpenLdap, Main Page, 2025) son esenciales en entornos con múltiples administradores y/o usuarios, pues posibilita el control centralizado de usuarios y sus roles a lo largo de todos los sistemas.

Resultados y discusión

Siguiendo la metodología expuesta en este artículo, a continuación, se ejemplificará un diseño para una plataforma de hospedaje compartido. Esta se implementaría sobre el servicio de Centro de Datos Virtual de ETECSA.

La visión general de la plataforma es ofrecer un servicio de hospedaje web a múltiples clientes, de modo que todas las páginas compartan los mismos recursos, pero de manera aislada. El diseño tuvo como objetivo ubicarlo en el Tier III Extendido, tomando las decisiones tecnológicas con el objetivo de promover posteriormente la plataforma a un Tier IV Extendido.

Se emplean cinco redes diferentes en este diseño:

- Red de administración a través de una VPN
- Red Pública
- Red de Servicio
- Red de Datos
- Red de Autenticación para aislar el tráfico proveniente del servicio de identidad

La plataforma distribuye sus funcionalidades en los servidores:

1. Firewall: servicio brindado por la infraestructura. Constituye el primer *firewall* de la plataforma, en el que se realiza el control de IP y puertos, así como los enrutamientos.

2. Balanceadores: constituyen la entrada de la plataforma y se implementa en modo activo-pasivo. Su principal función se lleva a cabo con el servicio Haproxy, la cual es distribuir el tráfico según el tipo de conexión que establezcan los clientes (FTP, HTTP, HTTPS) y balancear la carga entre los servidores que trabajan activo-activo, como es el caso del balanceo de las peticiones HTTP y HTTPS entre los dos servidores web. Adicionalmente, se establece como un segundo nivel de seguridad, debido al uso de la herramienta Fail2Ban, enfocada a mitigar el spam y los ataques DDoS.

3. WAF (*Web Access Firewall*): como tercera barrera defensiva, se aprovecha la robusta sinergia que presenta el servicio NGINX con el módulo ModSecurity, para procesar y detectar contenido malicioso en las URL que puedan derivar en inyecciones SQL o ataques de

fuerza bruta. Así como la detección de contenido sensible y un grupo de pequeñas vulnerabilidades, dotando a la plataforma de gran seguridad y confianza.

4. Web: son los servidores principales de la plataforma, donde se ejecutan los servicios de las páginas web, con el servicio de Apache de conjunto con múltiples versiones de PHP. Su diseño e implementación permite que los dos servidores dedicados a esta función trabajen de conjunto para procesar todas las peticiones.

5. Maxscale: toman su nombre del servicio que implementan, solución de balanceo específica de MariaDB. Trabajan en modo activo-pasivo e incorporan un servicio de cache para las consultas de base de datos, lo que disminuye el tiempo de respuesta y la carga sobre el clúster de base de datos.

6. Base de datos: estos servidores implementan MariaDB, en un esquema de máster-esclavo para las escrituras y activo-activo para las lecturas. Este doble estándar permite disminuir la posibilidad de datos corruptos y aumentar la velocidad de las consultas.

7. FTP: servicio de FTP implementado con vsftp, que los clientes pueden consumir para administrar el contenido de sus sitios.

8. IDM (Identity Manager): es el servicio de autenticación de la plataforma, en el cual se recogen los datos de los clientes y se emplean en los servidores web para encapsular a los clientes en sus directorios, de forma que tal no puedan acceder al contenido de otros clientes.

9. Servicio centralizado de NFS: es brindado por el Centro de Datos, crucial para reducir el consumo de espacio en disco de la plataforma, pues reduce la necesidad de redundar el contenido estático de los sitios y a su vez se encarga de generar las salvadas.

En la Figura 1 se muestra el diagrama de despliegue que reúne a los servidores, sus componentes y la interacción entre ellos.

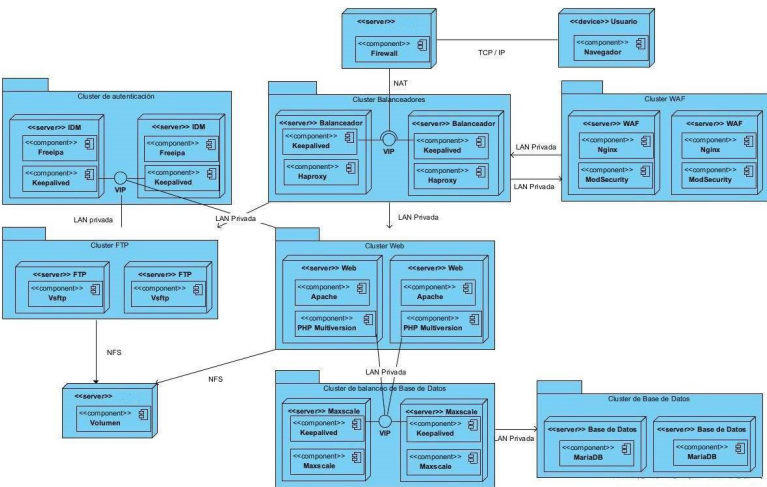


Figura 1. Diagrama de despliegue

Al analizar el gráfico de la Figura 2 se evidencia la efectividad en el diseño e implementación de las cuatro plataformas de hospedaje web de ETECSA: Hospedaje Web Empresarial (acoge a clientes estatales), Hospedaje Web Naturales (acoge a personas naturales y MYPI-MES), GOB.CU (acoge sitios web de prioridad nacional) y Centro de Información para la prensa (CIP, pensada para acoger periódicos digitales nacionales), las cuales asemejan su diseño al expuesto en este epígrafe. Los tiempos de disponibilidad de CIP y GOB.CU son perfectos, haciendo notar que CIP pertenece por sus características al Tier IV Extendido, mientras que las otras tres plataformas pertenecen al Tier III Extendido.

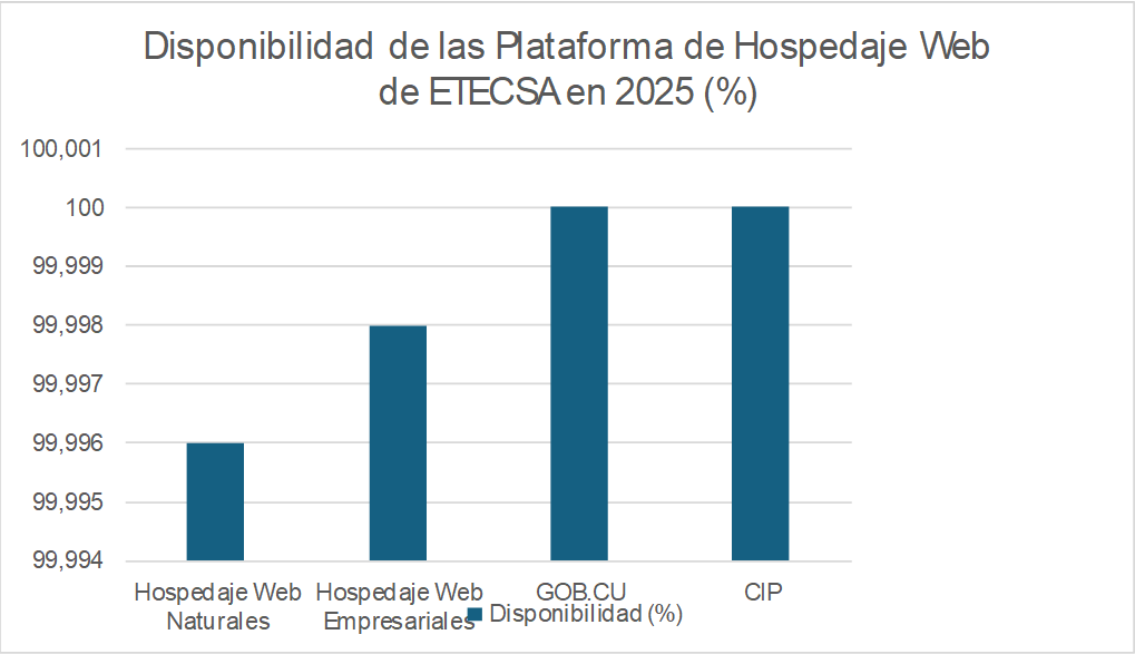


Figura 2. Disponibilidad de las plataformas de hospedaje web de ETECSA en 2025 (%)

El gráfico de la Figura 3 demuestra dos hechos: un diseño enfocado en la seguridad y correctamente implementado proveerá de resultados satisfactorios en el tiempo. Solo se ha registrado dos incidentes de ciberseguridad entre las cuatro plataformas en el año 2025 que hospedan a más de 500 páginas web. Sin embargo, ni los sistemas más seguros están exceptos de puntos de fallas, pues ambos incidentes se debieron a la obtención de las claves de administración por parte de agentes maliciosos.

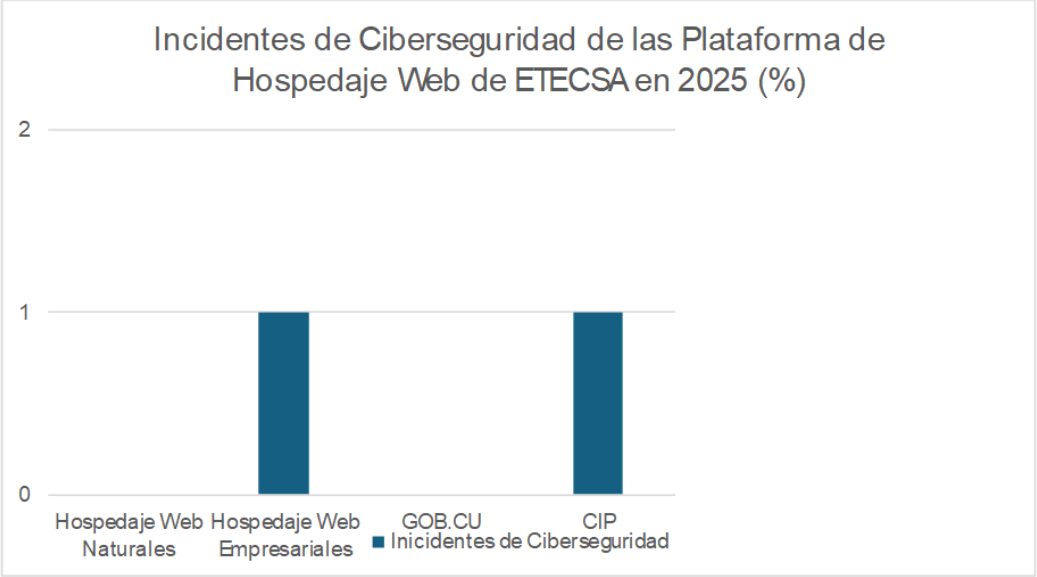


Figura 3. Incidentes de ciberseguridad de las plataforma de hospedaje web de ETECSA en 2025 (%)

Conclusiones

El Modelo Tier Extendido presentado en este artículo ofrece una guía clara y sencilla sobre las pautas a seguir en el diseño de la redundancia para los servicios informáticos. Además, facilita el levantamiento de un servicio informático y la identificación de los puntos de mejora en la optimización y disponibilidad. También provee las buenas prácticas de redundancia de servicios informáticos. Y, por último, no es una camisa de fuerza, sino una herramienta más de apoyo en el diseño y la toma de decisiones.

Referencias bibliográficas

Apache HTTP Server Project. (05 de 10 de 2025). Obtenido de Apache: <https://httpd.apache.org>

FreeIPA - Identity, Policy, Audit - FreeIPA Documentation. (05 de 10 de 2025). Obtenido de FreeIPA: <https://www.freeipa.org>

Gaceta Oficial No 45 Ordinaria de 4 de julio de 2019. (05 de 10 de 2025). Obtenido de *Gaceta Oficial de La República de Cuba*: <https://www.gacetaoficial.gob.cu/sites/default/files/goc-2019-o45.pdf>

GlusterFS. (05 de 10 de 2025). Obtenido de Gluster: <https://www.gluster.org>

Haproxy The Reliable, High Performance TCP/HTTP Load Balancer. (05 de 10 de 2025). Obtenido de Haproxy: <https://www.haproxy.org>

lsyncd. (05 de 10 de 2025). Obtenido de github: <https://github.com/lsyncd/lsyncd>

MariaDB Foundation - MariaDB.org. (05 de 10 de 2025). Obtenido de MariaDB: <https://mariadb.org>

memcached - a distributed memory object caching system. (05 de 10 de 2025). Obtenido de memcached: <https://memcached.org>

Modsecurity Project. (05 de 10 de 2025). Obtenido de Modsecurity: <https://modsecurity.org>

nginx. (05 de 10 de 2025). Obtenido de nginx: <https://www.nginx.org>

OpenLdap, Main Page. (05 de 10 de 2025). Obtenido de OpenLdap: <https://www.openldap.org>

pfsense. (05 de 10 de 2025). Obtenido de pfsense: <https://www.pfsense.org>

PostgreSQL: *The World's Most Advanced Open-Source Relational Database*. (05 de 10 de 2025). Obtenido de PostgreSQL: <https://postgresql.org>

Redis The Real-time Data Plarform. (05 de 10 de 2025). Obtenido de Redis: <https://redis.io>

rsync(1) - Linux man page. (05 de 10 de 2025). Obtenido de linux.die.net: <https://linux.die.net/man/1/rsync>

Tier Certification, Uptime Institute. (05 de 10 de 2025). Obtenido de Uptime Institute: <https://www.uptimeinstitute.com/Tier Certification>



Girasol tecnológico

Technological sunflower

Ing. Lázaro Santana Linares ^{1*}, Maikol Ismael Mirabal Hidalgo ²,
M. Sc. Raydel García Mesa ³

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

En la actualidad, el aprovechamiento racional de la energía es un aspecto fundamental para la humanidad. Para lograr la optimización de la energía solar obtenida por una instalación fotovoltaica existen dos metodologías: la primera consiste en mejorar los componentes internos de un panel fotovoltaico de manera que su rendimiento aumente y, la segunda, en aumentar la cantidad de radiación solar recibida por el panel. El presente artículo se enfoca en la segunda metodología. Para esto, se busca que el área del panel fotovoltaico permanezca en posición perpendicular a la radiación lumínica de la fuente de luz. Con tal objetivo, se muestra el desarrollo e implementación de un prototipo de seguidor solar de dos ejes, para ser aplicado a diversos sistemas fotovoltaicos y de captación solar. Esta aplicación permite que el sistema fotovoltaico incremente su producción de un 20 a un 40 %. Se diseñó y construyó un dispositivo de bajo costo, de construcción sencilla, con estructura flexible y adaptable

^{1*} Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE). Calle 9naB /282 y 284, Santa Fe, Playa, La Habana. lazarosantana9627@gmail.com

² Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE). Calle 9naB /282 y 284, Santa Fe, Playa, La Habana. maikolmirabal@nauta.cu. Afiliación institucional completa. Dirección postal. maikolmirabal@nauta.cu

³ Universidad Tecnológica de La Habana José Antonio Echeverría (CUJAE). Calle 9naB /282 y 284, Santa Fe, Playa, La Habana. raydel.gm@cime.cujae.edu.cu

a otros módulos solares, de funcionamiento automático y continuo, de bajo consumo de corriente eléctrica, y que puede ser utilizado en otras aplicaciones que requieran una actividad de seguimiento solar. Se utilizó una placa de Arduino Nano; motores de paso con su controlador; sensores LDR (Light Dependent Resistor), es decir, fotorresistencia; y un módulo Bluetooth para la comunicación inalámbrica con dispositivos Android. Además, se desarrolló una aplicación para facilitar su uso por el usuario, una batería y una placa electrónica para la conexión de todos los componentes.

Palabras clave: Seguidor solar, Arduino, Prototipo, Sistema fotovoltaico

Abstract

At present, the rational use of energy is a fundamental aspect for human communities. To achieve the optimization of the solar energy obtained by a photovoltaic installation there are two methodologies. The first is to improve the internal components of a photovoltaic panel so that its performance increases. The second is to increase the amount of solar radiation received by the panel. This article focuses on the second methodology. For this, it is sought that the area of the photovoltaic panel remains perpendicular to the light radiation of the light source. With this objective, the development and implementation of a prototype of a two-axis solar tracker is shown, to be applied to various photovoltaic and solar collection systems. This application allows the photovoltaic system to increase its production by 20 to 40%. A low-cost device was designed and built, with low electrical current consumption, of simple construction, with a flexible structure and adaptable to other solar modules, with automatic and continuous operation, and that 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, a Bluetooth module were used for wireless communication with Android devices. In addition, an application was developed to facilitate its use by the user, a battery and an electronic board for the connection of all the components.

Keywords: Solar tracker, Arduino, Prototype, Photovoltaic system

Introducción

Los requerimientos de la vida moderna están originando que la humanidad sea más dependiente de los recursos energéticos empleados en iluminación, refrigeración, calefacción y transporte. Lo anterior ha traído un alto consumo de combustibles fósiles ocasionando un agotamiento de estos, una aceleración del calentamiento global del planeta y una elevación del nivel de los océanos (Anusha, 2017). Los problemas de contaminación, riesgo y deterioro del medio ambiente son el motivo por el cual es importante buscar fuentes alternativas de energía a la nuclear y a la derivada de combustibles fósiles.

Afrontar las necesidades energéticas de manera sostenible contribuirá en gran medida a la solución de los retos de principio de siglo como la pobreza, el cambio climático, la seguridad alimentaria, entre otros (Casimiro *et al.*, 2018). La convergencia actual de diversas crisis (económica, junto con la continua volatilidad de los precios del petróleo y los alimentos) configura un escenario adecuado para plantear una nueva formulación de las políticas, así como para destinar mayores inversiones hacia un proceso de desarrollo más seguro y sostenible.

La cantidad de energía solar recibida anualmente por la Tierra es $1,5 \times 10^{18}$ KWh, lo que representa 10 000 veces el consumo de energía en ese mismo período, o sea, el Sol es el actor principal de los procesos biológicos en la tierra y puede ser considerado una fuente inagotable de energía que puede ser aprovechada mediante un adecuado sistema de captación y conversión a energía eléctrica y/o térmica, por mencionar solo algunas (Echenique *et al.*, 2018). Los sistemas de energía solar aprovechan la radiación solar incidente sobre la Tierra para generar energía eléctrica o calefacción. El aprovechamiento de la energía solar presenta ciertas dificultades sobre las cuales se está investigando para lograr de forma adecuada su aprovechamiento (Anusha, 2017).

En el caso de Cuba, el Sol brinda al territorio nacional a diario la energía equivalente a 0,5 litros de petróleo en cada metro cuadrado de la isla. Si calculamos la cantidad para 110 mil km² que tiene Cuba, llegamos a la sorprendente conclusión de que el país recibe diariamente en energía solar el equivalente a 55 millones de toneladas de petróleo (Ecured, 2020).

Sin embargo, de toda esta cantidad de energía, solo se aprovecha un porcentaje discreto, en comparación con los otros combustibles, debido a varios factores, entre los que se destacan los altos costos de las tecnologías para la captación de la energía solar y el aprovechamiento de estos sistemas.

Dentro de los distintos tipos de sistemas de captación solar destaca la fotovoltaica, la cual convierte la radiación proveniente del Sol en energía eléctrica. Existen dos formas de lograr un mejor aprovechamiento de la energía solar que se obtiene: (a) mejorar los componentes internos de las celdas fotovoltaicas (materiales y métodos de fabricación) de manera que su rendimiento aumente (*El Porvenir*, 2020), y (b) aumentar la cantidad de radiación solar recibida, buscando que el área del panel permanezca en posición perpendicular a la radiación solar (Onudi, 2009).

Con el empleo de instalaciones fotovoltaicas se puede obtener electricidad y emplearla en viviendas o con fines industriales; la electricidad obtenida puede usarse de manera directa o bien ser almacenada en acumuladores para luego utilizarse en horas nocturnas o en días que carecen de la presencia del Sol. En los últimos años el empleo de esta fuente de energía se ha ampliado desde usos comunes, como alumbrado público, alimentación de semáforos, calculadoras y otros equipos electrónicos, hasta llegar a la sorprendente aplicación en la transportation aérea, marítima y terrestre.

En los sistemas de aprovechamiento de energía solar es de gran importancia tener la capacidad de realizar un seguimiento adecuado del Sol, con la finalidad de poder adquirir la máxima cantidad de radiación en todo momento del día [Panati (2015); Plesz, *et al.*, (2009)] Con este fin, se utilizan los llamados seguidores solares, que son dispositivos electro-mecánicos que orientan la superficie captadora durante el recorrido aparente del Sol. El objetivo de este proyecto es presentar el desarrollo e implementación de un prototipo que permite realizar el seguimiento de la trayectoria solar, posibilitando así el aumento de la radiación captada por el módulo solar mediante el movimiento continuo del panel, para mejorar el rendimiento de una instalación fotovoltaica, siendo su construcción de bajo costo.

Materiales y métodos

En esta investigación se emplearon los siguientes materiales y métodos: la observación de trabajos relacionados con la temática en cuestión, el uso de Internet, el trabajo con artículos disponibles online sobre el tema, la entrevista con especialistas en paneles solares, estudio de los servomotores de Arduino y consultas bibliográficas en bibliotecas.

Seguidor solar

Un seguidor solar es un dispositivo conformado por una parte fija y una móvil, cuya finalidad es aumentar la obtención de radiación solar, para lo cual cuenta con una superficie de captación que debe permanecer perpendicular a los rayos del Sol durante el día y dentro de su rango de movimiento. Estos se usan en todas las tecnologías de seguimiento solar: energía solar fotovoltaica convencional, energía solar fotovoltaica de concentración y energía termosolar de concentración (Echenique *et al.*, 2018).

Un sistema de seguimiento solar maximiza la producción de electricidad de su sistema solar al mover sus paneles para seguir al Sol durante todo el día, lo que optimiza el ángulo en el que sus paneles reciben radiación solar. Los seguidores solares se utilizan, generalmente, para paneles solares montados en el suelo y grandes instalaciones solares independientes como los árboles solares.

Cuando los paneles solares están expuestos a la luz solar, el ángulo en el que los rayos solares se encuentran con la superficie del panel solar (conocido como el ángulo de incidencia) determina qué tan bien el panel puede convertir la luz entrante en electricidad. Cuanto más estrecho es el ángulo de incidencia, más energía puede producir un panel fotovoltaico. Los seguidores solares ayudan a minimizar este ángulo trabajando para orientar los paneles de modo que la luz los golpee perpendicularmente a su superficie (Plesz, *et al.*, 2009).

Los seguidores solares pueden ser clasificados según el tipo de movimiento que realicen y según el algoritmo de seguimiento.

Seguidor solar según el tipo de movimiento

Seguidor de un solo eje

La rotación de la superficie de captación se hace sobre un solo eje, este puede ser horizontal, vertical u oblicuo. Dicho tipo de seguimiento representa un mínimo grado de complejidad y su costo es menor en comparación con otros tipos de seguidores. La limitación de este tipo de seguidor consiste en no poder realizar un seguimiento completo del Sol ya que solo puede seguir ya sea el azimut o la inclinación solar, pero no ambas (*Plesz, et al., 2009*).

Seguidor de dos ejes

Este tipo de seguidor cuenta con dos grados de libertad y está en capacidad de realizar un seguimiento total del Sol, tanto en inclinación como en azimut, aunque el rendimiento de la instalación puede ser superior en comparación con los de un solo eje, es importante mencionar que el de dos ejes resulta ser más costoso (*Plesz, et al., 2009*) En la figura 1 se representan los seguidores solares según su tipo de movimiento.

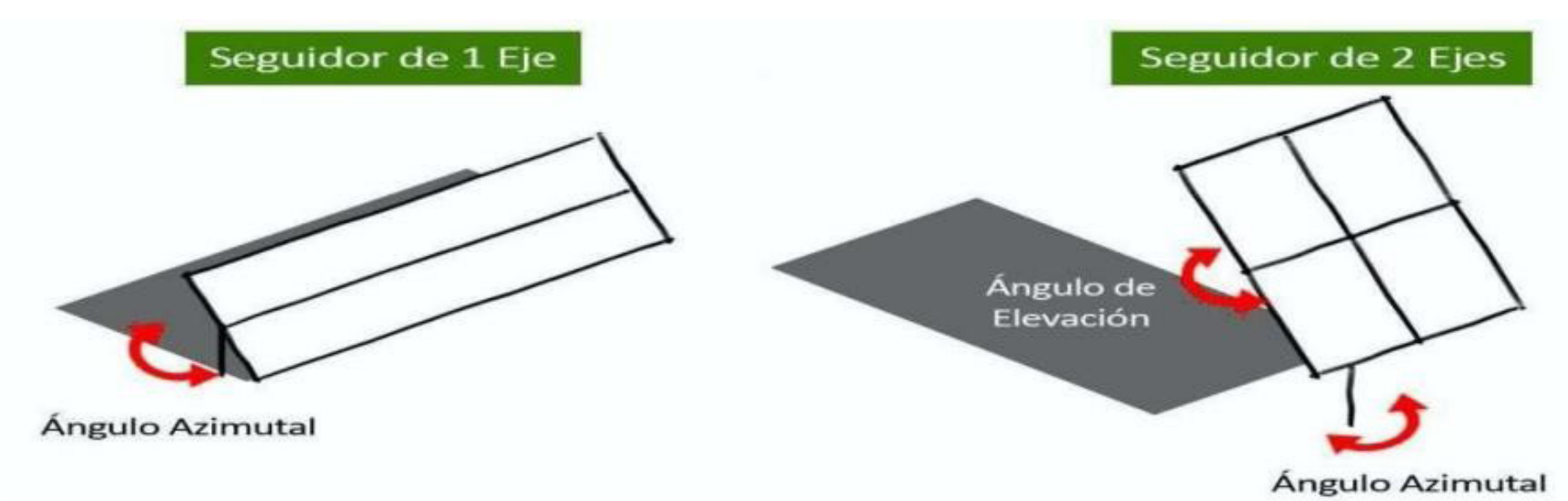


Figura 1. Esquema de seguimiento solar

Seguidor solar según el tipo de algoritmo de seguimiento

Seguimiento por reloj solar

Este tipo está sujeto a la unidad de tiempo de 24 horas y varía su posición respecto al ciclo de esta unidad, con un seguimiento efectivo de 12 horas. Efectúa su movimiento en un ángulo de 120 °. Para conseguir esto se le incorpora al dispositivo un Reloj de Tiempo Real (RTC), que se compone de un microcontrolador que cuenta el tiempo de manera precisa y, además, incorpora un sensor para compensar los cambios de temperatura que alteran los electrones del cristal de silicio (*Lakeou et al., 2006*)

Según la luminosidad

El algoritmo de este tipo de seguidor basa su funcionamiento en la señal entregada por uno o varios sensores, dependiendo de dicha señal se envía un comando de control a uno o varios motores para que se posicionen en el punto más adecuado de luminosidad. Este tipo de seguimiento resulta ser de fácil implementación (Plesz, *et al.*, 2009).

Con programación astronómica

Este tipo de seguidor presenta una total independencia de las condiciones climáticas ya que su algoritmo no requiere de sensores que indiquen cuál es el punto más luminoso. El seguimiento en este caso depende de una serie de ecuaciones que predicen la ubicación del Sol en cualquier momento. Aunque este modelo resulta ser de gran precisión, cabe mencionar que la implementación del algoritmo representa un alto grado de complejidad (Sierra *et al.*, 2008).

Se eligió para este proyecto un prototipo de seguidor solar que realice su movimiento en los dos ejes y que desarrolle un algoritmo de seguimiento según su luminosidad. Dispositivo económico, con componentes de bajo costo y reciclados. Para su realización se eligió una placa de Arduino Nano porque esta ofrece una gran compatibilidad con todos los módulos que existen en el mercado enfocados a Arduino, es de bajo costo y de programación sencilla y flexible. Una vez configurado, puede hacer un seguimiento solar de manera desatendida y automática.

Diseño general

El nuevo prototipo de seguidor solar está ahora constituido por tres etapas principales: sistema electrónico, sistema electromecánico y *software*. Antes de la confección del dispositivo se realizó la simulación en Proteus (Proteus Design Suite), como se observa en la figura 2. En dicha simulación se comprobó su correcto funcionamiento.

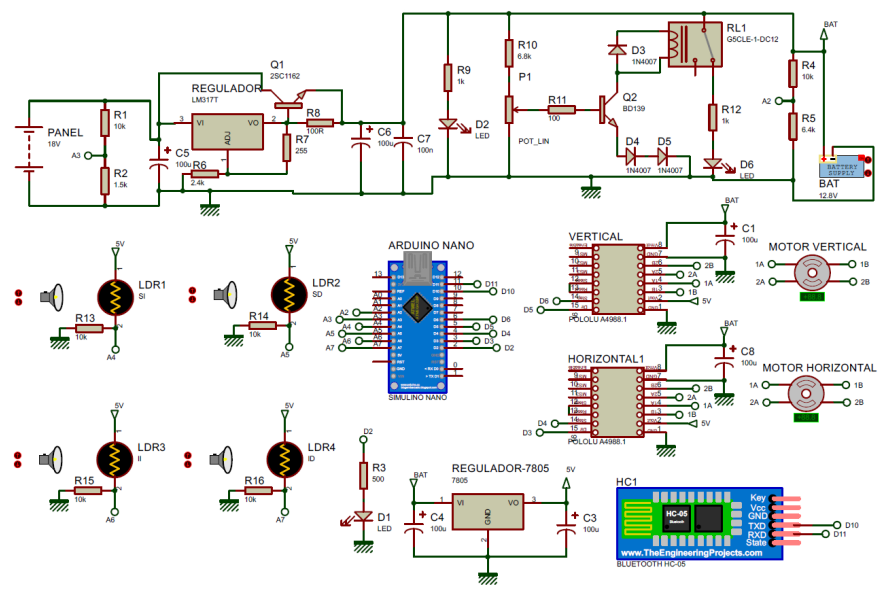
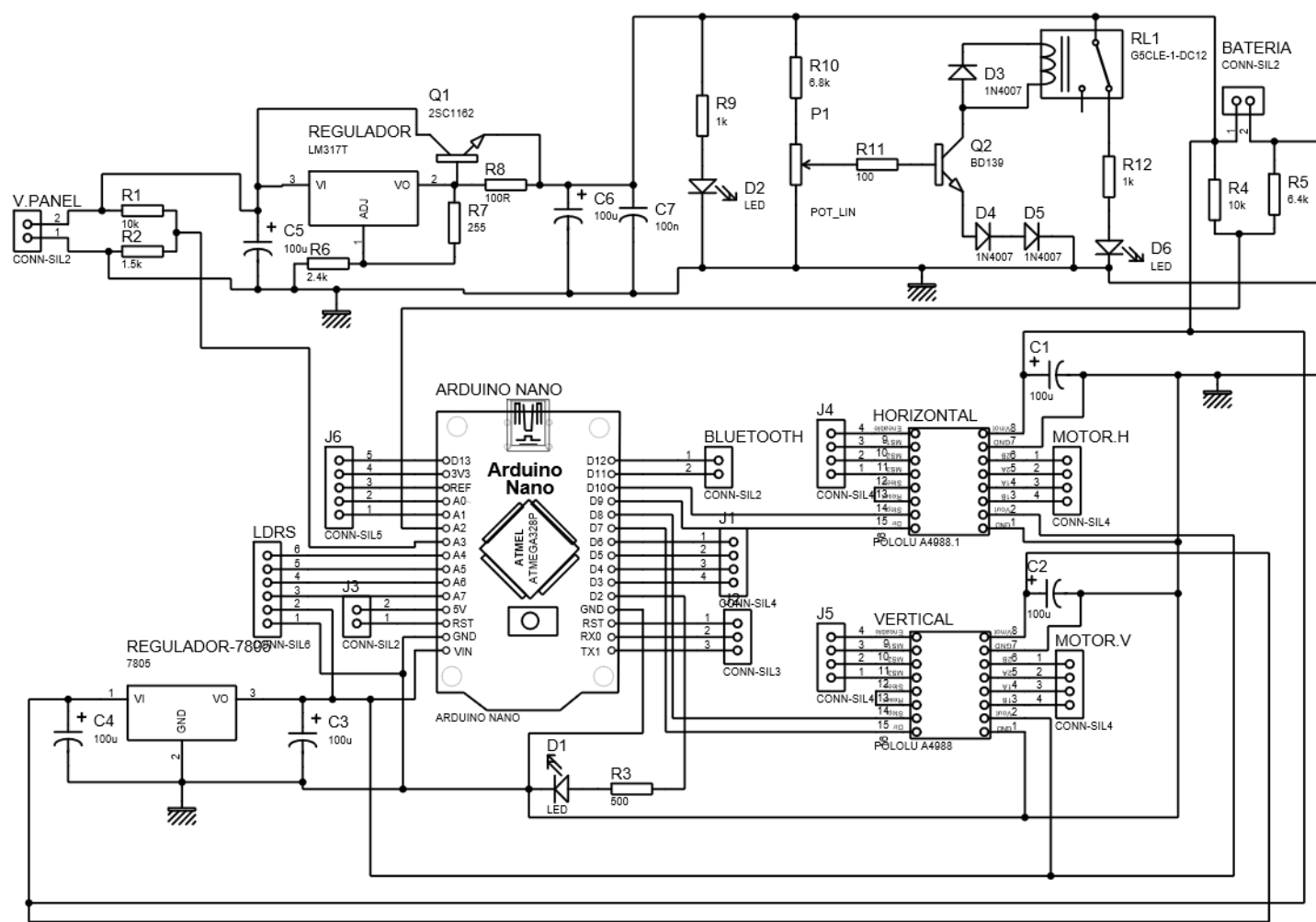


Figura 2. Simulación del prototipo en Proteus

En la figura 3 se ilustra el esquema electrónico del prototipo.



Microcontrolador

El microcontrolador de la placa Arduino se programa mediante el lenguaje de programación Arduino. Es un lenguaje de alto nivel con unas sentencias y sintaxis muy similares a las de lenguaje C. También posee un entorno de desarrollo basado en *Processing*, que permite la edición de un programa con el lenguaje Arduino, su verificación, su compilación y la grabación sobre el controlador (Sitiosolar, 2020).

El sistema de seguimiento usa la placa Arduino Nano (Figura 4) como controlador principal. Dicha placa será utilizada para el control de los motores a través de cuatro salidas digitales conectadas a dos controladores A4988, así como también será utilizada para leer la información

de los cuatro sensores de radiación por medio de cuatro entradas analógicas. En el cuadro 1 se observan las características técnicas de la placa Arduino Nano.



Figura 4. Arduino Nano

Cuadro 1. Características técnicas de la placa Arduino Nano

Microcontrolador	ATmega 328
Voltaje de entrada	7-12V
Voltaje de trabajo	5V
Pines digitales de E/S	22 (6 salidas PWM)
Pines analógicos de E/S	8
Corriente por pines de E/S	40 mA
Memoria Flash	32 KB con 2 KB para el bootloader
SRAM	2 KB
EEPROM	1 KB
Velocidad de reloj	16 MHz

Control de motor paso a paso A4988

La placa A4988 o driver A4988 «Pololu» (Figura 5) controla un motor paso a paso de hasta 2A. Posee cinco resoluciones diferentes: paso completo, medio paso, cuarto de paso, octavo de paso y dieciseisavo de paso. El control se realiza de forma que cada pulso de entrada escalón corresponde a un micropaso del motor paso a paso en la dirección seleccionada por el pin DIR (Lakeou *et al.*, 2006). Se utilizaron dos *drivers* A4988, para el control de los dos motores de paso utilizados, se configuraron para un funcionamiento a pasos completos y a 1A.



Figura 5. Driver A4988

Sensores de posición solar

Para el posicionamiento se emplearon sensores LDR o fotorresistencia, que consiste es una resistencia variable en función de la luz incidente sobre su superficie. Cuanto mayor sea la intensidad de la luz que incide en la superficie del LDR menor será su resistencia y cuanta menos luz incida mayor será su resistencia (Sitiosolar, 2020). Para el presente proyecto se dispusieron cuatro sensores LDR, uno para cada cuadrante del panel o módulo solar (superior derecho e izquierdo, inferior derecho e izquierdo), como se ilustra en la figura 6.

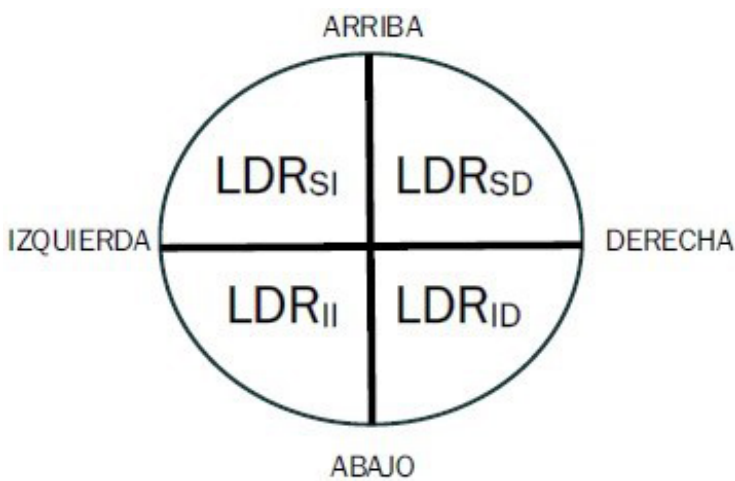


Figura 6. Distribución de los LDR

El sistema siempre lleva a que los cuatro sensores tengan la misma intensidad de luz, lo que indica que el panel está orientado hacia el Sol. Las señales acondicionadas provenientes de cada LDR son leídas en entradas independientes del Arduino Nano, el cual realiza su calibración, cálculo y ejecuta los movimientos correspondientes de los motores de paso. Se incorporó un diodo emisor de luz (LED) que permite visualizar el tiempo de calibración de los LDR.

Módulo Bluetooth

Al sistema se le incorporó el Módulo Bluetooth HC-05 (Figura 7). Este conecta el Arduino con un dispositivo de forma inalámbrica (Bluetooth), con la facilidad de operación de un puerto serial. Todos los parámetros del módulo se pueden configurar mediante

comandos AT. La comunicación Bluetooth se da entre dos tipos de dispositivos: un maestro y un esclavo. Se denomina Bluetooth al protocolo de comunicación diseñado especialmente para dispositivos de bajo consumo que requieren corto alcance de emisión y basados en transceptores de bajo costo.



Figura 7. Módulo Bluetooth HC-05

Batería

Para la acumulación de la carga eléctrica que genera el sistema foto-voltaico se desarrolló una batería con celdas de litio 18650 recicladas de laptops y baterías de vehículos eléctricos. Esta también se utiliza como fuente de alimentación del circuito electrónico y los dispositivos utilizados, lo que permite un sistema autoalimentado y de funcionamiento constante.

Se utilizaron un total de 12 celdas, conectadas en tres columnas y cuatro filas. Se obtuvo como resultado un batería de litio de 12,6V y 10A, similar a la que se ilustra en la figura 8.

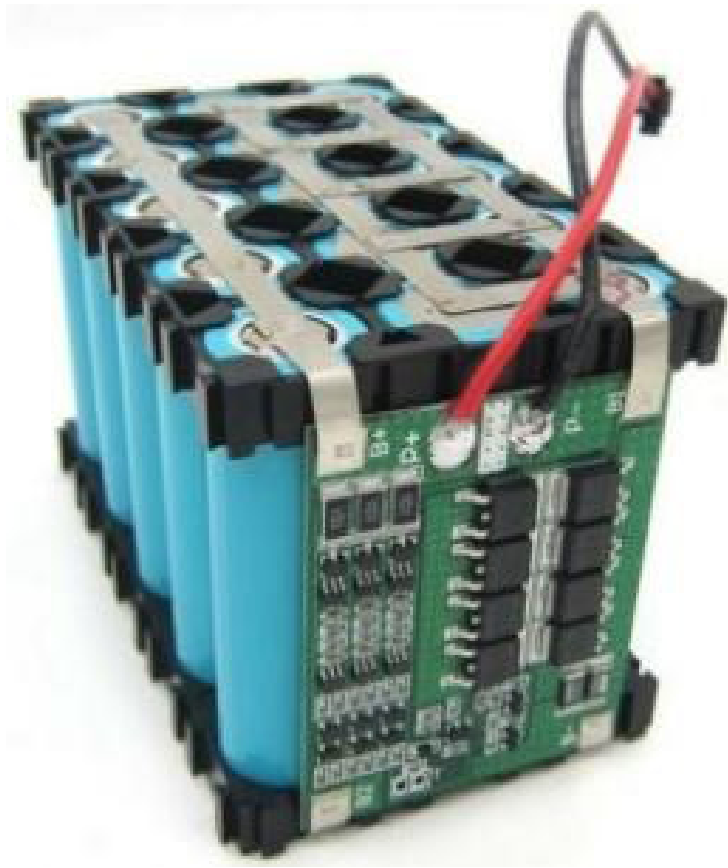


Figura 8. Batería.

Placa electrónica

Se desarrolló una placa de circuito impreso (PCB) para la conexión de los dispositivos electrónicos del prototipo: placa Arduino Nano, controladores A4988, sensores LDR y módulo Bluetooth. Además, se implementó un circuito para la regulación del voltaje entregado por el sistema fotovoltaico y la desconexión automática de la batería, esto facilitó la adecuada carga de la misma. Se utilizaron: resistencias de 100Ω 3W, 100Ω, 255Ω, 1KΩ, 1,5KΩ, 2,4KΩ, 6,4KΩ, 10KΩ y un potenciómetro; capacitores electrolíticos de 100uF 50V y 100uF 25V; diodos 1N4007; LEDs de 5mm 3,6V; un transistor 2SC1162 y un BD139, un relé 12V y un regulador de voltaje LM317T.

En dicho circuito se añadieron componentes electrónicos para la visualización, protección de los dispositivos y regulación del voltaje de alimentación. Dichos componentes son: regulador de voltaje 7805, capacitores electrolíticos de 100uF 50Vy 100uF 16V, resistencias de 500Ω y 10KΩ, y un LED de 5mm 3,6V.

En la figura 9 se observan las dos caras de la PCB desarrollada en Proteus. Sus dimensiones son: 97,3 mm de ancho y 121,5 mm de largo.

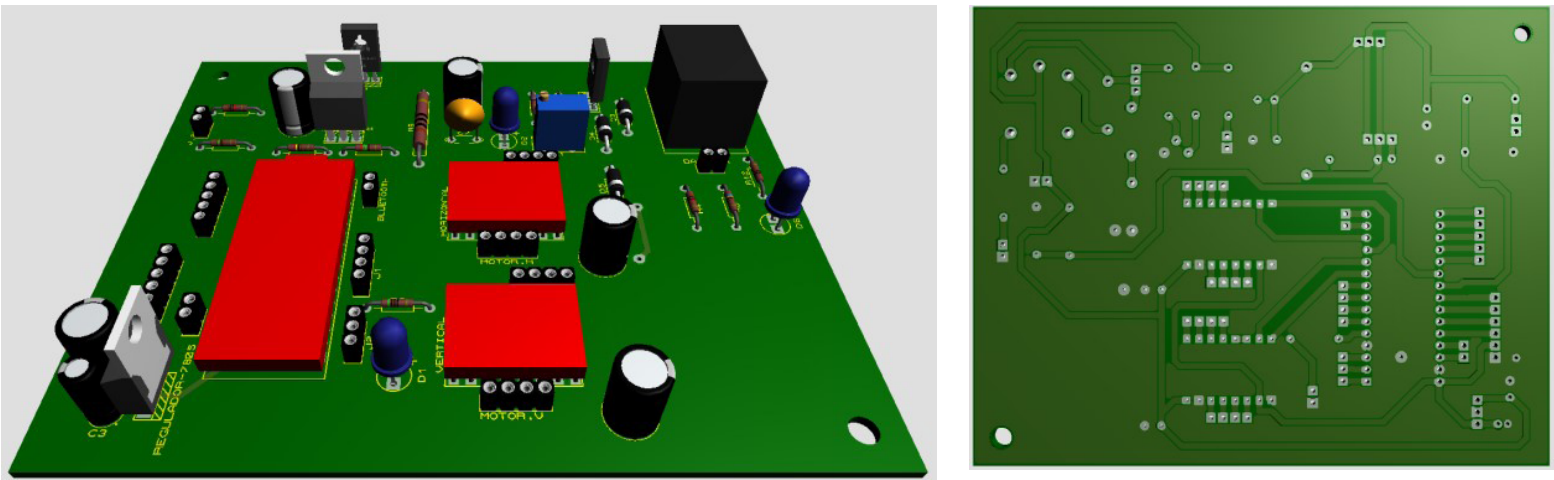


Figura 9. PCB del prototipo

Sistema electromecánico

Estructura metálica

Para la sujeción del panel solar se empleará una pieza metálica en forma de U en la cual descansará el módulo fotovoltaico. Dicha pieza descansará sobre una base metálica en forma de cubo, para este prototipo se utilizó un chasis reciclado de una fuente de alimentación de computadora. Dentro de esta base se colocará la placa de circuito impreso. Se utilizaron también reductores reciclados de impresoras en desuso para mejorar la movilidad del sistema.

Es importante señalar nuevamente que todo el conjunto descrito será muy ligero para evitar el uso de motores con grandes dimensiones, ya que aumentaría el costo y la complejidad del sistema.

Motores paso a paso

El motor paso a paso, conocido también como motor de pasos, es un dispositivo electromecánico que convierte una serie de impulsos eléctricos en desplazamientos angulares discretos, lo que significa que es capaz de girar una cantidad de grados dependiendo de sus entradas de control (Lakeou *et al.*, 2006). En este prototipo se utilizaron dos motores de paso EM-323 reciclados de una impresora EPSOM LX-300+. Los cuales tienen un paso de 3,75 ° (96 pasos por vuelta). En el cuadro 2 se muestran las características técnicas de dicho motor.

Cuadro 2. Características técnicas del motor de paso EM-323

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)

Softwares

IDE Arduino

Dado que el Arduino es una placa que ejecuta una serie de códigos previamente introducidos. Se necesita un programa denominado IDE (Integrated Development Environment o Entorno de Desarrollo Integrado) para cargar dichos códigos. Este IDE, instalado en una PC, es un entorno muy sencillo de usar y en él se escribe el programa a ejecutar por Arduino. Una vez escrito, se carga a través del puerto USB y Arduino comenzará a trabajar de forma autónoma (Sitiosolar, 2020) A grandes rasgos, se puede apreciar el funcionamiento del *software* desarrollado a través del diagrama de flujo de la figura 10.

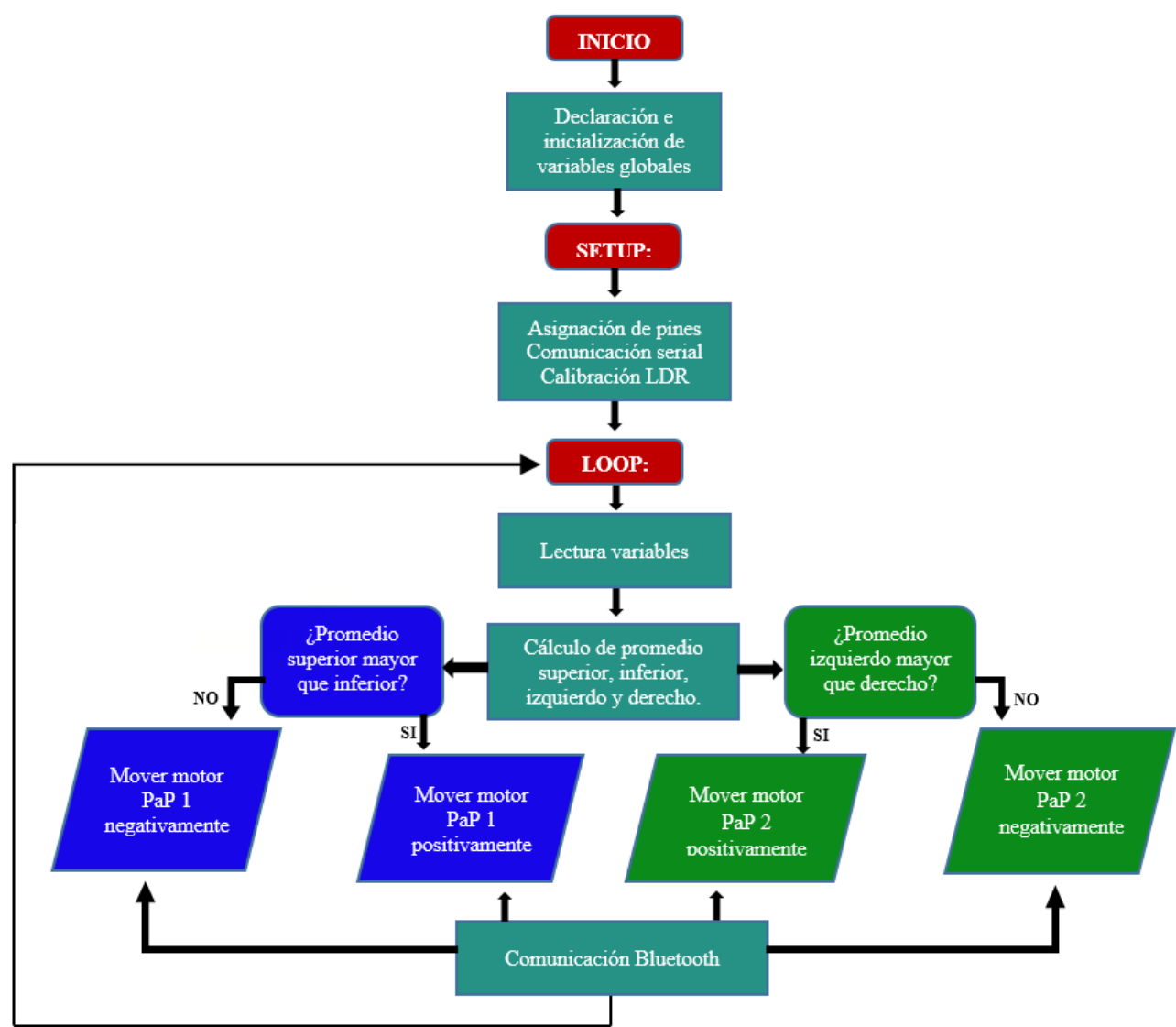


Figura 10. Diagrama de flujo básico

App Inventor

App Inventor es un entorno de desarrollo de *software* creado por Google Labs para la elaboración de aplicaciones destinadas al sistema operativo Android. El sistema es gratuito y se puede descargar con facilidad en la web. Se desarrolló en esta plataforma una aplicación propia para este sistema y compatible con dispositivos que tengan el sistema operativo Android. Dicha aplicación tiene una interfaz visual agradable, sencilla y fácil de utilizar. Permite mejorar la facilidad de control del panel solar por parte de los usuarios, así como la muestra de las lecturas de los valores de: Voltaje del Panel Solar, Voltaje de la Batería y Porcentaje de Carga de la Batería. Esta se muestra en la figura 11.



Figura 11. Aplicación del prototipo

La confección final del dispositivo se ilustra en la figura 12. Este prototipo se desarrolló para demostrar la funcionalidad del sistema de seguimiento solar propuesto. Sirve de base, para el desarrollo de otros sistemas de seguimiento con las mismas prestaciones, pero con característica adecuadas al módulo fotovoltaico utilizado.



Figura 12. Prototipo del seguidor solar

Resultados y discusión

Funcionamiento

Los LDR (fotorresistencias) ayudan a determinar en qué lugar existe más luminosidad durante el día, estos se colocaron en los vértices del panel. Para lograr una mayor exactitud en cuanto a la medición de la luminosidad, se deben cubrir las fotorresistencias alrededor para evitar la captación de la radiación solar difusa, en otras palabras, la propagación de la luz (ondas electromagnéticas) que se encuentran esparcidas y reflejadas en la atmósfera.

Las lecturas de estos LDR son calibradas y comparadas por el Arduino, que envía las señales a los controladores de los motores de paso para ejecutar los movimientos necesarios, por ejemplo, los grupos de LDR llamados izquierda y derecha son comparadas y si existe una diferencia mayor o menor al rango de sensibilidad determinado, entonces habrá de ejecutarse un movimiento correspondiente, de igual forma para los grupos de sensores arriba y abajo, solo que estos determinaran el movimiento del otro eje. De manera tal que la luz solar golpee de forma perpendicular la superficie del panel.

El módulo fotovoltaico transforma la energía solar captada en energía eléctrica. Esta es regulada para cargar la batería que alimenta

todo el sistema. Se desarrolló para ella un sistema de desconexión cuando se encuentra completamente cargada.

El módulo Bluetooth permite la comunicación inalámbrica entre el prototipo y el dispositivo que posea la aplicación Android desarrollada. Le facilita al usuario controlar el movimiento del sistema y conocer los valores de: Voltaje del Panel Solar, Voltaje de la Batería y Porcentaje de Carga de la Batería. La figura 13 ilustra el esquema de funcionamiento del prototipo desarrollado.

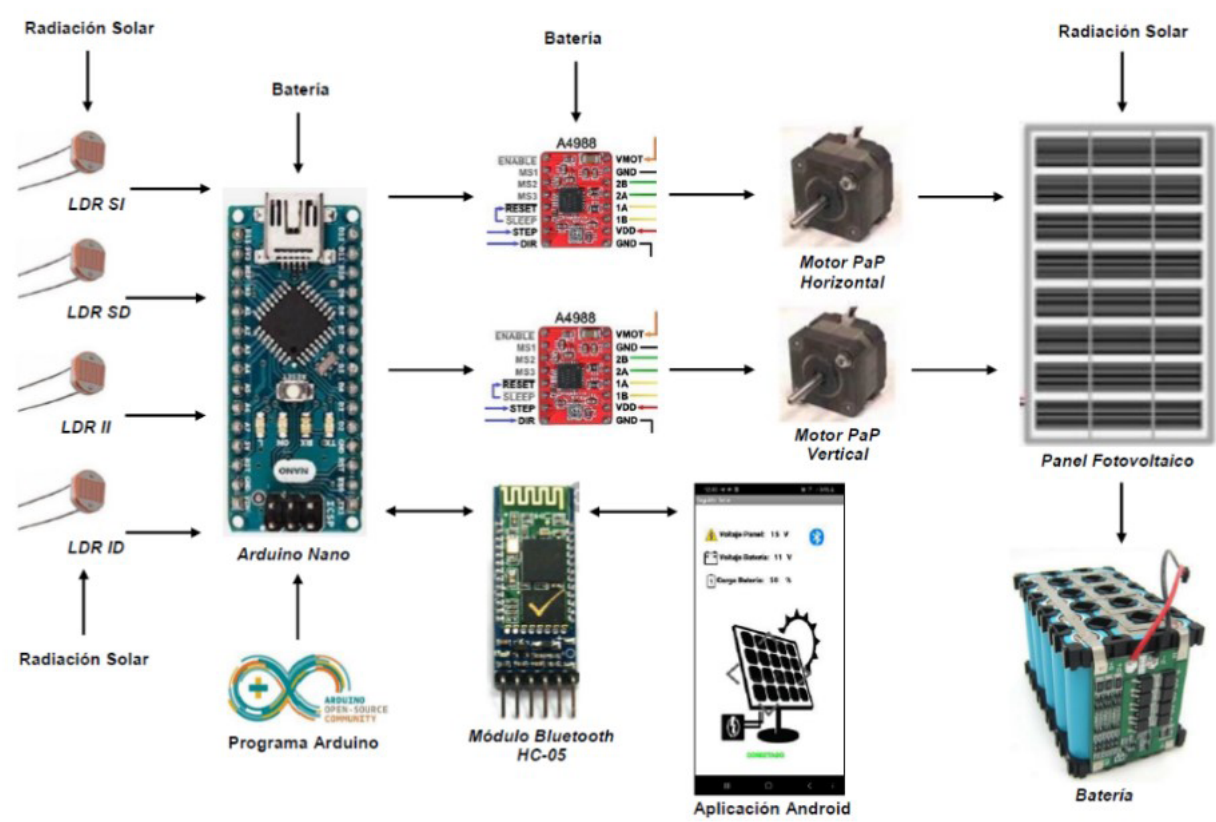


Figura 13. Esquema de funcionamiento del prototipo

Pruebas realizadas y resultados obtenidos

Las pruebas para validar el funcionamiento del dispositivo seguidor solar y el algoritmo se realizaron utilizando una fuente lumínica natural, sobre un prototipo a escala de una instalación fotovoltaica. utilizando el prototipo sin la función de seguidor en primera instancia y posteriormente con el dispositivo seguidor activado se tomaron varios valores para diferentes posiciones angulares.

Al comparar los resultados (mostrados en la Figura 14) se tiene que el aumento del rendimiento de la instalación con seguidor en comparación con la instalación estática es del 33,5 %.

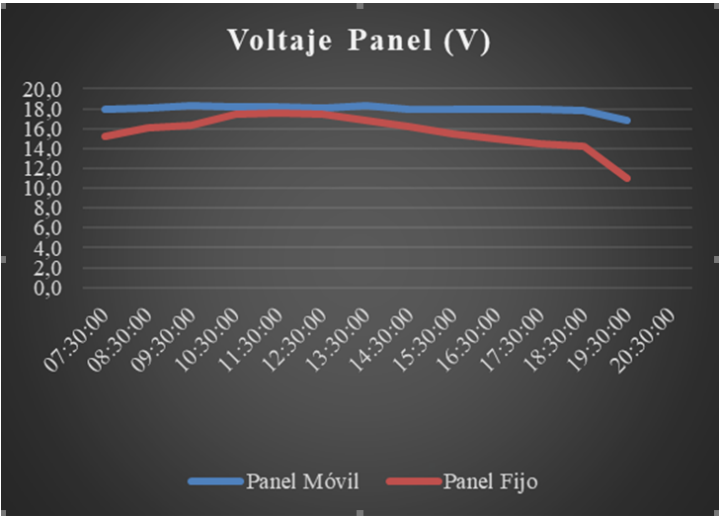


Figura 14. Comparación del voltaje medido en un panel fijo respecto a uno con el seguidor solar

Conclusiones

El prototipo construido cumple con las características requeridas de seguimiento en dos ejes, realizando el seguimiento del Sol. Esto aumenta la radiación captada por el módulo hasta un 33,5 % y, por tanto, mejorar el rendimiento de la instalación fotovoltaica. Los resultados obtenidos avalan que el seguidor solar de dos ejes desarrollado obtiene mejores prestaciones energéticas respecto de un sistema fotovoltaico con paneles fijos. Se logró la confección de un dispositivo de bajo costo, de bajo consumo de corriente eléctrica, de construcción sencilla, con estructura flexible y adaptable a otros módulos solares y de funcionamiento automático y continuo. El prototipo construido puede ser utilizado en otras aplicaciones que requieran una actividad de seguimiento solar como colectores solares, hornos solares, entre otros.

Referencias bibliográficas

- 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=253973.
- 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: ICRE-PQ.
- 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. OS-HUMARE; 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>.



Hacia una gestión de inventarios 4.0: Integración de tecnologías digitales en la cadena de suministro biofarmacéutica de Cuba

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

M. Sc. Zuleyka Calzado Mesa ^{1*}, Ing. Gabriela Ojeda de la Paz ²,
Ing. Damián Aldait García Pérez ³

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

La gestión de inventarios permite llevar un orden en el almacén y contar con mayor agilidad en las operaciones realizadas en él. Con un correcto control de este tipo de gestión, se logra que una empresa pueda satisfacer de una manera eficiente la demanda de productos a sus clientes. BioCubafarma es el grupo empresarial encargado de producir medicamentos, equipos y servicios de alta tecnología destinados al mejoramiento de la salud del pueblo cubano y orientados a la generación de bienes y servicios exportables. Cuenta con una gran parte de sus procesos informatizados, lo que optimizan muchas de sus operaciones. Sin embargo, se hace necesario el desarrollo de soluciones

^{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

tecnológicas faciliten el avance del Grupo en la transformación digital y en la evolución a la Industria 4.0. El presente artículo aborda los resultados de un proyecto de innovación sectorial realizado en la Empresa de Tecnología de la Información (ETI). Este tuvo como objetivo la introducción de etiquetas inteligentes en el sistema de gestión de inventarios de insumos que se utiliza en el grupo empresarial Biocubafarma; la modificación de dicho sistema agregándole los niveles de lote y ubicación; y el desarrollo de una aplicación en sistema Android que le permite al operario optimizar las operaciones en el almacén y comunicarse en tiempo real con el sistema de inventario.

Palabras clave: Etiquetas inteligentes, gestión de inventarios, industria 4.0, Lote, transformación digital

Abstract

Inventory management allows for organization in the warehouse and greater agility in the operations performed within it. With proper control of this type of management, a company can efficiently satisfy its customers' product demand. Biocubafarma is the business group responsible for producing medicines, equipment, and high-technology services, aimed at improving the health of the Cuban people and generating exportable goods and services. Many of its processes are computerized, optimizing many of its operations; however, it is necessary to develop technological solutions that allow the Group to continue advancing in digital transformation and the evolution towards Industry 4.0. This article addresses the results of a sectoral innovation project carried out at the Information Technology Company (ETi), which aimed to introduce smart labels into the inventory management system for supplies used by the Biocubafarma business group, the modification of said system by adding batch and location levels, and the development of an Android system application that allows the warehouse operator to optimize warehouse operations and communicate in real time with the inventory system.

Keywords: Smart labels; Inventory management; Industry 4.0; Batch; Digital Transformation

Introducción

«El inventario representa una reserva estratégica de materiales, materias primas, productos en proceso o bienes terminados que, si bien no se emplean de manera sistemática, garantizan la continuidad del servicio al cliente» (Cespón Castro, 2012). Según Schroeder (citado en Alemán Rodríguez, 2013), el inventario es una cantidad almacenada de materiales destinada a facilitar la producción o satisfacer la demanda del consumidor. En los enfoques antes mencionados se destaca que el inventario está construido por recursos físicos cuyo control riguroso es vital para evitar desabastecimientos y asegurar el buen funcionamiento de cualquier empresa o comercio.

La gestión de inventarios, definida por Cespón Castro (2012) como «el proceso que busca minimizar la cantidad almacenada sin afectar el servicio al cliente», se ha convertido en un proceso esencial para maximizar la eficiencia y rentabilidad empresarial. La logística, por su parte, integra la planificación y gestión de operaciones vinculadas al flujo de materias primas, productos semielaborados y terminados desde su origen hasta el consumidor final.

Con la llegada de la Industria 4.0 y la digitalización, la gestión de inventarios ha experimentado una transformación profunda mediante la automatización y el uso de tecnologías inteligentes. La implementación de etiquetas inteligentes, por su capacidad de almacenar datos, permite comunicarse de forma inalámbrica, la identificación a distancia, la trazabilidad y la gestión en tiempo real, mejorando la precisión y la agilidad en la cadena de suministro.

Biocubafarma, empresa líder en biotecnología y farmacéutica, ha fortalecido su proceso logístico conforme a estrictas regulaciones y ha logrado un seguimiento de la producción integral desde la recepción de materias primas hasta la entrega de productos terminados al Ministerio de Salud Pública (MINSAP). Sin embargo, persisten retos en el control a nivel de lote y ubicación de los productos del área de insumos, así como en el seguimiento de sus fechas de vencimiento en caso de productos alimenticios, imposibilitando una gestión óptima.

Frente a esta problemática, ETI emprendió el desarrollo de un proyecto de innovación sectorial para modernizar el sistema de gestión de

inventario Insumo a nivel de lote y ubicación. Asimismo, desarrolló una aplicación que gestiona las operaciones en un almacén y se comunica en tiempo real con el *software* de inventario. Además, en el caso de los productos, se incorporaron etiquetas inteligentes. Este novedoso proyecto es un claro ejemplo de cómo la digitalización y la Industria 4.0 pueden contribuir a optimizar la trazabilidad, eficiencia y competitividad en la industria biotecnológica y farmacéutica cubana.

Materiales y métodos

Entre los materiales y métodos que se utilizaron en el desarrollo de este proyecto se encuentran:

- **Análisis documental:** permitió la consulta de fuentes de información pertinentes para identificar el estado de la investigación sobre el tema; las diversas propuestas epistemológicas y aplicadas en función del análisis crítico del basamento teórico-metodológico; la explicación e interpretación; y la comparación de los resultados durante todo el proceso de diseño e implantación. Además, se centró en la revisión y estudio del marco regulatorio y normativo a nivel internacional, nacional y sectorial, así como la elaboración de toda la documentación de los sistemas informáticos desarrollados.

- **Observación:** proporcionó información, incluyendo la extraverbal con enfoque no participante. El desarrollo del proyecto se ajusta al procedimiento de desarrollo de software de la División de Sistemas Informáticos de la Empresa de Tecnologías de la Información (DSI-P-F1-01), que define la secuencia de operaciones durante el ciclo de vida del proyecto.

La metodología que se utilizó para el desarrollo del sistema fue Scrum, un enfoque de gestión ágil que facilita la administración de proyectos, programas y portafolios de cualquier tamaño y complejidad. Lo anterior asegura el flujo de información, la comunicación entre el equipo de trabajo y la entrega de valor oportunamente a los interesados de la organización. Además, ofrece los productos de forma iterativa e incremental, maximizando las oportunidades de obtener retroalimentación.

Se utilizaron también las siguientes tecnologías y herramientas informáticas:

- Mule ESB: una herramienta utilizada para la integración entre aplicaciones mediante servicios web.
- Flutter: *framework* de código abierto de Google utilizado para crear aplicaciones multiplataforma compiladas a partir de una única base de código (Flutter-Crea aplicaciones para cualquier pantalla, Desarrolladores de Android, s. f.).
- Java: lenguaje de programación orientado a objetos y multiplataforma. Su principal característica es la portabilidad, es decir cualquier código desarrollado en Java puede ejecutarse en distintos sistemas operativos siempre que cuenten con la Máquina virtual de Java (JVM, por sus siglas en inglés) instalada (*Esflutter*, s. f.).
- Sql server 2016: sistema gestor de base de datos que permite almacenar y posteriormente acceder a los datos de forma rápida y estructurada (OpenWebinars, s. f.).
- Windows Server 2019: distribución de Microsoft para el uso de servidores. Se trata de un sistema multiproceso y multiusuario que es muy utilizado gracias a las características y ventajas que ofrece (Axarnet, s. f.).
- Linux (Debian 10): sistema operativo adecuado para un amplio rango de dispositivos como portátiles, ordenadores de escritorio y servidores (Debian, s. f.).
- Framework Net 7: marco de desarrollo de *software* para compilar y ejecutar aplicaciones en Windows (Dotnet, s. f.).
- Lenguaje C#: lenguaje de programación moderno, basado en objetos y con seguridad de tipos. Permite a los desarrolladores crear aplicaciones seguras y sólidas que se ejecutan en .net (Microsoft Learn, s. f.).
- Windows Presentation Foundation (WPF): API para crear interfaces de usuario (UI) para aplicaciones de escritorio con el *framework* .net (Programarfacil, s. f.).

Resultados y discusión

El proyecto de innovación sectorial desarrollado para la integración de tecnologías digitales en la gestión de inventarios de Biocubafarma

mostró resultados positivos que contribuyeron a la modernización del sistema logístico en la cadena de suministro biofarmacéutica cubana.

La introducción de etiquetas inteligentes permitió identificar de manera automática y en tiempo real los insumos almacenados, mejorando de forma significativa la trazabilidad de los productos desde la recepción hasta su salida del almacén. La capacidad de estas etiquetas para contener información específica sobre lote, ubicación y fechas de vencimiento facilitó el control riguroso y la reducción de errores humanos en la gestión de inventarios. Este proyecto se enmarcó en la mejora del proceso de gestión de inventarios de Insumos, mediante la introducción de tecnologías innovadoras y redes ópticas pasivas con tecnología Gigabit Passive Optical Network (GPON), para contribuir a la transformación digital de la industria biotecnológica y farmacéutica cubana. A continuación, se detalla la ejecución de cada uno de los resultados definidos.

1-) Resultado 1: Modificado el Sistema de Gestión de Inventarios Insumo a nivel de lote.

El resultado principal de este trabajo fue la reingeniería del sistema de gestión de inventarios (Mistral) para operar a nivel de lote, un avance fundamental para Biocubafarma donde la trazabilidad y el control de caducidad son imperativos de calidad y seguridad.

Funcionalidades modificadas e implementadas

Se modificaron las operaciones de entrada y salida de productos para incorporar el nivel «lote». Las operaciones afectadas incluyen:

- **Entrada:** informe de recepción e informe de reclamación.
- **Salida:** vale de entrega, solicitud y vale de devolución, vale de salida a Orden de Trabajo (OT), otras salidas, transferencias de salidas y traspasos entre áreas.

Adicionalmente, se desarrollaron nuevas funcionalidades para la gestión en el almacén para este nuevo nivel:

- **Reubicación de Lotes:** permite mover lotes específicos entre ubicaciones, optimizando el espacio y priorizando productos según su fecha de caducidad.
- **Impresión de Etiquetas:** se implementó la generación e impresión de etiquetas DataMatrix para productos y lotes, así como códigos

de barras para la identificación de ubicaciones. Esto constituye la base física para la trazabilidad.

2-) Resultado 2: Desarrollar una aplicación en sistema Android con funcionalidades que intervengan en el proceso de la gestión de inventario vinculada al Sistema de Gestión de Inventario Insumos

Para dotar a los operarios de una herramienta ágil y en tiempo real, se desarrolló una aplicación Android. Esta aplicación se comunica con el sistema Mistral y permite la captura inmediata de información mediante la lectura de las etiquetas DataMatrix y de códigos de barras.

La aplicación replica y permite ejecutar, de manera remota y guiada, todas las operaciones de almacén modificadas en el sistema central, garantizando la integridad de los datos desde el punto de operación. Las funcionalidades implementadas en la app incluyen: informe de recepción, vale de entrega, vale de devolución, vale de salida a OT, otras salidas, transferencias, traspasos entre áreas, reubicación de lotes y la gestión de las ubicaciones por productos o por entradas.

El conjunto de resultados presentados describe la digitalización de los procesos de negocio: logístico y la gestión de inventario. La introducción de la trazabilidad a nivel de lote y la captura de datos en tiempo real a través de dispositivos móviles no solo optimiza el espacio y prioriza productos, sino que es un imperativo de calidad y seguridad, particularmente crítico en un sector como el farmacéutico (Biocubafarma). La *app* Android actúa como un puente crucial entre el mundo físico (etiquetas DataMatrix) y el sistema central (Mistral), eliminando demoras y reduciendo errores.

De igual forma, es importante resaltar que dichos resultados se encuentran a la vanguardia de las tendencias tecnológicas y de gestión logística, alineándose con los principios de la Industria 4.0. La solución no es una mera digitalización, sino una integración profunda que emplea tecnologías contemporáneas clave:

- **Trazabilidad en tiempo real y a nivel de lote:** es el estándar de oro en industrias reguladas como la farmacéutica y alimentaria.
- **Arquitectura de sistemas integrada (Mistral + App Android + Mule ESB):** refleja el paradigma de los sistemas de sistemas, donde

diferentes componentes software se comunican de manera fluida para ofrecer una solución unificada.

- **Uso de tecnologías móviles (Android) e identificación automática (DataMatrix):** tecnologías accesibles y de alto impacto que modernizan la interacción humano-sistema en el piso de almacén.
- **Automatización de procesos logísticos:** la reingeniería de procesos como los trasposos y la reubicación automatizada sitúan a la organización en un nivel de madurez digital avanzado.

Magnitud y características del aporte alcanzado

El aporte de este proyecto es de alta magnitud a nivel nacional, con potencial de repercusión internacional en contextos similares.

- **Repercusión nacional:** para el grupo Biocubafarma, entidad estratégica en la industria biofarmacéutica de Cuba, este desarrollo representa una solución propia y soberana a un problema crítico de calidad y eficiencia. Su implementación exitosa puede convertirse en un caso de éxito para la industria biofarmacéutica cubana.

Conclusiones

El proyecto ejecutó con éxito un plan integral de transformación digital para la industria biofarmacéutica cubana, logrando una modernización tecnológica sinérgica en tres pilares fundamentales.

Se digitalizó el núcleo del proceso logístico mediante la reingeniería del sistema de gestión de inventarios (Mistral) para operar a nivel de lote y el desarrollo de una aplicación Android. Esto introduce una trazabilidad completa y en tiempo real de los insumos, un avance crítico para garantizar la calidad y seguridad en el sector, optimizando además el espacio y la gestión del almacén.

En conjunto, estos resultados crean un ecosistema tecnológico cohesionado donde una infraestructura de red moderna (GPON) habilitan aplicaciones móviles (app Android) que digitalizan procesos logísticos esenciales (inventario por lote). Esta integración sinérgica no solo moderniza componentes individuales, sino que establece una base sólida para la eficiencia operativa, la seguridad y la continua innovación en la organización.

Referencias bibliográficas

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

Colectivo de autores. (2019). Diseño de una metodología para la estandarización de los sistemas de codificación y clasificación de productos en empresas cubanas. *Redalyc*. <https://www.redalyc.org/jatsRepo/4096/409659500005/html/index.html>

Colectivo de autores. (s.f.). *La gestión de stock*. McGraw-Hill Educación. <https://www.mheducation.es/bcv/guide/capitulo/8448612124.pdf>

Colectivo de autores. (2019). *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>

SAP. (2023). <https://www.sap.com/latinamerica/insights/what-is-digital-transformation.html>

Schroeder, R. (1992). *Administración de operaciones* (3ra ed.). McGraw Hill Interamericana.

Transformación digital en las empresas: características y tecnología. (2023). Impacto TIC. <https://impactotic.co/micrositios-tic/sectorti/transformacion-digital-en-las-empresas-caracteristicas-y-tecnologia>.



Diagnóstico de Madurez en Seguridad Digital para servicios de consultoría

Digital Security Maturity Assessment for Consulting Services

M. Sc. Noel Emilio Rojas Martos ^{1*}, M. Sc. Liban de Armas Granado ²

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

Este estudio presentó un modelo metodológico de Diagnóstico de Madurez en Seguridad Digital, orientado a instituciones con estructuras organizativas diversas. El objetivo fue desarrollar una herramienta capaz de identificar brechas, priorizar acciones y alinear la seguridad digital con los objetivos institucionales y de la política para la transformación digital, la agenda digital cubana y la estrategia de inteligencia artificial. El enfoque combinó una matriz de evaluación modular, entrevistas estratégicas y una hoja de ruta personalizada. La propuesta se estructuró en nueve dimensiones: liderazgo digital, puesto de trabajo digital, tecnologías, información y comunicación, políticas y estrategias de seguridad digital, operaciones digitales, cultura y clima digital, migración a la nube, marcos legales y regulatorios, y habilidades digitales. Se aplicaron técnicas cualitativas y escalas ordinales para

^{1*} M. Sc. Ingeniero. Especialista Comercial, Departamento de Proyectos, Dirección de Consultoría. DCCH. noel.rojas@etecsa.cu

² M. Sc. Ingeniero. Jefe Departamento de Proyectos, Dirección de Consultoría. DCCH. liban.dearmas@etecsa.cu

construir perfiles de madurez contextualizados, activando procesos de reflexión interna y planificación estratégica. Los resultados que se obtengan con su aplicación pueden evidenciar patrones de vulnerabilidad, como la ausencia de políticas formales, baja cultura de reporte y dependencia de actores individuales. Al mismo tiempo, se identificaron oportunidades de mejora sostenibles, alcanzables sin requerimientos técnicos complejos. La hoja de ruta permitió visualizar acciones escalonadas, adaptables a cada contexto institucional. El modelo demostró capacidad no solo para diagnosticar, sino para habilitar procesos de transformación organizacional. Su aplicación puede favorecer el fortalecimiento institucional, la preparación para auditorías externas y la integración de la seguridad digital como componente estratégico. Se propone su incorporación como fase fundacional en procesos de mejora continua y transformación digital.

Palabras clave: Diagnóstico, dimensiones, modelo, transformación, seguridad

Abstract

This study presented a methodological model for assessing digital security maturity, aimed at institutions with diverse organizational structures. Its objective was to develop a tool capable of identifying gaps, prioritizing actions, and aligning digital security with institutional goals as well as with the Digital Transformation Policy, the Cuban Digital Agenda, and the Artificial Intelligence Strategy. The approach combined a modular evaluation matrix, strategic interviews, and a customized roadmap. The model was structured around nine dimensions: Digital Leadership, Digital Workstation, 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 build contextualized maturity profiles, activating internal reflection and strategic planning processes. Results obtained through its application may reveal vulnerability patterns such as the absence of formal policies, low reporting culture, and reliance on individual actors. At the same time, sustainable improvement opportunities were identified,

achievable without complex technical requirements. The roadmap enabled the visualization of phased actions, adaptable to each institutional context. The model proved capable not only of diagnosing but also of enabling organizational transformation processes. Its application may support institutional strengthening, preparation for external audits, and the integration of digital security as a strategic component. Its incorporation is proposed as a foundational phase in continuous improvement and digital transformation initiatives.

Keywords: *Diagnosis; dimensions, model, transformation, security*

Introducción

Este estudio propuesto tuvo como objetivo desarrollar un modelo metodológico de Diagnóstico de Madurez en Seguridad Digital orientado a instituciones con estructuras organizativas diversas, para facilitar la identificación de brechas, priorizar acciones, apoyar procesos de transformación digital segura, priorizar acciones de mejora en función del nivel de madurez institucional, facilitar la alineación con marcos regulatorios y estándares internacionales y alinear la seguridad digital con los objetivos institucionales, en consonancia con la política para la transformación digital, la agenda digital cubana y la estrategia nacional de inteligencia artificial.

La evolución de la seguridad digital a nivel internacional ha dado lugar a una serie de conceptos clave que trascienden la protección técnica de sistemas y datos, y que hoy constituyen pilares para la evaluación de la madurez institucional (Von Solms & Van Niekerk, 2013). Dentro de esos conceptos destacamos los más relevantes para el diseño y aplicación de modelos de diagnósticos:

1. Resiliencia cibernética: capacidad de una organización para anticipar, resistir, recuperarse y adaptarse ante incidentes cibernéticos. Aplicación en el modelo: Se incorpora mediante indicadores de continuidad operativa, gestión de crisis, aprendizaje organizacional y flexibilidad adaptativa.

2. Seguridad digital como capacidad nacional: La seguridad digital es una capacidad estratégica que involucra legislación, infraestructura, educación, cooperación y gobernanza. Marco de referencia: Global

Cybersecurity Index (UIT). Aplicación en el modelo: Permite mapear el alineamiento institucional con políticas nacionales, estrategias sectoriales y marcos regulatorios.

3. Enfoque sociotécnico: La seguridad digital es un fenómeno que combina tecnología, personas, procesos y cultura. Aplicación en el modelo: Justifica la inclusión de dimensiones como liderazgo, cultura organizacional, percepción del riesgo y comunicación interna.

4. Gobernanza multinivel: La seguridad digital requiere articulación entre actores locales, nacionales e internacionales, públicos y privados. Aplicación en el modelo: Se evalúa la participación institucional en redes colaborativas, la interoperabilidad normativa y la capacidad de coordinación interinstitucional.

5. Madurez digital y seguridad por diseño La seguridad debe estar integrada desde la fase de diseño de procesos, sistemas y políticas. Aplicación en el modelo: Se diagnostica si la seguridad está incorporada estructuralmente o si responde a una lógica reactiva.

La incorporación de estos conceptos permite que el modelo diagnóstico trascienda la auditoría técnica y se convierta en una herramienta estratégica para la transformación institucional. Al evaluar las nueve dimensiones que abarcan el diagnóstico objeto de estudio: Liderazgo Digital, Puesto de Trabajo Digital, Tecnologías, Información y Comunicación, Políticas y Estrategias de Seguridad Digital, Operaciones Digitales, Cultura y Clima Digital, Migración a la Nube, Marcos Legales y Regulatorios, y Habilidades Digitales, este se posiciona como un instrumento alineado con las mejores prácticas internacionales y adaptable a contextos nacionales. Las dimensiones se estructuraron con técnicas cualitativas y escalas ordinales para construir perfiles de madurez contextualizados, activando procesos de reflexión interna y planificación estratégica.

La investigación se fundamentó en aportes teóricos y metodológicos de autores como Von Solms y Van Niekerk, quienes ampliaron el concepto de seguridad digital más allá de lo técnico; Siponen y Pahnla, que abordaron la adherencia organizacional a políticas de seguridad, las normativas cubanas Decreto-Ley 78/2023 «Sobre la

seguridad y protección de la información clasificada y limitada»; Decreto 104/2024 «Reglamento de la seguridad y protección de la información clasificada y limitada»; Decreto 360/2019 «Sobre la seguridad de las TIC y la defensa del Ciberespacio Nacional»; Resolución 128/2019 «Reglamento de Seguridad de las TIC»; Resolución 105/2021 «Reglamento sobre el Modelo de Actuación Nacional para la Respuesta a Incidentes de Ciberseguridad» y los marcos internacionales como el NIST Cybersecurity Framework (National Institute of Standards and Technology [NIST], 2018); las ISO/IEC 27001 y 27002 y CIS Controls. El diagnóstico propuesto permite también habilitar procesos de transformación organizacional mediante una hoja de ruta escalonada, adaptable y orientada a la acción.

Materiales y métodos

El Diagnóstico de Madurez en Seguridad Digital ha sido desarrollado con el propósito de evaluar de forma estructurada el estado actual de las capacidades, políticas y prácticas institucionales vinculadas a la gestión segura de la información y los sistemas digitales. Su aplicación permite identificar fortalezas, brechas y oportunidades de mejora, contribuyendo a la toma de decisiones estratégicas orientadas a la resiliencia organizacional y al cumplimiento normativo.

En el artículo de investigación propone un Diagnóstico de Madurez en Seguridad Digital para los servicios consultivos enfocado a la transformación digital. Para ello, fue necesario realizar un acercamiento al marco teórico y al estado del arte de los conceptos y modelos principales asociados a la ciberseguridad, así como el análisis de las regulaciones, normativas y recomendaciones de publicaciones de la UIT, empresas de ciberseguridad, las normativas cubanas relacionadas con el tema de investigación, de las tendencias y buenas prácticas identificadas. La investigación se ha sustentado en fuentes bibliográficas de una amplia gama de actores (reguladores, operadores, consultores, académicos).

Mediante el diagnóstico se pretende facilitar la identificación y vulnerabilidades asociadas a la seguridad digital y otras capacidades intangibles de los sectores presupuestado, empresarial y de otros actores económicos interesados en el proceso de la transformación digital.

Brinda la posibilidad de diagnosticar el Nivel de Madurez en Seguridad Digital, de trazar una hoja de ruta estratégica para la mejora cualitativa y cuantitativa de su gestión y de incrementar sus resultados. El diagnóstico tiene implicaciones prácticas porque constituye uno de los pilares del proyecto de diseño e implementación de los servicios de consultoría en la Empresa de Telecomunicaciones de Cuba. S.A. (ETECSA), para hacer una contribución a la sociedad cubana, a partir de las buenas prácticas implementadas; y puede tener un impacto positivo en el proceso de transformación digital del país. El beneficio económico está estimado sobre la base del ahorro por sustitución de importaciones, por concepto de diseño propio de la empresa y el valor para la protección de la información, sin necesidad de servicios consultivos externos.

En el desarrollo de esta investigación se combinaron métodos teóricos y estadísticos-matemáticos. Desde el punto de vista teórico, se procedió con la búsqueda, identificación y revisión de la literatura relacionada con el tema para recopilar la información de interés. Se utilizó el análisis y síntesis de toda la información consultada en la literatura especializada, proveniente de estudiosos del tema, empresas de ciberseguridad, casas consultoras, y organismos internacionales, entre otros.

Se trabajó el enfoque en sistema para garantizar la integración, interrelación, interdependencia y sinergia de las dimensiones que tributan al diagnóstico en su conjunto. Se implementó el método de ascenso de lo abstracto a lo complejo elaborando un sistema de abstracciones conceptuales con cada una de las dimensiones, así como los planos de análisis que posibilitaron el estudio de lo general a lo particular para obtener una imagen integral del proceso. Mediante el método histórico-lógico se logró enmarcar el proceso que es objeto de estudio en la historia y evolución, desde que aparece la ciberseguridad como ciencia hasta la actualidad.

Fueron utilizados métodos empíricos como la consulta bibliográfica, mediante la cual se acumuló una amplia bibliografía relacionada con el objetivo propuesto, y se procedió con la selección, revisión crítica y resumen para arribar a conclusiones. La observación científica fue utilizada para estudiar la experiencia práctica de diferentes diagnósticos de

ciberseguridad y los resultados de su implementación, a través de lo cual fue posible elaborar la formulación del problema, la comprobación de la hipótesis y proyectar la repercusión social de la solución a partir de la generalización del diagnóstico.

La investigación permitió el desarrollo de un test (tipo lista de chequeo) específico como instrumento para medir el Nivel de Madurez en Seguridad Digital como herramienta para diagnosticar el estado actual de organismos, empresas y organizaciones.

Resultados y discusión

El Diagnóstico de Madurez en Seguridad Digital está fundamentado en las buenas prácticas sobre el Índice Mundial de Ciberseguridad (Global Cybersecurity Index (GCI) 2020. Geneva: ITU. publicado por la Unión Internacional de Telecomunicaciones (International Telecommunication Union [ITU], 2020); forma parte de la tecnología TETR4DIG (Modelo de Gestión enfocado a la Transformación Digital. De Armas Granado, L., Díaz Monjiotti,2022) (Figura 1); evalúa el compromiso de las organizaciones (organismos y empresas) en materia de Seguridad Digital de acuerdo con los cinco pilares de la Agenda sobre Ciberseguridad Global (medidas jurídicas, técnicas, organizativas, capacitación y cooperación [Center for Internet Security (CIS), 2021] y está en correspondencia con los ocho ejes estratégicos de la Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia de Inteligencia Artificial. Está elaborado en forma de *test* (encuesta tipo lista de chequeo) para cada una de las dimensiones.

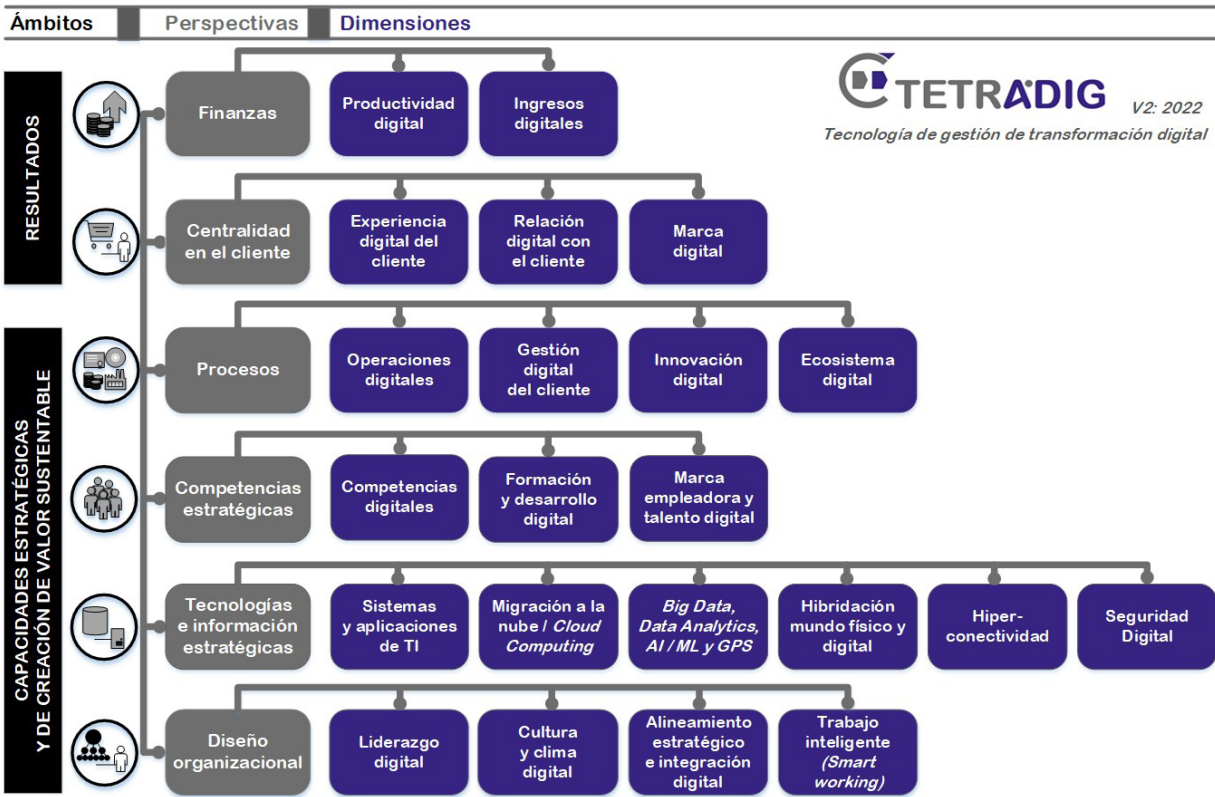


Figura 1. TETR4DIG: Modelo de gestión del cambio organizacional enfocado a la transformación digital (de Armas Granado, Liban; Díaz Monjiotti, Ela. 2022)

Sus objetivos son identificar fortalezas y debilidades en la infraestructura de la organización; identificar riesgos y vulnerabilidades; crear un plan de acción para mejorar la madurez en Seguridad Digital, incluyendo objetivos a corto, mediano y largo plazo, fomentar la conciencia y cultura de Seguridad Digital y preparar a la organización para el cumplimiento de las normas y políticas aprobadas a nivel de país.

Para la realización del diagnóstico se identificaron nueve dimensiones que forman parte del Modelo de Seguridad Digital (Figura 2) presentado durante los eventos «Ciberseguridad en las Telecomunicaciones» (ETECSA, 2023) y «XVI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información» (Palacio de las Convenciones 2024).



Figura 2. Modelo de Seguridad Digital basado en la tecnología TETR4DIG. (Rojas Martos, Noel E. 2024)

Estructura del modelo y definición de las dimensiones

A partir de la fundamentación del diagnóstico, de una revisión de las normativas cubanas y de los marcos internacionales y de la conceptualización de la tecnología TETR4DIG, se diseñó una herramienta evaluativa compuesta por nueve dimensiones estratégicas que permiten valorar el grado de avance, integración y sostenibilidad de la seguridad digital en entornos institucionales.

Estas dimensiones no se conciben como elementos aislados, sino como componentes interdependientes que configuran un ecosistema

digital seguro, resiliente y orientado al desarrollo. La representación gráfica del modelo (centrada en el concepto de Seguridad Digital como núcleo articulador) permite visualizar la relación sistémica entre liderazgo, políticas, tecnología, cultura, habilidades y marcos regulatorios.

Cada dimensión responde a criterios específicos de evaluación y se vincula directamente con los ejes estratégicos de la Política Cubana de Transformación Digital, lo que garantiza la pertinencia contextual del instrumento y su capacidad para orientar procesos de mejora continua, planificación estratégica y cumplimiento normativo. Cada una representa un componente estratégico que contribuye al fortalecimiento de la seguridad digital institucional y su evaluación permite identificar el nivel de madurez, integración y alineación con los ejes de la Política Cubana de *Transformación Digital*. A continuación, se describe el significado y alcance de cada dimensión evaluada en el *test*:

Liderazgo Digital: evalúa el compromiso de la alta dirección con la seguridad digital como eje transversal de la transformación institucional. Incluye la existencia de políticas claras, asignación de responsabilidades, y capacidad de decisión estratégica. Un liderazgo maduro impulsa la gobernanza digital y promueve una cultura organizacional orientada a la resiliencia.

Políticas y Estrategias de Seguridad Digital: analiza la presencia, actualización y aplicación de políticas institucionales relacionadas con la ciberseguridad, protección de datos y gestión de riesgos. Considera si estas políticas están alineadas con marcos normativos nacionales e internacionales, y si se integran en la planificación estratégica de la organización.

Puesto de Trabajo Digital: valora el grado de digitalización de los entornos laborales, incluyendo el uso de herramientas tecnológicas, automatización de procesos y acceso seguro a plataformas digitales. También contempla la capacitación del personal en el uso responsable y seguro de los recursos digitales.

Tecnologías de la Información y la Comunicación (TIC): examina la infraestructura tecnológica disponible, su nivel de interoperabilidad, conectividad, y capacidad para habilitar servicios digitales seguros.

Incluye la gestión de activos tecnológicos, la actualización de sistemas y la implementación de soluciones innovadoras.

Cultura y Clima Digital: mide el nivel de conciencia, participación y confianza de los actores institucionales en el entorno digital. Evalúa la existencia de campañas de sensibilización, prácticas inclusivas, y mecanismos para fomentar valores digitales como la responsabilidad, la ética y la colaboración.

Marcos Legales y Regulatorios: determina el grado de cumplimiento de la organización con las normativas vigentes en materia de protección de datos, identidad digital, ciberseguridad e inteligencia artificial. Incluye la existencia de mecanismos de auditoría, control legal y adaptación normativa.

Migración a la Nube: explora el uso de tecnologías emergentes, especialmente la computación en la nube, como estrategia para mejorar la eficiencia, escalabilidad y seguridad de los servicios digitales. Considera aspectos como la gestión de proveedores, la protección de datos en entornos virtuales y la continuidad operativa.

Operaciones Digitales: evalúa la transformación de procesos internos y servicios públicos mediante plataformas digitales, trámites en línea y ventanillas únicas. Mide la eficiencia operativa, la experiencia del usuario y la capacidad de respuesta institucional en entornos digitales.

Habilidades Digitales: analiza la formación, actualización y desarrollo de competencias digitales en el personal institucional. Incluye conocimientos en TIC, ciberseguridad, inteligencia artificial y gestión de datos, así como la existencia de programas de capacitación continua.

Los análisis obtenidos a través del *test* de Diagnóstico de Madurez en Seguridad Digital evidencian una estructura institucional que, si bien ha avanzado en la adopción de tecnologías y políticas digitales, aún enfrenta desafíos en la integración sistémica de la seguridad como eje transversal. La matriz analítica y el modelo dimensional permiten identificar fortalezas en áreas como infraestructura TIC y operaciones digitales, así como brechas en liderazgo estratégico, cultura organizacional y habilidades digitales.

La correspondencia entre las dimensiones evaluadas y los ejes estratégicos de la *Política Cubana de Transformación Digital* valida la pertinencia contextual del modelo, posicionándolo como una herramienta metodológica capaz de orientar procesos de mejora continua, planificación institucional y cumplimiento normativo. Además, al incorporar enfoques sociotécnicos y principios de gobernanza digital, el diagnóstico trasciende la auditoría técnica y se convierte en un instrumento de transformación organizacional. Este análisis no solo permite caracterizar el estado actual de la seguridad digital en las instituciones evaluadas, sino que también ofrece insumos concretos para la formulación de estrategias, la toma de decisiones y el fortalecimiento de capacidades, en función de una transformación digital segura, inclusiva y sostenible.

Articulación del modelo diagnóstico con la *Política Cubana de Transformación Digital*

Los resultados del Diagnóstico de Madurez en Seguridad Digital se organizaron en una matriz que vincula cada dimensión evaluada con los ejes estratégicos definidos en la *Política Cubana de Transformación Digital*. Esta articulación permite validar la pertinencia del modelo en el contexto nacional y evidenciar su capacidad para operacionalizar los principios rectores de la política pública. La matriz revela una correspondencia directa entre las dimensiones del modelo y los componentes estratégicos de la política, como se muestra a continuación (Tabla 1):

Tabla 1. Vinculación de las dimensiones con la Política para la Transformación Digital, la Agenda Digital Cubana y la Estrategia de Inteligencia Artificial y sus ocho ejes estratégicos.
Fuente: elaboración propia

Dimensión del Diagnóstico de Seguridad Digital	Vinculación con la Política Cubana	Ejes Estratégicos	Fundamentación
Liderazgo Digital	La política establece que el Estado lidera la transformación digital como “proceso transversal, estratégico y urgente” (p. 6), con un enfoque de gobernanza digital y participación multisectorial.	Marco Normativo, Gobierno Digital	El liderazgo impulsa la adopción de marcos legales, políticas públicas y gobernanza digital dentro de la organización.

Dimensión del Diagnóstico de Seguridad Digital	Vinculación con la Política Cubana	Ejes Estratégicos	Fundamentación
Puesto de Trabajo Digital	Se promueve la digitalización de procesos laborales, automatización y uso de herramientas digitales en sectores como salud, educación y administración pública (p. 12).	Economía Digital, Educación y Cultura Digital	Moderniza los entornos laborales, fomenta la productividad digital y promueve la alfabetización tecnológica del personal.
Tecnologías, Información y Comunicación (TIC)	Se prioriza el desarrollo de infraestructura digital, conectividad, interoperabilidad de sistemas y servicios digitales accesibles (p. 9).	Economía Digital, Gobierno Digital, Innovación	Las tecnologías habilitan servicios digitales, interoperabilidad, automatización y desarrollo de nuevos modelos de negocio.
Políticas y Estrategias de Seguridad Digital	Se reconoce la necesidad de una Estrategia Nacional de Ciberseguridad, protección de datos personales y resiliencia ante amenazas digitales (p. 10).	Ciberseguridad, Marco Normativo	Refuerza la protección de datos, la gestión de riesgos y el cumplimiento normativo en entornos digitales.
Operaciones Digitales	Se impulsa la transformación de servicios públicos, trámites en línea, plataformas de gobierno electrónico y ventanillas únicas digitales (p. 13).	Gobierno Digital, Economía Digital	Digitaliza procesos internos y servicios públicos, mejora la eficiencia y la experiencia del usuario.
Cultura y Clima Digital	Se promueve una cultura digital inclusiva, con énfasis en la alfabetización digital, participación ciudadana y confianza en el entorno digital (p. 11).	Educación y Cultura Digital, Contenidos Digitales	Promueve valores digitales, participación ciudadana y generación de contenidos digitales inclusivos.
Migración a la Nube	Se menciona la adopción de tecnologías emergentes como la computación en la nube para mejorar la eficiencia y seguridad de los servicios digitales (p. 14).	Innovación, Ciberseguridad	Facilita la escalabilidad, flexibilidad y seguridad de los servicios digitales mediante tecnologías emergentes.
Marcos Legales y Regulatorios	Se plantea la actualización del marco legal para regular la protección de datos, identidad digital, ciberseguridad e inteligencia artificial (p. 15).	Marco Normativo, Ciberseguridad	Asegura que la organización cumpla con leyes sobre protección de datos, identidad digital e IA.
Habilidades Digitales	Se prioriza la formación de talento digital, capacitación en IA, TIC y competencias digitales para todos los sectores (p. 16).	Educación y Cultura Digital, Innovación	Desarrolla capacidades en TIC, IA y ciberseguridad, alineadas con la formación continua y la innovación.

La correspondencia entre las dimensiones del modelo y los ejes estratégicos de la política cubana permite afirmar que el diagnóstico no solo evalúa el estado actual de la seguridad digital institucional, sino que también orienta su alineación con los objetivos nacionales. Esta validación contextual refuerza la utilidad del modelo como herramienta de planificación estratégica, mejora continua y rendición de cuentas.

Además, la matriz evidencia que la seguridad digital no se limita a aspectos técnicos, sino que abarca liderazgo, cultura, habilidades, normativas y procesos, en consonancia con los enfoques sociotécnicos y de gobernanza multinivel promovidos internacionalmente. En este sentido, el modelo contribuye a posicionar la seguridad digital como eje transversal de la transformación institucional.

Requisitos que mide el *test* por cada dimensión

Con el objetivo de operacionalizar el modelo de Diagnóstico de Madurez en Seguridad Digital, se diseñó un conjunto de 160 ítems distribuidos en las nueve dimensiones estratégicas. Cada ítem representa un requisito específico que permite evaluar el grado de cumplimiento, integración y sostenibilidad de prácticas, políticas y capacidades institucionales en materia de seguridad digital. Estos requisitos fueron formulados a partir de una revisión crítica de las normativas cubanas y de los marcos internacionales expuestos anteriormente, principios de gobernanza digital, y lineamientos de la *Política Cubana de Transformación Digital*. Asimismo, se incorporaron criterios sociotécnicos, organizacionales y normativos que permiten capturar la complejidad del entorno digital institucional.

La estructura del test responde a una lógica modular, donde cada dimensión agrupa requisitos que abarcan desde aspectos técnicos y normativos hasta factores culturales, operativos y estratégicos. Esta organización facilita la aplicación del instrumento en distintos tipos de instituciones, permite identificar brechas específicas y orienta la formulación de planes de mejora contextualizados. A continuación, se presentan los requisitos evaluados por cada dimensión, acompañados de una breve descripción que justifica su inclusión y relevancia diagnóstica (Tabla 2).

Tabla 2. Requisitos evaluados por cada dimensión, acompañados de una breve descripción que justifica su inclusión y relevancia diagnóstica. Fuente: elaboración propia

Nº	Dimensión	Objetivo de los Ítems	Criterios Evaluados (Resumen)	Ítems Evaluados
1	Liderazgo Digital	Identificar estructuras de liderazgo, asignación de responsabilidades y visión institucional.	Políticas aprobadas, responsables designados, planificación estratégica, cultura de seguridad, recursos asignados.	24
2	Políticas y Estrategias de Seguridad Digital	Verificar coherencia normativa, actualización y efectividad de las políticas.	Existencia, alineación legal, difusión, auditoría, protocolos de respuesta, participación institucional.	26
3	Puesto de Trabajo Digital	Determinar condiciones técnicas, uso seguro de tecnologías y capacitación del personal.	Herramientas digitales, protección de dispositivos, automatización, gestión de accesos, respaldo.	13
4	TIC (Tecnologías de la Información y la Comunicación)	Evaluar robustez, interoperabilidad y actualización de sistemas.	Infraestructura, interoperabilidad, monitoreo, escalabilidad, integración externa.	20
5	Cultura y Clima Digital	Identificar valores, prácticas y percepciones que favorecen la seguridad digital.	Sensibilización, percepción del riesgo, ética digital, participación, retroalimentación.	12
6	Marcos Legales y Regulatorios	Verificar alineación legal, auditoría y adaptación normativa.	Legislación vigente, estándares internacionales, auditoría, capacitación jurídica.	20
7	Migración a la Nube	Evaluar planificación, gestión de proveedores y protección de datos en la nube.	Estrategia de adopción, seguridad virtual, continuidad operativa, autenticación.	19
8	Operaciones Digitales	Determinar eficiencia operativa y experiencia del usuario.	Digitalización, automatización, interoperabilidad, monitoreo, retroalimentación ciudadana.	14
9	Habilidades Digitales	Identificar preparación técnica, programas formativos y alineación institucional.	Diagnóstico de competencias, formación continua, certificaciones, redes de aprendizaje.	21

La siguiente tabla tabla 3 sintetiza los principales componentes del test, donde cada dimensión agrupa un conjunto de ítems que permiten evaluar prácticas, capacidades y políticas institucionales vinculadas a la seguridad digital. Además del número de ítems evaluados, se incluyen recomendaciones clave que orientan la interpretación de los resultados y la formulación de acciones de mejora según el nivel de madurez identificado.

Tabla 3. Tabla resumen que sintetiza las nueve dimensiones del test de Diagnóstico de Madurez en Seguridad Digital, el número de ítems evaluados en cada una, y las recomendaciones clave según los resultados esperados. Fuente: elaboración propia

Nº	Dimensión	Ítems Evaluados	Recomendaciones según resultados esperados
1	Liderazgo Digital	24	Fortalecer el compromiso directivo, asignar responsables, integrar la seguridad en la planificación estratégica.
2	Políticas y Estrategias de Seguridad Digital	26	Formalizar y actualizar políticas, alinearlas con marcos normativos, garantizar su difusión y aplicación efectiva.
3	Puesto de Trabajo Digital	13	Digitalizar procesos laborales, proteger dispositivos, capacitar al personal en el uso seguro de tecnologías.
4	Tecnologías de la Información y la Comunicación (TIC)	20	Modernizar infraestructura, asegurar interoperabilidad, implementar mecanismos de monitoreo y actualización tecnológica.
5	Cultura y Clima Digital	12	Promover campañas de sensibilización, fomentar valores digitales, medir percepción y participación institucional.
6	Marcos Legales y Regulatorios	20	Asegurar cumplimiento normativo, capacitar en legislación vigente, participar en procesos regulatorios.
7	Migración a la Nube	19	Diseñar estrategias de adopción, seleccionar proveedores seguros, proteger datos y garantizar continuidad operativa.
8	Operaciones Digitales	14	Automatizar trámites, mejorar experiencia del usuario, integrar plataformas y evaluar desempeño operativo.
9	Habilidades Digitales	21	Implementar programas de formación continua, diagnosticar competencias, incentivar el desarrollo profesional.

Aplicación e Interpretación del Test

El *test* de Diagnóstico de Madurez en Seguridad Digital se puede aplicar mediante una combinación de entrevistas semiestructuradas, revisión documental y observación directa, adaptado a las características organizativas de cada institución evaluada. Los 160 ítems distribuidos en las nueve dimensiones permiten una evaluación modular, flexible y contextualizada, facilitando la identificación de fortalezas, brechas y oportunidades de mejora.

Cada ítem se valora en una escala ordinal que refleja el grado de cumplimiento institucional, permitiendo clasificar los resultados en cuatro niveles de madurez, utilizando como referencia el sistema de evaluación que propone la tecnología TETR4DIG:

Básico: procesos de seguridad digital sin documentar, en cambio constante, dispuestos especialmente para un fin de forma reactiva.

Inicial: procesos de seguridad digital que siempre se ejecutan igual, con resultados constantes. Iniciada la implementación de medidas de seguridad digital en algunas áreas de la entidad.

Estratégico (procesos de seguridad digital de integración estratégica. Implementando hoja de ruta de seguridad digital de forma holística e integrada, con orientación centrada en los recursos de la empresa y los clientes, procesos estandarizados, definidos y documentados que sufren algún tipo de revisión en el tiempo).

Innovador-disruptivo: procesos de seguridad digital para la protección de los datos y la información al nivel del estado del arte, liderazgo digitales, mejora continua de la eficacia de los procesos mediante cambios e innovación tecnológica, procesos ágiles, innovadores, flexibles, conectados, colaborativos, abiertos, con uso de datos relevantes con protección en más de un soporte tecnológico. Se adaptan de forma continua a los cambios.

Esta clasificación permite construir perfiles de madurez por dimensión, identificar patrones comunes entre instituciones, y orientar la formulación de planes de mejora específicos. Además, facilita la comparación longitudinal y la evaluación del impacto de intervenciones estratégicas en seguridad digital.

Conclusiones

El presente artículo ha propuesto y validado un modelo de Diagnóstico de Madurez en Seguridad Digital diseñado específicamente para servicios de consultoría institucional. A partir de un enfoque sociotécnico e interdisciplinario, el modelo permite evaluar el grado de integración, sostenibilidad y alineación estratégica de la seguridad digital en organizaciones públicas y privadas, en consonancia con los ejes de la *Política Cubana de Transformación Digital* y los marcos internacionales de referencia (ISO/IEC 27001, NIST, UIT).

La estructura modular del diagnóstico (compuesta por nueve dimensiones estratégicas y 160 ítems evaluativos) facilita una caracterización integral del entorno digital institucional, abarcando desde el liderazgo y la cultura organizacional hasta la infraestructura tecnológica, las políticas normativas y las habilidades del personal. Esta amplitud permite identificar brechas específicas, orientar planes de mejora y fortalecer capacidades organizativas en función de una transformación digital segura, inclusiva y resiliente.

Los resultados obtenidos evidencian que la seguridad digital no puede abordarse como un componente técnico aislado, sino como un proceso transversal que exige liderazgo comprometido, gobernanza efectiva, formación continua y articulación normativa. En este sentido, el modelo se posiciona como una herramienta metodológica útil para consultores, gestores y responsables institucionales que buscan integrar la seguridad digital en sus procesos de planificación, evaluación y toma de decisiones.

Su aplicación no sustituye los servicios de Ciberseguridad que hoy están en la cartera de servicios de la Dirección de Consultoría, sino que puede identificar debilidades y oportunidades para que estos puedan ser contratados por quienes realicen el diagnóstico.

Finalmente, se destaca el potencial del diagnóstico como instrumento de monitoreo longitudinal, adaptable a distintos contextos sectoriales y escalable en función de los avances tecnológicos y regulatorios. Su aplicación sistemática puede contribuir al fortalecimiento de la cultura de seguridad, la mejora de la calidad institucional y el cumplimiento de los objetivos estratégicos de transformación digital en Cuba y otros entornos similares.

Bibliografía

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* (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.
13. 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., & Pahlila, 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.

La Revolución de la IA en las Telecomunicaciones: Un Viaje del Pasado al Futuro

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

Rafael Alberto Noa Yanes ^{1*}, Ing. Ivette García Montero ²

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

Este artículo, derivado del seminario investigativo desarrollado en el marco del intercambio científico entre el Instituto Preuniversitario Vocacional de Ciencias Exactas Vladimir Ilich Lenin y ETECSA, analiza el impacto transformador de la inteligencia artificial (IA) en el sector de las telecomunicaciones. Mediante una revisión documental y un estudio de casos múltiples, se identificaron cuatro desafíos estructurales de la era pre-IA: la gestión manual del tráfico exponencial de datos, la saturación de los servicios de atención al cliente, el mantenimiento reactivo de la infraestructura y la ciberseguridad basada en firmas estáticas. Se presentan soluciones habilitadas por la IA, como redes autooptimizables, chatbots y asistentes virtuales, mantenimiento predictivo y sistemas de detección de anomalías en tiempo real, documentadas con casos de éxito de Google, Telefónica, Nokia, IBM, Movistar y Vodafone, entre otros. La discusión compara el modelo reactivo previo con el modelo proactivo y autónomo actual, evidenciando reducciones cuantificables. Se concluye que la IA ha pasado de ser una promesa futurista a un

^{1*} Instituto Preuniversitario Vocacional de Ciencias Exactas Vladimir Ilich Lenin

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

factor determinante de competitividad, y se recomienda su adopción estratégica, así como la inversión en investigación, desarrollo y alianzas academia-industria para preparar el talento joven hacia el futuro de las telecomunicaciones.

Palabras clave: Inteligencia artificial, telecomunicaciones, mantenimiento predictivo, ciberseguridad, automatización de redes.

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 centers, reactive infrastructure maintenance, and 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 cases 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 a futuristic promise to a decisive competitiveness factor, and strategic adoption 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.

Introducción

Las telecomunicaciones han recorrido un largo camino desde los primeros sistemas de comunicación a distancia: señales de humo, tambores, el telégrafo hidráulico del siglo IV a. C. y el telégrafo óptico, considerado el primer sistema moderno. En el siglo XIX, la telegrafía

eléctrica y, posteriormente, la telefonía sentaron las bases de la industria actual, con hitos como el primer cable trasatlántico (1858) y la fundación de compañías emblemáticas como la Electric Telegraph Company (1846) y AT&T (1885). La figura 1 sintetiza visualmente estos momentos clave y su conexión con la llegada de la Inteligencia Artificial (IA). Hoy, sin embargo, el desafío ya no es solo vencer la distancia física, sino gestionar el torrente de datos que circula por las redes.

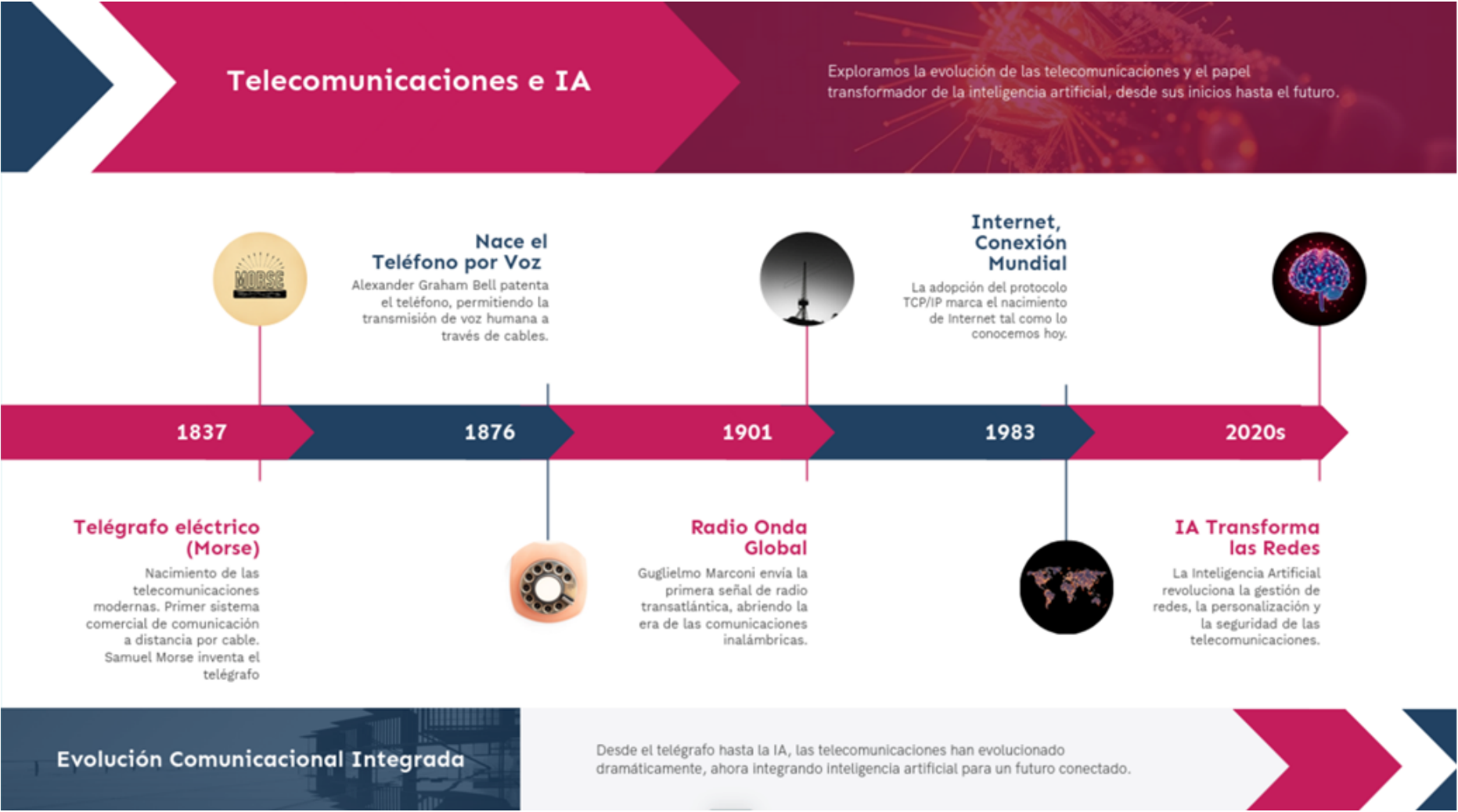


Figura 1. TETR4DIG: Modelo de gestión del cambio organizacional enfocado a la transformación digital (de Armas Granado, Liban; Díaz Monjiotti, Ela. 2022)

El presente artículo tiene como objetivo analizar el impacto transformador de la Inteligencia Artificial (IA) en el sector de las telecomunicaciones, identificando los principales problemas que enfrentaba la industria antes de su implementación y mostrando cómo la IA ha permitido superarlos. El trabajo se enmarca en el intercambio científico entre el Instituto Preuniversitario Vocacional de Ciencias Exactas Vladimir Ilich Lenin y ETECSA, con el propósito de fomentar la innovación colaborativa y preparar al talento joven para los retos del futuro digital.

La literatura especializada y los informes de empresas líderes (Cisco, Google, Telefónica, Nokia, IBM) han documentado avances significativos en áreas como la auto-optimización de redes, la atención al cliente mediante asistentes virtuales, el mantenimiento predictivo y la ciberseguridad proactiva. Sin embargo, este artículo no

solo recopila dichos aportes, sino que los organiza en un marco analítico que permite comprender la evolución desde un modelo reactivo hacia uno autónomo e inteligente. La novedad radica en la sistematización de estos casos de estudio y en su aplicación al contexto de operadores como ETECSA, donde la colaboración con instituciones educativas impulsa la transferencia de conocimiento y la adopción de tecnologías avanzadas.

Materiales y métodos

La investigación se desarrolló mediante un enfoque cualitativo, basado en la revisión y análisis documental de fuentes especializadas. Se empleó una metodología de estudio de casos múltiples, seleccionando empresas representativas del sector de las telecomunicaciones que han implementado soluciones de IA con resultados documentados públicamente.

Fuentes de información:

- Informes técnicos y comunicados de prensa de empresas líderes: Cisco, Google, AT&T, Telefónica, Nokia, Ericsson, Movistar, Vodafone, Orange y Verizon.
- Publicaciones de organismos internacionales e instituciones académicas, incluyendo IBM, el Laboratorio de Periodismo Luca de Tena y la Asociación Española de Ingenieros de Telecomunicación.
- Artículos especializados en revistas del sector y plataformas tecnológicas (Metaverso, Minsait, Aunoa).
- Materiales de referencia general (Google Cloud) para establecer definiciones y contexto histórico.

Procedimiento:

- **Identificación de desafíos pre-IA:** Se analizaron los problemas recurrentes documentados en la literatura previa a la adopción masiva de IA, clasificándolos en cuatro categorías: gestión del tráfico de datos, atención al cliente, mantenimiento de infraestructura y ciberseguridad.
- **Selección de casos de éxito:** Se eligieron empresas con implementaciones maduras de IA en cada una de las cuatro áreas, priorizando aquellas que reportaron métricas cuantitativas (reducción

de interrupciones, porcentaje de consultas automatizadas, disminución de falsas alarmas, etc.).

- **Análisis comparativo:** Se contrastaron las situaciones “antes” y “después” de la IA para cada desafío, extrayendo los elementos que evidencian una mejora sustancial.
- **Contextualización:** Se integraron los hallazgos en el marco del intercambio científico entre el IPVCE Vladimir Ilich Lenin y ETECSA, destacando cómo la colaboración academia-industria puede acelerar la adopción de estas tecnologías.

Resultados y discusión

Los cuatro desafíos de la era pre-IA: una radiografía de las limitaciones estructurales

El análisis documental realizado permitió identificar cuatro problemas recurrentes que caracterizaban la operación de las redes de telecomunicaciones antes de la incorporación masiva de inteligencia artificial. Estos desafíos no actuaban de forma aislada, sino que se retroalimentaban entre sí: la gestión manual del tráfico agravaba los cuellos de botella, los fallos imprevistos saturaban los centros de atención al cliente, y la seguridad reactiva dejaba ventanas de exposición que se ampliaban con el crecimiento exponencial de los datos. Comprender esta interrelación es clave para valorar el impacto transformador que la IA ha tenido al abordarlos de manera integral.

1. Crecimiento exponencial de datos y gestión manual de redes

El surgimiento de los teléfonos móviles e Internet provocó un aumento sin precedentes en la demanda de datos. Cada segundo, la demanda es mayor; el tráfico crece de manera progresiva y coloca una presión insostenible sobre infraestructuras no diseñadas para tal volumen. En regiones donde no se utiliza IA, los operadores supervisan el rendimiento de la red manualmente, emplean sistemas de automatización básicos para la configuración de dispositivos y realizan un análisis de datos limitado. Esto conduce a los denominados «cuellos de botella», que interrumpen la producción y degradan la experiencia del usuario. Un caso emblemático es Verizon, que experimentó este problema en su servicio de Atención al Cliente durante los picos

de demanda, resultando en tiempos de espera prolongados y una experiencia menos satisfactoria.

2. Saturación del servicio de atención al cliente

La inconformidad de los clientes por los cuellos de botella se canaliza hacia los centros de llamadas, que reciben a cada instante solicitudes, quejas y dudas. La demanda de este servicio también crece exponencialmente, pero la atención depende totalmente de la experiencia y conocimiento del operador humano, lo que exige una capacitación continua y genera largos tiempos de espera. El informe de IBM citado en la literatura señala que, antes de la adopción de chatbots, más del 60 % de las llamadas correspondían a consultas rutinarias, consumiendo una porción significativa de los recursos operativos.

3. Mantenimiento reactivo y demora en la respuesta a fallos

En la era pre-IA, los problemas de infraestructura solo se detectaban a través de informes de usuarios o mediante un monitoreo manual. Esto significaba que los técnicos intervenían después de recibir quejas o notar una disminución en el rendimiento. Un ejemplo paradigmático es AT&T, que entre 2007 y 2010 enfrentó graves congestiones en su red tras el lanzamiento del iPhone por Apple. La infraestructura no estaba preparada para manejar el aumento repentino del tráfico, y la ausencia de capacidades predictivas provocó interrupciones recurrentes durante eventos de alta demanda.

4. Ciberseguridad estática y detección limitada de amenazas

Las empresas de telecomunicaciones desarrollaban sus sistemas de protección basados en firewalls estáticos y bases de datos de firmas. Estos sistemas comparan el tráfico de red con patrones conocidos de actividad maliciosa, pero solo identifican ataques previamente registrados y requieren una actualización manual constante. Con el crecimiento progresivo del tráfico, el monitoreo se vuelve insostenible, generando “falsos positivos” (alarmas innecesarias) y “falsos negativos” (amenazas pasadas por alto). Esta metodología resultaba especialmente vulnerable ante ataques de día cero, como los vividos durante la ola de *ransomware* WannaCry en 2017, donde varias empresas con sistemas basados exclusivamente en firmas sufrieron infecciones.

A continuación en la figura 2 se presentan los cuatro desafíos sistematizados, acompañados de ejemplos concretos documentados:



Figura 2. Los cuatro grandes desafíos de las telecomunicaciones antes de la IA

Estos resultados evidencian que el modelo tradicional operaba de manera reactiva, con intervención humana como cuello de botella y con limitaciones estructurales para adaptarse al crecimiento vertiginoso de la demanda.

Soluciones habilitadas por la IA

Frente a un panorama dominado por la intervención humana, los sistemas rígidos y la incapacidad de anticiparse a los problemas, la inteligencia artificial ha irrumpido como un habilitador tecnológico que transforma radicalmente la operación de las telecomunicaciones. Las soluciones basadas en IA no se limitan a automatizar tareas repetitivas; introducen capacidades de aprendizaje, adaptación en tiempo real y toma de decisiones autónoma. A continuación se exponen los principales resultados documentados en la literatura y en los informes de empresas pioneras, organizados según los cuatro desafíos previamente identificados (Tabla 1).

Tabla 1. Soluciones habilitadas por la inteligencia artificial para cada desafío del sector telecomunicaciones

Desafío	Solución con IA	Casos de éxito y métricas documentadas
Gestión del tráfico	Redes que se auto-optimizan en tiempo real mediante análisis de grandes volúmenes de datos. La IA permite ajustar parámetros de forma dinámica, redistribuir ancho de banda y anticipar congestiones.	Google implementó el sistema B4 en sus Redes Definidas por Software (SDN), optimizando el uso de ancho de banda entre centros de datos globales. Cisco ha desarrollado redes autónomas que se autoconfiguran, se autoprotegen y se autoreparan, reduciendo drásticamente la necesidad de intervención humana. Huawei integró IA en sus redes 5G logrando eficiencia energética.
Atención al cliente	Chatbots y asistentes virtuales con procesamiento de lenguaje natural, disponibles 24/7, capaces de gestionar consultas repetitivas y ofrecer respuestas personalizadas basadas en el historial del usuario.	Según un informe de IBM, las empresas que emplean chatbots pueden manejar hasta el 80% de las consultas de rutina, lo que representa ahorros significativos en costos operativos. Movistar desarrolló Aura, un asistente virtual que permite gestionar servicios, consultas de facturación y recomendaciones personalizadas. Vodafone utiliza TOBi, Orange cuenta con Djingo y Verizon dispone de su propio chatbot para soporte técnico y asistencia en facturación.

Desafío	Solución con IA	Casos de éxito y métricas documentadas
Mantenimiento	Mantenimiento predictivo basado en sensores conectados a la infraestructura y algoritmos de Machine Learning que procesan grandes volúmenes de datos para identificar patrones, anomalías y desviaciones sutiles que indican un posible fallo futuro.	Telefónica implementó un proyecto de Mantenimiento Predictivo de Red que redujo en un 30% las interrupciones no planificadas . Nokia , con su plataforma Nokia Predictive Care , logró un 50% menos de falsas alarmas y una mejor disponibilidad de red. Ericsson provee la plataforma Ericsson Operations Engine , utilizada por operadores como Telia Company en Suecia, consiguiendo una reducción del 25% en las interrupciones del servicio .
Ciberseguridad	Sistemas de detección de anomalías en tiempo real, basados en aprendizaje automático, que analizan comportamientos en lugar de solo firmas conocidas. Permiten respuestas automáticas (aislamiento de sistemas comprometidos, bloqueo de IPs maliciosas, aplicación de parches) y se adaptan continuamente a nuevas tácticas de los ciberdelincuentes.	Los beneficios documentados incluyen detección rápida , reducción del tiempo de exposición a vulnerabilidades; disminución de falsos positivos y falsos negativos ; y capacidad de predicción de amenazas basada en patrones históricos y análisis de comportamientos. Todo ello se traduce en una mayor seguridad, comodidad y confianza para los clientes.

Discusión: el antes y el después, una transformación estructural

La comparación entre los escenarios pre-IA y post-IA revela una transformación que va más allá de una simple mejora incremental. Se trata de un cambio de paradigma en la forma de operar las telecomunicaciones, que afecta a la arquitectura de las redes, a la relación con los clientes y a la capacidad de respuesta ante contingencias.

Esta comparación evidencia que la IA no solo resuelve los problemas existentes, sino que redefine la naturaleza de la operación. Se pasa de un modelo reactivo, donde la tecnología actuaba como un soporte pasivo a la intervención humana, a un modelo proactivo y autónomo, donde la IA es un componente central que anticipa, decide y ejecuta. La novedad no reside únicamente en las tecnologías individuales (chatbots, SDN, sensores), sino en su integración en plataformas de gestión unificada que permiten un bucle cerrado de automatización: la red detecta una condición anómala, la IA toma una decisión y ejecuta la corrección sin intervención humana.

Además, los casos analizados demuestran que esta transformación es escalable y cuantificable. Las reducciones porcentuales documentadas (30 % en interrupciones, 50 % en falsas alarmas, 80 % en consultas rutinarias) no son anecdóticas; reflejan mejoras sostenidas que impactan directamente en la satisfacción del usuario, la eficiencia operativa y la rentabilidad. Empresas como Telefónica, Nokia y Ericsson han convertido estas capacidades en ofertas de servicio que ya son utilizadas por operadores de múltiples países, validando la madurez de la tecnología.

En conjunto, la evidencia recopilada confirma que la IA ha pasado de ser una promesa futurista a un factor determinante de competitividad en el sector de las telecomunicaciones. Su adopción no implica solo incorporar nuevas herramientas, sino reimaginar los procesos y la cultura operativa para aprovechar al máximo las capacidades de anticipación, automatización y aprendizaje continuo (Figura 3).



Figure 3. Impacto transformador de la IA en las telecomunicaciones: del modelo reactivo al proactivo/autónomo

Conclusiones

El presente trabajo ha permitido alcanzar varios objetivos fundamentales: el primero, identificar y caracterizar los cuatro desafíos fundamentales que enfrentaban las telecomunicaciones antes de la adopción de la IA: gestión manual del tráfico exponencial, saturación de la atención al cliente, mantenimiento reactivo y ciberseguridad estática. El segundo, demostrar, mediante casos de éxito documentados (Google, Telefónica, Nokia, IBM, etc.) que la IA ofrece soluciones efectivas, con reducciones cuantificables en interrupciones, falsas alarmas y costos operativos, así como mejoras sustanciales en la experiencia. El tercero, evidenciar el paso de un modelo reactivo a uno proactivo y autónomo, donde la inteligencia artificial permite anticipar problemas, automatizar respuestas y liberar al talento humano para tareas de mayor valor estratégico.

Más allá de recopilar información, este artículo sistematiza los hallazgos en un marco analítico que puede servir de referencia para operadores que aún se encuentran en etapas iniciales de adopción de IA. Asimismo, destaca la importancia de las alianzas entre operadores e instituciones educativas para formar a las nuevas generaciones en tecnologías emergentes, como las que aquí se describen.

Se sugiere profundizar en el estudio de la IA aplicada a redes 5G y 6G, al Internet de las Cosas (IoT) y a la hiperautomatización de centros de operaciones de red. También se recomienda explorar los retos éticos y de gobernanza asociados al uso intensivo de IA, así como desarrollar indicadores específicos para medir el retorno de inversión (ROI) en implementaciones de IA en entornos como el cubano, donde ETECSA puede actuar como catalizador de la transformación digital.

Bibliografía

- Asociación Española de Ingenieros de Telecomunicación. (s.f.). *Foro Histórico de las Telecomunicaciones*. Recuperado de <https://www.aeit.es/soyteleco/grupos-de-trabajo/foro-historico-de-las-telecomunicaciones>
- Aunoa. (s.f.). *Desafíos y Soluciones en el uso de Chatbots en Telecomunicaciones*. Recuperado de <https://aunoa.ai/blog/desafios-y-soluciones-en-el-uso-de-chatbots-en-telecomunicaciones>
- Google Cloud. (s.f.). *¿Qué es una Inteligencia Artificial o IA?* Recuperado de <https://cloud.google.com/learn/what-is-artificial-intelligence?hl=es-419>
- International Business Machines Corporation (IBM). (s.f.). *Chatbots*. Recuperado de <https://www.ibm.com/think/topics/chatbots>
- Laboratorio de Periodismo Luca de Tena. (s.f.). *Cinco lecciones sobre la evolución de los medios en 40 años: de la maqueta en papel a la Inteligencia Artificial*. Recuperado de <https://laboratoriodeperiodismo.org/cinco-lecciones-sobre-la-evolucion-de-los-medios-en-40-anos-de-la-maqueta-en-papel-a-la-inteligencia-artificial>
- Metaverso. (s.f.). *La Revolución de la IA en la Gestión del Tráfico de Red: Soluciones, Casos de Uso y Retos Éticos*. Recuperado de <https://metaverso.pro/blog/la-revolucion-de-la-ia-en-la-gestion-del-trafico-de-red-soluciones-casos-de-uso-y-retos-eticos>

Metaverso. (s.f.). *La Revolución de la IA en el Mantenimiento Predictivo de Infraestructuras de Telecomunicaciones*. Recuperado de <https://metaverso.pro/blog/la-revolucion-de-la-ia-en-el-mantenimiento-predictivo-de-infraestructuras-de-telecomunicaciones>

Minsait. (s.f.). *IA Aplicada a las Telecomunicaciones*. Recuperado de <https://www.minsait.com/es/insights/ia-aplicada-las-redes-de-telecomunicaciones>

Telefónica. (s.f.). *Programa de investigación sobre IA en Telecomunicaciones*. Recuperado de <https://www.telefonica.com/es/sala-comunicacion/blog/programa-investigacion-ia-industria-telecomunicaciones>



Sistema informático para la evaluación de impacto de las Tecnologías de la Información en las organizaciones

Computer system for evaluating the impact of Information Technologies in organizations

Ing. Ernesto Elias Elzaurdín Valdés ^{1*}, Ts. Meliza Leon Bencomo ²,
M. Sc. Mary Nelsa Bonne Cuza ³

Recibido: 01/2026 | Aceptado: 03/2026 | Publicado: 07/2026

Resumen

La transformación digital ha sido fundamental para lograr el éxito en las organizaciones, pero va más allá de implementar solamente la tecnología. Es por ello que se hace necesario un cambio cultural y organizacional. El impacto de las Tecnologías de la Información se mide según su alineación con los objetivos del negocio y su valor para las organizaciones. En Cuba precisamente, la dependencia tecnológica de los proveedores dificulta la renovación de las infraestructuras de tecnologías de la información, por lo que la evaluación del impacto es crucial. Esta

^{1*} Universidad de las Ciencias Informáticas, Cuba, Carretera San Antonio de los Baños km 2 ½ La Lisa, ernestoeev@uci.cu

² Universidad de las Ciencias Informáticas, Cuba, Carretera San Antonio de los Baños km 2 ½ La Lisa, mleonb@uci.cu

³ Universidad de las Ciencias Informáticas, Cuba, Carretera San Antonio de los Baños km 2 ½ La Lisa, mary@uci.cu

investigación busca desarrollar un sistema informático para reducir la complejidad en el proceso la evaluación del impacto de las tecnologías de la información en las organizaciones. Para ello, se hizo uso de la metodología ágil de desarrollo de *software* Extreme Programming, del marco de trabajo Django, del lenguaje de programación Python en el backend, HTML5, CCS3 y JavaScript para frontend. Esta solución debe ayudar a los especialistas de TI, trabajadores y directivos a enfrentar múltiples riesgos a la seguridad de la información y a proteger los activos más importantes para su organización.

Palabras clave: gestión de riesgos, medición de impacto, sistema informático, tecnologías de la información

Abstract

Digital transformation has been fundamental to achieving success in organizations, but it goes beyond just implementing technology, which is why a cultural and organizational change is necessary. The impact of Information Technologies is measured according to its alignment with business objectives and its value for organizations. In Cuba precisely, technological dependence on suppliers makes it difficult to renew information technology infrastructure, which is why impact assessment is crucial. This research seeks to develop a computer system to reduce the complexity in the process of evaluating the impact of information technologies on organizations. For this, the agile software development methodology Extreme Programming, the Django framework, the Python programming language in the back-end, HTML5, CCS3 and Java Script for the front-end were used. This solution should help IT specialists, workers and managers address multiple information security risks and protect the most important assets for their organization.

Keywords: risk management, impact measurement, computer system, information technologies

Introducción

Desde hace unos años las organizaciones apuestan por la transformación digital pues son evidentes las ventajas que aporta al negocio. Es importante destacar que esta pretende obtener beneficios en cuanto

al manejo de la información, los procesos, los recursos e incluso la reducción de errores humanos. Sin embargo, no se trata de implementar nuevas tecnologías, sino de lograr un cambio cultural y organizacional que garantice el éxito en las organizaciones (Liendo Afonso, 2023). Es evidente que, una vez realizadas las inversiones en infraestructura tecnológica, se debe garantizar la seguridad de estas, ya que hoy en día están muy presentes las amenazas cibernéticas que representan una vulnerabilidad para las organizaciones. Es por ello que se hace necesario centrar esfuerzos en implementar medidas de seguridad adecuadas para reducir los niveles de riesgos a los que se expone la información (Martínez Landrove, 2019).

El crecimiento de las infraestructuras de Tecnologías de la Información (TI) trae consigo un auge de las investigaciones sobre el impacto que representan para las organizaciones (Casanova, Calderón, 2020). Los resultados de varias investigaciones identificaron que, en la medida que sea mayor la alineación entre las TI y los objetivos del negocio, más amplio es el valor añadido que representan las infraestructuras TI para una organización (Pérez Lorences, 2014). El impacto se mide de acuerdo a la misión de la entidad, por lo que es vital comprender todos los activos de TI.

Cada activo tiene un valor y muchos son componentes clave para respaldar los servicios críticos que se brindan a los usuarios. Estos, además, influyen directamente en el capital y la valoración de la organización, así como los riesgos de TI pueden tener un impacto directo en el presupuesto. Para cada organización es vital y desafiante determinar las condiciones que realmente impactan a la misión; es muy importante analizar y comprender continuamente los recursos que cumplan con los objetivos y que pueden verse comprometidos por los riesgos de ciberseguridad (Quinn *et al.*, 2022). Un estudio exploratorio realizado por Casanova (2020) describe el estado de la gestión de las infraestructuras de TI en Cuba. Dicho estudio arrojó que en las organizaciones las mayores medias de impacto «se corresponden con la lentitud en la respuesta a las necesidades de la organización, lo cual implica un serio problema de alineamiento» (Casanova, 2020).

Además, destaca que «los problemas de implementar nuevos sistemas, debido a que implica un incremento de la complejidad de la gestión» (Casanova, 2020). Las organizaciones cubanas dependen tecnológicamente de sus proveedores, lo que dificulta la renovación periódica y pertinente de las infraestructuras TI.

De ahí que surge una conciencia sobre la importancia de la evaluación del impacto sobre la infraestructura. Cuba, por su condición de ser un país en desarrollo, no produce tecnología y, por tanto, debe importarla. Esto último representa un desafío debido al embargo económico, de ahí que la evaluación del impacto reviste una importancia especial (Casanova, Calderón, 2020). Para ello, existen marcos de referencia que describen de manera general cómo medir el impacto de la seguridad de la información; estos son muy genéricos, por lo que deben ser adaptados a los objetivos de las organizaciones y no existen herramientas que ayuden a documentar este análisis. Por lo anterior, la presente investigación se centra en la búsqueda de la reducción de la complejidad en la evaluación de impacto de las TI en las organizaciones a través del desarrollo de un sistema informático. El estudio se basa en el proceso de evaluación de impacto de TI en las organizaciones en el campo de acción de los sistemas informáticos que llevan a cabo esa gestión.

Materiales y métodos

El diseño teórico de la investigación se elaboró a partir de un análisis de los principales términos y definiciones relacionados con la evaluación de impacto. Asimismo, se realizó un estudio del estado de la cuestión en el que se tuvieron en cuenta los sistemas homólogos. Se seleccionó como metodología Extreme Programing (XP) por las características del proceso de desarrollo de software. Se optó desarrollar la aplicación con el lenguaje de programación Python v3.9.2 para backend y HTML5; CCS3 y JavaScript para frontend, marco de trabajo Django v4.1.3 y el gestor de base de datos PostgreSQL v11.0.2.

Los métodos teóricos utilizados fueron:

- 1. Analítico-sintético:** para el procesamiento de la información referente la evaluación de impacto en las organizaciones y arribar a las conclusiones de la investigación.

- 2. **Inductivo-deductivo:** para la elaboración del marco teórico de la investigación.
- 3. **Sistémico-estructural-funcional:** para la elaboración de la estrategia metodológica para el diseño e implementación del sistema informático de evaluación de impacto.

Como método empírico se utilizó la entrevista en función de conocer acerca de la evaluación de impacto en las organizaciones por parte del cliente y esclareció el estado actual del proceso de evaluación de impacto de TI en Cuba. La investigación se basa en el concepto de «impacto en los sistemas de gestión de seguridad de la información» de la ISO 27001. Se estudiaron y se tuvieron en cuenta para el desarrollo de la aplicación las buenas prácticas para la gestión de riesgos y la medición de impacto definidas por NIST (Marco de ciberseguridad del Instituto Nacional de Estándares y Tecnologías de Estados Unidos), la serie ISO 27000, por COBIT (Objetivos de Control de la Información y Tecnologías Afines) y por la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).

Resultados y discusión

Para medir el impacto de las TI en las organizaciones primero se debe realizar una valoración de los activos de TI de acuerdo con su criticidad y su importancia para la organización. Para ello, se debe tener en cuenta el valor de reemplazo del activo o las consecuencias para el negocio por la pérdida o compromiso de esos activos. Luego, se identifican las amenazas y se estima la probabilidad de ocurrencia (riesgo) (Figura 1). Esta información se puede obtener de los propietarios o los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones, de especialistas en seguridad de la información y de otras fuentes pertinentes. Los actores que interviene en el proceso de evaluación de impacto de TI dentro de las organizaciones son los especialistas de TI, los directivos y los trabajadores del negocio.



Figura 1. Descripción del proceso de medición de impacto

Para llevar a cabo el diseño e implementación del sistema informático destinado a la evaluación de impacto de las TI en las organizaciones se propone aplicación web que estará integrada en la Intranet corporativa. Esta herramienta permite realizar un inventario de activos de tecnología de la información y, posteriormente, estimar la importancia que posee cada activo para la organización a través del procesamiento de un grupo de criterios introducidos por el usuario. Además, contará con un inventario de amenazas que puedan afectar a los activos de la organización. Tendrá una funcionalidad para estimar el riesgo que corre cada activo dentro de la organización calculando el riesgo total que corre cada activo. Tendrá una función para estimar el impacto para la empresa la posibilidad de que los activos se vean afectados por las amenazas a las que está expuestos. Por último, los trabajadores de la organización tendrán la posibilidad de acceder al sistema para valorar su nivel de satisfacción con los activos de la empresa (Figura 2).

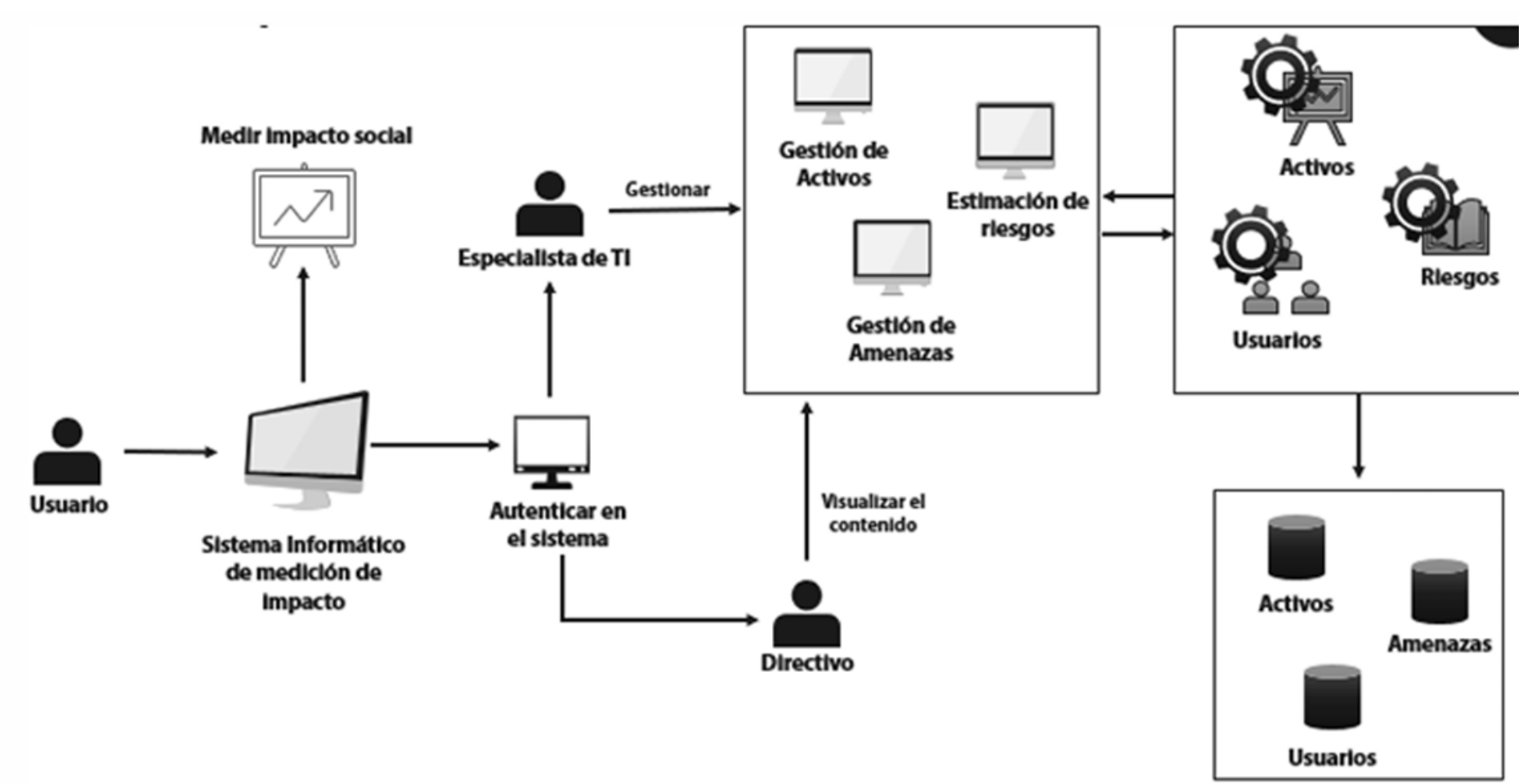


Figure 2. Descripción de la propuesta de solución

Se definen catorce requisitos funcionales, catorce historias de usuario y tres tarjetas CRC (Clase, Responsabilidad y Colaboración) que describen cómo autenticar usuarios en el sistema, gestionar activos, gestionar amenazas, calcular importancia, estimar riesgos, valorar servicios y medir impacto social. En la figura 3 se muestra como parte de la planificación del proceso de desarrollo la cantidad de iteraciones en

las que se divide el proyecto. Se definen, además, requisitos no funcionales de apariencia, *software*, *hardware*, seguridad, portabilidad, rendimiento, usabilidad y mantenibilidad.

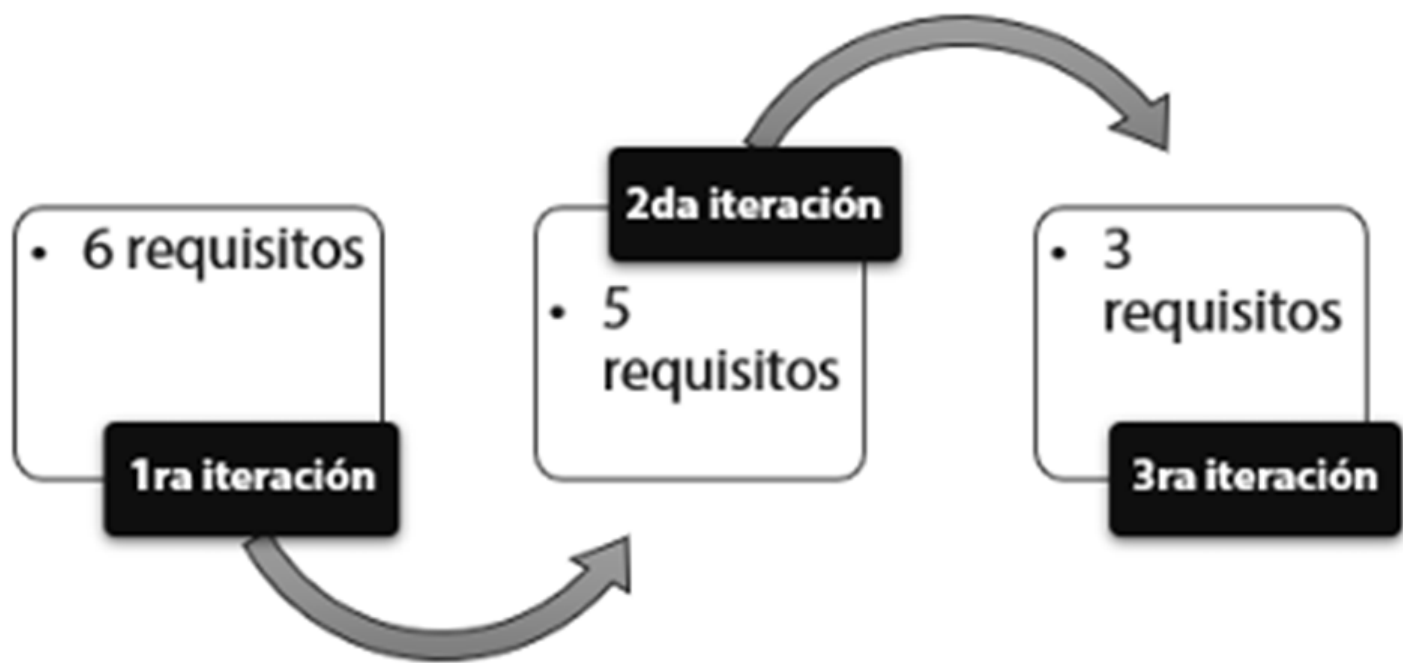


Figure 3. Planificación del proceso de desarrollo

El desarrollo del sistema se sustenta sobre el patrón arquitectónico Modelo-Vista-Controlador (MVC). En el caso del *framework* Django, este lo redefine como Modelo-Vista-Template: la vista actúa como controlador y los templates como las vistas. En cuanto al diseño, se emplearon los patrones GRASP siguientes: Experto, Creador, Bajo Acoplamiento, Controlador y Alta Cohesión. Estos describen los principios fundamentales del diseño de objetos y la asignación de responsabilidades, expresados en forma de patrones. Como modelo de datos se propusieron las entidades Activo, Usuario y Amenaza. La relación establecida entre los activos y las amenazas es de muchos a muchos, lo que da lugar a una entidad adicional que permite determinar la probabilidad de ocurrencia de ciertas amenazas sobre un activo (riesgo) (Figura 4).

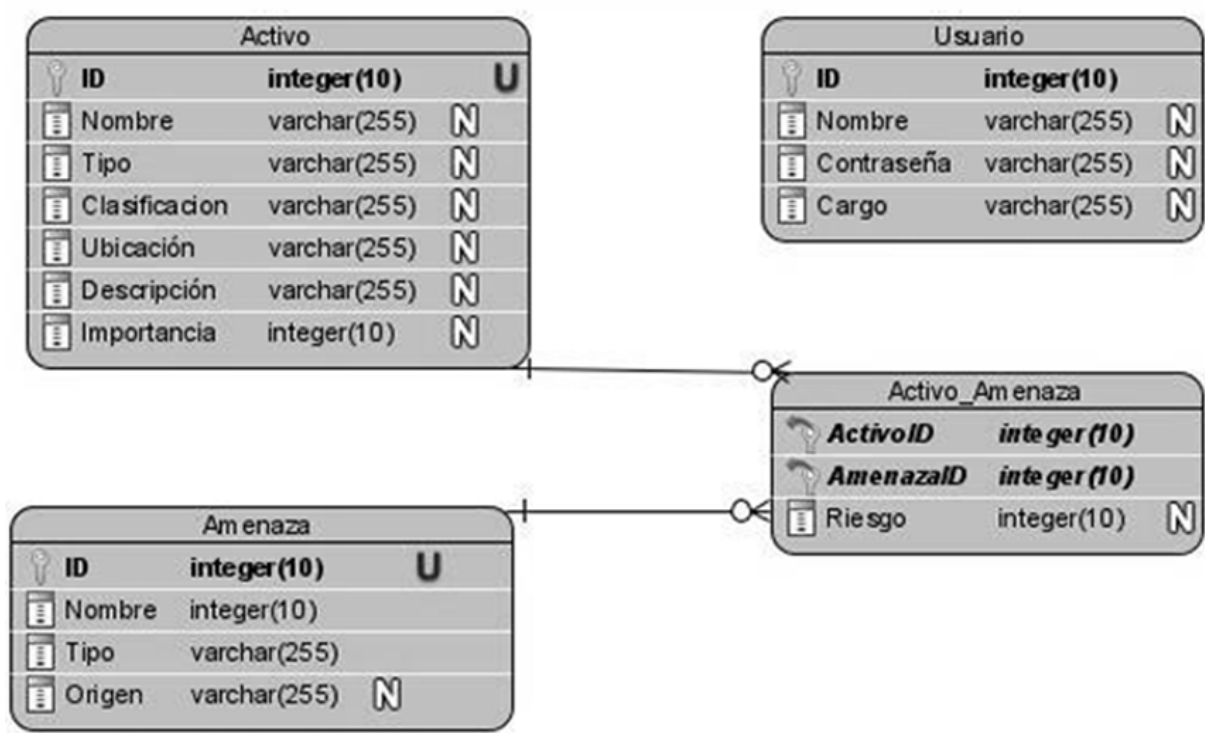


Figure 4. Modelo de datos de la propuesta de solución

Al ser una aplicación web se sustenta sobre la arquitectura cliente-servidor. Esta requiere de un servidor dedicado a alojar la información gestionada por el sistema. El cliente debe acceder a través de un navegador. Se propone como servidor web Apache y la conexión se debe establecer mediante el protocolo HTTPS por el puerto 443. El protocolo de transporte que se requiere para asegurar la entrega fiable y segura de la información TCP. En la figura 5 se representan los componentes y especificaciones necesarias para el despliegue de la solución.

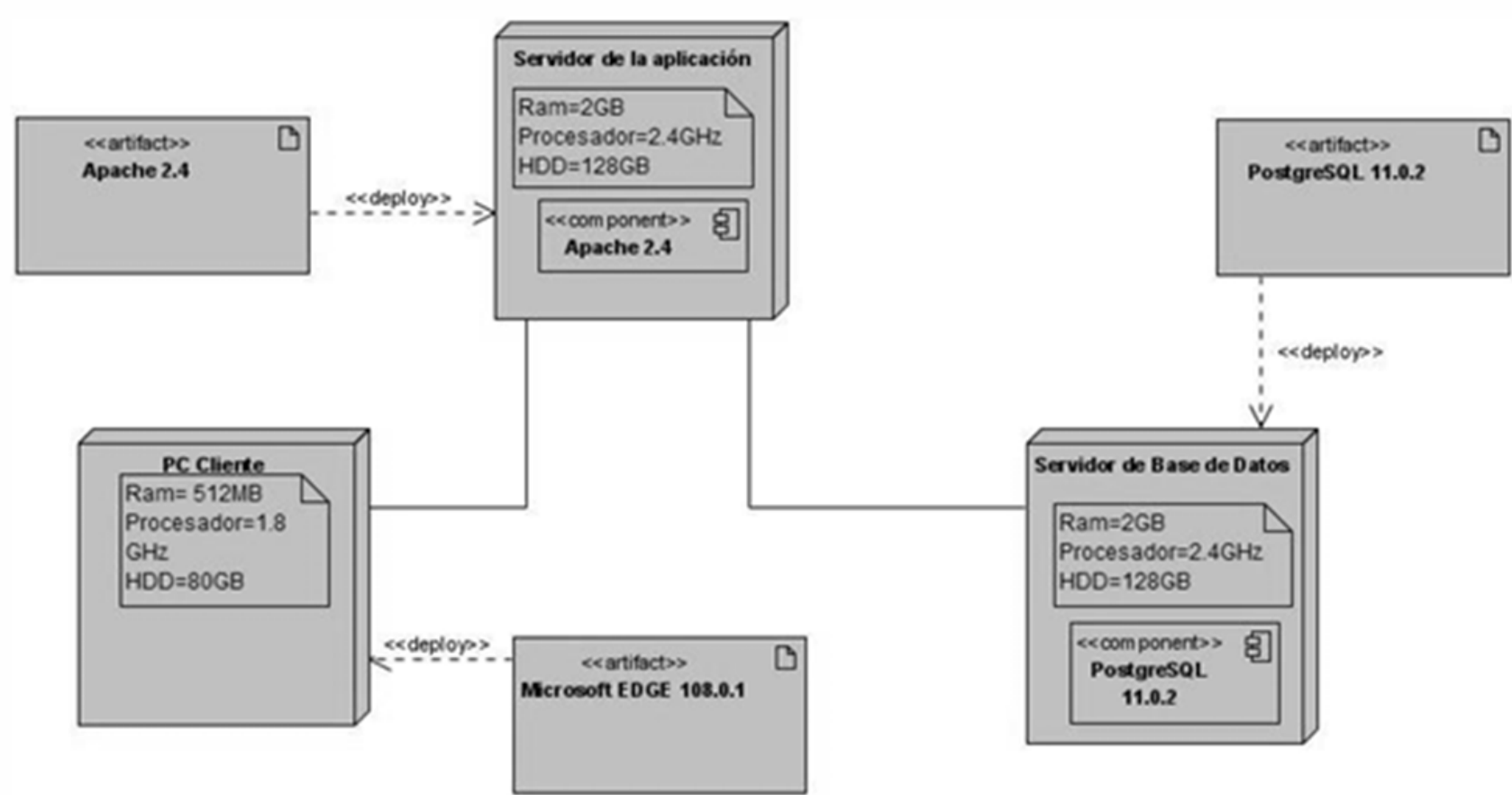


Figure 5. Propuesta de despliegue de la solución

Conclusiones

Una vez realizada la investigación y desarrollado el sistema informático para la evaluación de impacto de las TI en las organizaciones, se puede concluir que: la sistematización de los fundamentos teórico-metodológicos para la medición de impacto de TI en las organizaciones ayudó a esclarecer el proceso y así implementar una solución más acorde con los estándares de gestión de riesgo y medición de impacto; la planificación y diseño del sistema permitió organizar el proceso de desarrollo y tener una guía para la implementación de los requisitos; y se implementó un sistema informático que debe ayudar a los especialistas de TI, trabajadores y directivos de las organizaciones a reducir la complejidad en el proceso de gestión de riesgos y medición de impacto.

Referencias bibliográficas

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>

