Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2026,
Volumen 10, Número 2.

https://doi.org/10.37811/cl_rcm.v10i2

ARQUITECTURAS DE SEGURIDAD Y PREVENCIÓN DE ATAQUES EN REDES

SECURITY ARCHITECTURES AND ATTACK PREVENTION IN ENTERPRISE NETWORKS

MSc. Jonathan De Oleo Ramos
Universidad Latinoamericana y del Caribe, Venezuela

DOI: https://doi.org/10.37811/cl_rcm.v10i2.23614

Arquitecturas de seguridad y prevención de ataques en redes

Maria Teodolinda Ortega Ovalle[1]
maria.ortegao@up.ac.pa
https://orcid.org/0009-0000-3629-9751
Universidad de Panamá
Panamá

RESUMEN

El presente trabajo tiene como objetivo analizar las arquitecturas de seguridad aplicadas en redes empresariales y las estrategias de prevención de ataques más relevantes en el contexto actual de digitalización. Para ello, se empleó una metodología de revisión documental y análisis comparativo de modelos de seguridad, considerando tanto enfoques tradicionales como propuestas emergentes, tales como la defensa en profundidad y el modelo Zero Trust. Los hallazgos evidencian que las amenazas en redes corporativas son cada vez más sofisticadas, incluyendo ataques de ingeniería social, ransomware y explotación de vulnerabilidades, lo que exige un enfoque integral que combine tecnología, políticas organizacionales y capacitación de usuarios. Asimismo, se identificó que las pequeñas y medianas empresas enfrentan mayores dificultades para implementar estándares internacionales de seguridad, lo que genera brechas significativas en la protección de datos. Se concluye que la seguridad en redes empresariales debe concebirse como un proceso dinámico y multidimensional, en el que la prevención de ataques requiere la articulación de infraestructura tecnológica avanzada, gestión estratégica de la información y formación continua de los usuarios. Este enfoque integral permite fortalecer la resiliencia digital y garantizar la confianza en los entornos corporativos.

***Palabras Clave*:** Arquitecturas de seguridad; Redes empresariales; Prevención de ataques; Ciberseguridad; Zero Trust; Defensa en profundidad

[1] Autor principal
Correspondencia: maria.ortegao@up.ac.pa

Security Architectures and Attack Prevention in Enterprise Networks

ABSTRACT

This study aims to analyze the security architectures applied in enterprise networks and the most relevant attack prevention strategies in the current context of digitalization. A documentary review and comparative analysis of security models were conducted, considering both traditional approaches and emerging proposals such as defense in depth and the Zero Trust model. The findings reveal that threats in corporate networks are increasingly sophisticated, including social engineering attacks, ransomware, and vulnerability exploitation, which demand a comprehensive approach that integrates technology, organizational policies, and user training. Moreover, it was identified that small and medium-sized enterprises face greater challenges in implementing international security standards, which generates significant gaps in data protection. The results highlight that enterprise network security must be conceived as a dynamic and multidimensional process, where attack prevention requires the articulation of advanced technological infrastructure, strategic information management, and continuous user education. This holistic approach strengthens digital resilience and ensures trust in corporate environments, positioning cybersecurity not only as a technical necessity but also as a strategic factor for organizational sustainability and competitiveness.

Keywords: Security architectures; Enterprise networks; Attack prevention; Cybersecurity; Zero Trust; Defense in depth

Artículo recibido 20 marzo 2026
Aceptado para publicación: 15 abril 2026

INTRODUCCIÓN

La seguridad en redes empresariales se ha consolidado como un eje estratégico en la era digital, donde la información constituye uno de los activos más valiosos de las organizaciones. El tema central de este artículo es el estudio de las arquitecturas de seguridad y las estrategias de prevención de ataques en entornos corporativos, considerando tanto los modelos tradicionales como las propuestas emergentes que buscan responder a la creciente sofisticación de las amenazas cibernéticas.

El problema de investigación radica en la brecha entre la necesidad de contar con sistemas de seguridad robustos y la capacidad real de las empresas para implementarlos de manera efectiva. A pesar de la existencia de marcos normativos y tecnologías avanzadas, muchas organizaciones en especial las pequeñas y medianas carecen de recursos suficientes para garantizar una protección integral. Este vacío evidencia la urgencia de analizar cómo las arquitecturas de seguridad pueden adaptarse a distintos contextos y cuáles son las estrategias más eficaces para prevenir ataques.

La relevancia del estudio se fundamenta en que la seguridad digital es hoy un factor crítico para la sostenibilidad y competitividad empresarial. Un ataque exitoso puede comprometer datos sensibles, interrumpir operaciones críticas y afectar la confianza de clientes y socios. Por ello, la ciberseguridad no debe entenderse únicamente como un requisito técnico, sino como un componente estratégico que impacta en la continuidad del negocio y en la estabilidad del ecosistema digital global.

El marco teórico de este trabajo se apoya en la Arquitectura de Seguridad Empresarial (ESA), entendida como un marco integral que combina políticas, procedimientos y tecnología para proteger los activos de información y alinear las medidas de seguridad con los objetivos comerciales y la gestión de riesgos . Asimismo, se retoman los postulados de la defensa en profundidad y del modelo Zero Trust, que plantean la necesidad de múltiples capas de protección y la verificación constante de accesos, respectivamente. Estas teorías se complementan con categorías de análisis como gestión de identidades, segmentación de redes y capacitación de usuarios.

En cuanto a los antecedentes investigativos, estudios recientes destacan que la seguridad de redes empresariales requiere un enfoque integral que combine herramientas tecnológicas, políticas organizacionales y prácticas de monitoreo continuo, especialmente en el contexto del trabajo remoto y la creciente dependencia de servicios en la nube . Otros análisis subrayan que la forma en que se diseña

la arquitectura de red condiciona directamente su seguridad, ya que una infraestructura mal estructurada obliga a compensar con controles reactivos y excepciones que aumentan la vulnerabilidad. Este artículo busca aportar a dichos antecedentes una visión integradora que articule tecnología, gestión organizacional y formación de usuarios como pilares de la seguridad empresarial.

El contexto actual está marcado por la expansión del teletrabajo, la proliferación de dispositivos IoT y la creciente dependencia de servicios en la nube. Estos factores han transformado la naturaleza de las redes empresariales, ampliando la superficie de ataque y generando nuevos retos para las arquitecturas de seguridad. Además, el marco legal internacional exige mayor transparencia y responsabilidad en la gestión de datos, lo que incrementa la presión sobre las organizaciones para adoptar medidas efectivas de protección.

Finalmente, el objetivo general de este trabajo es analizar las arquitecturas de seguridad y las estrategias de prevención de ataques en redes empresariales, identificando sus fortalezas, debilidades y perspectivas futuras. Se busca demostrar que la seguridad digital debe concebirse como un proceso dinámico y multidimensional, en el que la prevención de ataques requiere la articulación de infraestructura tecnológica avanzada, políticas organizacionales claras y formación continua de los usuarios.

METODOLOGÍA

El presente estudio se desarrolló bajo un enfoque mixto, combinando elementos cualitativos y cuantitativos. El componente cualitativo permitió comprender en profundidad las arquitecturas de seguridad y las estrategias de prevención de ataques en redes empresariales, mientras que el componente cuantitativo se apoyó en estadísticas y reportes de ciberseguridad para contextualizar los hallazgos.

El tipo de investigación fue exploratorio y descriptivo. Exploratorio porque se indagó en modelos emergentes como Zero Trust y defensa en profundidad; descriptivo porque se detallaron las características de las arquitecturas de seguridad y los principales tipos de ataques que enfrentan las organizaciones.

El diseño de investigación fue no experimental y transversal, ya que se trabajó con información disponible en un momento específico, sin manipular variables, y se realizó un análisis comparativo de fuentes documentales y estudios previos.

La población de estudio estuvo conformada por literatura académica, informes técnicos de empresas de ciberseguridad y normativas internacionales. La muestra se delimitó a documentos publicados entre 2018 y 2025, seleccionados mediante un muestreo intencional.

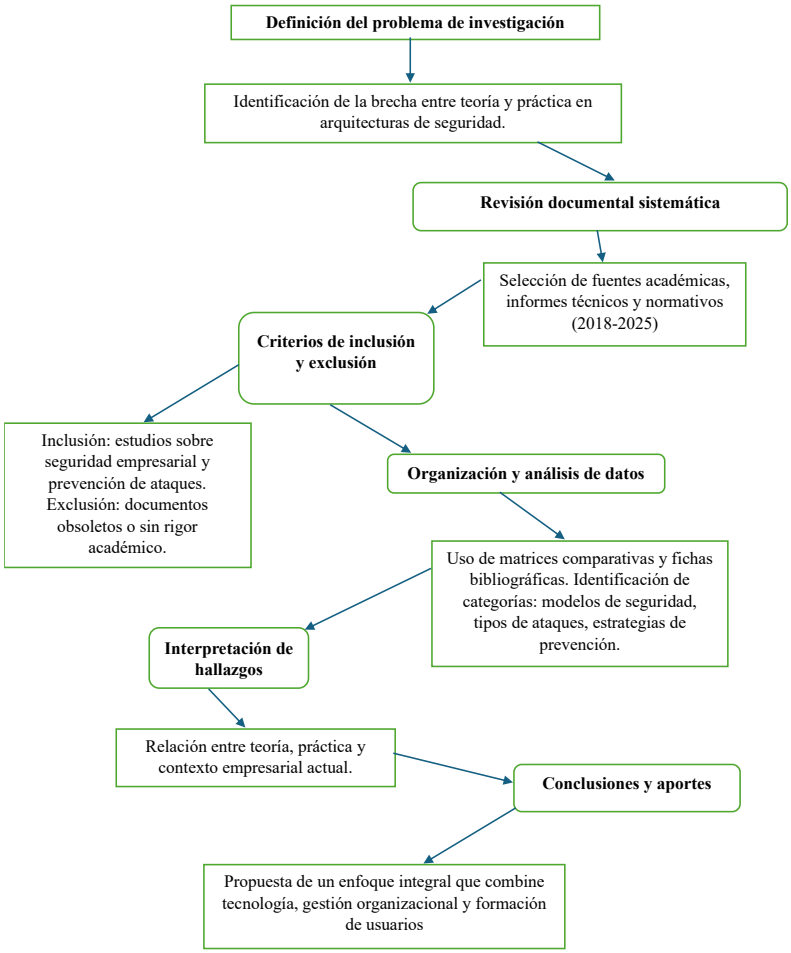
Las técnicas de recolección de datos incluyeron la revisión documental sistemática, apoyada en matrices de análisis comparativo y fichas de registro bibliográfico. Estas herramientas facilitaron la organización de la información y la identificación de categorías clave como: modelos de seguridad, tipos de ataques, estrategias de prevención y limitaciones en la implementación.

En cuanto a las consideraciones éticas, se respetaron los principios de integridad académica, citando todas las fuentes conforme al sistema APA (7ª edición). No se trabajó con datos sensibles ni confidenciales, lo que asegura la transparencia y replicabilidad del estudio.

Los criterios de inclusión se centraron en estudios y documentos que abordaran directamente la seguridad en redes empresariales, arquitecturas de protección y estrategias de prevención de ataques. Los criterios de exclusión descartaron publicaciones sin rigor académico, documentos obsoletos anteriores a 2018 y fuentes que no aportaran evidencia verificable.

Las limitaciones del estudio se relacionan con la dependencia de fuentes secundarias y la ausencia de trabajo de campo en organizaciones específicas, lo que restringe la validación empírica de algunos hallazgos. Sin embargo, esta limitación se compensa con la amplitud de la revisión documental y la diversidad de fuentes analizadas.

Figura 1. Diagrama de flujo metodológico



Marco Teórico

El estudio de las arquitecturas de seguridad en redes empresariales se sustenta en diversos enfoques teóricos y modelos que buscan garantizar la protección de los activos digitales. La seguridad informática, entendida como el conjunto de medidas destinadas a preservar la confidencialidad, integridad y disponibilidad de la información, se ha convertido en un campo interdisciplinario que combina principios de la ingeniería de sistemas, la gestión organizacional y la teoría del riesgo.

Principios fundamentales de la seguridad de la información

La tríada CIA (Confidencialidad, Integridad y Disponibilidad) constituye el marco conceptual básico de la seguridad digital. Estos principios orientan el diseño de arquitecturas de seguridad y permiten evaluar la eficacia de las medidas implementadas. La confidencialidad asegura que la información solo sea

accesible por usuarios autorizados; la integridad garantiza que los datos no sean alterados sin autorización; y la disponibilidad busca que los sistemas estén operativos cuando se requieran.

2. Teoría de la defensa en profundidad

La defensa en profundidad es uno de los enfoques más consolidados en la literatura de ciberseguridad. Este modelo plantea que la protección debe estructurarse en múltiples capas, de modo que si una medida falla, otras puedan contener el ataque. En redes empresariales, estas capas incluyen firewalls, sistemas de detección de intrusos, segmentación de redes, autenticación multifactor y monitoreo continuo. La teoría se fundamenta en la idea de redundancia y resiliencia, asegurando que la seguridad no dependa de un único punto de control.

Modelo Zero Trust

El modelo **Zero Trust** surge como respuesta a la creciente movilidad de los usuarios y la adopción de servicios en la nube. Su premisa central es “nunca confiar, siempre verificar”, lo que implica que cada acceso, interno o externo, debe ser autenticado y autorizado. Este enfoque rompe con la lógica tradicional de seguridad perimetral y se basa en la gestión estricta de identidades, el control granular de accesos y la supervisión constante de la actividad en la red.

Arquitectura de Seguridad Empresarial (ESA)

La Enterprise Security Architecture (ESA) propone un marco integral que combina políticas, procedimientos y tecnología para proteger los activos de información. Este modelo enfatiza la alineación entre las medidas de seguridad y los objetivos estratégicos de la organización, integrando la gestión de riesgos como un componente esencial. La ESA permite que la seguridad deje de ser un área aislada y se convierta en un factor transversal en la planificación empresarial.

Estudios previos y aportes relevantes

Diversos estudios han señalado que la efectividad de las arquitecturas de seguridad depende tanto de la tecnología como de la cultura organizacional. Investigaciones recientes destacan que la capacitación de usuarios es un factor crítico para reducir ataques de phishing y robo de credenciales, mientras que otros trabajos subrayan la necesidad de adoptar marcos normativos internacionales como ISO/IEC 27001 y NIST para estandarizar las prácticas de seguridad. Asimismo, se ha evidenciado que las pequeñas y

medianas empresas enfrentan mayores dificultades para implementar estas medidas, lo que genera brechas significativas en la protección de datos.

Contexto actual y tendencias emergentes

El marco teórico también debe considerar el contexto contemporáneo, caracterizado por la expansión del teletrabajo, la proliferación de dispositivos IoT y la creciente dependencia de servicios en la nube. Estas tendencias han ampliado la superficie de ataque y han impulsado el desarrollo de nuevas soluciones basadas en inteligencia artificial y aprendizaje automático, capaces de detectar patrones anómalos y anticipar amenazas. La integración de estas tecnologías en las arquitecturas de seguridad representa una evolución hacia modelos más dinámicos y adaptativos.

Tabla 1. Cuadro comparativo de modelos de seguridad en redes empresariales

Modelo / Arquitectura	Principios clave	Ventajas	Limitaciones	Aplicaciones típicas
Defensa en profundidad	Seguridad en múltiples capas (red, aplicación, usuario, datos).	Redundancia y resiliencia; si una capa falla, otra contiene el ataque.	Puede ser costosa y compleja de implementar; requiere coordinación entre capas.	Grandes corporaciones con infraestructura crítica; sectores financieros y gubernamentales.
Zero Trust	"Nunca confiar, siempre verificar"; autenticación y autorización constante.	Adaptado a entornos distribuidos y trabajo remoto; control granular de accesos.	Requiere cambios culturales y tecnológicos profundos; puede generar fricción en la experiencia del usuario.	Empresas con teletrabajo, servicios en la nube, y alta movilidad de usuarios.
Arquitectura de Seguridad Empresarial (ESA)	Marco integral que combina políticas, procedimientos y tecnología alineados con objetivos estratégicos.	Integra la seguridad con la gestión de riesgos y la planificación empresarial; enfoque holístico.	Implementación compleja; requiere compromiso de la alta dirección.	Organizaciones que buscan alinear seguridad con estrategia corporativa; proyectos de transformación digital.

RESULTADOS Y DISCUSIÓN

Los resultados obtenidos a partir de la revisión documental sistemática permiten identificar tres hallazgos principales: la diversidad de arquitecturas de seguridad aplicadas en redes empresariales, la

persistencia de vulnerabilidades asociadas tanto a factores tecnológicos como humanos, y la necesidad de un enfoque integral que combine tecnología, políticas organizacionales y capacitación de usuarios.

En primer lugar, se constató que las organizaciones tienden a adoptar modelos híbridos de seguridad, combinando elementos de la defensa en profundidad con principios del enfoque Zero Trust. Este hallazgo confirma la tendencia hacia arquitecturas más dinámicas y adaptativas, capaces de responder a la movilidad de los usuarios y al uso intensivo de servicios en la nube. La discusión con la teoría muestra que, aunque la defensa en profundidad sigue siendo un referente clásico, el modelo Zero Trust aporta un nivel adicional de control granular que resulta más pertinente en entornos distribuidos.

En segundo lugar, los resultados evidencian que las vulnerabilidades no se limitan a fallos tecnológicos, sino que también derivan de errores humanos y deficiencias organizacionales. La literatura revisada coincide en que la falta de capacitación y la ausencia de políticas claras de gestión de accesos son factores recurrentes que facilitan ataques como el phishing y el robo de credenciales. Este hallazgo se relaciona con estudios previos que subrayan la importancia de la cultura digital como componente esencial de la seguridad empresarial.

En tercer lugar, se identificó que las pequeñas y medianas empresas enfrentan mayores dificultades para implementar estándares internacionales de seguridad, lo que genera una brecha significativa en la protección de datos. Este resultado es consistente con investigaciones que señalan la desigualdad en la capacidad de inversión en ciberseguridad, lo que convierte a las PYMEs en objetivos frecuentes de ataques. La discusión con los antecedentes permite concluir que la seguridad empresarial no puede depender únicamente de la disponibilidad de recursos, sino que requiere estrategias adaptadas a cada contexto organizacional.

Desde una perspectiva interpretativa, los hallazgos permiten generalizar que la seguridad en redes empresariales debe concebirse como un proceso dinámico y multidimensional. La combinación de arquitecturas robustas, políticas organizacionales claras y formación continua de los usuarios constituye la base para fortalecer la resiliencia digital. La novedad científica de este trabajo radica en la articulación de estos tres pilares en un marco integrador, que supera la visión fragmentada de la seguridad como un asunto exclusivamente técnico.

Asimismo, se destaca lo controversial del debate entre la eficacia de los modelos tradicionales y la pertinencia de enfoques emergentes como Zero Trust. Mientras algunos autores sostienen que la defensa en profundidad sigue siendo suficiente, otros argumentan que la creciente complejidad de las redes exige un cambio de paradigma hacia modelos más estrictos y adaptativos. Esta discusión abre perspectivas teóricas sobre la evolución de las arquitecturas de seguridad y plantea la necesidad de investigaciones futuras que evalúen la efectividad de estos modelos en distintos contextos empresariales.

En términos prácticos, los resultados sugieren que las organizaciones deben priorizar la capacitación de sus usuarios, la implementación gradual de modelos Zero Trust y la adopción de políticas de gestión de riesgos alineadas con estándares internacionales. La pertinencia del trabajo se enmarca en la línea de investigación sobre ciberseguridad empresarial, aportando una visión integradora que puede servir de referencia para futuras investigaciones y para la toma de decisiones estratégicas en el ámbito corporativo.

CONCLUSIONES

El análisis realizado permite afirmar que la seguridad en redes empresariales debe concebirse como un proceso integral y dinámico, en el que convergen factores tecnológicos, organizacionales y humanos. La evidencia obtenida demuestra que ninguna arquitectura por sí sola es suficiente para garantizar la protección de los activos digitales; más bien, la combinación de enfoques como la defensa en profundidad, el modelo Zero Trust y la Arquitectura de Seguridad Empresarial ofrece un marco más sólido y adaptable a las exigencias actuales.

La postura que se sostiene en este trabajo es que la seguridad empresarial no puede limitarse a la instalación de herramientas tecnológicas, sino que requiere una cultura organizacional orientada a la gestión de riesgos y a la capacitación continua de los usuarios. Los hallazgos muestran que las vulnerabilidades más críticas se originan en la interacción humana y en la falta de políticas claras, lo que obliga a replantear la seguridad como un asunto transversal en la estrategia corporativa.

Asimismo, se concluye que las pequeñas y medianas empresas enfrentan un desafío particular, pues la escasez de recursos limita su capacidad de implementar estándares internacionales. Este aspecto abre un campo de investigación pendiente: cómo diseñar arquitecturas de seguridad escalables y accesibles que respondan a las necesidades de organizaciones con menor capacidad de inversión.

La novedad de este estudio radica en la articulación de modelos teóricos y hallazgos prácticos en un marco integrador que resalta la importancia de la resiliencia digital como factor de competitividad. Sin embargo, persisten interrogantes que merecen ser abordados en investigaciones futuras, como la efectividad real de la inteligencia artificial en la detección temprana de amenazas, el impacto de la proliferación de dispositivos IoT en la seguridad empresarial y la pertinencia de los marcos normativos internacionales en contextos locales.

En definitiva, este trabajo aporta una visión crítica y propositiva sobre las arquitecturas de seguridad en redes empresariales, subrayando que la prevención de ataques no es un objetivo estático, sino un proceso continuo que exige adaptación, innovación y cooperación entre actores tecnológicos, organizacionales y sociales.

REFERENCIAS BIBLIOGRÁFICAS

Behl, A., & Behl, K. (2021). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. https://doi.org/10.1093/wentk/9780197507414.001.0001

Cui, L., Xie, G., Qu, Y., & Gao, L. (2018). Seguridad y privacidad en las ciudades inteligentes: desafíos y oportunidades. *IEEE Access*, 6, 46134–46145. https://doi.org/10.1109/ACCESS.2018.2853985

Diesch, R., Pfaff, M., & Krcmar, H. (2020). Un modelo integral de factores de seguridad de la información para los responsables de la toma de decisiones. *Computers & Security*, 92, 101747. https://doi.org/10.1016/j.cose.2020.101747

Harvey, J., Pulone, L., Yocky, G., & Charles, E. (2024, mayo). Desafíos en la seguridad de la computación en la nube y sus soluciones. *ResearchGate*. [No DOI disponible]

IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Research.

ISO/IEC. (2018). *ISO/IEC 27001: Information security management systems – Requirements*. International Organization for Standardization. https://www.iso.org/standard/54534.html

Kaspersky Lab. (2022). *The state of cybersecurity in small and medium enterprises*. Kaspersky Research Report.

Microsoft. (2022). *Zero Trust Maturity Model*. Microsoft Security Whitepaper.

Narendra, R., Tadapaneni, H., & Shuaieb Sabri, M. (2020, junio). Desafíos de seguridad en la computación en la nube. *SSRN Electronic Journal*, 7(6), 1–6. https://doi.org/10.2139/ssrn.101747

National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture (SP 800-207)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

Okechukwu, I. (2023). Ciberseguridad en la era del Internet de las cosas: restricciones y soluciones. *Journal of Digital Learning and Distance Education*, 2(11), 1–9. https://doi.org/10.56778/JDLDE.V2I11.233

Sousa de Araujo, M., Souza Machado, B. A., & Passos, F. U. (2024, marzo). Resiliencia en el contexto de la ciberseguridad: una revisión de los conceptos fundamentales y la relevancia. *Applied Sciences*, 14(5), 2116. https://doi.org/10.3390/app14052116

Symantec. (2021). *Internet Security Threat Report*. Symantec Corporation.

Tello Macias, W. T. (2024). Arquitecturas de seguridad y prevención de ataques en redes empresariales. *Ciencia Interdisciplinaria Internacional*, 2(3), 1–22. https://doi.org/10.70577/cieninter.v2i3.10

World Economic Forum. (2022). *Global Cybersecurity Outlook 2022*. WEF Report.