Universidad CENFOTEC

Maestría Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 1

Comparativo de Marcos de Trabajo de Confianza Cero (*Zero Trust*) para Entornos de Trabajo Híbrido

Elaborado por:
Roy Javier Bolaños Alfaro

Abril 2026

ABSTRACT. In the current landscape of digital transformation, driven by cloud computing, mobility, and hybrid work models, traditional perimeter-based security architectures have proven inadequate. This has led to the emergence of the Zero Trust paradigm, which redefines cybersecurity through continuous verification, least privilege access, and the elimination of implicit trust. This article presents a comprehensive comparative analysis of the main Zero Trust frameworks, including NIST SP 800-207, MITRE, Microsoft, and Forrester. The research follows a qualitative approach based on systematic document review, content analysis, and theoretical triangulation. The findings reveal strong conceptual alignment among the frameworks, particularly in their foundational principles, while also highlighting significant differences in architectural approaches, maturity models, and implementation strategies. Additionally, critical challenges related to hybrid environments are identified, including interoperability, identity management, and unified visibility. The main contribution of this study lies in the development of technical and strategic criteria to support the effective adoption of Zero Trust in distributed organizational environments, representing an innovative approach by linking comparative analysis with real-world hybrid scenarios.

PALABRAS CLAVE: Zero Trust, Ciberseguridad, Entornos Híbridos, Arquitectura de Seguridad, Gestión de Identidades, Marcos de Trabajo

INTRODUCCIÓN

Durante los últimos años, la evolución de las tecnologías de la información ha generado una transformación estructural en la forma en que las organizaciones operan y gestionan sus recursos digitales, la migración hacia servicios en la nube, el uso generalizado de dispositivos móviles y la adopción del trabajo remoto han diluido las fronteras tradicionales del perímetro corporativo.

El modelo de seguridad perimetral, históricamente dominante, se basaba en la premisa de que los usuarios dentro de la red eran confiables, mientras que los externos representaban una amenaza, sin embargo, este enfoque ha perdido efectividad en entornos híbridos, donde los accesos se realizan desde múltiples ubicaciones, dispositivos y redes no confiables.

Como respuesta a esta problemática, surge el paradigma de Confianza Cero, el cual plantea un cambio radical en el enfoque de la seguridad de la información, en lugar de confiar por defecto, este modelo establece que toda solicitud de acceso debe ser verificada continuamente, considerando factores como identidad, contexto, estado del dispositivo y nivel de riesgo.

En este contexto, el presente estudio tiene como objetivo analizar comparativamente los principales marcos de trabajo de *Zero Trust*, con el fin de identificar sus similitudes, diferencias y aplicabilidad en entornos híbridos, aportando una base analítica que facilite la toma de decisiones estratégicas en ciberseguridad.

MATERIALES Y MÉTODOS

El presente estudio se enmarca en un enfoque metodológico cualitativo de carácter descriptivo, analítico y comparativo, orientado a examinar en profundidad los principales marcos de trabajo de Confianza Cero y su aplicabilidad en entornos de trabajo híbrido, la investigación se desarrolló bajo un diseño no experimental y transversal, dado que no se manipularon variables, sino que se analizaron en su contexto natural a partir de fuentes documentales especializadas.

DISEÑO DE LA INVESTIGACIÓN

El diseño metodológico adoptado responde a un esquema de análisis comparativo estructurado, el cual permite identificar patrones, afinidades y divergencias entre los distintos marcos de *Zero Trust*, este enfoque resulta pertinente debido a la naturaleza conceptual y normativa de los modelos analizados, los cuales no se prestan a medición cuantitativa directa, sino a evaluación interpretativa basada en criterios técnicos.

Se empleó una lógica inductivo-analítica, en la cual se partió del análisis individual de cada marco para posteriormente construir una visión integradora que permitiera establecer relaciones, complementariedades y diferencias sustanciales.

SELECCIÓN DE FUENTES Y CRITERIOS DE INCLUSIÓN

La selección de los marcos de referencia se realizó mediante un muestreo no probabilístico de tipo intencional, considerando aquellos modelos que cumplen con los siguientes criterios:

- Relevancia institucional y académica (organismos reconocidos internacionalmente)
- Nivel de adopción en la industria
- Actualidad y vigencia del marco
- Disponibilidad de documentación técnica detallada
- Aplicabilidad en entornos empresariales reales

Bajo estos criterios, se seleccionaron los siguientes marcos:

NIST SP 800-207: Documento normativo que establece las bases conceptuales y arquitectónicas de *Zero Trust*. Define componentes clave como el *Policy Engine (PE)*, *Policy Administrator (PA)* y *Policy Enforcement Point (PEP)*, así como principios de diseño y modelos de implementación.

MITRE Zero Trust Framework: Marco orientado a la implementación práctica, con énfasis en la madurez organizacional, la interoperabilidad de tecnologías y los desafíos reales en la adopción progresiva de *Zero Trust*.

Microsoft Zero Trust Model: Propuesta de carácter operativo basada en seis pilares fundamentales: identidad, dispositivos, aplicaciones, datos, infraestructura y redes. Incluye un modelo de madurez evolutivo que facilita la adopción gradual.

Forrester Zero Trust Extended (ZTX): Marco estratégico que introduce el concepto de *Zero Trust* ampliado, centrado en la protección de datos y el control de acceso basado en riesgo, con un enfoque en analítica avanzada y automatización.

TÉCNICAS DE RECOLECCIÓN DE DATOS

La información fue recolectada mediante revisión documental sistemática, utilizando como insumos principales:

- Documentos oficiales de cada marco
- Publicaciones técnicas especializadas

- Informes de organismos reconocidos
- Documentación académica de Trabajos Finales de Graduación

Para garantizar la consistencia en la recolección, se emplearon fichas de análisis documental, en las cuales se registraron, de manera estructurada, los elementos clave de cada marco, tales como:

- Principios fundamentales
- Componentes arquitectónicos
- Modelos de madurez
- Estrategias de implementación
- Enfoque en entornos híbridos

TÉCNICAS DE ANÁLISIS DE LA INFORMACIÓN

El procesamiento de la información se realizó mediante una combinación de técnicas cualitativas:

a) Análisis de contenido: se utilizó para identificar categorías conceptuales comunes entre los marcos, permitiendo clasificar la información en dimensiones analíticas homogéneas.

b) Matrices comparativas: se diseñaron matrices que permitieron contrastar los marcos en función de criterios previamente definidos, facilitando la visualización de similitudes y diferencias.

c) Triangulación teórica: se aplicó para validar los hallazgos mediante la comparación de múltiples fuentes, aumentando la confiabilidad y consistencia del análisis.

d) Síntesis integradora: permitió consolidar los resultados en una visión unificada, destacando relaciones de complementariedad entre los marcos analizados.

RESULTADOS

El análisis comparativo de los marcos de trabajo de Confianza Cero permitió identificar una alta convergencia conceptual entre las propuestas de NIST, MITRE, Microsoft y Forrester, particularmente en lo relativo a los principios fundamentales que sustentan este paradigma de seguridad. Todos los marcos coinciden en la necesidad de eliminar la confianza implícita dentro de la red organizacional, promoviendo un enfoque basado en la verificación continua de identidades y contextos, el acceso bajo el principio de mínimo privilegio y la asunción de compromiso como condición operativa permanente, esta coincidencia evidencia la consolidación de un núcleo teórico común que define a *Zero Trust* como un estándar emergente en la ciberseguridad moderna.

No obstante, a pesar de esta alineación conceptual, el estudio revela diferencias significativas en la forma en que cada marco traduce estos principios en arquitecturas e implementaciones concretas, el modelo propuesto por NIST se caracteriza por su rigurosidad técnica y su orientación normativa, estructurando la arquitectura *Zero Trust* a partir de componentes lógicos claramente definidos, como el Policy Engine, el Policy Administrator y el Policy Enforcement Point. Este enfoque proporciona una base sólida para el diseño de soluciones, pero puede resultar abstracto en contextos organizacionales que requieren guías más operativas.

En contraste, el enfoque de Microsoft presenta una orientación eminentemente práctica y operacional, estructurando la implementación de *Zero Trust* en torno a seis dominios clave: identidad, dispositivos, aplicaciones, datos, infraestructura y redes, este modelo facilita la adopción progresiva mediante un esquema de madurez claramente definido, permitiendo a las organizaciones transitar desde estados tradicionales hacia niveles avanzados de seguridad, asimismo, su énfasis en la identidad como eje central resulta particularmente relevante en entornos híbridos, donde los usuarios acceden desde múltiples contextos.

Por su parte, el marco desarrollado por MITRE introduce una perspectiva pragmática centrada en los desafíos reales de implementación, destacando aspectos como la interoperabilidad entre herramientas, la complejidad de

integración con sistemas heredados y la necesidad de una adecuada gobernanza. Este enfoque complementa los modelos más teóricos al evidenciar las brechas existentes entre el diseño conceptual y la ejecución práctica de *Zero Trust* en organizaciones reales.

Para el caso de Forrester, se observa una visión estratégica orientada al control del acceso basado en riesgo y la protección de los datos como activo crítico. Su modelo *Zero Trust Extended* (ZTX) enfatiza la automatización, la analítica avanzada y la toma de decisiones contextualizadas, introduciendo el principio de “denegar por defecto” como mecanismo fundamental de control, este enfoque amplía la perspectiva tradicional al incorporar capacidades dinámicas que responden a entornos altamente cambiantes.

En relación con la aplicabilidad en entornos de trabajo híbrido, los resultados evidencian que todos los marcos reconocen la identidad como el elemento central para la gestión de accesos, consolidándose como el punto de control más relevante en la arquitectura *Zero Trust*, de igual manera, se identifica la microsegmentación como una estrategia clave para limitar el movimiento lateral dentro de la red, reduciendo significativamente la superficie de ataque, sin embargo, también se destacan desafíos importantes, tales como la falta de visibilidad unificada, la complejidad en la correlación de eventos de seguridad y las dificultades asociadas a la integración de múltiples plataformas tecnológicas.

Adicionalmente, el análisis permitió identificar que los modelos de madurez propuestos por los distintos marcos convergen en una evolución progresiva desde esquemas tradicionales hacia arquitecturas completamente dinámicas y automatizadas, no obstante, se observa que muchas organizaciones se encuentran en estados intermedios de adopción, lo que implica la coexistencia de controles tradicionales con principios de *Zero Trust*, generando escenarios híbridos que requieren estrategias de transición cuidadosamente planificadas.

En síntesis, los resultados obtenidos demuestran que, si bien los marcos analizados presentan diferencias en su enfoque, nivel de abstracción y orientación práctica, estos no son excluyentes, sino complementarios, la integración de sus propuestas permite construir una visión más completa y robusta de la arquitectura *Zero Trust*, especialmente en contextos

organizacionales caracterizados por la distribución de recursos, la movilidad de usuarios y la creciente complejidad de las amenazas digitales.

DISCUSIÓN

Los resultados obtenidos a partir del análisis comparativo de los marcos de Confianza Cero permiten establecer que, si bien existe una convergencia sólida en los principios fundamentales, la principal diferenciación entre los modelos radica en su enfoque de implementación, nivel de abstracción y orientación estratégica u operativa, esta situación evidencia que *Zero Trust* no debe entenderse como un modelo único o estandarizado, sino como un paradigma adaptable, cuya efectividad depende en gran medida del contexto organizacional en el que se implementa.

Uno de los aspectos más relevantes identificados en el estudio es que la traducción de los principios teóricos a mecanismos prácticos de implementación constituye el principal desafío para las organizaciones, mientras marcos como NIST ofrecen una base conceptual robusta y estructurada, su nivel de abstracción puede dificultar su adopción directa en entornos empresariales sin un proceso de adaptación. En contraste, modelos como el de Microsoft facilitan la operacionalización mediante dominios claramente definidos, aunque pueden depender en mayor medida de ecosistemas tecnológicos específicos, lo que introduce consideraciones adicionales en términos de dependencia tecnológica e interoperabilidad.

En este sentido, el marco de MITRE aporta un valor significativo al evidenciar las brechas existentes entre el diseño conceptual y la implementación real, destacando problemáticas como la integración con sistemas heredados, la fragmentación de herramientas de seguridad y la necesidad de una gobernanza sólida. Este hallazgo refuerza la idea de que la adopción de *Zero Trust* no es únicamente un problema técnico, sino también organizacional y estratégico, que requiere alineación entre procesos, políticas y tecnologías.

Por otra parte, la perspectiva de Forrester introduce una dimensión adicional al enfatizar el control basado en riesgo y la protección de los datos como eje central de la seguridad, lo cual resulta especialmente relevante en entornos híbridos, la incorporación de analítica avanzada y automatización

permite evolucionar hacia modelos más dinámicos, capaces de adaptarse a condiciones cambiantes en tiempo real, sin embargo, este enfoque también implica mayores exigencias en términos de capacidades tecnológicas, madurez organizacional y gestión de información.

En relación con los criterios de evaluación identificados en el estudio, se observa que factores como la gestión de identidades, la visibilidad de los activos, la capacidad de integración y la automatización de controles son determinantes para el éxito de la implementación de *Zero Trust*, en particular, la identidad emerge como el elemento central sobre el cual se articulan los mecanismos de control, consolidándose como el nuevo perímetro de seguridad en entornos distribuidos. Esta transformación implica un cambio significativo respecto a los modelos tradicionales, donde la red constituía el principal punto de control.

Además, los resultados evidencian que los entornos de trabajo híbrido representan un escenario particularmente complejo, debido a la coexistencia de infraestructuras locales y servicios en la nube, así como a la diversidad de dispositivos y ubicaciones desde las cuales se accede a los recursos, en este contexto, la implementación de *Zero Trust* requiere no solo herramientas tecnológicas adecuadas, sino también una estrategia integral que contemple aspectos como la segmentación de la red, la gestión de accesos privilegiados y la monitorización continua.

Otro elemento relevante es la identificación de que muchas organizaciones se encuentran en niveles intermedios de madurez, donde coexisten controles tradicionales con prácticas de *Zero Trust*, en esta situación se generan desafíos adicionales, ya que puede introducir inconsistencias en las políticas de seguridad y aumentar la complejidad operativa, por lo tanto, la transición hacia un modelo completamente basado en Confianza Cero debe abordarse de manera progresiva, mediante una hoja de ruta claramente definida que permita minimizar riesgos y maximizar beneficios.

En síntesis, la discusión de los resultados permite concluir que la implementación efectiva de *Zero Trust* requiere un enfoque integral y multidimensional, que combine elementos conceptuales, técnicos y organizacionales, los marcos analizados no deben considerarse alternativas

excluyentes, sino componentes complementarios que, al integrarse adecuadamente, pueden proporcionar una solución más robusta y adaptable a las necesidades de los entornos híbridos modernos, este enfoque integrador constituye un aporte relevante del estudio, al proporcionar una visión práctica y estratégica para la adopción de arquitecturas de seguridad basadas en Confianza Cero.

RECOMENDACIONES Y CRITERIOS PARA UNA IMPLEMENTACIÓN *ZERO TRUST* EN UN ENTORNO HÍBRIDO

La implementación de un enfoque *Zero Trust* en un entorno híbrido exige reconocer que la identidad se convierte en el plano de control principal donde convergen los mecanismos de autenticación, autorización y verificación continua, por ello, se recomienda adoptar estrategias que fortalezcan este dominio, comenzando con la eliminación de credenciales débiles y la implementación obligatoria de autenticación multifactor resistente al phishing, asimismo, es esencial consolidar todas las identidades bajo un proveedor centralizado que permita la aplicación uniforme de políticas de acceso condicional basadas en riesgo, contexto y comportamiento, este proceso implica reducir la proliferación de cuentas locales, integrar directorios on-premise y de nube, y establecer mecanismos de autenticación robustos adecuados para arquitecturas distribuidas, el objetivo es que cada sesión, dispositivo y solicitud de acceso sea evaluada dinámicamente, eliminando cualquier vestigio de confianza implícita.

De igual forma, en los entornos híbridos se vuelve imprescindible integrar la postura de los dispositivos como un componente inherente a la lógica *Zero Trust*, los dispositivos, ya sean corporativos, personales o móviles, deben ser continuamente evaluados mediante sistemas centralizados de gestión de *Endpoints* y herramientas que garanticen su cumplimiento normativo, la verificación de la postura de seguridad (como el cifrado habilitado, los parches actualizados y la presencia de herramientas EDR) debe condicionar el acceso a los recursos, un dispositivo sin telemetría suficiente, incumplido o sospechoso debe restringirse automáticamente en función del riesgo, esta integración

permite evitar que *Endpoints* comprometidos se conviertan en vectores de ataque, especialmente al operar desde fuera del perímetro tradicional.

En materia de comunicaciones y segmentación, se recomienda adoptar una microsegmentación dinámica basada en identidad y contexto, dado que los modelos tradicionales de segmentación basados en subredes o VLAN carecen de la granularidad y flexibilidad necesarias en un entorno híbrido, resulta prioritario establecer políticas estrictas de “denegar por defecto”, limitando el tráfico lateral entre sistemas y servicios, tanto en la nube como en la infraestructura local, la segmentación lógica debe estar gobernada por políticas centralizadas que permitan restringir el acceso según la relevancia, sensibilidad o criticidad de los recursos, este enfoque no solo reduce la superficie de ataque, sino que impide que un compromiso aislado escale a múltiples sistemas.

Igualmente, es relevante la consolidación del monitoreo y la telemetría en una plataforma centralizada, permitiendo visibilidad *end-to-end* sobre identidades, aplicaciones, dispositivos y datos. Independientemente de la ubicación del recurso, la gestión de logs debe unificarse en un SIEM robusto que soporte la correlación de eventos provenientes tanto de servicios *cloud* como de entornos *on-premise*. Junto con ello, la implementación de herramientas de análisis de comportamiento (UEBA) y orquestación automática de seguridad (SOAR) resulta esencial para detectar comportamientos anómalos y responder a incidentes de manera rápida, coherente y automatizada. En un entorno híbrido, la telemetría no es un lujo, sino un requisito indispensable para aplicar *Zero Trust* de forma coherente y continua.

Un elemento crítico, dentro de la arquitectura *Zero Trust* híbrida, es la adopción de un modelo de políticas dinámicas, respaldadas por un motor de políticas capaz de evaluar en tiempo real variables como ubicación, tipo de dispositivo, riesgo estimado, historial de comportamiento, sensibilidad del recurso y nivel de privilegio del usuario, este modelo requiere que cada solicitud de acceso pase por un proceso de verificación contextual, eliminando los accesos permanentes y adoptando esquemas basados en permisos mínimos y acceso justo-a-tiempo (JIT), la política debe ajustarse constantemente según el nivel de riesgo, permitiendo que el sistema actúe de forma adaptativa e inteligente ante comportamientos inconsistentes o potencialmente maliciosos.

Por otra parte, la protección de los datos debe convertirse en un eje estratégico de la implementación *Zero Trust* híbrida, esto implica establecer mecanismos de clasificación de la información, aplicar políticas de cifrado en reposo y en tránsito, y habilitar controles avanzados de prevención de fuga de datos (DLP) tanto en herramientas de nube como en la infraestructura local, además, los datos sensibles deben estar sujetos a controles más estrictos de acceso, monitoreo continuo y restricciones basadas en la sensibilidad y contexto de cada interacción. En un entorno donde los datos se mueven entre plataformas, servicios y dispositivos, garantizar su integridad y confidencialidad requiere un enfoque multicapas que combine controles técnicos y normativos.

La automatización también juega un papel fundamental en la implementación *Zero Trust* híbrida, dado que los entornos distribuidos generan un volumen elevado de eventos y requieren un control continuo, se recomienda integrar soluciones de orquestación y automatización (SOAR) que permitan responder de manera eficiente a incidentes recurrentes, gestionar políticas en tiempo real y ejecutar procesos de remediación sin intervención humana, este enfoque reduce la carga operativa, minimiza errores manuales y permite que los equipos de seguridad se concentren en amenazas complejas, la automatización debe extenderse tanto a políticas de acceso como a operaciones de red, configuración de dispositivos, revisiones de seguridad y control de identidad.

En cuanto a gobernanza, cultura y gestión del cambio, la implementación de *Zero Trust* en entornos híbridos no puede considerarse únicamente un proceso técnico, es indispensable establecer una estructura de gobernanza sólida que incluya un comité de dirección, roles claramente definidos, políticas documentadas y métricas claras de adopción. La resistencia al cambio constituye uno de los obstáculos más citados por MITRE, por lo que es esencial un programa de comunicación interna que ayude a los empleados a comprender los beneficios del modelo, así como entrenamientos dirigidos a personal técnico y no técnico, la madurez organizacional es un factor determinante para el éxito o fracaso de *Zero Trust*.

Otra recomendación clave consiste en adoptar un modelo de implementación por fases, inicialmente, las organizaciones deben centrarse en los fundamentos: fortalecer la identidad, habilitar MFA, unificar logs y desarrollar inventarios de activos, posteriormente, deben avanzar hacia la visibilidad y el

control, implementando segmentación, acceso condicional y políticas de protección de datos y finalmente, deben aspirar a un estado de optimización, integrando automatización avanzada, respuesta adaptativa, protección de aplicaciones heredadas y *Zero Trust multicloud*, este enfoque gradual permite reducir riesgos, gestionar costos y asegurar la inserción progresiva del modelo.

La interoperabilidad entre plataformas de nube y entornos locales debe asegurarse mediante el uso de estándares abiertos, conectores híbridos y mecanismos de federación de identidades, es crucial evitar dependencias tecnológicas que limiten la capacidad de integración entre entornos heterogéneos, las políticas *Zero Trust* deben ser únicas, coherentes y consistentes, independientemente de la infraestructura donde se apliquen, la falta de interoperabilidad es una de las principales causas de inconsistencias operativas que debilitan el modelo.

Finalmente, la implementación *Zero Trust* en entornos híbridos requiere supervisión y mejora continua, el modelo debe revisarse regularmente, actualizarse ante nuevas amenazas, ajustarse según el comportamiento de los usuarios y ser evaluado mediante métricas de madurez. las aplicaciones *legacy* deben ser modernizadas progresivamente o protegidas con mecanismos de aislamiento y *proxies* que permitan integrarlas al modelo sin vulnerar su integridad, asimismo, *Zero Trust* debe integrarse a DevSecOps para garantizar que las nuevas aplicaciones se construyan desde el inicio bajo este paradigma de seguridad.

CONCLUSIONES

El presente estudio permitió analizar de manera integral los principales marcos de trabajo de Confianza Cero, evidenciando que este paradigma representa una evolución necesaria en la ciberseguridad contemporánea, especialmente frente a los desafíos derivados de la transformación digital y la consolidación de los entornos de trabajo híbrido. La investigación confirma que los modelos tradicionales basados en perímetros han perdido efectividad, lo que ha impulsado la adopción de enfoques centrados en la verificación continua y la eliminación de la confianza implícita.

Uno de los hallazgos más relevantes es la existencia de una alta convergencia conceptual entre los marcos analizados, particularmente en lo relativo a los principios fundamentales de *Zero Trust*, tales como el acceso de mínimo privilegio, la validación constante de identidades y la asunción de compromiso. Esta coincidencia sugiere la consolidación de un estándar emergente en la arquitectura de seguridad, que trasciende las diferencias entre organizaciones y proveedores tecnológicos.

Sin embargo, el estudio también evidencia que las principales diferencias radican en la forma en que estos principios son implementados, variando según el enfoque de cada marco. Mientras algunos modelos presentan una orientación más normativa y conceptual, otros ofrecen aproximaciones más prácticas y operativas. Esta diversidad no debe interpretarse como una limitación, sino como una oportunidad para que las organizaciones seleccionen y adapten los elementos que mejor se ajusten a sus necesidades y capacidades.

En este sentido, se concluye que los marcos de *Zero Trust* son complementarios y no excluyentes, ya que cada uno aporta valor desde distintas perspectivas: conceptual, estratégica, operativa y pragmática, la integración de estos enfoques permite construir arquitecturas de seguridad más completas, capaces de responder a la complejidad de los entornos tecnológicos actuales.

Otro aspecto fundamental identificado es el papel central de la identidad como nuevo perímetro de seguridad, desplazando el enfoque tradicional basado en la red. Este cambio implica una transformación significativa en la forma en que se gestionan los accesos y se protegen los recursos, especialmente en contextos donde los usuarios operan desde múltiples ubicaciones y dispositivos. La correcta gestión de identidades y accesos se convierte, por tanto, en un factor crítico para la implementación exitosa de *Zero Trust*.

Asimismo, se concluye que la adopción de este paradigma requiere un proceso progresivo y estratégico, más que una implementación inmediata o aislada. Las organizaciones deben considerar su nivel de madurez tecnológica, la integración con sistemas existentes y la necesidad de establecer mecanismos de gobernanza adecuados. En particular, los entornos híbridos representan un

desafío significativo, debido a la coexistencia de infraestructuras locales y servicios en la nube, lo que demanda soluciones flexibles y escalables.

Finalmente, el estudio destaca que el éxito en la implementación de *Zero Trust* no depende exclusivamente de la tecnología, sino de la alineación entre procesos, personas y herramientas, así como del compromiso organizacional con una cultura de seguridad continua, en este contexto, la adopción de un enfoque integral que combine distintos marcos de referencia se posiciona como la estrategia más adecuada para fortalecer la ciberseguridad en organizaciones modernas.

En síntesis, la arquitectura de Confianza Cero se consolida como un modelo indispensable para enfrentar los retos actuales de seguridad, proporcionando una base sólida para el desarrollo de estrategias adaptativas, resilientes y orientadas al riesgo en entornos de trabajo híbridos.

BIBLIOGRAFIA

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Arquitectura de confianza cero (NIST SP 800-207)* (Y. Á. Bettati, Trad.). Dreamlab Technologies Chile. https://dreamlab.net/wp-content/uploads/2024/11/Arquitectura_de_confianza_cero-NIST.SP_.800-207.pdf

Doherty, D. H., & McKenney, B. (2021, junio). *Zero trust architectures: Are we there yet?* MITRE Corporation. https://www.mitre.org/sites/default/files/2021-12/pr-21-1273-zero-trust-architectures-are-we-there-yet.pdf

Cunningham, C. (2018, enero 19). *The Zero Trust eXtended (ZTX) ecosystem: Extending zero trust security across your digital business*. Forrester Research, Inc. https://www.cisco.com/c/dam/m/en_sg/solutions/security/pdfs/forrester-ztx.pdf

Microsoft Corporation. (2020, octubre). *Zero Trust vision paper*. Microsoft. https://download.microsoft.com/download/f/9/2/f92129bc-0d6e-4b8e-a47b-288432bae68e/Zero_Trust_Vision_Paper_Final%2010.28.pdf