Universidad CENFOTEC

Escuela de Ciberseguridad

Tema:

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

Elaborado por:

Roy Javier Bolaños Alfaro

Diciembre, 2025

Tabla de Contenido

Abstract

Capítulo 1. Introducción

En los últimos 10 años, el modelo de la tecnología de la información ha sufrido una transformación sin igual, ya que es impulsada por la adopción masiva de la computación en la nube, la movilidad y la interconexión creciente de dispositivos. El proceso de digitalización, el cual creció de manera exponencial tras haber sufrido la crisis sanitaria mundial, derribó las fronteras tradicionales del espacio de trabajo, trayendo consigo un modelo hibrido, en el cual se combinan el trabajo remoto y el presencial como una nueva norma operativa a nivel mundial para las organizaciones. Si bien esta evolución de trabajo ha traído múltiples beneficios en cuanto a la flexibilidad y productividad, también ha desgastado los principios del modelo de la seguridad de la información que prevaleció durante años, el cual se basaba en la seguridad perimetral.

El enfoque tradicional, que a menudo se compara con una fortaleza medieval, se basa en la premisa de que todo lo que se encontraba dentro del perímetro de la red corporativa era inherentemente confiable, mientras que cualquier elemento externo era considerado una amenaza potencial. Con todo esto, a lo que llamábamos perímetro se disolvió. Ahora todos, ya sean empleados o usuarios acceden a recursos críticos desde cualquier parte del mundo donde se encuentren y aunado a esto utilizando una mezcla de dispositivos corporativos y personales (BYOD), y conectándose directamente a aplicaciones distribuidas en múltiples nubes (SaaS, IaaS). Esta nueva realidad ha generado que la superficie de ataque sea más extensa y porosa, dejando a las arquitecturas de seguridad legadas como una incoherencia ineficaz frente a las tácticas de los adversarios modernos.

Como respuesta directa a la falla de este modelo antiguo, surge un cambio de paradigma fundamental en la estrategia de ciberseguridad, el cual se denomina Confianza Cero (*Zero Trust*). Esta fue propuesta inicialmente hace más de una década y su relevancia hoy es innegable. Como tal la Confianza Cero más que un producto o un tipo de tecnología, es una estrategia que se fundamenta en un principio radicalmente simple pero poderoso de "nunca confiar, siempre verificar". Este principio, elimina la confianza que está implícita asociada a la ubicación en la red y exige una verificación estricta de la identidad y el contexto para cada solicitud de acceso a los recursos, sin que importe de

dónde provenga o a qué red esté conectado el solicitante. Se trata de un modelo enfocado en la protección de los datos y los activos, que asume que las amenazas pueden originarse tanto fuera como dentro de la red

La transición hacia una arquitectura de Confianza Cero representa un desafío considerable para las organizaciones. La principal dificultad no radica en la comprensión de su filosofía, sino en su implementación práctica. Diversos organismos de estandarización y firmas de análisis de la industria, como el Instituto Nacional de Estándares y Tecnología (NIST), Forrester Research y Gartner, han propuesto sus propios marcos de trabajo y modelos conceptuales para guiar esta implementación. Si bien todos comparten los principios básicos, difieren en su terminología, sus pilares fundamentales y sus enfoques arquitectónicos, creando un panorama más complejo y que a menudo se vuelve confuso para los que toman las decisiones.

Este trabajo de graduación surge precisamente de esta problemática. El objetivo de la presente investigación es realizar un análisis comparativo exhaustivo de los marcos de trabajo de Confianza Cero más populares, donde a través de una revisión sistemática de su estructura, componentes y principios, se evalúe su aplicabilidad, ventajas y desafíos de implementación, con un enfoque particular en las necesidades y realidades de los entornos de trabajo híbridos. En ese sentido, se busca poder dar la claridad a este complejo ecosistema y así ofrecer un recurso analítico que sirva como guía para que las organizaciones puedan seleccionar y adaptar de manera más informada el marco que mejor se alinee con su postura de seguridad, sus capacidades tecnológicas y sus objetivos de negocio.

1.1 Antecedentes del problema

Durante mucho tiempo, la ciberseguridad en las empresas funcionaba como proteger un castillo medieval, toda la información importante estaba dentro de los muros (la oficina), y se construía una "muralla digital" con herramientas como los firewalls para mantener a los extraños fuera. Se partía de una idea simple; si estabas dentro del castillo, eras de confianza; si estabas fuera, no lo eras. Si alguien necesitaba trabajar desde casa, se le daba un "túnel secreto"

(una VPN) para que pudiera entrar al castillo y ser considerado, de nuevo, como alguien de confianza.

Sin embargo, en los últimos años, la forma en que trabajamos cambió por completo y este modelo de castillo dejó de tener sentido, primero, mucha de la información y las aplicaciones importantes se mudaron a la nube (como cuando usamos Microsoft 365 o Google Drive), lo que significa que los datos ya no estaban guardados dentro del castillo, segundo, la gente empezó a usar sus propios teléfonos y computadoras personales para trabajar, y finalmente, el trabajo desde casa se convirtió en la nueva normalidad para la mayoría, en resumen, el trabajo ya no se hacía dentro de los muros del castillo, por lo que proteger solo esos muros se volvió inútil.

Los ciberdelincuentes se dieron cuenta de esto rápidamente, en lugar de intentar derribar la muralla, encontraron que era mucho más fácil engañar a una persona para que les diera sus "llaves", es decir, su usuario y contraseña, a través de correos falsos (*phishing*), el gran problema del modelo del castillo es que, una vez que un atacante robaba las llaves de un solo empleado, el sistema le daba acceso a casi todo, porque confiaba ciegamente en cualquiera que ya estuviera "dentro".

Para solucionar este enorme hueco de seguridad, nació una nueva filosofía llamada "Confianza Cero" (*Zero Trust*), la idea es muy sencilla y poderosa: dejar de confiar por defecto en cualquiera, incluso si ya está dentro de la red, ahora, la regla es "nunca confiar, siempre verificar", esto significa que el sistema debe comprobar la identidad de cada usuario y la seguridad de su dispositivo cada vez que intenta acceder a cualquier recurso, sin importar desde dónde se conecte.

Aquí es donde surge el problema que aborda esta investigación, aunque casi todos en el mundo de la ciberseguridad están de acuerdo en que la "Confianza Cero" es la estrategia correcta, no existe un único manual de instrucciones para aplicarla, diferentes organizaciones y expertos han creado sus propias guías o "marcos de trabajo", esta variedad de opciones, aunque bien intencionada, genera una gran confusión en las empresas que quieren adoptar este modelo, pero no saben por dónde empezar, qué guía seguir o cuál es la mejor para su situación de trabajo híbrido (con gente en la oficina y en casa), el

propósito de este trabajo es, precisamente, analizar y comparar estas guías para ofrecer una mayor claridad.

1.2 Definición y Descripción del Problema

La adopción acelerada de modelos de trabajo híbrido, catalizada por eventos globales recientes y la transformación digital, ha redefinido fundamentalmente el panorama de la ciberseguridad corporativa, el modelo de trabajo tradicional, confinado a un perímetro de red físico y protegido por defensas perimetrales (como *firewalls* y VPNs), ha quedado obsoleto, en el entorno híbrido, los empleados, dispositivos, aplicaciones y datos están distribuidos, accediendo a recursos corporativos desde redes no confiables (hogares, redes públicas) y utilizando a menudo dispositivos personales (BYOD).

Este nuevo paradigma disuelve el perímetro de seguridad tradicional, la superficie de ataque se ha expandido exponencialmente, y los métodos de seguridad basados en la ubicación (confiar en todo lo que está "dentro" de la red) ya no son viables ni seguros, una credencial comprometida o un dispositivo infectado en una red doméstica le pueden dar a un ciber atacante un acceso amplio e indebido a los sistemas centrales de una organización, como lo se ha visto en los crecientes ataques de ransomware y brechas de datos que explotan las debilidades del acceso remoto.

El mayor problema radica en la falta de un análisis comparativo sistemático y contextualizado, que permita identificar las fortalezas, limitaciones y puntos de convergencia de los principales marcos de trabajo de Confianza Cero en escenarios de trabajo híbrido, por tal razón, esta carencia dificulta la toma de decisiones estratégicas por parte de los responsables de ciberseguridad (CISOs, administradores de la seguridad cibernética), quienes deben seleccionar o adaptar un modelo que equilibre la protección de la información, la experiencia del usuario, la interoperabilidad tecnológica y la viabilidad de implementación.

Por tal razón, se plantea la necesidad de desarrollar un estudio comparativo de los marcos de trabajo de Confianza Cero aplicables a entornos híbridos, con el fin de establecer criterios técnicos y operativos que orienten a las organizaciones en la selección del enfoque más adecuado para su contexto, dicho análisis va a permitir una mejor comprensión práctica del modelo *Zero*

Trust y a la vez consolidar estrategias de ciberseguridad más resilientes y adaptadas a las nuevas formas de trabajo.

1.3 Justificación

La transformación digital y la adopción del trabajo híbrido han modificado de manera estructural la forma en que las organizaciones gestionan la identidad, el acceso y la protección de sus activos de información, este cambio ha disuelto los límites tradicionales del perímetro corporativo, exponiendo infraestructuras, servicios y datos a nuevas superficies de ataque. En este contexto, las estrategias de ciberseguridad basadas en la confianza implícita y el control perimetral resultan insuficientes para mitigar riesgos asociados a la movilidad, el acceso remoto y la adopción de servicios en la nube.

La arquitectura de Confianza Cero (*Zero Trust Architecture*, ZTA) representa una respuesta a estas limitaciones al basarse en la verificación continua, la segmentación y el control contextual de accesos, no obstante, su adopción práctica se enfrenta a una dificultad, por la existencia de múltiples marcos de trabajo con principios, componentes y estrategias heterogéneas, donde la ausencia de una guía comparativa clara genera ambigüedad y dudas en la toma de decisiones y con frecuencia conduce a implementaciones parciales o incorrectas con las necesidades del entorno híbrido.

El presente trabajo se justifica porque aporta un análisis comparativo técnico y estratégico de los principales marcos de Confianza Cero, con énfasis en su aplicabilidad a entornos laborales híbridos.

Dicho enfoque permitirá:

- Optimizar la toma de decisiones en materia de ciberseguridad, al ofrecer criterios más objetivos para seleccionar de mejor manera o combinar marcos de trabajo según las características y restricciones de cada organización.
- Reducir costos operativos y de implementación, al evitar inversiones en tecnologías o metodologías que no estén alineadas con las capacidades y prioridades institucionales de la empresa
- Aumentar la eficacia de las estrategias de protección, al identificar las prácticas y controles más adecuados para garantizar la seguridad de acceso y la integridad de los datos en escenarios distribuidos.

- Fortalecer la resiliencia organizacional, al promover un enfoque preventivo y adaptable frente a amenazas internas y externas.

Desde una perspectiva académica y científica, el trabajo representa un aporte al conocimiento sobre seguridad basada en marcos de Confianza Cero, al sistematizar y contrastar marcos de referencia esparcidos bajo un enfoque unificado y orientado al contexto del trabajo híbrido. Desde una perspectiva práctica, ofrece una guía de apoyo a los responsables de la ciberseguridad, como a los arquitectos de red y tomadores de decisión para poder alinear políticas de seguridad, procesos operativos y controles tecnológicos bajo criterios consistentes, medibles y sostenibles.

Como tal, la innovación del estudio radica en su enfoque comparativo aplicado a entornos híbridos, un escenario poco abordado de forma sistemática en la literatura académica y profesional, pese a su creciente relevancia en el mundo laboral actual. Al enlazar los marcos Confianza Cero (*Zero Trust*) con la realidad operativa de la movilidad laboral y la infraestructura distribuida, este trabajo contribuye directamente al fortalecimiento de la ciberseguridad organizacional en el marco de la nueva normalidad digital.

1.4 Viabilidad

La viabilidad del presente Trabajo Final de Graduación se analiza desde tres perspectivas: técnica, operativa y económica, este análisis permite demostrar que la investigación propuesta se puede elaborar de forma realista, eficiente y sin comprometer el funcionamiento de las instituciones involucradas ni requerir recursos extraordinarios.

1.4.1 Punto de Vista Técnico

El Trabajo Final de Graduación es técnicamente viable dado que el autor de este trabajo, en su calidad de investigador posee la formación y experiencia en ciberseguridad, conocimientos en la gestión de infraestructuras tecnológicas y administración de entornos corporativos híbridos, lo que le permite comprender en profundidad los principios y marcos de referencia de Confianza Cero (*Zero*

Trust), además, se cuenta con las competencias necesarias para aplicar metodologías de análisis comparativo, revisión documental y evaluación técnica de arquitecturas de seguridad.

El desarrollo del estudio no requiere infraestructura física ni laboratorios, ya que se fundamenta, en forma exclusiva, en análisis documental, revisión bibliográfica especializada de marcos normativos como (NIST SP 800-207) y documentación técnica de los principales proveedores y organismos internacionales, en este caso si se requieren validaciones o simulaciones conceptuales, se podrán realizar utilizando herramientas que sean de software libre o entornos virtualizados, lo cual está dentro de las capacidades y recursos del investigador.

Por lo tanto, desde el punto de vista técnico, el investigador dispone del conocimiento, los medios digitales y los recursos informáticos necesarios para ejecutar con solvencia todas las fases del trabajo.

1.4.2 Punto de Vista Operativo

Desde el punto de vista operativo, la investigación no interfiere con las actividades regulares de ninguna organización, ya que no implica intervención directa en sistemas productivos ni la modificación de infraestructuras reales, el proyecto se desarrolla de forma documental y analítica, basándose en fuentes confiables y en la recopilación de información de dominio público o académico.

En caso de requerirse información adicional o entrevistas con profesionales del sector, estas se podrán coordinar de manera remota, sin afectar la operación de las entidades participantes, asimismo, y de ser necesario, como investigador se dispondría del tiempo, los medios de comunicación y los espacios necesarios para realizar las actividades de recolección y análisis de información.

1.4.3 Punto de Vista Económico

El Trabajo Final de Graduación es económicamente viable, ya que no requiere de una inversión significativa en infraestructura ni en licenciamiento de ningún tipo de software, la mayor parte de los costos corresponde al tiempo de

dedicación del investigador y al uso de recursos computacionales personales, acceso a bases de datos académicas, herramientas ofimáticas disponibles en el entorno universitario y conexión a internet.

En caso de requerirse herramientas de modelado o de análisis comparativo, se utilizarán alternativas de software libre o versiones académicas sin costo adicional, por esta razón, el costo total del proyecto se considera un “costo teórico” asumido por el propio investigador, que cubre principalmente su tiempo, esfuerzo y acceso a recursos digitales necesarios para la elaboración del trabajo.

En consecuencia, la investigación es plenamente viable en términos técnicos, operativos y económicos, garantizando su ejecución dentro del marco temporal y de recursos definidos por la maestría.

1.5 Objetivos

1.5.1 Objetivo General

Realizar un análisis comparativo de los principales marcos de trabajo de Confianza Cero (*Zero Trust*), con el propósito de identificar sus similitudes, diferencias, fortalezas y limitaciones en el contexto de entornos laborales híbridos, con el fin de proponer criterios técnicos y estratégicos que orienten su adopción efectiva en organizaciones que combinan operaciones presenciales y remotas.

1.5.2 Objetivos Específicos

- Examinar los fundamentos conceptuales y arquitectónicos del modelo de Confianza Cero, incluyendo sus principios, componentes esenciales y lineamientos técnicos establecidos por los principales marcos de referencia.
- Describir las características, alcances y enfoques de implementación de los marcos de trabajo más representativos (NIST SP 800-207, Forrester ZTX, Microsoft *Zero Trust*, MITRE *Zero Trust* Architecture Playbook y Google BeyondCorp), destacando su aplicabilidad en diferentes tipos de infraestructura tecnológica.
- Comparar los marcos de trabajo seleccionados mediante criterios objetivos como nivel de madurez, orientación tecnológica, cobertura de controles, facilidad de integración y compatibilidad con entornos híbridos.
- Identificar los desafíos y oportunidades asociados con la adopción del modelo de Confianza Cero en escenarios híbridos, considerando aspectos de seguridad, usabilidad, costo y gobernanza.
- Proponer un conjunto de criterios o lineamientos prácticos que sirvan como guía para la selección e implementación de marcos de Confianza Cero en organizaciones que operan bajo esquemas de trabajo híbrido.

1.6. Alcances y Limitaciones

El presente apartado tiene como propósito delimitar los productos y resultados que se entregarán como parte del Trabajo Final de Graduación, así como establecer con claridad aquellos elementos que quedan fuera del alcance de la investigación. Con esto se busca evitar interpretaciones erróneas y garantizar una expectativa realista sobre los resultados del estudio.

1.6.1 Alcances

El proyecto comprenderá los siguientes alcances:

- Documento académico final: Se elaborará un documento técnico y científico que contenga el análisis comparativo de los principales marcos de trabajo de Confianza Cero (*Zero Trust*) aplicables a entornos laborales híbridos, conforme a las normas y lineamientos institucionales del Trabajo Final de Graduación.
- Matriz comparativa de marcos *Zero Trust*: Se desarrollará una matriz estructurada que evalúe y contraste los marcos NIST SP 800-207, Forrester ZTX, Microsoft *Zero Trust*, MITRE *Zero Trust* Architecture Playbook y Google BeyondCorp, considerando criterios como principios, arquitectura, madurez, aplicabilidad tecnológica y compatibilidad con entornos híbridos.
- Propuesta de lineamientos de adopción: Se entregará un conjunto de criterios técnicos y estratégicos que sirvan como guía de referencia para la selección e implementación del modelo de Confianza Cero en organizaciones con esquemas de trabajo híbrido.
- Informe de resultados y conclusiones: El documento final incluirá un análisis interpretativo de los hallazgos, las conclusiones derivadas del estudio y recomendaciones aplicables a nivel organizacional y estratégico.
- Presentación de defensa académica: Se elaborará una presentación oral y visual (diapositivas o exposición) para la defensa del TFG ante el comité evaluador, en la que se sintetizarán los principales resultados, hallazgos y aportes del trabajo.

1.6.2 Limitaciones

El proyecto no incluirá los siguientes elementos:

- Implementación práctica o técnica de los marcos de Confianza Cero en infraestructuras reales, laboratorios o entornos corporativos, el estudio se limita al análisis documental y conceptual.
- Evaluación de desempeño o pruebas de seguridad sobre plataformas, soluciones o herramientas comerciales vinculadas con *Zero Trust*.
- Desarrollo de software, aplicaciones o prototipos asociados a la adopción del modelo de Confianza Cero.
- Análisis financiero detallado de costos de implementación o retorno de inversión de los marcos de trabajo evaluados.
- Capacitaciones, talleres o ciclos de formación dirigidos a personal técnico o usuarios finales; el alcance se limita a la elaboración del documento académico y sus productos analíticos.
- Revisión exhaustiva de todos los marcos existentes sobre *Zero Trust*; el estudio se enfoca en los cinco marcos más representativos a nivel internacional.

1.7 Revisión de la literatura

1.7.1 Revisión sistemática

La revisión sistemática en este trabajo se centra en el paradigma de las arquitecturas de Confianza Cero (*Zero Trust* Architectures, ZTA) como modelo prevalente en ciberseguridad, abordando tanto su fundamento teórico como su aplicación práctica en entornos híbridos y multicloud, se seleccionaron como fuentes primarias los documentos de National Institute of Standards and Technology (NIST SP 800-207, 2020), MITRE Corporation (Informe "*Zero Trust* Architectures: Are We There Yet?", 2021), Microsoft Corporation ("*Zero Trust* Vision Paper", 2021) y el artículo de Forrester "The Definition of Modern *Zero Trust*" (2022), estas fuentes, reconocidas por su autoridad en el ámbito de la ciberseguridad, aportan un enfoque integral: normativo, estratégico, corporativo y analítico, la revisión sistemática busca extraer, comparar y sintetizar los principios clave, los componentes arquitectónicos y los retos de adopción del modelo, así como identificar los vacíos y debates emergentes en el estado de la cuestión.

1.7.2 Estado de la cuestión

En el contexto actual de la ciberseguridad, los modelos tradicionales basados en perímetros fijos y confianza implícita han demostrado ser insuficientes frente al incremento de amenazas avanzadas, la proliferación de dispositivos móviles, la adopción de la nube y el teletrabajo, el documento de NIST SP 800-207 define la ZTA como un enfoque que “niega la confianza implícita en toda entidad (usuario, dispositivo, red, carga de trabajo), y requiere verificación continua, mínimo privilegio y segmentación” (NIST, 2020), por su parte, MITRE analiza que la adopción de *Zero Trust* se está acelerando, pero muchas organizaciones aún no alcanzan niveles de madurez elevados, debido a desafíos de gobernanza, interoperabilidad y visibilidad, Microsoft, en su visión, propone seis pilares para la implementación operacional: identidades, dispositivos, redes, aplicaciones, datos e infraestructura, articulados a través de un modelo de madurez que define grados de transición (tradicional > avanzado > óptimo).

En el artículo de Forrester actualiza el marco conceptual bajo el título “The Definition of Modern *Zero Trust*”, indicando que *Zero Trust* “es un modelo de seguridad de la información que niega el acceso a aplicaciones y datos por defecto, la prevención de amenazas se logra otorgando accesos únicamente mediante políticas informadas por una verificación continua, contextual y basada en riesgo entre usuarios y sus dispositivos.” (Forrester, 2022). En su definición, Forrester resume tres principios: entidades no confiables por defecto; mínimo privilegio; y monitoreo de seguridad comprensivo, esta definición, según Forrester, no difiere de la de NIST, pero refuerza el carácter dinámico e integral del paradigma.

En conjunto, el estado de la cuestión señala que: 1) existe un consenso cada vez mayor sobre los principios de *Zero Trust*; 2) los retos prácticos siguen siendo significativos (por ejemplo, en la articulación de políticas granulares, la integración de tecnologías y la madurez organizacional); 3) la narrativa se ha expandido desde el ámbito técnico hacia el estratégico y operacional; y (4) aunque el modelo promete mayor resiliencia y control, aún es objeto de debate sobre su implementación, costes y métricas de éxito.

1.8 Planificación de la revisión

1.8.1 Formulación de la pregunta

La pregunta de investigación que guía esta revisión es la siguiente: ¿Cuáles son los fundamentos teóricos, arquitectónicos y prácticos que sustentan el modelo de Confianza Cero según los marcos de referencia del NIST, MITRE, Microsoft y Forrester, y cómo contribuyen a la consolidación de un enfoque integral de ciberseguridad para entornos híbridos?

Esta pregunta permite articular múltiples dimensiones: la conceptualización del paradigma, su estructuración arquitectónica y su aplicación en contextos reales, asimismo, permite contrastar perspectivas normativas, analíticas y corporativas.

1.8.2 Foco de la pregunta

El foco de la revisión se orienta hacia tres ejes principales:

- El **modelo conceptual** de *Zero Trust*: sus principios (por ejemplo “never trust, always verify”, mínimo privilegio, asunción de compromiso) y su evolución a través del tiempo.
- La **arquitectura y componentes técnicos** que facilitan su implementación: motor de políticas, puntos de decisión/aplicación, segmentación, verificación continua, etc.
- Las **estrategias de adopción y madurez organizacional**, que abarcan desde el viaje evolutivo de las organizaciones hasta los desafíos operativos y culturales que enfrentan, este enfoque permite profundizar en cómo los marcos seleccionados abordan cada eje y qué convergencias o divergencias emergen entre ellos.

1.8.3 Amplitud y calidad de la pregunta

La amplitud de esta pregunta está justificada por la necesidad de abarcar tanto la parte teórica como la práctica del paradigma *Zero Trust*, asegurando que el análisis no se quede únicamente en aspectos técnicos sino que también incorpore dimensiones estratégicas y organizacionales, las fuentes seleccionadas son recientes (2020-2022) y provienen de instituciones

reconocidas, lo que garantiza la calidad y relevancia de los datos, además, la pregunta está bien delimitada para un TFG: no es excesivamente amplia (por ejemplo “todos los modelos de seguridad”) ni demasiado restrictiva (no se reduce solo a “dispositivos móviles”), lo cual permite un análisis profundo pero manejable.

1.8.4 Identificación de fuentes

Para esta revisión se seleccionaron cuatro fuentes principales:

- NIST SP 800-207 (2020), que proporciona una base normativa y arquitectónica para *Zero Trust*.
- MITRE “*Zero Trust* Architectures: Are We There Yet?” (2021), que analiza la madurez organizacional y los retos de implementación.
- Microsoft “*Zero Trust* Vision Paper” (2021), que presenta un marco de madurez aplicada y los seis pilares del modelo.
- Forrester “The Definition of Modern *Zero Trust*” (2022), que actualiza la definición del paradigma y lo posiciona como un modelo de seguridad de la información dinámico y centrado en riesgo, estas fuentes fueron seleccionadas por su alta autoridad, su enfoque relevante para el tema de estudio, su actualidad y su diversidad de perspectivas (normativa, analítica, corporativa), la búsqueda incluyó revisión de bases de datos académicas, portales de instituciones de estándares, blogs de analistas reconocidos y documentos corporativos públicos.

1.8.5 Ejecución de la Revisión

La ejecución de la revisión se llevó a cabo mediante un proceso de análisis comparativo y sintético de las cuatro fuentes, con las siguientes fases: en primer lugar, se extrajeron las definiciones explícitas de *Zero Trust* y sus principios fundamentales; en segundo lugar, se identificaron los componentes arquitectónicos y los dominios técnicos de cada marco; en tercer lugar, se investigaron los modelos de adopción y madurez propuestos, así como los desafíos y beneficios reportados; finalmente, se contrastaron las convergencias y divergencias entre las fuentes para construir un panorama integrado, por ejemplo, NIST SP 800-207 define claramente los componentes lógicos (Policy Engine, Policy Administrator, Policy Enforcement Point) y describe tres enfoques

de implementación (identidad, microsegmentación, perímetros definidos por software), MITRE amplía el análisis hacia la madurez empresarial y los problemas de gobernanza, señalando que muchas organizaciones aún están en fases iniciales, Microsoft articula los seis pilares (identidades, dispositivos, redes, aplicaciones, datos, infraestructura) y propone un viaje en tres niveles de madurez, Forrester, por su parte, sintetiza el modelo como uno que “niega el acceso por defecto”, “otorga acceso solo mediante políticas basadas en verificación continua y contexto” y subraya que las entidades no confiadas por defecto, el mínimo privilegio y el monitoreo completo con los tres principios clave.

La comparación revela que pese a diferencias de enfoque (normativo vs. corporativo vs. analítico), existe una alta convergencia en los principios básicos y en la dirección del modelo, sin embargo, también emergen brechas: la definición práctica de métricas de éxito, la interoperabilidad de tecnologías, la cultura organizacional y la escalabilidad en entornos multinube, esta revisión sistemática, por tanto, proporciona un andamiaje conceptual y crítico para el TFG, que podrá apoyarse en estos hallazgos para formular hipótesis, construir el marco teórico y plantear futuras líneas de investigación.

Capítulo 2. Marco Teórico o Conceptual

2.1 Introducción al paradigma de Confianza Cero

El concepto de Confianza Cero (*Zero Trust*) representa una transformación profunda en la concepción tradicional de la ciberseguridad, en oposición de los modelos de defensa perimetral, en los que se asumía que los usuarios y dispositivos dentro de la red eran inherentemente confiables, la filosofía de ZT parte del principio de que ningún usuario, dispositivo o flujo de información debe considerarse confiable por defecto, independientemente de su ubicación dentro o fuera del perímetro corporativo, esta visión fue sistematizada por el Instituto Nacional de Estándares y Tecnología (NIST) en la publicación SP 800-207, donde se define la Arquitectura de Confianza Cero (*Zero Trust* Architecture, ZTA) como un conjunto de principios y modelos de seguridad destinados a minimizar la exposición al riesgo y prevenir el movimiento lateral de

amenazas dentro de la red. en este modelo, cada intento de acceso a un recurso requiere autenticación, autorización y evaluación continua de riesgos.

La adopción de este enfoque responde a los cambios estructurales en la operación tecnológica moderna y el crecimiento de la computación en la nube, la movilidad laboral, el auge del teletrabajo, la expansión del Internet de las Cosas (IoT) y el uso de entornos híbridos y multicloud en donde estas dinámicas han diluido los perímetros de red tradicionales, haciendo necesaria una arquitectura más dinámica, centrada en los activos y en la identidad, como propone la Confianza Cero.

2.2 Principios Fundamentales de la Arquitectura de Confianza Cero

Los fundamentos conceptuales de la Arquitectura de Confianza Cero (*Zero Trust* Architecture, ZTA) se basan en la redefinición del modelo tradicional de seguridad, desplazando la protección desde los perímetros estáticos hacia los activos, identidades y datos, la NIST SP 800-207 establece tres principios que sustentan toda la filosofía *Zero Trust*:

- **Nunca confiar, siempre verificar (Never Trust, Always Verify):**

Este principio sostiene que toda solicitud de acceso debe ser verificada sin importar su procedencia, no se debe asumir confianza ni siquiera dentro de la red interna, cada conexión, usuario, dispositivo o aplicación debe autenticarse y autorizarse dinámicamente con base en múltiples factores: identidad, contexto, localización, salud del dispositivo y nivel de riesgo, la confianza se convierte en una variable dinámica y contextual, y no en una condición permanente, este principio es el eje central que elimina la suposición tradicional de que “dentro de la red es seguro”.

- **Acceso con privilegios mínimos (Least Privilege Access):**

La ZTA restringe el acceso a los recursos de acuerdo con la estricta necesidad operativa. Se limita cada solicitud de acceso al mínimo nivel de permisos que requiere para su función, esto implica aplicar controles de acceso granulares, basados en atributos (ABAC), roles (RBAC), y políticas dinámicas

que se ajustan según el comportamiento y contexto de cada usuario o dispositivo, tal enfoque minimiza el impacto de cuentas comprometidas y reduce el riesgo de movimientos laterales dentro de la red, uno de los problemas más comunes en las arquitecturas perimetrales.

- **Asumir compromiso (Assume Breach):**

Bajo este principio, la organización parte de la premisa de que su entorno ya ha sido vulnerado o que puede serlo en cualquier momento. Por lo tanto, la estrategia se centra en la contención, detección y respuesta rápida, mediante segmentación de red, monitoreo continuo y cifrado integral, las acciones se dirigen a reducir el radio de impacto (blast radius), empleando microsegmentación, telemetría avanzada, inteligencia artificial (IA) y análisis de comportamiento.

De forma complementaria, MITRE (2021) y Microsoft (2021) también añaden otros principios de implementación como la evaluación continua del riesgo, la automatización de políticas y la visibilidad completa del entorno, garantizando una postura de seguridad adaptativa y proactiva

2.3 Componentes y Dominios Conceptuales del Modelo

La ZTA se articula en torno a seis dominios o pilares que conforman el ecosistema de control integral, propuestos por Microsoft y alineados con los principios de NIST y MITRE, cada dominio funciona como una fuente de señal, un plano de control y un recurso a defender.

- **Identidades**

Las identidades (humanas y/o no humanas (servicios, procesos, IoT) son el punto de partida del modelo, se establece un plano de control de identidad (Identity Control Plane) donde cada identidad se valida mediante autenticación multifactor (MFA), biometría, tokens de acceso, credenciales federadas o autenticación sin contraseñas, aquí, el objetivo es garantizar que solo las identidades verificadas y autorizadas accedan a recursos específicos bajo políticas de privilegios mínimos. Microsoft enfatiza que las identidades son la base del modelo *Zero Trust*, dado que representan la frontera de control más crítica.

- **Dispositivos**

Los dispositivos constituyen el segundo nivel de control. Cada endpoint (corporativo, personal (BYOD), IoT o servidor virtual) debe cumplir con los criterios de seguridad establecidos, como: parches actualizados, cifrado de disco, antivirus activo y postura de cumplimiento conforme a las políticas de la organización, como tal, MITRE sugiere incluir controles de evaluación de postura del dispositivo (device posture checks) y gestión unificada de *Endpoints* (UEM), asegurando que los dispositivos comprometidos o no gestionados sean bloqueados automáticamente.

- **Redes**

En la ZTA, la red deja de ser un perímetro confiable y se convierte en un canal cifrado y monitoreado, se aplican mecanismos como la microsegmentación, el control de tráfico este-oeste, y el Software Defined Perimeter (SDP) para limitar la comunicación entre zonas o recursos sensibles, además, toda la comunicación se cifra de extremo a extremo con protocolos como TLS y VPNs de acceso restringido, manteniendo visibilidad total del tráfico mediante monitoreo y análisis de paquetes.

- **Aplicaciones**

Las aplicaciones son el medio por el cual los usuarios acceden y manipulan datos, el modelo *Zero Trust* impone políticas para controlar el acceso, auditar el comportamiento del usuario y validar configuraciones seguras, incluso en entornos SaaS, PaaS o IaaS, también se promueve la detección de Shadow IT, el control de permisos in-app y el uso de API seguras y cifradas.

- **Datos**

El objetivo último del modelo es proteger los datos, independientemente de su ubicación o medio de almacenamiento, esto requiere clasificación, etiquetado y cifrado automático, junto con políticas de prevención de pérdida de datos (DLP) y acceso condicional basado en sensibilidad (ABAC), en este sentido, NIST destaca que el recurso de protección no es la red, sino los activos de información.

- **Infraestructura y Operaciones**

La infraestructura (ya sea física, virtual, o en la nube) debe contar con políticas de just-in-time access (JIT), gestión de configuración y visibilidad en tiempo real, las operaciones de seguridad adaptativas se logran mediante la integración de sistemas SOAR y SIEM, analítica avanzada y respuesta automática a incidentes.

2.4 Modelos de Referencia y Madurez

El modelo de madurez *Zero Trust* desarrollado por Microsoft es una herramienta conceptual que ayuda a las organizaciones a evaluar su nivel de adopción y planificar la transición hacia una ZTA completa

2.5 El modelo describe tres niveles evolutivos:

- Tradicional:

En este nivel, la seguridad depende de la infraestructura local (on-premises), con políticas estáticas, redes planas y autenticación básica, las organizaciones poseen visibilidad limitada sobre identidades, dispositivos y comportamiento del usuario.

- Avanzado:

Se incorporan identidades híbridas (federación entre AD y Azure AD), segmentación parcial de redes y controles de acceso condicional, se comienza a emplear analítica para evaluar riesgos y aplicar políticas dinámicas.

- Óptimo:

Representa la madurez plena de *Zero Trust*, las decisiones de acceso son totalmente contextuales y automatizadas, los datos están protegidos por cifrado integral, se aplica microsegmentación profunda, y los incidentes se detectan y responden automáticamente mediante IA y telemetría unificada.

De forma paralela, MITRE (2021) propone una arquitectura de referencia que destaca la integración entre múltiples tecnologías (ICAM, SOAR, segmentación y analítica), subrayando que ZTA es un marco estratégico, no un producto comercial, ambas visiones coinciden en que la adopción requiere madurez tecnológica y liderazgo institucional.

2.6 Enfoque Arquitectónico según NIST

El NIST, en su SP 800-207, muestra una arquitectura de referencia compuesta por elementos lógicos interconectados, que definen la forma en que se aplican las políticas de confianza cero:

- Motor de Políticas (Policy Engine, PE):

La cual evalúa las solicitudes de acceso según políticas, contexto y fuentes de datos confiables.

- Administrador de Políticas (Policy Administrator, PA):

Encargada de coordina la aplicación de las decisiones del PE y actualiza las reglas en tiempo real.

- Puntos de Aplicación de Políticas (Policy Enforcement Points, PEP):

En donde actúan como barreras dinámicas que permiten o deniegan el acceso al recurso según las decisiones del PE.

- Fuentes de datos de confianza:

Se incluyen repositorios de identidad, catálogos de activos, monitoreo de dispositivos, auditorías, registros y telemetría.

La NIST además establece tres variantes de implementación de la ZTA:

- Basada en identidad (Identity Governance): centrada en ICAM y autenticación fuerte.
- Basada en microsegmentación: usa software-defined networks para dividir la red en zonas seguras.
- Basada en perímetros definidos por software (SDP): se aplican políticas virtuales según usuarios, recursos y contexto.

El modelo de NIST enfatiza que la ZTA no reemplaza los sistemas perimetrales, sino que coexiste y evoluciona junto a ellos, mediante una migración progresiva que equilibre seguridad y continuidad operativa

2.7 Síntesis Conceptual

El paradigma de Confianza Cero constituye un cambio radical en la gestión de la ciberseguridad moderna, al pasar de un enfoque reactivo y perimetral a un modelo proactivo, continuo y centrado en la identidad, de la integración de los tres marcos (NIST, Microsoft y MITRE) surge una visión unificada:

- NIST aporta la base teórica y arquitectónica, definiendo principios, componentes y modelos de implementación.

- Microsoft traduce estos principios en un modelo de madurez operativo, aplicable a entornos híbridos y multicloud.

- MITRE ofrece una perspectiva estratégica y pragmática, centrada en la integración tecnológica y los desafíos reales de adopción.

En conjunto, estos enfoques delinean un marco conceptual robusto, sustentado en la verificación continua, la automatización, la segmentación inteligente y la gobernanza dinámica de acceso, elementos esenciales para lograr entornos seguros, resilientes y sostenibles frente a las amenazas cibernéticas contemporáneas.


Modelos
API
PaaS
SOAR
VPN
Azure AD
SP 800-207
SIEM
Google BeyondCorp
Redes
blast
Zero Trust
ZTX
TLS
radius
IoT
Dispositivos
SaaS
Forrester
NIST
federación
ZTA
BYOD
datos
identidades
ABAC
AD
Playbook
JIT
Microsoft
aplicaciones
MITRE
RBAC

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

El presente Trabajo Final de Graduación se enmarca dentro de una investigación de tipo descriptiva y comparativa, ya que busca analizar de manera detallada los marcos teóricos, arquitectónicos y estratégicos del modelo *Zero Trust* propuestos por NIST, MITRE, Microsoft y Forrester, es descriptiva porque documenta, caracteriza y explica los principios, componentes, estructuras y directrices de cada marco, también es comparativa, debido a que establece similitudes, diferencias y convergencias entre las propuestas, con el fin de construir un análisis integral que permita comprender la evolución y tendencias del modelo *Zero Trust* en entornos híbridos, adicionalmente, se considera una investigación documental, dado que se basa exclusivamente en la revisión, análisis y síntesis de fuentes primarias oficiales (NIST SP 800-207, MITRE Tech Watcher, Microsoft Zero Trust Vision Paper y el artículo de Forrester “The Definition of Modern *Zero Trust*”), sin recurrir a estudios de campo o experimentación directa.

3.2 Alcance Investigativo

El alcance de esta investigación es analítico-explicativo, ya que no solo describe los marcos *Zero Trust*, sino que también expone sus fundamentos conceptuales, justificaciones técnicas y recomendaciones prácticas, este nivel de alcance permite examinar cómo los principios de “nunca confiar, siempre verificar”, mínimo privilegio y verificación continua se operacionalizan en cada marco analizado, el alcance analítico permite profundizar en temas como los componentes arquitectónicos definidos por NIST (PE, PA, PEP), los seis pilares propuestos por Microsoft para entornos híbridos, el análisis de madurez y desafíos operacionales identificados por MITRE, así como la modernización conceptual planteada por Forrester, el alcance explicativo permite interpretar cómo estas visiones convergen hacia un modelo unificado de seguridad moderna y cómo contribuyen a la formulación de una propuesta comparativa válida para entornos de trabajo híbrido.

3.3 Enfoque

El enfoque metodológico adoptado es cualitativo, dado que el análisis se centra en la interpretación de documentos, marcos conceptuales, lineamientos técnicos y perspectivas estratégicas, este enfoque permite profundizar en el contenido de las fuentes y comprender las ideas, principios y modelos que sustentan la arquitectura de Confianza Cero, el análisis cualitativo se basa en la extracción y categorización de información textual relevante de los documentos oficiales, permitiendo identificar patrones, conceptos recurrentes, convergencias teóricas y diferencias significativas entre las propuestas de NIST, MITRE, Microsoft y Forrester, no se utilizan métricas numéricas ni análisis estadísticos, ya que el estudio está guiado por la comprensión conceptual más que por mediciones cuantitativas.

3.4 Diseño

El diseño de investigación es no experimental, transeccional y de análisis documental comparativo, se considera no experimental porque no manipula variables, sino que estudia fenómenos existentes a partir de su documentación, es transeccional porque se realiza en un único momento temporal, recopilando fuentes en un periodo determinado (2020–2022), asimismo, el diseño es documental y comparativo, ya que el estudio se basa en documentos oficiales que establecen marcos de referencia ampliamente aceptados en la industria, la comparación estructurada entre estos marcos permite identificar criterios, principios y recomendaciones relevantes para el desarrollo de una propuesta de análisis aplicable al entorno híbrido, este diseño facilita la comprensión de cómo diversos organismos y actores tecnológicos conceptualizan y operacionalizan el modelo *Zero Trust*.

3.5 Población y Muestreo

La población teórica corresponde a todos los documentos, normas, marcos de referencia y literatura científica relacionada con el modelo *Zero Trust*, dentro de esta población amplia, se seleccionó una muestra intencional y no

probabilística, integrada por fuentes consideradas representativas y de alta autoridad en la materia, la muestra está compuesta por:

- NIST SP 800-207 (2020): marco normativo estándar reconocido a nivel global.
- MITRE *Zero Trust* Architectures (2021): análisis estratégico y de madurez organizacional.
- Microsoft *Zero Trust* Vision Paper (2021): guía corporativa basada en seis pilares para entornos híbridos.
- Forrester "The Definition of Modern *Zero Trust*" (2022): actualización conceptual del paradigma, este muestreo intencional garantiza calidad, profundidad conceptual y relevancia directa al objeto de estudio, al seleccionar documentos con impacto significativo en la adopción del modelo *Zero Trust* a nivel global.

3.6 Instrumentos de Recolección de Datos

Los instrumentos utilizados para la recolección de datos fueron de naturaleza documental y analítica. Entre ellos destacan:

- **Fichas de lectura:** empleadas para registrar ideas principales, citas relevantes y conceptos clave presentes en cada documento analizado.
- **Matrices comparativas:** utilizadas para contrastar principios, componentes arquitectónicos, modelos de madurez y recomendaciones de implementación entre las cuatro fuentes.
- **Análisis de contenido:** para identificar categorías emergentes, relaciones conceptuales, definiciones y patrones comunes.
- **Revisión sistemática:** que permitió estructurar el proceso de búsqueda, selección y análisis de las fuentes de manera organizada y trazable, estos instrumentos aseguran un análisis riguroso y coherente, permitiendo construir una visión sólida y fundamentada del estado de la cuestión en *Zero Trust*.

3.7 Técnicas de Análisis de Información

Las técnicas principales empleadas en este estudio fueron las siguientes:

3.7.1 Análisis de contenido

Permite examinar los documentos identificando categorías clave como principios fundamentales, componentes arquitectónicos, enfoques de implementación y retos operativos. Se aplicó de forma inductiva y deductiva, combinando la identificación de patrones emergentes con la verificación de categorías teóricas preexistentes.

3.7.2 Triangulación teórica

Consiste en contrastar las propuestas de NIST, MITRE, Microsoft y Forrester para identificar convergencias y divergencias, esta técnica fortalece la validez interna del análisis comparativo y permite una interpretación multidimensional del modelo *Zero Trust*.

3.7.3 Síntesis integradora

Se empleó para consolidar los hallazgos de la revisión sistemática en un cuerpo teórico coherente que sirva como base para la formulación de la propuesta investigativa del TFG, esta síntesis permitió unificar perspectivas normativas, corporativas y analíticas en un marco conceptual consolidado.

3.8 Estrategia de Desarrollo de la Propuesta

La estrategia metodológica para desarrollar la propuesta comparativa del TFG se basa en cuatro fases:

Fase 1: Revisión documental profunda

Incluye el análisis detallado de los documentos de NIST, MITRE, Microsoft y Forrester, así como la revisión sistemática y el estado de la cuestión elaborados previamente, esta fase asegura una comprensión integral del fenómeno *Zero Trust*.

Fase 2: Construcción de matriz comparativa

Se elaborará una matriz de contraste que incluya principios, componentes arquitectónicos, modelos de madurez, enfoques de implementación, fortalezas, limitaciones y desafíos identificados en cada marco, esta matriz constituirá el núcleo del análisis comparativo.

Fase 3: Análisis crítico y síntesis

Sobre la base de la matriz comparativa, se realizará un análisis crítico que permita identificar:

- Coincidencias entre los marcos de referencia.
- Diferencias significativas en enfoque o alcance.
- Elementos complementarios que fortalecen la visión integral de *Zero Trust*.
- Oportunidades de adaptación del paradigma al contexto de entornos híbridos.

Fase 4: Formulación de la propuesta final

Con los hallazgos del análisis, se elaborará una propuesta teórico-conceptual que describa el modelo comparativo de *Zero Trust* como marco de referencia aplicable a organizaciones con ecosistemas híbridos, la propuesta integrará principios, lineamientos y recomendaciones surgidas de las cuatro fuentes analizadas.

Capítulo 4. Análisis del Diagnóstico

4.1 Introducción al Análisis Comparativo

El presente capítulo constituye el núcleo analítico de la investigación, donde se despliega el diagnóstico detallado de la revisión documental ejecutada en las fases previas, el propósito fundamental de esta sección es trascender la descripción individual de los marcos de referencia seleccionados (NIST SP 800-207, Microsoft *Zero Trust* Vision, MITRE's *Zero Trust* Architectures y el modelo Forrester *Zero Trust Extended* (ZTX)) para integrarlos en una evaluación comparativa rigurosa, En un contexto donde las organizaciones modernas operan mayoritariamente en ecosistemas híbridos, la adopción de un modelo de "talla única" resulta insuficiente; por tanto, este análisis busca construir cada propuesta para entender sus orígenes lógicos, sus implicaciones operativas y su viabilidad técnica real.

Para lograr este objetivo, se ha aplicado una metodología de triangulación de datos que permite contrastar las visiones teóricas (representadas principalmente por el estándar del NIST) con las aproximaciones pragmáticas y

comerciales (lideradas por Microsoft y Forrester), filtradas por la visión de realidad operativa que aporta MITRE, el diagnóstico se estructura en las cuatro dimensiones críticas en que se divide el paradigma: los principios rectores que definen la filosofía de seguridad, la arquitectura lógica y sus dominios de protección, los modelos de madurez que guían la evolución organizacional y, finalmente, la adaptabilidad específica de cada marco a los desafíos inherentes de los entornos híbridos, este enfoque multidimensional permite identificar no solo las convergencias conceptuales, sino también las brechas instrumentales que deben ser subsanadas para una implementación exitosa.

4.2 Análisis de la Dimensión 1: Principios Rectores

Al analizar los axiomas fundamentales que sustentan cada marco, se observa una convergencia filosófica hacia la eliminación de la confianza implícita, aunque la articulación de estos principios varía significativamente en función del público objetivo de cada documento, el estándar NIST SP 800-207 establece una base doctrinal exhaustiva compuesta por siete principios técnicos, este *framework* define que "todos los orígenes de datos y servicios de computación se consideran recursos", lo que implica una atomización de la seguridad que va más allá de los servidores tradicionales para incluir dispositivos IoT y microservicios, además, NIST es enfático en que "el acceso a los recursos individuales se concede por sesión", eliminando la persistencia de credenciales que tradicionalmente permitía el movimiento lateral de atacantes, esta granularidad teórica es vital para el cumplimiento normativo, pues obliga a una evaluación continua y dinámica del estado de seguridad de cada activo antes de otorgar acceso.

En contraste, la visión de Microsoft sintetiza esta complejidad doctrinal en tres mandatos operativos diseñados para ser consumibles por directores de seguridad (CISO) y equipos de TI: "Verificar explícitamente", "Usar acceso de privilegios mínimos" y "Asumir la brecha", mientras que el NIST describe el QUÉ (la condición técnica), Microsoft describe el CÓMO (la acción estratégica), por ejemplo, el principio de "Asumir la brecha" de Microsoft no es simplemente una postura pesimista, sino una directriz de diseño arquitectónico que obliga a segmentar redes y cifrar datos preventivamente, asumiendo que el perímetro ya

ha sido comprometido, Por su parte, Forrester, pionero del concepto, aporta principios centrados en la estrategia de datos, como el "Default Deny" (negar por defecto) y la centralidad de los datos, argumentando que la red es meramente un transporte hostil y que la seguridad debe viajar con el dato mismo, independientemente de dónde resida.

Por su parte MITRE añade una capa de realismo crítico a estos principios, su análisis sugiere que, si bien los principios de "nunca confiar, siempre verificar" son ideales, su aplicación rígida en infraestructuras heredadas (*legacy*) puede paralizar la operatividad del negocio, por ello, MITRE aboga por una interpretación resiliente de los principios, donde la confianza cero no es un interruptor binario, sino un gradiente de reducción de riesgo. El análisis comparativo revela que, para un entorno híbrido, la rigurosidad del NIST proporciona la métrica de auditoría necesaria, mientras que los principios de Microsoft ofrecen la hoja de ruta cultural y operativa para gestionar el cambio, siendo ambas visiones complementarias y no excluyentes entre sí.

Tabla 1. Comparación de marcos Zero Trust

Marco	Principios	Pilares	Enfoque Arquitectónico	Modelo de Madurez
NIST SP 800-207	Autenticación continua, mínimo privilegio, protección de recursos	Identidad, dispositivo, red, aplicación, datos, cargas de trabajo	Arquitectura lógica con PDP/PEP, microsegmentación	No define niveles, orienta migración gradual
MITRE	Evaluación de madurez, segmentación, gobernanza	Identidad, activos, políticas, monitoreo	Modelo basado en riesgos y madurez	Define etapas: incipiente, intermedio, avanzado
Microsoft	Modelo de seis pilares, telemetría, automatización	Identidades, dispositivos, aplicaciones, datos, infraestructura, redes	Modelo de madurez progresivo	Tres niveles: Tradicional, Avanzado, Óptimo
Forrester	Desperimetrización, control granular, confianza adaptativa	Usuarios, dispositivos, redes, aplicaciones, datos	Marco conceptual orientado a políticas	Conceptual, sin niveles formales

Figura 1: Tabla de comparación de marcos

Fuente: confección propia

4.3 Análisis de la Dimensión 2: Arquitectura Lógica y Componentes

La arquitectura lógica es donde las diferencias entre los marcos se hacen más tangibles, separándose entre modelos funcionales y modelos basados en dominios, la NIST SP 800-207 propone una abstracción puramente funcional que divide la arquitectura en dos planos: el Plano de Control y el Plano de Datos, en el centro de este modelo se encuentra el Punto de Decisión de Políticas (PDP), que actúa como el "cerebro" que evalúa las solicitudes, y el Punto de Aplicación

de Políticas (PEP), que actúa como el "músculo" que permite o deniega el tráfico, esta separación es la piedra angular para los entornos híbridos, ya que permite desacoplar la toma de decisiones (que puede estar centralizada en la nube) de la ejecución (que puede estar distribuida en firewalls locales, agentes en dispositivos o pasarelas web).

Por otro lado, Microsoft y Forrester estructuran sus arquitecturas en torno a "pilares" o dominios de protección, el modelo de Microsoft organiza la defensa en seis áreas técnicas: Identidad, *Endpoints* (dispositivos), Datos, Aplicaciones, Infraestructura y Red, esta taxonomía es altamente pragmática porque se alinea directamente con categorías de productos de seguridad existentes en el mercado como: IAM, EDR, DLP, etc., la identidad, en particular, es elevada por Microsoft a la categoría de "nuevo perímetro", actuando como el plano de control unificado que el NIST describe teóricamente.

El modelo ZTX (*Zero Trust Extended*) de Forrester amplía aún más este espectro al integrar explícitamente la "Automatización y Orquestación" y la "Visibilidad y Analítica" no como añadidos, sino como componentes estructurales del sistema, Forrester argumenta que sin una capacidad automatizada para procesar la telemetría de la red y responder a amenazas en tiempo real, la arquitectura de Confianza Cero es inoperable debido al volumen de decisiones de acceso que se deben tomar, el análisis de esta dimensión concluye que una arquitectura robusta para una organización híbrida debe adoptar la lógica de decisión del NIST (separación de planos) pero implementarla sobre los pilares definidos por Microsoft, asegurando que cada dominio (identidad, red, dispositivo) alimente con telemetría al motor de políticas central.

4.4 Análisis de la Dimensión 3: Modelos de Madurez

La transición hacia *Zero Trust* es un viaje evolutivo, y el análisis de los modelos de madurez de Microsoft y MITRE proporciona una hoja de ruta clara para medir el progreso del estadio inicial, denominado "Tradicional", se caracteriza por una dependencia casi total del perímetro de red físico, en esta fase, la identidad suele estar dividida (directorios locales *on-premise*) y la confianza se otorga en función de la dirección IP o la conexión física al cable de red, el diagnóstico señala que este modelo es insostenible para el trabajo híbrido,

ya que la extensión del perímetro mediante VPNs tradicionales rompe el principio de "asumir la brecha", permitiendo que un dispositivo remoto comprometido infecte toda la red interna.

El estadio "avanzado", donde se ubican la mayoría de las organizaciones en transición híbrida, introduce controles de nube y mecanismos de "políticas híbridas", aquí, las organizaciones comienzan a utilizar autenticación multifactor (MFA) y a segmentar el tráfico, pero a menudo retienen una arquitectura de "castillo y foso" para sus aplicaciones heredadas, MITRE advierte en su documento "Are We There Yet?" que este es el punto de mayor riesgo de estancamiento para las organizaciones que implementan herramientas modernas sobre arquitectura antigua, creando una falsa sensación de seguridad, la complejidad de gestionar políticas duplicadas (una para la nube, otra para local) aumenta la carga operativa y la posibilidad de errores humanos.

El estadio "óptimo" representa el ideal de una infraestructura totalmente automatizada, donde las políticas de acceso son dinámicas y se ajustan en tiempo real basándose en el riesgo del comportamiento del usuario y la salud del dispositivo, en este nivel, la microsegmentación es granular hasta el nivel de aplicación individual y la respuesta a incidentes es automática, el análisis revela que alcanzar este nivel requiere una inversión masiva en orquestación y que, como indica Forrester, es un proceso continuo de mejora, no un destino estático. Para este Trabajo Final de Graduación, este análisis de madurez justifica la necesidad de una propuesta que priorice la consolidación de la identidad híbrida como el paso crítico para avanzar del estadio Tradicional al Avanzado.

4.5 Análisis de la Dimensión 4: Viabilidad en Entornos Híbridos

Esta dimensión representa el aporte más significativo del diagnóstico al problema de investigación planteado, la realidad operativa de la mayoría de las organizaciones no es puramente "nube", sino una mezcla compleja de sistemas modernos y heredados, el análisis del NIST ofrece una validación técnica crucial para este escenario a través de sus modelos de despliegue de PEP (Policy Enforcement Points). El estándar reconoce explícitamente que los PEP pueden manifestarse como agentes instalados en servidores locales o como portales de

recursos ("Resource Portals"), lo que significa que es posible aplicar principios de *Zero Trust* a *mainframes* o servidores ERP antiguos sin necesidad de refactorizarlos, simplemente colocando una capa de control moderna frente a ellos.

Microsoft aborda la viabilidad híbrida desde la perspectiva de la identidad, su visión de "Identidad Híbrida" (mediante la sincronización de Active Directory local con Entra ID/Azure AD) permite que las mismas políticas de acceso condicional que protegen el correo en la nube protejan también una aplicación web interna, utilizando conectores como el Application Proxy, esto resuelve uno de los mayores dolores de cabeza del trabajo híbrido: la necesidad de VPNs para todo, al publicar aplicaciones internas de forma segura a través de la nube, se reduce la superficie de ataque de la red corporativa, sin embargo, MITRE aporta la contraparte necesaria al entusiasmo tecnológico, señalando los desafíos de integración. En entornos híbridos, la visibilidad unificada es difícil de lograr; los logs de un firewall perimetral antiguo tienen formatos distintos a los logs de acceso de una aplicación SaaS, MITRE enfatiza que la viabilidad de *Zero Trust* en entornos híbridos depende menos de comprar la herramienta "correcta" y más de la capacidad de ingeniería para integrar estas señales dispares en un sistema de monitoreo coherente. En conclusión, el análisis confirma que el modelo híbrido es viable y seguro, siempre que se utilice la identidad como el puente unificador entre el mundo *on-premise* y el mundo nube, dejando a la red en un segundo plano como mero transporte.

Capítulo 5. Propuesta de solución

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.