Metodología para el Control de Acceso a la Red Basado en Zero Trust en el Sector Financiero Colombiano

Luis Andrés Montoya Duffis

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

Año 2024

Metodología para el Control de Acceso a la Red Basado en Zero Trust en el Sector Financiero Colombiano

Luis Andrés Montoya Duffis

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Ciberseguridad

Director (a):

Héctor Fernando Vargas Montoya

Codirector (a):

Joel Carroll Vargas

línea de Investigación:

Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad

Medellín, Colombia

2024

Agradecimientos

Al culminar este trabajo, deseo expresar mi más profundo agradecimiento a todas las personas que me han acompañado y apoyado en este camino.

En primer lugar, a mi esposa Margarita, mi compañera de vida, por su inagotable paciencia, comprensión, amor y compromiso para cuidar nuestros hijos mientras desarrollaba este reto. Tus palabras de aliento, incluso en los momentos más desafiantes, me dieron la fuerza para seguir adelante. Tu apoyo incondicional ha sido fundamental para alcanzar este logro.

A mis hijos, Jacobo y Belén, quienes con su inocencia, sonrisas y curiosidad constante me recordaron cada día por qué vale la pena esforzarse. Ustedes son mi mayor inspiración, y este logro también es para ustedes. Espero que mi experiencia les sirva como un ejemplo de que nunca es tarde para perseguir los sueños.

A mis padres y mi familia extendida, por inculcarme desde niño los valores del esfuerzo y la disciplina. Sus enseñanzas han sido pilares fundamentales en mi vida y en cada etapa de este recorrido.

A mis profesores y mentores, gracias por compartir su conocimiento, por guiarme con paciencia y por enseñarme que siempre hay algo más por aprender. A mis compañeros de estudio, por las conversaciones enriquecedoras y el apoyo mutuo en esta travesía académica.

Finalmente, quiero dedicar unas palabras a quienes, como yo, se han planteado un gran reto en la vida. Este trabajo es testimonio de que no importa la edad, lo que realmente cuenta son las ganas y la disciplina con la que enfrentemos nuestros desafíos. Todo sueño es alcanzable si nos comprometemos con él, paso a paso, día a día.

A todos los que formaron parte de este viaje, de una u otra manera, mi más sincero agradecimiento. Este triunfo no es solo mío, es de todos ustedes.

Resumen

El presente trabajo desarrolla una metodología de seguridad informática fundamentada en el modelo de Zero Trust Network Access (ZTNA), para optimizar el control de acceso en el sector financiero colombiano. ZT se presenta como un paradigma innovador que elimina la confianza implícita y valida de manera estricta cada acceso a recursos de red. **Objetivo:** Proponer una metodología de seguridad informática basado en ZT para el control de acceso a nivel de red, y en ese sentido, minimizar los riesgos y la materialización de incidentes cibernéticos para el sector financiero colombiano. **Metodología:** La investigación se estructuró en cuatro fases: (1) diagnóstico del estado actual y categorización de riesgos operacionales; (2) evaluación y priorización de riesgos asociados a redes mediante matrices de impacto y probabilidad; (3) análisis comparativo de modelos ZT disponibles en la industria; y (4) validación de la metodología propuesta a través de pruebas controladas y simulaciones de ciberataques. **Resultados:** Tras implementar la metodología ZT, se observó una mejora en la gestión de riesgos: los inadmisibles disminuyeron al 20.83%, mientras los inaceptables aumentaron al 50%, reflejando una menor criticidad general. Además, los riesgos tolerables se incrementaron al 29.17%, destacando una mayor capacidad de control y mitigación. **Conclusión:** La metodología propuesta demuestra ser una estrategia efectiva para reforzar la ciberseguridad en el sector financiero colombiano, garantizando la confidencialidad, integridad y disponibilidad de la información crítica, y promoviendo una mayor resiliencia organizacional ante un panorama de amenazas en constante evolución.

Palabras clave: Ciberseguridad financiera, Zero Trust, Control de acceso, ZTNA, riesgos cibernéticos, Amenazas cibernéticas.

Abstract

This study develops a cybersecurity methodology based on the Zero Trust Network Access (ZTNA) model to optimize access control in the Colombian financial sector. ZT is introduced as an innovative paradigm that eliminates implicit trust and strictly validates each access to network resources. **Objective:** To propose a ZT-based cybersecurity methodology for network-level access control, aiming to minimize risks and the occurrence of cyber incidents in the Colombian financial sector. **Methodology:** The research was structured into four phases: (1) assessment of the current state and categorization of operational risks; (2) evaluation and prioritization of network-related risks using impact and probability matrix; (3) comparative analysis of ZT models available in the industry; and (4) validation of the proposed methodology through controlled tests and cyberattack simulations. **Results:** After implementing the ZT methodology, risk management showed significant improvements: inadmissible risks decreased to 20.83%, while unacceptable risks rose to 50%, reflecting a shift toward lower criticality risks. Additionally, tolerable risks increased to 29.17%, highlighting an enhanced capacity for control and mitigation. **Conclusion:** The proposed methodology proves to be an effective strategy for strengthening cybersecurity in the Colombian financial sector, ensuring the confidentiality, integrity, and availability of critical information while fostering greater organizational resilience in an ever-evolving threat landscape.

Keywords: Financial Cybersecurity, Zero Trust, Access Control, Banking Institutions, Security Methodologies, Cyber Threats.

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista Abreviaturas

Abreviatura	Término
ZTNA	Zero Trust Network Access
VPN	Redes Privadas Virtuales
SDP	Perímetro Definido por Software
SGSI	Sistema de Gestión de Seguridad de Información
MFA	Autenticación Multifactor
ZT	Zero Trust
PEPs	Puntos de Aplicación de Políticas
PDPs	Puntos de Decisión de Políticas
TI	Tecnologías de la Información
ZTA	Arquitectura Zero Trust
SSO	Inicio de Sesión Único
ML	Machine Learning
IoT	Internet de las Cosas
ZIoT	Zero Trust en IoT
DoS	Denegación de Servicio
DDoS	Ataques de Negación de Servicio Distribuido
SFC	Superintendencia Financiera de Colombia
SaaS	Software As a Service
SSE	Security Service Edge
POPs	Puntos de Presencia
ATO	Toma de Control de Cuentas
NGFW	Next Generation Firewall

Abreviatura	Término
ZTX	Zero Trust eXtended
HTTP	HyperText Transfer Protocol
FTP	File Transfer Protocol
APWG	Anti-Phishing
MITRE ATT & CK	Adversarial Tactics, Techniques, and Common Knowledge
NIST	Instituto Nacional de Estándares y Tecnología
CISA	Agencia de Seguridad de Infraestructura y Ciberseguridad
UEBA	Análisis de comportamiento de usuario/entidad
BYOD	Bring Your Own Device
EDR	Detección y Respuesta de Endpoints
DCIDS	Prevención de intrusiones distribuidas colaborativas
CSRF	Cross-site request forgery
XSS	Cross-site scripting
CISO	Responsable de la ciberseguridad de la organización financiera
CIAM	Customer Identity and Access Management
AHP	Proceso Analítico Jerárquico

Introducción

La ciberseguridad se ha convertido en un pilar fundamental para proteger sistemas informáticos, redes, dispositivos y datos frente a ataques malintencionados, accesos no autorizados y otras amenazas digitales [1]. Las amenazas cibernéticas incluyen desde malware y ransomware hasta ataques de denegación de servicio (DDoS), explotación de vulnerabilidades en software o hardware, y amenazas internas. Estos eventos representan un desafío creciente para las organizaciones, especialmente para aquellas que manejan datos sensibles y críticos como las instituciones financieras, ya que estas son objetivos atractivos para los ciberdelincuentes debido al volumen y valor de la información que manejan, lo que hace imperativa la adopción de medidas de seguridad robustas y adaptativas [2].

Tradicionalmente, el enfoque de control en las Tecnologías de la Información (TI) estuvo enfocado en un modelo perimetral que confiaba en la ubicación de los dispositivos y usuarios dentro de una red. Sin embargo, con el crecimiento del acceso remoto, la expansión de los entornos no controlados, como los lugares de trabajo híbridos, y las limitadas capacidades que tuvo este tipo de enfoque, los negocios se han visto en la necesidad de reforzar y reconsiderar la seguridad en la red [1].

En este contexto, John Kindervag acuñó el término "Zero Trust" o confianza cero (ZT, por sus siglas en inglés), mientras trabajaba en Forrester [3], un paradigma de ciberseguridad que elimina la confianza implícita en cualquier usuario o dispositivo, independientemente de su ubicación. En lugar de ello, cada acceso a los recursos de la red debe ser verificado y autorizado individualmente, minimizando así los riesgos de ataques cibernéticos [1], [3].

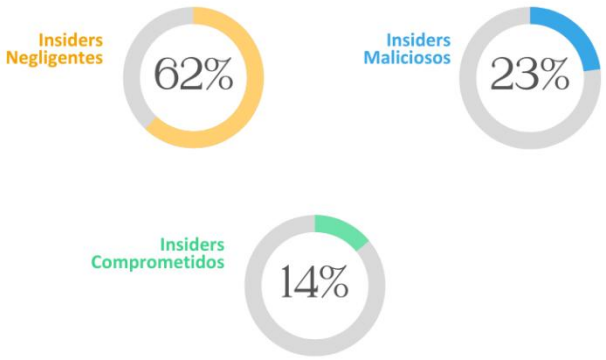
Con el auge de la metodología ZT, surgió el término de Arquitectura de ZT (ZTA), en la cual su implementación consta de varios componentes lógicos conectados, que se pueden implementar como un servicio local o como un servicio basado en la nube. De la ZTA hacen parte la gestión de identidades, gestión de credenciales, gestión de acceso, procedimientos operativos, gestión de entornos hostiles e infraestructura básica [1], [4]. Dentro de este marco, el Acceso a la Red de Confianza Cero (ZTNA, por sus siglas en inglés) juega un papel crucial al redefinir cómo se otorga acceso a la red. ZTNA permite a las organizaciones segmentar sus redes, proporcionando a los usuarios acceso solo a los recursos necesarios, lo que reduce significativamente las oportunidades para que los atacantes se muevan lateralmente una vez dentro del sistema. Esto es particularmente relevante en el sector financiero, donde las amenazas internas y externas siguen siendo una preocupación crítica [4], [5].

La seguridad de la información es un tema relevante en la industria financiera debido a la gran cantidad de información confidencial que se administra, además de la responsabilidad en protegerla de manera efectiva contra ciberataques. El valor de la confianza de las entidades financieras tiene su peso en la disponibilidad de los servicios y confidencialidad e integridad de la información; además, tienen la responsabilidad de cumplir con lo estipulado en la ley 1581 de 2012 sobre la protección de datos personales [6].

El confinamiento por la pandemia del COVID-19, fue un reto para las compañías contrarrestar los ataques a la red, dado que el teletrabajo abrió un sinnúmero de oportunidades para los ciberataques. A nivel mundial, el costo promedio de una filtración de datos según *International Business Machines* (IBM) en su informe del año 2023, sigue incrementándose con un total de (3.86, 4.24, 4.35, y 4.45 millones de dólares) en los años 2020, 2021, 2022 y 2023, respectivamente; siendo la industria de la salud la más afectada, seguida de la industria financiera [7]. Las credenciales robadas o comprometidas y el phishing y fueron los ciberdelitos más prevalentes, representando el 16% y el 15% de las violaciones de seguridad, respectivamente para el año 2023 [7].

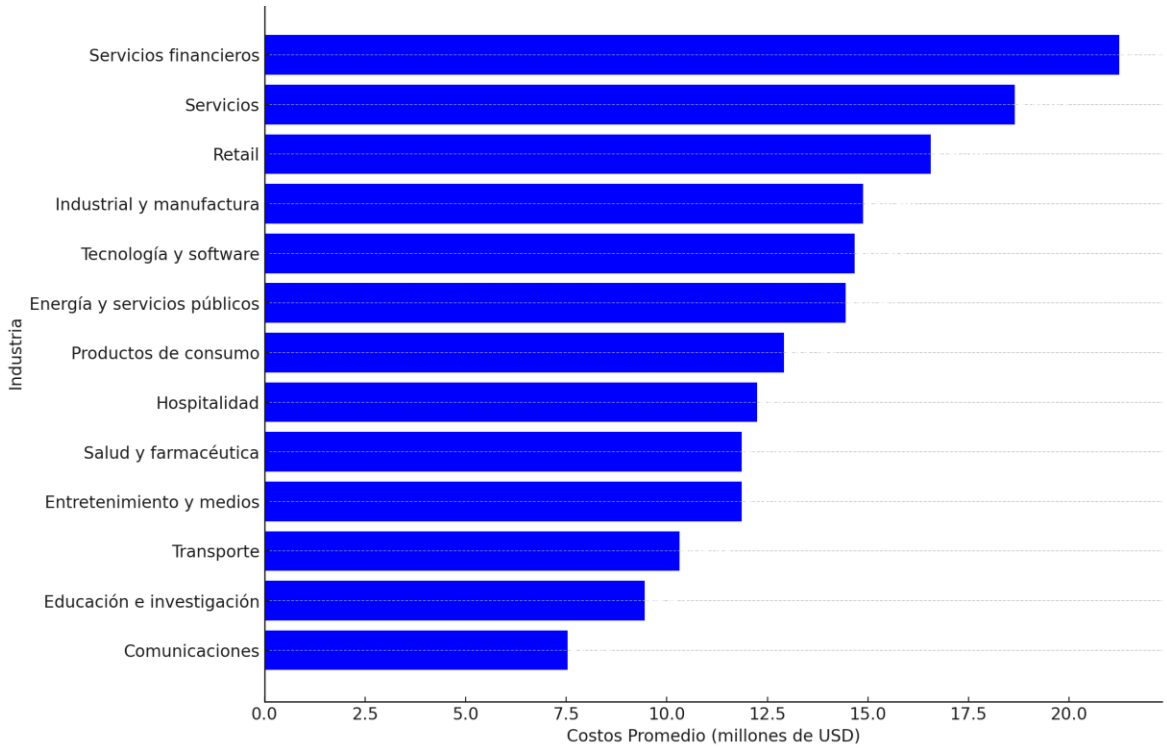
Por otro lado, el informe [8] resalta la creciente problemática de las amenazas internas en el sector financiero, donde el 24% de todas las violaciones de seguridad estuvieron relacionadas con *insiders*. Como se muestra en la Figura 1, desde 2018, las amenazas internas han aumentado un 20.3%, con los *insiders* negligentes causando el 62% de los incidentes, seguidos por los *insiders* malintencionados (23%) y los *insiders* comprometidos (14%). Estos datos resaltan que, aunque las empresas financieras adoptan tempranamente herramientas de ciberseguridad, estas no son suficientes para protegerse de todas las formas de ataque, especialmente las internas.

Figura 1. Violaciones por Insiders en el Sector Financiero. Adaptado de [8]



Como se muestra en la Figura 2, los altos costos asociados con la gestión de las amenazas internas en la industria financiera son significativos, con un promedio de $21.25 millones [9]. Esto destaca la necesidad de invertir en medidas de seguridad más robustas y estrategias de mitigación. Además, casi la mitad de todas las brechas de seguridad se deben a fallas de TI (23%) o errores humanos (22%) [7], lo que refuerza la importancia de mejorar tanto los sistemas tecnológicos como la capacitación de los empleados.

Figura 2. Costos para la Gestión de Amenazas Internas en la Industria Financiera. Adaptado de [9].



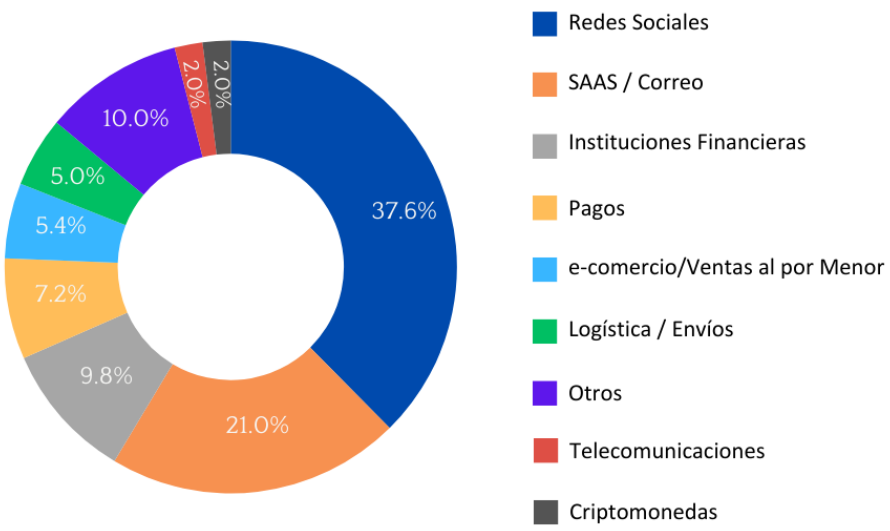
Adicional a lo anterior, el uso de protocolos de comunicación inseguros, como "*HyperText Transfer Protocol* (HTTP)", "*File Transfer Protocol* (FTP)" y otros protocolos de red, puede exponer los sistemas a ataques de intermediario (MITM), comprometiendo la integridad de las comunicaciones [10]. El sector financiero, que depende en gran medida de la integridad y confidencialidad de los datos, debe adoptar protocolos seguros como HTTPS y TLS, además de implementar sistemas de autenticación robustos y segmentación de red. La falta de una correcta implementación de estas medidas ha permitido que atacantes exploten vulnerabilidades técnicas en las redes financieras, causando daños significativos [11], [12].

Otro riesgo crítico en el entorno digital actual son los ataques de ingeniería social, como el phishing, que explotan la confianza de los empleados para obtener acceso no autorizado a información sensible [13], [14], [15]. El phishing, en particular, sigue siendo una de las técnicas más comunes y

efectivas para comprometer sistemas en el sector financiero. En 2022, el 40% de los ataques a nivel mundial utilizaron el phishing como vector inicial de ataque [16], destacando la necesidad de programas de capacitación continua y concientización de los empleados para reducir la vulnerabilidad interna y mitigar el riesgo.

El Grupo de Trabajo "*Anti-Phishing*" (APWG por sus siglas en inglés) reportó casi cinco millones de ataques de phishing a lo largo de 2023, estableciendo un nuevo récord anual. En el primer trimestre de 2024, APWG documentó 963,994 ataques de phishing, el total trimestral más bajo desde el cuarto trimestre de 2021. Este número es significativamente inferior a los 1,624,144 ataques registrados en el primer trimestre de 2023, que representó el pico máximo en las observaciones históricas de APWG. Dentro de los sectores más atacados, el sector financiero se ha consolidado como uno de los objetivos más recurrentes para los ataques de phishing. Sin embargo, se ha observado que el phishing contra el segmento de instituciones financieras (bancos) ha disminuido desde el primer trimestre de 2024 pasando de un 24.9% en el tercer trimestre de 2023 a un 14% en el cuarto trimestre de 2023, y al 9.8% en el primer trimestre de 2024 [15], (Figura 3).

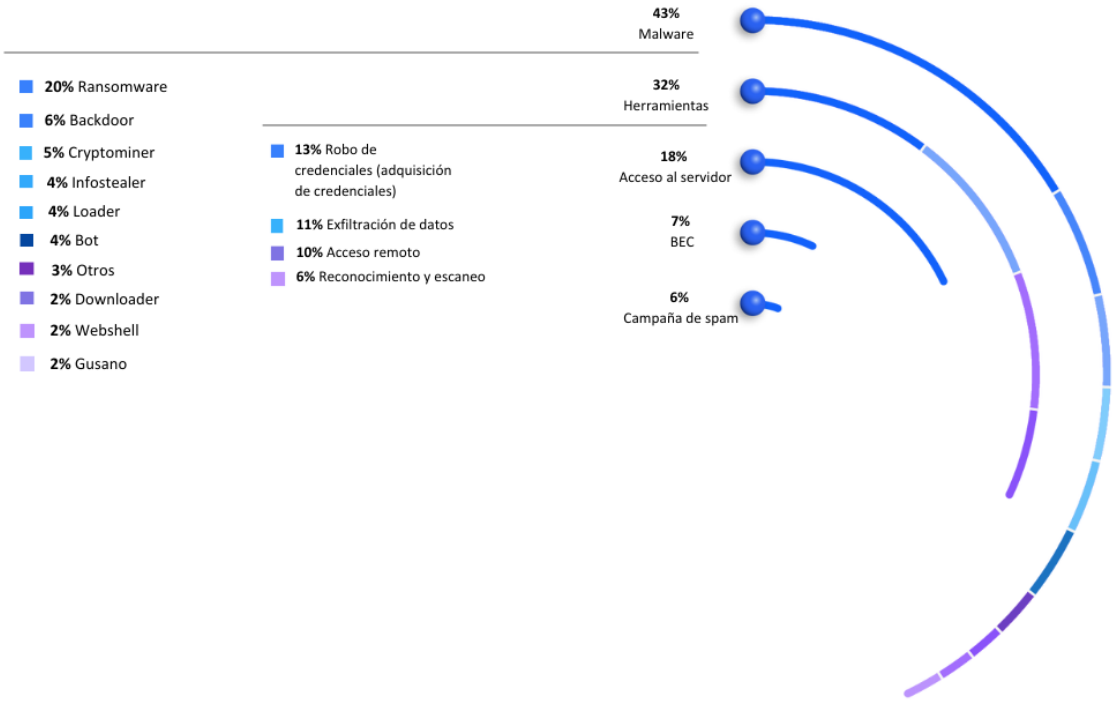
Figura 3. Ataques Phishing en el Primer Trimestre de 2024. Adaptado de [15].



Finalmente, los ataques de malware, especialmente el ransomware, han aumentado en frecuencia y sofisticación [17]. Según [18], el despliegue de malware fue la acción más común tomada por los actores de amenazas en las redes de las víctimas, ocurriendo en el 43% de los incidentes reportados. De estos incidentes, el 20% correspondió a casos de ransomware (Figura 4). El ransomware cifra los datos de las víctimas y exige un rescate para liberarlos, causando

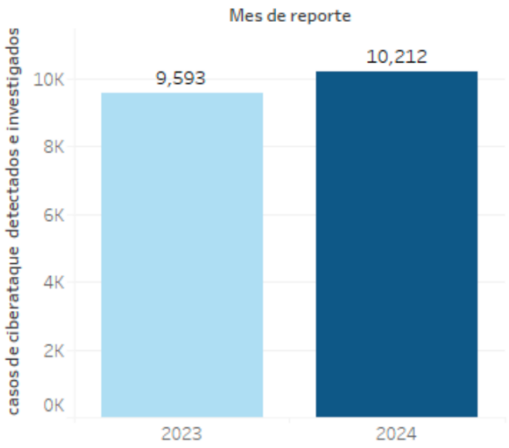
interrupciones significativas en las operaciones de las instituciones financieras. La adopción de malware por parte de los atacantes ha evolucionado, enfocándose ahora en el robo de credenciales [18], lo que resalta la importancia de la protección de la identidad como un elemento central en las estrategias de ZT.

Figura 4. Ataques Malware. Adaptado de [18].



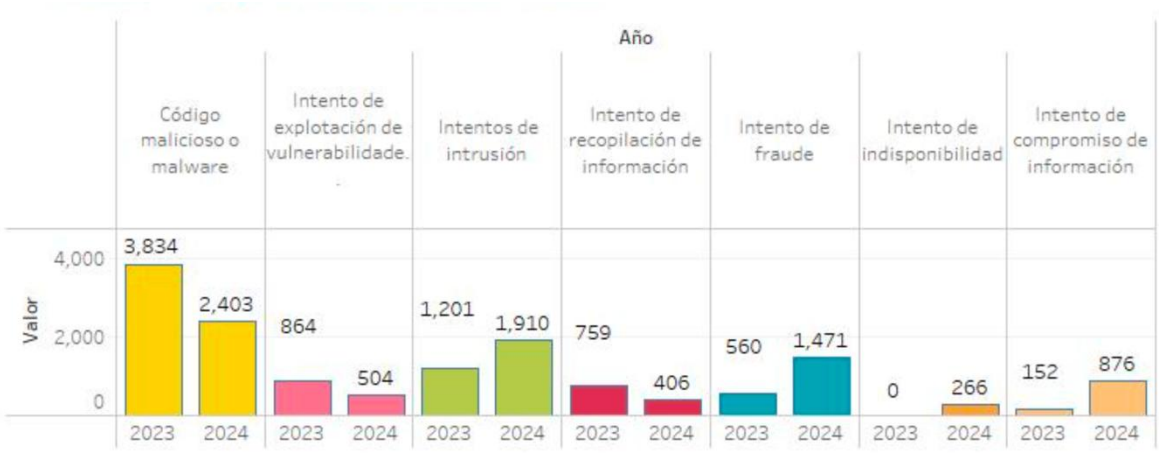
Al analizar esta problemática en el contexto colombiano, se constata que el país no ha quedado al margen de este fenómeno. De acuerdo con el informe mensual de Asobancaria, entre enero y mayo de 2024, Colombia y Estados Unidos encabezaron la lista de países con mayor número de incidentes cibernéticos [19]. Solo en el mes de mayo de 2024, se investigaron 1,932 ciberataques en cinco entidades financieras de Colombia. La Figura 5, muestra un aumento del 6% en el total de casos detectados e investigados en lo que va del año 2024 [19].

Figura 5. Ciberataques Detectados en Colombia en 2024 [19].



Durante este mismo período, se registraron 2,403 incidentes relacionados con código malicioso o malware, lo que representa una disminución del 37% en comparación con el mismo periodo del año anterior. Sin embargo, categorías como intentos de intrusión y fraude han mantenido una alta incidencia en comparación con el año 2023 [19], (Figura 6).

Figura 6. Total de Incidentes Relacionados con Malware y Otras Amenazas en Colombia: Comparativa del Periodo 2024 con 2023 [19].



Considerando lo expuesto anteriormente, el sector financiero es uno de los más expuestos a riesgos cibernéticos debido al manejo de grandes volúmenes de datos confidenciales y activos financieros. Por lo tanto, esta investigación se justifica por la necesidad urgente de fortalecer la ciberseguridad en el sector financiero colombiano, adaptándose a las nuevas realidades tecnológicas y protegiendo de manera eficiente la información sensible en un entorno digital en constante evolución.

Frente a esta situación, las organizaciones financieras de hoy, necesitan adoptar un modelo de seguridad que les permita reducir la brecha de problemas asociados a la no protección de los datos, reducir los impactos en la administración del control de acceso, ser más eficientes en la operación de seguridad, adaptarse de manera más efectiva a la complejidad del entorno, lo que puede incluir diferentes mecanismos de seguridad para un lugar de trabajo híbrido, a nivel de las personas, dispositivos, aplicaciones y datos donde quiera que se encuentren [5]. Es importante considerar que los ciberataques en Colombia vienen en aumento. Por lo tanto, minimizar los riesgos de seguridad en los sistemas informáticos y la materialización de incidentes cibernéticos, es una prioridad, no solo a nivel mundial sino también a nivel nacional [20].

En la última década se ha evidenciado que las empresas del sector financiero colombiano vienen realizando esfuerzos en materia de ciberseguridad y seguridad de la información con el fin de proteger los datos de clientes y empleados dentro y fuera del perímetro de red. Sin embargo, los diferentes problemas de seguridad suelen iniciar por falencias o inadecuada implementación de un modelo para el control de acceso a las aplicaciones en las redes corporativas, con lo cual, la identificación, autenticación y autorización dentro y fuera del perímetro genera una brecha de seguridad. Además, con la creciente adopción del trabajo remoto y el uso de dispositivos móviles, las empresas financieras enfrentan el desafío de proteger los datos en entornos no controlados

incluyendo el riesgo de amenazas internas, ya sea por parte de empleados malintencionados o por accidentes y errores involuntarios.

Por esta razón, la presente investigación tuvo como objetivo general “proponer una metodología de seguridad informática basado en Zero Trust (ZT) para el control de acceso a nivel de red, y en ese sentido, minimizar los riesgos y la materialización de incidentes cibernéticos para el sector financiero colombiano”.

Para alcanzar este objetivo se establecieron cuatro objetivos específicos. En primer lugar, fue “Categorizar el contexto operacional de las empresas del sector financiero, relacionado con el control de acceso”. El cumplimiento de este objetivo se abordó desde una encuesta basada en 4 aspectos fundamentales como: contexto operacional, control de acceso e identificación de riesgos, gestión de identidad e impacto y gestión de riesgos.

En segundo lugar, se “establecieron los diferentes riesgos que impactan el control de acceso asociados a las redes que puedan afectar la operación en un entorno financiero”. Con base en la información obtenida de la encuesta para el desarrollo del objetivo específico número uno, se realizó una matriz de riesgo con el fin de evaluar la probabilidad de ocurrencia de ataques a la red, definida como (raro, poco probable, posible y casi seguro); el impacto de los posibles ataques fue categorizado como (insignificante, menor, significativo, mayor y severo).

En tercer lugar, se “caracterizaron los diferentes modelos de ZT actuales en la industria que puedan ser aplicados al sector financiero y a la reducción de riesgos”. Se consideró el servicio de seguridad de borde (SSE) de Gartner y Forrester, con el fin de identificar los líderes y las mejores prácticas de ciberseguridad basadas en ZT, así como los métodos más efectivos para contrarrestar los ataques de acceso a la red y sus aplicaciones en la red interna o de forma remota.

Finalmente se propuso “validar en un ambiente controlado la metodología propuesta, a través de una prueba de escritorio, caso de estudio o simulación”. La metodología de Arquitectura de Red de Acceso de Zero Trust (ZTNA) seleccionada, fue evaluada por medio de un ambiente de prueba al realizar ataques controlados.

El alcance de estos objetivos representa una estrategia proactiva y adaptativa para asegurar la integridad, confidencialidad y disponibilidad de los datos en el sector financiero. Esto es de gran importancia ya que la globalización y la era de la hiperconectividad han traído importantes desarrollos, innovaciones y nuevas estrategias en el manejo de la información. No obstante, se ha convertido en un reto para el mundo corporativo, dado que cada día, la información que se almacena en la nube, se ha visto afectada por situaciones intrusivas que buscan acceder a información confidencial con el interés de hacer daño al interior de las organizaciones [21].

Esta investigación se estructura en diversas secciones que abarcan desde el marco teórico y el estado del arte, hasta la metodología empleada, los resultados obtenidos y las conclusiones derivadas, con el objetivo de ofrecer recomendaciones prácticas para fortalecer la ciberseguridad en las organizaciones financieras colombianas.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

1.1.1 Ciberseguridad: Contexto e Importancia

La ciberseguridad se define como el conjunto de técnicas, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados. Este campo abarca una amplia gama de soluciones técnicas y estratégicas que garantizan la confidencialidad, integridad y disponibilidad de la información en el entorno digital [22]. Además, la ciberseguridad no solo se refiere a la protección contra el acceso no autorizado, sino también a la defensa contra daños y la garantía de la operatividad continua de los sistemas y redes [22]. La ciberseguridad incluye múltiples disciplinas, desde la informática y la ingeniería hasta las ciencias sociales, debido a la naturaleza multifacética de las amenazas y las soluciones necesarias. Según [23], la ciberseguridad implica la recolección y coordinación de recursos, tanto humanos como técnicos, para proteger los sistemas de eventos que comprometan su integridad y propiedad.

La ciberseguridad ha experimentado una evolución significativa desde sus inicios en las décadas de 1970 y 1980 hasta la actualidad, reflejando los avances tecnológicos y la creciente sofisticación de las amenazas cibernéticas [24]. En los años 70, el concepto de ciberseguridad comenzó a tomar forma con la aparición de los primeros virus informáticos y los incidentes de hacking. Estos incidentes marcaron el inicio de la conciencia sobre la necesidad de proteger los sistemas informáticos contra el acceso no autorizado y el software malicioso [24]

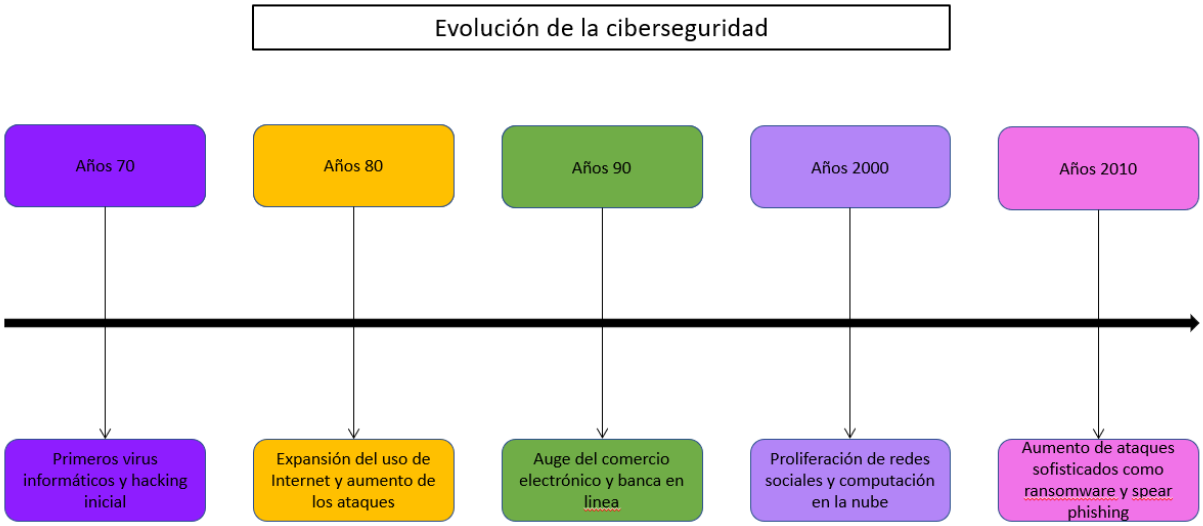
Durante, la década de 1980 se observó una expansión significativa del uso de internet, lo que aumentó la superficie de ataque para los cibercriminales [24]. La proliferación de redes interconectadas hizo que la protección de la información digital fuera una prioridad creciente para las organizaciones [25]. Posteriormente, en los años 90, el auge del comercio electrónico y la banca en línea transformó la ciberseguridad en una preocupación empresarial. Las transacciones financieras y la información personal comenzaron a transferirse en línea, lo que atrajo a los cibercriminales interesados en robar datos sensibles y monetizar sus actividades ilícitas. Este

período llevó al desarrollo de tecnologías de encriptación y las primeras medidas de seguridad robustas para proteger las transacciones digitales [24].

La década de 2000 trajo consigo la proliferación de las redes sociales, la computación en la nube y los dispositivos móviles, ampliando aún más la superficie de ataque para los cibercriminales [24]. Las plataformas de redes sociales comenzaron a recolectar grandes cantidades de datos personales, convirtiéndose en objetivos lucrativos para los ataques cibernéticos. La adopción generalizada de la computación en la nube también introdujo nuevos desafíos de seguridad, ya que los datos y servicios se desplazaron fuera de los perímetros de seguridad tradicionales [26].

Finalmente, en la década de 2010, los ciberataques se volvieron más sofisticados, frecuentes y focalizados. Los ataques dirigidos, como el phishing y el ransomware, se convirtieron en amenazas comunes, causando daños significativos a empresas y gobiernos. Los incidentes como el ataque de ransomware WannaCry en 2017 y la violación de datos de Equifax destacaron la necesidad de estrategias de ciberseguridad más avanzadas y una mayor colaboración internacional para combatir las amenazas cibernéticas [27]. La Figura 7 muestra la evolución de la ciberseguridad desde 1970 hasta 2010.

Figura 7. Evolución de la Ciberseguridad. [Elaboración propia].



1.1.2 Importancia de la ciberseguridad en la era digital actual

En la era digital actual, la ciberseguridad es crucial debido al aumento exponencial de datos que se almacenan y transfieren en línea; las organizaciones de todos los sectores dependen de sistemas informáticos y redes para operar eficientemente, lo que las convierte en objetivos potenciales para los ciberataques. Además, la protección de datos personales y empresariales es fundamental para mantener la confianza y la seguridad en la economía digital [28]. Por lo tanto, la ciberseguridad es esencial para prevenir pérdidas financieras, proteger la privacidad y garantizar la continuidad operativa. Los ciberataques pueden provocar interrupciones significativas en los servicios, afectar la reputación de las empresas y resultar en sanciones legales por no proteger adecuadamente la información sensible. Por tal motivo, invertir en ciberseguridad no solo protege contra ataques, sino que también es una medida preventiva crucial para el bienestar económico y social [29].

Los ciberataques pueden tener consecuencias devastadoras. Entre los efectos más comunes se encuentran la pérdida financiera y robo, información sensible comprometida, tiempo de inactividad del sistema y pérdida de productividad, consecuencias legales y regulatorias, daño a la reputación y confianza. A continuación, se presentan las brechas de seguridad y las consecuencias de estos eventos en el sector financiero.

- **Pérdida Financiera y Robo**

En el sector financiero, los ataques y brechas cibernéticas pueden resultar en pérdidas financieras devastadoras tanto directas como indirectas. Esto se debe a que los delincuentes pueden acceder a cuentas bancarias, realizar transferencias no autorizadas y efectuar compras fraudulentas, lo cual puede dejar a las instituciones financieras con grandes pérdidas monetarias y deudas inesperadas [30]. Además, los costos asociados con la respuesta y recuperación de un ataque cibernético, como la contratación de expertos en seguridad, la implementación de nuevas medidas de protección y la reparación de sistemas comprometidos, pueden ser sustanciales [31].

Así mismo, las instituciones financieras también enfrentan la pérdida de ingresos debido al tiempo de inactividad de los sistemas, afectando su capacidad para operar normalmente y dañando su reputación a largo plazo [32]. Esto conlleva a la pérdida de confianza de los clientes y socios comerciales que puede llevar a una disminución en las ventas y en las oportunidades de negocio futuras, agravando aún más las pérdidas financieras [33].

Un estudio reciente mostró el impacto de las brechas de datos en el valor de mercado de las empresas al utilizar un conjunto de datos que incluyeron información sobre brechas cibernéticas en 3,992 empresas públicas durante el período de 1990 a 2019. Los resultados mostraron que las brechas cibernéticas tuvieron un impacto negativo significativo en los rendimientos anormales a corto plazo. Este efecto negativo estuvo mayor en industrias con frecuencias de ataques más altas y cuando la información personal financiera estuvo involucrada. Además, los rendimientos

acumulativos negativos continuaron aumentando hasta 250 días después del anuncio del evento, subrayando el impacto prolongado de las brechas cibernéticas en el valor de las empresas [34].

- **Información Sensible Comprometida**

La exposición no autorizada de datos personales y de negocios es una grave consecuencia de los ataques cibernéticos en el sector financiero. Los atacantes que acceden a información personal, como nombres, direcciones y números de cédula, pueden utilizar estos datos para cometer robos de identidad y fraudes, lo cual puede llevar a las víctimas a enfrentarse a consecuencias legales y financieras significativas [35]. En el ámbito empresarial, la exposición de información sensible, como secretos comerciales y propiedad intelectual, puede tener efectos devastadores, incluyendo la pérdida de ventaja competitiva y daño a la posición del mercado [36].

Según la literatura, la legislación sobre protección de datos personales ha experimentado cambios significativos debido a la gran cantidad de información que se divulga sin autorización en internet [37]. Estos cambios han propuesto criminalizar los daños significativos a los derechos e intereses legítimos de las personas resultantes de la filtración de estos datos. Además, el uso no autorizado de datos personales en redes sociales por parte de organizaciones comerciales se está volviendo más común, lo que requiere un proyecto de ley que proteja los derechos de los usuarios [37].

En el ámbito financiero, la exposición de información sensible puede permitir que competidores accedan a estrategias comerciales, diseños de productos y otra información valiosa, lo cual puede resultar en una pérdida significativa de ingresos y oportunidades de negocio. Estos incidentes no solo afectan a las víctimas directas, sino que también pueden tener repercusiones amplias, como la pérdida de confianza de los clientes y socios comerciales [38].

[39], evaluó el papel crítico de la ciberseguridad en el sector financiero y los desafíos que enfrentan las instituciones financieras en el mundo digital actual, destacando que los ciberataques pueden causar interrupciones en los servicios y pérdidas de datos, lo que lleva a pérdidas irreparables en la actividad financiera y un impacto negativo en la economía global. Además, resalta cómo las instituciones financieras son objetivos atractivos para los cibercriminales debido al valor de los datos que manejan y la posibilidad de obtener grandes recompensas financieras mediante actividades ilícitas.

- **Tiempo de Inactividad del Sistema y Pérdida de Productividad**

El tiempo de inactividad debido a ataques cibernéticos puede resultar en una pérdida significativa de productividad en el sector financiero, ya que esto afecta la capacidad de la empresa en el cumplimiento de sus responsabilidades y servicios [40]. En sectores críticos como la banca, estos tiempos de inactividad ponen en riesgo la seguridad y bienestar financiero de las personas. La restauración de los sistemas afectados y la recuperación de la productividad pueden llevar tiempo y recursos considerables [41].

Adicionalmente, los empleados pueden verse impedidos para realizar sus tareas diarias, lo que provoca retrasos en proyectos importantes y una disminución en la eficiencia operativa. Además, puede afectar negativamente la experiencia del cliente, lo que puede llevar a una pérdida de confianza y lealtad por parte de los consumidores. Por lo tanto, la gestión adecuada de los tiempos de inactividad y la implementación de planes de recuperación efectivos son esenciales para minimizar el impacto de estos incidentes en la productividad y la operación general de la empresa [40], [41]

- **Consecuencias Legales y Regulatorias y ZT**

El incumplimiento de las normas de protección de datos puede llevar a responsabilidades legales significativas para las instituciones financieras. Las regulaciones de protección de datos, como el Reglamento General de Protección de Datos (GDPR) en la Unión Europea (UE), imponen multas y sanciones severas por no proteger adecuadamente la información sensible [42].

En Colombia, el incumplimiento de las normas de protección de datos, establecido en la Ley 1581 de 2012, puede generar sanciones importantes. La Superintendencia de Industria y Comercio tiene la facultad de imponer multas que pueden llegar hasta los 2,000 salarios mínimos legales vigentes, siendo estas multas sucesivas mientras persista el incumplimiento. Además, la Superintendencia puede suspender las actividades relacionadas con el tratamiento de datos por un periodo de hasta seis meses, o incluso ordenar el cierre temporal o definitivo de las operaciones si no se adoptan las medidas correctivas necesarias. Estas sanciones aplican únicamente a entidades privadas, y en el caso de entidades públicas, la Superintendencia remite los casos a la Procuraduría General para la investigación pertinente. Estas disposiciones refuerzan la necesidad de que las instituciones financieras cumplan rigurosamente con la normativa de protección de datos para evitar consecuencias legales y reputacionales [6]

La falta de cumplimiento con estas regulaciones no solo resulta en sanciones financieras sino también en la pérdida de confianza y credibilidad entre los clientes y el público en general. En consecuencia, las organizaciones deben implementar políticas y procedimientos adecuados para proteger la información sensible y asegurarse de que están preparadas para responder rápidamente a cualquier incidente de seguridad. La educación y capacitación continua de los empleados sobre las mejores prácticas de ciberseguridad también es crucial para minimizar el riesgo de violaciones de datos y las consecuencias legales asociadas [43].

- **Daño a la Reputación y Confianza**

La divulgación pública de incidentes de seguridad cibernética puede dañar gravemente la reputación y la marca de una institución financiera. La pérdida de confianza de los clientes puede llevar a una disminución en la lealtad y a una reducción en las ventas. Este daño, puede hacer que los clientes decidan llevar su negocio a competidores que perciben como más seguros y confiables. Además, las relaciones comerciales y las asociaciones pueden verse afectadas negativamente, ya

que los socios comerciales pueden dudar en asociarse con una organización percibida como vulnerable a los ataques cibernéticos [44], [45].

La reconstrucción de la reputación y la confianza después de un incidente de este tipo puede ser un proceso largo y costoso, afectando la sostenibilidad y el crecimiento a largo plazo de la empresa. Las instituciones financieras deben brindar respuesta a los incidentes de seguridad y tomar medidas proactivas para reforzar sus defensas a los ataques cibernéticos y restaurar la confianza del público. La comunicación efectiva con los clientes y partes interesadas sobre las acciones tomadas para prevenir futuros incidentes es esencial para mitigar el daño a la reputación [46].

Un estudio en 2018 señaló que la desestabilización del sistema financiero debido a ciberataques puede tener consecuencias globales y destaca que las instituciones financieras están en riesgo no solo por las amenazas tradicionales, sino también por la creciente sofisticación de los cibercriminales que utilizan técnicas avanzadas para evadir las medidas de seguridad. La defensa efectiva contra estas amenazas implica la interrupción de la capacidad de estos actores para acumular recursos, diseñar herramientas ofensivas y explorar debilidades en los sistemas financieros. El estudio discute que para abordar estas vulnerabilidades frente a los ciberataques es necesario la colaboración internacional y la formulación de políticas globales de ciberseguridad para enfrentar estas amenazas de manera efectiva y mantener la estabilidad del sistema financiero mundial [47].

Por otro lado [39] enfatiza que las amenazas cibernéticas pueden socavar la confianza de los clientes e inversores, provocando una fuga de activos y una disminución en la reputación de la institución financiera; también argumenta que las instituciones financieras deben adoptar un enfoque integral de la ciberseguridad, que incluya la evaluación continua de riesgos, la implementación de tecnologías avanzadas de seguridad y la formación de empleados en prácticas seguras. Este enfoque integral es esencial para reducir la cantidad de amenazas y pérdidas, y para mantener la estabilidad de las actividades financieras.

1.1.3 Riesgo y gestión de riesgos de ciberseguridad

El riesgo de ciberseguridad se refiere a la probabilidad y el impacto de que eventos adversos relacionados con ciberataques afecten la confidencialidad, integridad y disponibilidad de sistemas, datos y servicios [48]. En el sector financiero, estos riesgos pueden traducirse en pérdidas económicas, daño reputacional y disrupción de servicios esenciales [39]. Por lo tanto, la ciberseguridad es crítica para mantener la estabilidad y la continuidad operativa de las instituciones financieras. Esto es de gran importancia ya que el sector financiero juega un papel crucial en la liquidez económica y la funcionalidad del estado, y cualquier disrupción puede tener efectos de largo alcance en la economía global [39].

El sector financiero en América Latina y el Caribe ha experimentado una acelerada digitalización en los últimos años, lo cual ha traído consigo una serie de ventajas, como la facilidad de acceso a servicios bancarios y la eficiencia en las transacciones. Sin embargo, también ha incrementado su exposición a riesgos cibernéticos debido a un aumento en la superficie de ataque para los ciberdelincuentes. Según el informe de la OEA citado por ASOBANCARIA, el 92% de las entidades bancarias en la región identificaron algún tipo de evento de seguridad digital, y el 37% de estas entidades fueron víctimas de ataques exitosos [49]. Estos eventos de seguridad incluyen tanto intentos de ataque frustrados como ataques que lograron su objetivo. Esto resalta la necesidad de una ciberseguridad robusta y de una gestión efectiva de los riesgos cibernéticos para proteger la integridad de los sistemas financieros [39]. Las directrices regulatorias sugieren que las instituciones financieras deben adoptar políticas y marcos de gestión de riesgos más robustos para fortalecer la resiliencia del sector financiero frente a los riesgos cibernéticos sistémicos [50], [51].

- **Gestión de Riesgos en el Sector Financiero**

La información es uno de los activos más valiosos de cualquier organización, y en el sector financiero, la protección de la información es crucial para garantizar la confianza de los clientes y la eficacia en la gestión de servicios financieros. La Guía No. 7 de Gestión de Riesgos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) de Colombia proporciona un marco exhaustivo para la gestión de riesgos de seguridad de la información, y está alineada con normas internacionales como la ISO/IEC 27001 y 27005 [52].

Esta guía tiene como objetivo orientar a las entidades públicas en la gestión de riesgos de seguridad de la información. Sin embargo, sus principios y metodologías pueden ser aplicados al sector financiero para asegurar una protección integral de los activos de información. Esta Busca ayudar

a las instituciones a vincular la identificación y análisis de riesgos con los temas de seguridad de la información, garantizando una protección integral de los activos digitales [52]. Por otro lado, la norma ISO/IEC 27005 proporciona un marco estructurado y sistemático para la gestión de riesgos de seguridad de la información, lo cual es crucial para la toma de decisiones informadas y la implementación de controles adecuados. Esta norma es una extensión de la ISO/IEC 27001 y está diseñada para ayudar a realizar un análisis y una evaluación de riesgos detallados, permitiendo una implementación más efectiva de las medidas de gestión de seguridad de la información (SGSI), fortaleciendo la resiliencia de las instituciones financieras [53]

La implementación efectiva de estos marcos y directrices es esencial para proteger los activos digitales y mantener la confianza de los clientes en la capacidad de las instituciones financieras para proteger sus datos personales. Así mismo, asegura que la gestión de riesgos sea una práctica dinámica y adaptativa, capaz de enfrentar los desafíos de un entorno digital en constante cambio y cada vez más amenazado. A continuación, se explora la importancia, las principales etapas, estrategias y herramientas propuestas tanto en la guía como en la norma ISO/IEC 27005 para gestionar los riesgos en la seguridad de la información.

- **Importancia de la Gestión de Riesgos en el Sector Financiero**

La gestión de riesgos es un componente esencial de la seguridad de la información. Permite identificar, evaluar y mitigar los riesgos que pueden comprometer la confidencialidad, integridad y disponibilidad de los activos de información [52]. En el contexto del sector financiero, una adecuada gestión de riesgos garantiza que las operaciones y servicios se realicen sin interrupciones, protegiendo al mismo tiempo los datos sensibles de los clientes y las instituciones financieras (Tabla 1) [52].

Tabla 1. Etapas para la Gestión de Riesgos en el Sector Financiero, [52].

Etapas	Descripción
Compromiso de la Alta Dirección	En el sector financiero, es fundamental que la alta dirección esté comprometida con el proceso de gestión de riesgos. Su apoyo es crucial para la toma de decisiones y la implementación de las políticas de seguridad.
Conformación de un Equipo Interdisciplinario	La gestión de riesgos debe involucrar a un equipo que represente diferentes áreas de la institución financiera, permitiendo una visión completa y unificada de los riesgos.
Capacitación en la Metodología	El equipo debe estar capacitado en la metodología de gestión de riesgos para poder identificar, analizar y mitigar los riesgos de manera efectiva.

- **Criterios para la evaluación de riesgos**

La evaluación de riesgos es una parte fundamental de la gestión de riesgos en la seguridad de la información. Este proceso permite a las organizaciones identificar, analizar y priorizar los riesgos que podrían afectar sus activos de información críticos. Los criterios para la evaluación del riesgo son esenciales para asegurar que este proceso sea sistemático, consistente y efectivo [52].

Los criterios para la evaluación del riesgo incluyen una serie de parámetros y estándares que ayudan a medir la probabilidad y el impacto de los riesgos identificados. Estos criterios permiten a las organizaciones determinar cuáles riesgos son aceptables y cuáles requieren medidas de mitigación. Además, proporcionan una base para comparar diferentes riesgos y decidir sobre la asignación de recursos para su tratamiento. La Tabla 2. describe varios criterios para la evaluación de riesgos [52].

Tabla 2. Criterios para la Evaluación de Riesgos [52]**.**

Criterio	Descripción
Criterios de Evaluación del Riesgo	incluyen factores como el valor estratégico del proceso de información, la criticidad de los activos, los requisitos legales y reglamentarios, y las expectativas de las partes interesadas. Evaluar estos factores ayuda a determinar la importancia de los riesgos para la organización.
Criterios de Impacto	Se refieren al grado de daño o costos que un riesgo puede causar a la organización. Esto incluye incumplimiento de los requisitos legales, la pérdida de confidencialidad, integridad y disponibilidad de la información, así como el impacto financiero, reputacional y operativo.
Criterios de Aceptación del Riesgo	Definen los niveles de riesgo que la organización está dispuesta a aceptar. Los criterios de aceptación del riesgo están influenciados por las políticas, objetivos y tolerancia al riesgo de la organización, así como por las expectativas de las partes interesadas.

La literatura ha sugerido diferentes marcos que asisten en el proceso de evaluación y priorización de riesgos que pueden ser utilizados en el contexto de ZT. Dentro de estos marcos, el MITRE ATT&CK y el NIST (SP800-37) son herramientas esenciales en este contexto. La combinación de estos marcos permite a las organizaciones adoptar un enfoque integral y proactivo para la seguridad cibernética, fortaleciendo su postura defensiva en un entorno cada vez más complejo y desafiante [54].

El marco MITRE ATT&CK que por sus siglas en inglés significa *Adversarial Tactics, Techniques, and Common Knowledge*, es una base de datos curada que documenta las tácticas y técnicas utilizadas por adversarios cibernéticos en ataques reales [55]. Este marco ofrece una visión detallada de las amenazas cibernéticas y proporciona un mapeo de estas amenazas a las mitigaciones correspondientes [54], [55], Esto permite a las organizaciones identificar las tácticas y técnicas específicas que los adversarios pueden emplear en su infraestructura. En un modelo de ZT, este conocimiento es crucial para diseñar controles de seguridad que aborden directamente estas amenazas [56], [57].

Estas características, hace que MITRE ATT&CK ayude a las organizaciones a evaluar y priorizar los riesgos al mapear las técnicas de ataque conocidas a las mitigaciones efectivas. Esto facilita la implementación de medidas de seguridad que reduzcan la probabilidad y el impacto de ataques exitosos. La naturaleza dinámica del marco MITRE ATT&CK, que se actualiza regularmente con nuevas tácticas y técnicas, permite a las organizaciones mantener un enfoque de seguridad adaptativo y actualizado. Esto es fundamental para el modelo de ZT, el cual requiere una vigilancia continua y la capacidad de responder rápidamente a nuevas amenazas [58].

Por su parte, El NIST *Risk Management Framework* (RMF) (SP800-37) es un conjunto de directrices desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos para la gestión de riesgos de seguridad de la información. Este marco proporciona un enfoque estructurado para la evaluación, respuesta y monitoreo de riesgos, y está estrechamente alineado con otros estándares de seguridad como la ISO/IEC 27005. El RMF del NIST prescribe un proceso detallado para la evaluación de riesgos, que incluye la categorización de la información y los sistemas de información, la selección e implementación de controles de seguridad, y la evaluación de la efectividad de estos controles. En un entorno ZT, esta evaluación rigurosa es esencial para asegurar que todos los accesos y actividades sean continuamente monitoreados y verificados [59].

Adicionalmente, SP800-37 proporciona una lista de controles de seguridad (documentados en SP 800-53) que pueden ser utilizados para mitigar las amenazas identificadas. Estos controles cubren una amplia gama de áreas, desde la gestión de identidades y accesos hasta la protección de datos y la respuesta a incidentes. Así mismo, el marco NIST enfatiza la importancia del monitoreo continuo y la evaluación periódica de los controles de seguridad, lo cual se alinea perfectamente con el principio de ZT de mantener una vigilancia constante sobre todas las actividades y accesos dentro de la red [54], [60].

El uso de los marcos NIST RMF y MITRE ATT&CK para la evaluación y priorización de riesgos bajo el contexto de ZT ofrece numerosos beneficios, como se detalla en la Tabla 3.

Tabla 3. Beneficios de los Marcos NIST (SP800-37) y MITRE ATT&CK

Marcos	Beneficios	Referencia
NIST (SP800-37)	Proporciona un enfoque sistemático y repetible para la gestión de riesgos de seguridad de la información. Facilita el cumplimiento de diversas normativas y regulaciones de seguridad. Facilita la capacidad de adaptación a las necesidades específicas de diferentes organizaciones y entornos de TI	[61]
MITRE ATT&CK	Proporciona una visión holística de las amenazas y las técnicas de ataque. Ayuda a las organizaciones a fortalecer sus defensas mediante la identificación de brechas y la implementación de controles específicos. Facilita la alineación de las prácticas de seguridad con estándares reconocidos y mejores prácticas.	[54]

1.1.4 Zero Trust y Arquitectura de Zero Trust

- **Concepto de ZT y contexto histórico**

El concepto de ZT o Confianza Cero se basa en la premisa de que no se debe confiar implícitamente en ningún usuario o sistema, independientemente de si están dentro o fuera de la red de una organización. Este concepto se puede resumir en la frase "nunca confiar, siempre verificar" [1], [62], [63]. Esta filosofía ha llevado a que las organizaciones adopten ZT para cumplir con las demandas de las empresas modernas. Para entender su carácter revolucionario, es necesario analizar la evolución de este concepto y cómo este transforma el pensamiento tradicional sobre redes y seguridad empresarial (Figura 8).

Considerando esta frase, la literatura académica ha sugerido que este concepto ya estaba presente en las prácticas de ciberseguridad antes de ser formalmente nombrado así. En 1994, el término "Zero Trust" comenzó a aparecer en la literatura académica. Este concepto emergente proponía una visión revolucionaria de la ciberseguridad, donde se asumía que no se debería confiar en ninguna entidad dentro o fuera de la red corporativa por defecto. Esto representó un cambio significativo respecto al modelo tradicional de "castillo y foso", que confiaba en la protección de los perímetros de la red [64]. Este enfoque naciente instaba a verificar y autenticar cada solicitud de acceso independientemente de su origen, fomentando una postura de seguridad que enfatiza la defensa en profundidad [65].

En 2010, John Kindervag acuñó el término "confianza cero" mientras trabajaba en Forrester, y pronto se convirtió en un término común para una variedad de soluciones de ciberseguridad que priorizan la evaluación de la confianza en cada transacción en lugar de basarse en la ubicación en la red. Tanto el sector empresarial como las instituciones educativas han adoptado métodos de seguridad basados en Confianza Cero, dejando atrás la seguridad perimetral [66].

En 2014, Google implementó una arquitectura de ZT (ZTA) conocida como BeyondCorp, basada en los informes de Kindervag. Esta iniciativa ayudó a solidificar los conceptos de Confianza Cero en la comunidad de tecnologías de la información (TI). Sin embargo, tomó casi una década para que estas arquitecturas se generalizaran, impulsadas por la adopción creciente de servicios móviles y en la nube [67].

En 2018, Forrester publicó su informe titulado "The Zero Trust eXtended (ZTX) Ecosystem", en el cual evolucionó el modelo original de Zero Trust para adaptarlo a un entorno más complejo y dinámico incorporando nuevas áreas críticas como identidad, dispositivos, datos, cargas de trabajo y automatización, permitiendo un enfoque de seguridad más integral. Esta expansión del modelo responde a la creciente sofisticación de los ataques y la necesidad de proteger activos en entornos híbridos y en la nube; además, refuerza la importancia de una estrategia de ciberseguridad que combine visibilidad, segmentación y automatización [151].

Posteriormente, en 2019, Gartner introdujo el concepto de “Secure Access Service Edge” (SASE) o perímetro de acceso seguro, revitalizando el concepto de ZT al redefinirlo como Acceso a la Red de Confianza Cero (ZTNA) [67]. Seguidamente, el Instituto Nacional de Estándares y Tecnología (NIST) publicó en el 2020 el borrador del estándar "NIST SP 800-207". Este documento proporcionaba una guía detallada para organizaciones que deseaban implementar un enfoque ZT, abordando aspectos técnicos y operativos. La publicación de este documento fue un hito importante, ya que estableció un marco oficial y normativo para la adopción de ZT en entornos gubernamentales y empresariales, impulsando su adopción a gran escala [63].

En 2021, la Orden Ejecutiva 14028 del presidente de EE.UU. y el modelo de madurez de Zero Trust de la Agencia de Seguridad Nacional (NSA) impulsaron aún más la adopción de ZT. La EO 14028 establecía directrices para mejorar la seguridad cibernética en todo el gobierno federal, incluyendo la adopción de principios de ZT. El modelo de madurez de ZT de la NSA proporcionó un camino estructurado para que las agencias federales evaluaran y mejoraran su postura de seguridad a medida que migraban hacia una ZTA [68].

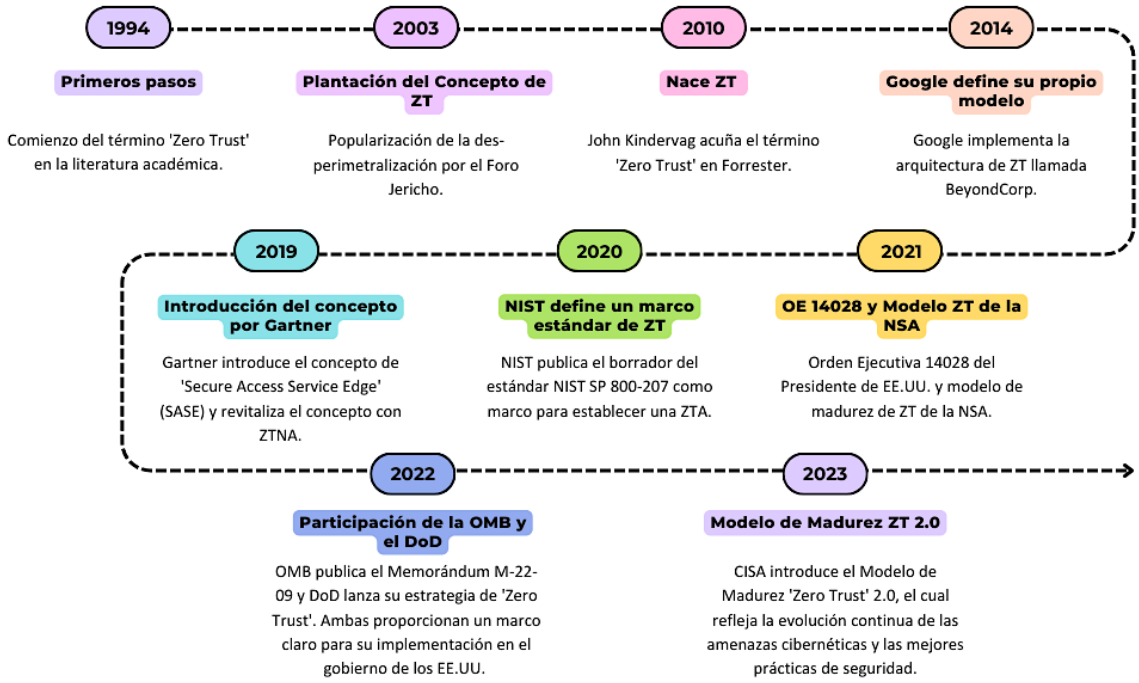
En 2022, la Oficina de Gestión y Presupuesto (OMB) publicó el Memorándum M-22-09, que formalizaba la transición del gobierno de los EE.UU. hacia los principios de ciberseguridad de ZT [69]. Además, el Departamento de Defensa (DoD) lanzó su estrategia de Zero Trust, estableciendo requisitos y plazos específicos para las agencias militares y de defensa. Estas iniciativas subrayaron el compromiso del gobierno federal con la adopción de Zero Trust, proporcionando un marco claro y directrices para su implementación a nivel nacional [70].

Finalmente, en 2023, la Agencia de Seguridad de Infraestructura y Ciberseguridad (CISA) introdujo el Modelo de Madurez Zero Trust 2.0, una actualización que refinaba y ampliaba las directrices anteriores para ayudar a las agencias federales a evaluar y mejorar su progreso en la implementación de ZT. El Modelo de Madurez 2.0 refleja la evolución continua de las amenazas cibernéticas y las mejores prácticas de seguridad, proporcionando un recurso valioso para organizaciones que buscaban fortalecer su postura de seguridad a través de una adopción más amplia y profunda de los principios de Zero Trust [71].

Considerando lo anteriormente descrito, La adopción de una filosofía de ZT ha generado impactos significativos en diferentes sectores. En el sector financiero, la adopción de prácticas de Confianza Cero es particularmente crucial debido a que las instituciones financieras manejan datos altamente sensibles y operan en un entorno regulatorio estricto. Por lo tanto, la implementación de un modelo de ZT puede mejorar significativamente la seguridad al garantizar que cada solicitud de

acceso se evalúe minuciosamente, minimizando el riesgo de brechas de seguridad y protegiendo los activos críticos de la organización. Al aplicar tecnologías avanzadas y enfoques dinámicos, las instituciones financieras pueden fortalecer su postura de seguridad y cumplir con los requisitos regulatorios, asegurando una protección robusta contra amenazas emergentes [62].

Figura 8. Historia de Zero Trust. [Elaboración propia].



- **Elementos de Zero Trust**

ZT se basa en el principio de que ningún usuario, dispositivo o aplicación debe ser confiado por defecto, incluso si se encuentran dentro de la red de una organización. Este enfoque moderno de la ciberseguridad es esencial para proteger contra amenazas internas y externas. La implementación de la Confianza Cero se realiza a través de varios elementos clave que aseguran una verificación continua y una protección integral. Según el Instituto Nacional de Estándares y Tecnología (NIST), estos elementos son esenciales para establecer una arquitectura de seguridad sólida y adaptable [63]. A continuación, se presentan los principales elementos de la Confianza Cero, cada uno diseñado para abordar diferentes aspectos de la seguridad dentro de una organización (Tabla 4).

Tabla 4. Elementos Clave de la Confianza Cero. Adaptado de [63].

Elemento de ZT	Descripción
Región de Confianza Implícita	Asumir la presencia de posibles atacantes dentro de la red de la empresa y priorizar la seguridad mediante la autenticación y el cifrado de comunicaciones.
Políticas de Uso de Dispositivos Personales (BYOD)	Permitir que los usuarios accedan a recursos empresariales utilizando dispositivos personales, aplicando políticas adecuadas.
Política de Seguridad	Mantener la seguridad al mover activos y cargas de trabajo entre infraestructuras propiedad de la empresa y otros entornos, incluyendo usuarios remotos y aplicaciones en la nube.
Suposición de Red Local No Confiable	Asumir que las conexiones de red locales de usuarios remotos no son confiables y que todo el tráfico puede ser vigilado y manipulado.
Menor Infraestructura Propiedad de la Empresa	En ciertas circunstancias, las entidades propiedad de la empresa pueden necesitar accesibilidad a la red local para funciones esenciales como la resolución de Sistema de Resolución de Dominio (DNS).
Controles de Acceso Responsivos al Contexto	Ajustar dinámicamente los controles de acceso basados en datos contextuales, asegurando niveles adecuados de seguridad según la situación y las amenazas potenciales.
Monitoreo y Validación Continuos	Mantener el monitoreo en tiempo real de las acciones de los usuarios, la salud de los dispositivos y el comportamiento de las aplicaciones, validando regularmente la efectividad de los controles de seguridad.
Protección de Datos Segura	Implementar mecanismos robustos de protección de datos, como cifrado y tokenización, y establecer controles de acceso estrictos.
Análisis del Comportamiento de Usuarios y Entidades	Utilizar análisis avanzados para examinar el comportamiento de usuarios y objetos, detectando patrones y anomalías que podrían indicar amenazas.
Ausencia de una Percepción Falsa de Seguridad	Mantener una verificación continua de credenciales, reconociendo que la familiaridad con la organización puede llevar a la identificación de vulnerabilidades por parte de insiders.

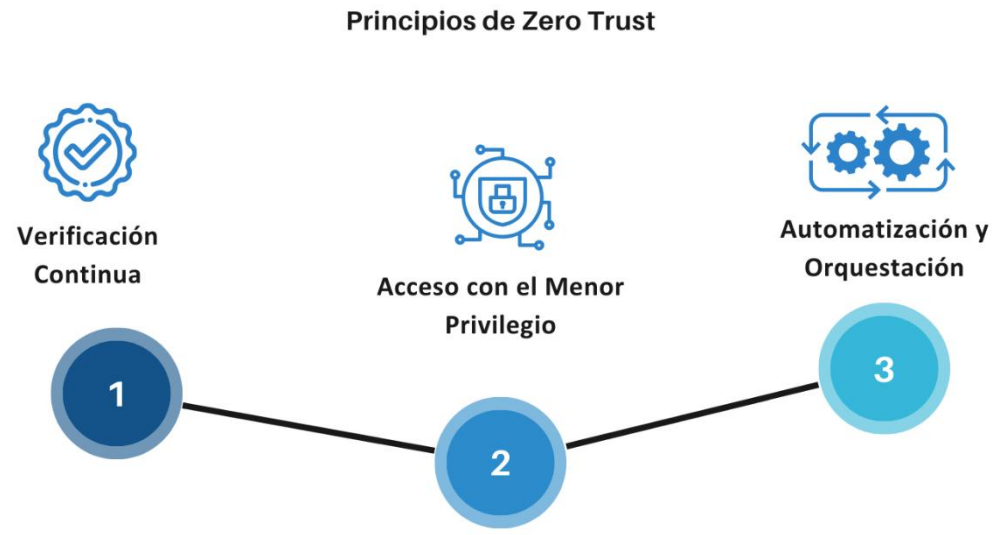
- **Principios de Zero Trust**

Tradicionalmente, en la infraestructura informática se distinguen dos tipos de redes: las redes confiables (internas) y no confiables (externas). ZT, en cambio, elimina esta distinción y asume

que toda red es no confiable, proponiendo que cada acceso debe ser autenticado y autorizado continuamente, sin importar la ubicación del usuario o dispositivo [1], [62], [63], [72].

Considerando esto, para implementar adecuadamente la filosofía de ZT, el NIST proporciona siete principios que deben ser considerados [63]. Sin embargo, diferentes organizaciones desglosan estos principios en tres fundamentales: verificación continua, acceso con el menor privilegio y automatización y orquestación (Figura 9) [62].

Figura 9. Principios de Zero Trust. Adaptado de [62].



A continuación, se explican brevemente estos principios:

1. **Verificación Continua**

   La confianza implícita no se otorga en ningún momento; cada solicitud de acceso debe ser autentificada y autorizada, garantizando que las entidades que interactúan con los recursos de la red sean legítimas [62], [63]. Este enfoque proactivo permite una detección temprana de amenazas y asegura que solo las entidades autorizadas puedan acceder a los recursos, limitando el riesgo de ataques internos [73].

2. **Acceso con el Menor Privilegio**

   Los usuarios y dispositivos solo reciben los permisos mínimos necesarios para cumplir sus funciones. Esto limita el alcance de los posibles daños en caso de un ataque y evita el

movimiento lateral dentro de la red [62], [74] . Este principio es clave para reducir la exposición a riesgos y cumplir con las normativas de seguridad [63].

3. **Automatización y Orquestación**

   La recopilación automatizada de contexto y la respuesta dinámica a incidentes se apoyan en inteligencia artificial y aprendizaje automático, mejorando la capacidad de las organizaciones para ajustar políticas en tiempo real [1], [62], [63]. La orquestación asegura una integración eficaz de diferentes herramientas de seguridad, creando un sistema cohesivo y adaptable [62].

- **Arquitectura de Zero Trust**

ZT redefine el enfoque de seguridad, eliminando la confianza implícita en redes internas o externas. Su principio fundamental, "nunca confiar, siempre verificar", asegura que cada solicitud de acceso sea autenticada y autorizada en tiempo real, independientemente de la ubicación o el origen de la solicitud [1], [62], [63], [72]. La ZTA implementa los principios descritos anteriormente al centrarse en proteger los recursos, no los segmentos de red, otorgando acceso solo cuando sea necesario y verificando las credenciales antes de establecer cualquier conexión [63].

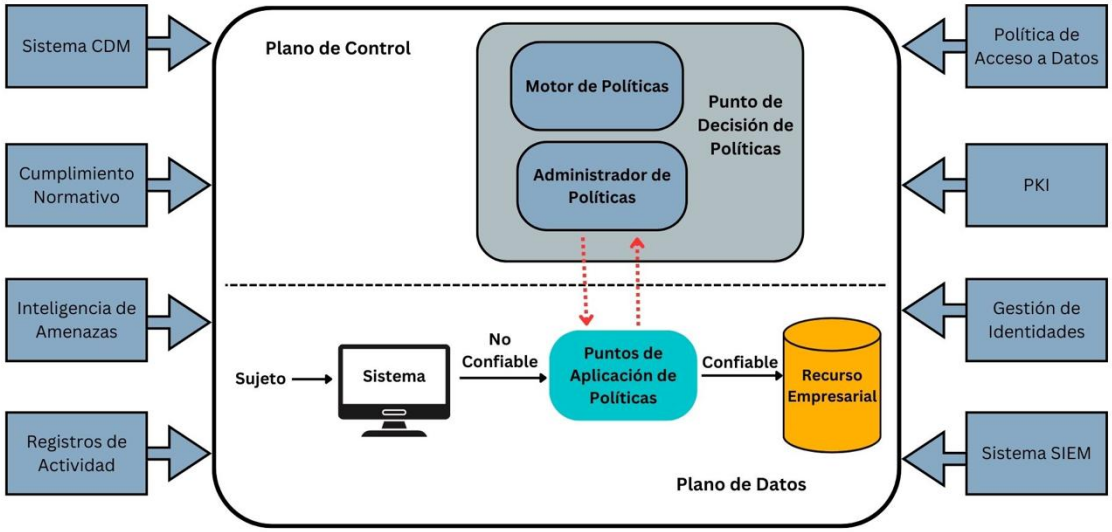
A diferencia de los modelos tradicionales basados en perímetros, ZTA responde a las tendencias actuales en redes empresariales, donde los usuarios remotos y los activos en la nube operan fuera de los límites físicos de la red de la empresa. En este sentido, la seguridad ya no se basa en la ubicación de la red, sino en el control riguroso de los accesos a los recursos [75]. La implementación de ZTA sigue las guías del NIST, como se detalla en la Publicación Especial SP800-207, que proporciona un marco para asegurar los recursos críticos en cualquier entorno [75]

Además, ZTA promueve una comprensión transparente de las actividades de procesamiento de datos, identificando datos sensibles y aplicando medidas de seguridad específicas para la prevención, detección y respuesta. Teniendo en cuenta esto, la confianza en la seguridad de los datos y el acceso a recursos no debe basarse únicamente en las promesas de proveedores o declaraciones de políticas aceptadas por los usuarios. Es esencial verificar esta confianza en los Puntos de Aplicación de Políticas (Policy Enforcement Point, PEPs) o Puntos de Decisión de Políticas (PDPs) antes de permitir cualquier acceso a datos o segmentos de red. Esta verificación requiere la segmentación de la red y la implementación de cortafuegos de próxima generación gestionados de manera centralizada como puntos de aplicación de políticas, ya sea en entornos en la nube, locales o proporcionados por proveedores de servicios de TI [76].

Para mitigar las incertidumbres, ya que no pueden eliminarse por completo, el enfoque se centra en la autenticación, la autorización y la reducción de las zonas de confianza implícita, todo ello manteniendo la disponibilidad y minimizando los retrasos en los mecanismos de autenticación. Las reglas de acceso se diseñan con la mayor granularidad posible para asegurar que se otorguen solo los privilegios mínimos necesarios para realizar la acción solicitada [63].

En este sentido, ZTA permite una detección más efectiva de ciberataques y accesos no autorizados a través del procesamiento centralizado de datos de seguridad y registros [63], [77], [78]. La combinación de la monitorización integral, el análisis de patrones de uso legítimo, la inteligencia de amenazas y la correlación de datos asegura una protección más robusta y adaptable frente a las amenazas emergentes, [79]. La Figura 10 ilustra la relación y las interacciones entre los componentes de ZTA.

Figura 10. Interacciones entre los Componentes de la Arquitectura Zero Trust. Adaptado de [63].



Considerando lo anterior, la adopción de una ZTA presenta numerosas ventajas. En primer lugar, mejora significativamente la seguridad al eliminar la confianza implícita en los usuarios y dispositivos dentro de la red, lo que reduce el riesgo de brechas internas y externas. En segundo lugar, la capacidad de integrar inteligencia de amenazas en tiempo real permite una respuesta rápida y adaptativa a nuevas amenazas, lo que es crucial en un panorama de ciberseguridad en constante evolución, lo cual proporciona a las empresas la agilidad necesaria para responder rápidamente a nuevos desafíos de seguridad. Finalmente, el control granular que ofrece la ZTA, permite una gestión más precisa y dinámica sobre quién accede a qué recursos y bajo qué condiciones [77], [78].

En síntesis, las organizaciones al aplicar el principio de "nunca confiar, siempre verificar", pueden fortalecer su postura de seguridad y proteger de manera efectiva sus activos más críticos en un entorno digital en constante evolución, contribuyendo así a que la organización logre una comprensión transparente de las actividades de procesamiento de datos, identifique datos

sensibles o críticos, y aplique niveles adecuados de medidas de seguridad relacionadas con la prevención, detección y reacción [63], [80].

Aunque la implementación de ZTA brinda varias ventajas, su adopción no está exenta de desafíos. La complejidad y el costo de establecer una ZTA pueden ser significativos, ya que requiere la integración cuidadosa de múltiples sistemas y tecnologías. La gestión de políticas también puede volverse complicada, especialmente en grandes organizaciones con una gran cantidad de usuarios y dispositivos. Además, la evaluación continua y el monitoreo pueden afectar el rendimiento de los sistemas si no se implementan de manera eficiente, lo que requiere una infraestructura robusta y bien diseñada [77].

- **Pilares Fundamentales de ZTA**

Los pilares de ZTA aseguran que se sigan los principios de confianza cero en toda la infraestructura de una organización. Diferentes estudios que han implementado la ZTA, se han basado en el marco de ZTA del NIST, el cual se estructura en varios pilares que son la Identidad, Dispositivos (Puntos Finales), Red, Aplicaciones y Cargas de Trabajo, Datos, visibilidad y analítica, e infraestructura (Figura 11). Estos pilares son esenciales para la implementación de una ZTA robusta y efectiva [63], [81], [82].

Figura 11. Pilares Fundamentales de ZTA [82].

Como se observa en la Figura 11, la ZTA mediante la evaluación continua del riesgo y un motor de validación en tiempo real de directivas de seguridad en su núcleo, proporciona una protección robusta a través del análisis de señales e inteligencia de amenazas. Este enfoque asegura que tanto las identidades como los dispositivos sean verificados y autenticados rigurosamente antes de concederles acceso a datos, aplicaciones, infraestructura y redes [63], [76], [78], [83], [84], [85]. Este proceso no solo previene accesos no autorizados, sino que también garantiza que los dispositivos conectados cumplan con los estándares de seguridad necesarios, minimizando así las vulnerabilidades y los posibles puntos de entrada para ataques cibernéticos. En conjunto, estos pilares forman una defensa sólida y adaptable que protege de manera proactiva los activos críticos en un entorno digital cada vez más complejo y amenazante [62], [63], [82].

Considerando lo anterior, el presente trabajo de tesis se centra específicamente en los pilares de **Identidad, Dispositivos y Red**, ya que estos son fundamentales para establecer una estrategia de ciberseguridad robusta y adaptable en las instituciones financieras de Colombia. Esto se debe a que esta estrategia no solo fortalece el control de acceso, sino que también mejora la seguridad interna, garantiza la protección de datos sensibles, mejora la capacidad de respuesta a amenazas y asegura el cumplimiento normativo, lo cual es esencial para mantener la confianza de los clientes y la integridad del sistema financiero colombiano. Considerando esto, a continuación, se describen los tres pilares en los cuales la tesis tiene su principal enfoque.

- **Identidad**

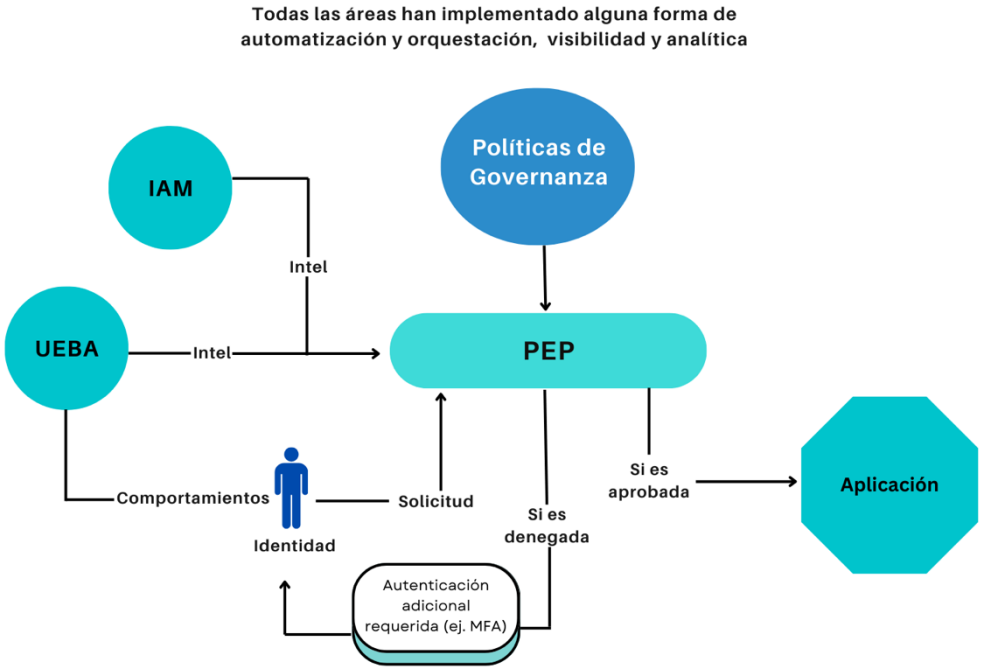
El pilar de la identidad es fundamental y generalmente el primero en cualquier modelo de madurez de ZTA. Este pilar se centra en el "quién" dentro de una infraestructura, identificando tanto a los usuarios humanos como a las entidades no humanas que solicitan acceso a datos, redes, aplicaciones y dispositivos. Por lo tanto, las herramientas de gestión de identidades y accesos (IAM) son esenciales en este contexto [77], [78], [81], [86], [87].

Un componente central de la Identidad en una ZTA es la autenticación. Garantizar que un usuario es quien dice ser es de máxima prioridad. Tradicionalmente, esto se logra mediante el uso de contraseñas, requiriendo que el usuario inicie sesión antes de otorgarle acceso. Sin embargo, en el marco de una ZTA, se recomienda encarecidamente el uso de herramientas de autenticación multifactor (MFA) [77]. Una manera de implementar MFA es requiriendo que el usuario apruebe el inicio de sesión en un dispositivo secundario, como una aplicación de autenticación en su teléfono. Otra opción es la autenticación sin contraseña, utilizando un token físico que el usuario posea, como una tarjeta inteligente, o mediante el uso de biometría [65]. El inicio de sesión único (SSO) es otro método de autenticación que puede incluirse. El SSO permite al usuario iniciar sesión una vez y obtener acceso a través de toda la organización. En el contexto de la ZTA, esto facilita una mayor visibilidad y análisis de las actividades y el perfil del usuario. A través del uso de estos métodos, la autenticación de usuarios puede volverse más fiable [77].

Una vez autenticado el usuario, debe ocurrir la autorización. En una ZTA, es crucial que incluso si un usuario es quien dice ser, solo se le otorgue el acceso mínimo necesario, conocido como el principio de menor privilegio. Aquí es donde entra en juego el Punto de Aplicación de Políticas (PEP) del marco NIST, imponiendo políticas sobre los usuarios que determinan qué autorizaciones pueden recibir [63]. Para adherirse realmente a los principios de confianza cero, incluso cuando se otorga autorización a un usuario, es necesario un monitoreo continuo. Esto puede lograrse mediante el uso de herramientas de IAM y análisis de comportamiento de usuario/entidad (UEBA) basadas en aprendizaje automático e inteligencia artificial. Estas herramientas pueden construir automáticamente perfiles de usuarios que determinen el nivel de riesgo y, de manera dinámica, establecer qué tipos de acceso pueden otorgarse [63], [77]

La implementación de estas estrategias dentro de una ZTA no solo asegura que la autenticación y autorización se manejen de manera robusta y dinámica, sino que también promueve una infraestructura resiliente que puede adaptarse rápidamente a nuevas amenazas, proporcionando un nivel de seguridad significativamente mejorado para proteger los activos críticos de la organización [79], [87], [88]. La Figura 12, presenta las características del pilar de identidad en una ZTA según el marco NIST.

Figura 12. Pilar de Identidad en la Arquitectura Zero Trust. Adaptado de [77].



Considerando que cualquier tráfico de red puede representar una amenaza constante, la filosofía de ZT sostiene que se debe asumir que cada usuario actúa de manera hostil y que las amenazas son ubicuas, tanto dentro como fuera de la red. En consecuencia, se restringirá automáticamente el acceso a cualquier tráfico que no cuente con una autorización explícita; es decir, todos los dispositivos, usuarios y flujos de red son continuamente autenticados, autorizados y validados al solicitar acceso [89]. Las estrategias de seguridad basadas en ZT otorgan los privilegios mínimos y el acceso a los recursos indispensables en el momento preciso, sin comprometer la capacidad para llevar a cabo una tarea específica; por lo que, al aplicar el principio de menor privilegio se contribuye a prevenir que los atacantes se desplacen lateralmente hacia recursos más críticos en caso de comprometer una cuenta o dispositivo [63].

Así mismo, el control de acceso es un elemento esencial de la seguridad que determina quién tiene permiso para acceder a determinados datos, aplicaciones y recursos y en qué circunstancias. Al igual que las claves y listas de invitados con aprobación previa protegen los espacios físicos, las directivas de control de acceso protegen los espacios digitales [90]. Las directivas de control de acceso dependen en gran medida de técnicas como la autenticación y la autorización, que permiten a las organizaciones verificar de forma explícita que los usuarios son quienes dicen ser y

que cuentan con el nivel adecuado de acceso basado en elementos contextuales como el dispositivo, la ubicación, el rol, entre otros [91], [92].

Como resultado, el control de acceso impide que los infiltrados u otros usuarios no autorizados accedan a información confidencial, como los datos de clientes y la propiedad intelectual. Además, reduce el riesgo de filtración de datos por parte de los empleados y mantiene a raya las amenazas web. Adicionalmente, en lugar de gestionarlos manualmente, las organizaciones con mayor seguridad dependen de soluciones de administración de identidad y acceso para implementar directivas de control de acceso [93]. Por ejemplo, modelos de confianza basados en *blockchain* han sido propuestos y desarrollados para la transparencia y precisión de los datos, mientras que el ZT se ha utilizado para la autenticación del usuario con el fin de mantener la integridad de los datos [94]. Para implementar con éxito un control de acceso en una estrategia de ZT, es necesario tener todos los usuarios creados en el directorio activo y federado, establecer una base establecida de los principios de la identidad, integrar todas las aplicaciones al directorio activo y verificar de forma explícita con autenticación fuerte [95].

En consecuencia, ZT se apoya en la identidad debido a que la información de identidad empleada para autenticar a un usuario desempeña un papel de gran importancia, ya que contiene datos esenciales como los atributos de identidad, los permisos de acceso, los patrones de comportamiento y la adscripción a roles y grupos. Según [96], el 97 % de los profesionales de seguridad informática coinciden en que la identidad representa uno de los elementos esenciales en un modelo de seguridad de ZT; la obtención de los datos de identidad necesarios implica además la necesidad de que todos los sistemas de seguridad se integren, respaldando así una estrategia de ZT. Esto lleva a que los sistemas de identificación y seguridad deban colaborar para obtener una visión más abarcadora del acceso y su utilización [97].

En la actualidad, las organizaciones en Colombia utilizan sistemas de información altamente tecnológicos para la gestión misional, lo que les permite ejecutar sus estrategias comerciales de manera efectiva. Dado a que la información se ha convertido en el valor más importante para muchas empresas, estas organizaciones reconocen la necesidad de proteger tanto los activos físicos como los intangibles. Por ello, deben desarrollar estrategias que garanticen la protección, confidencialidad e integridad de la información, cumpliendo con las regulaciones y estándares aplicables [98]. Esto hace que la seguridad de la información se convierta en prioridad para cualquier entidad, considerando la infraestructura tecnológica, organizacional y legal que debe ser protegida [99].

El enfoque sistemático propuesto por la ISO/IEC 27001 para la gestión de la seguridad de la información complementa el Pilar de Identidad, ya que establece políticas y procedimientos claros para la protección de los activos de información, alineando la estrategia de seguridad con los objetivos empresariales de la organización. Este enfoque ayuda a gestionar los riesgos de manera efectiva y asegura que se implementen controles adecuados para proteger la información sensible.

A raíz de lo descrito, la identidad es clave para la creación de políticas para ZT y para este enfoque, las políticas de acceso a los recursos empresariales se basan en la identidad y los atributos

asignados, además el requisito principal para el acceso a los recursos se basa en los privilegios de acceso otorgados a un usuario en cuestión [75]. Otros factores como el dispositivo utilizado, el estado del activo y los factores ambientales, pueden alterar el cálculo del nivel de confianza final y la autorización de acceso final, razón por la cual la gestión de usuarios y accesos será uno de los puntos que requiere mayor atención por parte de las entidades financieras en Colombia [49]. Tal como se observa en la Tabla 5, el compromiso de credenciales de usuarios privilegiados es el segundo rubro que más inquieta a las empresas grandes.

Tabla 5. Riesgos de Seguridad de la Información que Merecen Mayor Atención por Parte de la Entidad Financiera. Adaptado de [49].

Tipos de riesgo	Grande	Mediano	Pequeño	Total
Pérdida/robo de activos de información clasificada (Confidencial o sensible)	2,50	2,97	2,40	2,68
Indisponibilidad de servicio infraestructura crítica	3,67	3,06	3,63	3,37
Compromiso de credenciales de usuarios privilegiados	2,83	3,78	3,53	3,59
Secuestro de información	3,83	3,72	4,00	3,85
Denegación del servicio	5,50	4,25	3,97	4,24
Sabotaje o fraude a través de (personal interno)	3,50	4,31	4,50	4,32
Defacement v- Alteración en sitio web	6,17	5,91	5,97	5,96

Nota. En la tabla 5 se muestran 68 registros y los entrevistados priorizaban los riesgos del 1 al 7, siendo el 1 el riesgo más alto y 7 el riesgo más bajo.

Dicho de otra manera, la identidad se utiliza en el proceso de control de acceso para determinar qué recursos o acciones están disponibles y permitidas para un usuario en particular. Una vez que se ha establecido y autenticado la identidad, se pueden aplicar políticas de autorización para definir los permisos y privilegios asociados a esa identidad en función de roles, grupos u otras configuraciones específicas [94]. Ahora bien, la identidad en un modelo ZT, se refiere a la información que se utiliza para autenticar y autorizar a los usuarios que intentan acceder a los recursos una red o sistema. La identidad se utiliza para verificar quién es el usuario y determinar qué nivel de acceso se le debe otorgar [95].

Así pues, el control de acceso es un elemento esencial de la seguridad que determina quién tiene permiso para acceder a determinados datos, aplicaciones y recursos, y en qué circunstancias. Este mecanismo asegura que solo las personas adecuadas puedan ingresar, mientras que aquellas no autorizadas son bloqueadas. Cabe destacar que las políticas de control de acceso dependen en gran medida de técnicas como la autenticación y la autorización, las cuales permiten a las organizaciones verificar de forma explícita que los usuarios son quienes dicen ser y que poseen el nivel adecuado de acceso. Esto se basa en elementos contextuales como el dispositivo utilizado, la ubicación, el rol del usuario y otros factores relevantes [92].

Tomando en consideración lo anteriormente discutido, la identidad, la cual puede representar una persona, es el eje central de control en una ZTA. Si existe un interés de la identidad para acceder a un recurso se debe realizar un proceso de autenticación teniendo presente la validez de la identidad, permiso de acceder al recurso y siguiendo con el principio de mínimo privilegio [100]. La autenticación es el proceso que permite validar si una identidad puede acceder a un recurso.

En una ZTA, es fundamental implementar la MFA. Esta técnica reduce significativamente el riesgo de reutilización de usuarios y contraseñas al añadir una capa adicional de seguridad. De este modo, se dificulta que personas malintencionadas inicien sesión en nombre de otros, ya que los atacantes necesitarían tanto la contraseña como el acceso físico al dispositivo del usuario, como su teléfono. Es probable que las personas noten rápidamente si su teléfono desaparece, permitiéndoles reportarlo antes de que un atacante pueda utilizarlo para iniciar sesión. Según el NIST, esta medida es crucial para fortalecer la seguridad en la ZTA [101].

- **Pilar de Dispositivos**

Aunque gran parte de la atención en ZTA se ha centrado en la identidad, la postura de los dispositivos también juega un papel esencial al proporcionar el contexto necesario para decisiones de autorización basadas en el principio de menor privilegio de la postura de los dispositivos y su rol en las soluciones de ZT. La gestión segura de los dispositivos, también conocida como endpoints, es esencial para asegurar que todos los dispositivos conectados a una red sean autenticados y autorizados adecuadamente [102], [103].

La evolución de los ecosistemas de dispositivos, de homogéneos a diversos, ha transformado los enfoques tradicionales de control de acceso a la red. Anteriormente, los dispositivos gestionados eran predominantemente utilizados por empleados dentro de un perímetro de red seguro. Sin embargo, en la actualidad, la base de usuarios incluye empleados, *freelancers*, contratistas y terceros que utilizan tanto dispositivos corporativos como personales. Esto denota que los dispositivos en la red pueden no ser propiedad de la empresa ni ser configurables por ella [102]. Es decir, los visitantes y servicios contratados pueden incluir activos no empresariales que necesitan acceso a la red para realizar su función, lo que incluye políticas de "traiga su propio dispositivo" (*Bring Your Own Device*, BYOD). Esta diversificación, complica el control administrativo y eleva las preocupaciones de seguridad [65], [104].

Debido a lo anterior, las organizaciones deben ser aún más sensibles a qué dispositivos tienen acceso y a dónde. Cada dispositivo dentro de una organización debe ser considerado cuidadosamente. Al implementar una ZTA, es crucial tener en cuenta todos los activos en la infraestructura[105]. Esto abarca desde dispositivos personales hasta dispositivos remotos que pueden tener acceso a información, datos y recursos sensibles, como cuando los empleados trabajan desde casa.

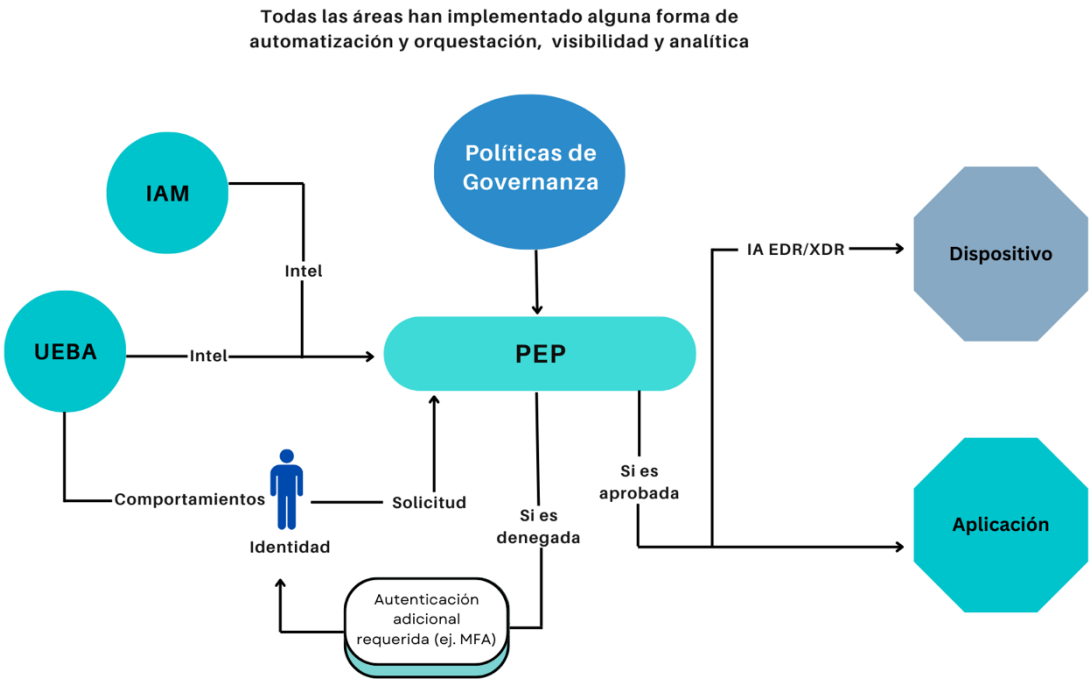
En este sentido, los dispositivos se han convertido en vectores significativos de ataques cibernéticos. El estudio [106], reveló que el 68% de las organizaciones había experimentado brechas de seguridad originadas en dispositivos de usuarios; estas brechas fueron exacerbadas por la pandemia, ya que las políticas de trabajo desde casa y BYOD aumentaron la responsabilidad de los usuarios sobre la seguridad de sus dispositivos, incrementando la probabilidad de vulnerabilidades no parcheada [102].

La confianza en los dispositivos es dinámica y depende del contexto, a diferencia de la identidad del usuario, que es relativamente estática. Las características de seguridad de un dispositivo, como el estado del firewall o la versión del sistema operativo, pueden cambiar y crear vulnerabilidades explotables. Debido a esto, los dispositivos también deben ser autenticados antes de permitirles la conexión a la red de la organización. Además, las configuraciones de un dispositivo deben cumplir con las políticas establecidas [77].

De este modo, los dispositivos deben pasar por algún tipo de protección contra amenazas, como las herramientas de Detección y Respuesta de Endpoints (EDR). Para continuar aplicando los principios de ZT, puede ser necesario utilizar herramientas EDR habilitadas por inteligencia artificial para detectar automáticamente amenazas y responder a ellas. Los EDR son cruciales en el modelo de ZTA, ya que cada uno de estos dispositivos puede convertirse en un punto de entrada para los atacantes si no se asegura adecuadamente [77]. Para proteger estos dispositivos, la literatura sugiere el uso de esquemas de encriptación ligeros, los cuales son adecuados para dispositivos con recursos limitados. La encriptación es vital para proteger los datos tanto en reposo como en tránsito [103].

La Figura 13 muestra cómo podrían verse las características del pilar de Dispositivos en una ZTA siguiendo el marco NIST. Esta representación visual es esencial para entender cómo los dispositivos se integran y cumplen con las políticas de una ZTA, asegurando que cada componente de la infraestructura esté adecuadamente protegido y monitoreado. La autenticación robusta y la protección continua contra amenazas son fundamentales para mantener la integridad y la seguridad de la red en un entorno cada vez más complejo e interconectado [77].

Figura 13. Pilar de Dispositivos en la Arquitectura Zero Trust. Adaptado de [77].



Es importante resaltar que algunos autores han discutido que los enfoques tradicionales de seguridad de dispositivos, como la gestión de dispositivos móviles (MDM) y la EDR, ofrecen cierto control, pero presentan desafíos significativos, especialmente con dispositivos personales. Por lo tanto, en el marco de ZTA, la postura del dispositivo es crucial para evaluar en tiempo real si se debe autorizar el acceso de un usuario. ZTA requiere verificaciones explícitas cada vez que un usuario intenta acceder a un recurso, utilizando tanto la identidad del usuario como la postura del dispositivo para tomar decisiones basadas en el principio de menor privilegio. La postura del dispositivo proporciona un contexto esencial que puede incluir la versión del sistema operativo, el estado del software antivirus y la configuración biométrica [102].

La filosofía de confianza cero, como lo establece NIST, se centra en la premisa fundamental de que ningún recurso es inherentemente confiable. Esto significa que ningún dispositivo o usuario, ya sea interno o externo, debe ser confiado por defecto, independientemente de su ubicación física o de red [63]. Por lo tanto, cada solicitud de acceso debe ser autenticada y autorizada de manera continua antes de concederle acceso a los recursos. Este enfoque contrasta con los modelos tradicionales de seguridad perimetral, donde los recursos dentro del perímetro se consideran inherentemente confiables. La ZTA, en cambio, asume que siempre puede haber una brecha y, por lo tanto, cada entidad debe ganarse y mantener su confianza de manera constante [105]

Las credenciales de los sujetos por sí solas son insuficientes para la autenticación de los dispositivos a un recurso empresarial. Los activos y flujos de trabajo que se mueven entre infraestructuras

empresariales y no empresariales deben mantener una política y postura de seguridad consistentes [73]. Esto incluye dispositivos que se trasladan de redes empresariales a redes no empresariales, como usuarios remotos, y cargas de trabajo que migran de centros de datos locales a instancias en la nube no empresariales. Por esta razón, para fortalecer la seguridad de los dispositivos, es esencial implementar medidas que permitan la autenticación continua y la evaluación de la postura de seguridad. Esto se puede lograr mediante la implementación de sistemas de monitoreo y reporte que proporcionen una visibilidad completa y en tiempo real de todos los dispositivos conectados a la red [107].

Cabe considerar que la consistencia en la aplicación de políticas de seguridad es esencial para asegurar que los dispositivos mantengan su postura de seguridad incluso cuando se mueven entre diferentes entornos. Esto incluye asegurar que los dispositivos mantengan las mismas medidas de seguridad ya sea que operen en redes empresariales o no empresariales. Esta consistencia es crucial para prevenir cualquier brecha de seguridad que pueda surgir debido a la transición entre diferentes entornos [63], [73].

La integración de tecnologías avanzadas como la implementación de *gateways* y la *blockchain*, también juegan un papel crucial en la arquitectura. En el contexto de la ZTA, los *gateways* son dispositivos críticos que actúan como puntos de control entre diferentes redes o entre una red interna y externa. Su función principal es autenticar y autorizar el tráfico de datos que entra y sale de la red, asegurando que solo los datos legítimos puedan pasar. Este control incluye la verificación de credenciales y la aplicación de políticas de seguridad basadas en el contexto, tales como la hora del día, la ubicación del dispositivo y el tipo de dispositivo [63], [108].

Asimismo, el *gateway* facilita la segmentación del tráfico de red, lo que significa que diferentes partes de la red están aisladas unas de otras. Esto es crucial para prevenir movimientos laterales en caso de que un atacante comprometa una parte de la red. Incluso, los *gateways* pueden filtrar paquetes de datos, bloqueando cualquier tráfico sospechoso o malicioso, y aplicar políticas de seguridad estrictas que se adaptan dinámicamente según el contexto de la solicitud [109].

De igual forma, la adopción de sistemas de detección y prevención de intrusiones distribuidas colaborativas (DCIDS) es esencial para abordar las vulnerabilidades de los dispositivos. Estas tecnologías permiten correlacionar y analizar múltiples piezas de evidencia sospechosa de diversas fuentes en la red, reduciendo así las tasas de falsos positivos y negativos. Sin embargo, la naturaleza distribuida de estas tecnologías aumenta la superficie de ataque, ya que los atacantes podrían dirigirse a múltiples nodos IDS para establecer un punto de apoyo furtivo [110].

La incorporación de la tecnología *blockchain*, conocida por su inmutabilidad y transparencia, ofrece nuevas oportunidades para mejorar la seguridad de los *endpoints* en una ZTA. Al integrar *blockchain,* se pueden crear registros inmutables y transparentes de todas las transacciones y eventos de seguridad. Esto asegura que los datos compartidos entre los nodos de los DCIDS no sean alterados, manteniendo la integridad de la información. Esta tecnología puede fortalecer el proceso de detección al proporcionar una capa adicional de seguridad para los datos de contexto de los dispositivos, como el estado del sistema operativo, los niveles de parches de software y las

direcciones IP de origen. Esta integración garantiza que incluso si un dispositivo es comprometido, los registros de seguridad y los datos de contexto no puedan ser manipulados, preservando así la confianza en la infraestructura de seguridad [110].

Aunque la integración de *blockchain* en ZTA presenta ventajas significativas, también plantea desafíos como el rendimiento y la sobrecarga computacional. Es crucial investigar más sobre cómo implementar *blockchain* de manera eficiente sin comprometer el rendimiento de la red. Además, la elección del tipo adecuado de *blockchain* (pública o privada, con permisos o sin permisos) es fundamental para garantizar que se cumplan los requisitos específicos de seguridad y operacionales de la organización.

- **Pilar de Red**

La seguridad de la red se refiere a las medidas de seguridad implementadas en las redes empresariales o institucionales para proteger sus activos de información y prevenir posibles ataques externos. Estas medidas incluyen la identificación y valoración de los activos de información, la definición de políticas de seguridad, la implementación de herramientas como cortafuegos, sistemas de detección de intrusos y redes Privadas Virtuales (VPN), y la realización de pruebas técnicas de penetración para evaluar la efectividad del sistema de seguridad [111]

Es importante destacar que la concientización del personal corporativo en temas de seguridad también es importante para garantizar la efectividad de las medidas de seguridad de la red [112]. Además, los componentes válidos para tener en cuenta en la seguridad de la red y los cuales se deberán abordar como parte de la investigación y prueba de su efectividad en la metodología son los firewalls, y el Perímetro Definido por Software (SDP). Esto es trascendental para complementar la revisión con la autenticación de la identidad y la postura del dispositivo con el fin de declarar la confianza [113].

Cabe considerar que, una política de seguridad establece qué elementos deben ser protegidos y qué se espera de los usuarios del sistema. Esto sirve como base para la planificación de la seguridad al diseñar nuevas aplicaciones o expandir la red existente, se detallan las responsabilidades de los usuarios como la protección de información confidencial y la creación de contraseñas robustas, entre otros. Además, la política de seguridad debe abordar la supervisión de la efectividad de las medidas de seguridad, lo que ayuda a identificar posibles intentos de eludir las defensas[114]. Por lo tanto, es crucial definir con claridad los objetivos de seguridad al desarrollar una política, ya que una vez creada, el siguiente paso es implementar sus reglas. Esto requiere la capacitación de los empleados y la incorporación de hardware y software necesarios para hacer cumplir dichas reglas [115].

En esta perspectiva, el acceso a la red en las organizaciones debe ser un punto clave no solo para el consumo de aplicaciones sino también para el fortalecimiento de la seguridad a nivel de infraestructura, verificando quién, qué, cuándo, dónde, por qué y cómo se conectan a los recursos empresariales, restringiendo el acceso y minimizando el riesgo de pérdida de datos. El aislamiento

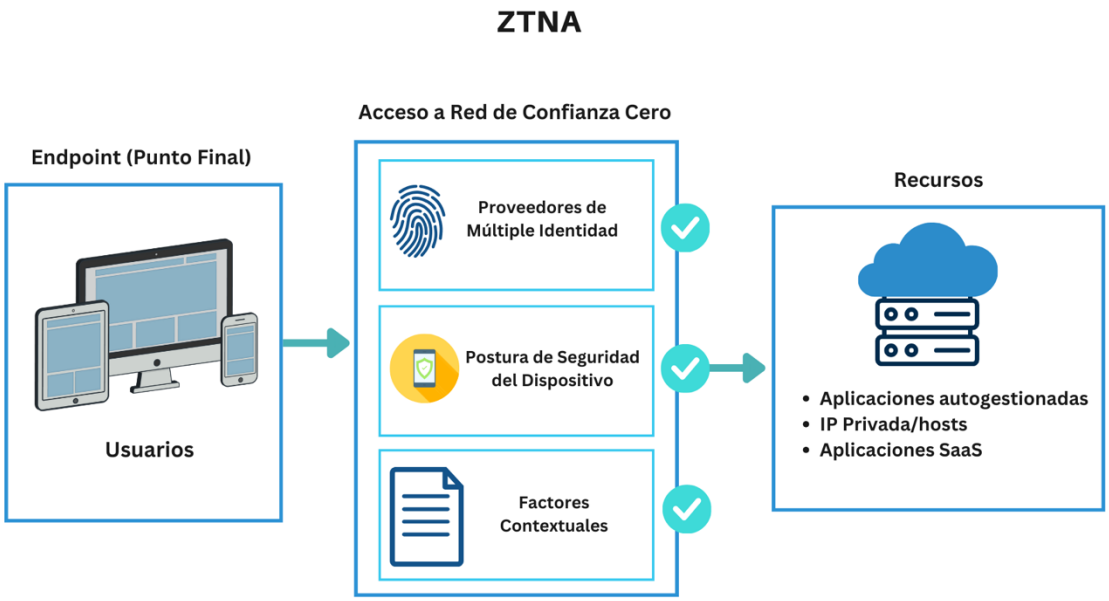
de accesos de red y de aplicaciones es fundamental; esto significa, permitir el acceso a la red, pero no acceso a todas las aplicaciones. Este aislamiento reduce los riesgos para la red, como la infección por dispositivos comprometidos, y solo otorga acceso a la aplicación a los usuarios autorizados [116]. ZTNA mejora la flexibilidad, la agilidad y la escalabilidad, lo que permite que los ecosistemas digitales funcionen sin exponer los servicios directamente a Internet, lo que reduce los riesgos de ataques distribuidos de denegación de servicio debido a que cada aplicación debe suscribirse en componentes de ZTNA con el fin de parametrizar la visibilidad y el acceso a la misma [88].

No obstante, durante los últimos años, el sector financiero ha experimentado una acelerada digitalización, cada vez son más los clientes que prefieren utilizar medios no presenciales para realizar transacciones bancarias, como pagos en línea o trámites a través de dispositivos móviles, además, en Colombia, se estima que el 81% de los internautas tiene acceso a servicios bancarios, y que de ese grupo, el 79,4% realizó operaciones bancarias en línea en el año 2018 [117]. Los bancos han sido pioneros en la implementación de medidas de seguridad para proteger a sus clientes, ya que el sector financiero ha sido tradicionalmente uno de los principales objetivos de las amenazas cibernéticas, tal como lo expresa [49], el 92% de las entidades bancarias en la región experimentaron algún tipo de evento de seguridad digital sean ataques exitosos o no y el 37% fueron víctimas de ataques exitosos y además, durante el año 2017 la motivación principal detrás de estos ataques fue de carácter económico afectando al 79% de las entidades bancarias víctimas [117].

1.1.5 Acceso a la Red de Confianza Cero (ZTNA)

El control de acceso es un componente crucial en ZTNA. Este modelo se basa en la autenticación continua y la evaluación de la confianza de la identidad y el contexto alrededor de una aplicación o un conjunto de aplicaciones antes de permitirles acceder a recursos específicos (Figura 14) [118]. La política de acceso en ZTNA se ajusta dinámicamente basándose en el comportamiento del usuario, la evaluación de riesgos y el contexto de la solicitud de acceso. Este enfoque centrado en la identidad y el contexto asegura que solo los usuarios y dispositivos autenticados y autorizados puedan acceder a aplicaciones específicas, en lugar de otorgar acceso amplio a toda la red [119]. Por lo tanto, ZTNA reduce la superficie de ataque y ofrece flexibilidad para colocar controles más cerca del recurso que se está protegiendo.

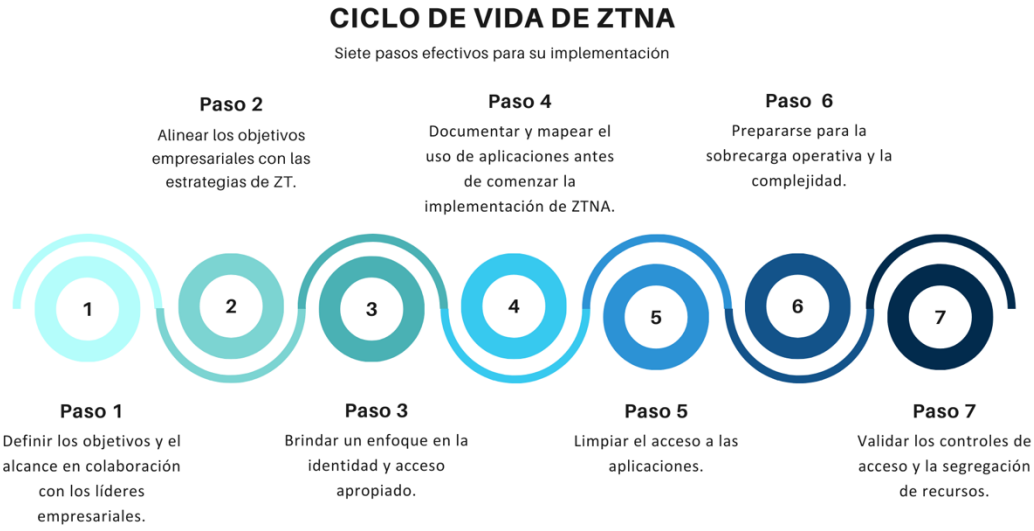
Figura 14. Modelo de Acceso a la Red de Zero Trust. Adaptado de [118].



Este modelo se alinea con los principios de la ZTA, que busca eliminar la confianza implícita en usuarios y dispositivos dentro de la red. En lugar de permitir acceso libre dentro de un perímetro una vez que un usuario ha sido autenticado, ZTNA asegura que cada intento de acceso a aplicaciones o recursos específicos se verifique y autorice, lo que complementa los controles definidos en ZTA [118], [119] [120]. Por tanto, ZTNA se convierte en una parte esencial de la implementación de ZTA, ya que provee las herramientas para llevar a cabo la verificación continua y la limitación de privilegios de acceso.

La implementación de ZTNA no es un proceso sencillo. Según [121], uno de los desafíos principales que enfrentan las organizaciones al implementar ZTNA es el desarrollo de políticas adecuadas, lo cual es esencial para el éxito de esta tecnología. De este modo, la adopción de ZTNA requiere un enfoque continuo y cíclico en la gestión del acceso remoto, adaptando las políticas de acceso a medida que cambian los niveles de riesgo y las necesidades del negocio. La Figura 15, describe brevemente el ciclo de vida para la incorporación de ZTNA.

Figura 15. Ciclo de vida de Acceso a la Red de Confianza Cero. Adaptado de [121].



A partir de lo señalado, diferentes estudios han discutido los beneficios de implementar un enfoque de ZTNA. Por ejemplo, varios estudios sobre el control de acceso basada en la identidad en el contexto de ZTNA destacó la importancia de identificar la legitimidad del usuario y evaluar las características de seguridad del usuario antes de permitir el acceso [86], [95], [96]. Este enfoque asegura que solo los usuarios y dispositivos que cumplen con los criterios de seguridad establecidos puedan acceder a los recursos de la red. Otro estudio implementó un modelo de control de acceso seguro para servicios en la nube utilizando principios de ZTNA. Este modelo empleó múltiples autenticaciones, clasificación de permisos y políticas dinámicas para gestionar el acceso a los recursos en un entorno de nube, garantizando así la seguridad y confiabilidad de los servicios [122].

Dado lo anterior, el principal beneficio de ZTNA radica en su capacidad para ofrecer seguridad a nivel granular. A diferencia de las redes privadas virtuales (VPNs), que permiten el acceso a la red completa una vez que se establece la conexión, ZTNA implementa un modelo de "nunca confiar, siempre verificar". Esto significa que cada solicitud de acceso a una aplicación es evaluada en función de múltiples factores, incluyendo la identidad del usuario, el dispositivo utilizado y el contexto de la solicitud. Esta verificación continua minimiza significativamente el riesgo de accesos no autorizados y movimientos laterales dentro de la red, ya que el acceso está estrictamente controlado y limitado a los recursos necesarios para cada usuario [123].

Además, ZTNA proporciona visibilidad completa sobre las conexiones y permite a las organizaciones aplicar políticas de seguridad detalladas y específicas. Esto es especialmente importante en entornos donde las aplicaciones son cada vez más distribuidas y accesibles desde múltiples ubicaciones y dispositivos. Con ZTNA, las políticas de acceso pueden ser dinámicas y adaptarse en tiempo real según el comportamiento del usuario y las condiciones del entorno, mejorando así la capacidad de respuesta ante amenazas [124].

Asimismo, [124] indica que muchas soluciones ZTNA ahora integran capacidades ligeras de validación de postura con puntajes de riesgo basados en el comportamiento del usuario. Por ejemplo, si un usuario conectado realiza una acción que se identifica como maliciosa, su puntaje de riesgo aumenta y se pueden activar políticas específicas al alcanzar ciertos umbrales configurados. Estas capacidades representan avances significativos hacia la implementación de un modelo de confianza adaptativa continua [88], [125]

A pesar de sus beneficios, ZTNA no elimina todos los riesgos. La implementación completa de ZTNA puede requerir más tiempo y esfuerzo del previsto inicialmente, lo que podría resultar en políticas excesivamente permisivas. Además, el intermediario de confianza podría convertirse en un punto único de falla, y su ubicación podría causar problemas de latencia para los usuarios. En adición, las credenciales comprometidas de los usuarios también representan una amenaza, ya que un atacante podría utilizarlas para observar y exfiltrar información sensible [88].

A partir de lo señalado, la industria financiera, debido a la naturaleza crítica de sus operaciones y la sensibilidad de los datos que maneja, se beneficia enormemente de la implementación de ZTNA ya que este proporciona un enfoque robusto para proteger estos activos. Varios autores han discutido como ZTA mejora la gestión de la confianza, al evaluar continuamente el comportamiento de los usuarios y al ajustar dinámicamente los controles de acceso [126], [127], [128]

Por otro lado, las instituciones financieras también enfrentan estrictos requisitos regulatorios y de cumplimiento que demandan niveles elevados de seguridad y control de acceso. Por lo tanto, la implementación de ZTNA facilita el cumplimiento de estos requisitos al proporcionar un control de acceso granular sobre quién puede acceder a qué recursos y cuándo. Adicionalmente, al mantener registros detallados de auditoría, ZTNA facilita la gestión del cumplimiento normativo y la responsabilidad. Auditable. Esto asegura que todas las interacciones con los sistemas financieros sean verificadas y autorizadas adecuadamente. Además, la capacidad de ZTNA para proporcionar acceso seguro a usuarios remotos es crucial en un entorno donde el teletrabajo se ha convertido en la norma [129]. Esta capacidad de control y monitoreo continuo es crucial para proteger los datos sensibles y reducir el riesgo de brechas de seguridad.

1.1.6 Marco de seguridad cibernética del NIST

El marco de ciberseguridad NIST es una guía de referencia para mejorar la seguridad de la información en organizaciones de diferentes sectores y tamaños. Este marco se compone de tres componentes principales: el Núcleo, los niveles de implementación y el perfil del marco, donde el núcleo presenta seis funciones clave de ciberseguridad; gobernar, identificar, proteger, detectar, responder y recuperar, junto con categorías y subcategorías específicas que detallan actividades y resultados de seguridad (Figura 16), [130]. Los niveles de implementación proporcionan un contexto sobre cómo una organización considera el riesgo de seguridad cibernética y los procesos establecidos para gestionar dicho riesgo. El perfil del marco representa los resultados que se basan en las necesidades empresariales que una organización ha seleccionado a partir de la identificación de oportunidades de mejora y la postura de seguridad cibernética; todo esto comparado con un perfil objetivo, es decir, su uso variará en función de la organización, misión única y riesgos.

Figura 16. Funciones del Núcleo [130].

En vista de lo anterior, el pilar de red es fundamental para la interacción de los otros pilares, ya que permite la conexión entre usuarios, dispositivos y aplicaciones. Para una infraestructura de red basada en confianza cero, es esencial que las herramientas de seguridad tengan una visibilidad completa y una comprensión del área de ataque y de todo lo conectado a la red. La segmentación

de la red es una solución basada en red que puede encajar en una ZTA, creando microperímetros y aplicando el principio de privilegio mínimo para el acceso a estos segmentos. Esta práctica es esencial para contener cualquier amenaza potencial, minimizando el impacto de un posible ataque cibernético al restringir el movimiento lateral dentro de la red. Además, la implementación de tecnologías de cifrado para la transmisión de datos y la gestión segura de claves criptográficas protege la integridad y confidencialidad de la información financiera [77], [131].

Este enfoque integral en la seguridad de la red es esencial para establecer una estrategia de ciberseguridad robusta y adaptable en las instituciones financieras, protegiendo tanto los datos como las operaciones críticas de la organización.

Tomando en consideración lo discutido, una ZTA establece un marco robusto para la seguridad, basado en la premisa de "nunca confiar, siempre verificar". Este enfoque asegura que todas las solicitudes de acceso sean autenticadas y autorizadas rigurosamente, independientemente de su origen. De este modo, ZTA proporciona un modelo integral para proteger los recursos de una organización contra amenazas tanto internas como externas. Dado este contexto, es esencial profundizar en una de las implementaciones clave de ZTA, el Acceso a Red de Confianza Cero (ZTNA), el cual se detalla continuación.

1.1.7 Proceso Analítico Jerárquico

El Proceso Analítico Jerárquico (AHP), desarrollado por Thomas L. Saaty en la década de 1970, es una metodología de toma de decisiones multicriterio que permite descomponer problemas complejos en una jerarquía de criterios y subcriterios más manejables [132]. A través de comparaciones por pares, el AHP facilita la asignación de pesos a cada criterio, integrando información cuantitativa y cualitativa para obtener una priorización coherente de alternativas [133]. Este enfoque es especialmente útil en contextos donde las decisiones involucran múltiples factores y perspectivas, proporcionando una estructura sistemática para la evaluación y selección de opciones.

La robustez del AHP se basa en su sólida fundamentación matemática, utilizando matrices recíprocas y cálculos de valores propios para garantizar la consistencia lógica en las evaluaciones [134]. Esta metodología ha sido ampliamente aplicada en diversos campos, incluyendo la gestión empresarial, la ingeniería y las ciencias sociales, debido a su capacidad para manejar tanto datos objetivos como subjetivos [135]. Además, el AHP ha evolucionado para incorporar técnicas como el AHP difuso y el AHP en grupo, ampliando su aplicabilidad en entornos con incertidumbre y decisiones colaborativas [136].

En el ámbito de la ciberseguridad, el AHP es una herramienta valiosa para la selección de modelos de ZT que contribuyen a mejorar la seguridad informática. La implementación de un enfoque ZT implica evaluar múltiples criterios, como la protección de datos, la autenticación continua, la

segmentación de redes y la gestión de identidades. El AHP permite descomponer este complejo proceso en una jerarquía estructurada, facilitando la comparación y priorización de diferentes soluciones de ZT según su alineación con los objetivos de seguridad de la organización [133]. Mediante comparaciones por pares, los decisores pueden asignar pesos a cada criterio, reflejando su importancia relativa y obteniendo una selección más informada y objetiva.

La integración del AHP en la selección de modelos ZT no solo mejora la eficacia en la toma de decisiones, sino que también permite una gestión más eficiente de los recursos al identificar las soluciones que ofrecen el mayor valor en términos de seguridad y operatividad [137]. Por ejemplo, al evaluar diferentes plataformas de autenticación multifactor, el AHP ayuda a determinar cuál proporciona el equilibrio óptimo entre seguridad, usabilidad y costo. Esto es crítico en ciberseguridad, donde las amenazas evolucionan constantemente y las decisiones deben ser tanto ágiles como estratégicas.

1.2 Estado del arte

ZT ofrece una variedad de enfoques de implementación que pueden utilizarse de manera combinada o individual. Estos enfoques incluyen la seguridad centrada en la identidad, la segmentación de la red, la seguridad centrada en aplicaciones y datos, perímetros definidos por software y la autenticación basada en riesgos (Tabla 6). Cada uno de estos enfoques contribuye a un marco integral de seguridad que aborda diversas dimensiones de las amenazas cibernéticas. Por ejemplo, la segmentación de la red limita el movimiento lateral y contiene posibles amenazas, mientras que la autenticación multifactorial y la encriptación de datos aseguran que solo entidades autorizadas puedan acceder a recursos críticos [128].

Tabla 6. Enfoques y Soluciones de Implementación de Zero Trust

Enfoque de Implementación	Descripción
Seguridad centrada en la identidad	Verifica y permite el acceso a identidades sin importar su ubicación en la red.
Segmentación de red	Divide la red en segmentos aislados para restringir el movimiento lateral y contener amenazas potenciales.
Seguridad centrada en aplicaciones y datos	Prioriza la protección de datos sensibles mediante encriptación y controles de acceso estrictos.
Perímetro definido por software	Establece perímetros de red adaptativos y seguros, ajustados a cada usuario o dispositivo.
Autenticación basada en riesgos	Evalúa los intentos de acceso considerando los riesgos asociados, proporcionando una autenticación más fuerte para actividades de alto riesgo o comportamientos anómalos.

Dada la información previa, a continuación, se destacan diferentes estudios reportados en la literatura que han abordado ZT como enfoque para mejorar la seguridad de los datos, recursos críticos, reducir los costos asociados con brechas de seguridad y mejorar la eficiencia en la gestión de accesos.

1.2.1 Implementación de ZT: enfoques y soluciones de implementación

Un estudio realizado en 2024 por [62] en Bradford, Reino Unido; presenta una metodología detallada de ZT mejorada con tecnología *blockchain* en la industria financiera. La implementación del marco se centró en tres áreas clave: la IAM, la seguridad de dispositivos y redes, y la protección de datos. Para ello, se utilizaron estándares avanzados de cifrado, sistemas de detección de intrusiones y monitoreo continuo de la red para proteger contra brechas externas e internas. Además, se implementó cifrado de extremo a extremo para proteger los datos sensibles y se llevaron a cabo auditorías de seguridad regulares. Los resultados se obtuvieron a través de pruebas exhaustivas y simulaciones que evaluaron la capacidad del marco propuesto para manejar diversas amenazas cibernéticas y su rendimiento operacional [62].

Uno de los hallazgos más destacados del marco propuesto por este estudio, fue la capacidad de mitigar eficazmente una variedad de ataques cibernéticos comunes en el sector financiero. Durante las pruebas de seguridad, el prototipo de la aplicación bancaria mostró una defensa robusta contra ataques sofisticados como inyecciones SQL, ataques de fuerza bruta, *cross-site request forgery* (CSRF), *cross-site scripting* (XSS) y ataques *man-in-the-middle*. Utilizando herramientas como Burp Suite, OWASP ZAP y Wireshark, se realizaron escaneos de vulnerabilidades y pruebas de seguridad que no detectaron vulnerabilidades significativas, lo que sugiere que los mecanismos de validación de entradas, gestión de sesiones y configuraciones de seguridad son efectivamente robustos [62].

Por otro lado, la integración de *blockchain* en la IAM proporcionó una capa adicional de seguridad ya que mejoró la autenticación y autorización de usuarios mediante contratos inteligentes en la *blockchain* de Ethereum, asegurando procesos descentralizados e inmutables. La naturaleza inmutable de *blockchain* complementó el requisito de verificación continua del modelo ZT, asegurando que los procesos de verificación fueran no solo rigurosos sino también transparentes y a prueba de manipulaciones. Esta integración resultó crucial para reforzar el componente IAM, ya que se sometió y resistió a varios ataques simulados durante el proceso de evaluación [62].

Estos hallazgos, validan la eficacia del modelo ZT mejorado con blockchain para proteger los datos críticos contra amenazas externas e internas, manteniendo la integridad y disponibilidad de los datos financieros esenciales. La capacidad del marco para proporcionar un entorno transaccional seguro y eficiente, junto con su alineación con los estándares de cumplimiento y regulaciones, lo posiciona como una solución viable y robusta para la ciberseguridad en la industria financiera.

Otra de las soluciones novedosas donde se han intentado disminuir los riesgos cibernéticos se refleja en la propuesta de intercambio de información en entornos de Internet de las Cosas (IoT) de ZT la cual fue desarrollado entre universidades de Pakistán y el Reino Unido. El estudio reciente describió una metodología integral para abordar las ciberamenazas y vulnerabilidades en entornos inteligentes mediante el uso de un modelo de control de acceso de ZT inspirado en *blockchain* (ZAIB) [79]. La metodología se centró en el diseño e implementación de un marco seguro que monitorea y facilita las comunicaciones dispositivo a dispositivo con diferentes niveles de mecanismos de control de acceso basados en parámetros ambientales y comportamiento de los dispositivos. Este modelo utiliza una ZTA y proporciona un análisis dinámico del comportamiento de los dispositivos IoT al calcular los niveles de confianza de cada solicitud. ZAIB aplica políticas variables generadas específicamente para cada escenario utilizando control de acceso basado en atributos (ABAC) [79].

Los resultados principales del estudio destacan varias ventajas del modelo ZAIB en la mejora de la seguridad en redes IoT. Primero, el modelo mostró ser eficaz en la protección de la infraestructura inteligente contra una amplia gama de ciberamenazas, incluyendo ataques que podrían comprometer servicios críticos y poner en riesgo vidas humanas. La evaluación de seguridad demostró que ZAIB satisface las necesidades de defensa activa y la aplicación de seguridad de extremo a extremo para los datos, usuarios y servicios involucrados en una red de *smart grid.* Además, la implementación de *blockchain* en ZAIB garantiza que los registros de actividad sean inmutables y que las registraciones de dispositivos y usuarios sean anónimas, lo cual es crucial para

mantener la privacidad y la integridad de los datos en entornos IoT. Los atributos y los historiales de niveles de confianza se gestionan de manera segura, lo que permite una política de acceso dinámico y adaptable a las condiciones cambiantes del entorno [79].

Así mismo, los autores de otro estudio, proponen un sistema de aprendizaje federado habilitado para seguridad ZT basada en *blockchain* llamado Skunk el cual fue desarrollado principalmente en Estados unidos y Singapur para abordar los requisitos de privacidad y procedencia de datos en las redes móviles 5G / 6G el cual utiliza una arquitectura basada en fragmentación en *blockchain* para permitir la implementación en entornos de fragmentación de red; en adición, utiliza mecanismos de seguridad de confianza cero para garantizar la seguridad y transparencia en el proceso de aprendizaje federado; de hecho, como caso de uso se ha considerado un escenario donde se detectan ataques en el IoT u otros dispositivos en una red 5G / 6G [138]. De acuerdo con lo discutido en el estudio, la metodología propuesta aborda soluciones a partir de *blockchain* el cual no es el común denominador de las empresas del sector financiero colombiano.

Aunque los resultados del uso de *blockchain* en la ciberseguridad y la gestión de accesos son prometedores, el sector financiero en Colombia y otros gremios relacionados aún no han desarrollado una infraestructura de cadena de bloques específica para sus operaciones financieras. Esta falta de implementación limita la aplicación práctica y el impacto potencial de la metodología y el alcance propuestos en este trabajo. Por lo tanto, aunque las investigaciones y desarrollos tecnológicos en torno a *blockchain* muestran un gran potencial para mejorar la seguridad y eficiencia en diversos sectores, su adopción en el ámbito financiero colombiano sigue siendo incipiente. Esto subraya la necesidad de continuar investigando y promoviendo la integración de *blockchain* en las prácticas financieras locales para alcanzar los beneficios demostrados en estudios como este.

El estudio realizado por [129] en Estados unidos, explora la relevancia de la Arquitectura de Red Zero Trust (ZTNA) en el contexto del trabajo remoto impuesto por la pandemia de COVID-19. El objetivo principal del estudio fue analizar cómo ZTNA puede mejorar la seguridad de los datos mediante la implementación de procesos de autenticación multifactor que requieren la verificación de la identidad de los usuarios o dispositivos antes de acceder a la red. Este enfoque es crucial para eliminar las debilidades del concepto tradicional de "castillo y foso", que permitía a los usuarios navegar libremente una vez que penetraban el contrafuego.

La metodología utilizada en este estudio incluyó una evaluación comparativa de las vulnerabilidades de las arquitecturas de seguridad tradicionales frente a los beneficios del enfoque ZT. En el estudio se analizaron varios casos de estudio de organizaciones que adoptaron ZTNA para proteger sus redes durante el período de trabajo remoto masivo. Los resultados mostraron que ZTNA no permite la penetración y segmentación de diferentes materiales, impidiendo que un individuo acceda a todos los recursos una vez dentro de la red [129].

Los hallazgos del estudio revelaron que la ZTA proporciona una experiencia de usuario simplificada y permite una gestión más eficiente de los contenidos y recursos de la red. Además, Deshpande argumenta que la adopción de ZTNA no solo es beneficiosa durante la pandemia, sino que también

ofrece ventajas a largo plazo. La ZTA es adaptable y puede integrarse fácilmente en las infraestructuras existentes, proporcionando una protección continua contra amenazas tanto internas como externas [129].

Un estudio publicado en 2022 por [123], [139] presenta una revisión comparativa de los modelos y marcos de ZTNA aplicados a la computación en la nube. El estudio se desarrolló en colaboración entre India, Dinamarca y Corea del Sur; el objetivo principal fue comparar las características específicas de los modelos de red en la nube basados ZT y sus implementaciones. Se hizo hincapié en cómo estos enfoques pueden mejorar la seguridad de las redes en la nube, que son cada vez más prevalentes en las instituciones financieras debido a su rentabilidad y accesibilidad.

La metodología empleada en este estudio incluyó la categorización de las características de ZTNA en tres tipos principales: modelos de red en la nube basados en ZT, marcos y pruebas de concepto. Los autores analizaron diversos estudios y casos de uso para identificar las mejores prácticas y los desafíos asociados con la implementación de ZTNA en estos entornos. Se destacaron los beneficios de ZTNA en términos de mejorar la visibilidad de la red, la automatización de la seguridad y la capacidad de prever y mitigar amenazas basadas en el comportamiento de los usuarios

Los hallazgos del estudio indican que ZTNA permite a los administradores de red abordar problemas críticos como la inhibición de amenazas cibernéticas internas y externas, la mejora de la visibilidad de la red y la automatización del cálculo de la confianza para las entidades de la red. Esto es particularmente relevante para las instituciones financieras, que deben gestionar grandes volúmenes de datos sensibles y asegurar transacciones financieras de manera efectiva. De este modo, la implementación de ZTNA puede proporcionar una capa adicional de seguridad, protegiendo datos críticos y garantizando el cumplimiento de normativas locales e internacionales [123], [139].

El estudio también abordó los desafíos específicos de la computación en la nube que pueden afectar la implementación de ZTNA. Entre estos se incluyen la gestión de la seguridad en plataformas de nube híbrida y la integración de nuevas tecnologías en la ZTNA. Los autores sugieren que las futuras investigaciones deben centrarse en desarrollar marcos más robustos y adaptativos que puedan integrarse fácilmente en las infraestructuras de nube existentes, proporcionando una protección continua y eficiente contra amenazas cibernéticas [123], [139].

Considerando lo anterior, La capacidad de ZTNA para prever y mitigar amenazas, junto con su adaptabilidad a diferentes entornos de nube, la convierte en una opción estratégica para las instituciones financieras colombianas que buscan mejorar su postura de seguridad y cumplir con las regulaciones de la industria.

El estudio realizado por [140] en Maryland, Estados unidos; analiza el uso de la ZTA para la seguridad de aplicaciones y redes en un entorno globalizado y migrado a la nube. El objetivo principal de este estudio fue revisar la aplicación de principios de ZT en la seguridad de redes en lugar de confiar en un perímetro tradicional. La metodología utilizada incluyó una investigación cualitativa sobre la inseguridad de las API en entornos ZT, destacando la importancia de no confiar

en recursos internos o externos sin una verificación adecuada. Para llevar a cabo la metodología, la investigación combinó estudios de caso y análisis cualitativos para evaluar la efectividad de ZTNA en la protección de redes y aplicaciones.

Los resultados del estudio indicaron que la adopción de ZTNA puede reducir significativamente las vulnerabilidades asociadas con las API inseguras, que a menudo son el eslabón más débil en la cadena de seguridad. Esta capacidad de ZTNA para proteger contra ataques cibernéticos maliciosos es particularmente relevante para las instituciones financieras que manejan datos sensibles y requieren una protección robusta contra accesos no autorizados [140].

El estudio también exploró diferentes soluciones de software para implementar el acceso seguro a aplicaciones y servicios para usuarios remotos utilizando ZTNA. Los hallazgos sugieren que la adopción de estas soluciones puede mejorar la seguridad y la eficiencia operativa permitiendo un acceso seguro y controlado a recursos críticos. En el contexto colombiano, donde la protección de datos es una prioridad, estas soluciones pueden proporcionar una capa adicional de seguridad para proteger la información confidencial de los clientes [140].

Además, los autores del estudio destacaron que la ZTA puede ser una herramienta eficaz para proteger las organizaciones contra ataques cibernéticos internos y externos. La capacidad de ZTNA para segmentar la red y limitar el acceso a recursos específicos garantiza que incluso si un atacante penetra una parte de la red, no podrá acceder a todos los recursos. Esta característica es especialmente valiosa para las instituciones financieras, que necesitan proteger datos altamente sensibles y cumplir con estrictas regulaciones de seguridad [140].

El estudio [103] desarrollado en Australia, ofrece una encuesta detallada del paradigma de seguridad ZT, que cuenta con un número creciente de defensores en el ámbito de la gestión de riesgos de infraestructuras críticas. El objetivo del estudio fue describir los principios fundamentales de ZT y revisar las numerosas opciones disponibles para la implementación exitosa de este paradigma. Los autores emplearon un enfoque descriptivo para presentar un análisis exhaustivo de las técnicas de autenticación y control de acceso en diferentes escenarios.

La metodología utilizada incluyó una revisión sistemática de la literatura y un análisis comparativo de las técnicas de seguridad convencionales, como la encriptación, la microsegmentación y la automatización de la seguridad. Los hallazgos indicaron que la ZTA puede mejorar significativamente la seguridad de las infraestructuras críticas al eliminar la confianza implícita en las entidades de la red. Esto es especialmente relevante para las instituciones financieras, que deben proteger datos sensibles y garantizar la continuidad del negocio en un entorno de amenazas cibernéticas en constante evolución [103].

Los autores también discutieron los desafíos asociados con los mecanismos de autenticación contemporáneos, los esquemas de control de acceso y las técnicas de computación de confianza y riesgo. Adicionalmente, se identificaron áreas clave para futuras investigaciones, como el desarrollo de enfoques más sofisticados para la orquestación de seguridad y la respuesta

automatizada a incidentes. Estos avances son cruciales para la implementación efectiva de ZT en infraestructuras críticas, incluidas las instituciones financieras [103].

El estudio también destacó la importancia de la microsegmentación y la automatización de la seguridad en la ZTA. La capacidad de segmentar la red en pequeñas partes y aplicar controles de seguridad específicos a cada segmento puede mejorar la protección contra ataques cibernéticos y reducir la superficie de ataque [103].

Un estudio realizado por [86] en Estados unidos, evaluó la implementación y efectividad de la ZTA basada en la identidad para mejorar la ciberseguridad en entornos de trabajo remoto y distribuidos. El estudio se centró en cómo la autenticación sin contraseñas mediante la plataforma FIDO2 puede aumentar la robustez de la ciberseguridad, eliminando las contraseñas estáticas y mejorando la autenticación de usuarios. Además, el estudio buscó identificar y analizar los desafíos operativos y las estrategias de implementación de ZTA, así como evaluar su impacto en la postura de seguridad de las organizaciones.

La metodología de este estudio se centró en un análisis de caso y una revisión exhaustiva de la literatura sobre la implementación de ZTA basada en la identidad. El autor, evaluó específicamente cómo la autenticación sin contraseñas mediante la plataforma FIDO2 puede mejorar la ciberseguridad en un entorno de trabajo remoto. Además, se emplearon estudios de caso seleccionados para proporcionar un análisis detallado de las estrategias de implementación de ZTA, los desafíos operativos y el impacto en la postura de seguridad [86].

Los hallazgos principales del estudio destacan que ZTA ofrece una solución robusta para la ciberseguridad al eliminar las contraseñas estáticas, lo que fortalece la autenticación de usuarios y aborda los desafíos modernos de seguridad cibernética. Asimismo, los estudios de caso revelaron que la implementación de ZTA y la autenticación FIDO2 mejoran significativamente la postura de seguridad al minimizar las vulnerabilidades asociadas con los ataques basados en contraseñas. También se identificó la importancia de la educación y concienciación del usuario para facilitar la transición hacia la autenticación sin contraseñas [86].

Sin embargo, el análisis de los estudios de caso mostró que la adopción de ZTA enfrenta varios desafíos operativos, como la compatibilidad de dispositivos, la integración del sistema y la educación del usuario. Estos obstáculos deben ser superados para garantizar una implementación exitosa de ZTA. Además, el estudio sugiere que las características de usabilidad de FIDO2, como la configuración manual y las actitudes de los usuarios hacia la autenticación sin contraseñas, son cruciales para su adopción generalizada [86].

Finalmente, el estudio concluyó que la integración de ZTA con tecnologías de autenticación sin contraseñas representa un cambio significativo hacia una postura de ciberseguridad más segura y robusta. Adicionalmente, artículo hizo recomendaciones para las organizaciones, como la necesidad de campañas de educación y concienciación del usuario, interfaces amigables y una planificación cuidadosa para la integración del sistema. El estudio también sugirió direcciones

futuras de investigación, como la mejora de las técnicas de autenticación y la exploración de enfoques sensibles a la privacidad para compartir contextos [86].

1.2.2 Otros enfoques y soluciones de implementación de ZT

BeyondCorp, una iniciativa de Google transforma el modelo de ZT al priorizar la seguridad centrada en usuarios y dispositivos en lugar de depender de los límites tradicionales de la red, eliminando la necesidad de VPNs. Este modelo incorpora componentes esenciales como Single Sign-On (SSO), proxies de acceso, motores de control, listas de usuarios y dispositivos, reglas de seguridad y una base de datos confiable. Este enfoque sigue las directrices del NIST para despliegues basados en agentes y gateways de dispositivos, creando un entorno robusto para proteger aplicaciones y servicios modernos [109].

No obstante, la transición a BeyondCorp puede enfrentar desafíos relacionados con la experiencia del usuario y la adaptación a nuevas políticas de seguridad. La evolución hacia BeyondProd, un servicio de seguridad nativo en la nube, ilustra la capacidad del modelo para adaptarse continuamente a las necesidades cambiantes de las organizaciones, proporcionando una solución de seguridad más flexible y eficiente en entornos de nube [94].

En el contexto colombiano, la implementación de BeyondCorp enfrenta varios desafíos. La infraestructura tecnológica y la disposición de las organizaciones para adoptar nuevas tecnologías son cruciales. Aunque el modelo es prometedor, su implementación requeriría inversiones significativas en capacitación y adaptación de infraestructura, lo cual podría ser un obstáculo para muchas empresas locales que operan con recursos limitados.

El modelo Forrester NGFW/ZTX, propuesto por Kindervag en 2010, segrega la red corporativa en segmentos de micro-core y perímetro (MCAP). Este enfoque es adecuado para organizaciones con numerosos dispositivos IoT y se alinea con el modelo de despliegue basado en portales de recursos de NIST. El marco Zero Trust eXtended (ZTX) de Forrester incluye siete dimensiones: redes, datos, personas, cargas de trabajo, dispositivos, visibilidad y análisis, automatización y orquestación. Esto permite entender cómo diferentes tecnologías contribuyen a la seguridad de la red. Sin embargo, el modelo tiene limitaciones en la autenticación de usuarios, lo que resalta la necesidad de tecnologías adicionales como IAM y VPNs [141].

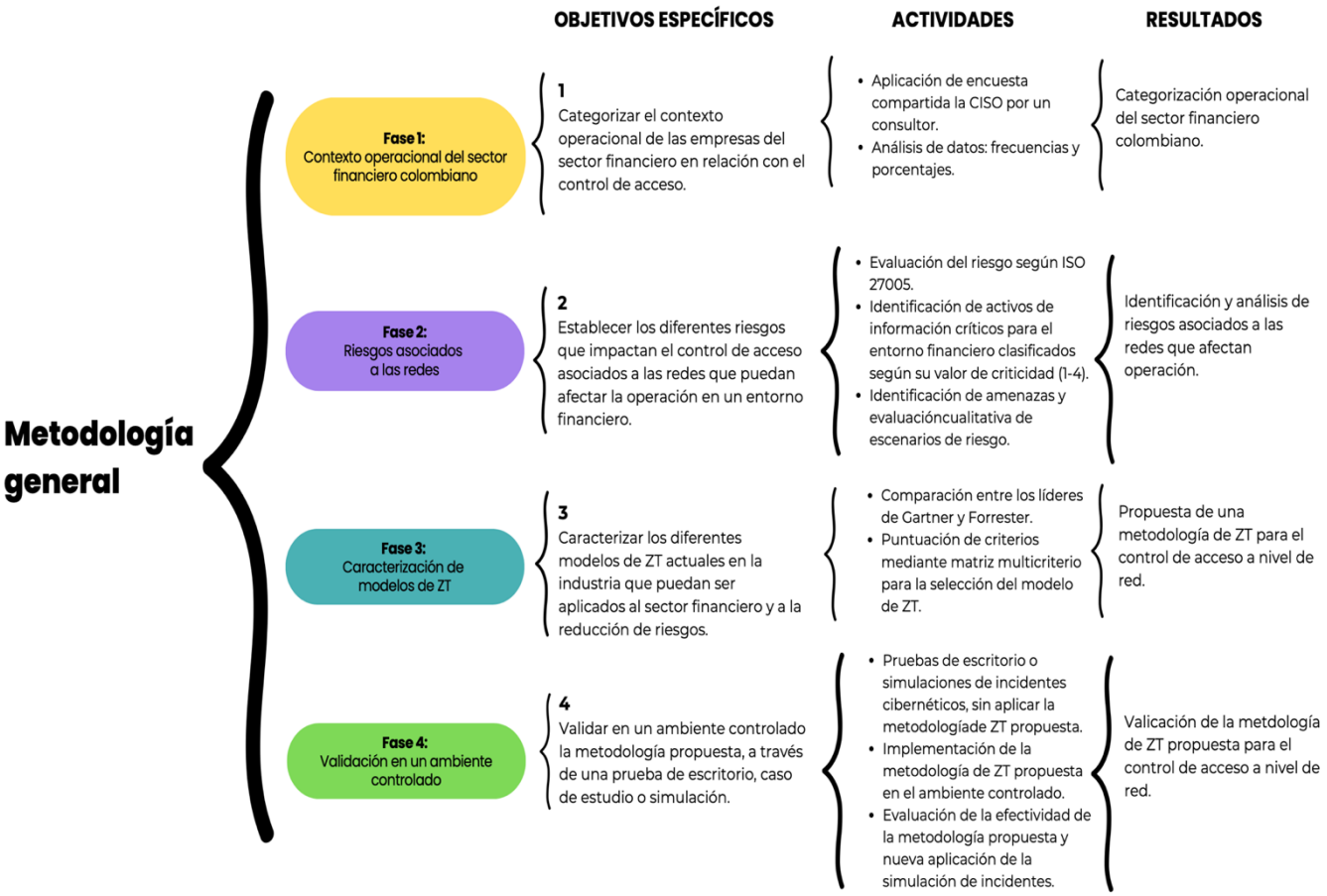
En Colombia, la adopción del modelo Forrester NGFW/ZTX también enfrenta desafíos. La integración de múltiples tecnologías y la capacitación del personal son esenciales para una implementación exitosa. Además, las inversiones necesarias pueden ser restrictivas en el contexto económico actual del país.

2. Metodología y Resultados

La estrategia aplicada para la construcción de una metodología basada en el modelo ZT para el control de acceso a nivel de red en el sector financiero colombiano es de tipo cualitativa. Este enfoque no solo permite una comprensión profunda de los fenómenos en cuestión desde una perspectiva del contexto operacional, sino que también facilita la identificación de desafíos específicos y la adaptación de soluciones a las necesidades reales del sector. Además, proporciona una metodología de ZTNA para explorar su implementación práctica y las implicaciones del modelo de ZTNA, garantizando que las soluciones propuestas sean efectivas y sostenibles.

En este capítulo se establece la metodología de cómo se lograron las fases respectivas y se entregan dentro del mismo, los resultados respectivos. La Figura 17, describe la metodología propuesta para el alcance de los objetivos propuestos en esta investigación. La metodología está basada en 4 fases para el diseño de una metodología de ZTNA con enfoque en la red, identidad y dispositivos

Figura 17. Descripción Metodológica de la Investigación



2.1 Metodología y resultados FASE 1

2.1.1 Metodología FASE 1: Contexto operacional del sector financiero colombiano

Para alcanzar el objetivo específico 1 *"categorizar el contexto operacional de las empresas del sector financiero en relación con el control de acceso"*, se diseñó una encuesta (Anexo A) con el fin de recolectar información detallada sobre la categorización del contexto operacional de las entidades del sector financiero de Colombia, específicamente relacionada con el control de acceso, la identificación de riesgos asociados a las redes y los activos de información relacionados a la línea de negocio.

La encuesta fue creada en Google Forms por su accesibilidad e incluyó un cuestionario con preguntas de selección múltiple tanto de respuesta única como múltiple para obtener datos precisos y variados. Como se detalla a continuación, el cuestionario se estructuró en cuatro componentes:

1. **Contexto operacional general de las empresas financieras:** para esta parte se formularon preguntas para identificar las infraestructuras de red, los controles de seguridad existentes, los flujos de datos y los sistemas o prácticas de gestión de acceso utilizados en estas empresas.
2. **Control de acceso e identificación de riesgos:** Se diseñaron preguntas enfocadas en el control de acceso e identificación de posibles vectores de ataque con el fin de determinar los procesos operativos que requieren un control de acceso seguro y confiable.
3. **Gestión de identidad:** Se elaboraron preguntas con el fin de comprender cómo se maneja la identidad y el acceso a los sistemas y datos en las empresas financieras de Colombia. Estas preguntas fueron diseñadas para evaluar si la organización dispone de sistemas o herramientas específicas de gestión de identidades, qué métodos de autenticación se emplean, cómo se administra el ciclo de vida de las identidades de empleados y usuarios, si se aplican políticas de acceso basadas en roles, cómo se manejan los privilegios de acceso de usuarios temporales o externos, y cuáles son los principales desafíos o riesgos relacionados con la gestión de identidades en las empresas.
4. **Impacto y gestión de riesgos:** en este aparte se hicieron preguntas enfocadas en la transformación digital que ha influido en las prácticas de control de acceso dentro de las empresas financieras de Colombia. Adicionalmente, las preguntas se formularon para determinar si la empresa tiene establecido un plan específico para gestionar incidentes de seguridad cibernética, particularmente aquellos relacionados con el control de acceso a la red.

La encuesta estuvo dirigida al responsable de la ciberseguridad de la organización financiera (CISO). Para ello, la encuesta fue compartida electrónicamente a un consultor de dichas organizaciones y para garantizar la veracidad de las respuestas, este mismo se encargó de su distribución entre los responsables de ciberseguridad de cada organización (véase anexo J); este enfoque asegura que las respuestas recopiladas provienen de los roles adecuados, ya que el consultor, familiarizado con la estructura interna de las entidades, seleccionó cuidadosamente a los participantes conforme a su rol y responsabilidad. La recolección de datos se llevó a cabo entre el 15 de mayo de 2024 y el 5 de junio de 2024.

Los datos recopilados fueron exportados a Microsoft Excel 365 para analizar frecuencias y proporciones de las respuestas de los encuestados. Los resultados se presentaron en gráficos y tablas para identificar tendencias y patrones. Además, para garantizar la confidencialidad y anonimato de los participantes, todos los datos se manejaron conforme a las normativas éticas establecidas por el Instituto Tecnológico Metropolitano (ITM).

2.1.2 Resultados FASE 1: Contexto operacional del sector financiero colombiano

La encuesta fue enviada a 23 empresas del sector financiero colombiano, de las cuales participaron 10 (43.5%). La Tabla 7, describe los hallazgos del contexto operacional relacionado con el control de acceso de las organizaciones del sector financiero colombiano.

Tabla 7. Descripción del Contexto Operacional Relacionado con el Control de Acceso de las Empresas Financieras de Colombia

Contexto Operacional Relacionado del Sector Financiero Colombiano

Tamaño de la empresa n (%)				
Grande	Mediana			
7 (70%)	3 (30%)			
Tipo de servicios financieros n (%)				
Banca comercial	Banca de inversión	Seguros	Otros	
8 (80%)	5 (50%)	4 (40%)	1 (10%)	
Tipo de medios de pago disponibles para clientes n (%)				
Tarjetas débito/crédito	Transferencias bancarias	Transacciones electrónicas	Pagos por medio de plataformas web	Pagos móviles tipo QR o NFC

9 (90%)	8 (80%)	7 (70%)	7 (70%)	6 (60%)
Implementación de controles de acceso para proteger redes y sistemas n (%)				
Autenticación multifactor	Monitoreo continuo de la actividad del usuario	Control de acceso basado en roles	CIAM e IAM	
10 (100%)	8 (80%)	6 (60%)	1 (10%)	
Uso de Sistemas de Gestión de Identidades (IAM) para administrar y controlar el acceso de usuarios a sistemas y datos n (%)				
Contraseña única con ID multifactor	Token físico	Contraseña única	En proceso de implementación	
7 (70%)	4 (40%)	3 (30%)	1 (10%)	
Gestión del Ciclo de Vida de Identidades de Usuario n (%)				
Procesos automatizados y centralizados		Procesos manuales y descentralizados		
6 (60%)		4 (40%)		
Manejo de los privilegios de acceso de los usuarios temporales o externos n (%)				
Procesos de aprobación y temporización automática		Asignación manual de privilegios		
5 (50%)		5 (50%)		

Como se describe en la Tabla 7, el análisis del contexto operacional de las empresas financieras en Colombia que respondieron la encuesta muestra que el 70% de estas son grandes y el 30% restantes son medianas. Este predominio de grandes empresas se justifica por las ventajas competitivas que poseen en términos de escala, diversificación de servicios y capacidad para cumplir con requisitos regulatorios más estrictos, lo cual es consistente con lo reportado en el reporte de infraestructura financiera del banco de la República de Colombia [142]; en cuanto a los servicios financieros, la banca comercial representó el 80% de los servicios ofrecidos, seguida por la banca de inversión (50%) y los seguros (40%).

Durante el análisis, se observó una adopción generalizada de métodos de pago digitales, incluyendo tarjetas de débito/crédito (90%), transferencias bancarias (80%), transacciones electrónicas (70%), pagos móviles (60%) y plataformas web (70%), lo que pone de relieve una tendencia hacia la digitalización de los servicios financieros en Colombia. Este fenómeno se alinea con los datos del reporte de infraestructura financiera, que menciona un aumento significativo en el uso de instrumentos de pago electrónicos, aunque reconoce que el país aún enfrenta desafíos para alcanzar niveles de adopción comparables con otras economías más avanzadas [142].

Por otro lado, este análisis reveló un enfoque significativo en la implementación de medidas de seguridad, reflejando una creciente preocupación por proteger la infraestructura crítica ante amenazas cibernéticas. Como se detalla en la Tabla 7, todas las empresas han adoptado medidas

básicas de seguridad, como la MFA y el monitoreo continuo de la actividad del usuario (80%). Sin embargo, solo el 60% utiliza controles de acceso basados en roles, y un escaso 10% ha adoptado sistemas avanzados de gestión de identidades como CIAM (Customer Identity and Access Management) o IAM. Esta tendencia sugiere que, si bien las empresas están tomando pasos importantes hacia la protección de sus activos digitales, todavía existen áreas de mejora en la adopción de tecnologías avanzadas de seguridad.

Estos hallazgos son consistentes con lo reportado en el informe del Banco de la República de Colombia, que subraya la necesidad de fortalecer la ciberresiliencia en el sistema financiero del país. El informe destaca que, aunque ha habido avances en la adopción de prácticas básicas de ciberseguridad, como las transferencias electrónicas y el uso de billeteras móviles, el sector financiero colombiano aún enfrenta retos significativos en términos de ciberseguridad avanzada y gestión de riesgos, especialmente ante el aumento de la digitalización de los servicios financieros y la creciente amenaza de ataques cibernéticos sofisticados [142].

En cuanto al uso de sistemas de IAM, se observó que la mayoría de las empresas utilizan contraseñas únicas con MFA (70%), mientras que solo un 10% está en proceso de implementación de nuevas medidas. Esto sugiere una lenta adopción de tecnologías avanzadas. Este enfoque integrado de IAM, que también incluye la implementación de tokens físicos, los cuales son utilizados por el 40% de las empresas financieras encuestadas, se enmarca en un esfuerzo más amplio por construir sistemas de autenticación inteligentes y resilientes que puedan adaptarse a las necesidades cambiantes de seguridad en entornos digitales complejos. Esto está en línea con la literatura, ya que se ha reportado que las organizaciones están reconociendo la importancia de diversificar y fortalecer sus métodos de autenticación para asegurar la integridad y confidencialidad de la información, especialmente en sectores críticos como el financiero [62], [144], [145].

Finalmente, se identificó una limitada adopción de sistemas avanzados de gestión de identidades, como CIAM e IAM, junto con una dependencia de procesos manuales y descentralizados para la administración del ciclo de vida de las identidades de usuario en el 40% de las empresas, lo que destaca una oportunidad para optimizar la eficiencia y fortalecer la seguridad en la gestión de accesos. Este resultado concuerda con los hallazgos reportados por [146], los cuales destacan la limitada divulgación de información sobre ciberseguridad en América Latina y la necesidad de aumentar la transparencia y mejorar las prácticas de gestión de ciberseguridad para fortalecer la resiliencia del sector financiero.

En síntesis, el análisis del contexto operacional de las empresas financieras en Colombia muestra una concentración significativa de grandes instituciones en el mercado, impulsada por ventajas competitivas y una fuerte orientación hacia la digitalización de los servicios financieros. Aunque se han implementado medidas básicas de ciberseguridad, como la MFA, aún existen oportunidades para mejorar mediante la adopción de tecnologías avanzadas de gestión de identidades y un enfoque más robusto en la ciberresiliencia.

Para una información más detallada, referirse al Anexo B.

2.2 Metodología y resultados FASE 2

2.2.1 Metodología FASE 2: Riesgos asociados a las redes

Para la consecución del segundo objetivo específico *"Establecer los diferentes riesgos que impactan el control de acceso asociados a las redes que puedan afectar la operación en un entorno financiero"* se ha seleccionado la ISO 27005 como marco para la evaluación del riesgo de seguridad de la información.

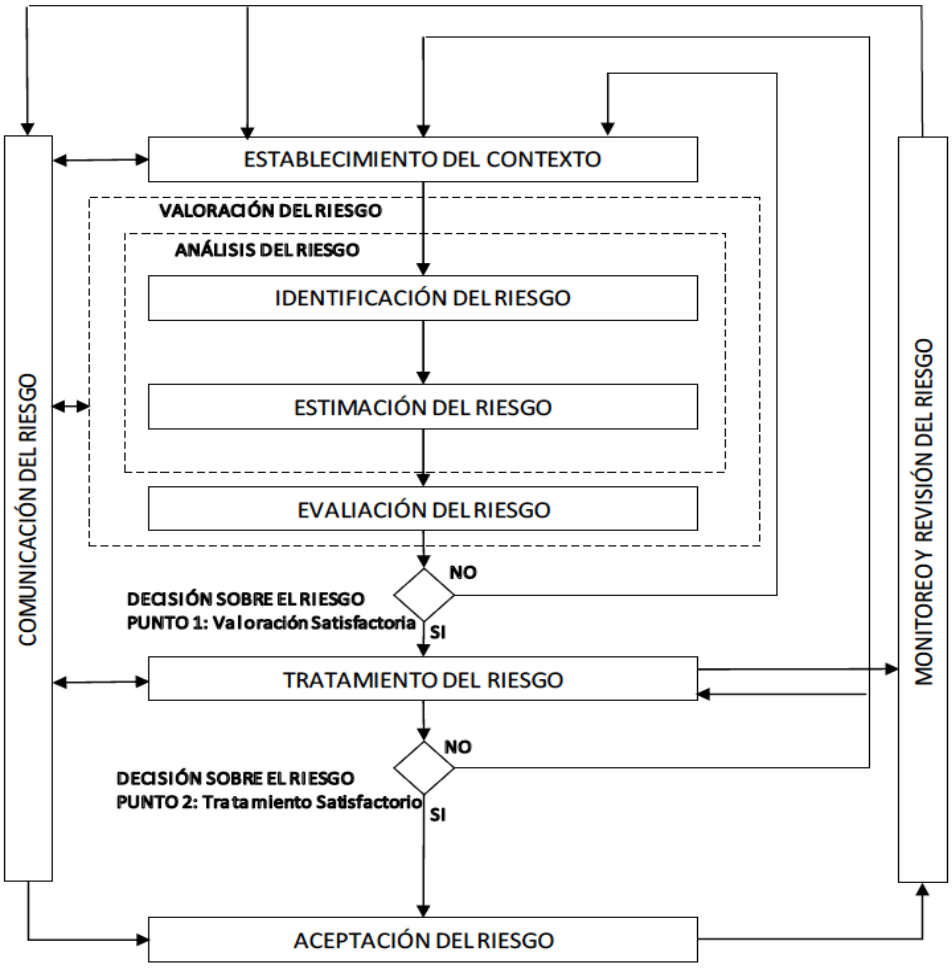
El uso de esta norma en la presente investigación proporciona un marco sistemático que permite a las instituciones financieras identificar, evaluar, priorizar y tratar riesgos de seguridad, complementando la ISO 27001 dentro de un SGSI; además, la Guía No. 7 de Gestión de Riesgos del MINTIC alineada con estas normas, refuerza esta necesidad al ofrecer un enfoque integral para la gestión de riesgos, aplicable tanto a entidades públicas como al sector financiero, garantizando una protección integral de los activos de información [52].

Por otro lado, la Superintendencia Financiera de Colombia (SFC) ha establecido directrices y normativas que, aunque no mencionan específicamente la ISO 27005, promueven prácticas alineadas con los principios de la familia ISO 27000, especialmente en temas de seguridad de la información y ciberseguridad. Estas normativas, como la Circular Externa 022 de 2010, buscan garantizar la confidencialidad, integridad y disponibilidad de la información de los clientes, mediante la implementación de controles robustos y mecanismos de cifrado, lo cual está en línea con los objetivos de las normas internacionales de seguridad de la información [147].

La ISO 27005 brinda un proceso estructurado que considera el análisis del contexto, la identificación de activos, la identificación y valoración de amenazas, la evaluación de escenarios de riesgo y el tratamiento del riesgo [53], (Figura 18). Es importante resaltar que el tratamiento del riesgo no estuvo dentro del alcance esta investigación.

Dado lo anterior, esta metodología, alineada con la norma ISO 27005 [53], ayuda a las organizaciones financieras a proteger sus activos críticos, especialmente aquellos relacionados con el control de acceso a las redes, y a mantener la confidencialidad, integridad y disponibilidad de su información. La Figura 18, ilustra el proceso para la gestión del riesgo en seguridad de la información. De las etapas allí descritas el tratamiento de riesgos, el monitoreo y revisión, y la comunicación del riesgo no se incluyeron en el presente trabajo.

Figura 18. Proceso para la Gestión del Riesgo en Seguridad de la Información [53]**.**



A continuación, se detallan las actividades implementadas para la evaluación del riesgo que impactan el control de acceso asociados a las redes:

La primera actividad consistió en definir el contexto y el alcance de la evaluación de riesgos mediante la identificación de los objetivos, las políticas de seguridad vigentes, las normativas aplicables y las expectativas de las partes interesadas. También se establecieron criterios claros para la evaluación, aceptación y niveles de riesgo tolerables en las organizaciones financieras. Para la definición del contexto, se usó la información obtenida de la encuesta desarrollada en la fase 1, que permitió comprender mejor los riesgos vinculados al control de acceso en las empresas financieras de Colombia.

Este proceso fue esencial para entender el entorno financiero en el que operan estas organizaciones, considerando factores internos y externos que pueden influir en la operación, lo cual es fundamental para establecer criterios de evaluación de riesgos adaptados al enfoque de ZT. Una vez definido el contexto, se identificaron los activos de información críticos para el entorno financiero, incluyendo activos tangibles, como servidores y dispositivos de red, e intangibles, como la información financiera y los procesos de negocio. Cada activo fue catalogado y clasificado según su valor y la criticidad para la organización, utilizando una escala de 1 a 4 (Anexo C). Este proceso permitió priorizar aquellos activos que son esenciales para el control de acceso a las redes.

En este sentido, identificar y clasificar los activos de información son cruciales para establecer un enfoque diferenciado en su protección, destinando mayores recursos y medidas de seguridad a aquellos que, por su relevancia o sensibilidad, requieren una protección más robusta. Este enfoque proporciona un inventario detallado que facilita la implementación de estrategias específicas de seguridad para los activos más valiosos y vulnerables, guiando a las organizaciones del sector financiero a tener foco en la contención.

Posteriormente, a partir de la encuesta realizada en la fase 1 (Anexo B) se identificaron diversas amenazas, abarcando posibles ataques cibernéticos como malware, movimiento lateral, suplantación de identidad, acceso no autorizado y ransomware. Estas amenazas surgen por vulnerabilidades en el acceso remoto y los sistemas internos, facilitando la infiltración y el movimiento dentro de la red. Esta evaluación permitió priorizar las amenazas que impactan el control de acceso, destacando la importancia de proponer una metodología basada en ZT para proteger los recursos y minimizar el impacto en la operación mediante políticas de acceso más seguras y dinámicas.

Tras la identificación de amenazas, se realizó una evaluación cualitativa de los escenarios de riesgo, combinando las amenazas identificadas con los activos vulnerables para crear escenarios hipotéticos de incidentes de seguridad. Cada escenario se analizó para determinar su impacto potencial en la operación financiera, utilizando matrices de riesgo que relacionan la probabilidad de ocurrencia de cada amenaza con su impacto correspondiente.

Este análisis permitió priorizar los riesgos según su nivel de criticidad, estableciendo niveles de probabilidad e impacto conforme a las directrices propuestas por la norma ISO/IEC 27005 [53]. Para ello, se consideraron categorías de probabilidad (raro, improbable, posible, probable, casi seguro) e impacto (insignificante, menor, significativo o intermedio, mayor, severo o superior). A partir de esta clasificación, se estableció un sistema de nivel de riesgo, asignando valores numéricos del 1 al 5 a los niveles de probabilidad e impacto, que luego fueron multiplicados para obtener el nivel de riesgo final.

Este análisis de escenarios hipotéticos de incidentes de seguridad es crucial para implementar la propuesta metodológica de control de acceso a la red basado en Zero Trust, ya que permite priorizar los riesgos según su nivel de criticidad y establecer estrategias o controles específicos para cada riesgo identificado.

2.2.2 Resultados FASE 2: Riesgos asociados a las redes

Se identificaron varios activos críticos en la infraestructura tecnológica de las entidades financieras de Colombia que requieren atención prioritaria en ciberseguridad. Entre estos activos destacaron los sistemas core de tarjetas y crediticio, que son esenciales para el procesamiento de información financiera sensible y, debido a su alto valor estratégico, se convierten en objetivos comunes de ataques. La vulnerabilidad de estos sistemas podría derivar en interrupciones operativas, pérdidas financieras significativas y un daño considerable a la reputación de las entidades. Asimismo, los backends de aplicaciones móviles y web, que son puntos clave de interacción con los usuarios, están expuestos a ataques comunes como la inyección de código y exploits de día cero (Anexo C). La protección de estos componentes es fundamental para salvaguardar la información de los usuarios y mantener la integridad de los sistemas.

Otro activo crítico identificado fue la información bancaria, cuya naturaleza altamente sensible requiere medidas robustas de protección para prevenir fraudes, robos de identidad y otros delitos. Esto lleva a la necesidad de implementar políticas estrictas de cifrado, autenticación multifactor y monitoreo continuo para mitigar riesgos y garantizar una protección constante frente a amenazas emergentes.

El análisis de la criticidad de los activos identificados revela que todos ellos se clasificaron como "confidenciales" debido a su alta criticidad (Anexo C). Los sistemas core de tarjetas y crediticio presentaron un nivel de criticidad de 16, ya que son esenciales para la estabilidad financiera y la continuidad operativa de las instituciones; su compromiso podría generar riesgos significativos en el ámbito legal y reputacional. De manera similar, los backends de las aplicaciones móviles y web, con un nivel de criticidad de 15, desempeñan un papel clave en la interacción segura con los usuarios, por lo que cualquier afectación en estos sistemas impactaría negativamente en la competitividad y las ventas. Por último, la información bancaria, que tuvo el nivel más alto de criticidad (18), destaca por su alta sensibilidad; una brecha en su seguridad tendría un severo impacto en términos legales, de confianza y reputación.

Con respecto a los controles actuales, la encuesta realizada en la fase 1 del estudio evidenció que las organizaciones financieras presentan múltiples vulnerabilidades críticas que comprometen su seguridad (Anexo B). Se identificó una falta generalizada de actualizaciones de seguridad y parches, ausencia de mecanismos MFA, deficiencias en la gestión de usuarios privilegiados, y problemas de configuración en diversos sistemas, como el núcleo de tarjetas (débito/crédito), sistemas core crediticios, aplicaciones móviles y web del backend, así como en la infraestructura de información bancaria. Adicionalmente, se observaron serias carencias en la segmentación de red y en la implementación de controles adecuados para mitigar los riesgos de acceso no autorizado y

denegación de servicio (Anexo B). Estas debilidades incrementan significativamente el riesgo de intrusión y exponen a la organización a posibles compromisos de seguridad.

La evaluación del escenario de riesgo reveló que los activos críticos identificados en el sector financiero de Colombia están expuestos a múltiples amenazas graves, como malware, movimiento lateral, suplantación de identidad, acceso no autorizado y ransomware (Tabla 8). La exposición del sector a estas amenazas es considerada de alto riesgo debido al impacto operacional que pueden causar. Por lo tanto, las instituciones financieras deben implementar medidas de protección robustas, como herramientas de seguridad avanzadas y estrategias de monitoreo proactivo, para mitigar el impacto de ataques cibernéticos complejos, incluyendo el movimiento lateral dentro de las redes una vez que se ha logrado el acceso inicial. Además, es esencial adoptar estrategias de resiliencia cibernética para mantener la estabilidad operativa bajo condiciones adversas y prevenir daños mayores, alineándose con los esfuerzos globales para fortalecer las defensas frente a amenazas emergentes. Es importante resaltar que si bien hay más amenazas declaradas por los CISO's en la encuesta (Ver Anexo B), solo se tuvieron en cuenta las asociadas al acceso y a la red ya que son las alineadas al objetivo general de la tesis.

Tabla 8. Identificación de Activos Críticos y Amenazas en el Sector Financiero e Colombia

AMENAZAS / **ACTIVOS**	Sistema core tarjetas (Debido/crédito)	Sistema core crediticios	Backend APP Movil	Backend APP Web	Información bancaria (Debito/Crédito/libranzas /Crédito Vehículo.)
Malware	**X**	**X**	**X**	**X**	**X**
Movimiento lateral (piboteo)	**X**	**X**	**X**	**X**	**X**
Suplantación de identidad	**X**	**X**	**X**	**X**	
Acceso no autorizado	**X**	**X**	**X**	**X**	**X**
Ransomware	**X**	**X**	**X**	**X**	**X**

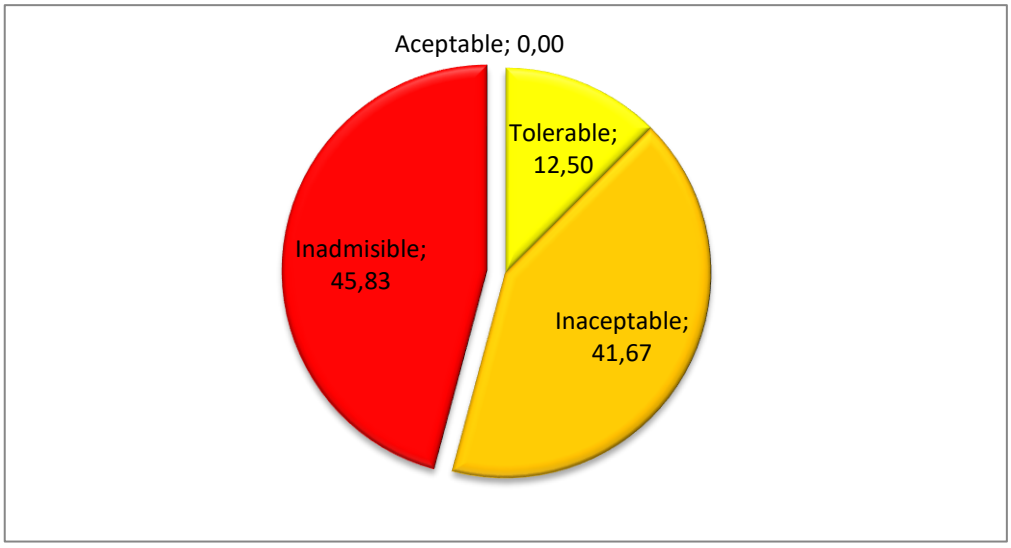
En cuanto a la identificación de riesgos, se identificaron 24, con una probabilidad de ocurrencia que va desde improbable hasta probable con consecuencias operativas de intermedio a superior (Tabla 9).

Tabla 9. Matriz de Riesgo Fase 2

Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4			(3) - (4) - (13) - (14) - (17) - (18) -	(1) - (2) - (5) -	(11) - (12) - (15) - (16) - (19) -
Posible	3			(22) - (23)		(20) - (21) - (24)
Improbable	2			(8) - (9) - (10) -	(6) - (7)	
Raro	1					

De estos 24 riesgos, 10 fueron inaceptables (naranja) y 11 inadmisibles (rojos), representando un 41.67% y 45.83%, respectivamente. Esto indica que casi la mitad de los escenarios evaluados requieren una acción inmediata debido a su alta probabilidad de ocurrencia y consecuencias operativas potenciales significativas. Por otro lado, los riesgos catalogados como tolerables representaron solo un 12.50% del total (Figura 19), lo que refleja que las medidas de control existentes son insuficientes para mitigar los riesgos más críticos.

Figura 19. Distribución Porcentual de los Riesgos Identificados



En resumen, la evaluación de los escenarios de riesgo mostró un alto nivel de amenazas críticas que impactan significativamente la confidencialidad de la información en las organizaciones financieras de Colombia. Entre las amenazas más relevantes se encuentran el malware, la suplantación de identidad, los accesos no autorizados y el ransomware, todas ellas con un riesgo elevado hacia la confidencialidad de la información. La probabilidad de ocurrencia de estas amenazas varió entre "probable" y "posible", mientras que su impacto se estimó entre "mayor" y "superior". Estas amenazas, en particular, afectan activos esenciales como los sistemas core de tarjetas de crédito, los sistemas crediticios, las aplicaciones móviles, los backends de aplicaciones web y la información bancaria (Anexo C). La materialización de cualquiera de estas amenazas podría comprometer la integridad de los datos, la continuidad de los servicios y la estabilidad operativa, destacando la necesidad urgente de reforzar los controles de seguridad para mitigar estos riesgos críticos.

Estos hallazgos son consistentes con lo reportado en la literatura académica. Por ejemplo, la falta de segmentación de red y controles de acceso inadecuados han sido identificados como factores críticos en la mayoría de las violaciones de seguridad cibernética [14], [87], [91]. De igual manera, la ausencia de actualizaciones y parches de seguridad es una de las principales causas de intrusiones [13], [148]. Adicionalmente, se ha documentado que el sector financiero enfrenta un aumento significativo de ataques debido a su dependencia de tecnologías digitales avanzadas [13], [39], [50]. En este contexto, la ciberseguridad debe ser tratada no solo como un aspecto técnico, sino como un componente esencial de la gestión de riesgos. Esto implica adoptar un enfoque proactivo, donde la colaboración entre sectores y la mejora continua de las estrategias de protección sean prioritarias para la detección temprana y prevención de amenazas [39].

En conjunto, los resultados obtenidos resaltan la urgencia de mejorar las medidas de seguridad existentes para mitigar estos riesgos y proteger la operación de las organizaciones financieras frente a posibles ataques cibernéticos. Para obtener más detalles sobre la identificación y evaluación de los riesgos en el sector financiero, consultar el Anexo C.

2.3 Metodología y resultados FASE 3

2.3.1 Metodología FASE 3: Caracterización de modelos de ZT

La metodología implementada para alcanzar el objetivo específico 3 *"Caracterizar los diferentes modelos de ZT actuales en la industria que puedan ser aplicados al sector financiero y a la reducción de riesgos"*, se estructuró en tres actividades interrelacionadas que se describen a continuación:

La primera actividad consistió en evaluar soluciones de Seguridad de Borde (SSE) disponibles en el mercado, utilizando como referencia el Cuadrante Mágico de Gartner [149] y las Olas de Forrester [150], dos herramientas ampliamente reconocidas en la investigación y consultoría en TIC. El Cuadrante Mágico de Gartner evalúa y clasifica a las empresas en diferentes cuadrantes en función de su capacidad de ejecución y visión integral, permitiendo identificar a las empresas líderes en diversos ámbitos de seguridad, como la red, la identidad y los dispositivos [149] . Por su parte, las Olas de Forrester proporcionan un análisis más detallado de las soluciones tecnológicas, considerando criterios como la efectividad, estrategia y presencia en el mercado [150]. La evaluación de estas herramientas permitió identificar a los proveedores que demostraron un rendimiento sobresaliente en la implementación de modelos de ZT.

A partir de estos resultados, la segunda actividad se centró en identificar y seleccionar las soluciones más adecuadas para fortalecer la ciberseguridad en el sector financiero de Colombia. Esto implicó un análisis detallado de las empresas líderes destacadas por Gartner y Forrester, con el fin de elegir aquellas que no solo sobresalieran en términos de seguridad, sino que también pudieran adaptarse a las necesidades específicas y al entorno regulatorio del país. Esta metodología garantiza un enfoque sistemático y basado en evidencia para la implementación de soluciones avanzadas de seguridad cibernética, logrando reducir riesgos de forma efectiva a través de la adopción de modelos de ZT.

La tercera actividad consistió en realizar una comparación detallada entre los líderes identificados por Gartner y Forrester, utilizando un Proceso de Jerarquía Analítica (AHP) basado en el método de

Saaty. Este enfoque se seleccionó por su capacidad para estructurar y analizar decisiones complejas, permitiendo descomponer el problema en criterios específicos para facilitar la comparación objetiva entre las soluciones líderes de seguridad. El modelo AHP se usó con el fin de identificar y seleccionar la empresa líder que mejor se ajustara a las necesidades del sector financiero colombiano, considerando tanto la efectividad en la protección de datos como su integración con las infraestructuras tecnológicas existentes.

Para lograr lo anterior, primero se definió el objetivo principal del análisis y se identificaron los criterios clave que influirían en la decisión final. Estos criterios fueron establecidos como factores esenciales, diseñados para incluir tanto aspectos cuantitativos como cualitativos relevantes para el contexto financiero. Una vez definidos el objetivo y los criterios, se construyó una jerarquía con el objetivo en el nivel superior, los criterios en un nivel intermedio y las alternativas de solución en el nivel inferior. Esta organización permitió un análisis estructurado, permitiendo la comparación directa de cada alternativa en relación con los criterios establecidos.

Considerando lo anterior, en el presente estudio se evaluaron cuatro criterios fundamentales para la selección del modelo líder que mejor se ajustara a las necesidades del sector financiero, los cuales se describen a continuación:

1. **Seguridad y protección avanzada:** Este criterio fue seleccionado porque las soluciones líderes identificadas por Gartner y Forrester deben ser capaces de identificar y mitigar amenazas cibernéticas como malware, suplantación de identidad y accesos no autorizados. Dado que el sector financiero maneja datos sensibles y está constantemente bajo el riesgo de ciberataques, las herramientas deben incluir mecanismos proactivos que ofrezcan protección integral y respuestas rápidas ante posibles vulnerabilidades. Esto asegura la continuidad de las operaciones y la confianza en los sistemas de seguridad.

2. **Compatibilidad e integración:** Este criterio se seleccionó porque las soluciones líderes de seguridad deben poder integrarse de manera eficiente con los sistemas operativos y aplicaciones empresariales existentes, como Windows, macOS y Linux sin interrumpir el flujo de trabajo. Esto es fundamental en el sector financiero, donde las interrupciones pueden afectar las operaciones críticas. La capacidad de integración sin problemas minimiza la necesidad de ajustes técnicos adicionales y asegura que la solución pueda operar junto con otros sistemas existentes sin generar conflictos.

3. **Escalabilidad y rendimiento:** Este criterio fue priorizado porque las soluciones deben ser capaces de manejar un número creciente de usuarios y dispositivos sin comprometer el rendimiento del sistema. En el sector financiero, donde la disponibilidad y la rapidez son esenciales para asegurar transacciones y servicios continuos, la capacidad de la solución para escalar es crucial. A través de la encuesta realizada en la fase 1 del estudio, se determinó que las soluciones debían soportar un mínimo de 500 usuarios, reflejando el tamaño promedio de las entidades financieras evaluadas. Esto asegura que la empresa líder que implementa el modelo de ZT no solo sea adecuada para las necesidades actuales, sino también para el crecimiento futuro, permitiendo a las instituciones expandir sus

operaciones sin enfrentar problemas de capacidad o necesidad de rediseñar la infraestructura de seguridad.

4. **Visibilidad y reportes granulares:** Para este criterio se consideró esencial que las herramientas tecnológicas ofrezcan la capacidad de monitorizar y registrar todos los accesos y actividades dentro de la red, asegurando que solo los usuarios y dispositivos autenticados y autorizados accedan a recursos específicos bajo políticas de seguridad estrictas. Esta visibilidad es clave para detectar patrones sospechosos y responder rápidamente ante cualquier posible amenaza. Además, la generación de reportes granulares facilita el cumplimiento de regulaciones y auditorías, asegurando que las políticas de seguridad se apliquen consistentemente y que solo usuarios autenticados accedan a recursos sensibles.

Este orden refleja la prioridad de proteger los datos sensibles y garantizar una integración fluida, seguida de la necesidad de mantener un rendimiento sólido y asegurar una visibilidad completa y detallada.

Posteriormente, se aplicó la técnica de comparación por pares, en la que cada criterio y alternativa fueron evaluados frente a los demás para determinar su importancia relativa. Esta metodología utilizó una escala de valores para asignar ponderaciones a cada criterio, estableciendo prioridades que reflejaban su relevancia en el contexto de la decisión, como se describe en la Tabla 10. Los resultados de estas comparaciones fueron sintetizados matemáticamente para calcular las ponderaciones finales, asegurando consistencia y coherencia en las evaluaciones. La comparación pareada, se usó para asegurar que las decisiones reflejaran de manera precisa las necesidades críticas del sector financiero, destacando criterios esenciales.

Tabla 10. Escala de Comparación Pareada.

Escala de Comparación pareada en AHP por Saaty		
Intensidad	**Definición**	**Explicación**
1	De igual importancia	2 actividades contribuyen de igual forma al mismo objetivo
3	Moderada importancia	La experiencia y el juicio favorecen levemente a una actividad sobre la otra
5	Importancia fuerte	La experiencia y el juicio favorecen fuertemente a una actividad sobre la otra
7	Muy fuerte	Una actividad es mucha más favorecida que la otra
9	Extrema	La evidencia que favorece una actividad sobre la otra es absoluta y totalmente clara
2,4,6,8	Valores intermedios	Cuando se necesita un compromiso de las partes entre valores adyacentes

Finalmente, las alternativas fueron calificadas según los criterios ponderados, proporcionando una vector promedio para cada opción. Este análisis permitió identificar de manera objetiva la solución

más adecuada para el sector financiero, asegurando que la selección estuviera respaldada por un proceso metodológico estructurado y basado en evidencia.

Los resultados obtenidos del modelo AHP permitieron identificar la solución de seguridad con el puntaje más alto, destacando a la empresa que mejor cumplió con los criterios establecidos. Basándose en el conocimiento y desempeño de la empresa seleccionada, se diseñó una metodología de ZT para su aplicación en el sector financiero colombiano. Esta propuesta toma como referencia el modelo de la empresa líder en términos de protección de datos, integración fluida, rendimiento eficiente y visibilidad detallada, asegurando que las necesidades específicas del sector se aborden de manera integral.

En resumen, para la selección de la mejor alternativa a usar haciendo uso del método AHP, se ejecutaron los siguientes pasos:

a) Identificación de alternativas a comparar.

b) Identificación de criterios

c) Realizar la matriz de comparación pareada entre criterios, normalizar y obtener el vector promedio.

d) Realizar la ponderación de criterios vs. elementos, normalizar y sacar vector promedio.

e) Obtener la matriz jerárquica final, seleccionando la opción con mayor peso.

2.3.2 Resultados FASE 3: Caracterización de modelos de ZT

- **Resultados de la Evaluación de Soluciones SSE**

La evaluación exhaustiva de las SSE disponibles en el mercado, utilizando como referencia el cuadrante mágico de Gartner muestra la clasificación de los proveedores según dos dimensiones: capacidad de ejecución e integridad de visión (Figura 2-4).

De acuerdo a este cuadrante, los líderes como Netskope, Zscaler y Palo Alto Networks, destacaron por su fuerte capacidad operativa y una visión integral que les permite ofrecer soluciones completas y efectivas. Netskope se distingue por mantener Puntos de Presencia (POPs) cerca de los centros de población clave y por su enfoque robusto en seguridad de datos, mientras que Palo Alto Networks sobresale por su gestión unificada de SSE y *firewalls on-premises*. Zscaler continúa fortaleciendo su posición a través del crecimiento en la seguridad de aplicaciones SaaS, aunque algunos clientes mencionan desafíos en el rendimiento y la complejidad del licenciamiento.

Fortinet aparece como un retador, mostrando buen rendimiento, pero con una estrategia menos desarrollada. Por tal motivo, este proveedor se enfoca en mejorar la cobertura de POPs y la integración de capacidades a través de su oferta FortiSASE. Por su parte, los visionarios, como Skyhigh Security y Lookout, presentan ideas innovadoras en seguridad de datos y visibilidad para aplicaciones de software por servicio o *"Software As a Service"* (SaaS), pero enfrentan desafíos en la ejecución y expansión de mercado. Finalmente, los jugadores de nicho como Versa Networks, Cloudflare, Broadcom e iboss se enfocan en soluciones específicas, con alcance limitado en comparación con los líderes. Por ejemplo, Broadcom, con su Symantec DLP Cloud, atiende principalmente a grandes empresas, mientras que Cloudflare sigue consolidando su presencia global a pesar de ciertas brechas técnicas.

La Figura 20 ilustra que, en el Cuadrante Mágico de Gartner, los líderes se sitúan en la parte superior derecha, lo que refleja su sobresaliente capacidad de ejecución y una visión estratégica integral. Netskope, Palo Alto Networks y Zscaler ocupan esta posición, demostrando que sus soluciones de seguridad son robustas, innovadoras y consistentes. Estos proveedores son reconocidos por encabezar el mercado con ofertas completas y bien integradas, además de tener una visión clara y anticipada sobre las futuras necesidades del sector, lo que refuerza su liderazgo en servicios de seguridad.

Figura 20. Cuadrante Mágico de Gartner [149].

La evaluación de las Olas de Forrester para soluciones SSE clasificó a los proveedores en cuatro categorías: líderes, fuertes ejecutores, contendientes y retadores, basándose en la calidad de sus ofertas actuales, la solidez de su estrategia y su presencia en el mercado (Figura 21). Este enfoque permite identificar qué empresas no solo destacan en la tecnología que ofrecen, sino que también poseen una visión estratégica clara y un sólido posicionamiento que les otorga ventaja competitiva dentro del sector.

Entre los líderes, Netskope, Forcepoint, Palo Alto Networks y Zscaler sobresalieron por sus soluciones integrales y avanzadas que priorizan la protección de datos y la seguridad de la fuerza laboral remota, al incorporar enfoques innovadores como el modelo de ZT. Netskope destacó por su fuerte énfasis en la protección de datos, con capacidades robustas para identificar y salvaguardar información sensible a través de múltiples entornos, desde los endpoints hasta la nube. Palo Alto Networks sobresalió porque integra de manera efectiva la seguridad de red y modelos de ZT, proporcionando sólidas funciones de ZTNA y mejoras significativas en seguridad de red. Zscaler fue reconocido por su conectividad robusta basada en ZT a una amplia gama de aplicaciones y dispositivos. Por último, Forcepoint se clasificó como líder al fortalecer su plataforma con herramietas avanzadas de Corredor de Seguridad de Acceso a la Nube (CASB) y prevención de pérdida de datos (DLP) adaptativo al riesgo.

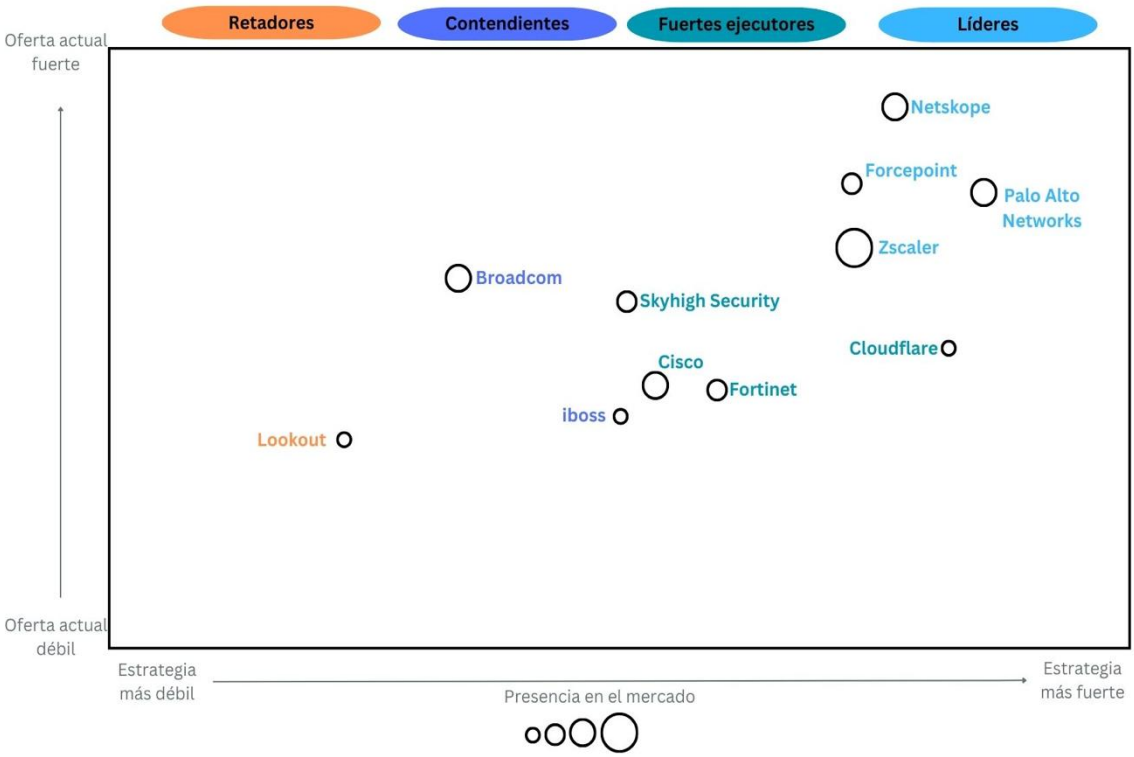
Los Fuertes ejecutores, como Cloudflare, Fortinet, Skyhigh Security y Cisco destacaron por su sólida capacidad operativa. Cloudflare ofrece rendimiento y facilidad de gestión, especialmente en entornos DevOps, aunque tiene áreas por mejorar en DLP. Fortinet combina funcionalidades clave como ZTNA, SWG, CASB y Aislamiento Seguro del Navegador (RBI), pero necesita fortalecer sus capacidades en clasificación de datos y DLP. Skyhigh Security se especializa en gestión de datos, aunque debe avanzar en conectividad y agilidad en la implementación. Cisco sobresalió por su seguridad de red avanzada, pero enfrenta desafíos en la entrega a través de la nube y en la expansión de su alcance global.

En la categoría se incluyeron a Iboss y Broadcom. Iboss se caracterizó por ofrecer soluciones SSE sencillas y con un fuerte soporte al cliente. Su enfoque basado en el modelo de ZT y una arquitectura unificada permite un despliegue rápido y eficiente, utilizando el mismo software para dispositivos móviles, portátiles y servidores. Sin embargo, Iboss necesita fortalecer sus capacidades en protección de datos y funciones de CASB. Por otro lado, Broadcom destacó en la priorización de acceso y la protección de datos, pero su enfoque en grandes empresas, prácticas de licenciamiento y lentitud en la entrega de nuevas características han recibido críticas.

Finalmente, en el grupo de los retadores Lookout sobresalió en la solución para endpoints con capacidades de cifrado y controles basados en el comportamiento del usuario. Aunque su sistema permite un control detallado de datos, requiere mejoras en la tecnología para la fuerza laboral remota y la generación de informes.

La Figura 21 permite la visualización de los proveedores según la fortaleza de su oferta actual, la efectividad de su estrategia y presencia en el mercado. Los líderes, como Netskope, Zscaler, Palo Alto Networks y Forcepoint, se sitúan en el extremo superior derecho, reflejando su fuerte capacidad de ejecución y visión estratégica. Cloudflare aparece cerca de estos, resaltando su rápido avance en la seguridad en la nube, mientras que otros como Fortinet y Skyhigh Security, aunque destacados, muestran áreas para mejorar en estrategia o integración tecnológica.

Figura 21. Olas de Forrester. Adaptado de [150].

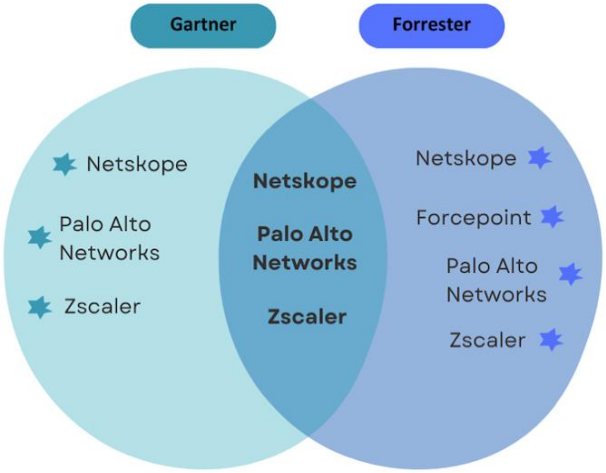


Los resultados de las evaluaciones del Cuadrante Mágico de Gartner y las Olas de Forrester, sugieren que la integración de modelos ZT y ZTNA es un factor clave que distingue a los líderes en el mercado de soluciones SSE. Estos enfoques proporcionan seguridad reforzada en entornos digitales al garantizar que el acceso a los recursos esté basado en la verificación continua de identidad y contexto, protegiendo datos sensibles y asegurando conexiones seguras. Los proveedores que adoptan estrategias centradas en ZT están mejor posicionados para abordar las demandas de seguridad actuales y futuras en las organizaciones.

- **Identificación de empresas líderes de Gartner y Forrester**

La comparación entre las evaluaciones de Gartner y Forrester permitió identificar a Netskope, Palo Alto Networks y Zscaler como líderes consolidados en el mercado de SSE, posicionándose destacadamente en ambas firmas (Figura 22).

Figura 22. Empresas Líderes Reconocidas por Gartner y Forrester



La identificación de empresas líderes basadas en SSE es fundamental para la adopción de ZTNA, ya que proporcionan soluciones integrales de seguridad que protegen el acceso a datos y aplicaciones, tanto en la nube como en entornos locales. Esto garantiza que solo los usuarios autorizados accedan a los recursos, lo cual es esencial para las empresas financieras que manejan grandes volúmenes de datos confidenciales, reduciendo significativamente el riesgo de brechas de seguridad [83].

Las empresas que fueron reconocidas como líderes tanto por Gartner como por Forrester refuerzan la confianza de las organizaciones financieras en la selección de soluciones SSE. Esta doble validación garantiza que dichos proveedores han sido evaluados bajo criterios rigurosos y desde múltiples perspectivas, resultando en soluciones tecnológicas consistentes, robustas y alineadas con las necesidades estratégicas de seguridad de las instituciones financieras [83].

Esta concordancia también minimiza el riesgo en la toma de decisiones de TI, especialmente en el ámbito de la seguridad de la información, donde una mala elección puede comprometer la protección de datos sensibles. Al optar por proveedores reconocidos por ambas firmas, las instituciones financieras pueden estar seguras de que eligen soluciones que han demostrado un rendimiento sobresaliente en tecnología, innovación y satisfacción del cliente [83].

Para las empresas financieras del país, esta coincidencia significa acceso a las mejores prácticas, tecnologías avanzadas y soporte al cliente de alta calidad. Esto les permite adaptarse rápidamente a nuevas amenazas y garantizar el cumplimiento normativo, protegiendo a su vez la confianza de los clientes, lo que es esencial para su estabilidad en el entorno competitivo colombiano. Por lo tanto, apoyarse en los líderes del mercado SSE es clave para desarrollar una metodología ZT

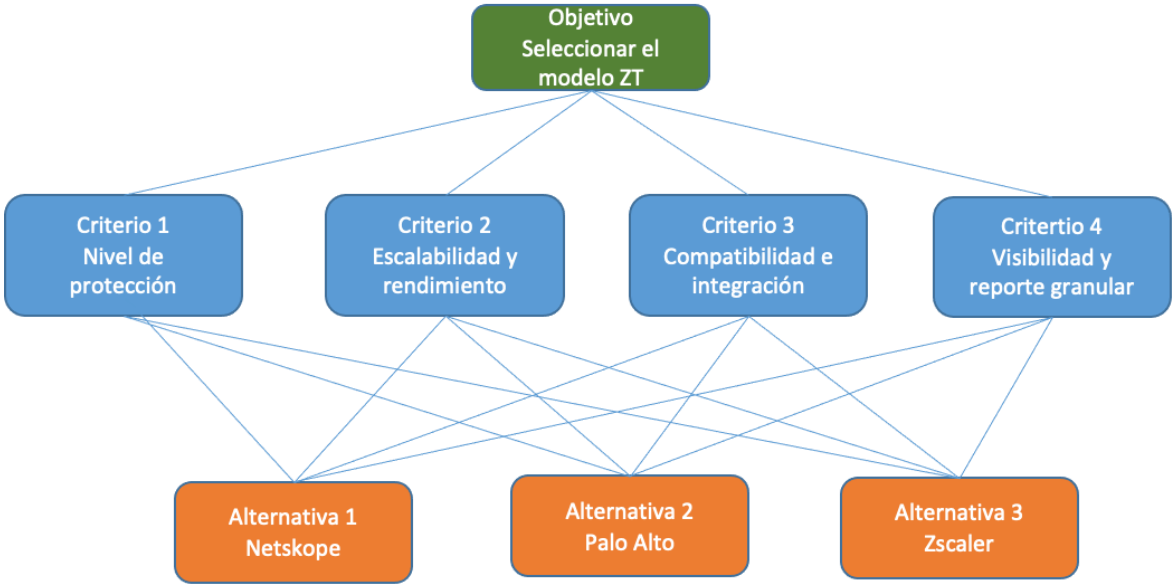
centrada en la gestión de identidad y control de acceso, asegurando la mejor protección contra amenazas internas y externas

- **Comparación de empresas líderes y selección mediante el modelo AHP**

Una vez identificadas las empresas líderes consideradas por Gartner y Forrester, se definió el objetivo principal del análisis: seleccionar la empresa líder (y su producto) para implementar el modelo ZT más adecuado en el contexto financiero colombiano. Para ello se han ejecutado los 5 pasos de la metodología AHP.

Como se describe en la Figura 23 para lograr este objetivo, se construyó una estructura jerárquica, donde el objetivo central de seleccionar el modelo ZT se situó en el nivel superior. En el nivel intermedio se establecieron los cuatro criterios clave que guiaron el proceso de evaluación: nivel de protección, escalabilidad y rendimiento, compatibilidad e integración, y visibilidad y reporte granular. En el nivel inferior de la jerarquía se consideraron tres alternativas de solución, representadas por las empresas Netskope, Palo Alto y Zscaler.

Figura 23. Modelo AHP



La estructura jerárquica facilitó la identificación de la empresa que mejor se ajusta a los requerimientos del entorno financiero, proporcionando una base sólida para tomar decisiones estratégicas en la implementación del modelo ZT.

La matriz de comparación pareada mostró que el nivel de protección fue el criterio más relevante, con un vector promedio de 0.55, destacando la importancia de ofrecer una protección robusta en este contexto. El segundo criterio más importante fue la compatibilidad e integración, con un

vector promedio de 0.28 (Tabla 11). Criterios como escalabilidad y rendimiento (0.13), visibilidad y reporte granular (0.05) tuvieron un peso menor en la decisión (Tabla 11).

Tabla 11. Matriz de Comparación Pareada

Matriz de Comparación Pareada									
	Nivel de protección	Escalabilidad y rendimiento	Compatibilidad e integración	Visibilidad y reporte granular	**Matriz normalizada**				**Vector promedio**
Nivel de protección	1.00	5.00	3.00	9.00	0.61	0.45	0.68	0.45	0.55
Escalabilidad y rendimiento	0.20	1.00	0.20	5.00	0.12	0.09	0.05	0.25	0.13
Compatibilidad e integración	0.33	5.00	1.00	5.00	0.20	0.45	0.23	0.25	0.28
Visibilidad y reporte granular	0.11	0.20	0.20	1.00	0.07	0.02	0.05	0.05	0.05
Totales	1.64	11.20	4.40	20.00					

Con base en el análisis de la matriz jerárquica, **Netskope** se posicionó como la solución más destacada, alcanzando un puntaje total del **50.22%.** Este resultado estuvo principalmente impulsado por su sobresaliente desempeño en compatibilidad e integración (0.69) y un fuerte nivel de protección (0.45), aspectos que fueron ponderados con los mayores pesos relativos en la evaluación. La escalabilidad y rendimiento de Netskope también contribuyeron positivamente con un valor de 0.41, reforzando su idoneidad como solución integral para las necesidades del sector financiero colombiano (Tabla 12).

El Anexo D, proporciona un desglose completo de la ponderación de los criterios y la evaluación de cada proveedor en función de su desempeño en la matriz.

Tabla 12. Matriz Jerárquica

Matriz Jerárquica					
	Nivel de protección	Escalabilidad y rendimiento	Compatibilidad e integración	Visibilidad y reporte granular	**Total**
Netskope	0.45	0.41	0.69	0.19	50.22%
Palo alto	0.45	0.33	0.07	0.72	34.19%
Zscaler	0.09	0.26	0.25	0.08	15.59%
Ponderación	0.55	0.13	0.28	0.05	

Basados en estos resultados, Netskope fue seleccionado como modelo para proponer los pasos de la metodología de Zero Trust para su aplicación en el sector financiero colombiano. Esta empresa líder al destacar en los criterios más relevantes como nivel de protección y compatibilidad e integración, proporciona una base sólida para la implementación de una estrategia ZT efectiva, asegurando una protección integral, facilidad de integración con las infraestructuras existentes, y un rendimiento adecuado para las necesidades de las instituciones financieras del país.

- **Propuesta metodológica para el control de acceso a la red basado en Zero Trust en el sector financiero colombiano**

Las instituciones financieras en Colombia enfrentan un panorama de ciberseguridad cada vez más complejo y dinámico, donde la protección de la información y la continuidad operativa son fundamentales. Para enfrentar estos desafíos, en la presente tesis se propone la implementación de un modelo de seguridad ZT, que parte de la premisa de que ninguna entidad, ya sea interna o externa, es automáticamente confiable.

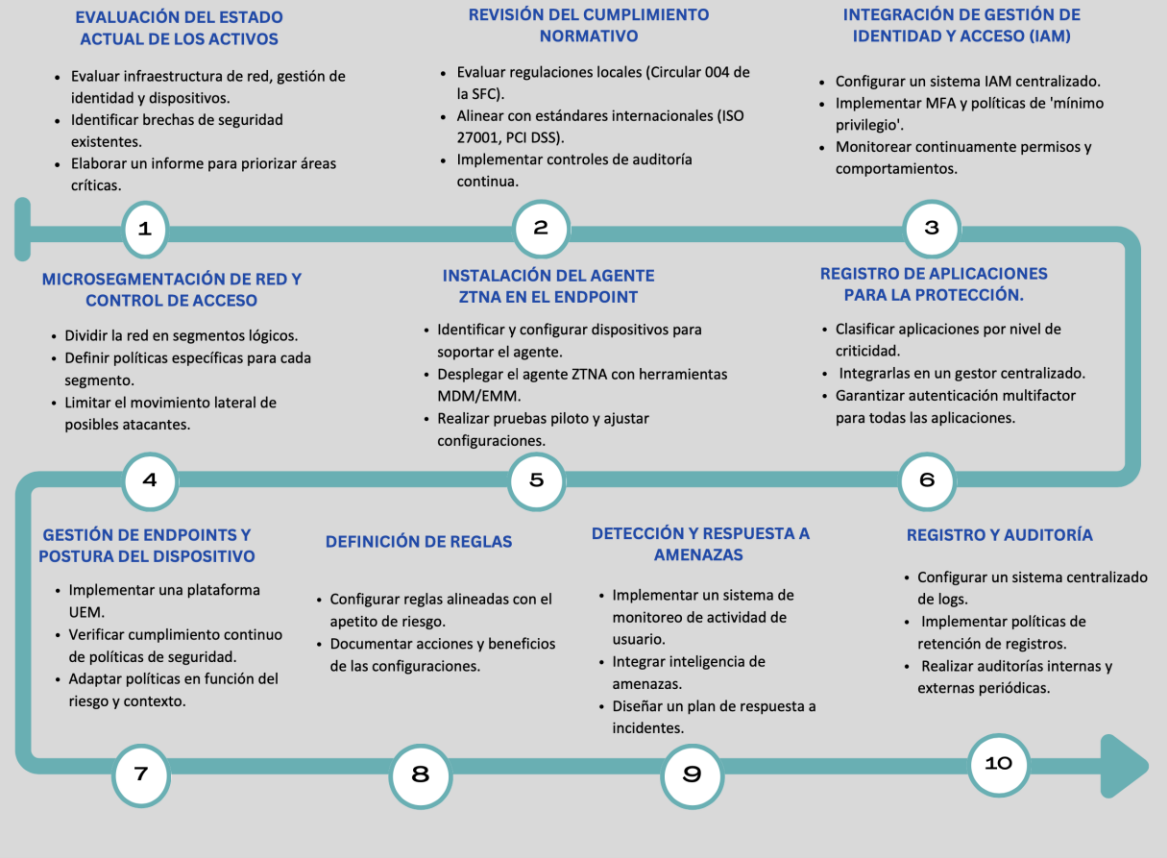
A continuación, se presenta una metodología integral para la adopción de ZT, diseñada para ajustarse a las necesidades específicas de las instituciones financieras colombianas. Los pasos propuestos se desarrollaron tomando como referencia a **Netskope**, la empresa líder seleccionada, asegurando que la metodología no solo ofrezca protección de activos críticos y cumplimiento normativo, sino que también incorpore las mejores prácticas del sector en el modelo ZT. Este enfoque estructurado facilita la implementación de una estrategia de seguridad robusta, alineada con los estándares y demandas del sector financiero.

Es importante resaltar que la metodología propuesta desarrolla el tratamiento de los riesgos identificados en el objetivo 2, de los cuales cubrirá los riesgos que tienen como amenaza el malware, movimiento lateral, suplantación de identidad y acceso no autorizado. Sin embargo, los riesgos relacionados a la amenaza Ransomware no son cubiertos por esta metodología, ya que esta busca atacar los riesgos a partir del control de acceso a la red y a las aplicaciones teniendo en

cuenta una postura del dispositivo. Esto se debe a que un Ransomware cifra la información del dispositivo, por ende, no se podrá tener acceso a ninguna aplicación.

La metodología, que se describe a continuación en la Figura 24, aborda desde la evaluación inicial de activos y cumplimiento normativo hasta la integración de herramientas avanzadas como la gestión de IAM y la detección y respuesta a amenazas, con un énfasis en la microsegmentación de red, la gestión de endpoints y la postura del dispositivo. Esta estructura garantiza un enfoque progresivo y detallado para una implementación efectiva del modelo ZT.

Figura 24. Diagrama de la Metodología Propuesta para el Control de Acceso a la Red Basado en Zero Trust



Paso 1: Levantamiento del Estado Actual de los Activos

La implementación efectiva de un modelo Zero Trust (ZT) requiere una metodología estructurada y exhaustiva. El primer paso crucial en este proceso consiste en llevar un levantamiento del estado actual de la infraestructura de la institución. Este análisis debe incluir una revisión minuciosa de la infraestructura de red, los sistemas de gestión de identidad y los dispositivos de punto final conectados a la red. Para realizar esta revisión, es esencial comprender la estructura de la red, las rutas de acceso actuales, y el perfil de acceso de los dispositivos y usuarios a los recursos disponibles. En esta etapa, también se deben identificar las brechas de seguridad existentes, tales como sistemas no actualizados, configuraciones incorrectas o acceso no supervisado a recursos sensibles. Además, es necesario evaluar las herramientas y prácticas actuales de autenticación y autorización para identificar áreas que requieran mejoras inmediatas.

Una vez completada esta evaluación inicial, es imperativo proceder a la identificación de las necesidades específicas de seguridad de las instituciones financieras. Esta fase debe incluir una evaluación de los riesgos inherentes a las operaciones diarias, como la gestión de transacciones financieras, la protección de datos de clientes y la capacidad de respuesta ante ciberataques. La evaluación debe considerar los requisitos únicos de cada departamento dentro de la institución, dado que diferentes áreas pueden presentar distintos niveles de riesgo y necesidades de seguridad. Por ejemplo, los sistemas que manejan información financiera confidencial requerirán controles de seguridad más rigurosos en comparación con los sistemas administrativos.

El resultado de esta evaluación exhaustiva será un informe comprensivo que destacará las áreas de mayor riesgo y vulnerabilidad, proporcionando una hoja de ruta para las mejoras necesarias. Este informe servirá como base para las decisiones de diseño de la infraestructura ZT, asegurando que las inversiones en seguridad se prioricen de manera que maximicen la mitigación de riesgos. Además, el análisis inicial permitirá a la institución medir el progreso en la implementación del modelo ZT, garantizando el cumplimiento de los objetivos de seguridad establecidos.

Paso 2: Revisión del Cumplimiento Normativo

En la implementación del modelo ZT en el sector financiero colombiano, el cumplimiento normativo se configura como un aspecto fundamental. Por lo tanto, el segundo paso en esta metodología es identificar y comprender a fondo las normativas relevantes que rigen la Seguridad de la Información y el Control de Acceso en el contexto colombiano. Este proceso comienza con la evaluación de regulaciones específicas, como la Circular 004 de 2019 de la Superintendencia Financiera de Colombia (SFC), que establece directrices sobre seguridad de la información. La comprensión de esta normativa es esencial para definir los estándares mínimos que las instituciones financieras deben cumplir para asegurar la confidencialidad, integridad y disponibilidad de la información.

Posteriormente, es esencial alinear la infraestructura de seguridad con estándares internacionales reconocidos, como la norma ISO 27001, que ofrece un marco para la Gestión de la Seguridad de la Información, y el PCI DSS, particularmente relevante para las instituciones que gestionan datos de tarjetas de pago. La adopción de estos estándares no solo facilita el cumplimiento de las regulaciones locales, sino que también refuerza la postura de la institución en términos de ciberseguridad, garantizando la aplicación de mejores prácticas globales.

Asimismo, es crucial colaborar estrechamente con los equipos legales y de cumplimiento normativo para asegurar que todas las políticas de seguridad estén alineadas con las regulaciones aplicables. Este paso incluye la adaptación de configuraciones de seguridad, la documentación de procesos y procedimientos, y la capacitación del personal para familiarizarlos con los requisitos normativos.

Además, se debe establecer un proceso continuo de evaluación del cumplimiento para asegurar que la institución se mantenga alineada con las normativas, especialmente a medida que estas

evolucionan. Este proceso implica realizar auditorías internas regulares y la implementación de controles automatizados para la supervisión en tiempo real del cumplimiento, minimizando el riesgo de sanciones regulatorias y asegurando la integridad de la institución. De este modo, no solo se asegura el cumplimiento normativo, sino también la preparación ante nuevos desafíos de seguridad.

Paso 3: Integración de Gestión de Identidad y Acceso (IAM)

La implementación del modelo ZT en el sector financiero requiere una metodología sólida para la IAM, dado que la protección de datos es crucial. De este modo, el tercer paso de la metodología propuesta se centra en establecer un sistema de IAM centralizado que controle de manera eficiente el acceso a los recursos, determinando quién tiene acceso, a qué recursos y bajo qué condiciones.

Para lograr esto, primero, se debe implementar un sistema IAM que gestione integralmente el ciclo de vida de las identidades, desde la incorporación hasta la eliminación de accesos. Este sistema debe permitir la creación de perfiles detallados que reflejen las funciones laborales específicas de los usuarios. Por lo tanto, es necesario configurar el sistema para asignar permisos de acceso basados en roles, asegurando que cada usuario tenga acceso únicamente a los recursos necesarios para el desempeño de su función.

En paralelo, se debe integrar la MFA para añadir una capa adicional de seguridad. Esta integración es esencial para reforzar el principio de "mínimo privilegio", limitando el acceso a recursos sensibles solo a usuarios que puedan autenticar su identidad de manera robusta. La MFA debe ser implementada de manera que permita una gestión centralizada y automatizada de permisos, facilitando la actualización de estos en respuesta a cambios en las funciones laborales o en los requerimientos de seguridad.

A continuación, se debe realizar un mapeo exhaustivo de las identidades y sus permisos actuales, identificando excesos de privilegios o accesos innecesarios. Basado en este análisis, se aplicarán políticas de "mínimo privilegio" para restringir el acceso a los recursos a los usuarios y dispositivos que realmente lo requieran.

Es fundamental establecer un sistema de monitoreo continuo que permita la detección de patrones de comportamiento anómalos, como intentos de acceso fuera del horario habitual o desde ubicaciones inusuales. Las anomalías detectadas deben generar alertas automáticas y activar medidas de seguridad adicionales, tales como solicitudes de autenticación adicional o la revocación temporal del acceso.

Finalmente, el sistema IAM debe ser dinámico y adaptarse a los cambios en la organización y en el entorno de amenazas. Por esta razón, las políticas de acceso deben ser revisadas y actualizadas regularmente para reflejar las modificaciones en las funciones de los usuarios, en la estructura organizativa y en las amenazas emergentes.

La integración de la IAM con MFA mejorará la capacidad de las instituciones financieras para prevenir accesos no autorizados, identificando y abordando riesgos antes de que se materialicen. De esta manera, una gestión eficaz de identidad y acceso no solo protege los activos críticos, sino que también asegura el cumplimiento normativo, manteniendo una documentación y control riguroso de todas las identidades y accesos.

Paso 4: Microsegmentación de Red y Control de Acceso

La microsegmentación es una técnica clave en la estrategia de ZT, que permite dividir la red en segmentos más pequeños y lógicamente aislados, cada uno con sus propias políticas de seguridad. En una institución financiera, donde la protección de datos sensibles es crítica, la microsegmentación ayuda a limitar el movimiento lateral de posibles atacantes dentro de la red.

El principal paso en la implementación de la microsegmentación es realizar un mapeo detallado de la red. Este proceso implica identificar los flujos de datos y las interacciones entre aplicaciones y sistemas. Con esta información, se pueden definir segmentos lógicos que reflejen tanto las necesidades operativas como las de seguridad de la institución financiera. Cada segmento debe ser diseñado para garantizar una protección adecuada, acorde con su función y nivel de sensibilidad de los datos que maneja.

Paso 5: Instalación del agente ZTNA en el endpoint

Para implementar un control de acceso basado en Zero Trust en el sector financiero colombiano, es importante comenzar con la identificación de los endpoints que requieren el agente ZTNA. En esta fase inicial, se realiza un análisis exhaustivo de los dispositivos que se conectarán a la red, verificando que cumplan con los requisitos mínimos de hardware y software necesarios para soportar el agente. Es importante definir las políticas de seguridad y acceso que regirán el comportamiento del agente, ajustadas a los principios de Zero Trust, tales como la aplicación de mínimos privilegios y la segmentación del acceso a recursos.

Una vez identificados los dispositivos, se procede al despliegue automatizado del agente ZTNA en cada uno de los endpoints. Para lograr esto, se deben emplear herramientas de gestión de dispositivos como MDM/EMM, que permiten distribuir el agente de manera remota y eficiente, minimizando la intervención manual. Este despliegue automatizado asegura que la instalación se realice de manera consistente en todos los dispositivos, reduciendo el riesgo de errores humanos y garantizando una rápida implementación. El despliegue debe estar acompañado de monitoreo en tiempo real para detectar y corregir cualquier anomalía durante la instalación, asegurando que todos los endpoints cumplan con los requisitos de seguridad antes de ser autorizados para acceder a la red.

La configuración del agente ZTNA es un paso crucial en esta metodología, ya que determina cómo se controlará el acceso a los recursos de la red. Antes de proceder con la instalación, se deben

definir las configuraciones predeterminadas del agente en función de las políticas de seguridad establecidas por la organización. La IAM debe ser un componente obligatorio en estas configuraciones, así como la segmentación del acceso a los recursos según la identidad y el contexto del usuario. Esta configuración debe ser lo suficientemente flexible para permitir su ajuste en función de las necesidades operativas, pero también robusta para garantizar la protección continua de los endpoints.

Después de la instalación y configuración inicial, el sistema debe someterse a pruebas exhaustivas para validar que el agente ZTNA funcione correctamente en diversos escenarios operacionales. Estas pruebas asegurarán que los dispositivos solo puedan acceder a los recursos que se les han autorizado, y que cualquier intento de acceso no autorizado sea bloqueado inmediatamente. Además, se debe verificar que el agente esté correctamente integrado con otras soluciones de seguridad existentes, como los cortafuegos de próxima generación (NGFW) y los sistemas de EDR, para garantizar una visibilidad completa del comportamiento del endpoint.

El monitoreo continuo es una parte esencial de la metodología, asegurando que todos los dispositivos cumplan con las políticas de seguridad en todo momento. Además, debe garantizarse que las actualizaciones del agente ZTNA se realicen automáticamente, con el fin de mantener la seguridad frente a amenazas emergentes. El proceso de actualización debe ser fluido y transparente para los usuarios, sin interrumpir la operación normal de los dispositivos.

Finalmente, se recomienda realizar una prueba piloto en un entorno controlado para validar el comportamiento del sistema. Esta prueba permite simular diversos escenarios y garantizar que el control de acceso sea efectivo, dinámico y capaz de ajustarse a las necesidades del sector financiero colombiano. Al integrar el despliegue automatizado, la configuración adecuada y un monitoreo continuo, se refuerza la protección de la red y se garantiza que los endpoints estén alineados con los principios de Zero Trust, minimizando así el impacto de amenazas en la operación de la organización.

Paso 6: Registro de aplicaciones que serán parte de la protección

El registro de aplicaciones comienza con la identificación de todas las aplicaciones que interactúan con la red y los criterios de la organización, aplicaciones propias o de terceros. Para ello, es fundamental realizar una evaluación que clasifique estas aplicaciones según su nivel de criticidad, tomando en cuenta el tipo de datos que manejan y su relevancia para las operaciones financieras.

Una vez identificadas, las aplicaciones deben ser registradas en un gestor centralizado que permita un control y monitoreo constante. Este gestor debe ser capaz de integrar tanto aplicaciones locales como en la nube o de terceros asegurando que el control de acceso esté alineado con las políticas de segmentación de red establecidas por el enfoque Zero Trust. El registro debe incluir información clave como los roles de usuarios que pueden acceder a cada aplicación, los permisos asignados, y el nivel de autenticación requerido.

Es indispensable que todas las aplicaciones registradas estén protegidas mediante un mecanismo de autenticación multifactor, que garantice que solo usuarios autorizados accedan a ellas. Además, debe evaluarse la interacción entre las aplicaciones para detectar y mitigar posibles vulnerabilidades que puedan comprometer la seguridad de la red.

Para mantener la efectividad del registro, es necesario establecer un ciclo de revisión continua, donde se verifique la actualización de las aplicaciones y se asegure que cumplen con las políticas de seguridad vigentes. Las auditorías periódicas permiten confirmar que las aplicaciones registradas siguen siendo seguras y están alineadas con los principios de Zero Trust, lo que minimiza los riesgos de acceso no autorizado y ataques internos.

Paso 7: Gestión de Endpoints y Postura del Dispositivo

En un entorno ZT, la seguridad de los dispositivos que acceden a la red es tan importante como la seguridad de la red misma. Por lo tanto, en este paso se propone la implementación de una plataforma de Gestión Unificada de Endpoints (UEM) para asegurar que todos los dispositivos conectados cumplan con las políticas de seguridad de las instituciones.

El primer paso en este enfoque metodológico es desplegar una plataforma UEM que permita la administración centralizada de todos los dispositivos conectados a la red, incluyendo computadoras, dispositivos móviles, cajeros automáticos y terminales de punto de venta. La UEM facilita la aplicación coherente de políticas de seguridad en todos los endpoints, sin importar su tipo o ubicación.

Una de las actividades relevantes en la metodología es hacer una clasificación de los endpoints administrados y no administrados, ya que a partir de esta diferenciación se pueden aplicar políticas de seguridad, evaluar riesgos, denegar accesos y aplicar políticas de acceso granulares. Esto se hace

A continuación, se debe establecer un proceso de verificación continua de la postura de seguridad de los dispositivos. Antes de permitir el acceso a la red, cada dispositivo debe ser sometido a una evaluación que verifique su cumplimiento con las políticas de seguridad. Esta evaluación incluye la comprobación del estado de actualización del sistema operativo, la presencia de software de seguridad activo (como antimalware, control de navegación, DLP en el endpoint, entre otros) y la identificación de posibles vulnerabilidades. Los dispositivos que no cumplan con estos requisitos podrán ser aislados, bloqueados, retados (MFA) con accesos condicionales.

Una vez que los dispositivos están conectados, la UEM debe ser capaz de detectar y responder a amenazas en tiempo real. Esto implica la implementación de herramientas que monitoricen el tráfico de red y los comportamientos de los dispositivos, detectando patrones anómalos como accesos no autorizados o tráfico inusualmente alto.

Es esencial que las políticas de seguridad sean adaptativas y basadas en el riesgo. Estas políticas deben configurarse para evaluar continuamente el contexto y el riesgo asociado con cada solicitud de acceso, aplicando controles dinámicos que se ajusten a las condiciones cambiantes. El modelo de "Denegación por Defecto" debe ser implementado, de manera que todas las solicitudes de acceso sean denegadas automáticamente a menos que se concedan explícitamente, garantizando así que solo se permita el acceso cuando se cumplan todos los criterios de seguridad.

El principio de "Mínimo Privilegio" debe ser aplicado para asegurar que los permisos otorgados a usuarios y dispositivos se limiten estrictamente a lo necesario para realizar sus funciones. Esto reduce la exposición a riesgos innecesarios y fortalece la seguridad general.

El marco de actuación debe incluir controles de cuarentena, donde el dispositivo con incumplimientos solo puede acceder a recursos limitados, como actualizaciones de seguridad o herramientas de remediación, hasta que se solucionen las deficiencias. Las acciones de remediación también pueden incluir el aislamiento de la estación de trabajo, el bloqueo de acceso a aplicaciones críticas, o la activación de un proceso de (MFA para verificar la identidad del usuario). Además, se pueden implementar medidas de “coaching” para informar al usuario sobre la necesidad de cumplir con las políticas de seguridad y cómo corregir cualquier incumplimiento.

La Tabla 13 detalla las políticas de remediación y acciones correctivas recomendadas para la protección de sistemas.

Tabla 13. Descripción de Políticas de Remediación y Acciones Correctivas

Políticas de Remediación y Acciones Correctivas	**Descripción**
Aislamiento de la Estación	Si un dispositivo es detectado con una vulnerabilidad crítica o sin los parches necesarios, la estación puede ser automáticamente aislada del resto de la red, permitiendo solo el acceso a servidores de parcheo y actualización.
Bloqueo de Acceso a Aplicaciones	Si un usuario intenta acceder a aplicaciones sensibles desde un dispositivo que no cumple con las políticas de seguridad, se puede bloquear su acceso a esas aplicaciones hasta que se resuelvan las deficiencias.
Reto al Usuario (MFA)	En caso de detectar un comportamiento sospechoso o un acceso desde un dispositivo que acaba de salir de cuarentena, se puede exigir al usuario que se autentique nuevamente utilizando MFA antes de permitirle el acceso a los recursos.
Coaching del Usuario	Si un dispositivo no cumple con una política de seguridad debido a una acción del usuario, como la instalación de una aplicación no aprobada, se podría enviar automáticamente una sesión de "coaching" que explique al usuario la política y cómo corregir el problema.

Para maximizar la efectividad de las políticas de seguridad adaptativas y basadas en el riesgo, se propone integrar motores de evaluación de riesgo/confianza en la infraestructura de seguridad de las instituciones financieras. Estos motores evaluarán en tiempo real cada solicitud de acceso, determinando el nivel de riesgo asociado. Cuando se detecta un riesgo elevado, por ejemplo, un intento de acceso desde una ubicación inusual o un dispositivo desconocido, el motor de riesgo debe activar medidas adicionales de seguridad. Estas medidas pueden incluir la solicitud de MFA adicional o una revisión manual de la solicitud antes de permitir el acceso. Este enfoque permite ajustar las políticas de seguridad de forma dinámica, adaptándose a amenazas específicas sin afectar la eficiencia operativa.

Adicionalmente, es crucial establecer un proceso sistemático de revisión y actualización de las políticas de seguridad. Esto incluye la realización de auditorías internas periódicas para evaluar la efectividad de las políticas y la implementación de herramientas de análisis en tiempo real para detectar y corregir cualquier brecha en las políticas existentes. La revisión continua de las políticas asegura que estas permanezcan alineadas con las amenazas emergentes y los cambios en las operaciones de la institución.

Este enfoque metodológico asegura la protección continua de los activos críticos en un entorno de seguridad dinámico y en constante evolución.

Paso 8: Definición de Reglas

En este paso de la metodología para el sector financiero colombiano, es relevante destacar que las configuraciones aquí definidas no son exhaustivas y pueden ampliarse o adaptarse según el apetito de riesgo y las políticas específicas de cada organización. A continuación, se detallan las reglas de configuración, las acciones recomendadas y los beneficios asociados, los cuales están diseñados para abordar de manera efectiva los riesgos identificados en las etapas iniciales de la metodología (Tabla 14).

Tabla 14. Reglas de Configuración

	Verificación postura dispositivo	**Bloqueo de descarga archivos maliciosos**	**Inspección de tráfico web y SSL**	**Aislamiento automático de dispositivos comprometidos**	**Autenticación MFA para acceso seguro**	**Control de acceso basado en riesgo**	**Control de carga de archivo a la nube**	**Validación continua de la postura de la seguridad**
Reglas para riesgos vinculados con amenaza malware	**Configurar:** Política para que permita acceso solo a dispositivos que cumplen con ciertos criterios de seguridad; ejemplo, tener un antivirus actualizado y activo. **Acciones:** Bloquear o restringir los dispositivos que no cumplan con estos requisitos. **Beneficio:** Esto reduce la posibilidad de que dispositivos vulnerables o comprometidos introduzcan malware.	**Configurar:** Política para inspeccionar los archivos que los usuarios intenten descargar, buscando extensiones de archivo específicas como .exe, .zip, o archivos sospechosos según la clasificación de malware de Netskope. **Acciones:** Bloquear o restringir los dispositivos que no cumplan con estos requisitos. **Beneficio:** Al bloquear la descarga de archivos potencialmente peligrosos (como ejecutables y archivos comprimidos),	**Configurar:** Políticas que inspeccionen el tráfico web en busca de malware, basadas en la categoría "Threat Protection". **Acciones:** Bloquear automáticamente la descarga de archivos maliciosos o la comunicación con sitios conocidos por hospedar malware. **Beneficio:** La inspección del tráfico web en tiempo real te permite detectar y bloquear conexiones a sitios maliciosos que pueden distribuir malware o actuar como comandos y control (C2) para infecciones existentes.	**Configurar:** Política para aislar cualquier dispositivo que presente comportamiento sospechoso, como conexiones no habituales a servidores externos o descargas de archivos no autorizados. **Acciones:** Bloquear o aislar los dispositivos que no cumplan con estos requisitos. **Beneficio:** Si un dispositivo muestra signos de estar comprometido (comportamiento anómalo o conexiones sospechosas), se aísla automáticamente, evitando que el malware se	**Configurar:** Política para requerir MFA cada vez que los usuarios accedan a recursos críticos o aplicaciones SaaS importantes. **Acciones:** Bloquear o solicita MFA para acceso a aplicaciones que no soliciten MFA. **Beneficio:** Requerir MFA protege contra el uso no autorizado de credenciales robadas, que a menudo es una táctica utilizada por los actores de malware para infiltrarse en las redes y sistemas.	**Configurar:** Política para que, si el riesgo supera un umbral definido, se deniegue el acceso o se restrinja. Usar **Risk Score** de la solución. **Acciones:** Bloquear o restringir el acceso para usuarios con un riesgo elevado. **Beneficio:** Esta regla ajusta dinámicamente los niveles de acceso según el nivel de riesgo del usuario o dispositivo. Si se detectan comportamientos sospechosos, el acceso se limita, reduciendo el riesgo de propagación de malware.	**Configurar:** Política para inspeccionar el contenido y tipo de archivo **Acciones:** Bloquear los archivos maliciosos o no permitidos por tu estrategia de DLP. **Beneficio:** Evitar que dispositivos comprometidos suban archivos maliciosos a la nube ayuda a prevenir la distribución de malware a través de plataformas de almacenamiento en la nube como también el riesgo de fuga de información.	**Configurar:** Política para que se valide continuamente la postura de seguridad del dispositivo, como la presencia de actualizaciones de seguridad, software antimalware, etc.. **Acciones:** Terminar una sesión o restringir el acceso si el dispositivo deja de cumplir con la postura. **Beneficio:** Monitorear continuamente la postura de seguridad del dispositivo garantiza que si un dispositivo pierde su nivel de protección durante una sesión (por ejemplo, desactivando el antimalware), se revoca el acceso, previniendo posibles infecciones.

		evitas que el malware se descargue e infecte dispositivos de la red.		propague a otras partes de la red.				
	Autenticación Multifactor	**Control de Acceso Basado en Riesgo**	**Verificación de Comportamientos Anómalos**	**Control por Ubicación Geográfica**	**Validación continua de la postura de la seguridad**	**Revalidación de Autenticación Durante la Sesión**	**Control de Sesión y Tiempo de Expiración**	
Reglas para riesgos vinculados con amenaza Suplantación de identidad	**Configurar:** Integrar el ZTNA con el proveedor de MFA (OKTA, AZure AD o Google Authenticator) y luego política para que, antes de conceder acceso a aplicaciones críticas o datos sensibles, los usuarios deban autenticarse con MFA. **Acciones:** Seleccionar "solicitar MFA" en las opciones de acción para que sea obligatorio. **Beneficio:** Protege contra el uso de credenciales robadas al	**Configurar:** Política para que se restrinja el acceso si el **Risk Score** es alto, lo que podría indicar un intento de suplantación (por ejemplo, debido a inicios de sesión inusuales desde ubicaciones o dispositivos sospechosos).. Nota: Usar **Risk Score** de la solución. **Acciones:** Bloquear o restringir el acceso para usuarios con un riesgo alto. **Beneficio:** Permite bloquear o restringir el acceso si el	**Configurar:** Política para monitorear actividades inusuales, como múltiples intentos fallidos de inicio de sesión o intentos de acceso desde ubicaciones geográficas inusuales. **Acciones:** Bloquear para detener estos intentos de acceso desde ubicaciones geográficas inusuales. **Beneficio:** Detectar comportamientos que no son normales para un usuario legítimo puede ayudar a bloquear accesos fraudulentos antes de que el daño ocurra.	**Configurar:** Política para restringir o bloquear el acceso desde ciertas ubicaciones geográficas, por ejemplo, países donde no operas o de donde no debería haber actividad legítima. **Acciones:** Bloquear ubicaciones no autorizadas o sospechosas. **Beneficio:** Al limitar el acceso desde ubicaciones donde no debería haber tráfico legítimo, reduces la posibilidad de que atacantes externos intenten acceder a las cuentas de los usuarios mediante	**Configurar:** Política que valide continuamente la postura de seguridad del dispositivo, como la presencia de actualizaciones de seguridad, software antimalware, etc.. **Acciones:** Terminar una sesión, restringir el acceso o bloquear si el dispositivo deja de cumplir con la postura. **Beneficio:** Monitorear continuamente la postura ayuda a que, si un dispositivo pierde su nivel de protección durante una sesión, se revoca el acceso.	**Configurar:** Política para forzar una nueva verificación de identidad o MFA si se detectan cambios sospechosos durante la sesión, como una IP diferente o un comportamiento inusual. **Acciones:** Seleccionar "solicitar MFA" en las opciones de acción o terminar la sesión. **Beneficio:** Ayuda a cortar el acceso si un atacante toma el control de una sesión legítima.	**Configurar:** Política para finalizar sesiones automáticamente después de un tiempo predeterminado o si se detectan múltiples inicios de sesión en un corto periodo. **Acciones:** Terminar la sesión que está abierta. **Beneficio:** Limitar el tiempo que un atacante puede explotar una cuenta si logra acceder.	

	requerir una segunda forma de verificación, asegurando que solo el usuario legítimo pueda acceder, incluso si el atacante tiene la contraseña.	sistema detecta un riesgo alto, evitando que atacantes con comportamiento sospechoso accedan a la red.		la suplantación de identidad.				
	Autenticación Multifactor	**Validación continua de la postura de la seguridad**	**Control por Ubicación Geográfica**	**Control de Acceso Basado en la Identidad del Usuario**	**Control de Sesión y Tiempo de Expiración**	**Verificación de Comportamientos Anómalos**	**Revalidación de Autenticación Durante la Sesión**	
Reglas para riesgos vinculados con amenaza acceso no autorizado	**Configurar:** Integrar el ZTNA con el proveedor de MFA (OKTA, AZure AD o Google Authenticator,..) y luego política para que, antes de conceder acceso a aplicaciones críticas o datos sensibles, los usuarios deban autenticarse con MFA. **Acciones:** Seleccionar "solicitar MFA" en las opciones de acción para que sea obligatorio. **Beneficio:**	**Configurar:** Política que valide continuamente la postura de seguridad del dispositivo, como la presencia de actualizaciones de seguridad, software antimalware, etc.. **Acciones:** Terminar una sesión, restringir el acceso o bloquear si el dispositivo deja de cumplir con la postura. **Beneficio:** Monitorear continuamente la postura ayuda	**Configurar:** Política para restringir o bloquear el acceso desde ciertas ubicaciones geográficas, por ejemplo, países donde no operas o de donde no debería haber actividad legítima. **Acciones:** Bloquear ubicaciones no autorizadas o sospechosas. **Beneficio:** Al limitar el acceso desde ubicaciones donde no debería haber tráfico legítimo, reduces la posibilidad de que atacantes externos intenten	**Configurar:** Política para restringir o permitir acceso solo a usuarios con los roles apropiados, de acuerdo a los perfiles definidos en tu Active Directory o LDAP. **Acciones:** Bloquear o restringir el acceso a cualquier perfil distinto a los autorizados. **Beneficio:** Controlar el acceso según la identidad del usuario permite garantizar que solo los empleados con los permisos	**Configurar:** Política para finalizar sesiones automáticamente después de un tiempo predeterminado o si se detectan múltiples inicios de sesión en un corto periodo. **Acciones:** Terminar la sesión que está abierta. **Beneficio:** Limitar la duración de las sesiones y forzar el cierre de sesiones inactivas previene que usuarios no autorizados tomen el control de sesiones activas, lo que minimiza riesgos de accesos no autorizados.	**Configurar:** Política para monitorear actividades inusuales, como múltiples intentos fallidos de inicio de sesión o intentos de acceso desde ubicaciones geográficas inusuales. **Acciones:** Bloquear para detener estos intentos de acceso desde ubicaciones geográficas inusuales. **Beneficio:** Detectar comportamientos fuera de lo habitual permite bloquear intentos de acceso no	**Configurar:** Política para forzar una nueva verificación de identidad o MFA si se detectan cambios sospechosos durante la sesión, como una IP diferente o un comportamiento inusual. **Acciones:** Seleccionar "solicitar MFA" en las opciones de acción o terminar la sesión. **Beneficio:** Si un atacante logra acceder a una sesión legítima, la revalidación continua evita que mantenga acceso, obligando a un	

	Protege contra el uso de credenciales robadas al requerir una segunda forma de verificación, asegurando que solo el usuario legítimo pueda acceder, incluso si el atacante tiene la contraseña.	a que si un dispositivo pierde su nivel de protección durante una sesión, se revoca el acceso.	acceder a las cuentas de los usuarios mediante la suplantación de identidad.	adecuados puedan acceder a aplicaciones específicas, lo que reduce el riesgo de acceso no autorizado.		autorizado que pueden resultar de cuentas comprometidas o suplantación de identidad.	nuevo proceso de autenticación si se detectan cambios.	
Reglas para riesgos vinculados con amenaza movimiento lateral	**Segmentación de la Red**	**Control de Acceso Basado en la Identidad del Usuario**	**Validación continua de la postura de la seguridad**	**Revalidación de Autenticación Durante la Sesión**	**Política de Zonas de Confianza**	**Verificación de Comportamientos Anómalos**	**Control de Sesión y Tiempo de Expiración**	**Monitoreo y Control de Tráfico Interno (Este-Oeste)**
	Configurar: Política que limite el acceso de los usuarios a segmentos específicos de la red basados en su rol o función y bloquear el acceso a otros segmentos de la red no asignados al usuario. **Acciones:** Bloquear o restringir a los usuarios que quieran acceder a segmentos de red no autorizados.	**Configurar:** Política para restringir o permitir acceso solo a usuarios con los roles apropiados, de acuerdo a los perfiles definidos en tu Active Directory o LDAP. **Acciones:** Bloquear o restringir el acceso a cualquier perfil distinto a los autorizados. **Beneficio:** Controlar el acceso según la	**Configurar:** Política que valide continuamente la postura de seguridad del dispositivo, como la presencia de actualizaciones de seguridad, software antimalware, etc.. **Acciones:** Terminar una sesión, restringir el acceso o bloquear si el dispositivo deja de cumplir con la postura. **Beneficio:** Monitorear continuamente la	**Configurar:** Política para forzar una nueva verificación de identidad o MFA si se detectan cambios sospechosos durante la sesión, como una IP diferente o un comportamiento inusual. **Acciones:** Seleccionar "solicitar MFA" en las opciones de acción o terminar la sesión. **Beneficio:** Si un atacante logra acceder a una	**Configurar:** Políticas que asignen usuarios y aplicaciones a zonas de confianza específicas y política para que los usuarios dentro de una zona no puedan acceder a otras zonas sin pasar por un proceso de autenticación y revisión de permisos. **Acciones:** Bloquear cualquier intento de acceso cruzado entre zonas sin autorización.	**Configurar:** Política para monitorear actividades inusuales, como múltiples intentos fallidos de inicio de sesión o intentos de acceso desde ubicaciones geográficas inusuales. **Acciones:** Bloquear para detener estos intentos de acceso desde ubicaciones geográficas inusuales. **Beneficio:** Detectar comportamientos	**Configurar:** Política para finalizar sesiones automáticamente después de un tiempo predeterminado o si se detectan múltiples inicios de sesión en un corto periodo. **Acciones:** Terminar la sesión que está abierta. **Beneficio:** Limitar la duración de las sesiones y forzar el cierre de sesiones inactivas previene que usuarios no autorizados tomen el control de	**Configurar:** Políticas que monitoreen el tráfico entre aplicaciones y servicios internos dentro de la red (tráfico este-oeste) para alertar o bloquear tráfico inusual entre servidores o segmentos de red que normalmente no se comunican entre sí. **Acciones:** Alertar o bloquear el tráfico sospechoso. **Beneficio:** Monitorear el tráfico interno entre aplicaciones y servidores evita que un atacante mueva datos o se desplace lateralmente dentro de la red sin ser detectado.

	Beneficio: Al segmentar la red, limitas la capacidad del atacante de moverse lateralmente entre diferentes servidores o aplicaciones. Esto asegura que si comprometen un área de la red, no puedan moverse a otra	identidad del usuario permite garantizar que solo los empleados con los permisos adecuados puedan acceder a aplicaciones específicas, lo que reduce el riesgo de acceso no autorizado.	postura ayuda a que si un dispositivo pierde su nivel de protección durante una sesión, se revoca el acceso.	sesión legítima, la revalidación continua evita que mantenga acceso, obligando a un nuevo proceso de autenticación si se detectan cambios.	**Beneficio:** Las zonas de confianza limitan el movimiento lateral al dividir la red en segmentos aislados que requieren una validación adicional para moverse de una a otra.	fuera de lo habitual permite bloquear intentos de acceso no autorizado que pueden resultar de cuentas comprometidas o suplantación de identidad.	sesiones activas, lo que minimiza riesgos de accesos no autorizados.	

Paso 9: Detección y Respuesta a Amenazas

En la estrategia de ZTNA, la detección y respuesta a amenazas (TDDR) es fundamental, especialmente en el sector financiero, donde las brechas de seguridad pueden tener consecuencias severas. Para implementar esta estrategia de manera efectiva, se sugiere la adopción de un enfoque metodológico que incluya varias etapas clave.

Primero, es esencial integrar inteligencia de amenazas en la ZTNA. Este componente debe incluir una variedad de fuentes de datos, tales como feeds globales de amenazas, datos históricos de incidentes y análisis en tiempo real de patrones de tráfico. La inteligencia de amenazas permitirá la identificación y bloqueo de tráfico malicioso en el borde de la red antes de que acceda a los sistemas internos. Por lo tanto, la integración de esta inteligencia debe mejorar la capacidad de la organización para anticipar y neutralizar ataques potenciales, adaptándose proactivamente a nuevas vulnerabilidades.

En segundo lugar, se debe implementar un sistema de Monitoreo de la Actividad del Usuario (UAM). Este sistema debe permitir la vigilancia continua de las actividades de los usuarios para detectar comportamientos que puedan indicar amenazas internas o compromisos de cuentas. El monitoreo debe incluir la identificación de accesos en horarios inusuales, intentos repetidos de exfiltración de datos y accesos no autorizados a sistemas sensibles. Basado en los patrones sospechosos detectados, el sistema tendrá la capacidad de activar medidas preventivas, tales como el bloqueo temporal de cuentas, la solicitud de MFA adicional o la generación de alertas para el equipo de seguridad. Estas medidas aseguran una respuesta inmediata y efectiva ante posibles amenazas.

Finalmente, es crucial desarrollar y mantener un plan integral de respuesta a incidentes. Este plan debe definir claramente los procedimientos a seguir en caso de una violación de seguridad, incluyendo la contención del incidente, la erradicación de la amenaza, la recuperación de los sistemas afectados y la comunicación con las partes interesadas. El plan debe detallar protocolos específicos para diferentes tipos de incidentes, como infecciones de malware, intentos de exfiltración de datos y accesos no autorizados a sistemas críticos. Además, debe ser probado y actualizado regularmente para garantizar su efectividad frente a amenazas emergentes, asegurando que el equipo de seguridad esté preparado para ejecutar las acciones necesarias de manera oportuna y eficaz.

Con este enfoque metodológico, la combinación de herramientas EDR, inteligencia de amenazas, monitoreo de la actividad del usuario y un plan de respuesta a incidentes proporciona a las instituciones financieras en Colombia una capacidad avanzada para detectar, responder y mitigar amenazas en tiempo real. Esta integración fortalece la defensa de la red y minimiza el impacto de los incidentes de seguridad, garantizando la protección continua de los activos críticos y manteniendo la resiliencia operativa en un entorno de amenazas en constante evolución.

Paso 10: Registro y Auditoría

La configuración de un sistema de registro centralizado es una parte fundamental de la implementación de ZT en una institución financiera. Por lo tanto, este sistema debe ser configurado para integrar todos los dispositivos de red y soluciones ZTNA, asegurando que cada uno envíe registros al servidor centralizado. La primera fase en este proceso implica la configuración de los dispositivos y aplicaciones para que dirijan sus logs al servidor de registro, asegurando que toda la actividad relevante se capture en un solo punto.

Para fortalecer la capacidad de monitoreo y detección de amenazas, es esencial incorporar herramientas avanzadas como SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response) y CASB (Cloud Access Security Broker). Un SIEM permite recopilar, analizar y correlacionar eventos de seguridad en tiempo real, ayudando a detectar patrones anómalos y posibles ataques de manera temprana. Complementariamente, un SOAR automatiza la respuesta ante incidentes al integrar diferentes herramientas de seguridad, reduciendo el tiempo de reacción y mejorando la eficiencia del equipo de ciberseguridad. Por su parte, un CASB añade una capa de protección adicional al monitorear y controlar el acceso a servicios en la nube, asegurando que las políticas de seguridad se apliquen de manera uniforme y que las amenazas en entornos cloud sean identificadas y mitigadas rápidamente. La integración de estas soluciones con un enfoque de Zero Trust permite una vigilancia continua y una respuesta más ágil frente a los riesgos emergentes.

A continuación, se deben establecer y documentar las políticas de retención de registros, de acuerdo con los requisitos normativos como la Circular 004 de 2019 de la Superintendencia Financiera de Colombia. Estas políticas deben especificar el tiempo durante el cual los registros deben ser almacenados, facilitando tanto el cumplimiento regulatorio como las investigaciones en caso de incidentes. Implementar un sistema de gestión automatizado para la retención y eliminación de registros ayudará a garantizar que los datos se gestionen de manera efectiva y conforme a las normativas.

Para el análisis de los registros, se deben desplegar herramientas especializadas que permitan identificar patrones sospechosos y correlacionar eventos de seguridad. Estas herramientas deben ser configuradas para emitir alertas en tiempo real ante la detección de actividades inusuales y para generar informes detallados que apoyen la gestión de la seguridad. La capacidad de estas herramientas para analizar datos de forma integral y en tiempo real es crucial para la identificación temprana de amenazas.

Además, es necesario establecer un protocolo de auditoría regular de los registros. Las auditorías deben ser realizadas periódicamente, tanto internamente como por auditores externos, para revisar la integridad y exactitud de los registros, así como la correcta aplicación de las políticas de seguridad. El protocolo de auditoría debe incluir pasos detallados para la revisión de los registros, la identificación de brechas de seguridad y la generación de recomendaciones para la mejora de las políticas y procedimientos.

Finalmente, se debe implementar un ciclo de mejora continua en el manejo de los registros. Este ciclo implica la revisión y actualización regular de las políticas de retención y análisis de registros, así como la evaluación y mejora de las herramientas utilizadas para la auditoría. La incorporación de retroalimentación y la adaptación a nuevas amenazas son esenciales para mantener la eficacia del sistema de registro y la postura de seguridad de la institución.

Con estos pasos metodológicos, se asegura una gestión eficaz de los registros de seguridad, el cumplimiento con las regulaciones aplicables y el fortalecimiento de la defensa contra amenazas en un entorno de ciberseguridad en constante cambio.

2.4 Metodología y resultados FASE 4

2.4.1 Metodología FASE 4

Para alcanzar el objetivo específico “validar la metodología propuesta”, se implementaron pruebas en un ambiente controlado que incluyeron simulaciones de diferentes escenarios de riesgo. Estos escenarios fueron diseñados para abordar algunos de los riesgos ya identificados en la fase 2 y que están asociados con acceso no autorizado, suplantación de identidad y ataques de comando y control (malware). El proceso metodológico incluyó la configuración de un ambiente de prueba haciendo uso de Netskope (solución más destacada de acuerdo con la matriz multicriterio), el análisis comparativo de resultados antes y después de aplicar la metodología y la actualización de la matriz de riesgo para evaluar la reducción de amenazas en el sector financiero de Colombia.

Acorde a lo anterior, se realizaron 3 escenarios asociados a ataques informáticos; es importante resaltar que se realizó una selección cuidadosa de aquellos que permitieran evaluar el modelo sin comprometer la estabilidad del entorno y se descartaron amenazas de alto impacto, como el ransomware, debido al riesgo de que la simulación pudiera salirse de control y generar efectos no deseados en el ambiente de prueba.

- Escenario 1: Acceso no autorizado
- Escenario 2: Suplantación de identidad
- Escenario 3: Malware

A continuación, se detalla cada uno de ellos.

- **Escenario 1: Acceso No Autorizado**

Se configuró un entorno aislado utilizando una máquina virtual ubicada en un VPC de AWS, configurada con políticas restrictivas de acceso en su *security group*. Solo se permitió el acceso desde conectores específicos denominados *Publishers* de Netskope, que establecen una conexión saliente hacia la nube, evitando la exposición directa del servicio de escritorio remoto a internet.

Desde el lado del consumidor, un agente instalado en la máquina remota capturó el tráfico hacia el servicio de escritorio remoto, redirigiéndolo a la nube de Netskope de forma transparente. Se

demostró que, en ausencia del agente, no se podía establecer la conexión con el servicio remoto, mientras que su instalación permitió el acceso controlado. Este enfoque eliminó la necesidad de asignar direcciones IP públicas a las máquinas, garantizando la seguridad del acceso.

- **Escenario 2: Suplantación de Identidad**

Se implementó una clasificación de dispositivos basada en condiciones predefinidas. Las máquinas administradas (*Corp_Devices*) fueron identificadas por la presencia de un antimalware (Falcon) y el sistema operativo Sonoma (MacOS). Las máquinas que no cumplieron estas condiciones fueron clasificadas como no administradas (*Unmanaged*).

Para validar este escenario, se configuró un usuario interno con permisos específicos y se intentó acceder desde una máquina de un contratista que no cumplía con las condiciones de seguridad. Aunque la máquina del contratista poseía las credenciales del usuario interno, no pudo acceder a las aplicaciones debido a las políticas de control que restringieron el acceso de dispositivos no administrados. Este resultado confirmó la efectividad de los controles en prevenir la suplantación de identidad.

- **Escenario 3: Ataque de Comando y Control (Malware)**

Se simuló un ataque en una estación de trabajo comprometida con malware. Al ejecutarse, el malware reportó información del sistema operativo y detalles de la víctima a una instancia de SharePoint utilizada como servidor de comando y control. Posteriormente, se emitieron instrucciones remotas para desactivar un proceso de seguridad clave (Falcon) en la máquina afectada.

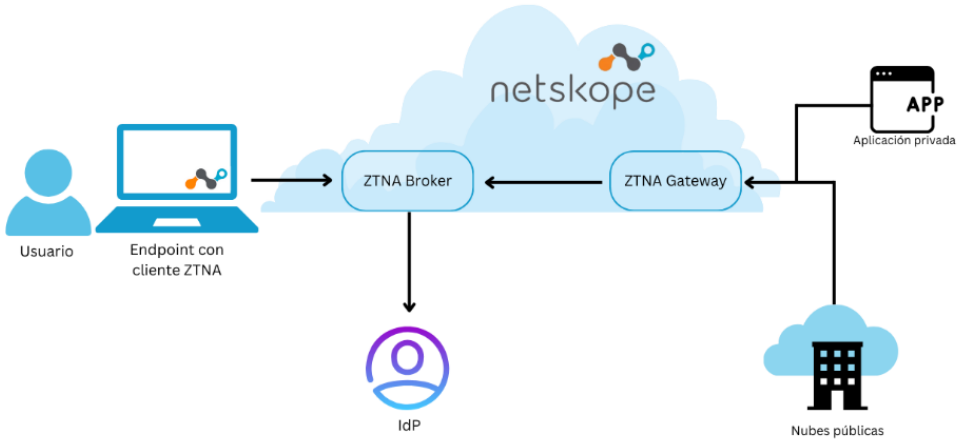
Una vez desactivado el proceso, la máquina fue reclasificada como no administrada debido al incumplimiento de la postura de seguridad establecida. En consecuencia, se restringió el acceso a las aplicaciones corporativas, cumpliendo con las políticas de seguridad definidas. Este escenario permitió evaluar la capacidad de la metodología para mitigar riesgos derivados de ataques de malware.

Los resultados obtenidos en los tres escenarios permiten obtener un comparativo de la matriz de riesgos antes y después de la implementación de la metodología propuesta. Este análisis permitirá determinar si efectivamente se logró una reducción en los niveles de riesgo asociados con los escenarios evaluados. La comparación entre las matrices proporcionará evidencia cuantitativa sobre la efectividad de los controles implementados en un ambiente controlado, permitiendo validar la robustez de la metodología para gestionar riesgos en entornos organizacionales.

2.4.2 Resultados FASE 4

Antes de presentar los resultados de los escenarios evaluados es importante recordar la arquitectura conceptual que sirvió como base para el desarrollo de la metodología (Figura 25).

Figura 25. Arquitectura Conceptual



A continuación, para cada escenario de prueba, se presentará una comparación entre el estado inicial y el resultado posterior a la aplicación de los pasos 5, 6 y 7 de la metodología propuesta en los escenarios de riesgo evaluados.

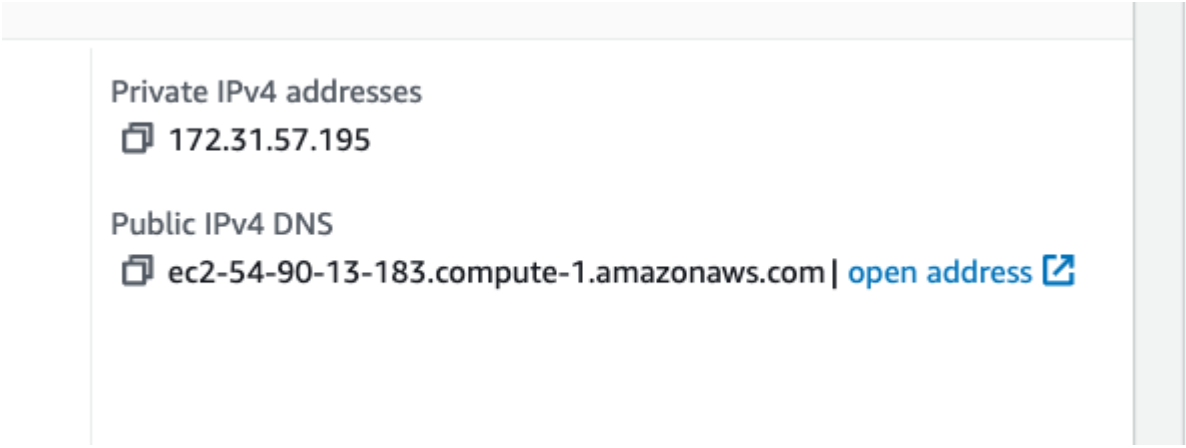
- **Escenario 1. Acceso no autorizado**

Es necesario demostrar que, en ausencia del agente, no era posible establecer la conexión con el servicio remoto, mientras que su instalación habilitaba un acceso controlado.

a) Sin agente y sin configuraciones en las máquinas y herramientas

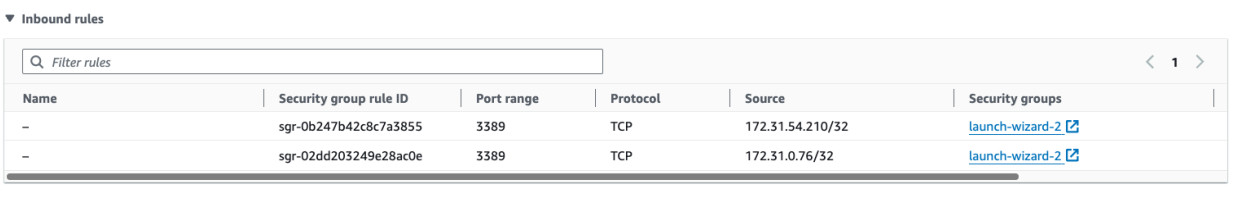
En este escenario, la máquina virtual se encontraba en un ambiente aislado que ofrecía servicios de escritorio remoto. Esta máquina estaba ubicada en un VPC de AWS y asignada a una dirección IP privada específica del entorno, garantizando su aislamiento y control (Figura 26).

Figura 26. Máquina Virtual Asignada a una IP Privada



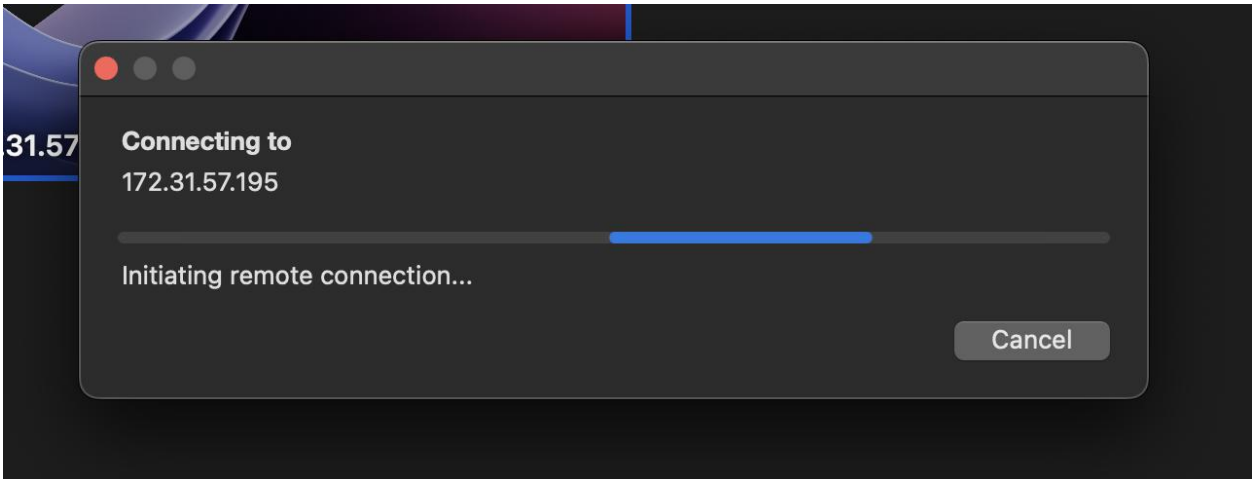
Como se muestra en la Figura 27, la máquina está aislada del exterior mediante políticas de acceso configuradas en su *security group*, las cuales permiten exclusivamente el acceso a la aplicación a través de los conectores instalados dentro del entorno. Esta configuración garantiza un control estricto sobre las conexiones, reforzando la seguridad del ambiente.

Figura 27. Configuración de Políticas de Acceso para el Aislamiento Exterior de la Máquina



Dado que la máquina no tiene el agente instalado y no se lleva a cabo el proceso de autenticación correspondiente, la conexión no puede establecerse, ya que el recurso no está expuesto a Internet. Al intentar acceder, se obtiene el siguiente resultado (Figura 28):

Figura 28. Restricción de Acceso por Falta de Autenticación y Agente



Como se evidencia, en la Figura 28, el sistema permanece intentando establecer la conexión sin éxito. Esto demuestra que, ante una amenaza como el acceso no autorizado, la configuración actual reduce significativamente la probabilidad de que dicha amenaza se materialice.

b) Con agente y con configuraciones en las máquinas y ZTNA

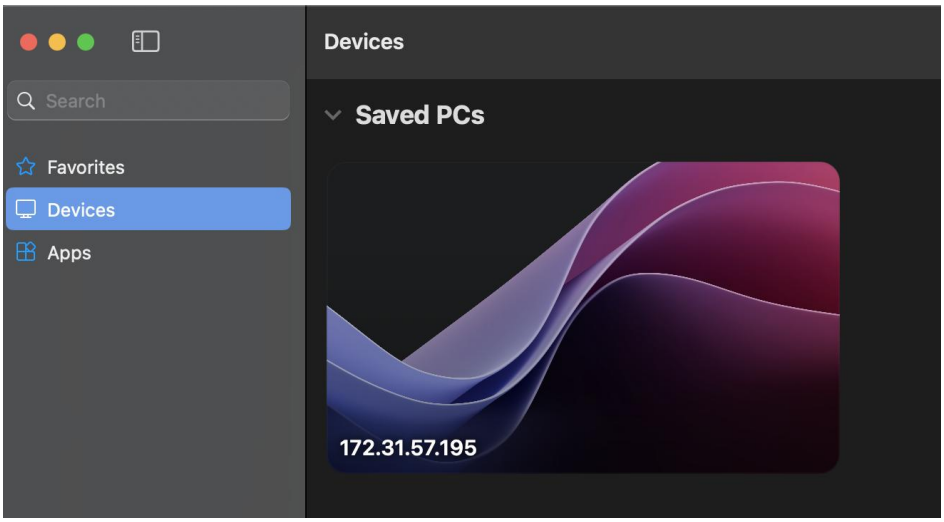
Desde la perspectiva del cliente, la máquina que intenta conectarse al servicio remoto cuenta con un agente instalado que captura el tráfico dirigido hacia dicho servicio y lo redirige de manera transparente a través de la nube del ZTNA. Al ser los *Publishers* máquinas virtuales que establecen conexiones salientes hacia la nube del ZTNA, permiten el tránsito seguro de las sesiones desde la estación MAC hacia el servicio remoto, estación Windows. Esta arquitectura elimina la necesidad de exponer aplicaciones internas a Internet. En este caso, la configuración se aplica específicamente a una máquina que ofrece un servicio de acceso remoto. Para más detalles sobre las configuraciones de este escenario, consultar el Anexo E.

El aspecto más relevante en la protección contra accesos no autorizados es que la máquina remota no necesita obtener una dirección IP dentro del dominio de enrutamiento donde se encuentra la aplicación. Por lo tanto, no puede conectarse directamente a dicha red. La conexión con la aplicación solo es posible a través de la nube del ZTNA utilizando exclusivamente la dirección IP local asignada y su respectivo agente.

Aunque las redes de la aplicación y del cliente están completamente aisladas, la conexión puede establecerse de manera segura mediante la solución ZTNA. A continuación, se presentan los resultados que evidencian este comportamiento:

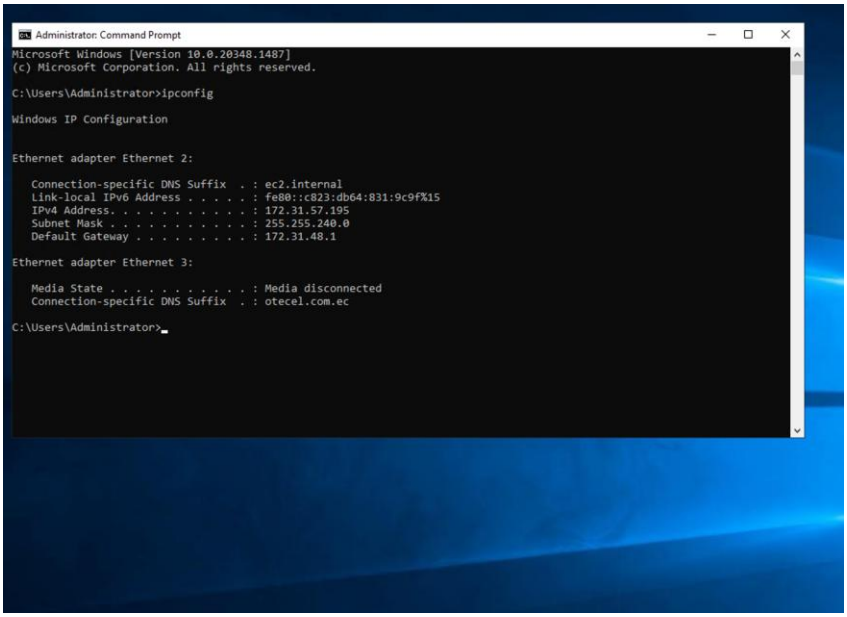
En la Figura 29, el acceso a la máquina Windows, ubicada en la VPC de AWS desde la estación MAC en un segmento de red diferente es exitosa mediante el uso de la solución ZTNA. En este escenario, la máquina Windows no está directamente expuesta a la red pública ni a segmentos de red externos.

Figura 29. Acceso Exitoso con ZTNA entre Segmentos de Red Diferentes



En la Figura 30, se confirma la conexión establecida a la máquina Windows en AWC.

Figura 30. Conexión Establecida a Máquina Windows en AWS



Nota: Se debe tener presente que la dirección IP utilizada para establecer la conexión es la misma asignada a la máquina expuesta en la VPC de AWS.

- **Escenario 2. Suplantación de Identidad - Máquina de un usuario contratista intenta personificar una máquina corporativa al contar con credenciales de un empleado interno**

En este caso, el recurso objetivo es una aplicación a la que un ciberdelincuente intenta acceder, habiendo obtenido previamente las credenciales del usuario legítimo.

El primer paso para mitigar este riesgo fue configurar la declaración de postura de la organización. Según esta configuración, las máquinas administradas (*Corp_Devices*) se identifican mediante dos criterios clave: la presencia de un antimalware específico (Falcon) y el sistema operativo Sonoma (MacOS). Las máquinas que no cumplan con estas condiciones se clasificarán como no administradas (*Unmanaged*), restringiendo automáticamente su acceso a los recursos organizacionales. Esta postura permite que el acceso a las aplicaciones internas esté estrictamente limitado a dispositivos que cumplan con los estándares de seguridad establecidos, reduciendo significativamente el riesgo de accesos no autorizados, incluso si las credenciales del usuario son comprometidas.

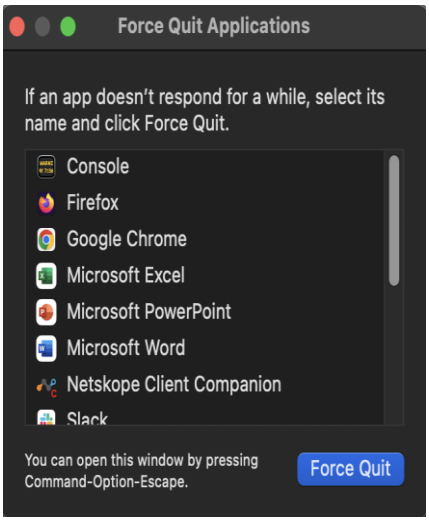
Para más detalles sobre estas configuraciones y su implementación, consulte el Anexo G.

a. Intento de acceso a aplicación sin agente por parte de contratista.

En el escenario de un contratista que intenta suplantar a un usuario interno, su máquina no cumple con las condiciones necesarias para ser reconocida como administrada, ya que no tiene instalado el antimalware corporativo requerido en la estación de trabajo y debe cumplir con el sistema operativo con la versión específica que administra la organización. Por lo tanto, incluso si el contratista posee las credenciales del empleado, no podría acceder al aplicativo debido a las restricciones definidas por las políticas de seguridad.

Como se evidencia en la Figura 31, el contratista no tiene el servicio del antimalware corporativo en ejecución en su estación, confirmando así que su dispositivo no cumple con los requisitos establecidos.

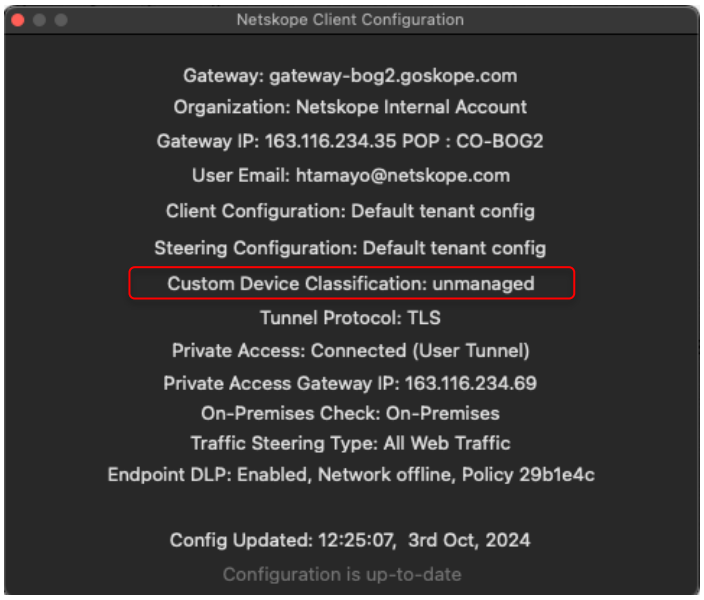
Figura 31. Denegación de Acceso a Contratista por Incumplimiento de Requisitos Corporativos



Aunque se observan varios procesos en ejecución en la máquina, no se encontró el servicio específico llamado *Falcon*. Esto confirma que el antimalware corporativo no está activo en la estación de trabajo del contratista.

A continuación, se presenta la clasificación de este dispositivo en la red, la cual corresponde a *no administrada* (*Unmanaged*), de acuerdo con las políticas de seguridad definidas por la organización (Figura 32). Esta clasificación refuerza la postura de seguridad al restringir el acceso de dispositivos que no cumplen con los requisitos establecidos.

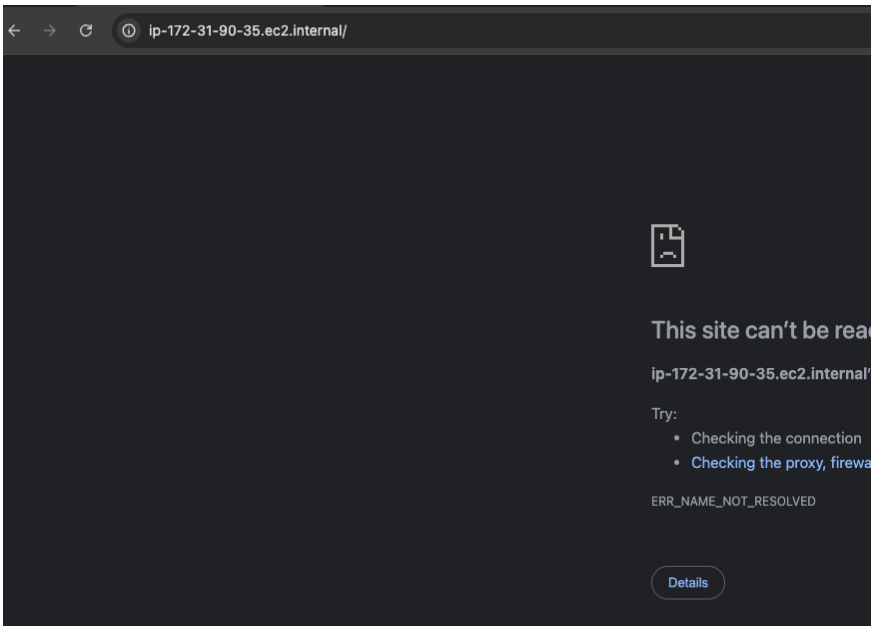
Figura 32. Postura de Seguridad: Dispositivo Clasificado como no Administrado



El resultado esperado es que el sistema niegue el acceso al dispositivo *Unmanaged*, alineándose con las restricciones definidas en la declaración de postura de seguridad de la organización. Como se observa en la Figura 33, la aplicación web de la organización ni siquiera logra cargar, lo que imposibilita cualquier intento de autenticación, incluso si el ciberdelincuente cuenta con las credenciales legítimas del usuario.

Este comportamiento demuestra que las políticas de seguridad aplicadas están funcionando correctamente, ya que los dispositivos clasificados como *Unmanaged* no tienen acceso al recurso, asegurando así que solo los dispositivos que cumplen con las condiciones establecidas puedan interactuar con las aplicaciones corporativas.

Figura 33. Evidencia de Seguridad: Dispositivos No Administrados sin Acceso a Recursos

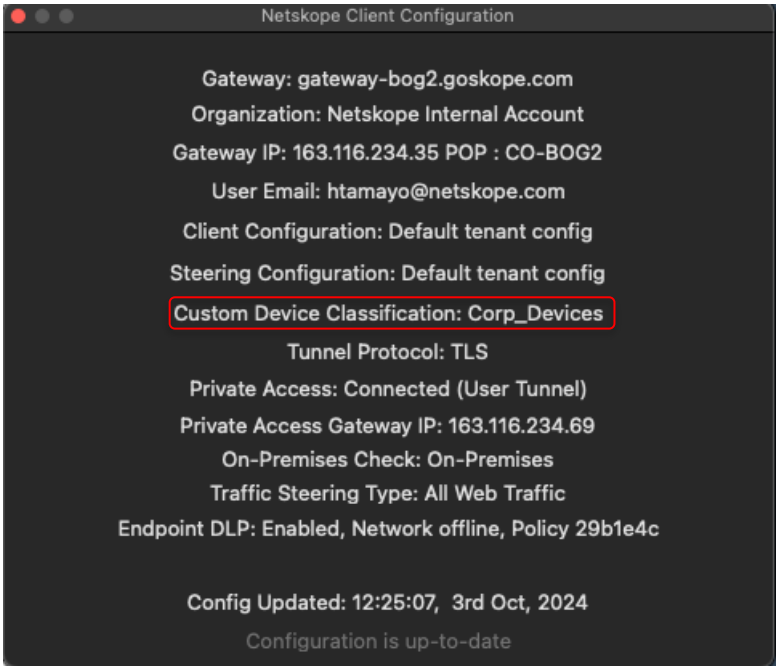


b. Intento de acceso a la aplicación con agente por parte del empleado.

En el escenario de un empleado que desea acceder a su aplicación utilizando una estación de trabajo que cumple con la postura de seguridad parametrizada, el acceso debería ser permitido, ya que el dispositivo satisface las condiciones requeridas.

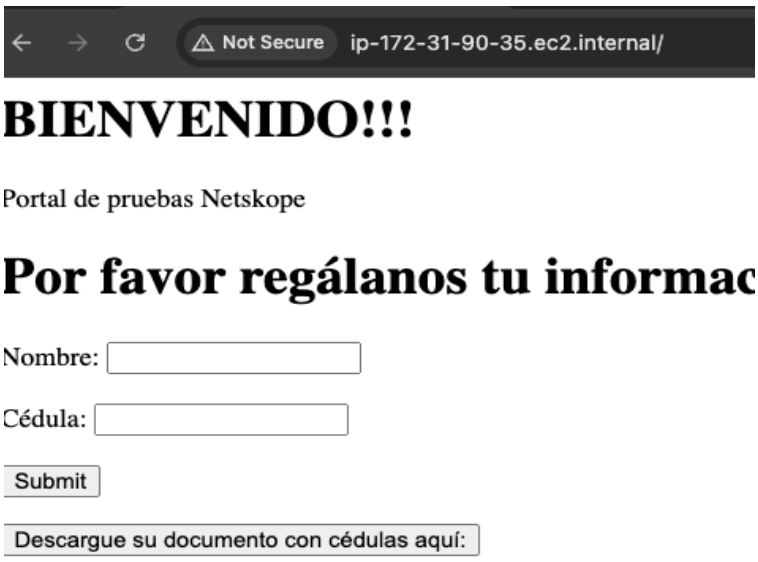
A continuación, se presenta evidencia de que el empleado y su estación de trabajo tienen el antimalware organizacional (*Falcon*) en ejecución. Esto clasifica la estación como un dispositivo administrado (*Corp_Devices*), cumpliendo así con los estándares de seguridad establecidos por la organización (Figura 34).

Figura 34. Cumplimiento de Postura de Seguridad: Evidencia de Dispositivo Administrado



Al satisfacer esta condición, se confirma que la máquina está habilitada para acceder a la aplicación (Figura 35). El acceso controlado demuestra la efectividad de la postura de seguridad parametrizada, garantizando que solo los dispositivos que cumplen con los requisitos puedan interactuar con los recursos corporativos de forma segura y confiable.

Figura 35. Acceso Controlado: Dispositivo Habilitado Según Postura de Seguridad

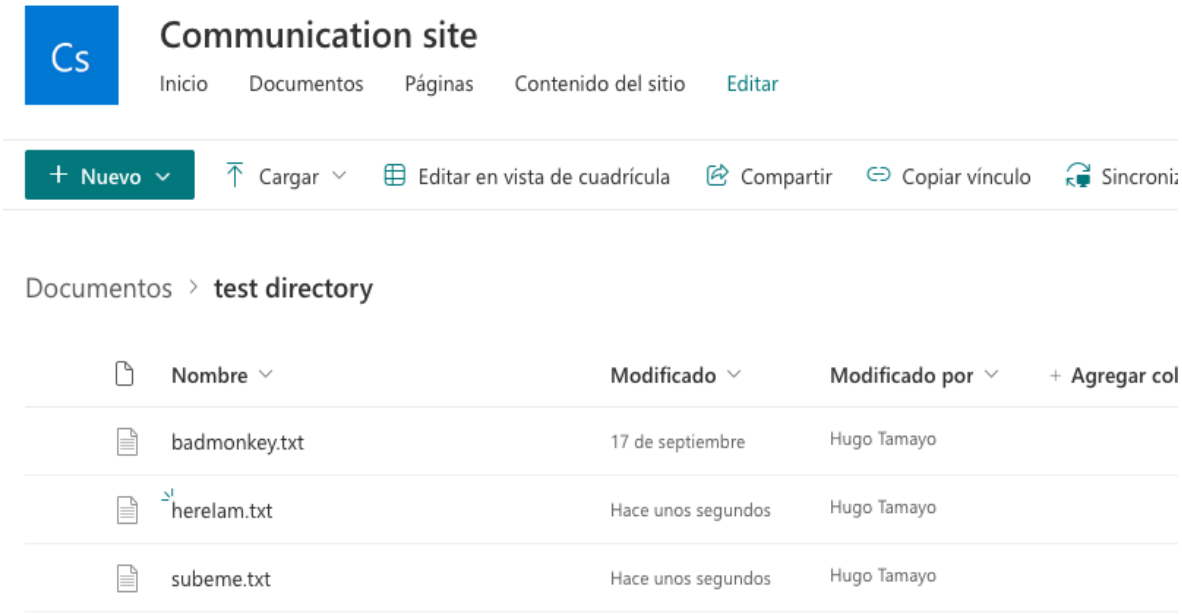


- **Escenario 3 - Ataque de comando y control en la estación**

Se simula el ataque a una estación de trabajo comprometida con malware y al ejecutarse, el malware reportó información del sistema operativo y detalles de la víctima a una instancia de *SharePoint* utilizada como servidor de comando y control. En la Figura 36 se evidencia el *SharePoint* con los documentos

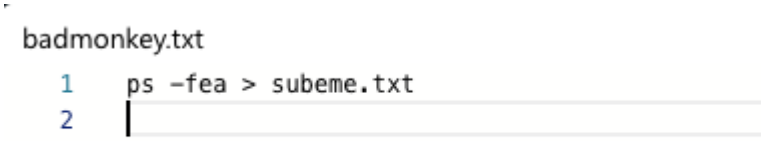
El cliente es comprometido con un malware que le pide al usuario actualizar la máquina para empezar su ejecución. A continuación, se muestra el *SharePoint* con los documentos creados.

Figura 36. Simulación de Ataque con Malware a Estación de Trabajo: Reporte de Información al *SharePoint*



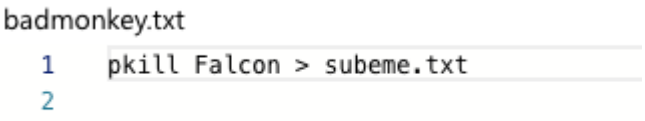
En el *SharePoint* del ciberdelicuente se encuentra un archivo (badmonkey.txt) por medio del cual, se enviaron las solicitudes o los procesos que se deseaba ejecutar en la máquina de la víctima. En este caso, se envió un comando para conocer los procesos que se encontraban en ejecución en la estación de trabajo (Figura 37).

Figura 37. Uso de Badmonkey.txt para Ejecución de Comandos en Máquina Víctima



El resultado de este comando se corrigió en otro archivo, lo que permitió al atacante identificar el software de seguridad en ejecución en el equipo y desactivar uno de los procesos de seguridad en el equipo, en este caso el proceso “Falcon” (Figura 38).

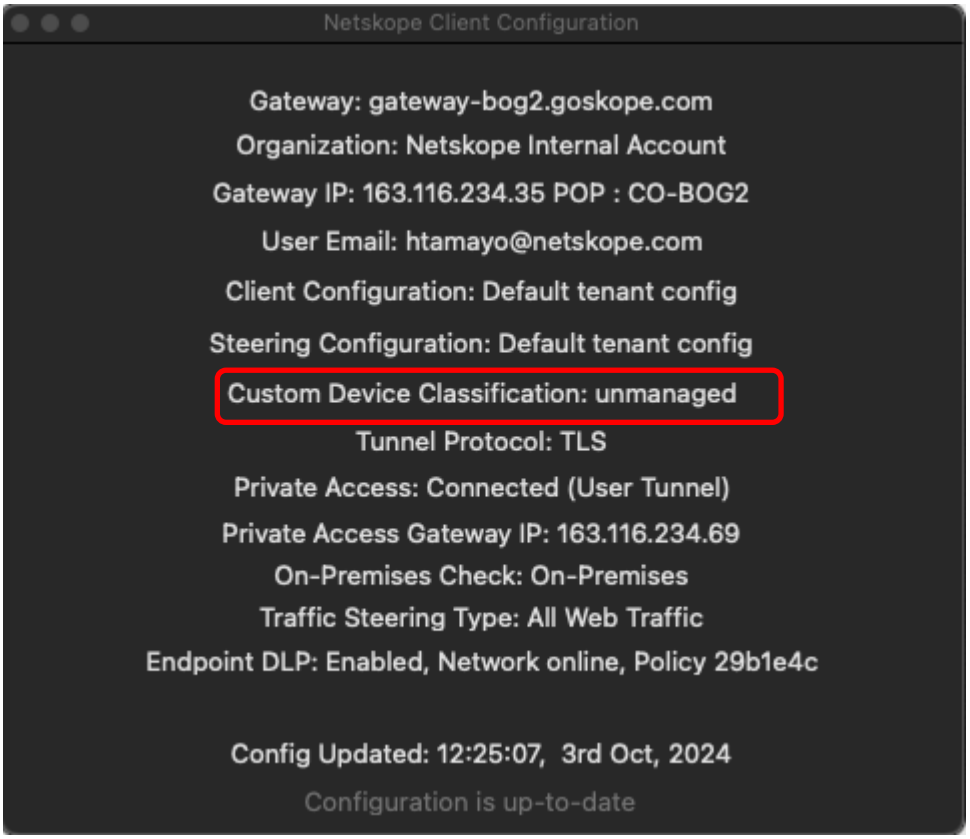
Figura 38. Desactivación del Proceso Falcon Tras Identificación de Software de Seguridad



a) Máquina con agente y no cumple definiciones.

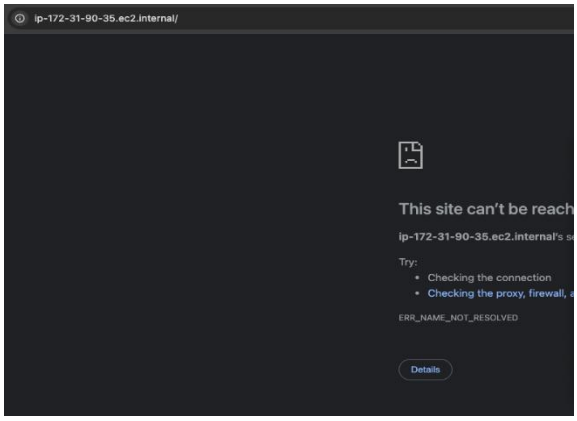
Una vez desactivado el proceso (Falcon), la máquina se reclasificó como no administrada (*unmanaged*) debido al incumplimiento de la postura de seguridad establecida (Figura 39).

Figura 39. Reclasificación de Máquina como No Administrada por Incumplimiento de Postura de Seguridad



Como se muestra en la Figura 40, al hacer la desactivación del proceso de seguridad, la máquina ya no se encuentra en cumplimiento de postura por lo que es clasificada como *Unmanaged*; en consecuencia, se restringe el acceso a la aplicación corporativa, cumpliendo con las políticas de seguridad definidas. Este escenario permite evaluar la capacidad de la metodología para mitigar riesgos derivados de ataques de malware, aclarando que su función no es eliminar el malware sino restringir el acceso a una estación con riesgo a ver la información sensible de una compañía.

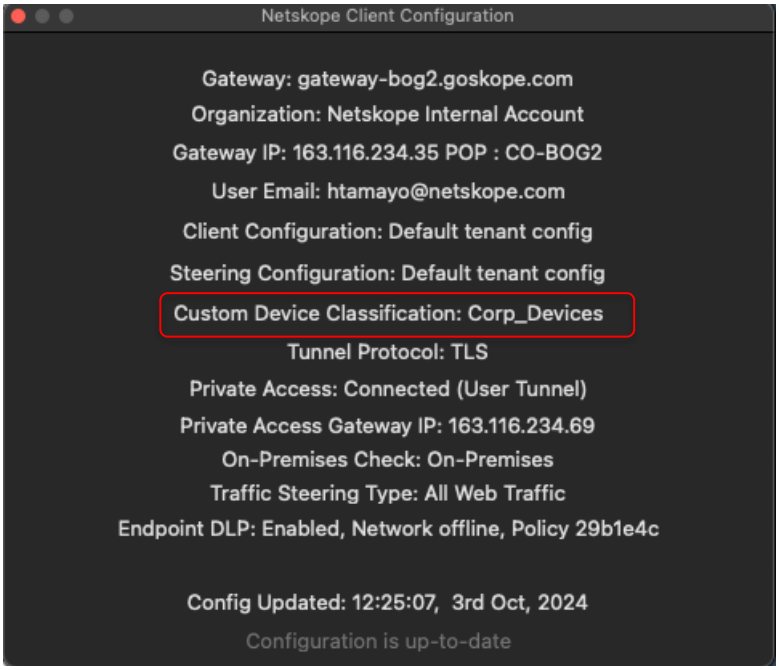
Figura 40. Restricción de Acceso a Aplicación Corporativa por Clasificación No Administrada



b) Máquina con agente y si cumple las definiciones

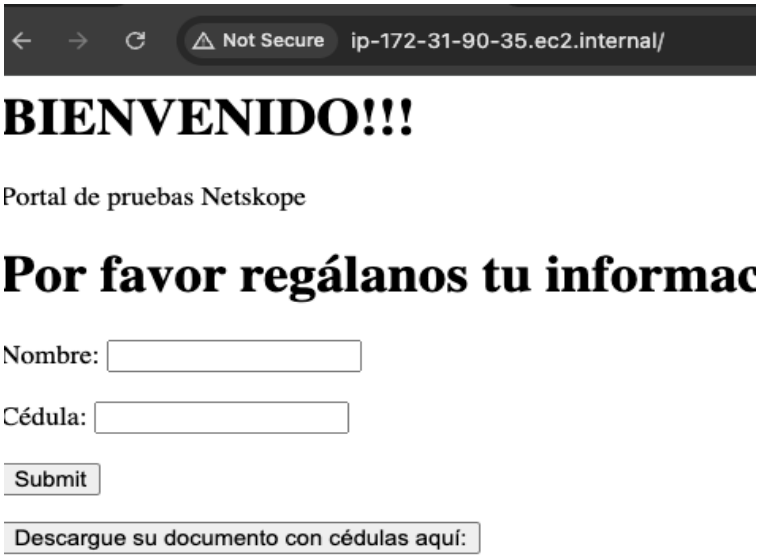
A continuación, se puede evidenciar que la maquina si tiene corriendo el antimalware organizacional (Falcon), por ende clasificó la estación como administrada (*Corp_Devices*) (Figura 41).

Figura 41. Clasificación de Estación como Administrada por Antimalware Activo



Al cumplir con esta condición, se confirma está autorizada para acceder a la aplicación y efectivamente lo realiza, como se muestra en la Figura 42.

Figura 42. Autorización y Acceso Exitoso a la Aplicación tras Cumplimiento de Condiciones de Seguridad



- **Evaluación del riesgo posterior a la implementación de la metodología ZT propuesta**

Tras implementar en un modo controlado la metodología de ZT propuesta, se identificaron un total de 24 riesgos asociados a las redes descritos en la fase 2, cuya probabilidad de ocurrencia varió entre "posible" y "raro", mientras que las consecuencias operativas oscilaron entre "intermedias" y "superiores" (Tabla 15).

Tabla 15. Matriz de Riesgo Fase 4

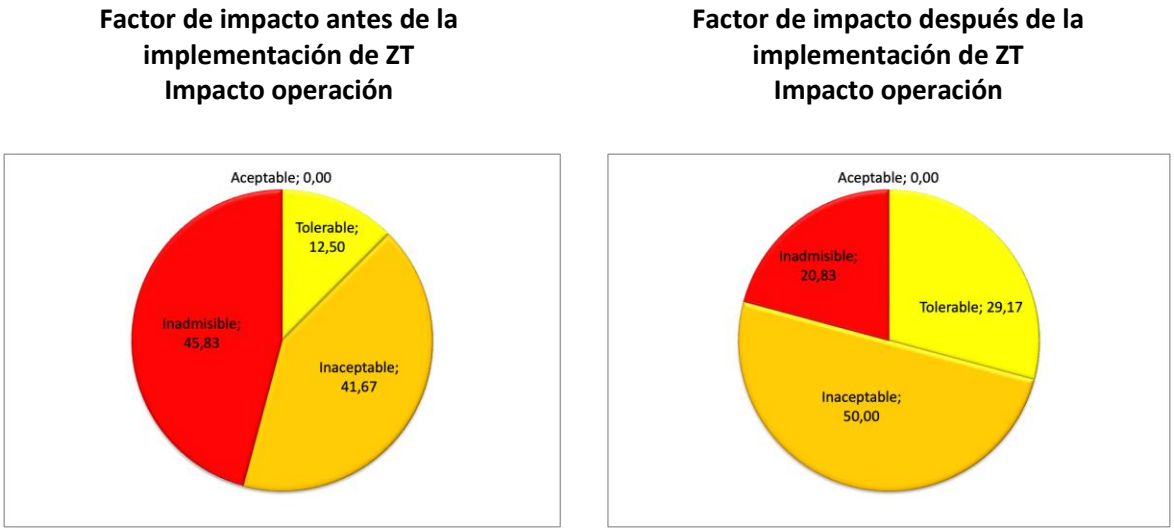
Probabilidad		Consecuencia				
	valor	Insignificante	Menor	Intermedio	Mayor	Superior
		1	2	3	4	5
Casi seguro	5					
Probable	4					
Posible	3			(3) - (4) - (13) - (14) - (17) - (18) -	(1) - (2) - (5) -	(11) - (12) - (15) - (16) - (19) -
Improbable	2			(22) - (23) -		(20) - (21) - (24) -
Raro	1			(8) - (9) - (10) -	(6) - (7) -	

- **Comparación entre la evaluación de riesgos antes y después de la implementación de la metodología de ZT en el sector financiero de Colombia**

En el análisis posterior a la implementación de la metodología ZT, considerando los resultados técnicos implementados, se observó una mejora en la clasificación de los riesgos. En comparación con los resultados previos, la proporción de riesgos inadmisibles disminuyó de manera importante, pasando a representar el 20.83% del total. Simultáneamente, los riesgos inaceptables aumentaron al 50%, indicando una transformación hacia riesgos de menor criticidad en relación con los inadmisibles. Además, la proporción de riesgos tolerables creció hasta alcanzar el 29.17%, evidenciando una mayor capacidad para gestionar y mitigar los riesgos dentro de parámetros controlados (Figura 43).

Este cambio en la distribución refleja la efectividad de la metodología ZT implementada para reducir los riesgos más críticos y redistribuirlos hacia categorías más manejables, aunque aún persiste el desafío de alcanzar niveles de riesgo aceptables.

Figura 43. Comparación de Riesgos Antes y Después de la Implementación de ZT en el Sector Financiero Colombiano



3. Conclusiones, recomendaciones y trabajos futuros

3.1 Conclusiones

La evaluación del contexto operacional del sector financiero colombiano revela un predominio de grandes instituciones, sustentado en ventajas competitivas asociadas a la escala, diversificación de servicios y cumplimiento regulatorio. Este entorno ha favorecido una orientación hacia la banca comercial y la digitalización, con una notable adopción de métodos de pago electrónicos que, si bien han mejorado la eficiencia, aún enfrentan desafíos para igualar estándares internacionales. En cuanto a la ciberseguridad, las empresas han avanzado en la implementación de medidas, como la autenticación multifactor, pero persisten brechas en la adopción de tecnologías avanzadas de gestión de identidades, lo que representa una oportunidad para fortalecer la protección de la infraestructura crítica y asegurar la resiliencia frente a amenazas cibernéticas crecientes. Estos hallazgos subrayan la importancia de consolidar la digitalización y mejorar la ciberseguridad para obtener mayor estabilidad (disponibilidad) y competitividad del sector financiero colombiano en el contexto global.

El análisis de riesgos realizado evidencia que las redes asociadas al entorno financiero enfrentan riesgos que impactan el control de acceso y, por ende, la estabilidad operativa de las instituciones. Activos críticos como los sistemas core de tarjetas, los backends de aplicaciones móviles y web, y la información bancaria son propensos a vulnerabilidades, con niveles de criticidad elevados debido a la importancia de sus activos de información. La implementación de una segmentación de red adecuada, el fortalecimiento de los controles avanzados de gestión de identidades y la aplicación oportuna de parches y actualizaciones de seguridad son medidas clave para reducir la exposición a amenazas como el malware, el movimiento lateral, la suplantación de identidad y el ransomware. Al adoptar estas prácticas, las organizaciones financieras pueden aumentar la resiliencia de sus operaciones, proteger sus datos sensibles y fortalecer la confianza.

Además, casi el 90% de los riesgos identificados en la fase 2 fueron clasificados como inaceptables o inadmisibles, reflejando la necesidad de seguir implementando medidas (controles) de seguridad para reducir los riesgos residuales. Esto resalta la necesidad de una estrategia integral que permita reforzar la seguridad en las redes, proteger los activos críticos de información y tecnológicos para tener una mejor continuidad de la operación en un entorno financiero altamente digitalizado.

La caracterización de los modelos actuales de ZT en la industria, con enfoque en su aplicabilidad al sector financiero colombiano, ha evidenciado que las soluciones líderes, como Netskope, Palo Alto Networks y Zscaler, destacan por su capacidad operativa, visión integral y alineación con las necesidades críticas de seguridad del sector. La metodología propuesta, basada en Netskope como solución líder seleccionada mediante el análisis AHP, permitió proponer una metodología de ZTNA mediante 10 pasos estructurados lo que facilita tener enfoque robusto de seguridad ZT que aborda riesgos prioritarios a través de la microsegmentación de red, la integración de IAM, y la gestión de endpoints, entre otros. Este enfoque no solo proporciona una protección integral contra accesos no autorizados y movimientos laterales, sino que también refuerza el cumplimiento normativo y asegura una postura adaptativa frente a amenazas emergentes. Al implementar esta estrategia, las instituciones financieras en Colombia pueden reforzar la protección de activos críticos, fortalecer su confianza operativa y adaptarse al dinámico panorama regulatorio y de amenazas, ayudando a tener una mejor postura ante el ciber riesgo.

La validación de la metodología ZT en ambientes controlados demostró su efectividad en la mitigación de riesgos críticos asociados a diferentes escenarios de amenaza, como accesos no autorizados, suplantación de identidad y ataques de comando y control. A través de configuraciones específicas, como la implementación de agentes de seguridad, políticas de acceso estrictas, segmentación de usuarios y posturas de dispositivos, se logró controlar el acceso a dispositivos (recursos corporativos) que cumplieron con las posturas de seguridad definidas. Los resultados evidencian que la metodología propuesta no solo restringe la exposición de aplicaciones a redes públicas, sino que también mejora la capacidad de respuesta ante intentos de explotación de vulnerabilidades. En el caso de accesos no autorizados, por ejemplo, se verificó que los dispositivos sin agentes no podían establecer conexiones con servicios remotos, mientras que aquellos con agentes correctamente configurados lograron conexiones seguras. Asimismo, en los escenarios de suplantación de identidad y ataques de malware, la clasificación dinámica de dispositivos "administrados" o "no administrados" ayudó en la protección de datos sensibles al restringir el acceso de estaciones comprometidas o no conformes.

En términos cuantitativos, tras la implementación de la metodología de ZT, se observó un aumento del 16.67% en los riesgos tolerables, lo que refleja una mayor capacidad para gestionar amenazas dentro de parámetros controlados y una mejora en la postura de seguridad general. De manera significativa, los riesgos inadmisibles se redujeron en un 25.00%, evidenciando un impacto positivo en la probabilidad de ocurrencia de las amenazas más críticas. Aunque también se registró un aumento del 8.33% en los riesgos inaceptables, es de aclarar que este cambio es un reflejo natural del proceso de mitigación, ya que los riesgos más altos fueron reducidos y redistribuidos entre las diferentes categorías. Este fenómeno destaca la necesidad de optimizar aún más las estrategias implementadas para seguir transformando los riesgos inaceptables en niveles tolerables. En general, estos hallazgos refuerzan la efectividad de la metodología ZT para mejorar el panorama de riesgos del sector financiero colombiano, validando su capacidad para reducir riesgos cibernéticos y proporcionando una base sólida para su implementación en entornos operativos reales.

Finalmente, la metodología de seguridad de información basada en ZT propuesta para el control de acceso a nivel de red en el sector financiero colombiano demuestra su potencial para abordar

las brechas identificadas en la infraestructura tecnológica actual, mitigando riesgos críticos asociados a accesos no autorizados, suplantación de identidad y ataques avanzados. A través de un enfoque estructurado, que incluye microsegmentación, integración de IAM y gestión de *endpoints*, se logró transformar riesgos inadmisibles en niveles más controlados, reforzando la resiliencia frente a amenazas emergentes y garantizando el cumplimiento normativo. La validación en entornos controlados mostró una mejora significativa en la gestión de riesgos y en la protección de activos críticos, sentando las bases para su implementación en escenarios reales. De esta manera, la metodología no solo optimiza la seguridad operativa del sector, sino que también posiciona a las instituciones financieras colombianas como líderes en la adopción de estrategias avanzadas de ciberseguridad, contribuyendo a su estabilidad y competitividad en un entorno global altamente digitalizado y regulado.

3.2 Recomendaciones y trabajos futuros

Las recomendaciones derivadas de los hallazgos y conclusiones se centran en el fortalecimiento integral de la seguridad informática en el sector financiero colombiano, abordando los riesgos críticos identificados y promoviendo la adopción de tecnologías avanzadas. Es fundamental que las instituciones financieras consoliden la digitalización mediante la implementación de soluciones robustas como la metodología Zero Trust (ZT), asegurando que la protección de activos críticos sea prioritaria. Este esfuerzo debe incluir una estrategia de microsegmentación de red, la integración avanzada de herramientas de gestión de identidades (IAM) y la optimización de la gestión de endpoints para reducir el impacto de accesos no autorizados y amenazas cibernéticas avanzadas.

Asimismo, se debe realizar una actualización continua de parches y mejoras de seguridad para minimizar las vulnerabilidades asociadas al malware, movimiento lateral, ransomware y otras amenazas críticas. Esta acción requiere que las instituciones implementen controles estrictos en la clasificación y monitoreo dinámico de dispositivos, diferenciando claramente entre estaciones administradas y no administradas para limitar el acceso a datos sensibles y aplicaciones críticas. Además, los resultados en entornos controlados sugieren la necesidad de extender esta validación a operaciones reales, ajustando las configuraciones según sea necesario para optimizar la reducción de riesgos inaceptables y maximizar la resiliencia ante escenarios de amenaza emergentes.

El enfoque regulatorio también debe ser reforzado, garantizando el cumplimiento de normativas locales e internacionales, lo que permitirá a las instituciones financieras no solo fortalecer su postura operativa, sino también posicionarse como líderes en el panorama regional. Este compromiso con estándares avanzados de ciberseguridad contribuirá significativamente a la estabilidad y confianza en el sector, favoreciendo la competitividad en un entorno global altamente digitalizado. Finalmente, se recomienda establecer programas de capacitación para el personal, enfocados en el manejo de tecnologías de seguridad emergentes y en la gestión proactiva de

riesgos, fomentando una cultura organizacional resiliente y preparada para enfrentar los desafíos del panorama cibernético actual.

Para las PyMEs del sector financiero colombiano que buscan implementar la metodología de ZT sin altos costos, se recomienda combinar soluciones *open source* como WireGuard para conexiones seguras, Keycloak para la gestión de identidades con AMF, y OpenZiti para microsegmentar aplicaciones y controlar accesos según políticas estrictas (ZTNA). Adicionalmente, se recomienda complementar con firewalls como PfSense u OPNsense para segmentar la red y monitoreo lógico con soluciones como ELK Stack para registrar y alertar sobre actividades sospechosas, así se podría desarrollar una ZTA robusta, económica y escalable, maximizando la ciberseguridad con recursos accesibles.

Nuevos trabajos de cara al futuro podrían ser:

Definir e implementar Indicadores Clave de Desempeño (KPI) para evaluar el progreso y la efectividad de la metodología de control de acceso a la red basada en Zero Trust en el sector financiero colombiano. Estos indicadores podrían medir aspectos como la reducción del riesgo de accesos no autorizados, la eficiencia en la detección y respuesta a incidentes, el impacto en la experiencia del usuario y el cumplimiento normativo. La aplicación de estos KPI permitiría validar la metodología, identificar áreas de mejora y ajustar su implementación para optimizar su desempeño en escenarios dinámicos de ciberseguridad.

Desarrollar una metodología híbrida que integre elementos de otros modelos de seguridad mencionados, como marcos de referencia basados en **NIST 800-207 (Zero Trust Architecture)**, con el objetivo de enriquecer el enfoque de Zero Trust. En particular, se podría explorar la incorporación de un modelo de madurez que permita evaluar el nivel de adopción y efectividad de la metodología en diferentes organizaciones del sector financiero. Este modelo podría definir etapas de implementación progresiva, desde una adopción inicial hasta un estado de optimización, proporcionando un camino estructurado para la mejora continua en la gestión de la ciberseguridad.

Por último, integrar en la metodología propuesta con la visión y las metas estratégicas de las entidades financieras, asegurando que su adopción no solo responda a necesidades técnicas, sino que también se alinee con la cultura organizacional y los objetivos de negocio. Esto implicaría el desarrollo de un marco de implementación que contemple factores como la cultura de seguridad, el cambio organizacional y la gobernanza, facilitando la adopción efectiva del enfoque Zero Trust. Además, se podrían establecer modelos de gestión del cambio y estrategias de comunicación para responder a la sensibilización y el compromiso de todas las áreas involucradas, fortaleciendo la sostenibilidad y el impacto de la metodología a largo plazo.

Anexos

A. Anexo: Diseño de Encuesta para la Categorización e Identificación de Riesgos en el Sector Financiero Colombiano

Le agradecemos por completar esta encuesta. Su participación nos ayudará a comprender mejor el contexto operacional de las empresas del sector financiero en Colombia, especialmente en relación con el control de acceso y la identificación de riesgos asociados a las redes. Esta encuesta es parte de una tesis de maestría en ciberseguridad y todos los datos serán tratados de manera confidencial. La encuesta le tomará aproximadamente 10 minutos.

Parte 1: Contexto Operacional

1. **¿Cuál es el tamaño de su empresa del sector financiero?**
    - Pequeña (menos de 50 empleados)
    - Mediana (50-200 empleados)
    - Grande (más de 200 empleados)

2. **¿Qué tipo de servicios financieros ofrece su empresa? *(Seleccione todas las que correspondan)***
    - Banca comercial
    - Banca de inversión
    - Seguros
    - Fondos de pensiones
    - Otros (especificar): _____

3. **¿Qué tipo de medios de pago están a disposición de sus clientes?** ***(Seleccione todas las que correspondan)***
    - Tarjetas débito/crédito
    - Transferencias bancarias
    - Transacciones electrónicas
    - Pagos móviles tipo QR o NFC
    - Pagos por medio de plataformas web
    - Otros (especificar): _____

4. **¿Tiene su empresa un conjunto de políticas para la seguridad de la información, aprobadas por la alta dirección, publicadas y comunicadas?**
    - Sí
    - No
    - Tal vez

Parte 2: Control de Acceso e Identificación de Riesgos

5. **¿Qué aspectos de la seguridad de la información considera más críticos para la protección de datos personales?** ***(Seleccione todas las que correspondan)***
    - Control de acceso a sistemas y datos sensibles
    - Gestión de riesgos de seguridad de la información
    - Cumplimiento normativo y regulatorio
    - Otros (especificar): _____

6. **¿Qué desafíos identifica su empresa en relación con el control de acceso y la gestión de la seguridad de la información en el entorno financiero?**

    - Falta de recursos y presupuesto adecuados
    - Complejidad tecnológica y de infraestructura
    - Cumplimiento normativo y regulaciones cambiantes
    - Amenazas internas y externas

- Arquitecturas tecnológicas complejas
- Otros (especificar): _____

7. **¿Qué tipo de controles de acceso implementa su empresa para proteger sus redes y sistemas? *(Seleccione todas las que correspondan)***

   - Autenticación multifactor (por ejemplo, contraseña más token)
   - Control de acceso basado en roles
   - Monitoreo continuo de la actividad del usuario
   - Otros (especificar): _____

Parte 3: Gestión de Identidades

8. **¿Su empresa utiliza algún sistema o herramienta de gestión de identidades (IAM) para administrar y controlar el acceso de los usuarios a los sistemas y datos?**
   - Sí
   - No
   - En proceso de implementación

9. **¿Qué métodos de autenticación utiliza su empresa para verificar la identidad de los usuarios que acceden a sistemas y datos sensibles? *(Seleccione todas las que correspondan)***
   - Contraseña única o multifactor
   - Biometría (por ejemplo, escaneo de huellas dactilares, reconocimiento facial)
   - Tarjetas inteligentes (smart cards)
   - Tokens de seguridad
   - Otros (especificar): _____

Parte 4: Impacto y Gestión de Riesgos

10. **¿Cuáles considera que son los principales desafíos o riesgos relacionados con la gestión de identidades en su empresa?** ***(Seleccione todas las que correspondan)***
    - Acceso no autorizado debido a credenciales débiles o comprometidas
    - Dificultades para gestionar identidades en entornos distribuidos
    - Cumplimiento normativo y regulaciones de privacidad
    - Complejidad en la integración de sistemas IAM
    - Otros (especificar): _____
11. **¿Su empresa cuenta con un plan de gestión de incidentes de seguridad cibernética que incluye acciones específicas para abordar problemas de control de acceso?**
    - Sí, tenemos un plan establecido y probado
    - Sí, pero está en desarrollo
    - No tenemos un plan formalizado
    - No estoy seguro/a

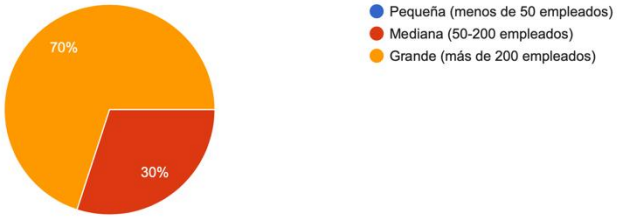
12. **¿Tiene algún otro comentario o información relevante que le gustaría compartir sobre el control de acceso y la seguridad cibernética en su empresa?**

¡Gracias por su participación! Sus respuestas son importantes para nuestro análisis del contexto operacional y las prácticas de seguridad en el sector financiero de Colombia.

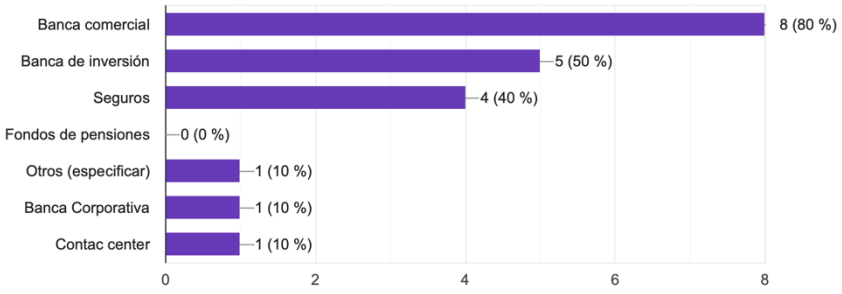
B. Anexo: Respuestas de la Encuesta sobre la Categorización e Identificación de Riesgos en el Sector Financiero Colombiano

Parte 1: Contexto Operacional

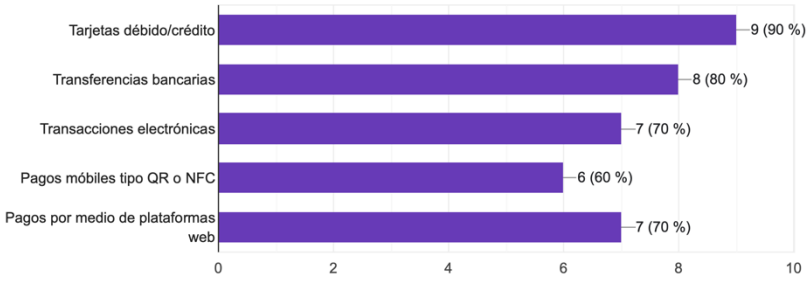
¿Cuál es el tamaño de su empresa del sector financiero?
10 respuestas



¿Qué tipo de servicios financieros ofrece su empresa? (Seleccione todas las que correspondan)
10 respuestas

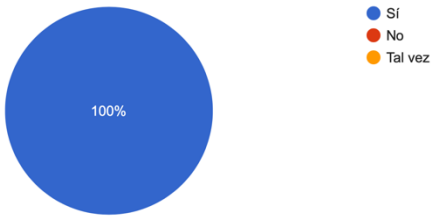


¿Qué tipo de medios de pago tienen a disposición para sus clientes? (Seleccione todas las que correspondan)
10 respuestas



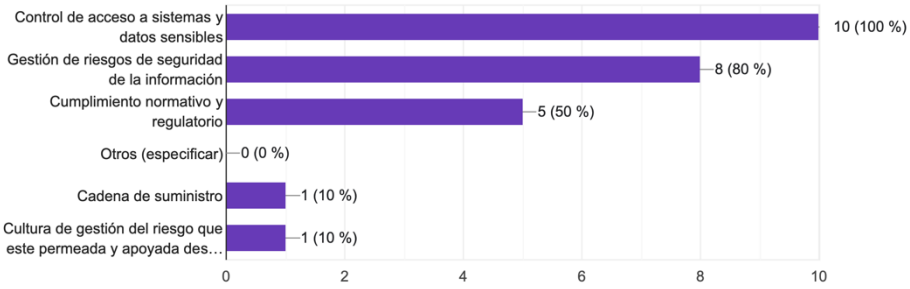
¿Tiene su empresa un conjunto de políticas para la seguridad de la información, aprobada por la alta dirección, publicada y comunicada?

10 respuestas



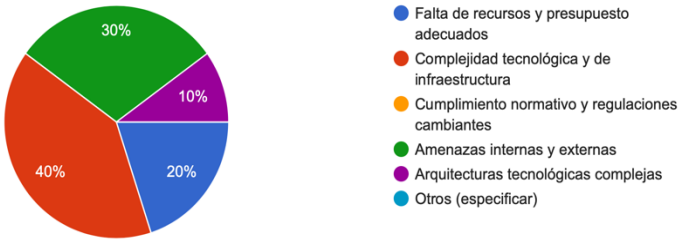
¿Qué aspectos de la seguridad de la información considera más críticos para la protección de datos personales? (Seleccione todas las que correspondan)

10 respuestas



¿Qué desafíos identifica su empresa en relación con el control de acceso y la gestión de la seguridad de la información en el entorno financiero?

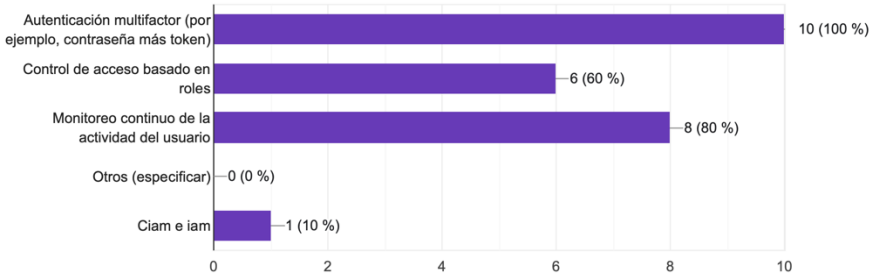
10 respuestas



Parte 2: Control de Acceso e Identificación de Riesgos

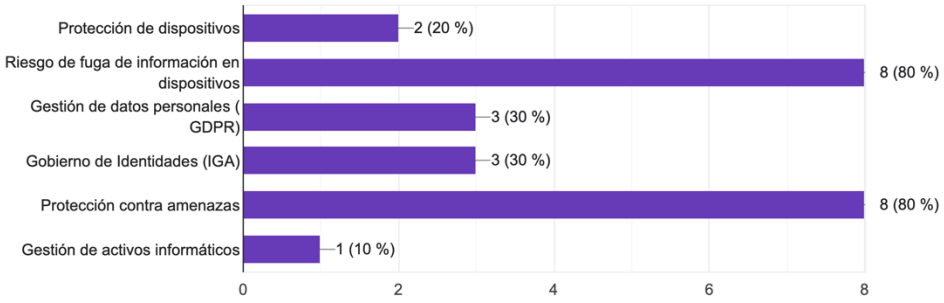
¿Qué tipo de controles de acceso implementa su empresa para proteger sus redes y sistemas?

10 respuestas



¿Cuáles considera que son los principales desafíos en la gestión de dispositivos en su empresa?

10 respuestas

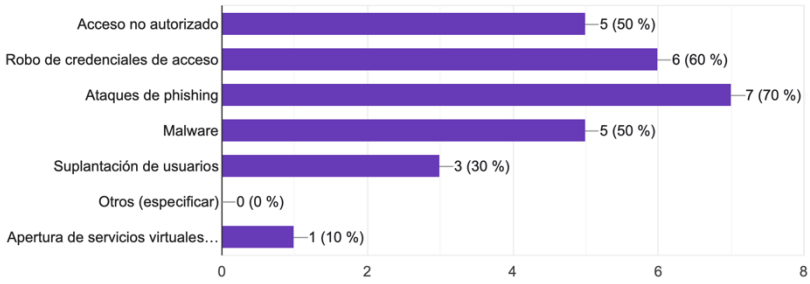


¿Su empresa realiza evaluaciones externas de seguridad donde se revisa el control de acceso?

9 respuestas

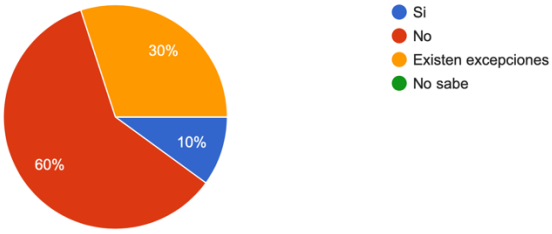
¿Cuáles considera que son las principales amenazas asociadas al control de acceso a la red que más probabilidad de ocurrencia se presentan en s...mpresa? (Seleccione todas las que correspondan)

10 respuestas



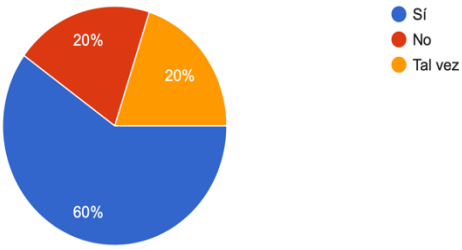
¿En su empresa es permitido que dispositivos no administrados accedan a su red corporativa?.

10 respuestas



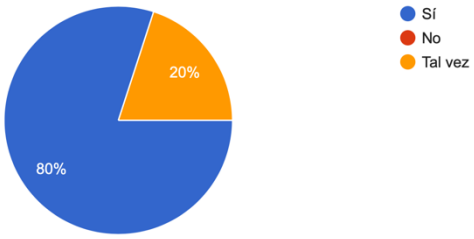
¿Su empresa cuenta con controles de seguridad y/o protocolos para que dispositivos no administrados accedan a su red corporativa?

10 respuestas



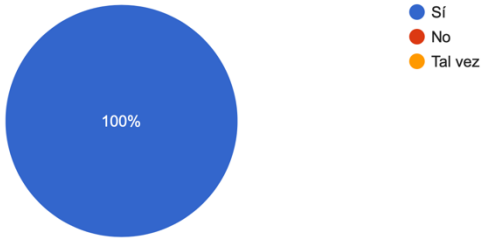
¿Su empresa, cuenta con políticas y medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesa...en los lugares en los que se realiza teletrabajo?.

10 respuestas



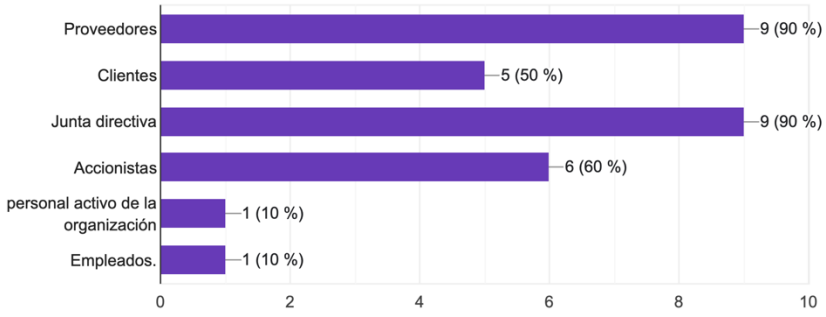
¿Su empresa cuenta con un programa de formación en ciberseguridad obligatorio en sus empleados?

10 respuestas



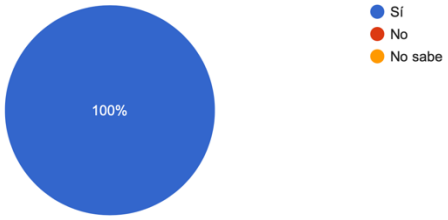
¿El plan de formación en ciberseguridad se extiende a?

10 respuestas



¿Su compañía cuenta con procesos formales de creación, modificación y cancelación de usuarios?.

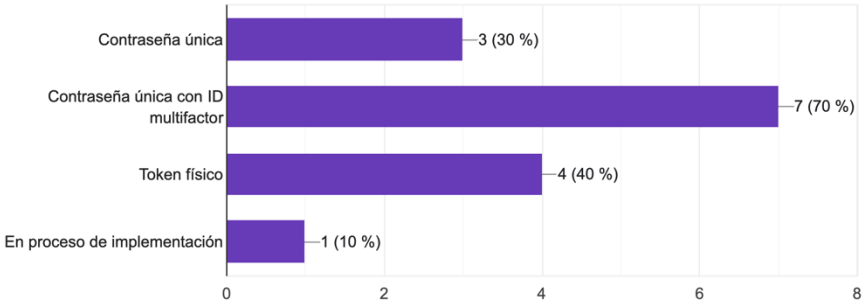
10 respuestas



Parte 3. Gestión identidad

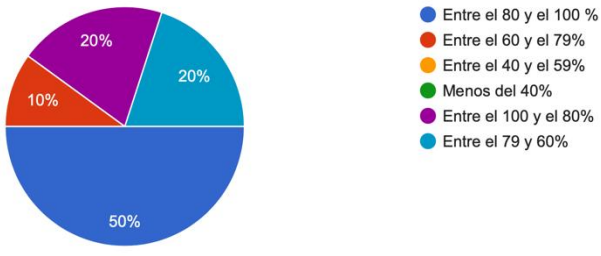
¿Su empresa utiliza algún sistema o herramienta de gestión de identidades (IAM) para administrar y controlar el acceso de los usuarios a los sistemas y datos?

10 respuestas



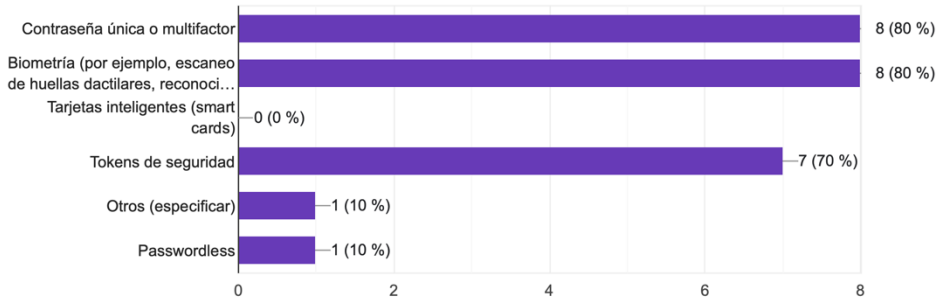
¿Cuál es el porcentaje de cobertura de los controles de ciberseguridad en su empresa?

10 respuestas



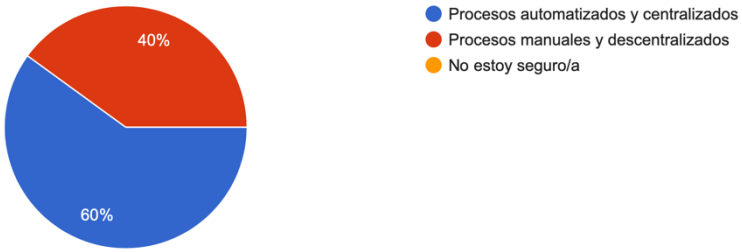
¿Qué métodos de autenticación utiliza su empresa para verificar la identidad de los usuarios que acceden a sistemas y datos sensibles? (Seleccione todas las que correspondan)

10 respuestas



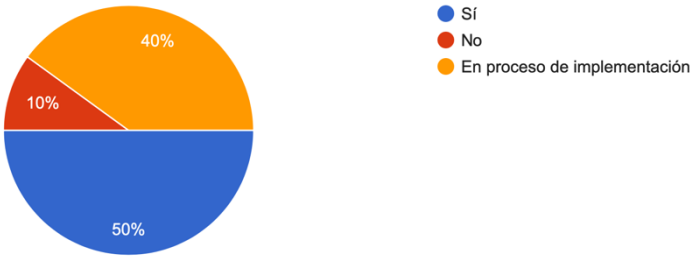
¿Cómo se gestiona el ciclo de vida de las identidades de los empleados y usuarios en su empresa? (por ejemplo, creación, modificación, desactivación)

10 respuestas



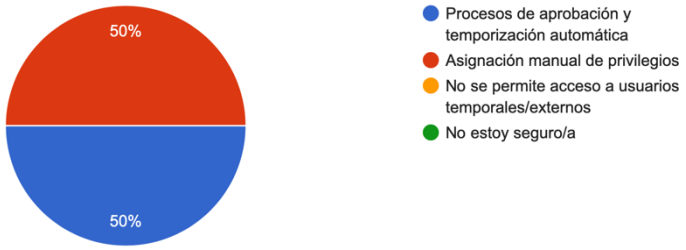
¿Su empresa implementa políticas de acceso basadas en roles (RBAC) para definir y controlar los privilegios de los usuarios?

10 respuestas



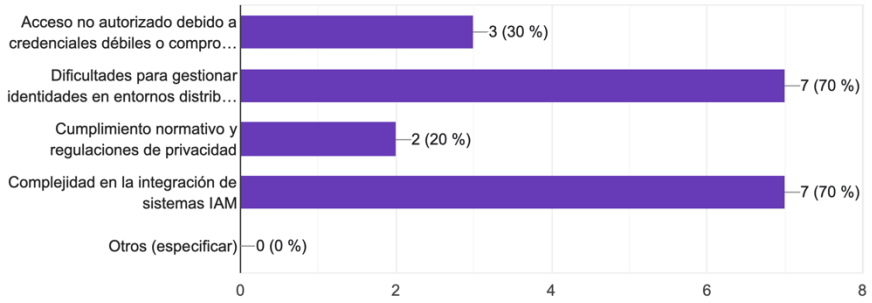
¿Cómo se manejan los privilegios de acceso de los usuarios temporales o externos (por ejemplo, contratistas, consultores) en su empresa?

10 respuestas



¿Cuáles considera que son los principales desafíos o riesgos relacionados con la gestión de identidades en su empresa?

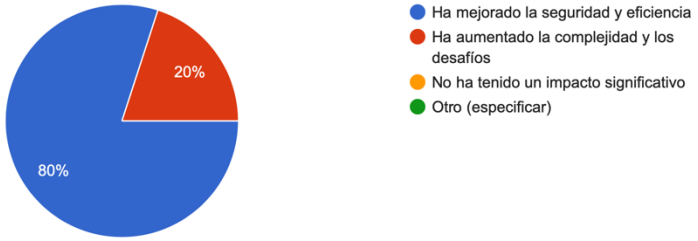
10 respuestas



Parte 4: Impacto y Gestión de Riesgos

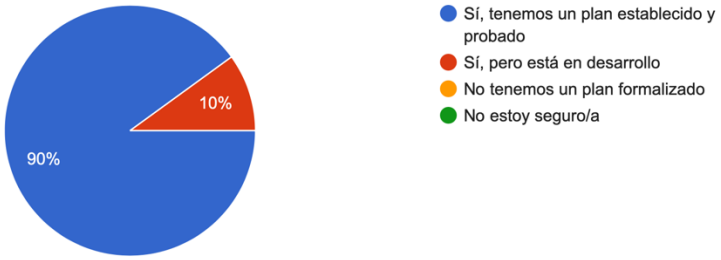
¿Cómo ha impactado la transformación digital en las prácticas de control de acceso en su empresa?

10 respuestas



¿Su empresa cuenta con un plan de gestión de incidentes de seguridad cibernética que incluye acciones específicas para abordar problemas de control de acceso?

10 respuestas



¿Tiene algún otro comentario o información relevante que le gustaría compartir sobre el control de acceso y la seguridad cibernética en su empresa?

3 respuestas

- La tecnología está disponible, el reto es mover las áreas internas que ofrecen resistencia en el uso e implementación.
- Se están revisando iniciativas como *Passwordless* para reducir la exposición inherente al manejo de contraseña sobre ataques de ingeniería social.
- La seguridad de la información y la cibdrseguridad es definida desde la JUNTA Directiva y es de estricto cumplimiento a todo nivel. La no adopción de los lineamientos es causal de despido.

C. Anexo: Identificación y Evaluación de Riesgos Asociados a las Redes – Fase 2

Definición del contexto /Alcance
Se realizará un mapa de riesgos para la infraestructura interna hasta el nivel de sistema operativo.

Identificación de Activos

ACTIVOS /RECURSOS
Sistema core tarjetas (Debido/crédito)
Sistema core crediticios
Backend APP Movil
Backend APP Web
Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo..)

Clasificación de Activos según Nivel de Criticidad

- **Pública:** Si el valor es igual o inferior a 8
- **Privada:** Si el valor está entre 9 y 14
- **Confidencial:** Si el valor es mayor o igual a 15

Activo	Afectación sobre los planes de negocio (finanzas)	Tipo de destinatario	Afecta legalmente a la empresa	Afecta las ventas o una ventaja competitiva	Tiene afectación sobre la seguridad	Nivel de criticidad	
Sistema core tarjetas (Débito/crédito)	4	4	3	4	1	16	Confidencial
Sistema core crediticios	4	4	3	4	1	16	Confidencial
Backend APP Movil	4	4	2	4	1	15	Confidencial
Backend APP Web	4	4	2	4	1	15	Confidencial
Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo)	4	4	4	4	2	18	Confidencial

Implementación de Controles Actuales en los Activos Identificados

Efectividad de Controles
• 0% = No se cuenta con controles • 25% = Algunos controles están implementados, pero no funcionan adecuadamente o son limitados (no cubren todo el riesgo) • 50% = todos los controles propuestos están implementados, pero no se valida su efectividad. • 75%= Todos los controles están implementados, se verifican su efectividad, pero no se monitorea ni se hacen planes de mejora continua. • 100%= La totalidad de controles están implementados, se miden, monitorean y se generan planes de acción para su mantenimiento (líneas base periódicas y auditorias).

Activos	Vulnerabilidades	Controles actuales implementados en el activo.	Clasificación del activo	Efectividad de los controles = Eficiencia + Eficacia
Sistema core tarjetas (Débito/crédito)	Ausencia de parches de seguridad, Ausencia de actualizaciones permanente, Ausencia de entrenamiento en gestión segura de la infraestructura No se evidencia un control de navegación en los servidores Ausencia de logs para el monitoreo de seguridad del activo Ausencia de MFA para la autenticación en las estaciones Problemas de configuración Falta segmentación de red		Confidencial	0%
Sistema core crediticios	CVE-2023-28298 En el kernel del SO - negación de servicio CVE-2016-7217 Permite a un atacante ejecutar código remoto		Confidencial	0%

	No se evidencia una gestión de usuarios privilegiados Ausencia de entrenamiento en gestión segura de la infraestructura No se evidencia un control de navegación en los servidores Ausencia de MFA para la autenticación en las estaciones Problemas de configuración Falta segmentación de red			
Backend APP Movil	CVE-2021-3939 Permite obtener privilegios root y tomar control total de un servidor explotando error corrupción memoria en servicio de componente de cuentas GNOME CVE-2018-1092 permitir a un atacante bloquear un sistema vulnerable tras causar una denegación de servicio al montar un sistema de archivos EXT4 modificado para ello. No se evidencia una gestión de usuarios privilegiados No se evidencia un control de navegación en los servidores Ausencia de MFA para la autenticación en las estaciones		Confidencial	0%

	Problemas de configuración Falta segmentación de red			
Backend APP Web	CVE-2001-0867 Cisco 12000 with IOS 12.0 and line cards based on Engine 2 does not properly filter does not properly filter packet fragments even when the "fragment" keyword is used in an ACL, which allows remote attackers to bypass the intended access controls. Falta segmentación de red Plagas		Confidencial	0%

Información bancaria (Débito/crédito/libranzas/Crédito Vehículo)	CVE-2007-5419 El enrutador 3Com 3CRWER100-75 con software 1.2.10ww, cuando habilita un servidor virtual opcional, configura este servidor para aceptar todas las direcciones IP de origen en la interfaz externa (Internet), a menos que el usuario seleccione otras opciones, lo que podría exponer el enrutador a llamadas entrantes no deseadas. tráfico de atacantes remotos, como se demuestra al configurar un servidor virtual en el puerto 80, que permite a los atacantes remotos acceder a la interfaz de administración web.		Confidencial	0%

Inventario de Amenazas

Listado amenazas	Factor de riesgos
Malware	**AMENAZAS TIC**
Movimiento lateral (Piboteo)	**AMENAZAS TIC**
Suplantación de identidad	**AMENAZAS TIC**
Acceso no autorizado	**AMENAZAS TIC**
Ransomware	**AMENAZAS TIC**

Escenarios de Riesgo y Consecuencias en Activos Críticos del Sistema Financiero Colombiano

No.	Escenario de los riesgos	Agente Generador	Efecto o consecuencia
(1)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema core tarjetas (Débito/crédito)	Agente externo	Confidencialidad
(2)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema core crediticios	Agente externo	Confidencialidad
(3)	Posibilidad que la amenaza: Malware, afecte el activo: Backend APP Movil	Agente externo	Confidencialidad
(4)	Posibilidad que la amenaza: Malware, afecte el activo: Backend APP Web	Agente externo	Confidencialidad
(5)	Posibilidad que la amenaza: Malware, afecte el activo: Información bancaria (Débito/crédito/libranzas/Crédito Vehículo)	Agente externo	Confidencialidad
(6)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Sistema core tarjetas (Débito/crédito)	Agente externo	Confidencialidad
(7)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Sistema core crediticios	Agente externo	Confidencialidad
(8)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Backend APP Movil	Agente externo	Confidencialidad
(9)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Backend APP Web	Agente externo	Confidencialidad
(10)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Información bancaria (Débito/crédito /libranzas/Crédito Vehículo)	Agente externo	Confidencialidad
(11)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Sistema core tarjetas (Débito/crédito)	Agente externo	Confidencialidad
(12)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Sistema core crediticios	Agente externo	Confidencialidad
(13)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Backend APP Movil	Agente externo	Confidencialidad
(14)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Backend APP Web	Agente externo	Confidencialidad
(15)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Sistema core tarjetas (Débito/crédito)	Agente externo	Confidencialidad

(16)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Sistema core crediticios	Agente externo	Confidencialidad
(17)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Backend APP Movil	Agente externo	Confidencialidad
(18)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Backend APP Web	Agente externo	Confidencialidad
(19)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Información bancaria (Débito/crédito /libranzas/Crédito Vehículo)	Agente externo	Confidencialidad
(20)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema core tarjetas (Debido/credito)	Agente externo	Confidencialidad
(21)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema core crediticios	Agente externo	Confidencialidad
(22)	Posibilidad que la amenaza: Ransomware, afecte el activo: Backend APP Movil	Agente externo	Confidencialidad
(23)	Posibilidad que la amenaza: Ransomware, afecte el activo: Backend APP Web	Agente externo	Confidencialidad
(24)	Posibilidad que la amenaza: Ransomware, afecte el activo: Información bancaria (Débito/crédito /libranzas/Crédito Vehículo)	Agente externo	Confidencialidad

Evaluación del Riesgo

No.	Escenario de riesgos	PROBABILIDAD		IMPACTO OPERACIÓN		Riesgo P*Impacto Cliente Mercado	Clasificación del activo
(1)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema core tarjetas (Débito/crédito)	Probable	4	Mayor	4	16	Confidencial
(2)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema core crediticios	Probable	4	Mayor	4	16	Confidencial
(3)	Posibilidad que la amenaza: Malware, afecte el activo: Backend APP Movil	Probable	4	Intermedio	3	12	Confidencial
(4)	Posibilidad que la amenaza: Malware, afecte el activo: Backend APP Web	Probable	4	Intermedio	3	12	Confidencial
(5)	Posibilidad que la amenaza: Malware, afecte el activo: Información bancaria (Débito/crédito/libranzas/Crédito Vehículo..)	Probable	4	Mayor	4	16	Confidencial
(6)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Sistema core tarjetas (Débito/crédito)	Improbable	2	Mayor	4	8	Confidencial
(7)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Sistema core crediticios	Improbable	2	Mayor	4	8	Confidencial
(8)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Backend APP Movil	Improbable	2	Intermedio	3	6	Confidencial
(9)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Backend APP Web	Improbable	2	Intermedio	3	6	Confidencial
(10)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Información bancaria (Débito/crédito/libranzas/Crédito Vehiculo..)	Improbable	2	Intermedio	3	6	Confidencial
(11)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Sistema core tarjetas (Débito/crédito)	Probable	4	Superior	5	20	Confidencial
(12)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Sistema core crediticios	Probable	4	Superior	5	20	Confidencial

(13)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Backend APP Movil	Probable	4	Intermedio	3	12	Confidencial
(14)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Backend APP Web	Probable	4	Intermedio	3	12	Confidencial
(15)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Sistema core tarjetas (Débito/crédito)	Probable	4	Superior	5	20	Confidencial
(16)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Sistema core crediticios	Probable	4	Superior	5	20	Confidencial
(17)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Backend APP Movil	Probable	4	Intermedio	3	12	Confidencial
(18)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Backend APP Web	Probable	4	Intermedio	3	12	Confidencial
(19)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Información bancaria (Débito/crédito/libranzas/Crédito Vehículo..)	Probable	4	Superior	5	20	Confidencial
(20)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema core tarjetas (Débito/crédito)	Posible	3	Superior	5	15	Confidencial
(21)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema core crediticios	Posible	3	Superior	5	15	Confidencial
(22)	Posibilidad que la amenaza: Ransomware, afecte el activo: Backend APP Movil	Posible	3	Intermedio	3	9	Confidencial
(23)	Posibilidad que la amenaza: Ransomware, afecte el activo: Backend APP Web	Posible	3	Intermedio	3	9	Confidencial
(24)	Posibilidad que la amenaza: Ransomware, afecte el activo: Información bancaria (Débito/crédito/libranzas/Crédito Vehículo..)	Posible	3	Superior	5	15	Confidencial

D. Anexo: Modelo AHP para la Selección de la empresa líder en Modelo Zero Trust

Ponderación de criterios vs. elementos							
	Nivel de protección			Matriz normalizada			Vector promedio
	Netskope	Palo alto	Zscaler				
Netskope	1.00	1.00	5.00	0.45	0.45	0.45	0.45
Palo alto	1.00	1.00	5.00	0.45	0.45	0.45	0.45
Zscaler	0.20	0.20	1.00	0.09	0.09	0.09	0.09
Totales	2.20	2.20	11.00				

	Escalabilidad y rendimiento			Matriz normalizada			Vector promedio
	Netskope	Palo alto	Zscaler				
Netskope	1.00	1.00	2.00	0.4	0.3	0.5	0.4
Palo alto	1.00	1.00	1.00	0.4	0.3	0.3	0.3
Zscaler	0.50	1.00	1.00	0.2	0.3	0.3	0.3
Totales	2.50	3.00	4.00				

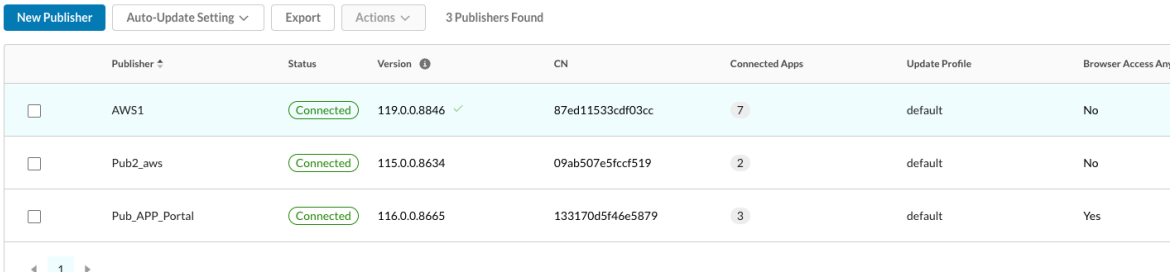
	Compatibilidad e integración			Matriz normalizada			Vector promedio
	Netskope	Palo alto	Zscaler				
Netskope	1.00	7.00	5.00	0.7	0.5	0.8	0.7
Palo alto	0.14	1.00	0.17	0.1	0.1	0.0	0.1
Zscaler	0.20	6.00	1.00	0.1	0.4	0.2	0.2
Totales	1.34	14.00	6.17				

	Visibilidad y reporte granular			Matriz normalizada			Vector promedio
	Netskope	Palo alto	Zscaler				
Netskope	1.0	0.2	3.0	0.16	0.15	0.27273	0.19
Palo alto	5.0	1.0	7.0	0.79	0.74	0.63636	0.72
Zscaler	0.3	0.1	1.0	0.05	0.11	0.09091	0.08

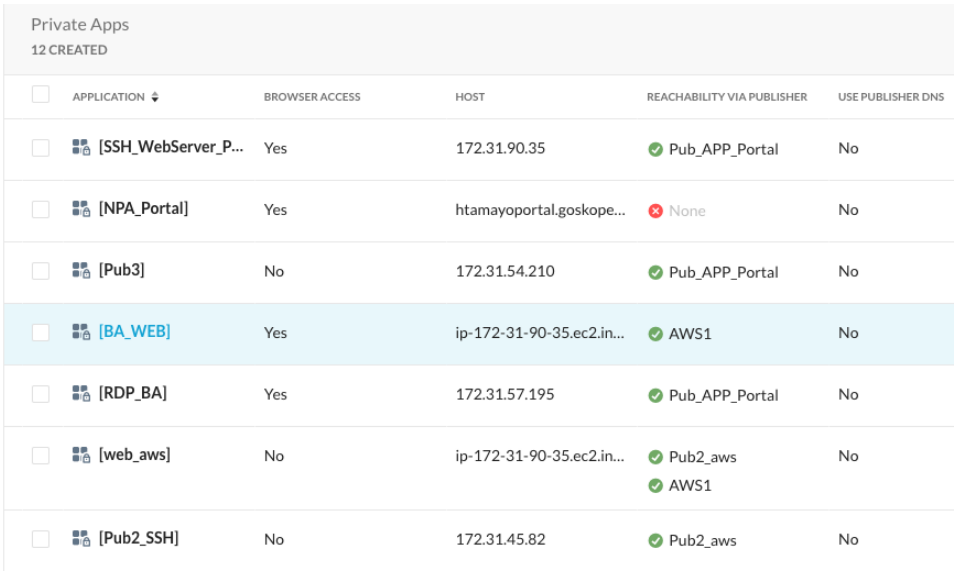
Totales	6.3	1.3	11.0

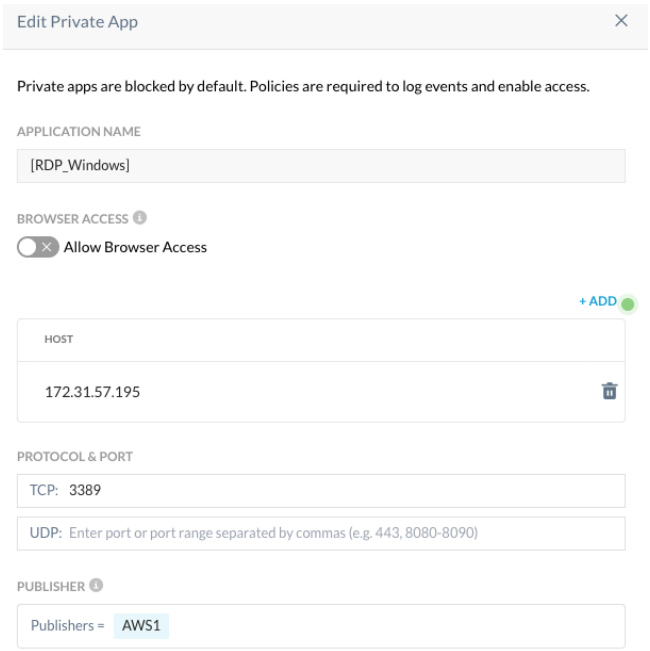
E. Anexo: Configuraciones comunes en los 3 escenarios

Publisher conectados desde los sitios remotos hacia la nube del ZTNA

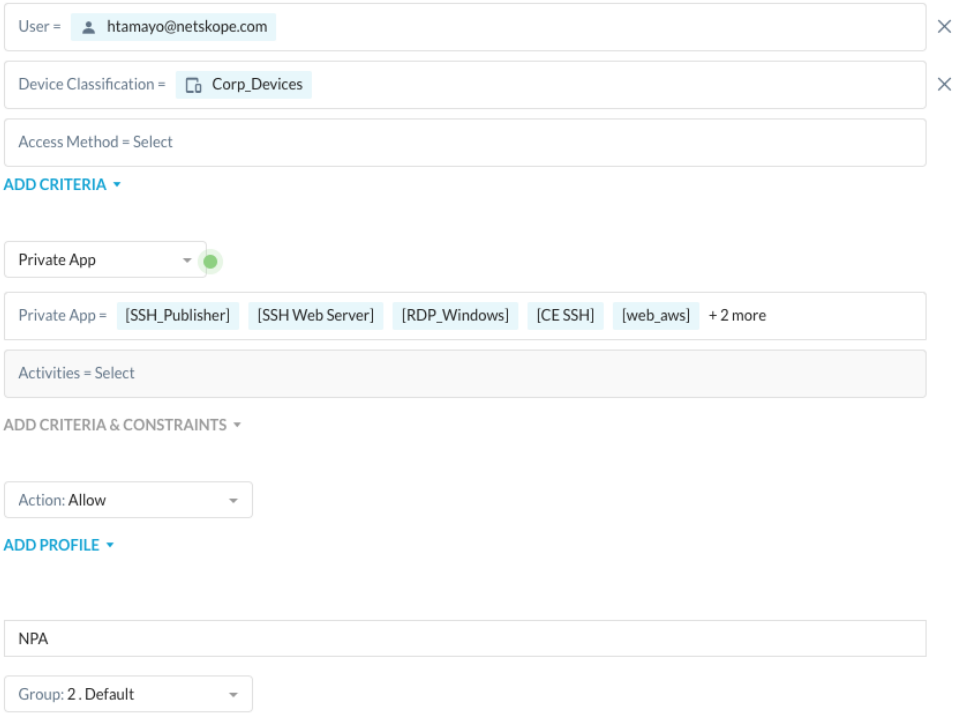


Definición de aplicaciones





Reglas de control de acceso



Logs de acceso a la aplicación

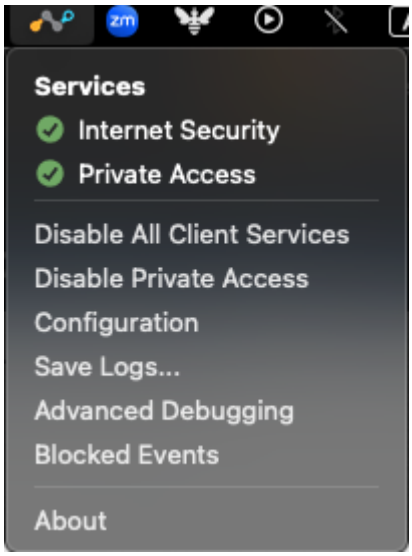
Network Events
2,584 CREATED

Sort by: Time EXPORT

TIME	USER	APPLICATION	DESTINATION IP ADDRESS	DESTINA...	IP PROTOCOL	POLICY NAME	ACTION	TOTAL BYTES	BYTES UPLOADED	BYTES DOWNLOADED
10/3/2024 12:18 PM	htamayo@netsko...	[web_aws]		HTTP...	TCP	NPA	Allow	496 Bytes	324 Bytes	172 Bytes
10/3/2024 12:17 PM	htamayo@netsko...	[web_aws]		HTTP...	TCP	NPA	Allow	1.783KB	878 Bytes	948 Bytes
10/3/2024 12:09 PM	htamayo@netsko...	[RDP_Windows]		RDP (...	TCP	NPA	Allow	811.9KB	152.2KB	659.7KB
10/3/2024 11:35 AM	htamayo@netsko...	[web_aws]		HTTP...	TCP	NPA	Allow	3.045KB	1.885KB	1.16KB
10/3/2024 11:34 AM	hugotamayo@hta...	[BA_WEB]		HTTP...	TCP	NPA BA	Allow	3.042KB	1.45KB	1.592KB
10/3/2024 11:32 AM	hugotamayo@hta...	[RDP_BA]		RDP (...	TCP	test_BA	Allow	47.5KB	3.998KB	43.5KB
10/3/2024 11:28 AM	hugotamayo@hta...	[RDP_BA]		RDP (...	TCP	test_BA	Allow	1.018KB	958 Bytes	84 Bytes

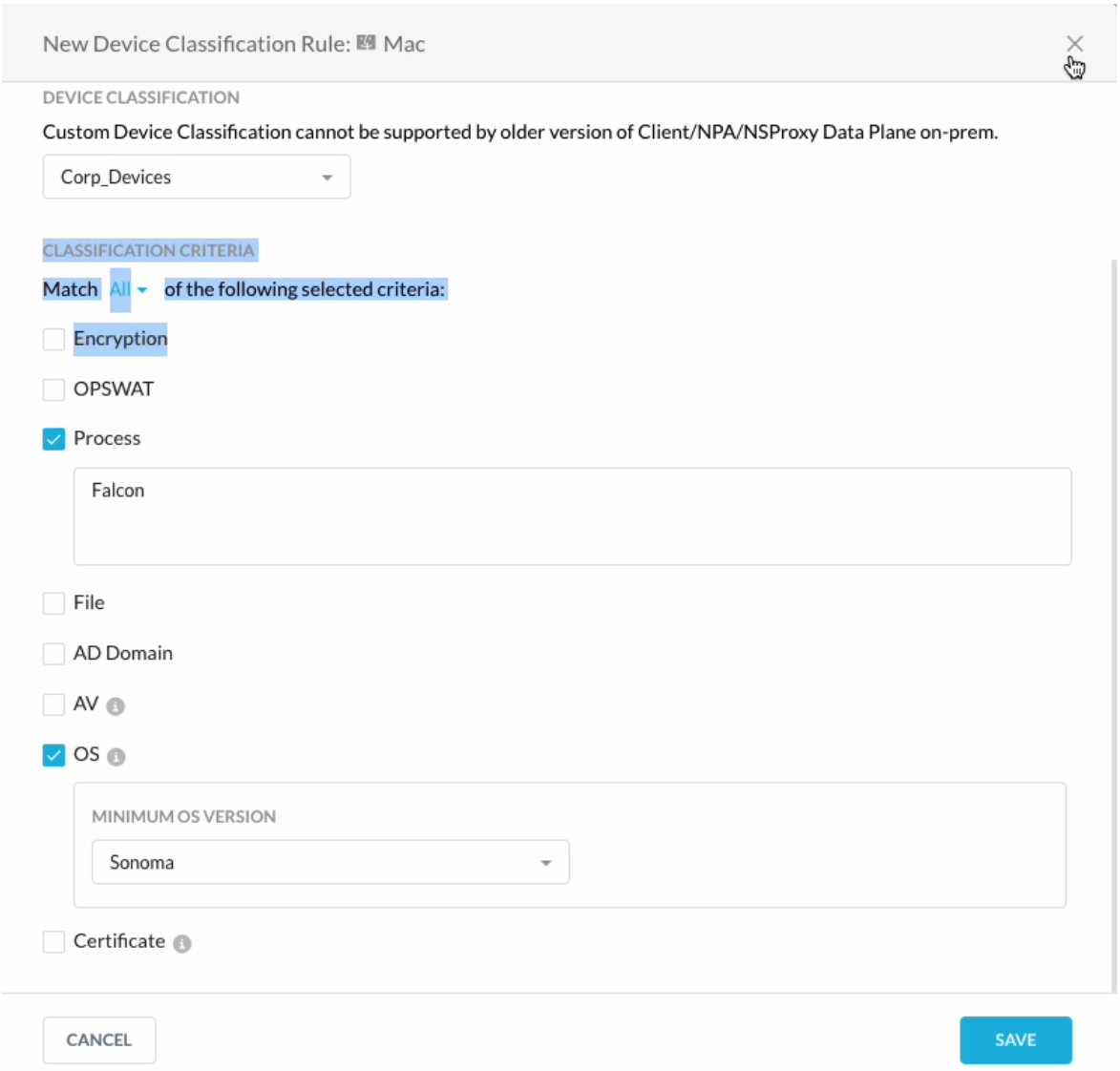
F. Anexo: Configuraciones escenario 1 – Acceso no autorizado

Desde la perspectiva del cliente, se cuenta con un agente instalado en la máquina remota, que se encarga de capturar el tráfico hacia la aplicación y dirigirlo hacia la nube del ZTNA de forma transparente.

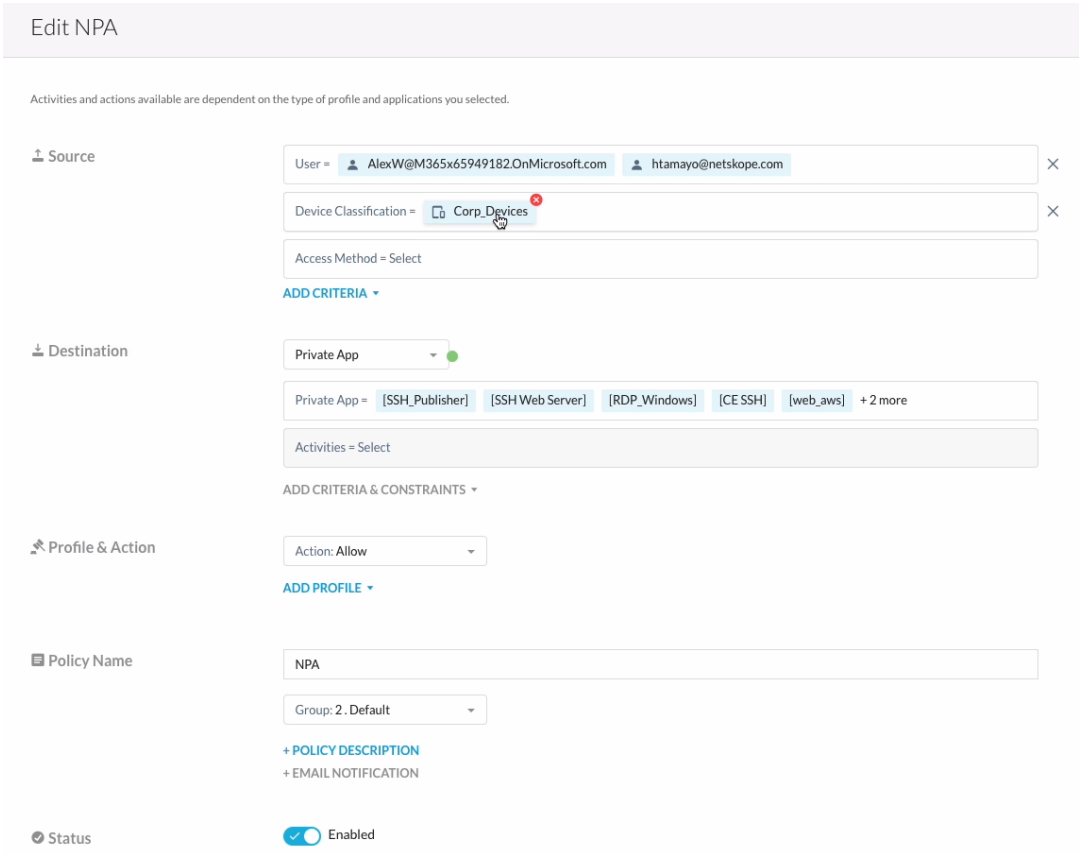


G. Anexo: Configuraciones escenario 2 – Suplantación de identidad

Configuración de postura para dispositivos corporativos MacOs, donde mínimamente se solicita que el antimalware llamado Falcon este corriendo en la maquina y que el Sistema operativo sea desde la menor versión declarada como Sonoma.



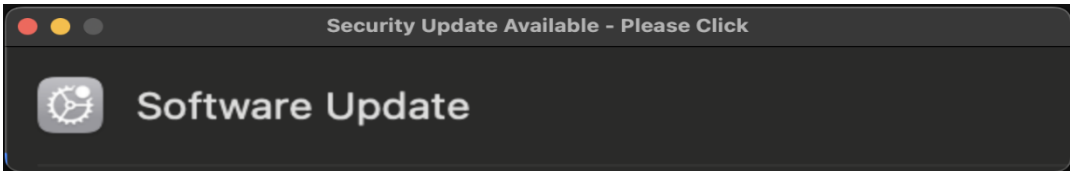
Adicional, se agregan las políticas de acceso en las cuales se dejan explícitos el usuario y los grupos de usuarios que serán parte del análisis de la regla, el tipo de aplicación sobre la cual va a ejecutar la regla y la acción; que en este caso es Permitir (Allow).



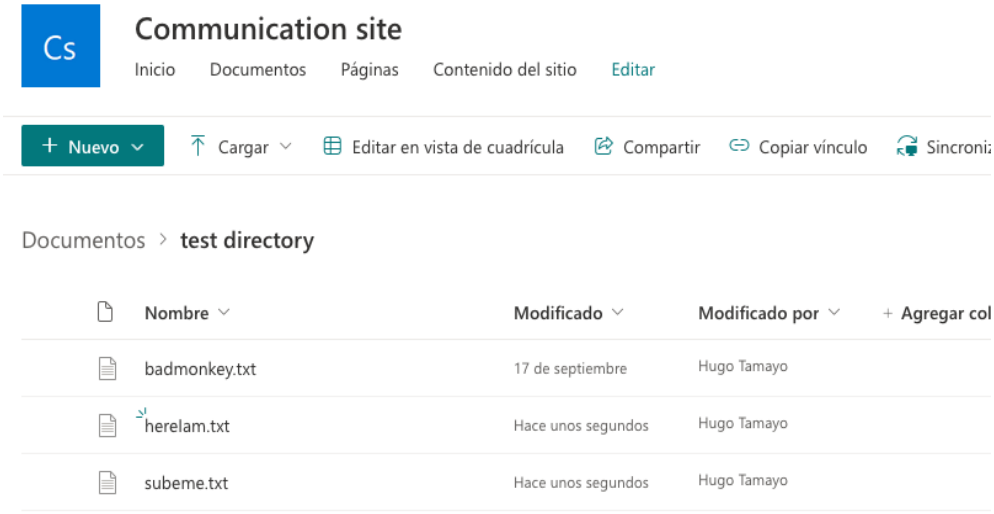
H. Anexo: Configuraciones escenario 3 – Malware

Al hacer clic en el botón que se ofrece, el malware se ejecuta y reporta con la nube de comando y control que en este caso es una instancia de Sharepoint, indicando el sistema operativo y otros detalles de la víctima:

Botón que ofrece el malware



***SharePoint* que se crea con la información de la estación de la victima**



Información en los documentos en el comando y control del atacante

herelam.txt

```
1   usuario: htamayo
2   hostname: H71PWCX7DC
3   SO: ProductName:        macOS
4   ProductVersion:     14.7
5   BuildVersion:       23H124
6
```

Otro de los archivos en la nube se encarga de enviar instrucciones remotas a la máquina de la víctima, en este caso buscando obtener el listado de procesos en ejecución en la máquina:

badmonkey.txt

```
1   ps -fea > subeme.txt
2
```

El resultado de este comando es recogido en otro archivo, lo que le permite al atacante identificar el software de seguridad ejecutándose en el equipo:

subeme.txt

```
  UID   PID  PPID   C STIME   TTY           TIME CMD
    0     1     0   0 23Sep24 ??        69:47.64 /sbin/launchd
    0  1127     1   0 23Sep24 ??        13:58.92 /usr/libexec/logd
    0  1128     1   0 23Sep24 ??         0:00.47 /usr/libexec/smd
    0  1129     1   0 23Sep24 ??         3:35.98 /usr/libexec/UserEventAgent (System)
    0  1131     1   0 23Sep24 ??         0:14.01 /System/Library/PrivateFrameworks/Uninstall.framework/Resources/uninstalld
    0  1132     1   0 23Sep24 ??        11:34.95 /System/Library/Frameworks/CoreServices.framework/Versions/A/Frameworks/FSEvents.framework/Versions/A/Support/fseventsd
    0  1133     1   0 23Sep24 ??         0:55.07 /System/Library/PrivateFrameworks/MediaRemote.framework/Support/mediaremoted
    0  1136     1   0 23Sep24 ??         2:51.50 /usr/sbin/systemstats --daemon
  278  1138     1   0 23Sep24 ??         0:02.51 /System/Library/PrivateFrameworks/MobileAccessoryUpdater.framework/Support/accessoryupdaterd 120
    0  1139     1   0 23Sep24 ??         6:20.82 /usr/libexec/configd
    0  1140     1   0 23Sep24 ??         0:00.59 endpointsecurityd
    0  1141     1   0 23Sep24 ??         9:10.34 /System/Library/CoreServices/powerd.bundle/powerd
    0  1142     1   0 23Sep24 ??         0:03.28 /usr/libexec/IOMFB_bics_daemon
  289  1143     1   0 23Sep24 ??         0:14.57 /System/Library/PrivateFrameworks/BiomeStreams.framework/Support/biomed
    0  1145     1   0 23Sep24 ??         0:07.04 /usr/libexec/amfid
    0  1147     1   0 23Sep24 ??         0:00.11 /usr/libexec/remoted
    0  1149     1   0 23Sep24 ??         0:00.25 /usr/libexec/keybagd -t 15
  200  1150     1   0 23Sep24 ??         0:04.12 /System/Library/PrivateFrameworks/MobileSoftwareUpdate.framework/Support/softwareupdated
    0  1152     1   0 23Sep24 ??         0:13.27 /usr/libexec/watchdogd
    0  1156     1   0 23Sep24 ??        36:46.29 /System/Library/Frameworks/CoreServices.framework/Frameworks/Metadata.framework/Support/mds
  240  1157     1   0 23Sep24 ??         0:00.85 /System/Library/CoreServices/iconservicesd
    0  1158     1   0 23Sep24 ??         0:01.41 /usr/libexec/kernelmanagerd
    0  1159     1   0 23Sep24 ??         0:21.68 /usr/libexec/diskarbitrationd
    0  1163     1   0 23Sep24 ??         6:42.78 /usr/libexec/coreduetd
    0  1164     1   0 23Sep24 ??         0:24.37 /usr/sbin/syslogd
    0  1167     1   0 23Sep24 ??         1:10.63 /usr/libexec/thermalmonitord
    0  1168     1   0 23Sep24 ??        10:25.93 /usr/libexec/opendirectoryd
    0  1169     1   0 23Sep24 ??         0:39.96 /System/Library/PrivateFrameworks/ApplePushService.framework/apsd
    0  1170     1   0 23Sep24 ??        16:51.49 /System/Library/CoreServices/launchservicesd
  266  1171     1   0 23Sep24 ??         0:14.94 /usr/libexec/timed
  213  1172     1   0 23Sep24 ??         0:02.45 /System/Library/PrivateFrameworks/MobileDevice.framework/Versions/A/Resources/usbmuxd -launchd
    0  1173     1   0 23Sep24 ??         0:41.94 /usr/sbin/securityd -i
    0  1178     1   0 23Sep24 ??         0:00.03 autofsd
    0  1179     1   0 23Sep24 ??         5:02.60 /usr/libexec/dasd
  241  1181     1   0 23Sep24 ??         2:19.80 /usr/sbin/distnoted daemon
    0  1182     1   0 23Sep24 ??         0:00.20 /System/Library/PrivateFrameworks/AppleCredentialManager.framework/AppleCredentialManagerDaemon
    0  1184     1   0 23Sep24 ??         0:00.03 /usr/libexec/dirhelper
    0  1185     1   0 23Sep24 ??         0:00.28 /System/Library/CoreServices/logind
```

El atacante procede a desactivar uno de los procesos de seguridad en el equipo, en este caso el proceso “Falcon”.

badmonkey.txt

```
1    pkill Falcon > subeme.txt
2
```

I. Anexo: Disminución de riesgos y materialización de incidentes cibernéticos para el sector financiero colombiano posterior a la implementación de la metodología ZT propuesta.

Controles actuales

0% = No se cuenta con controles
25% = Algunos controles controles están implementados, pero no funcionan adecuadamente o son limitados (no cubren todo el riesgo)
50% = todos los controles propuestos están implementados, pero no se valida su efectividad.
80%= Todos los controles están implementados, se verifican su efectividad, pero no se monitorea ni se hacen planes de mejora continua.
100%= La totalidad de controles están implementados, se miden, monitorean y se generan planes de acción para su mantenimiento (línas bases periódicas y auditorias).

Activos	Vulnerabilidades	Controles actuales implementados en el activo	Clasificación del activo	Efectividad de los controles = Eficiencia + Eficacia

Sistema core tarjetas (Débito/crédito)	Ausencia de parches de seguridad, Ausencia de actualizaciones permanente, Ausencia de entrenamiento en gestión segura de la infraestructura No se evidencia un control de navegación en los servidores Ausencia de logs para el monitoreo de seguridad del activo Ausencia de MFA para la autenticación en las estaciones Problemas de configuración Falta segmentación de red	**Autenticación multifactor (MFA) (Paso 3):** Implementación MFA para todas las estaciones de trabajo y puntos de acceso críticos, asegurando que solo usuarios autenticados puedan interactuar con el sistema. **Segmentación de red (Paso 4):** Implementación de políticas de microsegmentación para restringir el acceso a segmentos específicos de la red donde residen las aplicaciones core. **Actualizaciones automatizadas (Paso 5):** Configuración de parches automáticos y monitoreo continuo para garantizar que el sistema operativo y las aplicaciones estén protegidas frente a vulnerabilidades conocidas. **Control de navegación**	confidencial	80%

		(Pasos 4 y 7): Configurar reglas en firewalls y servidores para restringir el tráfico no autorizado. **Gestión de Configuraciones (Paso 8):** Revisión y corrección de configuraciones para eliminar problemas y asegurar conformidad con las políticas de seguridad. **Control de Acceso Basado en Identidad (Pasos 3 y 8):** Implementación de políticas de acceso condicional que permiten conexiones únicamente desde dispositivos seguros y usuarios verificados. **Monitoreo activo de seguridad (Paso 10):** Implementación de sistemas de gestión de logs para analizar en tiempo real el tráfico y los accesos no autorizados al sistema.		

Sistema core crediticios	CVE-2023-28298 En el kernel del SO - negación de servicio CVE-2016-7217 Permite a un atacante ejecutar código remoto No se evidencia una gestión de usuarios privilegiados Ausencia de entrenamiento en gestión segura de la infraestructura No se evidencia un control de navegación en los servidores Ausencia de MFA para la autenticación en las estaciones Problemas de configuración Falta segmentación de red	**Autenticación Basada en Dispositivos (Paso 3):** Validación de dispositivos administrados antes de otorgar acceso, bloqueando aquellos no conformes con la postura de seguridad. **Gestión de Identidades Privilegiadas (Paso 3):** Configuración de controles específicos para usuarios con privilegios, limitando su acceso y auditando sus actividades. **Segmentación del Sistema (Paso 4):** Microsegmentación para aislar la infraestructura de crédito, reduciendo el alcance de posibles ataques. **Mitigación de Vulnerabilidades Específicas (Paso 5):** Aplicación de parches críticos para	confidencial	80%

		vulnerabilidades como CVE-2023-28298 (negación de servicio) y CVE-2016-7217 (ejecución remota de código). **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrado avanzado de tráfico para prevenir accesos no autorizados. **Gestión de Configuraciones (Paso 8):** Revisión y corrección de configuraciones para eliminar problemas. **Registro y Auditoría de Actividades (Paso 10):** Implementación de logs centralizados para registrar cualquier actividad sospechosa y facilitar auditorías.		

Backend APP Movil	CVE-2021-3939 Permite obtener privilegios root y tomar control total de un servidor explotando error corrupción memoria en servicio de componente de cuentas GNOME CVE-2018-1092 permitir a un atacante bloquear un sistema vulnerable tras causar una denegación de servicio al montar un sistema de archivos EXT4 modificado para ello. No se evidencia una gestión de usuarios privilegiados No se evidencia un control de navegación en los servidores Ausencia de MFA para la autenticación en las estaciones Problemas de configuración	**Políticas Basadas en Roles (RBAC) (Pasos 3 y 8):** Restricciones de acceso basadas en los roles de usuarios y sus necesidades específicas. **Aislamiento de Entornos (Paso 4):** Aislamiento de las APIs y servicios móviles en redes específicas, limitando el acceso a través de políticas estrictas de segmentación. **Parches de Seguridad (Paso 5):** Corrección de vulnerabilidades críticas como CVE-2021-3939 (privilegios root) y CVE-2018-1092 (denegación de servicio), asegurando que el sistema operativo y las aplicaciones estén protegidos. **Validación Dinámica de Dispositivos (Paso 7):** Clasificación de dispositivos	confidencial	80%

	Falta segmentación de red	en "administrados" o "no administrados" basada en la presencia de herramientas de seguridad específicas, como antimalware o configuraciones de sistema aprobadas. **Control de Navegación en los Servidores (Pasos 4 y 7):** Configuración de firewalls para evitar conexiones salientes no autorizadas desde los servidores backend.		

Backend APP Web	CVE-2001-0867 Cisco 12000 with IOS 12.0 and line cards based on Engine 2 does not properly filter does not properly filter packet fragments even when the "fragment" keyword is used in an ACL, which allows remote attackers to bypass the intended access controls. Falta segmentación de red Plagas	**Acceso Controlado (Pasos 3 y 8):** Integración de conexiones a través de un agente ZTNA que verifica dispositivos y usuarios antes de otorgar acceso. **Segmentación Granular (Paso 4):** Aislamiento de la aplicación web backend de otras capas de la red mediante políticas de microsegmentación. **Control de Navegación (Pasos 4 y 7):** Configuración de firewalls para restringir tráfico no autorizado. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrado avanzado de tráfico. **Protección Contra Vulnerabilidades Críticas (Paso 5):** Actualización de configuraciones en dispositivos de red (como	confidencial	80%

		routers Cisco) para mitigar vulnerabilidades como CVE-2001-0867, asegurando que los controles ACL funcionen correctamente. **Gestión de Configuraciones (Paso 8):** Revisión y corrección de configuraciones para eliminar problemas. **Monitoreo de Actividades Web (Paso 10):** Análisis continuo de tráfico para identificar y bloquear intentos de explotación. **Monitoreo Activo de Seguridad (Paso 10):** Uso de SIEM para centralizar y analizar logs.		

Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo..)	CVE-2007-5419 El enrutador 3Com 3CRWER100-75 con software 1.2.10ww, cuando habilita un servidor virtual opcional, configura este servidor para aceptar todas las direcciones IP de origen en la interfaz externa (Internet), a menos que el usuario seleccione otras opciones, lo que podría exponer el enrutador a llamadas entrantes no deseadas. tráfico de atacantes remotos, como se demuestra al configurar un servidor virtual en el puerto 80, que permite a los atacantes remotos acceder a la interfaz de administración web.	**Validación de IPs de Origen (Pasos 3 y 4):** Configuración de controles para aceptar conexiones únicamente desde direcciones IP predefinidas o agentes ZTNA. **Segmentación en el Entorno Bancario (Paso 4):** Aislamiento de los sistemas de gestión bancaria en redes separadas, reduciendo la superficie de ataque. **Reforzamiento de Configuraciones del Enrutador (Paso 5):** Deshabilitación de configuraciones predeterminadas y restricciones estrictas para mitigar vulnerabilidades como CVE-2007-5419, que permitían accesos no autorizados al puerto 80. **Seguridad en la**	confidencial	80%

		Transmisión de Datos (Paso 7): Implementación de protocolos seguros como HTTPS/TLS para todas las comunicaciones relacionadas con información bancaria. **DLP y Cifrado (Paso 7):** Protección de datos financieros sensibles. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrado avanzado de tráfico. **Gestión de Configuraciones (Paso 8):** Revisión y corrección de configuraciones para eliminar problemas. **Control de Acceso Basado en Identidad (Pasos 3 y 8):** Implementación de políticas de acceso condicional que permiten conexiones únicamente desde dispositivos seguros		

		y usuarios verificados. **Monitoreo de Accesos Remotos (Paso 10):** Supervisión continua del tráfico entrante y saliente desde los servidores virtuales para identificar y mitigar actividades sospechosas. **Registro y Auditoría de Actividades (Paso 10):** Implementación de logs centralizados para registrar cualquier actividad sospechosa y facilitar auditorías.		

Clasificación con controles para objetivo 4

No.	Escenario de riesgos	PROBABILIDAD		IMPACTO INFORMACIÓN		Riesgo P*Impacto Cliente Mercado	Clasificación del activo	Controles Actuales del activo	Efectividad del control
(1)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema core tarjetas (Débito/crédito)	Posible	3	Mayor	4	12	confidencial	**Antimalware:** Implementación de soluciones antimalware robustas. **Monitoreo Continuo (Paso 3 y 9):** Detectar actividades anómalas. **Microsegmentación de Red (Paso 4):** Limitar movimiento lateral. **Actualizaciones Automáticas (Paso 5):** Mantener sistemas actualizados para prevenir vulnerabilidades. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrar tráfico malicioso.	80%

(2)	Posibilidad que la amenaza: Malware, afecte el activo: Sistema core crediticios	Posible	3	Mayor	4	12	confidencial	**Antimalware:** Protección avanzada contra malware. **Segmentación y Control de Acceso (Paso 4 y 3):** Restringir accesos y monitorizar tráfico. **Cifrado de Datos (Paso 7):** Asegurar la integridad y confidencialidad de los datos. **Inteligencia de Amenazas (Paso 9):** Integrar fuentes de inteligencia para identificar y bloquear malware.	80%
(3)	Posibilidad que la amenaza: Malware, afecte el activo: Backend APP Móvil	Posible	3	Intermedio	3	9	confidencial	**Antimalware en Dispositivos Móviles:** Soluciones antimalware instaladas. **Autenticación y IAM (Paso 3):** Asegurar que solo dispositivos confiables accedan. **Actualizaciones y Parches (Paso 5):**	80%

								Corregir vulnerabilidades. **Cifrado de Datos (Paso 7):** Proteger datos en tránsito. **Monitoreo Continuo (Paso 9):** Detectar comportamientos anómalos en la aplicación.	
(4)	Posibilidad que la amenaza: Malware, afecte el activo: Backend APP Web	Posible	3	Intermedio	3	9	confidencial	**Antimalware en Servidores Web:** Protección contra malware en servidores. **Ciclo de Vida de Desarrollo Seguro (SDLC):** Minimizar vulnerabilidades en el desarrollo. **Pruebas de Seguridad (Paso 3 y 5):** Identificar y corregir vulnerabilidades. **WAF y Seguridad de API (Paso 7):** Filtrar y proteger las interfaces de la aplicación. **Monitoreo y Respuesta (Paso 9):**	80%

								Detectar y responder a infecciones de malware rápidamente.	
(5)	Posibilidad que la amenaza: Malware, afecte el activo: Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo..)	Posible	3	Mayor	4	12	confidencial	**Antimalware en Sistemas de Almacenamiento: Protección de datos sensibles. Gestión de Accesos y IAM (Paso 3):** Limitar accesos a datos sensibles. **Segmentación de Red (Paso 4):** Aislar sistemas que manejan información bancaria. **DLP y Cifrado (Paso 7):** Prevenir la exfiltración de datos. **Monitoreo y Auditorías (Pasos 9 y 10):** Detectar y	80%

								registrar actividades sospechosas.	
(6)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Sistema core tarjetas (Débito/crédito)	Raro	1	Mayor	4	4	confidencial	**Gestión de Accesos (Paso 3):** Limitar permisos según roles específicos. **Microsegmentación de Red (Paso 4):** Limitar la comunicación entre segmentos. **Antimalware y Firewalls (Pasos 4 y 7):** Detectar y bloquear tráfico malicioso. **Políticas de Mínimo Privilegio (Pasos 7 y 8):** Restringir accesos innecesarios entre sistemas. **Monitoreo y Respuesta (Paso 9):** Identificar patrones de movimiento lateral.	80%

(7)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Sistema core crediticios	Raro	1	Mayor	4	4	confidencial	**Gestión de Accesos (Paso 3):** Asegurar que solo usuarios autorizados tengan acceso. **Segmentación y Control de Acceso (Pasos 4 y 3):** Aislar sistemas críticos. **Políticas de Acceso Granular (Pasos 7 y 8):** Minimizar privilegios de acceso entre sistemas. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 9):** Filtrar tráfico entre segmentos. **Monitoreo Continuo (Paso 9):** Detectar intentos de movimiento lateral.	80%

(8)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Backend APP Móvil	Raro	1	Intermedio	3	3	confidencial	**Antimalware en Dispositivos Móviles:** Protección contra malware. **Gestión de Accesos (Paso 3):** Restringir accesos según identidad y contexto. **Segmentación de Red (Paso 4):** Aislar el tráfico de la aplicación móvil. **Cifrado de Datos (Paso 7):** Proteger datos en tránsito. **Monitoreo de Actividades (Paso 9):** Detectar accesos inusuales desde dispositivos móviles.	80%

(9)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Backend APP Web	Raro	1	Intermedio	3	3	confidencial	**Microsegmentación (Paso 4):** Limitar el acceso desde la aplicación web a otros sistemas. **Pruebas de Seguridad (Paso 5):** Identificar y mitigar vulnerabilidades. **WAF y Seguridad de API (Paso 7):** Prevenir explotación de vulnerabilidades. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrar tráfico malicioso. **Monitoreo y Respuesta (Paso 9):** Detectar y bloquear intentos de movimiento lateral.	80%

(10)	Posibilidad que la amenaza: Movimiento lateral (Piboteo), afecte el activo: Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo..)	Raro	1	Intermedio	3	3	confidencial	**Políticas de Acceso Basadas en Roles (Pasos 3 y 8):** Restringir accesos según roles específicos. **Segmentación de Red (Paso 4):** Aislar sistemas que manejan información bancaria. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrar tráfico malicioso. **DLP y Cifrado (Paso 7):** Proteger datos sensibles. **Monitoreo y Respuesta (Paso 9):** Detectar movimientos laterales hacia sistemas de información bancaria.	80%

(11)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Sistema core tarjetas (Débito/crédito)	Posible	3	Superior	5	15	confidencial	**Gestión de Identidades y Accesos (Paso 3):** Implementar IAM robusto con MFA. **Clasificación de Dispositivos (Paso 3):** Asegurar que solo dispositivos administrados accedan. **Antimalware y Firewalls (Paso 7 y 4):** Prevenir accesos mediante protección contra malware. **Políticas de Autenticación Estrictas (Paso 8):** Verificar identidades de usuarios. **Monitoreo de Actividades (Paso 9):** Detectar accesos sospechosos.	80%
(12)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Sistema core crediticios	Posible	3	Superior	5	15	confidencial		80%

(13)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Backend APP Móvil	Posible	3	Intermedio	3	9	confidencial	**Autenticación Segura (Paso 3):** Implementar protocolos robustos. **Gestión de Identidades (Paso 3):** Verificar identidades de dispositivos. **Antimalware en Dispositivos Móviles (Paso 7):** Prevenir accesos mediante protección contra malware. **Control de Acceso Basado en Roles (Paso 8):** Restringir funcionalidades según identidades verificadas. **Monitoreo de Accesos (Paso 9):** Detectar intentos de acceso no autorizados.	80%

(14)	Posibilidad que la amenaza: Suplantación de identidad, afecte el activo: Backend APP Web	Posible	3	Intermedio	3	9	confidencial	**Autenticación y Autorización (Paso 3):** Implementar MFA y IAM. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrar tráfico malicioso. **WAF y Seguridad de API (Paso 7):** Prevenir suplantaciones a través de vulnerabilidades. **Políticas de Acceso Granular (Paso 8):** Limitar accesos según identidades verificadas. **Monitoreo y Auditoría (Paso 9 y 10):** Detectar y registrar accesos fraudulentos.	80%

(15)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Sistema core tarjetas (Débito/crédito)	Posible	3	Superior	5	15	confidencial	**IAM y MFA (Paso 3):** Controlar y verificar accesos. **Microsegmentación (Paso 4):** Restringir acceso a segmentos específicos. **Antimalware y Firewalls (Pasos 4 y 7):** Prevenir accesos mediante protección contra malware. **Políticas de Acceso Basadas en Roles (Paso 7 y 8):** Limitar accesos según necesidades laborales. **Monitoreo Continuo (Paso 9):** Detectar y alertar sobre accesos inusuales.	80%

(16)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Sistema core crediticios	Posible	3	Superior	5	15	confidencial	**IAM y MFA (Paso 3):** Controlar y verificar accesos. **Microsegmentación (Paso 4):** Restringir acceso a segmentos específicos. **Antimalware y Firewalls (Pasos 4 y 7):** Prevenir accesos mediante protección contra malware. **Monitoreo y Respuesta (Paso 9):** Identificar y bloquear accesos no autorizados. **Revisión y Auditoría (Paso 10):** Verificar accesos regularmente.	80%

(17)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Backend APP Movil	Posible	3	Intermedio	3	9	confidencial	**Autenticación Segura (Paso 3):** Verificar identidades. **Gestión de Dispositivos (Paso 7):** Asegurar que solo dispositivos autorizados accedan. **Antimalware en Dispositivos Móviles (Paso 7):** Prevenir accesos mediante protección contra malware. **Políticas de Acceso Granular (Paso 8):** Limitar accesos según roles y necesidades. **Monitoreo de Actividades (Paso 9):** Detectar intentos de acceso no autorizados.	80%

(18)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Backend APP Web	Posible	3	Intermedio	3	9	confidencial	**Autenticación y Autorización (Paso 3):** Implementar MFA. **Segmentación de Accesos (Paso 4):** Limitar el acceso a funcionalidades críticas. **WAF y Seguridad de API (Paso 7):** Prevenir accesos no autorizados. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrar tráfico malicioso. **Monitoreo y Auditoría (Paso 9 y 10):** Detectar y registrar accesos fraudulentos.	80%

(19)	Posibilidad que la amenaza: Acceso no autorizado, afecte el activo: Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo..)	Posible	3	Superior	5	15	confidencial	I**AM y MFA (Paso 3):** Controlar accesos estrictamente. **Firewalls de Próxima Generación (NGFW) (Pasos 4 y 7):** Filtrar tráfico malicioso. **Políticas de Mínimo Privilegio (Paso 7 y 8):** Limitar accesos a lo estrictamente necesario. **Monitoreo Continuo (Paso 9):** Detectar accesos no autorizados. **Auditorías Regulares (Paso 10):** Verificar y asegurar la integridad de los accesos.	80%
(20)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema core tarjetas (Débito/crédito)	Improbable	2	Superior	5	10	confidencial		0%
(21)	Posibilidad que la amenaza: Ransomware, afecte el activo: Sistema core crediticios	Improbable	2	Superior	5	10	confidencial		0%

(22)	Posibilidad que la amenaza: Ransomware, afecte el activo: Backend APP Móvil	Improbable	2	Intermedio	3	6	confidencial		0%
(23)	Posibilidad que la amenaza: Ransomware, afecte el activo: Backend APP Web	Improbable	2	Intermedio	3	6	confidencial		0%
(24)	Posibilidad que la amenaza: Ransomware, afecte el activo: Información bancaria (Débito/Crédito/libranzas/Crédito Vehículo..)	Improbable	2	Superior	5	10	confidencial		0%

J. ANEXO: MANIFESTACIÓN DE PARTICIPACIÓN EN LA DISTRIBUCIÓN DE ENCUESTA

MANIFESTACIÓN DE PARTICIPACION EN LA DISTRIBUCIÓN DE ENCUESTA

Medellin, 20 enero 2025

A quien corresponda,

Por medio del presente, manifiesto apoyé en la distribución de la encuesta de ciber riesgo utilizada para el desarrollo de la investigación titulada **"Metodología para el Control de Acceso a la Red Basado en Zero Trust en el Sector Financiero Colombiano"** que está efectuando el señor **Luis Andres Montoya Duffis** como parte del programa de maestría en la Institución Universitaria ITM.

Los datos asociados en esta encuesta fueron recolectados mediante el formulario creado por el estudiante la cual se ejecutó entre el **15 de mayo al 5 de junio**, utilizando un instrumento para la obtención de información relacionada con la **categorización e identificación de riesgos en el sector financiero.**

Dicho instrumento fue distribuido a una muestra de CISO's del sector financiero colombiano.

Atentamente,

Tatiana M. Gómez Sarmiento

Tatiana Marcela Gómez Sarmiento
Consultor de Seguridad de la Información y Ciberseguridad
Ingeniera de Sistemas
Certificaciones Auditor interno en sistemas de Gestión de la seguridad de la información, Ciberseguridad y protección de la Privacidad ISO/IEC 27001:2022, ISO 22301-2019 - SGS
Tatiana.gomez9310@gmail.com

MANIFESTACIÓN DE PARTICIPACION EN LA DISTRIBUCIÓN DE ENCUESTA

Medellin, 20 enero 2025

A quien corresponda,

Por medio del presente, manifiesto apoyé en la distribución de la encuesta de ciber riesgo utilizada para el desarrollo de la investigación titulada **"Metodología para el Control de Acceso a la Red Basado en Zero Trust en el Sector Financiero Colombiano"** que está efectuando el señor **Luis Andres Montoya Duffis** como parte del programa de maestría en la Institución Universitaria ITM.

Los datos asociados en esta encuesta fueron recolectados mediante el formulario creado por el estudiante la cual se ejecutó entre el **15 de mayo al 5 de junio**, utilizando un instrumento para la obtención de información relacionada con la **categorización e identificación de riesgos en el sector financiero.**

Dicho instrumento fue distribuido a una muestra de CISO's del sector financiero colombiano.

Atentamente,

Gustavo Díaz
Especialista de Seguridad de la Información y Ciberseguridad
Ingeniero de Sistemas, Harvard Leadership Program
Associate C-CISO, CRISC, CDPSE, CISA, ISO 27001 LA
Email: gdiazro@hotmail.com

MANIFESTACIÓN DE PARTICIPACION EN LA DISTRIBUCIÓN DE ENCUESTA

Medellin, 20 enero 2025

A quien corresponda,

Por medio del presente, manifiesto apoyé en la distribución de la encuesta de ciber riesgo utilizada para el desarrollo de la investigación titulada **"Metodología para el Control de Acceso a la Red Basado en Zero Trust en el Sector Financiero Colombiano"** que está efectuando el señor **Luis Andres Montoya Duffis** como parte del programa de maestría en la Institución Universitaria ITM.

Los datos asociados en esta encuesta fueron recolectados mediante el formulario creado por el estudiante la cual se ejecutó entre el **15 de mayo al 5 de junio**, utilizando un instrumento para la obtención de información relacionada con la **categorización e identificación de riesgos en el sector financiero.**

Dicho instrumento fue distribuido a una muestra de CISO's del sector financiero colombiano.

Atentamente,

Javier Gil Arango
Consultor de Seguridad de la Información y Ciberseguridad
Ingeniero de sistemas
Especialista en Gerencia de la Información
Certificado CBCP
Certificado ITIL
Metodologías ágiles y prueba
Javier.gil.arango@gmail.com

MANIFESTACIÓN DE PARTICIPACION EN LA DISTRIBUCIÓN DE ENCUESTA

Medellin, 20 enero 2025

A quien corresponda,

Por medio del presente, manifiesto apoyé en la distribución de la encuesta de ciber riesgo utilizada para el desarrollo de la investigación titulada "**Metodología para el Control de Acceso a la Red Basado en Zero Trust en el Sector Financiero Colombiano**" que está efectuando el señor **Luis Andres Montoya Duffis** como parte del programa de maestría en la Institución Universitaria ITM.

Los datos asociados en esta encuesta fueron recolectados mediante el formulario creado por el estudiante la cual se ejecutó entre el **15 de mayo al 5 de junio**, utilizando un instrumento para la obtención de información relacionada con la **categorización e identificación de riesgos en el sector financiero.**

Dicho instrumento fue distribuido a una muestra de CISO's del sector financiero colombiano.

Atentamente,

Diana Lorena Toro B. Date: 2025.01.22 08:10:11 -05'00'

Diana Toro
Especialista de Seguridad de la Información y Ciberseguridad
Ingeniera Electrónica.
Especialista en Seguridad de la información.
Master en Auditoría, Seguridad, Gobierno y Derecho de las TIC
Auditora Líder ISO 27001:2022, ITIL, Auditora interna continuidad del negocio ISO 22301, Gestor de Ciberseguridad ISO 27032, Oficial de Datos personales ISO 27018, PMP (Project Management Professional), Análisis de indicadores ISO 27004:2016, Datos personales ISO 270017:2019, Mentalidad Ofensiva.
dilotobe@gmail.com

Bibliografía

[1] P. Dhiman *et al.*, "A Review and Comparative Analysis of Relevant Approaches of Zero Trust Network Model," *Sensors*, vol. 24, no. 4, p. 1328, Feb. 2024, doi: 10.3390/s24041328.

[2] R. Prasad and V. Rohokale, "Cyber Threats and Attack Overview," 2020, pp. 15–31. doi: 10.1007/978-3-030-31703-4_2.

[3] C. Cunningham, "A Look Back At Zero Trust: Never Trust, Always Verify," Forrester. Accessed: Jun. 25, 2024. [Online]. Available: https://www.forrester.com/blogs/a-look-back-at-zero-trust-never-trust-always-verify/

[4] M. Saleem, M. R. Warsi, and S. Islam, "Secure information processing for multimedia forensics using zero-trust security model for large scale data analytics in SaaS cloud computing environment," *Journal of Information Security and Applications*, vol. 72, p. 103389, Feb. 2023, doi: 10.1016/j.jisa.2022.103389.

[5] E. Casildo and B. Corey, "The Total Economic Impact™ Of Zero Trust Solutions From Microsoft ," Cambridge, MA, Dec. 2021. Accessed: Apr. 17, 2024. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWRIEi

[6] Departamento Administrativo de la Función Pública, "Ley Estatuaria 1581 DE 2012." Accessed: Oct. 08, 2024. [Online]. Available: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

[7] International Business Machines (IBM), "Cost of a Data Breach Report 2023," 2023. Accessed: Jun. 25, 2024. [Online]. Available: https://www.ibm.com/reports/data-breach

[8] Inc. Proofpoint, *Managing Insider Threats in Financial Services*. 2021. Accessed: Jul. 01, 2024. [Online]. Available: https://www.proofpoint.com/au/resources/e-books/managing-insider-threats-in-financial-services

[9] Ponemon Institute, "2022 Cost of Insider Threats Global Report," Jan. 2022. Accessed: Jul. 01, 2024. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://protectera.com.au/wp-content/uploads/2022/03/The-Cost-of-Insider-Threats-2022-Global-Report.pdf

[10] Z. Musliyana, M. Dwipayana, A. Helinda, and Z. Maizi, "Improvement of Data Exchange Security on HTTP using Client-side Encryption," *J Phys Conf Ser*, vol. 1019, p. 012073, Jun. 2018, doi: 10.1088/1742-6596/1019/1/012073.

[11] O. Rudzeyt, U. Dobrzhinskii, and V. Titanov, "Vulnerability assessment of data transmission protocols in information systems," *Russian journal of resources, conservation and recycling*, vol. 9, no. 1, Mar. 2022, doi: 10.15862/16ITOR122.

[12] A. Ali and V. P. Singh, "Comparative Analysis of Transport Layer Security (TLS) Versions," *Int J Res Appl Sci Eng Technol*, vol. 11, no. 12, pp. 680–684, Dec. 2023, doi: 10.22214/ijraset.2023.57430.

[13] D. Dhingra, S. Ashok, and U. Kumar, “Demystifying Global Cybersecurity Threats in Financial Services,” 2021, pp. 181–202. doi: 10.4018/978-1-7998-6975-7.ch010.

[14] L. Ali, “Cyber Crimes-A Constant Threat For The Business Sectors And Its Growth (A Study Of The Online Banking Sectors In GCC),” *The Journal of Developing Areas*, vol. 53, no. 1, pp. 267–279, 2019, doi: 10.1353/jda.2019.0016.

[15] Anti-Phishing Working Group, “Phishing Attack Trends Report – 1Q 2024,” May 2024. Accessed: Jun. 25, 2024. [Online]. Available: https://apwg.org/trendsreports/

[16] Unit 42, “Si sabe qué buscan los atacantes, sabrá qué tiene que proteger más.,” 2022.

[17] C. M. Williams, R. Chaturvedi, and K. Chakravarthy, “Cybersecurity Risks in a Pandemic,” *J Med Internet Res*, vol. 22, no. 9, p. e23692, Sep. 2020, doi: 10.2196/23692.

[18] International Business Machines Corporation (IBM), “X-Force Threat Intelligence Index 2024,” Armonk, NY, Feb. 2024. Accessed: Jul. 02, 2024. [Online]. Available: https://www.ibm.com/reports/threat-intelligence

[19] Y. Pregonero and J. Rincon, “Informe Mensual de ciberseguridad, Reporte Mayo 2024,” Bogotá,Colombia, May 2024.

[20] D. Salazar Castellanos, “¿Por qué hay una ola de ciberataques en Colombia y el país está tan vulnerable?,” *Bloomberg Línea*, Jan. 25, 2023. Accessed: Jun. 25, 2024. [Online]. Available: https://www.bloomberglinea.com/2023/01/25/por-que-hay-una-ola-de-ciberataques-en-colombia-y-el-pais-aun-es-tan-vulnerable/#:~:text=Hasta%20finales%20de%20diciembre%20Colombia,al%20mismo%20per%C3%ADodo%20de%202021..

[21] F. Bautista García, L. Mesa Guzmán, and L. F. Blanco, “IA para la protección y Prevención de Amenazas. Informe Anual de Ciberseguridad. 2023,” 2023, Accessed: Jun. 25, 2024. [Online]. Available: https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

[22] D. Craigen, N. Diakun-Thibault, and R. Purse, “Defining Cybersecurity,” *Technology Innovation Management Review*, vol. 4, no. 10, pp. 13–21, Oct. 2014, doi: 10.22215/timreview/835.

[23] F. Schiliro, “Towards a Contemporary Definition of Cybersecurity,” *arXiv:2302.02274*, Feb. 2023, doi: https://doi.org/10.48550/arXiv.2302.02274.

[24] M. Warner, “Cybersecurity: A Pre-history,” *Intelligence and National Security*, vol. 27, no. 5, pp. 781–799, Oct. 2012, doi: 10.1080/02684527.2012.708530.

[25] K. Tarhan, “Historical Development of Cybersecurity Studies: A Literature Review and Its Place in Security Studies,” *Przeglqd Strategiczny*, no. 15, pp. 393–414, Feb. 2023, doi: 10.14746/ps.2022.1.23.

[26] K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, “Cybersecurity education: Evolution of the discipline and analysis of master programs,” *Comput Secur*, vol. 75, pp. 24–35, Jun. 2018, doi: 10.1016/j.cose.2018.01.015.

[27] B. Fonseca and J. D. Rosen, “Cybersecurity in the US: Major Trends and Challenges,” in *The New US Security Agenda*, Cham: Springer International Publishing, 2017, pp. 87–106. doi: 10.1007/978-3-319-50194-9_4.

[28] M. Veale and I. Brown, “Cybersecurity,” *Internet Policy Review*, vol. 9, no. 4, Dec. 2020, doi: 10.14763/2020.4.1533.

[29] R. J. Harknett and J. A. Stever, “The New Policy World of Cybersecurity,” *Public Adm Rev*, vol. 71, no. 3, pp. 455–460, May 2011, doi: 10.1111/j.1540-6210.2011.02366.x.

[30] C. M. Kahn and W. Roberds, “Credit and Identity Theft,” *SSRN Electronic Journal*, 2005, doi: 10.2139/ssrn.814026.
[31] S. Sproule and N. Archer, “Measuring identity theft and identity fraud,” *International Journal of Business Governance and Ethics*, vol. 5, no. 1/2, p. 51, 2010, doi: 10.1504/IJBGE.2010.029555.
[32] M. E. Johnson, “Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain,” *Journal of Management Information Systems*, vol. 25, no. 2, pp. 97–124, Sep. 2008, doi: 10.2753/MIS0742-1222250205.
[33] L. D. Roberts, D. Indermaur, and C. Spiranovic, “Fear of Cyber-Identity Theft and Related Fraudulent Activity,” *Psychiatry, Psychology and Law*, vol. 20, no. 3, pp. 315–328, Jun. 2013, doi: 10.1080/13218719.2012.672275.
[34] K. M. Hogan, G. T. Olson, J. D. Mills, and P. A. Zaleski, “An Analysis of Cyber Breaches and Effects on Shareholder Wealth,” *Int J Econ Bus*, vol. 30, no. 1, pp. 51–78, Jan. 2023, doi: 10.1080/13571516.2023.2168994.
[35] F. Cassim, “Protecting Personal Information in the Era of Identity Theft: Just how Safe is our Personal Information from Identity Thieves?,” *Potchefstroom Electronic Law Journal*, vol. 18, no. 2, pp. 68–110, Mar. 2015, doi: 10.4314/pelj.v18i2.02.
[36] M. M. KLEINER and M. L. BOUILLON, “Information Sharing of Sensitive Business Data with Employees,” *Industrial Relations: A Journal of Economy and Society*, vol. 30, no. 3, pp. 480–491, Sep. 1991, doi: 10.1111/j.1468-232X.1991.tb00800.x.
[37] E. B. Vered and I. A. Sementsova, “On the issue of strengthening the criminal and legal protection of employee personal data,” *Voprosy trudovogo prava (Labor law issues)*, no. 8, Aug. 2021, doi: 10.33920/pol-2-2108-03.
[38] J. Pavur and C. Knerr, “GDPArrrrr: Using Privacy Laws to Steal Identities,” Dec. 2019.
[39] I. DOROSH, “Cyber security and its role in the financial sector: threats and protection measures,” *Economics. Finances. Law*, vol. 10, no., pp. 48–51, Oct. 2023, doi: 10.37634/efp.2023.10.10.
[40] Z. Hassanzadeh, R. Biddle, and S. Marsen, “User Perception of Data Breaches,” *IEEE Trans Prof Commun*, vol. 64, no. 4, pp. 374–389, Dec. 2021, doi: 10.1109/TPC.2021.3110545.
[41] B. Schneier, “Risks of third-party data,” *Commun ACM*, vol. 48, no. 5, p. 136, May 2005, doi: 10.1145/1060710.1060744.
[42] M. D. White and C. Fisher, “Assessing Our Knowledge of Identity Theft,” *Crim Justice Policy Rev*, vol. 19, no. 1, pp. 3–24, Mar. 2008, doi: 10.1177/0887403407306297.
[43] T. J. Smedinghoff, “The State of Information Security Law: A Focus on the Key Legal Trends,” *EDPACS*, vol. 37, no. 1–2, pp. 1–52, Jan. 2008, doi: 10.1080/07366980701838449.
[44] F. Gogolin, I. Lim, and F. Vallascas, “Cyberattacks on Small Banks and the Impact on Local Banking Markets,” *SSRN Electronic Journal*, 2021, doi: 10.2139/ssrn.3823296.
[45] S. Goel and H. A. Shawky, “Estimating the market impact of security breach announcements on firm values,” *Information & Management*, vol. 46, no. 7, pp. 404–410, Oct. 2009, doi: 10.1016/j.im.2009.06.005.
[46] L. Tosoni, “Article 4(12). Personal data breach,” in *The EU General Data Protection Regulation (GDPR)*, Oxford University PressNew York, 2020, pp. 188–195. doi: 10.1093/oso/9780198826491.003.0018.
[47] J. Harvey, “The Financial Sector’s Vulnerabilities, Villains, and Options for Defense,” *Military Cyber Affairs*, vol. 3, no. 2, Dec. 2018, doi: 10.5038/2378-0789.3.2.1062.

[48] G. Strupczewski, “Defining cyber risk,” *Saf Sci*, vol. 135, p. 105143, Mar. 2021, doi: 10.1016/j.ssci.2020.105143.

[49] Organización de los Estados Americanos. and Asobancaria, “Estado de la ciberseguridad en el Sistema Financiero Colombiano,” 2020. Accessed: Apr. 15, 2024. [Online]. Available: www.oas.org/ext/DesktopModules/MVC/OASDnnModules/Views/Item/Download.aspx?type=1&id=732&lang=2

[50] Md. H. Uddin, Md. H. Ali, and M. K. Hassan, “Cybersecurity hazards and financial system vulnerability: a synthesis of literature,” *Risk Management*, vol. 22, no. 4, pp. 239–309, Dec. 2020, doi: 10.1057/s41283-020-00063-2.

[51] E. Kopp, L. Kaffenberger, and C. Wilson, “Cyber Risk, Market Failures, and Financial Stability,” *IMF Working Papers*, vol. 17, no. 185, Aug. 2017, doi: 10.5089/9781484313787.001.

[52] Ministerio de Tecnologías de la Información y las Comunicaciones (MINTEC), “Guía de Gestión de Riesgos - Guía No. 7 .” Accessed: Apr. 15, 2024. [Online]. Available: https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150516:Guia-de-gestion-de-riesgos

[53] International Organization for Standardization (ISO), “Information security, cybersecurity and privacy protection — Guidance on managing information security risks (ISO/IEC 27005:2022).,” Tech. rep. International Organization for Standardization (ISO).

[54] B. van, “The ZEro Trust Decision Making (ZEDEC) Method: Selecting Relevant Relevant Zero Trust Concepts to Mitigate High-Priority Risks,” Master’s Thesis, Utrecht University, Netherlands., 2023.

[55] MITRE, “MITRE ATT&CK Framework.” Accessed: Jun. 26, 2024. [Online]. Available: https://attack.mitre.org/

[56] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework,” *Sensors*, vol. 21, no. 9, p. 3267, May 2021, doi: 10.3390/s21093267.

[57] B. E. Strom, A. Applebaum, D. P. Miller, K. C. Nickels, A. G. Pennington, and C. B. Thomas, “MITRE ATT&CK®: Design and Philosophy,” 2018. Accessed: Jun. 26, 2024. [Online]. Available: https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy

[58] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, “SoK: The MITRE ATT&CK Framework in Research and Practice,” Apr. 2023.

[59] M. Metheny, “Applying the NIST risk management framework,” in *Federal Cloud Computing*, Elsevier, 2017, pp. 117–183. doi: 10.1016/B978-0-12-809710-6.00005-6.

[60] Joint Task Force, “Guide for applying the risk management framework to federal information systems : a security life cycle approach,” Gaithersburg, MD, Feb. 2010. doi: 10.6028/NIST.SP.800-37r1.

[61] M. Barrett *et al.*, “Approaches for federal agencies to use the cybersecurity framework,” Gaithersburg, MD, Mar. 2020. doi: 10.6028/NIST.IR.8170.

[62] C. Daah, A. Qureshi, I. Awan, and S. Konur, “Enhancing Zero Trust Models in the Financial Industry through Blockchain Integration: A Proposed Framework,” *Electronics (Basel)*, vol. 13, no. 5, p. 865, Feb. 2024, doi: 10.3390/electronics13050865.

[63] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero Trust Architecture,” Gaithersburg, MD, Aug. 2020. doi: 10.6028/NIST.SP.800-207.

[64] Gartner, “Execute on Zero Trust Principles to Improve Your Security and Risk Posture,” 2023. Accessed: Jul. 06, 2024. [Online]. Available: https://www.gartner.com/en/publications/zero-trust-principles-to-improve-security-playbook

[65] S. Teerakanok, T. Uehara, and A. Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” *Security and Communication Networks*, vol. 2021, pp. 1–10, May 2021, doi: 10.1155/2021/9947347.

[66] J. Kindervag, S. Balaouras, and lindsey Coit, “No More Chewy Centers: Introducing The Zero Trust Model of Information Security.,” Cambridge, USA, Sep. 2010. Accessed: Jul. 06, 2024. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[67] Zscaler, “Breve historia de la confianza cero: de la pizarra a la Casa Blanca,” San José, CA, 2022. Accessed: Jul. 06, 2024. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.zscaler.es/resources/infographics/brief-history-zero-trust.pdf

[68] Federal Register, “Executive Order 14028 of May 12, 2021 ,” *Fed Regist*, vol. 86, no. 93, pp. 26633–26647, May 2021, Accessed: Jul. 06, 2024. [Online]. Available: https://www.govinfo.gov/content/pkg/FR-2021-0517/pdf/2021-10460.pdf.

[69] S. D. Young, “Memorandum for the heads of executive departments and agencies,” Washington, D.C., Jan. 2021. Accessed: Jul. 06, 2024. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[70] Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, “Zero Trust Reference Architecture ,” United States of America, Sep. 2022. Accessed: Jul. 06, 2024. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[71] Agencia de Ciberseguridad y Seguridad de Infraestructura (Cybersecurity and Infrastructure Security Agency) and División de Ciberseguridad (Cybersecurity Division), “Modelo de madurez de confianza cero Version 2.0,” Apr. 2023. Accessed: Jul. 06, 2024. [Online]. Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cisa.gov/sites/default/files/2024-05/zero_trust_maturity_model_v2_508%20%281%29_ES.pdf

[72] M. Lemon, “Implementing Zero Trust: A Comprehensive Guide to Best Practices,” Nov. 21, 2023, *Linkedln*. Accessed: Apr. 15, 2024. [Online]. Available: https://www.linkedin.com/pulse/implementing-zero-trust-comprehensive-guide-best-matt-lemon-phd-emfze/

[73] R. M. Habash and M. Khalel, “Zero Trust Security Model for Enterprise Networks,” *Iraqi Journal of Information and Communication Technology*, vol. 6, no. 2, pp. 68–77, Jan. 2024, doi: 10.31987/ijict.6.2.223.

[74] D. Tyler and T. Viana, “Trust No One? A Framework for Assisting Healthcare Organisations in Transitioning to a Zero-Trust Network Architecture,” *Applied Sciences*, vol. 11, no. 16, p. 7499, Aug. 2021, doi: 10.3390/app11167499.

[75] Akamai, “How-To Guide: Zero Trust Security Transformation,” 2019, *Akamai*. Accessed: Apr. 15, 2024. [Online]. Available: www.akamai.com/site/en/documents/white-paper/how-to-guide-zero-trust-security-transformation.pdf

[76] Price Waterhouse Cooper (PwC), “Zero Trust architecture: a paradigm shift in cybersecurity and privacy,” Price Waterhouse Cooper (PwC), Singapore. Accessed: Apr. 15, 2024. [Online]. Available: www.pwc.com/sg/en/publications/assets/page/zero-trust-architecture.pdf

[77] N. L. Seymour, “Zero Trust Architectures: A Comprehensive Analysis and Implementation Guide,” Master of Science, The University of Memphis, Memphis, United States, 2023.

[78] E. B. Fernandez and A. Brazhuk, “A critical analysis of Zero Trust Architecture (ZTA),” *Comput Stand Interfaces*, vol. 89, p. 103832, Apr. 2024, doi: 10.1016/j.csi.2024.103832.

[79] S. M. Awan, M. A. Azad, J. Arshad, U. Waheed, and T. Sharif, “A Blockchain-Inspired Attribute-Based Zero-Trust Access Control Model for IoT,” *Information*, vol. 14, no. 2, p. 129, Feb. 2023, doi: 10.3390/info14020129.

[80] J. Blankenship *et al.*, “Manage Insider Risk With Zero Trust,” Jul. 2023. Accessed: Jun. 26, 2024. [Online]. Available: https://reprints2.forrester.com/#/assets/2/424/RES179512/report

[81] J. Kujo, “Implementing Zero Trust Architecture for Identities and Endpoints with Microsoft tools,” Master, Jamk University of Applied Sciences, Jyväskylä, Finlandia, 2023.

[82] Softeng, “¿Por qué tu empresa debería adoptar una estrategia de seguridad Zero Trust?,” Softeng. Accessed: Aug. 01, 2024. [Online]. Available: https://www.softeng.es/blog/por-que-tu-empresa-deberia-adoptar-una-estrategia-de-seguridad-zero-trust/

[83] J. Kindervag, S. Balaouras, and K. Mak, “BuildSecurity Into Your Network’s DNA: The Zero Trust Network Architecture.,” Nov. 2012. Accessed: Jun. 26, 2024. [Online]. Available: https://www.forrester.com/report/Build-Security-Into-Your-Networks-DNA-The-Zero-Trust-Network-Architecture/RES57047

[84] J. Kindervag, S. Balaouras, and lindsey Coit, “Build Security Into Your Network’s DNA: The Zero Trust Network Architecture,” Cambridge, MA, Nov. 2010. Accessed: Apr. 17, 2024. [Online]. Available: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf

[85] National Cyber Security Centre, “Zero trust architecture design principles,” Guidance. Accessed: Apr. 17, 2024. [Online]. Available: https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust

[86] A. Gunuganti, “Identity Based - Zero Trust,” *Journal of Artificial Intelligence, Machine Learning and Data Science*, vol. 1, no. 2, pp. 492–497, Jun. 2023, doi: 10.51219/JAIMLD/anvesh-gunuganti/133.

[87] Y. G. Wu, W. H. Yan, and J. Z. Wang, “Real identity based access control technology under zero trust architecture,” in *2021 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, IEEE, Aug. 2021, pp. 18–22. doi: 10.1109/ICWCSG53609.2021.00011.

[88] A. McQuaid, N. MacDonald, J. Watts, and R. Kaur, “Market Guide for Zero Trust Network Access,” Aug. 2023. Accessed: Apr. 17, 2024. [Online]. Available: https://www.netskope.com/lp-gartner-market-guide-for-zero-trust-network-access-sem?utm_source=google&utm_medium=paidsearch&utm_campaign=APAC-ZTNA&utm_agn=&utm_content=652826536515&utm_term=zero%20trust%20network%20access&campaignid=19901953584&agroupid=147651029516&utm_audience=kwd-

807062058887&matchtype=p&network=g&device=c&utm_placement=&gad_source=1&gclid=CjwKCAjw5v2wBhBrEiwAXDDoJSuRA5lE_mxV0xbwtFV_BNKEHZBpriu7Uc1dU47ckLBF5m7GwH6nBxoCu0MQAvD_BwE

[89] Google Cloud, "¿Qué es la seguridad de confianza cero?" Accessed: Apr. 15, 2024. [Online]. Available: https://cloud.google.com/learn/what-is-zero-trust?hl=es

[90] Microsoft, "¿Qué es el control de acceso?" Accessed: Apr. 15, 2024. [Online]. Available: https://www.microsoft.com/es-co/security/business/security-101/what-is-access-control

[91] O. Michael, "Access Control," *Cybersecurity*, Nov. 06, 2023. Accessed: Apr. 17, 2024. [Online]. Available: https://www.linkedin.com/pulse/access-control-olayenikan-michael-sdqtf/?trackingId=ARelcvhkQFegD8rohbq9DA%3D%3D

[92] J. E. Jaén Solorzáno, "Diseño e implementación del control de acceso a la red Cisco Identify Services Engine (ISE)," Maestría de Seguridad Informática Aplicad, Escuela Superior Politécnica del Litoral, Guayaquil, 2015.

[93] N. Magnus and S. Übelcaker, "Control de acceso a la red mediante IEEE 802.1X en redes cableadas," *Linux Magazine, nº 59*, pp. 43–49, 2010.

[94] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Med Inform Decis Mak*, vol. 20, no. 1, p. 256, Dec. 2020, doi: 10.1186/s12911-020-01275-y.

[95] G. Moore, J. Davies, B. Carter, A. Buck, and N. Adam, "Securing identity with Zero Trust." Accessed: Apr. 15, 2024. [Online]. Available: https://learn.microsoft.com/es-es/security/zero-trust/deploy/identity

[96] Dimensional Research, "Identity is the Zero Trust Keystone - A Global Survey of Security and IT Professionals," Oct. 2021. Accessed: Apr. 15, 2024. [Online]. Available: https://www.sailpoint.com/identity-library/identity-is-the-zero-trust-keystone/

[97] SailPoint, "Las identidades son el nuevo perímetro, así que asegúrese de que estén protegidas." Accessed: Apr. 15, 2024. [Online]. Available: https://www.sailpoint.com/es/solutions/zero-trust/#:~:text=vuelva%20a%20autenticarse.,%C2%BFPor%20qu%C3%A9%20Zero%20Trust%20se%20apoya%20en%20la%20identidad%3F,pertenencia%20a%20roles%20y%20grupos

[98] A. A. Aponte Agudelo, "Modelo de seguridad para plataformas IAAS de la empresa Virgin," Universidad Nacional Abierta y a Distancia - UNAD, Bogotá D.C, 2018. Accessed: Apr. 15, 2024. [Online]. Available: https://repository.unad.edu.co/handle/10596/22392

[99] G. Rodriguez Gahona, "Análisis comparativo de los modelos defensa en profundidad y mspi, para la implementación de la seguridad informática en el sector privado del país," Monografía, Universidad Nacional Abierta y a Distancia, Bogotá D.C, 2020. Accessed: Apr. 15, 2024. [Online]. Available: https://repository.unad.edu.co/handle/10596/38717

[100] A. Weinert, "Evolving Zero Trust - Lessons learned and emerging trends," Nov. 03, 2021, *Microsoft Corporation*.

[101] National Institute of Standards and Technology - NIST, "Back to Basics: What's multi-factor authentication - and why should I care?," Blog. Accessed: Apr. 17, 2024. [Online]. Available: https://www.nist.gov/blogs/cybersecurity-insights/back-basics-whats-multi-factor-authentication-and-why-should-i-care

[102] P. Andre de Vera, “What is Device Posture’s Role in Zero Trust?,” Twingate. Accessed: Aug. 01, 2024. [Online]. Available: https://www.twingate.com/blog/what-is-device-posture-zero-trust

[103] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, “Zero Trust Architecture (ZTA): A Comprehensive Survey,” *IEEE Access*, vol. 10, pp. 57143–57179, 2022, doi: 10.1109/ACCESS.2022.3174679.

[104] S. Teerakanok, T. Uehara, and A. Inomata, “Migrating to Zero Trust Architecture: Reviews and Challenges,” *Security and Communication Networks*, vol. 2021, pp. 1–10, May 2021, doi: 10.1155/2021/9947347.

[105] P. Phiayura and S. Teerakanok, “A Comprehensive Framework for Migrating to Zero Trust Architecture,” *IEEE Access*, vol. 11, pp. 19487–19511, 2023, doi: 10.1109/ACCESS.2023.3248622.

[106] Ponemon Institute, “Ponemon Institute Reveals 68% of Organizations Were Victims of Successful Endpoint Attacks in 2019,” *CISION PRWeb*, Jan. 29, 2020. Accessed: Aug. 01, 2024. [Online]. Available: https://www.prweb.com/releases/ponemon-institute-reveals-68-of-organizations-were-victims-of-successful-endpoint-attacks-in-2019-852268367.html

[107] L. Meng, D. Huang, J. An, X. Zhou, and F. Lin, “A continuous authentication protocol without trust authority for zero trust architecture,” *China Communications*, vol. 19, no. 8, pp. 198–213, Aug. 2022, doi: 10.23919/JCC.2022.08.015.

[108] B. Chen *et al.*, “A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture,” *IEEE Internet Things J*, vol. 8, no. 13, pp. 10248–10263, Jul. 2021, doi: 10.1109/JIOT.2020.3041042.

[109] Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, “A Survey on Zero Trust Architecture: Challenges and Future Trends,” *Wirel Commun Mob Comput*, vol. 2022, pp. 1–13, Jun. 2022, doi: 10.1155/2022/6476274.

[110] L. Alevizos, V. T. Ta, and M. Hashem Eiza, “Augmenting zero trust architecture to endpoints using blockchain: A <scp>state-of-the-art</scp> review,” *Security and Privacy*, vol. 5, no. 1, pp. 1–27, Jan. 2022, doi: 10.1002/spy2.191.

[111] J. J. Marín Valencia, A. Patiño Valencia, and J. C. Acevedo Bedoya, “Implementación de un sistema de seguridad perimetral informático usando VPN, firewall e IDS,” *Revista Universidad Católica de Oriente*, vol. 31, no. 45, pp. 84–99, Sep. 2020, doi: 10.47286/01211463.284.

[112] R. F. Barboza Gilces, A. O. Gallegos Vinces, and V. M. Contreras Arcos, “Implementación de un esquema de seguridad perimetral en la red de datos de una empresa de servicios financieros,” Maestría en Seguridad Informática Aplicada , Escuela superior politécnica del litoral, Guayaquil, 2017.

[113] J. Grady, “The evolution of ZTNA to fully support zero trust strategies,” May 11, 2022, *Palo Alto Networks*.

[114] International Business Machines Corporation (IBM), “Política y objetivos de seguridad.” Accessed: Apr. 17, 2024. [Online]. Available: https://www.ibm.com/docs/es/i/7.5?topic=ssw_ibm_i_75/rzaj4/rzaj40j0securitypolco.html

[115] Ministerio de Tecnologías de la Información y las Comunicaciones - MINTEC, “Elaboración de la política general de seguridad y privacidad de la información,” Bogotá, DC, 2016. Accessed: Apr. 17, 2024. [Online]. Available:

https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/150520:Elaboracion-de-la-politica-general-de-seguridad-y-privacidad-de-la-informacion

[116] B-Secure, "¿Qué es ZTNA (Zero Trust Network Access)?" Accessed: Apr. 15, 2024. [Online]. Available: https://www.b-secure.co/blog/que-ztna-zero-trust-network-access

[117] L. Almagro and S. Castro, *Desafíos del riesgo cibernético en el sector financiero para Colombia y América Latina*, 1st ed. OEA, Asobancaria, 2019. Accessed: Apr. 17, 2024. [Online]. Available: https://www.asobancaria.com/biblioteca/desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-colombia-y-america-latina/

[118] Cloudflare, "What is Zero Trust Network Access (ZTNA)?," Cloudflare. Accessed: Aug. 02, 2024. [Online]. Available: https://www.cloudflare.com/en-gb/learning/access-management/what-is-ztna/

[119] S. Kak, "Zero Trust Evolution & Transforming Enterprise Security," Master, California State University, San Marcos, 2022. Accessed: Aug. 02, 2024. [Online]. Available: https://scholarworks.calstate.edu/concern/theses/41687p91q?locale=it

[120] A. Hope, "COVID-19 pushed most firms to adopt zero trust security model, a new study found ," CPO Magazine. Accessed: Aug. 02, 2024. [Online]. Available: https://www.cpomagazine.com/cyber-security/covid-19-pushed-most-firms-to-adopt-zero-trust-security-model-a-new-study-found/#:~:text=More%20than%20three%2Dquarters%20(76,a%20Zero%20Trust%20security%20architecture.

[121] D. Koeppen, N. MacDonald, and J. Watts, "7 Effective Steps for Implementing Zero Trust Network Access," Oct. 2022. Accessed: Aug. 02, 2024. [Online]. Available: https://www.gartner.com/en/conferences/hub/identity-access-management-conferences/insights/implementing-zero-trust-network-access

[122] P. Lv, C. Sun, and Q. Li, "Research and Application of Grid Cloud Service Security Access Control Technology Based on Zero Trust Model," in *2023 International Conference on Data Science and Network Security (ICDSNS)*, IEEE, Jul. 2023, pp. 1–7. doi: 10.1109/ICDSNS58469.2023.10245681.

[123] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, "Security of Zero Trust Networks in Cloud Computing: A Comparative Review," *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 2022, doi: 10.3390/su141811213.

[124] K. Hatakeyama, D. Kotani, and Y. Okabe, "Zero Trust Federation: Sharing Context under User Control towards Zero Trust in Identity Federation," in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE, Mar. 2021, pp. 514–519. doi: 10.1109/PerComWorkshops51409.2021.9431116.

[125] A. McQuaid, N. MacDonald, J. Watts, and R. Kaur, "Market Guide for Zero Trust Network Access," Aug. 2023. Accessed: Aug. 02, 2024. [Online]. Available: https://www.gartner.com/en/documents/4632099

[126] A. Dhanaraj, "Putting Zero Trust Architecture into Financial Institutions," Cloud Security Alliance. Accessed: Jul. 31, 2024. [Online]. Available: https://cloudsecurityalliance.org/blog/2023/09/27/putting-zero-trust-architecture-into-financial-institutions

[127] A. Kennedy, “Adaptive Trust: Zero Trust Architecture in a Financial Services Environment,” Bank Policy Institute. Accessed: Jul. 31, 2024. [Online]. Available: https://bpi.com/adaptive-trust-zero-trust-architecture-in-a-financial-services-environment/

[128] S. Sarkar and M. Jahira, “The Evolution of Zero Trust in the Financial Sector: Strengthening Cybersecurity.” Accessed: Jun. 26, 2024. [Online]. Available: https://www.synpulse.com/en/insights/the-evolution-of-zero-trust-in-the-financial-sector-strengthening-cybersecurity#:~:text=Zero%20Trust%20symbolises%20a%20pivotal,sensitive%20financial%20data%20and%20systems.

[129] Dr. A. Deshpande, “Relevance of Zero Trust Network Architecture amidts and it’s rapid adoption amidts Work From Home enforced by COVID-19,” *Psychology and Education Journal*, vol. 58, no. 1, pp. 5672–5677, Jan. 2021, doi: 10.17762/pae.v58i1.2190.

[130] National Institute of Standards and Technology (NIST), “El Marco de Seguridad Cibernética (CSF) 2.0 del NIST,” Gaithersburg MD, Feb. 2024. doi: 10.6028/NIST.CSWP.29.spa.

[131] W. R. Simpson and F. Kevin E, “Network Segmentation and Zero Trust Architectures ,” in *Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE)*, Proceedings of the World Congress on Engineering, Ed., London, UK: Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE), Jul. 2021, pp. 201–206.

[132] T. L. Saaty, “Decision making with the analytic hierarchy process,” *International Journal of Services Sciences*, vol. 1, no. 1, p. 83, Jan. 2008, doi: 10.1504/IJSSCI.2008.017590.

[133] A. Ishizaka and A. Labib, “Review of the main developments in the analytic hierarchy process,” *Expert Syst Appl*, vol. 38, no. 11, pp. 14336–14345, Oct. 2011, doi: 10.1016/j.eswa.2011.04.143.

[134] M. Brunelli, *Introduction to the Analytic Hierarchy Process*, 1st ed. Cham: Springer International Publishing, 2015. doi: 10.1007/978-3-319-12502-2.

[135] O. S. Vaidya and S. Kumar, “Analytic hierarchy process: An overview of applications,” *Eur J Oper Res*, vol. 169, no. 1, pp. 1–29, Feb. 2006, doi: 10.1016/j.ejor.2004.04.028.

[136] T. L. Saaty and L. G. Vargas, *Models, Methods, Concepts & Applications of the Analytic Hierarchy Process*, 2nd ed., vol. 175. Boston, MA: Springer New York, NY, 2012. doi: 10.1007/978-1-4614-3597-6.

[137] W. Ho, “Integrated analytic hierarchy process and its applications – A literature review,” *Eur J Oper Res*, vol. 186, no. 1, pp. 211–228, Apr. 2008, doi: 10.1016/j.ejor.2007.01.004.

[138] E. Bandara, X. Liang, S. Shetty, R. Mukkamala, A. Rahman, and N. W. Keong, “Skunk — A Blockchain and Zero Trust Security Enabled Federated Learning Platform for 5G/6G Network Slicing,” in *2022 19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, IEEE, Sep. 2022, pp. 109–117. doi: 10.1109/SECON55815.2022.9918536.

[139] S. Sarkar, G. Choudhary, S. K. Shandilya, A. Hussain, and H. Kim, “Security of Zero Trust Networks in Cloud Computing: A Comparative Review,” *Sustainability*, vol. 14, no. 18, p. 11213, Sep. 2022, doi: 10.3390/su141811213.

[140] F. A. Qazi, “Study of Zero Trust Architecture for Applications and Network Security,” in *2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, IEEE, Dec. 2022, pp. 111–116. doi: 10.1109/HONET56683.2022.10019186.

[141] T. Vang and M. L. Lind, “Factors Influencing Cloud Computing Adoption in a Zero-Trust Environment,” *Res Sq*, pp. 1–31, Jul. 2023, doi: https://doi.org/10.21203/rs.3.rs-3152878/v1.
[142] H. Vargas *et al.*, “Financial Infrastructure Report 2023,” Bogotá, Colombia, Dec. 2023. doi: 10.32468/rept-sist-pag.eng.2023.
[143] H. A. Rivera Rodríguez, A. Vanegas, R. D. Suarez, and A. L. Parra Pérez, “Turbulencia Empresarial en Colombia: Caso Sector Financiero ,” *SSRN Electronic Journal*, no. 81, pp. 2–29, Nov. 2010, doi: 10.2139/ssrn.1698979.
[144] A. Puchta, F. Böhm, and G. Pernul, “Contributing to Current Challenges in Identity and Access Management with Visual Analytics,” in *Data and Applications Security and Privacy XXXIII*, vol. 11559, S. N. Foley, Ed., springer, Cham, 2019, pp. 221–239. doi: 10.1007/978-3-030-22479-0_12.
[145] L. Wang, Y. Chen, T. Wu, and S. Hu, “A Practice of Zero Trust Architecture in Financial Transactions,” *International Journal of Information and Communication Engineering*, vol. 17, no. 12, pp. 692–698, 2023.
[146] M. Ramírez, L. Rodríguez Ariza, M. E. Gómez Miranda, and Vartika, “The Disclosures of Information on Cybersecurity in Listed Companies in Latin America—Proposal for a Cybersecurity Disclosure Index,” *Sustainability*, vol. 14, no. 3, p. 1390, Jan. 2022, doi: 10.3390/su14031390.
[147] Superintendencia Financiera de Colombia (SFC), “Circular Externa 022 de 2010: Seguridad y Calidad de Información, Requerimientos Mínimos y Modelos Tecnológicos,” Bogotá, Colombia, Sep. 2011.
[148] Fortinet, “2H 2023 Global Threat Landscape Report,” Sunnyvale, California, May 2024. Accessed: Jul. 01, 2024. [Online]. Available: https://www.fortinet.com/search?q=2H+2023+Global+Threat+Landscape+Report
[149] C. Winckless, T. Lintemuth, and D. Koeppen, “Magic Quadrant for Security Service Edge.,” Apr. 2024. Accessed: Jun. 26, 2024. [Online]. Available: https://www.gartner.com/doc/reprints?id=1-2HBI6A0S&ct=240417&st=sb
[150] D. Holmes, “The Forrester Wave™: Security Service Edge Solutions, Q1 2024. ,” Mar. 2024. Accessed: Jun. 26, 2024. [Online]. Available: https://reprints2.forrester.com/#/assets/2/2602/RES180561/report
[151] S. Turner, C. Cunningham, J.Blankenship, S. Balaouras, A. Tatro y P. Dostie, “The Zero trust eXtended Ecosystem: Networks” Forrester, 2021