ZERO TRUST: UNA SOLUCIÓN PARA LA CIBERSEGURIDAD EN EMPRESAS COLOMBIANAS

BRAYAN ARLEY CRUZ SENDOYA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

ZERO TRUST: UNA SOLUCIÓN PARA LA CIBERSEGURIDAD EN EMPRESAS COLOMBIANAS

BRAYAN ARLEY CRUZ SENDOYA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

Joel Carroll Vargas
Director de Trabajo de Grado

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2024

NOTA DE ACEPTACIÒN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, 12 de diciembre del 2024

DEDICATORIA

Dedico esta monografía a mis padres, Timon, Laura y Angie, quienes siempre han sido un pilar fundamental. Agradezco su apoyo, amor y paciencia, que han sido un impulso durante todo el proceso de construcción de este trabajo, permitiéndome culminar con éxito esta etapa de mi vida.

AGRADECIMIENTOS

Quiero expresar mi gratitud a los tutores y directores de curso, quienes, con sus conocimientos transmitidos, han contribuido a mi crecimiento profesional en el área de la seguridad informática.

Agradezco a DISAN LATAM, en especial a Gabriel Gutiérrez y Diego Orozco, gerentes corporativos de tecnología, quienes, por medio de su apoyo y confianza, han contribuido a mi desarrollo intelectual y profesional.

A todas las personas mencionadas y a aquellas que, de alguna u otra manera, han dejado huella a lo largo de mi vida, dedico este trabajo. Sin su apoyo e influencia, no habría podido llegar hasta aquí.

Por último, quiero agradecer a todas las fuentes bibliográficas y académicas consultadas, que han sido fundamentales para enriquecer mi conocimiento en Zero Trust.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

Pág.

GLOSARIO

AISLAMIENTO DE RED: Como dice CloudFlare[1]**,** Es la práctica de separar segmentos de red o sistemas en entornos aislados para reducir la propagación de amenazas y limitar el acceso no autorizado.

ATRIBUCIÓN DE CONTEXTO: Como dice el Departamento de Defensa de los estados unidos[2], El proceso de recopilar y evaluar información sobre el usuario, dispositivo, ubicación y contexto antes de permitir el acceso a un recurso o servicio.

AUTENTICACIÓN MULTIFACTOR (MFA): Como dice Microsoft[3], Un método de autenticación que requiere que los usuarios proporcionen más de un factor de autenticación para verificar su identidad.

AUTENTICACIÓN SIN CONTRASEÑA: Un método de autenticación que elimina la dependencia exclusiva de las contraseñas para verificar la identidad de los usuarios.

CONTROL DE ACCESO BASADO EN POLÍTICAS: "Una política de control de acceso es un conjunto de condiciones que, una vez evaluadas, determinan las decisiones de acceso"[4]. La aplicación de políticas de seguridad que definen qué usuarios, dispositivos o aplicaciones tienen permiso para acceder a recursos específicos.

EVALUACIÓN DE CONFIANZA CONTINUA: Es un concepto que define la evaluación y verificación periódica de la confiabilidad de usuarios, dispositivos y aplicaciones a medida que interactúan con los recursos de la red. "El enfoque de confianza cero es evaluar constantemente todas las transacciones"[5].

---

[1] CLOUDFLARE | Seguridad Zero Trust. [Anónimo]. Cloudflare [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

[2] DEPARTMENT OF defense Zero Trust Overlays [Anónimo]. (Junio, 2024). [Consultado el 4, mayo, 2024]. Disponible en Internet: https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf.

[3] EVOLVING ZERO Trust [Anónimo]. Microsoft [página web]. (Noviembre, 2021). [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT.

[4] IBM SECURITY Verify Access [Anónimo]. IBM - United States [página web]. [Consultado el 27, junio, 2024]. Disponible en Internet: https://www.ibm.com/docs/es/sva/10.0.8?topic=administration-access-control-policies.

[5] ¿QUÉ ES Zero Trust? [Anónimo]. Trend Micro [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.trendmicro.com/es_es/what-is/what-is-zero-trust.html.

MICROSEGMENTACIÓN: Según lo especifica uno de Palo Alto Networks[6], Es Técnica de seguridad que divide una red en segmentos más pequeños y controla el tráfico entre ellos mediante políticas de seguridad granulares.

POLÍTICA DE CONFIANZA MÍNIMA: Es un término que define el principio de seguridad que establece que los usuarios y dispositivos solo deben tener los permisos y accesos mínimos necesarios para realizar su trabajo.

SUPERVISIÓN CONTINUA: Como dice WatchGuard[7]**,** El monitoreo constante de usuarios, dispositivos y actividades en tiempo real para detectar y responder a cualquier comportamiento anómalo o indicio de amenazas.

ZERO TRUST (CONFIANZA CERO): "Zero Trust es un modelo de seguridad basado en el principio de mantener controles de acceso estrictos y no confiar en nadie por defecto, ni siquiera en los que ya están dentro del perímetro de la red"[8].

[6] ¿QUÉ ES la microsegmentación? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 21, septiembre, 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cyberpedia/what-is-microsegmentation.

[7] QUÉ PODEMOS esperar de un enfoque Zero Trust | WatchGuard Technologies [Anónimo]. WatchGuard | Comprehensive Cybersecurity Solutions [página web]. [Consultado el 19, junio, 2024]. Disponible en Internet: https://www.watchguard.com/es/wgrd-news/blog/que-podemos-esperar-de-un-enfoque-zero-trust.

[8] CLOUDFLARE | Seguridad Zero Trust. [Anónimo]. Cloudflare [página web]. [Consultado el 10, abril, 2023]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

RESUMEN

A lo largo del tiempo, y más específicamente en los últimos años, diversas empresas, tanto pequeñas como medianas, han enfrentado dificultades debido a la falta de profesionales, concienciación e inversión en el ámbito de la ciberseguridad. Esto ha obstaculizado el crecimiento y la adopción del modelo de confianza cero (Zero Trust) en Colombia. Esta situación no se corresponde con el aumento de la frecuencia de ciberataques. Ante la necesidad de reducir los riesgos organizacionales, se ha impulsado el crecimiento del enfoque de seguridad Zero Trust, el cual emplea numerosos controles y principios de seguridad para abordar los distintos desafíos mediante técnicas preventivas diseñadas para ofrecer una protección avanzada contra las amenazas.

Con la desaparición de la distinción entre el trabajo en un lugar fijo y el trabajo desde cualquier ubicación, especialmente tras el impulso del teletrabajo durante la pandemia, cada vez más empleados trabajan de manera distribuida y remota, convirtiendo esta modalidad en algo habitual. El enfoque de seguridad Zero Trust se aplica en diversas áreas de la empresa, abarcando dispositivos y datos, y llevando a cabo una validación exhaustiva de toda la actividad de los usuarios dentro de la organización. Este modelo consiste en implementar políticas que impiden acciones no permitidas o no verificadas, utilizando la microsegmentación de software para proporcionar a los equipos de seguridad empresarial la agilidad necesaria para modificar políticas de manera rápida y efectiva, cumpliendo de la mejor forma posible con los requisitos de las empresas colombianas que buscan evolucionar continuamente en su ciberseguridad.

En esta monografía, se realiza una revisión sistemática que reconoce los conceptos y principios de Zero Trust, brindando información y recomendaciones para las empresas colombianas interesadas en adquirir e implementar este enfoque. El objetivo es minimizar el riesgo de amenazas internas y externas, manteniendo la integridad y confidencialidad de la información y de los sistemas de la organización. Esta investigación contribuye a la comprensión y adaptación del modelo Zero Trust, proporcionando información práctica y relevante para aquellas empresas colombianas que desean fortalecer su seguridad cibernética.

Palabras Clave: Ciberseguridad, Confianza Cero, Zero Trust, Empresas Colombianas, Teletrabajo, Microsegmentación, Amenazas internas, Amenazas externas, Protección de la información, Evolución de la ciberseguridad.

ABSTRACT

Over time, and more specifically in recent years, various companies, both small and medium-sized, have faced challenges due to the lack of professionals, awareness, and investment in the field of cybersecurity. This has hindered the growth and adoption of the Zero Trust model in Colombia. This situation does not align with the increasing frequency of cyberattacks. Given the need to reduce organizational risks, the growth of the Zero Trust security approach has been promoted, employing numerous security controls and principles to address various challenges through preventive techniques designed to provide advanced protection against threats.

With the disappearance of the distinction between working in a fixed location and working from anywhere, especially after the boost in remote work driven by the pandemic, an increasing number of employees are working in distributed and remote environments, making this mode of work more common. The Zero Trust security approach is applied in various areas of the company, covering devices and data, and conducting thorough validation of all user activities within the organization. This model involves implementing policies that prevent unapproved or unverified actions, using software micro-segmentation to provide corporate security teams with the agility needed to quickly and effectively adjust policies, meeting the requirements of Colombian companies seeking to continuously evolve their cybersecurity.

In this monograph, a systematic review is conducted that acknowledges the concepts and principles of Zero Trust, providing information and recommendations for Colombian companies interested in adopting and implementing this approach. The goal is to minimize the risk of internal and external threats, maintaining the integrity and confidentiality of the organization’s information and systems. This research contributes to the understanding and adaptation of the Zero Trust model, offering practical and relevant information to those Colombian companies aiming to strengthen their cybersecurity.

Keywords: Cybersecurity, Zero Trust, Colombian companies, Remote work, Micro-segmentation, Internal threats, External threats, Information protection, Cybersecurity evolution.

INTRODUCCIÓN

En la era digital, en la que la información de los sistemas críticos se encuentra bajo una amenaza constante, la seguridad se ha convertido en una preocupación esencial para cualquier tipo de sector. Los enfoques tradicionales de seguridad ya no son suficientes ante los sofisticados ataques y la evolución de las amenazas cibernéticas, especialmente en los entornos híbridos corporativos, “Zero Trust tiene como objetivo minimizar y reducir su superficie de ataque mediante la implementación de estrictos controles de acceso, monitoreo continuo y autenticación de múltiples factores”[9]. Frente a este contexto, surge el concepto de confianza cero (Zero Trust), un enfoque de ciberseguridad que, gracias a su flexibilidad, ha ganado nuevos adeptos.

El enfoque de Zero Trust rompe con los paradigmas antiguos, donde el acceso a una red organizacional implicaba confianza automática en cualquier identidad. Este enfoque desconfía constantemente, asumiendo que cualquier usuario o dispositivo en la red puede ser un atacante potencial o estar comprometido. Bajo este enfoque, se requiere autenticación y autorización continua y granular, así como una verificación constante para asegurar la integridad y seguridad de los recursos y activos de la red. El objetivo principal de Zero Trust es proteger los diferentes activos de una organización mediante el establecimiento de controles y medidas de seguridad basadas en el contexto, el comportamiento y la segmentación. Como dice Torres[10], Al aplicar este enfoque, se implementan controles de acceso granulares y políticas de seguridad adaptativas que garantizan que usuarios y dispositivos solo accedan a los recursos necesarios según su identidad, contexto y comportamiento, promoviendo así una mayor visibilidad y un análisis continuo para detectar posibles anomalías en tiempo real.

La presente monografía tiene como objetivo comprender en profundidad el enfoque de Zero Trust, basado en una revisión sistemática de documentación que apoye el entendimiento de los fundamentos teóricos de Zero Trust, su arquitectura y componentes clave, con el fin de generar una guía de implementación para las empresas colombianas. Asimismo, se validarán las diferentes tecnologías que habilitan este enfoque, sus beneficios y desafíos, además de la normatividad aplicable, evaluando el impacto y los beneficios potenciales de acuerdo con las necesidades de la era digital.

---

[9] GUÍA DE seguridad Zero Trust para la empresa digital - SafePaaS [Anónimo]. SafePaaS [página web]. [Consultado el 21, septiembre, 2024]. Disponible en Internet: https://www.safepaas.com/es/articles/zero-trust-security-guide-for-the-digital-enterprise/.

[10] INCREMENTO DE ciberataques en Colombia demanda estrategia Zero Trust [Anónimo]. Tecnogus [página web]. [Consultado el 28, febrero, 2023]. Disponible en Internet: https://www.tecnogus.com.co/incremento-de-ciberataques-en-colombia-demanda-estrategia-zero-trust/.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

En Colombia, la ciberseguridad se ha convertido en un tema sensible, especialmente ante escenarios en los que, debido a ciberataques, se han visto comprometidos servicios hospitalarios, servicios públicos, grandes empresas, pequeñas empresas. ”El primero en noviembre de 2022, cuando Ransomhouse robó datos clasificados del Grupo Keralty; el segundo en septiembre de 2023 cuando IFX Networks sufrió un ataque que afectó a cerca de 760 entidades públicas y privadas”[11].

Como dice el balance de ciberseguridad del Centro Cibernético de la Policía Nacional[12], durante el año 2022 se registraron aproximadamente 65.000 denuncias en dicha entidad, lo que refleja un aumento en los problemas relacionados con la ciberseguridad, particularmente después de la pandemia. Como dice Cisco[13], este periodo impulsó el trabajo desde casa o en modalidad híbrida, lo que ha dado mayor relevancia a la seguridad en las empresas. En este contexto, el enfoque de seguridad Zero Trust se presenta como una alternativa innovadora que reduce los riesgos de ciberataques y protege los activos cibernéticos de las organizaciones. Ante este panorama, se requiere un marco estratégico de seguridad que enfrente los retos de las empresas, las cuales deben adoptar estrategias de ciberseguridad acordes con la nueva realidad organizacional.

Como dice Akamai Technologies[14], El modelo Zero Trust minimiza el riesgo de que objetos maliciosos afecten un perímetro protegido y, una vez dentro, se muevan para extraer datos. Además, garantiza decisiones dinámicas de seguridad en el acceso, basadas en la identidad, los dispositivos y el contexto del usuario.

---

[11] OBANDO, Jairo. Ciberseguridad en Colombia: panorama completo de su estado en 2023 – Linktic. Linktic [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia.

[12] BALANCE DE CIBERSEGURIDAD 2022 [Anónimo]. Inicio | CAI Virtual [página web]. [Consultado el 27, marzo, 2024]. Disponible en Internet: https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf.

[13] ESTUDIO GLOBAL del trabajo híbrido de Cisco, 2022 [Anónimo]. Cisco: Software, Network, and Cybersecurity Solutions - Cisco [página web]. [Consultado el 15, noviembre, 2023]. Disponible en Internet: https://www.cisco.com/c/dam/global/es_mx/solutions/collateral/hybrid-work/hybrid-work-study-market-factsheet.pdf.

[14] MODELO DE seguridad Zero Trust [Anónimo]. Akamai [página web]. [Consultado el 18, septiembre, 2024]. Disponible en Internet: https://www.akamai.com/es/glossary/what-is-zero-trust.

Zero Trust ha ganado tanta relevancia como herramienta de protección en ciberseguridad, Como dice la orden ejecutiva 14028[15], en mayo del 2021, Estados Unidos aprobó su implementación en el gobierno, lo que subraya la importancia de avanzar hacia una arquitectura Zero Trust. Esto ha motivado a empresas tanto públicas como privadas a seguir este enfoque.

Como dice Forbes Colombia[16], En el caso de Colombia, sin embargo, la falta de profesionales en ciberseguridad y de especialistas en la implementación y adopción de Zero Trust, junto con la carencia de concienciación e inversión en esta área, han dificultado la comprensión y adopción del modelo Zero Trust en las empresas colombianas y en Latinoamérica.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo se puede implementar el enfoque de seguridad Zero Trust en las organizaciones colombianas para mejorar su postura de seguridad ante las amenazas cibernéticas?

[15] EXECUTIVE ORDER 14028: Improving the Nation's Cybersecurity [Anónimo]. U.S. General Services Administration [página web].]. [Consultado el 19, septiembre, 2024]. Disponible en Internet: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028.

[16] LÓPEZ AGUDELO, David. Universal Zero Trust: la estrategia clave para enfrentar la nueva realidad de ciberseguridad. Forbes Colombia [página web].]. [Consultado el 22, agosto, 2024]. Disponible en Internet: https://forbes.co/2024/08/22/negocios/universal-zero-trust-la-estrategia-clave-para-enfrentar-la-nueva-realidad-de-ciberseguridad.

2. JUSTIFICACIÓN

Con el fin de preservar su información, las empresas buscan la mejor manera de garantizar la fiabilidad y la integridad de sus datos, evitando incidentes de seguridad que puedan afectar la credibilidad comercial de la organización, impactando directamente la continuidad del negocio y su crecimiento. “Alrededor de 2003, las ideas que llevaron a la confianza cero comenzaron a rebotar dentro del Departamento de Defensa de EE. UU., lo que llevó a un informe de 2007. Aproximadamente al mismo tiempo, un grupo informal de expertos en seguridad de la industria llamado Foro de Jericó acuñó el término «desperímetro», Kindervag cristalizó el concepto y le dio un nombre en su informe de septiembre de 2010”[17]. El enfoque de confianza cero tiene más de diez años de antigüedad, pero debido a los recientes incidentes en diferentes tipos de organizaciones, ha experimentado un crecimiento exponencial, que se espera continúe en el futuro. “Un reciente reporte del Índice de Inteligencia de Amenazas X-Force de IBM para 2024 ha informado sobre una creciente crisis de identidad global a medida que los cibercriminales explotan cada vez más las identidades de los usuarios para comprometer empresas en todo el mundo”[18], El modelo Zero Trust se centra en la prevención y en la suposición de ataque, considerando que los ataques pueden provenir no solo del exterior, sino también desde dentro de la propia organización.

Como dice Carrillo[19],La nueva realidad de los trabajadores, quienes antes estaban confinados a un único lugar y ahora operan desde sus hogares u otros entornos, hace urgente que las empresas refuercen su seguridad cibernética. Los entornos domésticos no ofrecen los mismos niveles de seguridad que las instalaciones empresariales, lo que los convierte en puntos vulnerables que los ciberdelincuentes pueden aprovechar para acceder a redes corporativas.

La confianza cero puede ayudar a las empresas colombianas a enfrentar los nuevos y emergentes desafíos en el ámbito de la ciberseguridad. Además, ofrece herramientas para mejorar la seguridad organizacional y limitar el alcance de los daños en caso de una brecha de seguridad. Como dice Microsoft[20], Incluso si una

[17] MERRITT, Rick. ¿Qué Es Zero-Trust? - Blog oficial de NVIDIA Latino América. Blog oficial de NVIDIA Latino América [blog].]. [Consultado el 28, octubre, 2022]. Disponible en Internet: https://la.blogs.nvidia.com/blog/que-es-zero-trust/.

[18] COLOMBIA SIGUE siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM [Anónimo]. Forbes Colombia [página web]. (28, febrero, 2024). [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica.

[19] LA SEGURIDAD Zero-Trust como garantía del trabajo remoto e híbrido - Artículo para Asociación @aslan [Anónimo]. Asociación @aslan [página web].]. [Consultado el 16, mayo, 2023]. Disponible en Internet: https://aslan.es/la-seguridad-zero-trust-como-garantia-del-trabajo-remoto-e-hibrido/.

[20] INFORMACIÓN GENERAL sobre el marco de adopción de Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 16, abril, 2024].

empresa no logra adoptar completamente el enfoque de confianza cero de manera inmediata, su flexibilidad permite una implementación gradual, ajustada a las necesidades actuales, lo que facilita la adaptación de la seguridad a futuro.

Colombia, como potencia en diversas industrias, tanto a nivel nacional como internacional, puede beneficiarse del análisis sistemático de este enfoque de seguridad cero a través de estudios como la monografía. Esta investigación brinda una guía práctica para aquellas empresas colombianas preocupadas por la ciberseguridad, proporcionando conocimientos y herramientas accesibles para defenderse de los ataques que ocurren a diario, basándose en la implementación del modelo Zero Trust, y anticipándose a interrupciones en sus operaciones.

Como dice IBM[21],El desarrollo de un escenario de preparación basado en la confianza cero posiciona a las empresas colombianas al nivel de organizaciones en otros países, fortaleciendo la base de seguridad cibernética y potenciando su capacidad de generar oportunidades para los residentes del país. A través de una revisión sistemática, las empresas pueden adquirir los conocimientos necesarios para implementar Zero Trust de manera exitosa, sentando una base sólida que sirva como ejemplo y motivación para cualquier tipo de organización en Colombia.

Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/adopt/zero-trust-adoption-overview.

[21] IBM. ¿Qué es Zero Trust? | IBM. IBM - United States [página web].]. [Consultado el 20, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Proponer una guía del enfoque de seguridad Zero Trust, por medio de una revisión sistemática de literatura, facilitando la comprensión, planificación e implementación de Zero Trust en las organizaciones colombianas.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar una revisión sistemática de la literatura sobre el enfoque Zero Trust, metodologías, herramientas de seguridad informática.

- Determinar las metodologías de seguridad Zero Trust existentes, identificando su aplicabilidad y efectividad en el contexto de las organizaciones colombianas, con el objetivo de recomendar las más adecuadas para su implementación.

- Desarrollar una guía de implementación basada en conjunto de enfoques para orientar la implementación efectiva del modelo Zero Trust en las organizaciones colombianas, debió a la necesidad de fortalecer la postura de ciberseguridad en un entorno cada vez más complejo y vulnerable.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Modelo de seguridad confianza Cero

“En la actualidad, la frontera del perímetro de la seguridad de la red empresarial se ha ampliado debido a la proliferación de tecnologías en la nube, dispositivos IoT y personal remoto. Como resultado, el método tradicional basado en el perímetro se volverá obsoleto y menos eficiente para proteger a la empresa de las amenazas cibernéticas”[22]. En el ámbito de la ciberseguridad, el enfoque de "Confianza Cero" supone un cambio radical respecto a los paradigmas tradicionales de seguridad, ya que no se basa en segmentos de red o demarcaciones empresariales, bajo la creencia de que estos están seguros por sí mismos. Este modelo no otorga confianza en función de las empresas o de los tipos de conexión de los individuos, ni toma en cuenta la ubicación de la red, ya sea local o en internet.

El modelo de Confianza Cero enfoca sus esfuerzos en los usuarios y activos de manera individual, sin importar quiénes sean o dónde se encuentren. Como dice CloudFlare[23],La autenticación se realiza de forma individual en cada entidad empresarial antes de conceder al usuario el permiso necesario para acceder a la información requerida.

4.1.2 Modelo de defensa en seguridad en profundidad

El término de “defensa en profundidad”, consiste en la defensa en profundidad consiste en usar varias medidas de seguridad para proteger la integridad de la información. Este planteamiento cubre todos los aspectos de la seguridad empresarial, y es deliberadamente redundante cuando es necesario. “Si se vulnera una línea de defensa, las otras capas están preparadas para evitar que las amenazas se infiltren. De este modo, se combaten las vulnerabilidades de seguridad que inevitablemente existen en la tecnología, el personal y las operaciones de una red”[24].

---

[22] A COMPREHENSIVE Framework for Migrating to Zero Trust Architecture [Anónimo]. IEEE Xplore [página web]. (10, febrero, 2023).]. [Consultado el 20, abril, 2024]. Disponible en Internet: http://ieeexplore.ieee.org/document/10052642.

[23] SEGURIDAD ZERO Trust [Anónimo]. CLOUDFLARE [página web]. [Consultado el 21, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

[24] GUIJARRO, Alfonso. YEPEZ, Jesica. Defensa en profundidad aplicado a un entorno empresarial. Revista Espacios. 2018. nro 42. pp 19-28. ISSN 0798 1015.

4.2 MARCO CONCEPTUAL

4.2.1 Zero Trust

“La confianza cero es una postura (o paradigma) holística de ciberseguridad cuyo principio fundamental es que no se confía implícitamente en los usuarios solo porque están dentro de la red”[25]. El enfoque de confianza cero Trust es un enfoque de seguridad que se basa en la verificación de identidad de los usuarios y dispositivo que tienen o intenta acceso a redes privadas, sin discriminar si se encuentran dentro o fuera de la red. Como dice Fortinet[26], ZTNA (Acceso de Confianza Cero) es la tecnología principal asociada a la arquitectura Zero Trust, incorporando principios y tecnología es un enfoque completo de seguridad de red donde proporciona un acceso seguro y sencillo a aplicaciones, sim importar donde el usuario se encuentre.

La seguridad tradicional en las redes informáticas confía en todos y en todo lo que se encuentra dentro de la red. En contraste, una arquitectura de Confianza Cero (Zero Trust) no confía en nadie ni en nada.

“Para implementar con éxito una arquitectura Zero Trust, las organizaciones deben conectar la información de todos los dominios de seguridad. Los equipos de seguridad de toda la empresa deben ponerse de acuerdo sobre las prioridades y armonizar las políticas de acceso”[27]. Los modelos de seguridad tradicionalmente se basan en el concepto de perímetro, donde es difícil obtener acceso desde el exterior y se confía en cualquier entidad dentro de dicho perímetro. Sin embargo, si un atacante logra ingresar, este puede moverse libremente dentro de la red.

Esta vulnerabilidad en los sistemas perimetrales se debe a que las empresas ya no están centralizadas en un único lugar. Actualmente, la información se encuentra dispersa, lo que dificulta establecer un control de seguridad efectivo.

---

[25] IMPLEMENTING ZERO Trust Security in the Public Sector [Anónimo]. Gartner [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

[26] ZERO TRUST Network Access (ZTNA) para controlar el acceso a las aplicaciones | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.fortinet.com/lat/solutions/enterprise-midsize-business/network-access/application-access.

[27] WHAT IS Zero Trust Security? Principles of the Zero Trust Model [Anónimo]. crowdstrike.com [página web]. (17, abril, 2023). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/.

Como dice Red Seguridad[28], La seguridad Zero Trust implica que no se confía en ninguna entidad, ya sea interna o externa, y se verifica a todos aquellos que requieren acceso a la red. Se ha comprobado que esta capa adicional de seguridad previene la filtración de datos, lo que podría traducirse en una gran afectación monetaria. Por este motivo, muchas empresas en la actualidad consideran el enfoque de "cero confianza" como un punto de partida fundamental.

4.2.2 Principios rectores de Zero Trust

En la Tabla 1 se evidencian los principios que rigen la metodología Zero Trust.

Tabla 1 Principios rectores de Zero Trust

Verificar explícitamente	Usar acceso con privilegios mínimos	Suponer incumplimiento
Autentique y autorice siempre en función de todos los puntos de datos disponibles.	Limite el acceso de los usuarios con Just-In-Time y Just-Enough-Access (JIT/JEA), políticas adaptables basadas en riesgos y protección de datos.	Minimice el radio de explosión y el acceso al segmento. Verifique el cifrado de extremo a extremo y use análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.

Fuente: Tomado de WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (14, abril, 2023). [Consultado el 17, abril, 2023]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust.

Al principio, en lugar de asumir que todo lo que está detrás de una red corporativa es seguro, el modelo Zero Trust asume que la red puede estar comprometida y verifica cada solicitud como si proviniera de un dispositivo no controlado. Este modelo enseña a nunca confiar y siempre verificar.

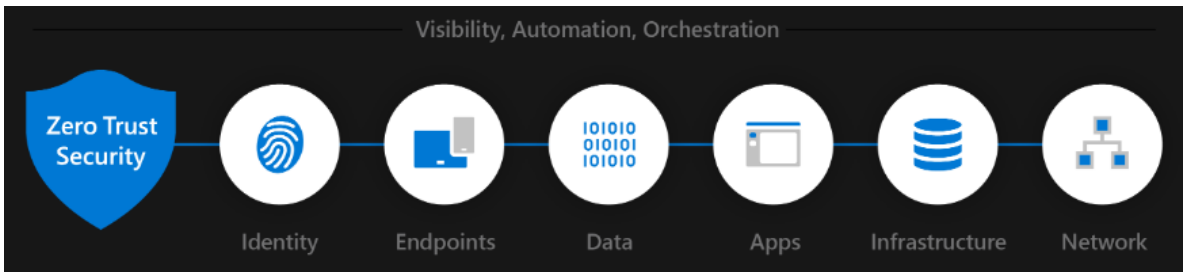
[28] ¿POR QUÉ el modelo Zero Trust es importante en las organizaciones? [Anónimo]. Red Seguridad [página web]. (6, mayo, 2022). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.redseguridad.com/actualidad/ciberseguridad/por-que-el-modelo-zero-trust-es-importante-en-las-organizaciones_20220506.html.

Como dice Microsoft[29], Es un modelo completamente diseñado para adaptarse al entorno actual, abarcando la fuerza híbrida inmóvil de las personas, dispositivos, aplicaciones y datos, sin importar dónde se encuentren.

Como dice INCIBE[30], Este enfoque debe extenderse a todo el patrimonio de la empresa y asumirse como una filosofía de seguridad integrada en la estrategia corporativa de extremo a extremo. Esto se logra mediante la implementación de tecnologías que apoyen la confianza cero en seis de los elementos más fundamentales. Cada uno de estos elementos representa un punto de control para las aplicaciones y los recursos críticos que deben ser defendidos en el entorno organizativo.

En la Figura 1, se evidencian los pilares que componen el modelo de seguridad Zero Trust.

Figura 1 Elementos fundamentales Zero trust



Fuente: Tomado de WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (14, abril, 2023). [Consultado el 17, abril, 2023]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust.

Cada organización, dependiendo de sus necesidades específicas, presenta requisitos distintos en cuanto a la implementación de tecnologías, ya sean existentes o nuevas. Estos factores pueden influir de diversas maneras en la planificación y ejecución de un esquema de seguridad Zero Trust.

[29] WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (14, abril, 2023). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust.

[30] METODOLOGÍA ZERO Trust: fundamentos y beneficios [Anónimo]. INCIBE [página web]. (9, octubre, 2023). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios.

4.2.3 Identidad

En la actualidad, el lugar de trabajo redefine los perímetros de seguridad organizacionales, ya que el trabajo híbrido permite a los empleados laborar desde cualquier ubicación y aceptar que utilicen sus propios dispositivos para trabajar de manera remota (BYOD). Esto también afecta cómo se accede a la información fuera de la red corporativa, tanto por colaboradores externos como por socios y proveedores. La identidad ”Se enfoca en verificar y autorizar usuarios y dispositivos antes de otorgar acceso a la red. Puede incluir la implementación de una solución de gestión de acceso e identidad (IAM) o autenticación multifactor (MFA)”[31], Las organizaciones están dejando atrás los entornos locales en favor de un entorno híbrido. Los controles establecidos en las organizaciones de forma local ya no son suficientes en este nuevo escenario. Estos controles deben trasladarse a los lugares donde se manipulan los datos, es decir, a los dispositivos y dentro de las aplicaciones que los procesan, “La infraestructura crítica es un entorno ideal para adoptar el modelo Zero Trust (confianza cero), dado que está diseñada para un fin y, en consecuencia, tiene un tráfico de red previsible (además de prestarse poco a la aplicación de parches)”[32].

“Una estrategia de Confianza cero requiere la comprobación explícita de la identidad, el uso de principios de acceso con privilegios mínimos y la asunción de infracción”[33]. Las identidades representan el conjunto de personas, servicios y dispositivos. El modelo Zero Trust opera de manera flexible y granular en cuanto al acceso a los datos.

- Las entidades deben ser verificadas mediante una autenticación fuerte antes de acceder a cualquier recurso organizacional.
- Los accesos deben ser compatibles y adecuados para esa identidad al momento de acceder a los recursos.
- Incluso después de acceder a los recursos, se debe seguir el principio de privilegios mínimos.

Una vez validadas las identidades, se puede proporcionar acceso a los recursos de la organización, dependiendo de las políticas asignadas a esa identidad, sin dejar de lado los riesgos y el análisis continuo que deben aplicarse.

---

[31] SEGURIDAD ZERO Trust: Una guía completa [Anónimo]. ENTRUST [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.entrust.com/es/resources/learn/zero-trust.
[32] PROTECCIÓN DE la infraestructura crítica con el modelo Zero Trust [Anónimo]. Palo Alto Networks [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cybersecurity-perspectives/zero-trust-for-critical-infrastructure.
[33] WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (14, abril, 2023). [Consultado el 17, abril, 2023]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust.

4.2.4 Puntos de Conexión

Las empresas actuales enfrentan una situación compleja y diversa en cuanto a los puntos de conexión desde los cuales se accede a los datos. Estos puntos pueden ser administrados o no administrados, e incluso ser propiedad de la organización. Esta diversidad de dispositivos con diferentes configuraciones representa un desafío considerable, ya que amplía la superficie de ataque y dificulta la implementación de un control de seguridad uniforme. “En un enfoque de Confianza cero, se aplican las mismas directivas de seguridad independientemente de si el dispositivo es propiedad corporativa o personal a través de Bring Your Own Device (BYOD). si el dispositivo está totalmente administrado por TI o solo se protegen las aplicaciones y los datos”[34]. Esto puede convertirse en uno de los pilares más débiles del modelo de seguridad Zero Trust, ya que la falta de uniformidad en la gestión de los dispositivos y su configuración incrementa el riesgo de vulnerabilidades que los atacantes podrían aprovechar.

Basado en el modelo de "nunca confiar, siempre verificar", es crucial que todos los puntos finales, tanto los dispositivos propios como los de terceros que acceden a los recursos de la red, sean verificados. Asimismo, es esencial considerar las aplicaciones que acceden a los datos de la organización, ya que estas constituyen un vector crítico dentro de la estrategia de seguridad Zero Trust.

“Las prácticas modernas de ciberseguridad requieren la aceptación por parte de todos a una arquitectura común y políticas de gobernanza”[35]. Por tal motivo las políticas de seguridad deben ser administradas por el departamento de TI independientemente de la propiedad del dispositivo, asegurando que tanto las aplicaciones como los datos estén protegidos. Estas políticas deben aplicarse a todos los puntos de conexión, sin importar el tipo de dispositivo utilizado, la ubicación desde donde se accede a la red corporativa o el medio de conectividad empleado.

Es fundamental destacar que las aplicaciones ejecutadas en los puntos de conexión deben garantizar la seguridad para evitar la filtración, pérdida accidental o intencionada, y comprometer la integridad de los datos corporativos.

Como menciona Microsoft, en la guía de Implementación, Los puntos de conexión deben regirse por reglas claras y claves para el modelo de seguridad Zero Trust, tales como:

---

[34] PROTECCIÓN DE puntos de conexión con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 20, febrero, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/endpoints.

[35] IMPLEMENTACIÓN DE la seguridad de confianza cero en el sector público [Anónimo]. Gartner [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

- Las políticas de seguridad deben aplicarse de manera centralizada a través de la nube y las redes de internet, cubriendo todos los dispositivos para proteger las aplicaciones y garantizar que estos cumplan con las normativas de seguridad y manejen adecuadamente los riesgos.

- Las aplicaciones deben ser aprovisionadas de manera segura y configuradas correctamente, asegurando que estén actualizadas y listas para su despliegue.

- Deben existir mecanismos que permitan una respuesta rápida y oportuna en caso de que se detecte una posible vulneración de la seguridad.

- "Es necesario establecer sistemas de control de acceso que determinen y apliquen los controles correspondientes a la política vigente para acceder a los datos"[36].

4.2.5 Aplicaciones

Las aplicaciones pueden ofrecer numerosas prestaciones a una organización. Es responsabilidad de la organización encontrar el punto de equilibrio en el uso de estas aplicaciones, asegurando tanto el acceso como el control de la información crítica. En promedio, las organizaciones utilizan alrededor de 1,000 aplicaciones diferentes. El 80 % de los empleados emplean aplicaciones no autorizadas que nadie ha revisado, y que podrían incumplir las políticas de seguridad y cumplimiento de la empresa, "No proteger la privacidad de la información de sus clientes puede poner en peligro tanto a su negocio como a sus clientes. Al no mantener la confidencialidad de los datos, el primer riesgo que aumenta es el de las fugas de datos"[37].

Como dice Microsoft[38], El modelo Zero Trust apoya a cualquier tipo de organización en la protección de las aplicaciones y los datos que estas manejan, mediante las siguientes acciones:

---

[36] PROTECCIÓN DE puntos de conexión con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (17, abril, 2024). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/endpoints.

[37] VERITAS TECHNOLOGIES. La importancia de la privacidad de datos y el cumplimiento: guía completa. The Leader in Enterprise Data Management | Veritas [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.veritas.com/es/mx/information-center/data-privacy.

[38] PROTECCIÓN DE aplicaciones mediante la confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (30, abril, 2024). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/applications.

- Descubrimiento de Shadow IT a través de controles y tecnologías.
- Validación de las aplicaciones y garantía de los niveles de permisos adecuados.
- Análisis en tiempo real para limitar el acceso.
- Monitoreo y análisis de comportamientos anormales.
- Control de las acciones de los usuarios.
- Configuraciones seguras mediante validación.

4.2.6 Datos

Los datos están protegidos bajo el esquema de seguridad Zero Trust. Este modelo ofrece una serie de principios de seguridad para las organizaciones, ayudando a proteger sus recursos mediante la implementación de los siguientes fundamentos:

- Verificación explícita: Se "buscan sustituir la confianza implícita por la confianza explícita, para evolucionar del «confiar, pero verificar» al «verificar, y luego confiar». Esta orientación reduce el riesgo y aumenta la agilidad de la empresa, al evaluar continuamente la confianza del usuario y del dispositivo a partir de la identidad, el acceso adaptativo y análisis exhaustivos"[39]. La autenticación y autorización del acceso a los datos deben verificarse en función de la identidad del usuario, la ubicación, el estado del dispositivo, los servicios y las cargas de trabajo, así como la clasificación de los datos.

- Acceso con privilegios mínimos: "El principio de mínimos privilegios garantiza que los usuarios solo tengan el acceso que realmente necesitan, lo cual reduce el posible impacto negativo de la apropiación de cuentas y las amenazas internas"[40]. Mediante políticas adaptables basadas en riesgos, se limita el acceso de los usuarios a lo estrictamente necesario, protegiendo tanto los datos como la productividad.

- Suposición de incumplimiento: "Zero Trust opera bajo el supuesto de que las infracciones son inevitables y que es posible que los adversarios ya estén presentes dentro de la red. Esta mentalidad cambia el enfoque de prevenir

[39] LAS CINCO fases de la adopción de zero trust: de la confianza implícita a la explícita - eSemanal - Noticias del Canal [Anónimo]. eSemanal - Noticias del Canal [página web]. (21, diciembre, 2021). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://esemanal.mx/2021/12/las-cinco-fases-de-la-adopcion-de-zero-trust-de-la-confianza-implicita-a-la-explicita.

[40] ¿QUÉ ES el principio de mínimos privilegios? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/access-management/principle-of-least-privilege/.

infracciones a minimizar su impacto y reducir la superficie de ataque"[41]. Basado en el principio de no confiar en nada y suponer incumplimiento, se minimiza la exposición segmentando el entorno, validando la organización de extremo a extremo, y visibilizando la detección de amenazas para mejorar las defensas.

Incrementar la defensa de los datos en profundidad, "Es necesario controlar el acceso a los datos, pero no es suficiente para ejercer el control sobre el movimiento de datos y evitar la pérdida de datos involuntaria o no autorizada"[42].

Las organizaciones deben clasificar los diferentes tipos de datos según su nivel de sensibilidad, permitiendo identificar los datos confidenciales, tanto si están almacenados en las instalaciones como si son gestionados en servicios en la nube. Esta clasificación es esencial para la protección de la información, la cual se fortalece al aplicar el principio de privilegios mínimos. Al implementar controles de acceso a la información sensible, como el cifrado y otras medidas de protección, se reducen los riesgos de seguridad, siempre en concordancia con las políticas de seguridad y cumplimiento.

La prevención de pérdida de datos es otro aspecto crucial, "El modelo reduce el tiempo necesario para detectar las filtraciones, lo que permite que las organizaciones minimicen los daños y reduzcan la pérdida de datos"[43]. Ya que los controles de acceso por sí solos no son suficientes, es necesario verificar y controlar toda actividad y movimiento de datos, especialmente cuando se trata de información sensible que podría generar incidentes de seguridad. Esto permite a las organizaciones anticiparse a posibles problemas. Asimismo, la gestión de riesgos internos debe centrarse en actuar sobre señales de comportamiento que puedan indicar actividades maliciosas, reduciendo así las probabilidades de violación de datos y detectando conductas sospechosas.

"Esto no solo proporciona un registro de auditoría claro si se produce una quiebra de seguridad, sino que también facilita la prueba de que has hecho todo lo posible

[41] COMPRENDER EL modelo de seguridad Zero Trust - SSL.com [Anónimo]. SSL.com [página web]. (7, mayo, 2024). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.ssl.com/es/artículo/Comprender-el-modelo-de-seguridad-de-confianza-cero/.

[42] Microsoft. (2023, noviembre 14). [Consultado el 10, junio, 2024]. Disponible en Internet: Proteger datos con Zero Trust. Microsoft Learn. https://learn.microsoft.com/es-es/security/zero-trust/deploy/data.

[43] DEFINICIÓN Y explicación de confianza cero [Anónimo]. Kaspersky [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/zero-trust?srsltid=AfmBOoqDvyd9sKoItJjV0GloP6uHOmg26olR_MxZLvFL3Ip0D7a0S8XW.

para cumplir los requisitos y estándares de privacidad de datos"[44]. Una adecuada gobernanza de datos es vital para minimizar su exposición. Los datos confidenciales deben seguir un ciclo de vida bien definido, limitando su propagación y reduciendo el número de copias. Al finalizar dicho ciclo, los datos que ya no sean necesarios deben ser eliminados para evitar riesgos de filtración.

4.2.7 Infraestructura

La infraestructura, ya sea local o en la nube, es un vector crítico de amenazas. "Los especialistas hacen hincapié en que no hay una infraestructura de confianza cero estándar para todos. Cada empresa, y por tanto cada implementación de ZT, será distinta. Asimismo, la infraestructura de ZT se implementa normalmente a lo largo del tiempo en una serie de proyectos de modernización de la infraestructura más pequeños"[45]. Es fundamental centrarse en la infraestructura que soporta los servicios de TI, el modelo Zero Trust ofrece un enfoque integral que incluye:

- Evaluar las versiones de los componentes.
- Revisar la gestión de la configuración.
- Ampliar los privilegios estrictamente necesarios para fortalecer las defensas.
- Utilizar la telemetría para detectar posibles anomalías o ataques.
- Bloquear automáticamente comportamientos riesgosos y aplicar las medidas correspondientes.

4.2.8 Redes

"El Acceso a la red Zero Trust (ZTNA) es la tecnología que permite implementar un modelo de seguridad Zero Trust. "Zero Trust" es un modelo de seguridad informática que asume que las amenazas están presentes tanto dentro como fuera de una red"[46]. Zero Trust cambia el paradigma tradicional de las redes, abriendo la posibilidad de una mayor interconexión de dispositivos y redes. No se parte de la premisa de que todo detrás del firmware corporativo es seguro; más bien, se asume que cualquier violación es inevitable. En este contexto, la administración de identidades desempeña un papel crucial.

---

[44] ¿QUÉ ES la confianza cero? Google Cloud [Anónimo]. Google Cloud [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://cloud.google.com/learn/what-is-zero-trust?hl=es.

[45] ¿QUÉ ES la arquitectura Zero Trust? [Anónimo]. Trend Micro [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.trendmicro.com/es_es/what-is/what-is-zero-trust/zero-trust-architecture.html.

[46] ¿QUÉ ES el Acceso a la red Zero Trust (ZTNA)? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/access-management/what-is-ztna/.

Existen tres objetivos clave en la gestión de redes dentro del modelo Zero Trust:

- Anticiparse a los ataques.
- Minimizar el daño y la velocidad de propagación.
- Aumentar la dificultad de intrusión en los espacios en la nube.

4.2.9 Fundamentos de Zero Trust

- Supervisión y validación continuos

"Visibilidad y control sobre quién tiene acceso a qué recursos. Esto ayuda a detectar rápidamente cualquier actividad sospechosa y bloquear el acceso a los recursos en consecuencia"[47]. Zero Trust verifica la identidad y los privilegios de los usuarios, así como la identidad y la seguridad de los dispositivos. Los inicios de sesión y las conexiones se agotan periódicamente una vez establecidos, lo que obliga a volver a verificar continuamente a usuarios y dispositivos.

- Mínimo privilegio

Los usuarios se les otorga el privilegio de ingresar a sólo ciertas partes, a las partes que realmente necesitan minimizando una posible exposición a partes que no requieren acceso

La implementación del mínimo privilegio implica una gestión de los permisos de los usuarios.

- Control de acceso a los dispositivos

Zero Trust requiere controles estrictos sobre los accesos. Los sistemas de confianza cero tienen que controlar los diferentes tipos de dispositivos que intentan acceder a recursos de red, asegurando la autorización y evaluar todos los dispositivos para asegurarse de que no se hayan puesto en riesgo. Minimizando la superficie de ataque de la red.

- Microsegmentación

"Con la microsegmentación, las organizaciones pueden ir más allá de los simples perímetros centralizados basados en red hasta una segmentación completa y

[47] METODOLOGÍA ZERO Trust: fundamentos y beneficios [Anónimo]. INCIBE [página web]. (9, octubre, 2023). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios.

distribuida mediante micro-perímetros definidos por software."[48] La microsegmentación es la buena práctica de seguridad de dividir los perímetros de seguridad en pequeñas partes que permitan el acceso a solo ciertas partes las personas con acceso únicamente tendrán acceso a una zona establecida nunca, aunque no por error.

- Evitar el movimiento lateral

El movimiento lateral es cuando un atacante se desplaza dentro de una red después de haber accedido a ella. El movimiento lateral puede ser difícil de detectar incluso al descubrir el punto de entrada del atacante, porque este ya se habrá movido para poner en riesgo otras partes de la red.

La confianza cero está diseñado para contener a los atacantes del modo que no se puedan mover lateralmente. "Al restringir el acceso solo a las aplicaciones y recursos específicos que un usuario necesita para realizar su trabajo, se reduce la superficie de ataque y se minimiza el riesgo de movimiento lateral de los atacantes en la red, disminuyendo las posibilidades de un ataque exitoso"[49]. Como el acceso de Zero Trust está segmentado y tiene que restablecerse de forma periódica, un atacante no puede moverse a otros microsegmentos de la red. Una vez detectado la presencia del atacante, el dispositivo o la cuenta de usuario en riesgo pueden ponerse en cuarentena, impidiendo el acceso a otras partes.

- Autenticación Multifactor (MFA)

"La autenticación multifactor (MFA**)** es un sistema de seguridad sólido que requiere que los usuarios presenten dos o más factores de verificación para acceder a un recurso"[50]. La autenticación multifactor (MFA) es utilizada en la metodología de seguridad Zero Trust. MFA requiere más de una prueba para autenticar a un usuario; no es suficiente con introducir solo una contraseña para obtener acceso. Además de la contraseña, generalmente se solicita una segunda prueba, como un mensaje de texto o una notificación en una aplicación, para validar que se trata de la misma persona.

[48] PROTECCIÓN DE redes con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (16, abril, 2024). [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/networks.

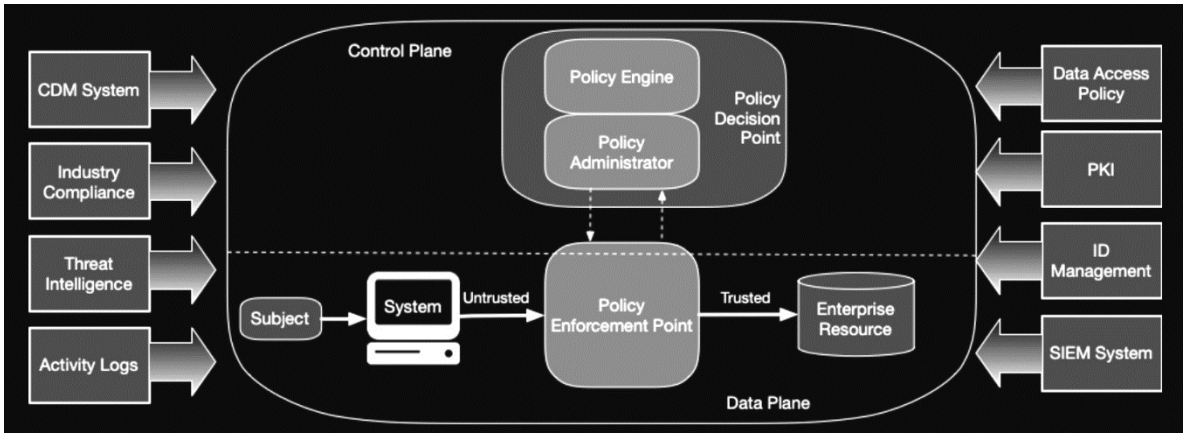
[49] METODOLOGÍA ZERO Trust: fundamentos y beneficios [Anónimo]. INCIBE [página web]. (9, octubre, 2023). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios.

[50] ENHANCING SECURITY with Multi-Factor Authentication in Zero Trust Model [Anónimo]. ISMS.online [página web]. (9, octubre, 2023). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.isms.online/knowledge/multifactor-authentication-and-zero-trust/.

Este enfoque debe aplicarse a toda la organización, a través de las implementaciones existentes y en todas las fases de seguridad, ya que pueden influir en la forma en que se ejecuta y se adopta el modelo Zero Trust.

En la Figura 2, se evidencia los componentes que deben aplicarse en la implementación del enfoque de seguridad Zero Trust.

Figura 2 Implementación Modelo Zero Trust



Fuente: Tomado de MERRITT, Rick. ¿Qué Es Zero-Trust? - Blog oficial de NVIDIA Latino América. Blog oficial de NVIDIA Latino América [blog]. (28, octubre, 2022). Disponible en Internet: https://la.blogs.nvidia.com/blog/que-es-zero-trust/.

Zero Trust es un conjunto de principios orientados para una política de seguridad moderna, su enfoque según el cuadro anterior utiliza información de seguridad y administración de eventos, recopilando datos, mitigando, diagnosticando para analizar y responder ante los resultados y eventos que se descubren.

4.3 MARCO HISTÓRICO

4.3.1 Antes del 2004

El perímetro, como postura de seguridad, fue utilizado durante décadas, “Los intentos iniciales surgen para segmentar la red utilizando VLAN o subredes, un enfoque extremadamente limitado sin autenticación, con restricciones mínimas y pocas capacidades de seguridad interna”[51]. Hasta la aparición de la computación en la nube, momento en que dichos perímetros comenzaron a desdibujarse, lo que

[51] BREVE HISTORIA de la confianza cero [Anónimo]. Líder en ciberseguridad y confianza cero | Zscaler [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.zscaler.es/resources/infographics/brief-history-zero-trust.pdf.

obligó a los equipos de seguridad a replantear el diseño de estos como parte esencial de la adopción de medidas de seguridad corporativa.

4.3.2 2004 - Concepto Zero Trust

El marco de seguridad comenzó a establecerse como concepto en 2004 por el Foro de Jericó, un consorcio internacional de seguridad. En este foro se debatieron los problemas potenciales de los enfoques de seguridad tradicionales basados en perímetros y se desarrolló un nuevo concepto en el que el perímetro no existía. Este enfoque requería múltiples capas para afianzarse, incluyendo el cifrado y la autenticación a nivel de los datos.

En una presentación de 2004, Paul Simmonds, miembro de Foro de Jericho,"En su presentación, señaló que "quizás lo que realmente se requiere es un nuevo modelo [de seguridad de datos]". Definió la desperimetrización como un concepto que implica "un conjunto de soluciones dentro de un marco que permite elegir y combinar" y lo denominó defensa en profundidad"[52].

Este análisis los llevó a considerar que necesitaban un modelo flexible y adaptativo, en el cual el perímetro quedara desdibujado y se adoptaran marcos de soluciones orientados a una defensa en profundidad.

4.3.3 2010 - Nacimiento "Confianza Cero"

"El analista de Forrester Research, John Kindervag, popularizó el término confianza cero cuando presentó la idea de que una organización no debe extender la confianza a nada dentro o fuera de sus perímetros." [53], Trasladando el perímetro al interior.

4.3.4 2011 - Beyond Corp Google

"BeyondCorp es la implementación de Google de un modelo de seguridad fiable de tipo confianza cero. Se basa en una década de experiencia en Google, en combinación con ideas y prácticas recomendadas de la comunidad. BeyondCorp pasa los controles de acceso del perímetro de red a usuarios concretos, por lo que

[52] PRATT, Mary K. History and Evolution of Zero Trust Security. WhatIs [página web]. (12, octubre, 2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security.
[53] PRATT, Mary K. History and Evolution of Zero Trust Security. WhatIs [página web]. (12, octubre, 2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security.

permite trabajar de forma segura desde prácticamente cualquier ubicación sin necesidad de una VPN tradicional"[54].

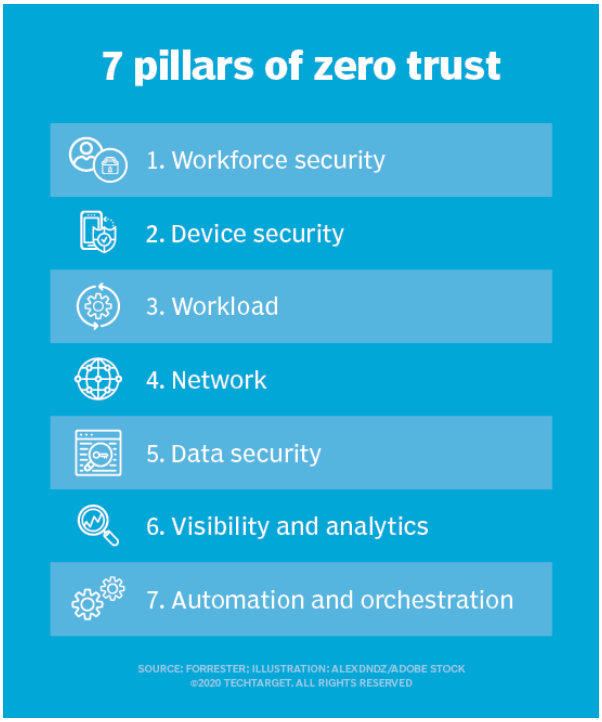
A partir de 2009, Google lanzó esta iniciativa en respuesta a diversos ciberataques, como la operación Aurora. Esta iniciativa permitió a sus empleados trabajar de manera remota de forma segura sin utilizar una VPN. En 2014, Google publicó un artículo que dio un impulso significativo al ideal de confianza cero.

4.3.5 2018 - Pilares básicos de Confianza Cero

A medida que grandes corporaciones adoptaban este concepto, los investigadores y proveedores continuaron desarrollando y afianzando la idea de "confianza cero" mediante herramientas que facilitan su implementación.

En la Figura 3, se evidencias los 7 pilares básicos propuestos para Implementar el modelo de Seguridad Zero trust.

Figura 3 7 Pilares de Zero Trust



Fuente: Tomado de Forrester Illustration: ALEXDNDZ/Adobe Stock (2020).

[54] BEYONDCORP: SEGURIDAD empresarial con el modelo de confianza cero [Anónimo]. Google Cloud [página web]. (2023). [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://cloud.google.com/beyondcorp?hl=es.

Como dice Pratt[55], En 2018, Forrester introdujo el concepto del ecosistema de Zero Trust, donde estableció los siete pilares básicos.

Ese mismo año, NIST publicó el documento SP-800-207, una guía detallada para la arquitectura de Zero Trust que establecía las pautas y los componentes centrales. "Está destinado a ayudar a comprender la confianza cero para los sistemas civiles no clasificados y proporcionar una hoja de ruta para migre e implemente conceptos de seguridad de confianza cero en un entorno empresarial"[56].

4.3.6 2019 – ZTNA / SASE

Como dice Zscaler, Gartner introdujo el acceso a la red de confianza cero llamada ZTNA (Zero Trust Network Access), describiendo los diferentes productos y servicios que brindan la confianza cero. Gartner también introdujo SASE (Security Access Service Edge). ZTNA y SASE trabajan en conjunto como capas de seguridad en el modelo de red, parte de la confianza cero. "La confianza cero, acuñada por primera vez por el mundo académico en la década de 1990, se considera cada vez más como un pilar de las estrategias de seguridad modernas"[57].

4.3.7 2020 - El NIST define un marco estándar de confianza cero

"El NIST publica el documento SP 800-207 como marco unificado para establecer una arquitectura de confianza cero (ZTA) e introduce el primer cambio real de la definición de confianza cero en el contexto de la red"[58].

4.3.8 2021- Casa Blanca y su estrategia de confianza cero

"Gobierno Federal de EE. UU. anunció la Orden Ejecutiva 14028 de EE. UU. Dicha orden establece un marco para ayudar a proteger a las organizaciones del sector

---

[55] PRATT, Mary K. History and Evolution of Zero Trust Security. WhatIs [página web]. (12, octubre, 2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security.

[56] SP 800-207, Zero Trust Architecture | CSRC [NIST]. NIST Computer Security Resource Center | CSRC [página web]. (2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://csrc.nist.gov/pubs/sp/800/207/final.

[57] IMPLEMENTING ZERO Trust Security in the Public Sector [Anónimo]. Gartner [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

[58] BREVE HISTORIA de la confianza cero [Anónimo]. Líder en ciberseguridad y confianza cero | Zscaler [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.zscaler.es/resources/infographics/brief-history-zero-trust.pdf.

público y privado de la cadena de suministro y otros tipos de vulneraciones de seguridad."[59] Como dice Lazarus[60], La orden ejecutiva emitida por el Gobierno de Estados Unidos, conocida como la Orden Ejecutiva 14028, titulada "Mejora de la seguridad cibernética de la nación", establece que las agencias federales deben implementar medidas de seguridad que disminuyan significativamente el riesgo de sufrir ataques cibernéticos exitosos contra la infraestructura digital del gobierno federal. En concordancia con esta orden ejecutiva, el 26 de enero de 2022, la Oficina de Gerencia y Presupuesto (OMB, por sus siglas en inglés) emitió el memorando 22-09, donde se presentó la estrategia federal Zero Trust, en apoyo a la Orden Ejecutiva 14028.

En respuesta a los repetidos incidentes maliciosos de seguridad cibernética que han tenido un impacto significativo en la infraestructura crítica, la economía y las necesidades fundamentales de la sociedad, el Gobierno Federal de Estados Unidos ha anunciado la Orden Ejecutiva 14028. Esta orden establece un marco de trabajo destinado a proteger a las organizaciones tanto del sector público como del privado contra violaciones en la cadena de suministro y otros tipos de infracciones.

Como dice la Casa Blanca[61], La orden enfatiza la importancia de establecer estándares de seguridad básicos y tiene como objetivo ayudar a las organizaciones a protegerse, detectar y responder a las amenazas de seguridad cibernética mediante la implementación de las mejores prácticas delineadas en las directrices del Instituto Nacional de Estándares y Tecnología (NIST) y los marcos de trabajo de Zero Trust.

4.3.9 2022 - Adopción Masiva

"El gobierno de EE. UU. exige la confianza cero, La Oficina de Gestión y Presupuesto exige la adopción de principios de confianza cero para todas las agencias para 2024"[62]. La Oficina de Administración y Presupuesto de la Casa

[59] ORDEN EJECUTIVA sobre servicios de seguridad de ciberseguridad | IBM® [Anónimo]. IBM - United States [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/es-es/services/executive-order-cybersecurity.

[60] ORDEN EJECUTIVA 14028 y la cadena de suministro de software - Lazarus Alliance, Inc. [Anónimo]. Leading IT Cyber Security Services | Lazarus Alliance, Inc. [página web]. (18, julio, 2024). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://lazarusalliance.com/es/executive-order-14028-and-the-software-supply-chain/.

[61] EXECUTIVE ORDER on Improving the Nation's Cybersecurity | The White House [Anónimo]. The White House [página web]. (12, mayo, 2021). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[62] BREVE HISTORIA de la confianza cero [Anónimo]. Líder en ciberseguridad y confianza cero | Zscaler [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.zscaler.es/resources/infographics/brief-history-zero-trust.pdf.

Blanca publicó detalles de su estrategia orientada a la confianza cero, en la cual alertó que las diferentes agencias deben cumplir con los estándares y objetivos orientados a la seguridad cibernética para finales del año 2024, y así reforzar las defensas que tiene el gobierno contra amenazas cada vez más sofisticadas. En el caso de las agencias federales de Estados Unidos, tienen hasta el 2024 para cumplir con los 5 objetivos de la confianza cero: identidad, dispositivos, redes, aplicaciones y datos.

Durante este año, "(CISA) publicó su Arquitectura de referencia técnica de seguridad en la nube y el Modelo de madurez de confianza cero para comentarios públicos. Al anunciar el lanzamiento , CISA explicó que, a medida que el gobierno federal continúa expandiéndose más allá del perímetro de red tradicional, es imperativo que las agencias implementen medidas de protección de datos en torno a la seguridad en la nube y la confianza cero"[63].

4.3.10 Actualidad y Futuro

El concepto de Zero Trust ha pasado de ser una discusión entre especialistas a convertirse en un enfoque ampliamente aceptado y aplicado por organizaciones de todo el mundo. Como dice Microsoft[64], El 2021, confirmó esta tendencia, señalando que las organizaciones que avanzan hacia un modelo de confianza cero seguirán creciendo de acuerdo con los requerimientos actuales y los de los próximos años.

Dado que el modelo de confianza cero no es un único producto proporcionado por un solo proveedor, muchas organizaciones ya han comenzado a tomar medidas hacia su adopción, a menudo sin ser plenamente conscientes de ello.

La implementación del modelo por parte del gobierno de Estados Unidos ha impulsado a los gobiernos estatales y de otros países a considerarlo una necesidad crítica, pese a que se basa en el principio de "verificación primero, confianza después".

Diversos proveedores importantes y organizaciones han trazado rutas hacia la confianza cero, ofreciendo pasos de implementación para que cualquier tipo y tamaño de organización que busque orientación pueda comprender el proceso de adopción de Zero Trust.

---

[63] PRATT, Mary K. History and Evolution of Zero Trust Security. WhatIs [página web]. (12, octubre, 2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security.

[64] INFORMACIÓN GENERAL sobre el marco de adopción de Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (16, abril, 2024). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/adopt/zero-trust-adoption-overview.

Como dice Microsoft[65], se estima que muchas organizaciones que iniciaron su camino hacia la confianza cero en 2021 podrían alcanzar el 76% de su implementación en 2024. Asimismo, se proyecta que las empresas que comenzaron este proceso durante el presente año podrían lograr un 36% de avance. Esto establece una ruta clara para cualquier organización que desee adaptarse al entorno de trabajo híbrido, permitiéndoles crecer sin la necesidad de una delimitación física de su red y abrirse a nuevos servicios orientados a su expansión y protección corporativa.

4.4 MARCO CIENTÍFICO O TECNOLÓGICO

4.4.1 Teoría de seguridad cibernética

El modelo de *Zero Trust* se basa en la idea fundamental de que no se debe confiar automáticamente en ninguna entidad o actividad en la red. Cada entidad debe verificarse constantemente en función de su identidad y las solicitudes de acceso que realice. Este enfoque se alinea con los principios de la seguridad cibernética, "La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes"[66].

4.4.2 Arquitectura de red y segmentación

Zero Trust se centra en la segmentación de redes independientes y en políticas de acceso granulares para proteger a los usuarios y dispositivos, "La segmentación de la red es un modelo arquitectónico que divide una red en varios segmentos o subredes, cada uno de los cuales funciona como una pequeña red propia. Esto

[65] INFORMACIÓN GENERAL sobre el marco de adopción de Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (16, abril, 2024). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/adopt/zero-trust-adoption-overview.

[66] ¿QUÉ ES la ciberseguridad? [Anónimo]. Kaspersky [página web]. [Consultado el 03, octubre, 2023]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

permite a los administradores de red aplicar políticas detalladas para controlar el flujo de tráfico entre las distintas subredes"[67].

4.4.3 Tecnologías habilitadoras

Zero Trust emplea una amplia variedad de tecnologías que proporcionan una seguridad adaptativa y contextual, incluyendo autenticación, autorizaciones, controles de acceso, análisis de comportamientos y una visibilidad mejorada de la red. "Las Tecnologías Habilitadoras son tecnologías intensivas en conocimiento, que han sido identificadas como inductoras de innovaciones en diversos sectores económicos, y que potencialmente podrían provocar altas disrupciones en la economía y la sociedad en los próximos 10-15 años, según distintos estudios internacionales de prospectiva tecnológica"[68].

4.4.4 Estándares y marcos de Referencia

Existen varios marcos de referencia y estándares que pueden ayudar a las organizaciones a implementar Zero Trust, como: el NIST SP-800-207,Microsoft Zero Trust Framework, Google BeyondCorp, Forrester Zero Trust Ecosystem, CIS Controls, Entre otros.

4.5 MARCO LEGAL

- NORMATIVO

4.5.1 ISO 27001:2022

Como dice ISO[69],Es una norma internacional que establece los requisitos para el Sistema de Gestión de Seguridad de la Información (SGSI), proporcionando un paso a paso para un marco de implementación, operación y mantenimiento, con un enfoque en la mejora continua de la seguridad de la información de una organización. Esta es la versión más reciente, publicada por ISO en 2022. Un punto

[67] ¿QUÉ ES la segmentación de la red? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 03, octubre, 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cyberpedia/what-is-network-segmentation.
[68] ¿QUÉ SON las Tecnologías Habilitadoras? [Anónimo]. Inndromeda [página web]. (13, octubre, 2020). [Consultado el 03, octubre, 2024]. Disponible en Internet: https://inndromeda.es/actualidad/que-son-las-tecnologias-habilitadoras.
[69] ISO/IEC 27001:2022 [Anónimo]. ISO [página web]. (2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.iso.org/es/contents/data/standard/08/28/82875.html.

clave en esta actualización es la identificación y gestión de los riesgos de la seguridad de la información.

4.5.2 ISO 31000

Como dice ISO[70],Norma internacional orientada a la gestión de riesgos, que proporciona un enfoque integral y directrices para su implementación. Está diseñada para apoyar a cualquier tipo de organización, ya sea pública o privada, en el análisis y evaluación de riesgos. Es aplicable a la mayoría de las actividades laborales relacionadas con la gestión de riesgos y ofrece recomendaciones de mejores prácticas. Esta norma desarrolla técnicas para garantizar la seguridad y la protección en el lugar de trabajo.

4.5.3 NIST SP-800-207

Como dice NIST[71], El documento sobre la Arquitectura Zero Trust proporciona directrices detalladas sobre cómo implementar una arquitectura de confianza cero en las organizaciones. Publicado por el NIST, es una referencia importante para comprender y aplicar los conceptos de Zero Trust en entornos organizacionales, abarcando tanto la implementación como los aspectos técnicos de esta arquitectura.

4.5.4 CIS

Según dice AWS[72], Los Controles Críticos de Seguridad del CIS son un conjunto de mejores prácticas prescriptivas, priorizadas y simplificadas, que se pueden emplear para mejorar la ciberseguridad de manera efectiva. Actualmente, profesionales de ciberseguridad de todo el mundo utilizan los Controles CIS y colaboran en su desarrollo mediante un proceso de consenso comunitario.

---

[70] NORMA INTERNACIONAL ISO 31000 [Anónimo]. Rama Judicial de Colombia: Información y servicios para la justicia [página web]. (Febrero, 2018). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486.

[71] SP 800-207, Zero Trust Architecture | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. (Agosto, 2020). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://csrc.nist.gov/pubs/sp/800/207/final.

[72] ¿QUÉ SON los puntos de referencia del CIS? - Explicación de los puntos de referencia del CIS - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/cis-benchmarks/.

4.5.5 ITIL

Según dice IBM[73], ITIL es un conjunto de publicaciones que reúne las mejores prácticas para la gestión de servicios de tecnología de la información. Su objetivo es ofrecer orientación sobre cómo proporcionar servicios de TI de alta calidad, así como definir los procesos, funciones y capacidades necesarios para respaldarlos. Además, ITIL describe procesos, procedimientos, tareas y listas de verificación que no están diseñados específicamente para ninguna organización o tecnología en particular. Estas prácticas pueden aplicarse a estrategias de gestión del conocimiento y pueden utilizarse en conjunto con software de Gestión de Servicios de TI (ITSM, por sus siglas en inglés).

4.5.6 CSIRT Gobierno de Colombia

Según dice CSIRT[74], Creado por el gobierno colombiano para gestionar y reaccionar de manera centralizada ante los incidentes cibernéticos, el CSIRT unifica las diferentes tipologías de cibercriminales que pueden atacar al gobierno, apoyando así la gestión eficiente de los riesgos.

- LEGAL

4.5.7 Ley 1266 de 2008

Según dice GOV colombiano[75], Esta ley se enfoca en la protección y regulación de datos personales, estableciendo disposiciones para garantizar el adecuado manejo de la información personal, tanto en organizaciones privadas como públicas.

4.5.8 Ley 1273 de 2009

Según dice GOV colombiano[76], Contempla los delitos informáticos en Colombia, definiendo y sancionando conductas como el acceso indebido a sistemas

[73] IBM. ¿Qué es ITIL? | IBM. IBM - United States [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/mx-es/topics/it-infrastructure-library.
[74] CSIRT GOBIERNO [Anónimo]. Gobierno Digital 2020 [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno.
[75] LEY 1266 de 2008 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (31, diciembre, 2008). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.
[76] LEY 1273 de 2009 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (5, enero, 2009). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492.

informáticos, la intervención de datos y los daños informáticos, además de establecer medidas para contrarrestar estas infracciones.

4.5.9 Ley 1581 de 2012

Según dice GOV colombiano[77], La Ley de Protección de Datos Personales regula el manejo, procesamiento y protección de los datos personales en Colombia. Documenta los derechos de los titulares de los datos y las obligaciones de quienes los retienen y recopilan.

4.5.10 Ley 1341 de 2009

Según dice GOV colombiano[78], Es el marco general de regulación de las tecnologías de la información y las comunicaciones (TIC) en Colombia. Aunque no se enfoca exclusivamente en la ciberseguridad, establece disposiciones para la protección de infraestructuras críticas y sienta las bases para el desarrollo de políticas de ciberseguridad en el país.

4.5.11 Decreto 620 de 2020

Según dice GOV colombiano[79], Este decreto reglamenta la Ley 1341 de 2009 y establece disposiciones para garantizar la protección de la infraestructura crítica de las tecnologías de la información y las comunicaciones en Colombia. Además, define los mecanismos de cooperación y coordinación entre las entidades responsables de la ciberseguridad.

[77] LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (17, octubre, 2012). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.
[78] LEY 1341 de 2009 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (30, julio, 2009). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913.
[79] DECRETO 620 de 2020 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (2, mayo, 2020). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337.

4.5.12 Decreto 338 de 2022

Según dice GOV colombiano[80], Establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital y crea el modelo y las instancias de gobernanza de seguridad digital, entre otras disposiciones.

5. DISEÑO METODOLÓGICO

La presente monografía se desarrollará mediante una revisión sistemática de la información proporcionada por diversas fuentes, las cuales servirán como base para el análisis del enfoque Zero Trust.

5.1 ¿QUÉ ES UNA REVISIÓN SISTÉMICA?

"Una revisión sistemática es un tipo de estudio científico, en el que se recopila toda la información generada por investigaciones de un tema o pregunta determinados"[81]. Una revisión sistemática es un resumen organizado y claro de la información disponible que busca responder a una pregunta específica. Se basa en múltiples artículos y fuentes confiables, lo que le otorga un alto nivel de evidencia.

Este tipo de revisión se caracteriza por seguir un proceso transparente y comprensible. Se recopila, selecciona y evalúa críticamente toda la información relevante relacionada con la pregunta planteada.

En una revisión sistemática se analiza toda la información generada por investigaciones previas sobre un tema determinado. "El proceso de confección de una revisión sistemática comienza con el planteamiento de una pregunta clínica específica y estructurada que determinará los términos que serán utilizados en la búsqueda en las bases de datos y el tipo de artículos útiles para responder dicha pregunta"[82]. Esto sintetiza la evidencia disponible sobre dicho tema. Para garantizar la calidad y minimizar el sesgo, debe ser realizada por un equipo en el que, al menos, dos personas participen de manera independiente en cada etapa del proceso.

---

[80] DECRETO 338 de 2022 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (8, marzo, 2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866.

[81] BIBLIOGUÍAS: REVISIONES sistemáticas: Definición: ¿qué es una revisión sistemática? [Anónimo]. Inicio - Biblioguías - BiblioGuías at Biblioteca Universidad de Navarra [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://biblioguias.unav.edu/revisionessistematicas/que-es-una-revision-sistematica.

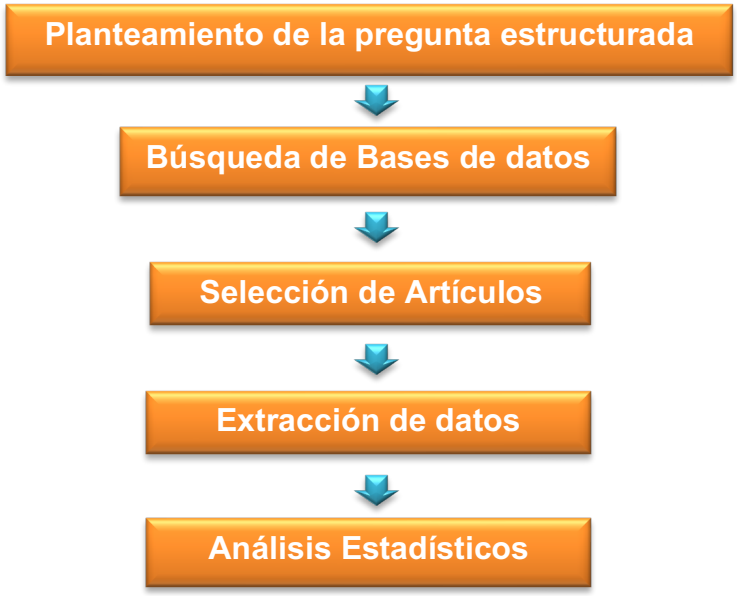
[82] REVISIONES SISTEMÁTICAS: definición y nociones básicas [Anónimo]. SCIELO [página web]. (Diciembre, 2018). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-01072018000300184.

Existen otros tipos de revisiones, como las narrativas o bibliográficas, pero estas no siguen la metodología estructurada propia de la revisión sistemática.

5.1.1 ¿Como realizar una evaluación sistémica?

En la Figura 4, se evidencia el paso a paso para realizar una revisión sistémica.

Figura 4 Proceso de elaboración de Una Revisión Sistemática



Fuente: Elaboración Propia (2023).

"Para llevar a cabo con eficacia una revisión bibliográfica sistemática, es fundamental seguir un conjunto estructurado de instrucciones que abarquen una planificación exhaustiva, una metodología rigurosa y una documentación meticulosa"[83]. La revisión sistemática propuesta consiste en una revisión exhaustiva de la literatura, utilizando la crítica y el conocimiento previo de manera ordenada, precisa y analítica. Se presenta un análisis crítico de un tema específico, señalando las similitudes e inconsistencias en la literatura consultada. Esta actividad es de carácter retrospectivo y aporta información dentro de un periodo de tiempo determinado.

[83] ¿QUÉ ES una revisión sistemática de la literatura? | Qué es, diferencias y cómo hacer una [Anónimo]. ATLAS.ti [página web]. [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://atlasti.com/es/guias/revisiones-bibliograficas/revision-sistematica.

Una buena revisión sistemática debe cumplir con las siguientes características:

- Ser sistemática: solo se utilizarán documentos que tengan relevancia determinante, evitando fuentes irrelevantes.
- Resaltar documentos clave: se destacarán aquellos documentos que ayuden a comprender la problemática de la investigación a un nivel más profundo.
- Crítica: los conocimientos deben presentarse de manera crítica, mostrando las limitaciones de las conclusiones y señalando los aspectos faltantes en la metodología.
- Actualidad: la documentación de más de 5 o 10 años será descartada para abordar la problemática principal, salvo estudios emblemáticos que hayan influido en el desarrollo del tema.

Como dice Universidad de navarra[84], Pasos para elaborar una revisión sistemática:

- Planificación: Es clave planificar la revisión, su alcance y viabilidad, realizando una búsqueda preliminar y definiendo el tipo de revisión sistemática más acorde con los objetivos planteados.
- Definición de la pregunta de investigación: Formulada la pregunta de investigación, se deben establecer criterios de inclusión y exclusión, y redactar un protocolo detallado que describa cómo se llevará a cabo la revisión.
- Búsqueda exhaustiva: El equipo deberá buscar exhaustivamente todos los estudios, publicados o no, que respondan a la pregunta planteada, evaluando su confiabilidad.
- Análisis y síntesis: Se resumirán los resultados para obtener una visión completa del volumen de evidencia disponible.
- Publicación: Al presentar e interpretar los resultados, la revisión sistemática se convertirá en una fuente confiable de evidencia para la toma de decisiones.

La presente monografía aplicará el marco normativo para generar un conjunto de pasos que permitan llevar a cabo el cumplimiento regulatorio dentro de las organizaciones que buscan implementar Zero Trust. Es primordial, por lo tanto,

[84] BIBLIOGUÍAS: REVISIONES sistemáticas: Pasos o Etapas para realizar una revisión sistemática [Anónimo]. Inicio - Biblioguías - BiblioGuías at Biblioteca Universidad de Navarra [página web]. (20, septiembre, 2024). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://biblioguias.unav.edu/revisionessistematicas/pasos-realizar-revisionsistematica.

recomendar el uso de la metodología GRC, la cual apoyará a cualquier tipo de organización en la consecución de sus objetivos y en el manejo de la incertidumbre, garantizando el cumplimiento dentro del marco de gobernanza establecido.

5.2 GRC (GOBIERNO, RIESGO, CUMPLIMIENTO)

"GRC, proveniente de las siglas en inglés de «Governance, Risk, and Compliance», es una metodología y un enfoque que se utiliza para unificar los procesos de gobernanza, riesgo y cumplimiento"[85]. El enfoque GRC es una estrategia integral destinada a la gestión de los aspectos relacionados con la gobernanza, el riesgo y el cumplimiento dentro de una organización. Este enfoque es crucial para el buen desempeño empresarial y para garantizar el cumplimiento de las leyes, regulaciones y estándares aplicables.

El GRC busca integrar estos tres componentes en un marco coherente y coordinado, lo que garantiza una gestión eficaz que permite una visión global de los aspectos críticos de la organización. Además, apoya la toma de decisiones informadas y la gestión proactiva del riesgo, asegurando el cumplimiento de los requisitos legales y normativos.

- **Componentes de GRC:**

5.2.1 Gobernanza

Implica los procesos y políticas estructuradas con responsabilidades claramente definidas, que apoyan la dirección y el control de una organización. "Define las responsabilidades de las principales partes interesadas, como la junta directiva y la alta dirección. Por ejemplo, una buena gobernanza corporativa ayuda al equipo de trabajo a incorporar la política de responsabilidad social de la empresa en los planes"[86]. Esto garantiza la toma de decisiones informadas y una adecuada gestión del riesgo.

[85] ¿QUÉ ES GRC? Gobierno, riesgo y cumplimiento [Anónimo]. GlobalSuite Solutions [página web]. (28, diciembre, 2023). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.globalsuitesolutions.com/es/que-es-grc-gobierno-riesgo-cumplimiento/.

[86] ¿EN QUÉ consiste el GRC? - Explicación sobre el enfoque de gobernanza, riesgo y cumplimiento - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/grc/.

5.2.2 Riesgo

Se refiere a la incertidumbre asociada a los objetivos de la organización y a la posibilidad de que ocurran situaciones que afecten su capacidad para cumplirlos. “Una gestión de riesgos adecuada ayuda a las empresas a identificar estos riesgos y a encontrar formas de corregirlos. Las empresas utilizan un programa de gestión de riesgos empresariales para predecir posibles problemas y minimizar las pérdidas”[87]. La gestión del riesgo incluye la evaluación, mitigación y monitoreo de riesgos, utilizando estrategias para prevenir, mitigar o transferir dichos riesgos.

5.2.3 Cumplimiento

“El cumplimiento implica seguir las reglas, leyes y regulaciones establecidas por los organismos del sector y las políticas corporativas internas. El enfoque GRC implica contar con procedimientos que garanticen que las actividades empresariales cumplan con las regulaciones correspondientes”[88]. Lo cual comprende todas las leyes, regulaciones, estándares y políticas internas o externas que la organización debe cumplir. Incluye la implementación de controles en los procesos para asegurar que la organización cumpla con todas las normativas aplicables.

La Figura 5, evidencia la estructura GRC (Gobierno, Riesgo y Cumplimiento) y cómo engloba estos componentes para proporcionar una visión global de los aspectos de una organización.

[87] ¿EN QUÉ consiste el GRC? - Explicación sobre el enfoque de gobernanza, riesgo y cumplimiento - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/grc/.

[88] ¿QUÉ ES GRC? Gobierno, riesgo y cumplimiento [Anónimo]. GlobalSuite Solutions [página web]. (28, diciembre, 2023). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.globalsuitesolutions.com/es/que-es-grc-gobierno-riesgo-cumplimiento/.

Figura 5 Estructura GRC

Fuente: Tomado de METODOLOGÍA GRC [Anónimo]. GRC Total [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://grctotal.com/metodologia/.

6. ¿QUÉ ES ZERO TRUST?

Zero Trust puede catalogarse como una estrategia o metodología de seguridad que se basa en la filosofía de que ninguna persona ni dispositivo, tanto dentro como fuera de la red de la organización, debe tener acceso a los sistemas o datos hasta que se considere estrictamente necesario. La confianza cero significa no otorgar confianza implícita en ningún caso.

Este tipo de estrategia o modelo surge de la necesidad impuesta por la nueva normalidad, en la que las organizaciones desempeñan un papel más relevante en la transformación digital, gestionando cambios continuos en un entorno empresarial en constante evolución.

Como dice P. Phiayura and S. Teerakanok[89], Zero Trust requiere actualizar los modelos de seguridad que tradicionalmente se han utilizado durante décadas, ya que estos no cumplen con requisitos como la agilidad, la mejora en la experiencia del usuario o la capacidad de adaptación frente a la constante evolución de las amenazas. Varias organizaciones están implementando el modelo de confianza cero para abordar los desafíos de esta nueva normalidad en entornos híbridos, no centrados en un único espacio geográfico ni en un único dispositivo controlado.

[89] P. PHIAYURA AND S. TEERAKANOK. A Comprehensive Framework for Migrating to Zero Trust Architecture. IEEE [página web]. (2023). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://ieeexplore.ieee.org/document/10052642.

“Zero Trust como filosofía se adapta mejor a los entornos informáticos modernos que los enfoques de seguridad más tradicionales”[90]. La confianza cero representa una transformación significativa para cualquier organización, que requiere la adopción y gestión de cambios de extremo a extremo. Este proceso de transformación conlleva tiempo y exige la aceptación de todas las partes interesadas de la empresa. Por lo tanto, los líderes empresariales y tecnológicos juegan un papel fundamental en la implementación de un enfoque versátil y flexible.

Existen tres componentes clave para que una organización pueda establecer e implementar el modelo de Zero Trust:

- Visibilidad: Es necesario que tanto los dispositivos como los activos a proteger puedan ser monitoreados. Para ello, se debe identificar todos los dispositivos y activos, ya que no se puede monitorear aquello que no se sabe que existe. “El modelo Zero Trust exige una visibilidad, una aplicación de las políticas y un control homogéneos, ya sea en el dispositivo directamente o en la nube”[91]. Es fundamental contar con visibilidad de todos los recursos pertenecientes a la organización.

- Políticas: Se trata de implementar controles que permitan el acceso a la información únicamente a personas específicas o, en el caso de Zero Trust, en cantidades y condiciones específicas, requiriendo controles minuciosos, “Se asegura de que la interacción cumpla con los requisitos condicionales de las políticas de seguridad de la organización. Una estrategia de seguridad Zero Trust también autentica y autoriza cada dispositivo, flujo de red y conexión basándose en políticas dinámicas, utilizando el contexto de la mayor cantidad de fuentes de datos posible”[92].

- Automatización: Asegura que las políticas se apliquen correctamente y permite la rápida ejecución de medidas frente a posibles incidentes, “Dado que cada una de estas áreas individuales genera sus propias alertas pertinentes, se necesita una funcionalidad integrada para administrar el flujo de datos resultante para defenderse mejor contra las amenazas y validar la confianza en una transacción”[93].

---

[90] SEGURIDAD ZERO Trust | ¿Qué es una red Zero Trust? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

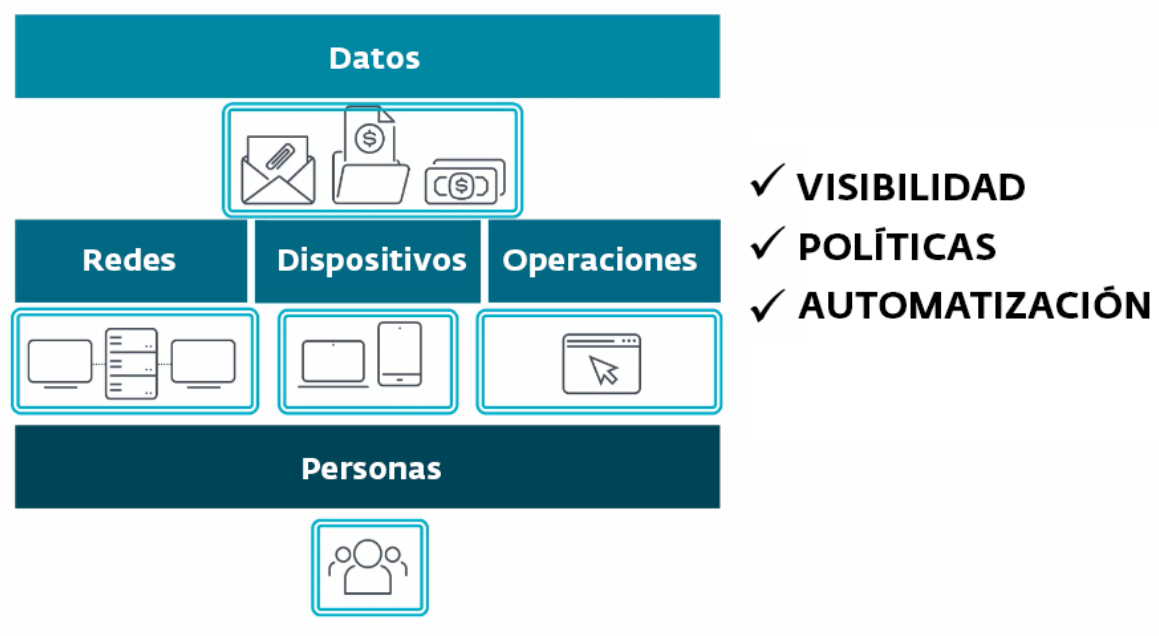
[91] ¿QUÉ ES una arquitectura Zero Trust (confianza cero)? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cyberpedia/what-is-a-zero-trust-architecture.

[92] IBM. ¿Qué es Zero Trust? | IBM. IBM - United States [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust.

[93] VISIBILIDAD, AUTOMATIZACIÓN y orquestación con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (28, mayo, 2024). [Consultado el 25,

La Figura 6, evidencia los aspectos que se deben tener en cuenta en la implementación de la metodología Zero Trust (visibilidad, políticas, automatización), considerando como base a las personas y los medios utilizados para acceder a los datos como fin.

Figura 6 Aspectos implementación Zero Trust



Fuente: Tomado de RAGGI, Nicolás. Qué es el modelo de seguridad Zero Trust y por qué creció su adopción. Award-winning news, views, and insight from the ESET security community [página web]. (14, septiembre, 2020). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.welivesecurity.com/la-es/2020/09/14/zero-trust-que-es-modelo-seguridad-crecio-adopcion/.

6.1 ¿CÓMO FUNCIONA ZERO TRUST?

Para comprender cómo opera Zero Trust en la práctica, puede imaginarse que un guardia de seguridad representa a Zero Trust, y su ronda de vigilancia es equivalente al monitoreo constante. Aunque el guardia conozca bien el edificio que protege, siempre revisa cada área durante su ronda.

El modelo de seguridad de confianza cero se basa en la autenticación y autorización de cada dispositivo antes de permitirle acceder a los recursos o transferir datos en

septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/visibility-automation-orchestration.

una red privada. No importa si el dispositivo se encuentra dentro o fuera del perímetro de la red; este modelo combina análisis, filtrado y registro para verificar el comportamiento del dispositivo en la red y monitorear continuamente cualquier señal de riesgo.

Si un usuario o dispositivo muestra indicios de comportarse de manera diferente a lo habitual, se le considera una posible amenaza y se le supervisa con mayor detenimiento.

Este cambio de estrategia aborda numerosas amenazas de seguridad comunes y mitiga el riesgo de que un atacante aproveche una vulnerabilidad en el perímetro para acceder a información confidencial, “La seguridad perimetral tradicional dependía de firewalls, VPN y gateways para separar las zonas de confianza de los usuarios no confiables. Pero a medida que los "empleados móviles" comenzaron a acceder a la red a través por su propia cuenta, con sus propios dispositivos, se empezaron a crear perímetros borrosos”[94].

Para implementar esta estrategia, “La identificación de usuarios y dispositivos es un factor clave para el cumplimiento de arquitectura de confianza cero. Se accede a las credenciales de identidad a través de MFA, incluidas las basadas en certificados. y/o medios biométricos para los mecanismos de autenticación ofrecidos en dispositivos móviles“[95]. Es necesario establecer controles de acceso a los activos, utilizar autenticación multifactor, cifrar los datos, contar con visibilidad de la red y monitorear continuamente todas las entidades. Además, se deben aplicar políticas de seguridad basadas en el principio de privilegio mínimo.

La adopción del enfoque de confianza cero requiere el apoyo de la alta dirección, ya que, con el tiempo, los ataques más críticos se vuelven más comunes. Los líderes empresariales de todas las áreas funcionales deben priorizar la seguridad adoptando este enfoque.

Zero Trust funciona al integrar soluciones verticales con un objetivo común y subjetivo, abarcando capacidades, resultados comerciales y métricas medibles del estado de la seguridad.

El CISO (Chief Information Security Officer) generalmente establece la estrategia basada en diferentes opciones propuestas por las tecnologías de seguridad. La

[94] RAMIRO, Ruben. ¿ Que es Zero Trust en ciberseguridad ? CIBERSEGURIDAD .blog [página web]. (14, junio, 2019). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://ciberseguridad.blog/que-es-zero-trust-en-ciberseguridad/.

[95] APPLYING ZERO Trust Principles to Enterprise Mobility [Anónimo]. CISA [página web]. (Marzo, 2022). [Consultado el 24, septiembre, 2024]. Disponible en Internet: https://www.cisa.gov/sites/default/files/2023-01/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf.

adopción y comprensión del modelo de confianza cero requieren la aceptación de otros miembros de alto nivel, “Este enfoque enfatiza la limitación de la superficie de ataque, eliminando metódicamente el acceso de usuarios con privilegios excesivos e implementando medidas de autenticación sólidas. Esto significa que los CISO se centran en la visibilidad de extremo a extremo, entendiendo quién accede a qué activos a través de qué dispositivos y redes”[96].

El Cuadro 1, se evidencian las funciones que pueden desempeñar los miembros de la alta dirección, alineados con la visión de seguridad integrada a Zero Trust.

Cuadro 1 Roles Alta Dirección Zero Trust

Role	Responsabilidad	Interés de confianza cero
Director Ejecutivo (CEO)	Responsable del negocio	Zero Trust proporciona un enfoque integrado de la seguridad en todas las capas digitales.
Director de Marketing (CMO)	Responsable de la visión y ejecución de marketing.	Zero Trust permite la rápida recuperación de la infracción y potencia la función responsable de informar para una organización de cara al público, lo que permite contener las infracciones sin pérdida de reputación.
Director de información (CIO)	Responsable de TI en su conjunto	Los principios de Zero Trust eliminan las soluciones de seguridad verticales que no están alineadas con los resultados comerciales y habilitan la seguridad como plataforma, que sí se alinea con los resultados comerciales.
Director de seguridad de la información (CISO)	Responsable de la implementación del programa de seguridad.	Los principios de Zero Trust proporcionan una base suficiente para que la organización cumpla con varios estándares de seguridad y permite que la organización proteja los datos, los activos y la infraestructura.
Director de tecnología (CTO)	Arquitecto Jefe en la empresa	Zero Trust ayuda con la alineación de tecnología defendible alineada con los resultados comerciales. Con Zero Trust, la seguridad se integra en cada arquitectura.
Director de operaciones (COO)	Responsable de la ejecución operativa.	Zero Trust ayuda con la gobernanza operativa; el “cómo hacer” de la visión de seguridad y la revelación de quién hizo qué y cuándo. Ambos están alineados con los resultados comerciales.
Director financiero (CFO)	Responsable de la gobernanza y el gasto.	Zero Trust ayuda con la responsabilidad del gasto y la defensa del gasto; una forma medible de obtener una medida basada en el riesgo contra la seguridad y el gasto de Zero Trust alineado con los resultados comerciales.

Fuente: Tomado de ZERO TRUST adoption framework overview [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, abril, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview.

[96] CISO ZERO Trust Perspectives: Balancing Influence and Complexity |… [Anónimo]. Appgate [página web]. (21, noviembre, 2023). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.appgate.com/blog/ciso-zero-trust-perspectives-balancing-influence-complexity-and-business-objectives.

6.2 METODOLOGÍA USADA POR ZERO TRUST

La metodología de confianza cero se basa en 3 principios, en la Tabla 2, se evidencias las descripción de los 3 principios y como estos se ven reflejados en las organizaciones.

Tabla 2 Tabla 2 Principios Zero Trust

Principio	Descripción técnica	Descripción del negocio
Verificar explícitamente	Autentique y autorice siempre en función de todos los puntos de datos disponibles, incluida la identidad del usuario, la ubicación, el estado del dispositivo, el servicio o la carga de trabajo, la clasificación de datos y las anomalías.	Este principio requiere que los usuarios verifiquen quiénes son, utilizando más de un método, para que las cuentas comprometidas obtenidas por piratas informáticos no puedan acceder a sus datos y aplicaciones. Este enfoque también requiere que los dispositivos sean reconocidos como autorizados para acceder al entorno e, idealmente, que estén administrados y en buen estado (no comprometidos por malware).
Usar acceso con privilegios mínimos	Limite el acceso de los usuarios con acceso justo a tiempo y suficiente (JIT/JEA), políticas adaptables basadas en riesgos y protección de datos para ayudar a proteger tanto los datos como la productividad.	Este principio limita el radio de explosión de una posible infracción, de modo que si una cuenta se ve comprometida, el daño potencial es limitado. Para las cuentas con mayores privilegios, como las cuentas de administrador, esto implica el uso de capacidades que limitan cuánto acceso tienen estas cuentas y cuándo tienen acceso. También implica el uso de niveles más altos de políticas de autenticación basadas en riesgos para estas cuentas. Este principio también implica la identificación y protección de datos sensibles. Por ejemplo, una carpeta de documentos asociada con un proyecto confidencial solo debe incluir permisos de acceso para los miembros del equipo que lo necesiten. Estas protecciones juntas limitan cuánto daño puede causar una cuenta de usuario comprometida.
Suponer incumplimiento	Minimice el radio de explosión y el acceso al segmento. Verifique el cifrado de extremo a extremo y use análisis para obtener visibilidad, impulsar la detección de amenazas y mejorar las defensas.	Este principio asume la probabilidad de que un atacante obtenga acceso a una cuenta, identidad, punto final, aplicación, API u otro activo. Para responder, Microsoft protege todos los activos en consecuencia para limitar el daño. Este principio también implica la implementación de herramientas para la detección continua de amenazas y la respuesta rápida. Idealmente, estas herramientas tienen acceso a señales integradas en su entorno y pueden tomar acciones automatizadas, como deshabilitar una cuenta, para reducir el daño lo antes posible.

Fuente: Tomado de ZERO TRUST adoption framework overview [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, abril, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview.

6.2.1 Verificar explícitamente

“El objetivo de la verificación de identidad es confirmar y establecer un vínculo entre la información reclamada identidad y la existencia real del solicitante involucrado en la prueba de identidad proceso”[97]. En un entorno de confianza donde coexisten usuarios y dispositivos, es necesario autenticar y autorizar basándose en todos los puntos de datos disponibles, como la identidad del usuario, la condición del dispositivo, la clasificación de los datos y las anomalías. El enfoque Zero Trust no depende de una ubicación específica, sino de los usuarios, aplicaciones y dispositivos, permitiendo el acceso a las aplicaciones y datos requeridos desde cualquier lugar.

Se establecen medidas de protección contra intentos de explotación de información confidencial, sin distinguir si provienen de personal interno o externo.

6.2.2 Privilegios mínimos

“El principio de mínimo privilegio es el concepto de que a los usuarios se les debe conceder sólo los privilegios que necesitan para realizar sus funciones laborales”[98]. Es indispensable conocer quiénes son los usuarios que intentan acceder a un servicio o recurso, basándose en la validación de los niveles de acceso permitidos a las infraestructuras, previamente verificados.

Se requiere la implementación de controles que proporcionen el acceso de forma condicional y que puedan validar directamente si la entidad cuenta con los privilegios necesarios para el acceso solicitado, asegurando así que cada persona tenga el acceso correspondiente. El acceso con privilegios mínimos limita a los usuarios a un acceso justo, en el momento adecuado y con la suficiente autorización.

6.2.3 Suponer incumplimiento

“La premisa es hacer lo contrario a lo que hacen las redes tradicionales, que nos permite conectarnos a una red y luego validar quién es. Aquí la idea es primero

[97] REGISTRO DE Publicaciones Técnicas de NIST SP 800-63A [Anónimo]. Instituto Nacional de Estándares y Tecnología [página web]. (Agosto, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.ipd.pdf.

[98] ¿QUÉ ES el principio del mínimo privilegio o zero trust? [Anónimo]. IDRIC [página web]. (21, noviembre, 2022). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.idric.com.mx/blog/post/que-es-el-principio-del-minimo-privilegio-o-zero-trust.

validar y después permitir una conexión, lo que trae como consecuencia evitar la proliferación de ataques cibernéticos de gran escala"[99]. El modelo parte de la premisa de no confiar en nadie. En base a esto, se debe asumir que existe una infracción constante en los sistemas de información. Para evitar que esta infracción se propague, los sistemas deben modificar cada solicitud.

Al realizar una inspección continua del tráfico de usuarios en busca de actividades sospechosas, se puede limitar el acceso y garantizar que los usuarios actúen de manera correcta a través de verificaciones. Un escaneo constante de actividades sospechosas permite a los profesionales de seguridad tomar medidas en tiempo real.

6.3 HERRAMIENTAS UTILIZADAS POR ZERO TRUST

6.3.1 Firewalls de próxima generación (NGFW)

"Un cortafuegos de próxima generación (NGFW) es la convergencia de la tecnología de cortafuegos tradicional con otras funciones de filtrado de dispositivos de red, como el control de aplicaciones en línea, un sistema integrado de prevención de intrusiones (IPS), capacidades de prevención de amenazas y protección antivirus, para mejorar la seguridad de la red empresarial"[100]. Estos dispositivos proporcionan una mayor visibilidad y control del tráfico en la red, permitiendo la segmentación y la aplicación de diferentes políticas de acceso basadas en la identidad. Incorporan capacidades avanzadas, como la inspección de paquetes a nivel de aplicación, prevención de intrusiones y filtrado de paquetes tradicionales de red.

Esto los diferencia de los firewalls tradicionales, ya que incluyen servicios de seguridad como la detección de malware, mitigación y filtrado de contenido web. Combinan los servicios UTM con las funciones propias del firewall, brindando una protección integral en un único dispositivo y plataforma.

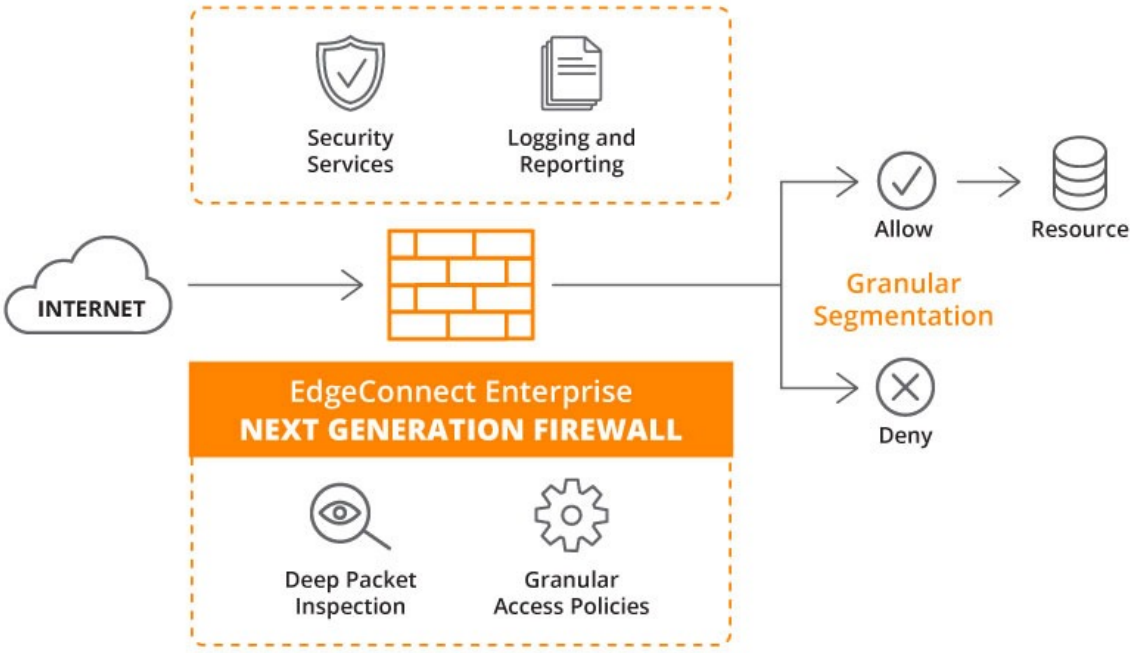
En la Figura 7, se evidencia como es el funcionamiento de NGFW, como mediante la inspección de tráfico y la aplicación de reglas y políticas puede proporcionar o denegar accesos a recursos de red.

---

[99] UNIVERSAL ZERO Trust: la estrategia clave para enfrentar la nueva realidad de ciberseguridad [Anónimo]. Forbes Colombia [página web]. (22, agosto, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://forbes.co/2024/08/22/negocios/universal-zero-trust-la-estrategia-clave-para-enfrentar-la-nueva-realidad-de-ciberseguridad.

[100] WHAT IS a Next-Generation Firewall? [Anónimo]. Líder en ciberseguridad y confianza cero | Zscaler [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.zscaler.es/resources/security-terms-glossary/what-is-next-generation-firewall.

Figura 7 NGFW (Next Generation Firewall)



Fuente: Tomado de ¿QUÉ ES un firewall de próxima generación (NGFW)? [Anónimo]. HPE Aruba Networking [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw.

6.3.2 Autenticación multifactor (MFA)

"Un sistema robusto de autenticación multifactor (MFA) para verificar la identidad de los usuarios, dispositivos y aplicaciones que intentan acceder a recursos en la red. Esto puede incluir técnicas como contraseñas fuertes, biometría, tokens de seguridad y certificados digitales"[101]. Lo cual proporciona a los usuarios múltiples factores de autenticación para acceder a un recurso, como una contraseña, token físico, aplicaciones móviles o biometría. Esto agrega una capa adicional de seguridad, validando la identidad de los usuarios de manera más robusta y compleja que con una contraseña común.

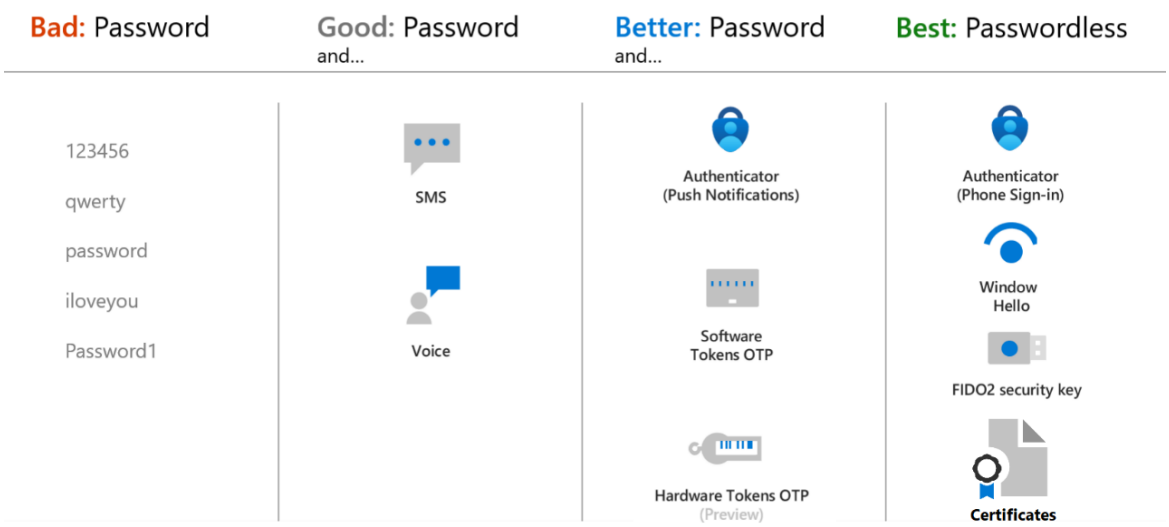
Se abandonan las prácticas de factor único, en las que un atacante solo necesita concentrarse en vulnerar una contraseña para suplantar al usuario. En el caso de la MFA (autenticación multifactor), si un atacante logra comprometer una contraseña

[101] PÉREZ, Anna. Zero Trust: la nueva tendencia en estrategias de ciberseguridad. OBS Business School [página web]. (9, abril, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.obsbusiness.school/blog/zero-trust-la-nueva-tendencia-en-estrategias-de-ciberseguridad.

pero no cuenta con un segundo método de autenticación que valide que es la persona que dice ser, no podrá continuar, lo que dificulta significativamente el acceso a la información por atacantes.

Siguiendo las mejores prácticas, se aconseja generar contraseñas más seguras acompañadas de un segundo factor de autenticación, sin comprometer la facilidad de uso según la necesidad. En la Figura 8, se evidencia cómo la combinación de contraseñas robustas con un segundo factor de autenticación, dependiendo del propósito, puede ofrecer una mayor seguridad y facilidad de uso.

Figura 8 MFA (Multi-Factor Authentication)



Fuente: Tomado de CONSIDERACIONES DE implementación para la autenticación multifactor de Microsoft Entra - Microsoft Entra ID [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (4, octubre, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-mx/azure/active-directory/authentication/howto-mfa-getstarted#plan-user-rollout.

6.3.3 Control de acceso basado en políticas

“Se centra en definir controles de acceso a través de políticas basadas en información contextual en tiempo real. Esto significa que las decisiones de acceso se toman considerando factores como los atributos del usuario, la información del dispositivo, la ubicación y la hora de acceso”[102]. Permite aplicar políticas y definir accesos granulares para limitar los privilegios de los usuarios y dispositivos. Estas

[102] EL PODER de la gobernanza del acceso basada en políticas: PBAC vs RBAC - SafePaaS [Anónimo]. SafePaaS [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.safepaas.com/es/articles/the-power-of-policy-based-access-governance/.

políticas incluyen restricciones basadas en la identidad, el contexto, la ubicación y otros factores relevantes al momento de conceder acceso.

La aplicación de estas políticas integra a los usuarios con las directrices establecidas por la organización, otorgándoles acceso a los sistemas de acuerdo con los roles y características que la organización determine.

6.3.4 Microsegmentación de red

Consiste en la creación de segmentos de seguridad dentro de la red, agrupados de acuerdo con controles de seguridad definidos para cada segmento único, "El término "micro-perímetro" se basa en el concepto de segmentar la red para limitar la posibilidad de que un posible atacante salte con facilidad de un lado a otro de la misma. Estos "micro-perímetros" deben construirse alrededor de la información sensible una vez se han identificado los flujos que sigue la misma"[103].

Es especialmente útil en redes empresariales que requieren interconexión, ya que permite segmentar la conectividad de manera ágil, lo que facilita la implementación de una nueva capa de seguridad en la red. Esto protege los datos y dispositivos existentes al tiempo que se adoptan tecnologías modernas, como las nubes y la tecnología móvil.

6.3.5 Herramientas de cifrado de datos

Como dice Kaspersky[104], el cifrado es la técnica que convierte datos de un formato legible a uno codificado, haciéndolos accesibles y procesables solo después de ser descifrados. Se utiliza principalmente en la seguridad de los datos para garantizar que la información no pueda ser robada ni leída con fines maliciosos.

El cifrado es una herramienta común en el día a día, desde la información que se ingresa en un navegador hasta los datos bancarios en las cuentas de ahorro. Todas estas aplicaciones utilizan cifrado de datos, también conocidos como algoritmos de cifrado. Solo las personas o herramientas autorizadas pueden acceder a esta información, utilizando técnicas de cifrado simétrico o asimétrico, según las necesidades específicas.

---

[103] MODELO ZERO Trust | Todo lo que debes que saber [Anónimo]. Sealpath [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.sealpath.com/es/blog/modelo-zero-trust-ciberseguridad/.

[104] CIFRADO DE datos y cómo hacerlo [Anónimo]. Kaspersky [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/encryption?srsltid=AfmBOooR--1N7adyygTvPCZQLKAN-BkDRjIDWcUS9lKpJcreQCfS2s8O.

6.3.6 Soluciones de visibilidad y monitoreo de red

"La confianza cero proporciona a las organizaciones visibilidad precisa y en tiempo real sobre el comportamiento de los usuarios, el estado de los dispositivos y el tráfico de red"[105]. Una de las principales características de la confianza cero es el monitoreo constante de todas las entidades dentro de una red, desconfiando de cualquier movimiento o acción que puedan realizar.

Las soluciones de monitoreo proporcionan métricas en tiempo real sobre el estado de la red, así como informes de análisis o incidentes que puedan estar ocurriendo. Además, monitorean los diferentes recursos de red y establecen reglas de umbrales aceptables, identificando aquellos que se desvían de estos parámetros. Estas soluciones son plataformas asequibles y fáciles de usar para el monitoreo de redes WAN distribuidas geográficamente, proporcionando información valiosa en tiempo real para prevenir posibles incidentes de seguridad.

7. METODOLOGÍAS ZERO TRUST

Dentro de las metodologías existentes de Zero Trust, se presenta una variedad que puede alinearse según el tamaño y la complejidad de la organización, considerando que algunas metodologías son mucho más complejas que otras, dependiendo de la magnitud de la empresa.

Existen otros factores que pueden ser determinantes al adoptar una metodología para implementar Zero Trust, como los recursos disponibles, ya que se deberá invertir tiempo, dinero y personal adecuado para asegurar una correcta implementación.

Otro factor para tener en cuenta es el sector al que pertenece la organización. Algunas metodologías ofrecen mayores beneficios en sectores específicos, lo que facilita la adaptación y adopción de Zero Trust, generando valor adicional.

Entre las metodologías reconocidas de Zero Trust, se revisarán algunas en términos de su aplicabilidad y efectividad, proporcionando una visión general de sus alcances para ser implementadas en las organizaciones colombianas.

[105] ¿QUÉ ES la confianza cero? | Una guía completa de la seguridad de confianza cero [Anónimo]. Elastic — The Search AI Company | Elastic [página web]. (2022). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.elastic.co/es/what-is/zero-trust.

7.1 NIST ZERO TRUST ARCHITECTURE

La metodología NIST Zero Trust Architecture (ZTA) ofrece a las organizaciones colombianas un marco integral que les permite mejorar la seguridad de su infraestructura de TI. Este marco se presenta en el documento NIST Special Publication 800-207, “El documento proporciona un marco para describir los riesgos de privacidad y las estrategias de mitigación, así como una proceso para que una empresa identifique, mida y mitigue los riesgos para la privacidad del usuario y la privacidad Información almacenada y procesada por una organización. Esto incluye información personal utilizada por la empresa para respaldar las operaciones de ZTA y cualquier atributo biométrico utilizado en la solicitud de acceso evaluaciones”[106].

Al adoptar un enfoque de confianza cero basado en la metodología de las NIST, las organizaciones colombianas pueden:

7.1.1 Reducir el riesgo de ciberataques

Como dice NIST[107], ZTA elimina la confianza implícita en la red, descartando la antigua creencia de que estar dentro de una red garantiza seguridad suficiente, lo que dificulta que los atacantes obtengan acceso a recursos confidenciales.

Los principios de ZTA, como la autenticación y autorización continuas, el acceso mínimo necesario y la segmentación de redes, ayudan a contener las infracciones y a limitar el daño potencial en caso de un incidente de seguridad.

7.1.2 Mejorar la visibilidad y el control

Como dice NIST[108], ZTA proporciona una visión centralizada de todos los usuarios, dispositivos y actividades en la red, previniendo comportamientos inusuales basados en reglas previamente estipuladas. Esto permite a las organizaciones identificar y responder rápidamente a amenazas potenciales.

[106] ZERO TRUST Architecture [Anónimo]. NIST [página web]. (Agosto, 2020). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
[107] Ibíd ., p.39
[108] Ibíd ., p.29

7.1.3 Aumentar la agilidad y la escalabilidad

Como dice NIST[109], ZTA es una arquitectura flexible y escalable que puede adaptarse a las necesidades cambiantes de las organizaciones, la cual puede implementarse en fases según la priorización de riesgos de la organización.

Facilita la adopción de nuevas tecnologías y el cumplimiento de regulaciones, ya que puede considerarse una metodología modular, donde una parte puede cumplir con la regulación a la que se somete la organización colombiana.

7.1.4 Mejorar el cumplimiento

"ZTA ayuda a las organizaciones a cumplir con una amplia gama de regulaciones de seguridad, como PCI DSS, HIPAA y SOC 2"[110]. Ideales para ciertas organizaciones colombianas que operan en sectores que requieren estas normativas.

Esto puede reducir el riesgo de multas y sanciones legales, ya que al adoptar la metodología Zero Trust se cubren la mayoría de las necesidades y requisitos regulatorios establecidos por el Gobierno Colombiano.

7.2 MICROSOFT ZERO TRUST SECURITY MODEL

El modelo de seguridad Zero Trust de Microsoft ofrece un enfoque integral de seguridad que puede ayudar a las organizaciones colombianas a proteger sus datos y recursos contra el acceso no autorizado. Se basa en el principio de "nunca confiar y siempre verificar", lo que significa que cada solicitud de acceso se autentica, autoriza y cifra completamente antes de otorgarse. "Zero Trust está diseñado para adaptarse a las complejidades del entorno moderno que acoge a la fuerza laboral móvil y protege las cuentas de los usuarios, los dispositivos, las aplicaciones y los datos dondequiera que se encuentren"[111].

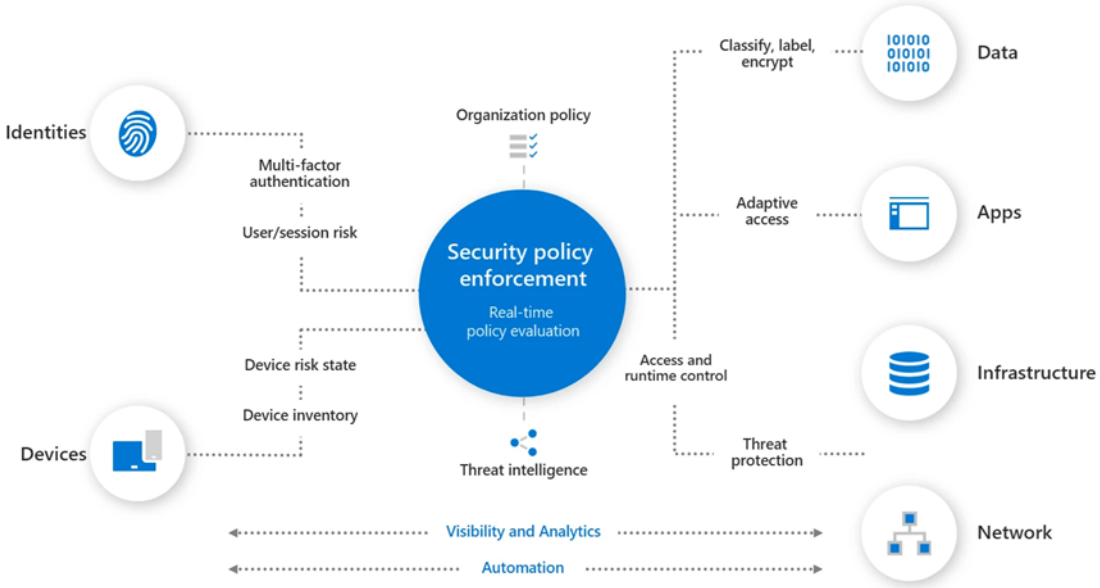
Este modelo ayuda a evitar que los atacantes accedan a información confidencial, incluso si lograran comprometer las credenciales o el dispositivo de un usuario de

[109] ZERO TRUST Architecture [Anónimo]. NIST [página web]. (Agosto, 2020). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
[110] Ibíd ., p.16
[111] WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12, abril, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview.

la organización. Microsoft ofrece recursos en su página web para una implementación efectiva de Zero Trust.

En la Figura 9, se evidencia la arquitectura de referencia propuesta por Microsoft para la arquitectura Zero Trust.

Figura 9 Arquitectura Microsoft Zero Trust



Fuente: Tomado de NEW MICROSOFT guidance for the DoD Zero Trust Strategy | Microsoft Security Blog [Anónimo]. Microsoft Security Blog [página web]. (16, abril, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.microsoft.com/en-us/security/blog/2024/04/16/new-microsoft-guidance-for-the-dod-zero-trust-strategy/.

Este modelo se destaca por:

7.2.1 Aplicabilidad

El modelo de seguridad Zero Trust de Microsoft es aplicable a organizaciones de todos los tamaños e industrias. Es especialmente adecuado para aquellas con una fuerza laboral distribuida o que utilizan aplicaciones basadas en la nube. “Las organizaciones de hoy necesitan un nuevo modelo de seguridad que se adapte de forma más efectiva a la complejidad del entorno moderno, que aproveche el lugar de trabajo híbrido y que proteja a las personas, los dispositivos, las aplicaciones y

los datos donde sea que se encuentren"[112]. Es ideal para las organizaciones que adoptaron un modelo de teletrabajo o híbrido tras la pandemia. Además, el modelo puede implementarse en una variedad de entornos, incluidos locales, híbridos y en la nube.

7.2.2 Efectividad

Se ha demostrado que el modelo de seguridad Zero Trust de Microsoft es efectivo para reducir el riesgo de filtraciones de datos. Como dice Balaoura[113], un estudio de Forrester Research encontró que las organizaciones que implementaron este modelo tenían un 70% menos de probabilidades de sufrir una filtración de datos en comparación con aquellas que no lo hicieron, gracias a las premisas de "nunca confiar y siempre verificar".

7.2.3 Beneficios

Como dice Microsoft[114], Además de reducir el riesgo de filtraciones de datos, el modelo de seguridad Zero Trust de Microsoft puede ofrecer otros beneficios a las organizaciones colombianas, entre los cuales se incluyen:

- Postura de seguridad mejorada: El modelo ayuda a identificar y mitigar los riesgos de seguridad antes de que puedan causar daños, mediante reglas, automatizaciones y validaciones.

- Complejidad reducida: Simplifica la gestión de la seguridad, facilitando el control del acceso a los recursos, reduciendo la cantidad de entornos y permitiendo una respuesta proactiva ante comportamientos inusuales.

- Mayor agilidad: Permite a las organizaciones adaptarse rápidamente a las necesidades cambiantes de seguridad. Al funcionar de manera modular, se

[112] MODELO DE Confianza cero - Arquitectura de seguridad moderna | Seguridad de Microsoft [Anónimo]. Your request has been blocked. This could be due to several reasons. [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.microsoft.com/es-mx/security/business/zero-trust.

[113] BALAOURAS, Stephanie. Zero Trust Security: The Business Benefits And Advantages. Forrester [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.forrester.com/zero-trust/.

[114] ADOPTING A Zero Trust approach is a technology and business imperative [Anónimo]. Microsoft [página web]. (Marzo, 2022). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/adopting-zero-trust-infographic-final-5-business-scenarios.pdf?culture=es-co&country=co.

pueden abordar ciertos riesgos de mayor prioridad alineados con la confianza cero, dejando otras fases para una implementación posterior.

- Costos reducidos: Ayuda a disminuir los costos asociados a filtraciones de datos y otros incidentes de seguridad. Comparativamente, el costo de implementar la metodología de Microsoft es menor que el de una recuperación tras un incidente de seguridad.

Dado que es una metodología proporcionada por Microsoft, se enfoca en muchos de los productos que esta compañía ofrece. Al ser uno de los proveedores más utilizados a nivel mundial, es posible que las organizaciones ya cuenten con alguno de estos productos, lo que facilita la implementación de los principios de Zero Trust. Microsoft ofrece una serie de recursos para ayudar a las organizaciones a implementar este modelo de seguridad, entre los cuales se incluyen:

- Microsoft Entra ID: "Microsoft Entra ID es un servicio de administración de identidades y acceso basado en la nube que los empleados pueden usar para acceder a recursos externos. Entre los recursos de ejemplo se incluyen Microsoft 365, Azure Portal y miles de otras aplicaciones SaaS"[115]. Es una solución de administración de identidad y acceso (IAM), que puede utilizarse en entornos locales, en la nube o híbridos para aplicar los principios de Zero Trust.

- Microsoft Defender for Cloud: Es una solución de seguridad en la nube diseñada para proteger los recursos basados en la nube contra amenazas, "Microsoft Defender for Cloud es una plataforma de protección de aplicaciones nativas de la nube (CNAPP) que se compone de medidas y prácticas de seguridad diseñadas para proteger las aplicaciones basadas en la nube frente a diversas amenazas cibernéticas y vulnerabilidades"[116].

- Microsoft Sentinel: Es una solución de gestión de eventos e información de seguridad (SIEM) basada en la nube, utilizada para detectar y responder a amenazas de seguridad, "Microsoft Sentinel es una Administración de eventos e información de seguridad (SIEM) escalable, nativa de la nube, que

[115] ¿QUÉ ES Microsoft Entra ID? - Microsoft Entra [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (28, mayo, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/entra/fundamentals/whatis.

[116] ¿QUÉ ES Microsoft Defender for Cloud? - Microsoft Defender for Cloud [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (8, agosto, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/azure/defender-for-cloud/defender-for-cloud-introduction.

ofrece una solución inteligente y completa para SIEM y orquestación, automatización y respuesta de seguridad (SOAR)"[117].

7.3 GOOGLE BEYONDCORP

BeyondCorp es el enfoque de Google para la seguridad Zero Trust, basado en la eliminación del perímetro de seguridad tradicional y la protección de los recursos en función de la identidad y el contexto del usuario. Es aplicable a una amplia gama de organizaciones y entornos, lo que contribuye a mejorar la seguridad, la visibilidad, el control, la agilidad, la escalabilidad y a optimizar los costos.

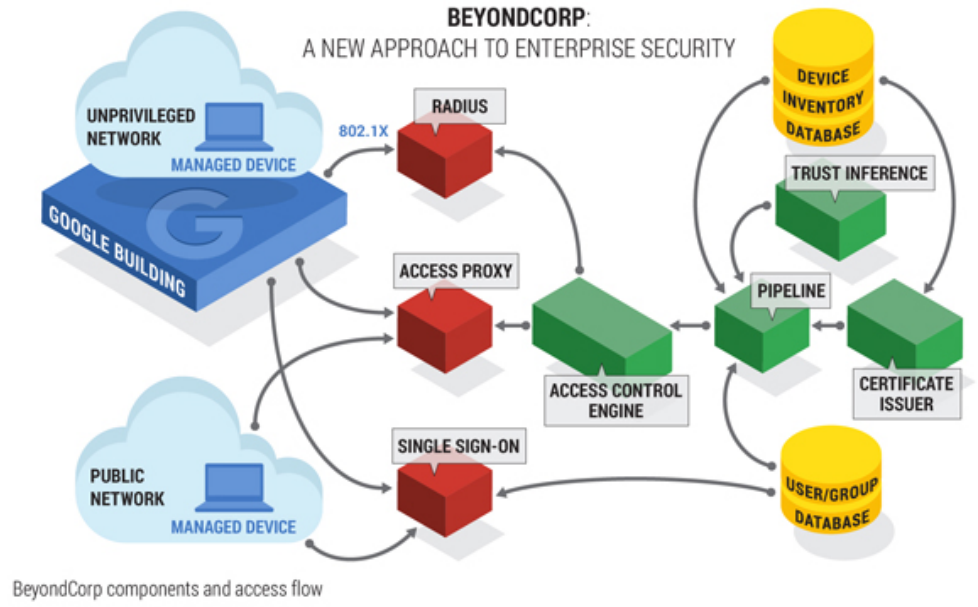
"BeyondCorp es la implementación del modelo de confianza cero de Google. Se basa en una década de experiencia de Google, combinada con ideas y prácticas recomendadas de la comunidad. Debido a que traslada los controles de acceso del perímetro de la red a los usuarios individuales, BeyondCorp habilita el trabajo seguro desde prácticamente cualquier ubicación y sin la necesidad de una VPN tradicional"[118].

La Figura 10, se visualiza como los componentes de arquitectura coordinados se orquestan bajo la metodología BeyondCorp.

[117] ¿QUÉ ES Microsoft Sentinel? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (22, mayo, 2024). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/azure/sentinel/overview?tabs=azure-portal.

[118] SEGURIDAD EMPRESARIAL de confianza cero de BeyondCorp [Anónimo]. Google Cloud [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://cloud.google.com/beyondcorp?hl=es-419.

Figura 10 Arquitectura BeyondCorp



Fuente: Tomado de BEYONDCORP | Run Zero Trust Security Like Google [Anónimo]. BeyondCorp [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.beyondcorp.com/.

Existen dos principios fundamentes en BeyondCorp:

7.3.1 Control de acceso a la red y a las aplicaciones

En BeyondCorp, un sistema inteligente decide quién puede acceder a la red, evaluando cada solicitud según el usuario, dispositivo y ubicación. Este sistema, que funciona como un guardián digital, asegura que solo las personas autorizadas entren y que los datos estén protegidos.

7.3.2 Visibilidad

“Una vez que un usuario tiene acceso a la red o las aplicaciones de una organización, la organización debe ver e inspeccionar continuamente todo el tráfico para identificar cualquier actividad no autorizada o contenido malicioso”[119]. Sin visibilidad podría existir una pérdida de datos sin conocimiento de esta perdida.

[119] WHAT IS BeyondCorp? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.paloaltonetworks.com/cyberpedia/what-is-beyondcorp.

Google BeyondCorp es aplicable a:

- Amplia gama de organizaciones: Organizaciones de todos los tamaños e industrias, desde pequeñas empresas hasta grandes corporaciones multinacionales. Su enfoque modular permite adaptarlo a las necesidades específicas de cada organización, incluyendo aquellas ubicadas en Colombia.

- Diversos entornos: Puede implementarse en una variedad de entornos, como redes locales, nubes públicas, nubes privadas y entornos híbridos. Su flexibilidad le permite ajustarse a las necesidades de cualquier organización, “Diseño sin perímetro, Conectarse desde una red particular no debe determinar a qué servicios puede acceder”[120].

- Soporte para múltiples plataformas: BeyondCorp es compatible con una amplia gama de plataformas y dispositivos, tales como portátiles, computadoras de escritorio, dispositivos móviles y navegadores web.

Al implementar esta metodología, se incrementa la efectividad en:

- Mejora de la seguridad: Ayuda a las organizaciones a mejorar su seguridad al reducir la superficie de ataque y eliminar la confianza implícita en la red, basada en enfoques tradicionales,” Consciente del contexto, el acceso a los servicios se concede en función de lo que sabemos sobre usted y su dispositivo”[121].

- Protección contra amenazas avanzadas: Ofrece protección frente a una variedad de amenazas avanzadas, como malware, ransomware y phishing, entre otras.

- Mejora de la visibilidad y el control: “Controles de acceso dinámicos, Todo acceso a los servicios debe ser autenticado, autorizado y encriptado”[122]. BeyondCorp brinda a las organizaciones mayor visibilidad y control sobre el acceso a la red, permitiéndoles identificar y responder rápidamente a amenazas o comportamientos inusuales que podrían ser indicios de una acción malintencionada.

[120] BEYONDCORP | Run Zero Trust Security Like Google [Anónimo]. BeyondCorp [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.beyondcorp.com/.
[121] BEYONDCORP | Run Zero Trust Security Like Google [Anónimo]. BeyondCorp [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.beyondcorp.com/.
[122] Ibíd .

- Incremento de la agilidad y la escalabilidad: Facilita la agilidad y la escalabilidad al permitir un acceso seguro a los recursos desde cualquier lugar, lo que favorece el trabajo remoto.

- Reducción de costos: Contribuye a la reducción de costos en seguridad al simplificar la administración de la red y disminuir la necesidad de hardware y software de seguridad tradicionales.

Esta solución es ideal para organizaciones colombianas que buscan proteger datos sensibles de sus clientes o que requieren un acceso seguro a aplicaciones y recursos internos.

7.4 FORRESTER ZERO TRUST MODEL

El modelo Zero Trust de Forrester proporciona un marco centrado en el cliente para la implementación de esta estrategia. Define cinco principios clave para la seguridad: confianza cero, microsegmentación, análisis continuo, respuesta automática y gobierno centrado en el riesgo.

"Forrester desarrolló el modelo y acuñó el nombre Zero Trust en 2009 como una alternativa muy necesaria a los antiguos modelos de seguridad basados en perímetros. El modelo se convirtió en el estándar de oro entre los equipos de seguridad que trabajan para defenderse de violaciones devastadoras"[123]. La metodología es una herramienta valiosa que puede ayudar a las organizaciones a mejorar su seguridad, siendo aplicable y efectiva. Además, ofrece una serie de beneficios adicionales, como una mayor visibilidad y control de la actividad en la red, una mayor confianza por parte de los clientes y una gestión de la seguridad más simplificada.

La metodología del modelo Zero Trust de Forrester apoya a las organizaciones de la siguiente manera:

- Proporciona un marco de referencia claro y conciso: Ofrece una guía paso a paso para implementar una estrategia de seguridad Zero Trust, lo que facilita que organizaciones de todos los tamaños y sectores puedan adoptarla y apropiarla internamente.

- Se adapta a las necesidades específicas de la organización: No es una solución única para todos, sino que puede ajustarse a las necesidades específicas de cada organización, alineándose con su visión estratégica, en la cual la seguridad está diseñada para impulsar el logro de sus metas. Esto

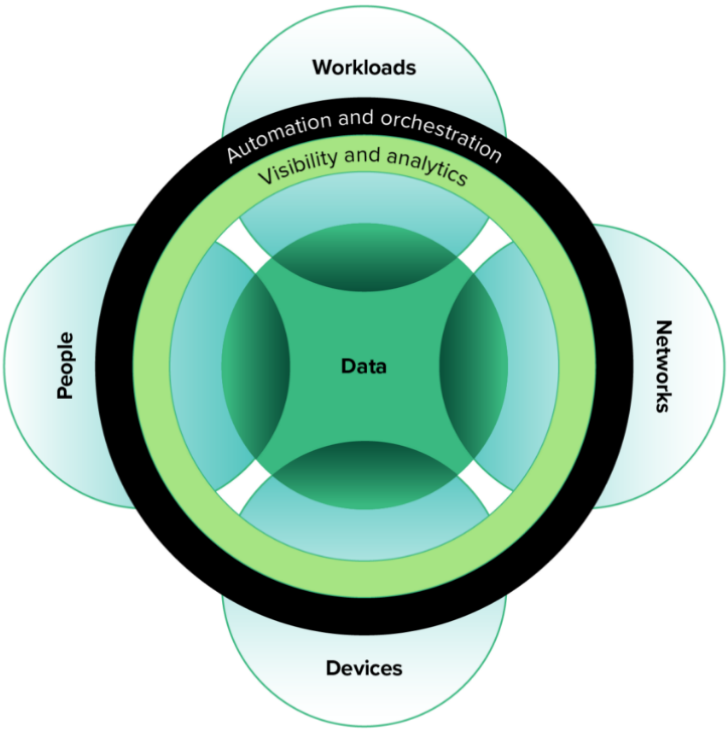
[123] BALAOURAS. Stephanie. Forrester [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.forrester.com/zero-trust/.

se debe a que el modelo se basa en principios, y no en prescripciones específicas enfocadas en soluciones vinculadas a marcas concretas.

- Puede implementarse de manera incremental: Como Dice Balaouras[124],No es necesario implementarlo de una sola vez. Las organizaciones pueden comenzar adoptando los principios básicos del modelo y luego ir ampliando gradualmente su aplicación, según las necesidades y los riesgos identificados.

La Figura 11, evidencia como Forrester propone un modelo para la seguridad de la información.

Figura 11 Modelo Forrester



Fuente: Tomado de BALAOURAS. Stephanie. Forrester [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.forrester.com/zero-trust/.

El modelo proporciona directrices para guiar una implementación efectiva, ya que:

[124] BALAOURAS. Stephanie. Forrester [página web]. [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.forrester.com/zero-trust/.

- Reduce el riesgo de ciberataques: Ayuda a las organizaciones a disminuir el riesgo de ciberataques al eliminar los puntos de confianza implícitos en las redes tradicionales.
- Mejora la protección de datos: Permite a las organizaciones proteger mejor sus datos mediante un control estricto sobre el acceso a los mismos.
- Simplifica la gestión de la seguridad: Facilita la gestión de la seguridad al centralizar las políticas de acceso y control, integrando la estrategia Zero Trust en los procesos de la organización.

El modelo mejora la visibilidad de la red y optimiza su control, lo que permite una detección más efectiva de posibles amenazas. Esto se convierte en un factor diferencial para cualquier cliente de una organización en Colombia, ya que pueden tener la certeza de que la empresa que maneja sus datos implementa medidas sólidas para protegerlos.

7.5 GARTNER ZERO TRUST ACCESS

El enfoque se centra en la seguridad del acceso a los recursos, proporcionando un marco para evaluar y seleccionar las soluciones de acceso de confianza cero (Zero Trust) adecuadas para una organización.

“La transición a la confianza cero requiere, en última instancia, una evolución en su enfoque de la gestión de identidades, dispositivos, aplicaciones, datos, redes y otros componentes del ecosistema de seguridad. El paso 1 es un cambio de mentalidad en los principios clave de seguridad”[125].

La metodología Gartner Zero Trust Access es aplicable a una amplia gama de organizaciones, independientemente de su tamaño, industria o ubicación. Es especialmente útil para aquellas que:

- Cuentan con una fuerza laboral remota o híbrida significativa.
- Manejan datos sensibles.
- Se enfrentan a un alto riesgo de ciberataques.
- Necesitan cumplir con regulaciones estrictas de cumplimiento.

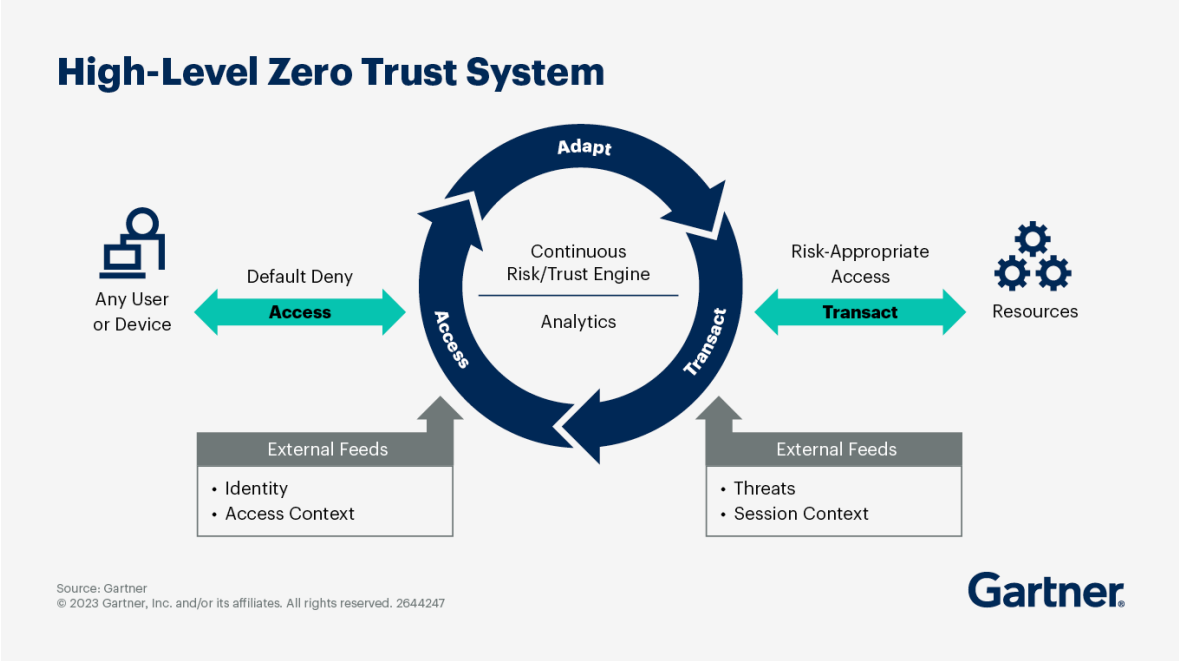
Esta metodología ofrece varios beneficios a las organizaciones, entre los que se incluyen:

[125] IMPLEMENTING ZERO Trust Security in the Public Sector [Anónimo]. Gartner [página web]. (2023). [Consultado el 25, septiembre, 2024]. Disponible en Internet: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

- Mayor seguridad: Reduce el riesgo de ciberataques al eliminar el concepto tradicional de "perímetro de red". Esto significa que los actores malintencionados no pueden acceder fácilmente a la red interna tras comprometer un solo punto de entrada.
- Mejor visibilidad y control: Otorga a las organizaciones una mayor visibilidad sobre el acceso a sus recursos, lo que les permite identificar y detener rápidamente actividades sospechosas, evitando así incidentes mayores.
- Mayor agilidad: Facilita la implementación y gestión de nuevas aplicaciones y servicios, sin la necesidad de crear una infraestructura de red nueva para cada uno, lo que además refuerza la seguridad en los planes de crecimiento de la organización.
- Reducción de costos: Ayuda a las organizaciones a reducir gastos al eliminar la necesidad de hardware y software tradicionales, como las VPN. Con la adopción del enfoque de confianza cero, existen diversas soluciones y precios que pueden ser considerados según las necesidades de la organización.

La Figura 12, evidencia como es aplicable la metodología en una organización.

Figura 12 Zero Trust System



Fuente: Tomado de IMPLEMENTING ZERO Trust Security in the Public Sector [Anónimo]. Gartner [página web]. (2023). [Consultado el 25, septiembre, 2024].

Disponible en Internet: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

Como dice CTOPerú[126], Aunque esta metodología presenta numerosos beneficios, también conlleva desafíos que deben ser considerados, ya que su implementación puede resultar compleja. Es esencial que las organizaciones planifiquen cuidadosamente el proceso.

Algunos de los pasos clave para la implementación incluyen:

- Identificar los recursos que deben protegerse.
- Evaluar las necesidades de acceso de los usuarios.
- Seleccionar una solución de confianza cero.
- Implementar la solución seleccionada.
- Probar y validar la solución.
- Monitorear y mantener la solución a lo largo del tiempo.

7.6 ZERO TRUST MATURITY MODEL DE SANS INSTITUTE

Se considera una herramienta de apoyo para que las organizaciones evalúen su estado actual de madurez en Zero Trust y desarrollen una hoja de ruta para su implementación.

“Un enfoque integral de Zero Trust abarca usuarios, aplicaciones e infraestructura. Zero Trust requiere una autenticación sólida de la identidad del usuario, la aplicación de políticas de "privilegios mínimos" y la verificación de la integridad del usuario. Aplicar Zero Trust a las aplicaciones elimina la confianza implícita con varios componentes de las aplicaciones cuando se comunican entre sí”[127].

El modelo se basa en cinco pilares:

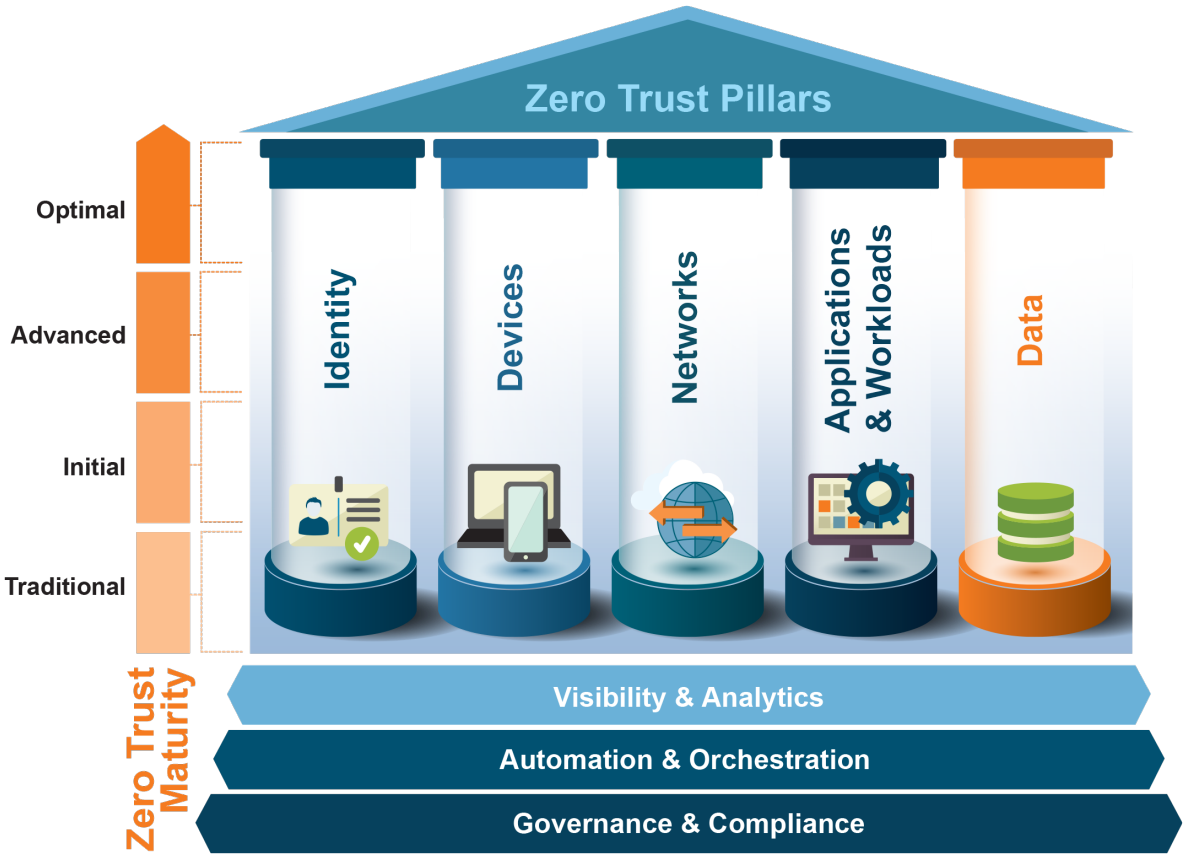
- Identidad: Garantizar que solo los usuarios y dispositivos autorizados puedan acceder a los recursos, aplicando el principio del menor privilegio posible.

[126] CAVASSA, Franca. 63% de las organizaciones han implementado Zero Trust. CTOPerú [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://ctoperu.pe/articulo/38767/63-de-las-organizaciones-han-implementado-zero-trust/?p=2.
[127] WHAT IS Zero Trust Architecture? | SANS Institute [Anónimo]. Cyber Security Training | SANS Courses, Certifications & Research [página web]. Disponible en Internet: https://www.sans.org/blog/what-is-zero-trust-architecture/.

- Dispositivos: Asegurar que los dispositivos cumplan con las políticas de seguridad antes de acceder a los recursos, garantizando el cumplimiento de las políticas organizacionales.
- Redes: Segmentar las redes y aplicar controles de acceso granulares para limitar el movimiento lateral de los atacantes; en caso de una intrusión, reducir la superficie de ataque.
- Aplicaciones y cargas de trabajo: Proteger las aplicaciones y cargas de trabajo contra ataques conocidos y desconocidos, basándose en la detección de comportamientos inusuales.
- Datos: Proteger los datos en reposo, en tránsito y en uso, sin importar la forma en que estos existan.

La Figura 13, evidencia los pilares según el modelo de SANS INSTITUTE y como este incluye capacidad transversales apoyando la maduración de la metodología.

Figura 13 CISA's Pilares Zero Trust



Fuente: Tomado de ZERO TRUST Blog Series - Blog 1: Adopting a Zero Trust Mindset | SANS Institute [Anónimo]. Cyber Security Training | SANS Courses,

Certifications & Research [página web]. (22, agosto, 2022). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.sans.org/blog/zero-trust-blog-1-adopting-zero-trust-mindset/.

Incluye tres capacidades transversales esenciales para una implementación exitosa de Zero Trust:

- Visibilidad y análisis: Obtener visibilidad de todos los usuarios, dispositivos, redes, aplicaciones y datos dentro del entorno corporativo.
- Automatización y orquestación: Automatizar las tareas de seguridad repetitivas y orquestar las respuestas ante incidentes, reduciendo los tiempos de reacción.
- Gobernanza: Establecer políticas y procedimientos claros para la gestión de la seguridad bajo el enfoque de Zero Trust.

"Cada organización debe considerar su postura y tecnologías de ciberseguridad empresariales actuales, los recursos de ciberseguridad, los activos de TI de alto valor, la tolerancia al riesgo, los requisitos regulatorios, así como la misión y los objetivos organizacionales para establecer un plan que realice mejoras hacia la confianza cero en la forma y el plazo que tengan más sentido y sean alcanzables para la organización"[128]. Este enfoque puede apoyar a las organizaciones colombianas en:

- Mejorar la seguridad: Reducir el riesgo de ciberataques al limitar el acceso a los recursos y al detectar y responder con mayor rapidez a las amenazas.
- Aumentar la agilidad: Facilitar la adopción de nuevas tecnologías y la transición a modelos de negocio más flexibles.
- Reducir los costos: Disminuir los costos de seguridad al simplificar la gestión y automatizar las tareas de seguridad repetitivas.

La metodología es aplicable a organizaciones de todos los tamaños e industrias, y el marco de referencia puede adaptarse para satisfacer las necesidades específicas de cada una.

Se trata de una herramienta valiosa que puede apoyar a las organizaciones colombianas en la mejora de su postura de seguridad. Al seguir las pautas del marco, las organizaciones pueden desarrollar una estrategia de Zero Trust que sea efectiva y adaptable a sus necesidades específicas.

[128] ZERO TRUST Blog Series - Blog 1: Adopting a Zero Trust Mindset | SANS Institute [Anónimo]. Cyber Security Training | SANS Courses, Certifications & Research [página web]. (22, agosto, 2022). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.sans.org/blog/zero-trust-blog-1-adopting-zero-trust-mindset/.

8. GUÍA DE IMPLEMENTACIÓN ZERO TRUST

En el panorama actual de amenazas en constante evolución, donde cada avance tecnológico puede desencadenar una nueva forma de vulnerabilidad cibernética, los enfoques de seguridad tradicionales ya no resultan suficientes. La arquitectura Zero Trust ofrece un modelo de seguridad más robusto y adaptable, que puede ayudar a las organizaciones colombianas a proteger sus datos y activos más valiosos.

Esta guía proporciona una estructura para implementar Zero Trust en una organización colombiana. Acompaña al lector a través de los pasos esenciales, desde la definición de los objetivos de seguridad hasta la implementación de las tecnologías y procesos necesarios.

8.1 PASO 1: DEFINIR SUS OBJETIVOS DE SEGURIDAD

El primer paso consiste en realizar un inventario de los datos, aplicaciones, activos y servicios que se requieren proteger. Esto permite identificar y definir la superficie de ataque potencial, evitando la implementación de políticas y herramientas en toda la infraestructura de manera indiscriminada.

Se debe priorizar la información o los activos considerados sensibles, o aquellos que puedan ser de interés para posibles atacantes. Dependiendo del sector en el que opere la organización, se definen distintos elementos que requieren protección bajo la metodología Zero Trust.

Para comprender claramente los objetivos a proteger, es necesario comenzar a desarrollar una estrategia para alcanzarlos, la cual puede estructurarse en tres fases:

8.1.1 Identificar Activos Críticos

“Los activos críticos son aquellos cuyo rendimiento y disponibilidad tienen un impacto significativo en la capacidad de una organización para cumplir con sus objetivos comerciales y operativos”[129]. Se deben identificar los datos, aplicaciones y sistemas esenciales para las operaciones de la organización. Estos activos deben

[129] QUÉ ES la criticidad y cuál es su importancia [Anónimo]. Euroinnova International Online Education [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.euroinnova.com/ingenieria/articulos/criticidad#definicion-de-activos-criticos.

recibir la máxima protección y constituir el foco principal de la metodología Zero Trust.

8.1.2 Comprender las Amenazas

Es fundamental analizar las amenazas potenciales que enfrenta la organización, tales como ataques cibernéticos, malware, errores internos y desastres naturales. Este análisis ayuda a priorizar los esfuerzos de seguridad.

8.1.3 Establecer Metas Específicas y Medibles

Se deben definir objetivos claros y cuantificables para la implementación de Zero Trust. Por ejemplo, reducir las brechas de datos en un 90% o mejorar el tiempo de respuesta ante incidentes en un 50%. Estos objetivos deben tener en cuenta factores como el tiempo, los costos y el personal dedicado. Una de las ventajas de la metodología Zero Trust es que permite su implementación gradual, según las necesidades de la organización.

8.2 PASO 2: EVALUAR EL ENTORNO ACTUAL

Una vez identificados los objetivos a asegurar, el siguiente paso es evaluar el entorno actual de dichos objetivos. Esto incluye identificar usuarios, dispositivos, aplicaciones y datos, entre otros. También es fundamental comprender cómo funcionan los flujos de trabajo y cómo se accede a los datos dentro de la organización. Esta información apoyará en la identificación de las áreas de mayor riesgo para la organización y en la determinación de dónde deben enfocarse los esfuerzos en pro de la seguridad.

“Conozca a los usuarios, los datos y los recursos para crear políticas de seguridad coordinadas acordes con la empresa. Este proceso requiere descubrir y clasificar los recursos en función del riesgo, definiendo límites de recursos granulares y separando a los usuarios según los roles y las funciones”[130].

Para evaluar el entorno, se puede dimensionar el entorno actual mediante los siguientes pasos:

[130] IBM. ¿Qué es Zero Trust? | IBM. IBM - United States [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust.

8.2.1 Inventario de Activos

“Los activos informáticos de una empresa son los recursos tecnológicos de la información y la comunicación (TIC) que emplea para gestionar la información que maneja”[131]. Se debe realizar un inventario completo de todos los usuarios, dispositivos, aplicaciones y datos del entorno. Esto incluye información sobre la ubicación, propiedad y niveles de acceso. Para este fin, es recomendable utilizar una herramienta de gestión de archivos, la cual ayudará a automatizar los inventarios y a clasificar los activos.

8.2.2 Mapeo de Flujos de Trabajo

Analizar cómo fluyen los datos a lo largo de la organización, identificando los puntos de acceso y las rutas que podrían ser explotadas por atacantes. Es importante tener en cuenta aquellos datos que se consideren críticos para el negocio, “El análisis de datos ayuda a las empresas a obtener una mayor visibilidad y un conocimiento más profundo de sus procesos y servicios”[132].

8.2.3 Evaluación de Vulnerabilidades

Es fundamental realizar evaluaciones de seguridad periódicas para identificar posibles vulnerabilidades en aplicaciones y dispositivos. Se recomienda utilizar herramientas que identifiquen las vulnerabilidades en los sistemas, priorizando la remediación de aquellas que sean más críticas para la organización. Asimismo, se deben emplear herramientas que permitan monitorear redes y detectar actividades inusuales que puedan desencadenar una amenaza.

“El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad”[133]. Una herramienta valiosa utilizada en el ámbito de la seguridad informática es la matriz de riesgos. Dentro de la estrategia para evaluar el entorno y dimensionar dónde se deben enfocar los esfuerzos de seguridad de la metodología Zero Trust, el uso de una matriz de riesgos brindaría información

[131] QUÉ SON los activos informáticos y cómo se valoran [Anónimo]. Perito Informático - Peritaje informático [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://peritoinformatico.es/que-es-un-activo-informatico-y-como-se-valoran/.

[132] ¿QUÉ ES el análisis de datos? - Explicación del análisis de datos - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/data-analytics/.

[133] GUÍA DE gestión de riesgos [Anónimo]. MINTIC [página web]. (2016). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf.

importante sobre los aspectos críticos que presentan un mayor riesgo dentro de la organización y que requieren mayor atención.

8.2.4 Análisis de Permisos de Acceso

"Un permiso de acceso es una clase de permiso diseñado para gestionar el acceso a áreas definidas en las que se realiza trabajo. Los permisos de acceso se pueden utilizar para gestionar el acceso a empleados internos y visitantes o contratistas externos"[134]. Es necesario revisar los permisos de acceso de todos los usuarios y grupos. Se debe asegurar que solo se otorgue acceso a los recursos necesarios para la realización de las tareas asignadas, siguiendo la premisa del mínimo privilegio posible. Es crucial priorizar aquellos accesos con privilegios elevados.

8.3 PASO 3: DESARROLLAR UNA ESTRATEGIA ZERO TRUST

Una vez se tenga una comprensión clara de los objetivos y del entorno actual, se debe comenzar a desarrollar una estrategia Zero Trust. Cabe recordar que Zero Trust es un modelo flexible que puede adoptarse de manera gradual y que es adaptable a las necesidades cambiantes de la organización. Para lograr el éxito en la implementación del modelo de seguridad, es fundamental contar con la colaboración de las diferentes áreas que componen la organización, además de tener en cuenta que la inversión en nuevas tecnologías es necesaria para asegurar un modelo de protección a largo plazo.

La estrategia debe incluir los siguientes elementos:

8.3.1 Principios Zero Trust

Como dice Microsoft[135], Los principios Zero Trust son los fundamentos de la estrategia y deben adoptarse para guiar todas las decisiones relacionadas con la implementación de Zero Trust en la organización.

[134] IBM MAXIMO Health, Safety and Environment version 8.1 and later, and SaaS [Anónimo]. IBM - United States [página web]. (25, junio, 2024). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/docs/es/mhs-and-em/continuous-delivery?topic=permits-access.
[135] ¿QUÉ ES la confianza cero? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (15, abril, 2024). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/zero-trust-overview.

- Principio de Mínima Confiabilidad

Nunca se debe confiar de forma predeterminada en ningún usuario, dispositivo o solicitud de acceso; siempre se debe asumir que ya se está siendo atacado.

- Verificación Constante

Se debe verificar continuamente la identidad y la confiabilidad de todos los usuarios, dispositivos y solicitudes de acceso. “Cada nueva entrada a un sistema o solicitud de acceso a datos nuevos debe incluir algún tipo de autenticación para verificar la identidad del usuario”[136].

- Protección de los Datos

Se deben proteger los datos en todo momento, tanto en reposo como en tránsito. No se debe confiar en que la información está asegurada al 100%. Es necesario clasificar, encriptar y establecer etiquetas para determinar los tipos de datos y su protección.

- Reducción de la Superficie de Ataque

Se debe limitar el acceso a los recursos únicamente a los usuarios y dispositivos que lo necesiten. Permitir el acceso a recursos no requeridos hace que los sistemas sean más vulnerables.

- Segmentación Granular “Microsegmentación”

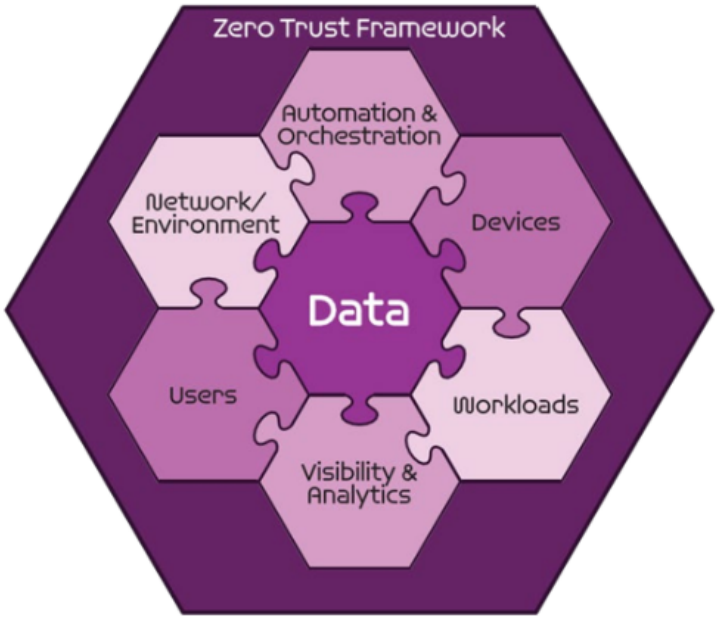
Se debe segmentar la red en zonas de seguridad para aislar los recursos críticos y contener posibles brechas. La microsegmentación de la red reduce el impacto de un posible ataque.

Los pilares de Zero Trust deben ser identificados dentro de la estrategia de implementación. Estos existen en pro de la protección de la información, y todas las funciones están interrelacionadas para asegurar el correcto funcionamiento de la metodología.

La Figura 14, se visualiza los principios Zero Trust y como estos se orquestan al redes de los datos.

[136] ¿QUÉ ES la seguridad zero trust? [Anónimo]. Netskope [página web]. [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://www.netskope.com/es/security-defined/what-is-zero-trust.

Figura 14 Marco de referencia Zero trust



Fuente: Tomado de ¿QUÉ ES la confianza cero? | Una guía completa de la seguridad de confianza cero [Anónimo]. Elastic — The Search AI Company | Elastic [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.elastic.co/es/what-is/zero-trust.

8.3.2 Factores de confianza

Los factores de confianza en la metodología Zero Trust son los elementos utilizados para evaluar la confiabilidad de los usuarios, dispositivos y solicitudes de acceso. Estos factores deben ser tenidos en cuenta:

- Identidad del Usuario

"La autenticación de usuarios es el proceso de verificar que los usuarios son quienes dicen ser. Es una parte crucial de la ciberseguridad, que permite a las organizaciones controlar el acceso a los sistemas y datos"[137]. Se refiere a elementos como el nombre de usuario, la contraseña, la autenticación multifactor (MFA) y la biometría. Una estrategia de confianza cero requiere la verificación explícita de la identidad, el uso de principios de acceso con privilegios mínimos y la asunción de

[137] AUTENTICACION DE usuario [Anónimo]. Silverfort [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.silverfort.com/es/glossary/user-authentication/.

posibles infracciones. Todo lo que pueda confirmar que el usuario que está ingresando a un recurso es realmente quien dice ser es fundamental.

- Salud del Dispositivo

"Conjuntos de reglas y condiciones que se usan para evaluar la configuración de los dispositivos administrados"[138]. El estado del sistema operativo, el software, el antivirus actualizado y los parches de seguridad son factores esenciales para garantizar que el dispositivo cuenta con un nivel adecuado de seguridad. Estos elementos validan que los dispositivos utilizados por los usuarios cumplen con los requisitos mínimos para acceder a los recursos corporativos.

- Comportamiento del Usuario

"El análisis del comportamiento de usuarios y entidades, o UEBA, es un tipo de software de seguridad que utiliza análisis de comportamiento, algoritmos de aprendizaje automático y automatización para identificar comportamientos anormales y potencialmente peligrosos de usuarios y dispositivos"[139]. Las soluciones UEBA (User and Entity Behavior Analytics) utilizan lo que aprenden para identificar comportamientos anómalos y clasificarlos según el riesgo que representan. Por ejemplo, varios intentos fallidos de autenticación en un breve período de tiempo o patrones anormales de acceso al sistema podrían indicar una amenaza interna, lo que generaría una alerta con una puntuación de riesgo baja. El análisis de patrones de acceso y la detección de anomalías permiten prevenir posibles violaciones de seguridad.

- Ubicación del Dispositivo

"La georreferenciación es el proceso de alinear imágenes satelitales u otros tipos de mapas con coordenadas geográficas del mundo real"[140]. El uso de geofencing, VPN y la detección de acceso remoto permite determinar y delimitar desde dónde y cómo se puede acceder a los recursos de manera geográfica, lo que reduce la exposición a posibles atacantes.

---

[138] DIRECTIVAS DE cumplimiento de dispositivos en Microsoft Intune [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (4, julio, 2024). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/mem/intune/protect/device-compliance-get-started.

[139] IBM. ¿Qué es el análisis del comportamiento de usuarios y entidades (UEBA)? | IBM. IBM - United States [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/mx-es/topics/ueba.

[140] WHAT IS Georeferencing? [Anónimo]. LocationIQ - API de geocodificación inversa gratuita, API de geocodificación, API de autocompletado [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://es.locationiq.com/glossary/georeferencing.

- Reputación del Dispositivo

La verificación en listas negras, el análisis de malware y la evaluación del comportamiento y reputación de los dispositivos pueden ayudar a prevenir incidentes de seguridad en la organización.

8.3.3 Políticas de acceso

"Una política de control de acceso es un conjunto de condiciones que, una vez evaluadas, determinan las decisiones de acceso"[141]. Las políticas de acceso representan un paradigma fundamental en la seguridad informática, reemplazando la mentalidad tradicional de "perímetro de confianza" por un enfoque más robusto y proactivo. En este nuevo modelo para las organizaciones, se asume que ninguna entidad, ni siquiera dentro de la red corporativa, es intrínsecamente confiable. Por lo tanto, se implementan medidas de seguridad rigurosas para verificar y validar continuamente la identidad, el estado y las autorizaciones de cada usuario, dispositivo y solicitud de acceso.

Los principios fundamentales que sustentan las políticas de acceso de Zero Trust son:

- Principio de Mínima Confiabilidad

"Zero Trust (confianza cero) adopta un enfoque de privilegios mínimos: solo otorga a los usuarios, dispositivos, aplicaciones y sistemas el nivel de privilegio mínimo necesario para hacer su trabajo. Un usuario solo tiene acceso a cosas específicas (aplicaciones, servicios, etc.) a través de una ruta predefinida, lo que evita que un hacker cause mucho daño en el caso de que pueda acceder a la red."[142]. Las políticas deben establecerse partiendo de la premisa de no confiar en ningún usuario, dispositivo o solicitud de acceso de forma predeterminada. Por lo tanto, toda interacción debe estar sujeta a autenticación y autorización rigurosas, independientemente de su origen.

- Verificación Constante

Dentro de las políticas se debe establecer que la verificación de la identidad y la confiabilidad sea un proceso continuo. Se deben emplear mecanismos como la

[141] IBM SECURITY Verify Access [Anónimo]. IBM - United States [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/docs/es/sva/10.0.8?topic=administration-access-control-policies.
[142] PELKEY, Laura. Protecting data with the principle of least privilege. Salesforce [página web]. (10, mayo, 2023). [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://security.salesforce.com/es/blog/protecting-data-with-the-principle-of-least-privilege.

autenticación multifactor (MFA), el análisis de comportamiento del usuario (UEBA) y la detección de anomalías, para monitorear en tiempo real las actividades y evaluar el riesgo asociado a cada acceso.

- Protección de los Datos

La protección de la información confidencial es primordial dentro de las políticas de acceso. Estas deben garantizar que los datos estén encriptados tanto en reposo como en tránsito, y que solo los usuarios y dispositivos autorizados tengan acceso a ellos.

- Reducción de la Superficie de Ataque

"Reducir la superficie expuesta a ataques implica proteger los dispositivos y la red de la organización, lo que deja a los atacantes con menos oportunidades de realizar sus ataques"[143]. Limitar el acceso a los recursos únicamente a los usuarios y dispositivos que lo necesitan es crucial para minimizar la superficie de ataque. Esto se logra mediante la implementación de los principios de "justo a tiempo" y "solo lo suficiente", donde los usuarios obtienen únicamente los permisos necesarios para cumplir con sus tareas específicas, especificando los alcances y limitaciones dentro de las políticas.

- Segmentación Granular

La segmentación de la red en zonas de seguridad permite aislar los recursos críticos y contener las brechas de seguridad. “Las redes Zero Trust también utilizan la microsegmentación. La microsegmentación es la práctica de dividir los perímetros de seguridad en pequeñas zonas para mantener un acceso separado para las diferentes partes de la red”[144]. Esta segmentación debe definirse en relación con los recursos críticos dentro de las políticas, de manera que, si un atacante compromete un segmento, su acceso quede limitado a esa área específica, impidiendo que se propague a otras zonas de la red.

8.3.4 Tecnologías Zero Trust

Las tecnologías de Confianza Cero (Zero Trust) son la base para implementar una estrategia de seguridad robusta en una organización, basadas en su estructura y

[143] USAR REGLAS de reducción de la superficie expuesta a ataques para evitar la infección de malware - Microsoft Defender for Endpoint [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (2, mayo, 2024). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/defender-endpoint/attack-surface-reduction.

[144] CLOUDFLARE | Seguridad Zero Trust. [Anónimo]. Cloudflare [página web]. [Consultado el 22, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

desarrolladas específicamente para protegerla contra amenazas en constante evolución. Estas herramientas trabajan en conjunto para crear un entorno de confianza cero, donde cada usuario, dispositivo y solicitud de acceso se verifica y valida rigurosamente antes de otorgar acceso a recursos valiosos.

- Gestión de Identidad y Acceso (IAM)

“Los sistemas de Gestión de identidad y acceso (IAM) verifican las identidades de los usuarios y controlan sus privilegios”[145]. La gestión de identidad y acceso (IAM) es uno de los principios más importantes de la seguridad de Confianza Cero, ya que permite controlar y administrar las identidades de los usuarios, desde empleados hasta clientes y socios externos. Esto se puede lograr mediante la verificación de credenciales robustas, compuestas por contraseñas complejas, acompañadas de autenticación multifactor (MFA) y, si es posible, biometría.

Zero Trust opera bajo el principio de "nunca confiar, siempre verificar", lo que implica que la identidad se convierte en el elemento fundamental que impulsa el proceso de verificación. En lugar de depender de estructuras anteriores, como los perímetros de red, Zero Trust centrado en la identidad pone énfasis en las identidades individuales y sus atributos asociados para determinar los permisos de acceso, “Al adoptar un enfoque centrado en la identidad, las organizaciones pueden lograr un control más granular sobre los privilegios de acceso y así reducir la posible superficie de ataque”[146].

Todo esto es necesario para autorizar y otorgar permisos de acceso en función de los roles que desempeñan dentro de la organización, supliendo sus necesidades específicas. Se pone especial atención en los accesos privilegiados, controlando el acceso a repositorios considerados confidenciales, limitando los datos a los que se puede acceder y monitoreando las actividades realizadas.

- Gestión de Dispositivos Móviles (MDM)

Con el creciente número de dispositivos móviles que acceden a la red corporativa, la gestión de dispositivos móviles (MDM - mobile device management) es crucial para proteger los datos y la infraestructura. “MDM es una solución que utiliza software como componente para el aprovisionamiento de dispositivos móviles y que

[145] ¿QUÉ ES la gestión de identidad y acceso? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/access-management/what-is-identity-and-access-management/.
[146] ¿QUÉ ES identidad cero confianza? [Anónimo]. Silverfort [página web]. [Consultado el 16, marzo, 2024]. Disponible en Internet: https://www.silverfort.com/es/glossary/identity-zerotrust.

a la vez protege los activos de una organización"[147]. A través del MDM, se pueden registrar y administrar los dispositivos que utilizan la red corporativa, basándose en políticas de seguridad y actuando como un medio para actualizar software.

En el entorno colombiano, es necesario poder bloquear y borrar de manera segura y remota los dispositivos extraviados o robados, con el fin de proteger los datos corporativos.

Existen miles de aplicaciones diseñadas para dispositivos móviles, por lo que es fundamental gestionar qué aplicaciones se pueden instalar y proteger los dispositivos contra posibles aplicaciones maliciosas.

- Puertas de Enlace de Acceso a la Red (NGFW)

Los Firewall de nueva generación (NGFW) actúan como guardianes de la red, filtrando y controlando el tráfico entrante y saliente. Estos cortafuegos realizan una inspección profunda, analizando el contenido de los datos e identificando y bloqueando tanto amenazas conocidas como nuevas.

Los NGFW suelen contar con capacidades de prevención de intrusiones, lo que ayuda a detectar y bloquear posibles actividades maliciosas en la red, desde intentos de acceso no autorizado hasta ataques más sofisticados.

"Un firewall de próxima generación (NGFW) permite o bloquea el tráfico entre redes. Los NGFW suman capacidades avanzadas como inspección de paquete a nivel de la aplicación y prevención de intrusiones hasta capacidades de firewall de red de filtrado de paquetes tradicionales"[148]. Como guardianes de la red, pueden restringir o bloquear el acceso a aplicaciones y recursos web y en la nube, reduciendo riesgos y mejorando la productividad según las políticas de las organizaciones que los implementan.

- Prevención de Intrusiones en Redes (IPS)

"Un sistema de prevención de intrusiones (IPS) ayuda a las organizaciones a identificar el tráfico malicioso y bloquea de manera proactiva el ingreso de dicho tráfico a su red"[149]. Los sistemas de prevención de intrusiones (IPS) complementan

[147] ¿ QUÉ ES la gestión de dispositivos móviles (MDM)? | IBM. IBM - United States [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/mobile-device-management.
[148] ¿QUÉ ES un firewall de próxima generación (NGFW)? [Anónimo]. HPE Aruba Networking [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw/.
[149] ¿QUÉ ES un IPS (Sistema de Prevención de Intrusiones)? | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips.

a los NGFW al proporcionar una capa adicional de protección en tiempo real contra ataques sofisticados. Las capacidades del IPS incluyen la detección de anomalías basadas en comportamientos inusuales que podrían indicar un posible ataque. Además, utilizando firmas de ataques conocidos, pueden proteger el tráfico de red.

- Seguridad en la Nube

Con la creciente adopción de la nube, las organizaciones necesitan soluciones de seguridad específicas para proteger los datos y aplicaciones alojados en ella. Existen organizaciones que no solo han adoptado una nube, sino que operan en múltiples nubes. La seguridad en la nube abarca la restricción de los recursos en la nube, para que solo aplicaciones, servidores y usuarios autorizados tengan acceso.

La información en tránsito y en reposo en la nube utiliza técnicas de cifrado para salvaguardar la información mediante métodos criptográficos robustos. Todo el tráfico, datos y acciones en la nube son monitoreados y registrados, formando un registro que permite identificar alteraciones.

- Integración y Automatización

Las tecnologías de Confianza Cero mencionadas, y muchas otras, no funcionan de manera aislada. Para una protección completa, es esencial integrar estas herramientas y automatizar los flujos de trabajo de seguridad. Esto permite una respuesta rápida y efectiva ante amenazas, minimizando el riesgo de brechas de seguridad. Al existir comunicación entre las herramientas, es posible mitigar incidentes de seguridad a mayor velocidad, previniendo y controlando las amenazas de manera automatizada, con un menor número de personal a cargo.

“Uno de los cambios significativos en las perspectivas que es un sello distintivo de los marcos de seguridad de Confianza cero es pasar de la confianza de forma predeterminada a la confianza por excepción”[150].

8.4 PASO 4: IMPLEMENTAR SU ESTRATEGIA ZERO TRUST

Una vez construida la estrategia de Zero Trust, se puede comenzar con su implementación. Esto implicará la adopción de las tecnologías y procesos necesarios, así como la capacitación de los empleados sobre los nuevos procedimientos de seguridad.

[150] VISIBILIDAD, AUTOMATIZACIÓN y orquestación con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (28, mayo, 2024). [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/visibility-automation-orchestration.

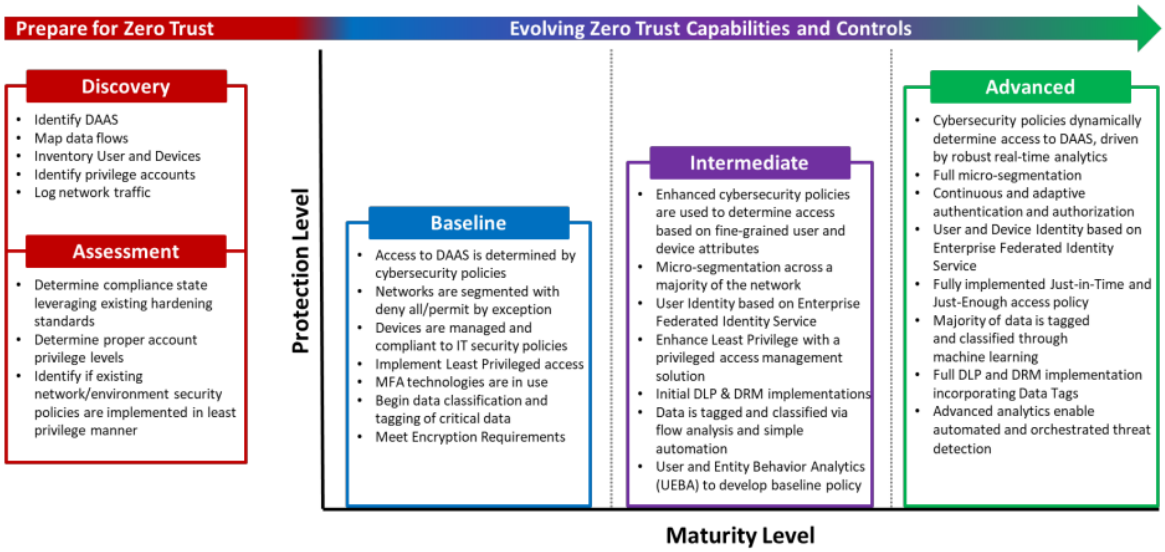
La implementación de la estrategia Zero Trust requiere integrar las tecnologías y procesos seleccionados en el entorno organizacional. Para implementar exitosamente Zero Trust, se deberán seguir los siguientes pasos:

8.4.1 Definir un Plan de Implementación

Basándose en la flexibilidad de la metodología Zero Trust, se debe establecer un cronograma de implementación que incluya fases y metas definidas. Este cronograma debe considerar tiempos de adquisición, configuración, pruebas y capacitación de las herramientas incorporadas, para que sea ejecutable dentro de plazos realistas y no genere afectaciones económicas a la organización. Se deben establecer fechas concretas para cada fase y asignar responsabilidades para la ejecución de cada una.

En la Figura 15, se evidencia una propuesta del modelo de maduración para la implementación de Zero Trust, la cual proporciona información valiosa sobre el estado de madurez de la estrategia Zero Trust dentro de la organización.

Figura 15 Modelo de madurez Zero Trust



Fuente: Tomado de MODELO de madurez del Department of Defense (DOD) [Anónimo]. LinkedIn [página web]. [Consultado el 07, marzo, 2024]. Disponible en Internet: https://media.licdn.com/dms/image/C4E12AQFGtcUjYPFSkw/article-inline_image-shrink_1500_2232/0/1633999949954?e=1720051200&v=beta&t=jrwZoDAK1zA_zfZ0f1_BskWVZbz78DT9xraps-lirlY.

En cada fase de implementación, es fundamental identificar un equipo con las cualidades y experiencia necesarias, asignar roles y responsabilidades, y asegurar la disponibilidad de tiempo y recursos financieros para la ejecución.

Para llevar a cabo una implementación adecuada, se deben evaluar los riesgos o amenazas potenciales y desarrollar planes de mitigación frente a los riesgos asociados, con el objetivo de asegurar el correcto desarrollo del proceso.

Una vez definido el plan y asignado el equipo encargado, se debe informar a las partes interesadas sobre los objetivos, beneficios y el impacto que traerá dicha implementación.

8.4.2 Implementar las Tecnologías Zero Trust

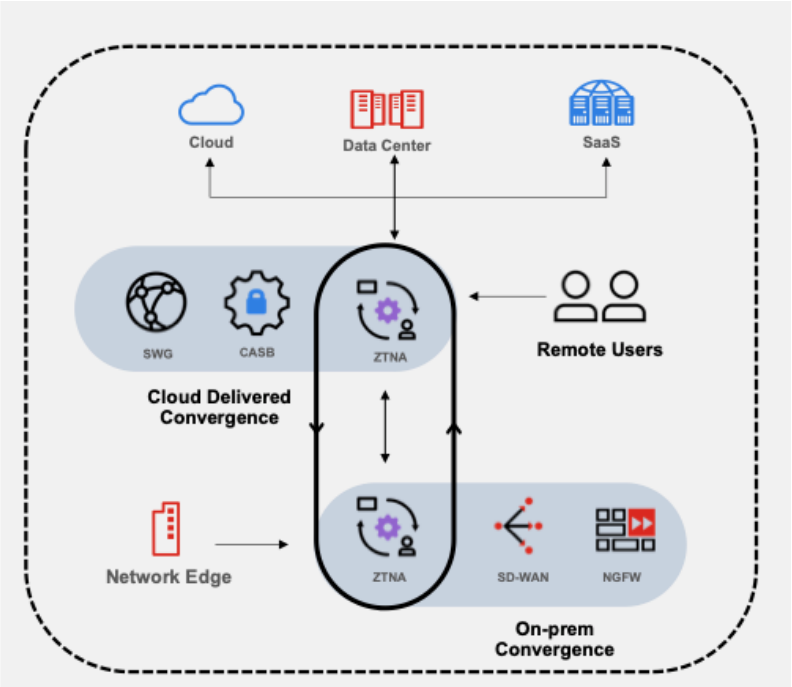
Una vez seleccionados los mecanismos de Zero Trust a implementar, se deben seguir los lineamientos y mejores prácticas indicados por el proveedor y las metodologías correspondientes. Estos pueden variar según el proveedor. Las configuraciones deben alinearse con las necesidades de la organización, integrando las herramientas con los sistemas y procesos ya existentes dentro de la misma.

Dependiendo de la marca de la tecnología implementada, los proveedores generalmente ofrecen ejemplos, guías, capacitación y acompañamiento para asegurar una implementación exitosa. Un ejemplo de esto es Fortinet, que ofrece explicaciones y recursos sobre cómo funcionan sus tecnologías, como su solución de borde de confianza cero, para apoyar la implementación, “El programa gratuito incluye todos los cursos de seguridad informática, desde el apoyo para seguridad de redes, seguridad dinámica de nube, operaciones de seguridad impulsadas por IA hasta el acceso a redes con zero trust”[151].

La Figura 16, evidencia un ejemplo de confianza de Borde Zero Trust ofrecida por la marca Fortinet, este tipo de guía varía según la marca y herramientas que se deseen implementar.

[151] CURSO DE ciberseguridad para profesionales de TI | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://www.fortinet.com/lat/training/cybersecurity-professionals.

Figura 16 Ejemplo Borde de confianza Zero Fortinet



Fuente: Tomado de ¿QUÉ ES Borde de confianza cero? | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.fortinet.com/lat/resources/cyberglossary/zero-trust-edge.

Es necesario realizar pruebas exhaustivas para garantizar el correcto funcionamiento de las herramientas implementadas, validando que las configuraciones cumplan con los requisitos de seguridad y rendimiento. Se deben ajustar las configuraciones según sea necesario, basándose en los resultados de cada prueba, para optimizar el rendimiento y la seguridad esperada.

Las herramientas deben ser administradas por usuarios previamente designados, quienes deben recibir capacitación sobre su manejo, gestión y mantenimiento, asegurando que comprendan los alcances y las políticas implementadas.

8.4.3 Establecer Políticas y Procedimientos

Los accesos de usuarios, dispositivos y aplicaciones deben estar claramente definidos en las políticas, estableciendo procedimientos para la gestión de identidades y accesos. Dichas políticas deben ser comunicadas a todos los empleados, asegurando que se utilice un lenguaje adecuado para que sean comprensibles y que los empleados comprendan su rol y responsabilidad en la seguridad.

Para asegurar el cumplimiento de las políticas y procedimientos, se deben generar controles de auditoría que verifiquen el cumplimiento de las regulaciones y estándares relevantes. Estas auditorías permitirán evaluar la efectividad de las medidas de seguridad mediante el monitoreo y registro de actividades, bajo el marco de la metodología Zero Trust.

"Muchas de estas políticas de confianza cero están orientadas a mejorar la visibilidad de la seguridad de una organización e identificar rápidamente actividades sospechosas. Si una cuenta comprometida intenta realizar acciones para las que carece de privilegios o intenta cruzar los límites de un segmento sin autorización, la organización puede tomar medidas para bloquear la cuenta o el tráfico sospechoso"[152]. Es importante revisar y actualizar los procedimientos y políticas según sea necesario, para adaptarlos a los cambios en el entorno y las amenazas actuales. Cuando se realicen estos cambios, deben ser comunicados a todas las partes interesadas.

8.5 PASO 5: MONITOREAR Y AJUSTAR LA ESTRATEGIA

La estrategia de Zero Trust establecida dentro de la organización no es algo estático, sino que debe ser monitoreada y ajustada continuamente a medida que cambian las necesidades de la organización y el panorama de amenazas.

El entorno de amenazas cibernéticas está en constante cambio, por lo que es crucial monitorear y ajustar la estrategia de Zero Trust de manera continua mediante los siguientes aspectos:

8.5.1 Monitoreo del Entorno

El entorno de ciberseguridad evoluciona y cambia constantemente, por lo cual es necesario monitorear que la estrategia de Zero Trust siga siendo efectiva frente a los nuevos tipos de amenazas. En caso de encontrar posibles falencias, se debe actuar sobre ellas. Estas falencias pueden detectarse mediante la recopilación de datos de seguridad y el análisis de registros para identificarlas. Además, se puede recurrir a pruebas de penetración con herramientas especializadas, actuando de manera proactiva.

[152] WHAT IS a Zero Trust Policy? [Anónimo]. Check Point [página web]. [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.checkpoint.com/es/cyber-hub/network-security/what-is-zero-trust/what-is-a-zero-trust-policy/.

Estas acciones permiten:

- Recopilación de datos: Implementar herramientas que recopilen información sobre usuarios, dispositivos, actividades, tráfico de red y eventos de seguridad.

- Análisis de datos: Utilizar herramientas analíticas para procesar y comprender los datos recopilados, identificando patrones, anomalías y posibles amenazas.

- Visualización de datos: Crear paneles de control y alertas para presentar información de seguridad relevante a los equipos de respuesta a incidentes y a los responsables de la toma de decisiones.

8.5.2 Evaluación y Revisión

Como dice CISA[153], La efectividad de la estrategia de Zero Trust debe ser evaluada para asegurar que cumpla con los objetivos para los cuales fue diseñada. Se espera que los niveles requeridos de esfuerzo y los beneficios obtenidos aumenten de forma significativa a medida que la madurez de la confianza cero avanza entre los pilares y dentro de estos. A medida que se traza el proceso de ZTA, se deben explorar oportunidades para promover la madurez de los pilares, con el fin de alinearse con las necesidades específicas de la misión y apoyar un mayor crecimiento en otros pilares. Esto implica evaluar las tecnologías implementadas, junto con los procesos y políticas de seguridad que las acompañan, con el objetivo de identificar áreas de mejora y posibles oportunidades de optimización.

Con base en los hallazgos del monitoreo y la evaluación, es necesario realizar cambios en la estrategia y en las configuraciones de seguridad. Esto puede incluir:

- Adopción de nuevas tecnologías: Implementar soluciones de seguridad nuevas o mejoradas para abordar amenazas emergentes y brechas de seguridad identificadas.

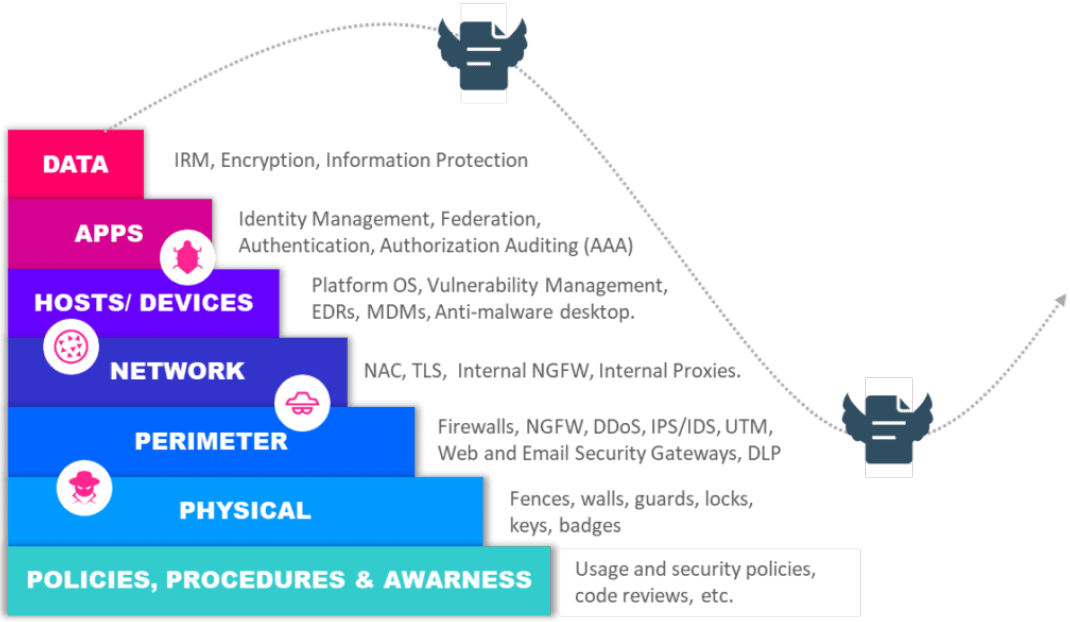
- Actualización de políticas: Revisar y actualizar las políticas de seguridad para reflejar los cambios en el entorno empresarial y las amenazas de seguridad.

[153] MODELO DE madurez de confianza cero [Anónimo]. Agencia de Ciberseguridad y Seguridad de Infraestructura CISA [página web]. (Abril, 2023). [Consultado el 26, septiembre, 2024]. Disponible en Internet: https://www.cisa.gov/sites/default/files/2024-05/zero_trust_maturity_model_v2_508%20(1)_ES.pdf.

- Mejora de procesos: Optimizar los procesos de seguridad existentes, como la gestión de identidades y accesos, la respuesta a incidentes y la recuperación ante desastres.

La Figura 18, se evidencia como las herramientas utilizadas en Zero Trust, son flexibles y adaptables a las necesidades organizaciones para poder impulsar aquellos pilares que se encuentren en un estado de madurez menor, pudieron promover a un buen nivel a todos los pilares de la metodología Zero trust.

Figura 17 Herramientas usadas en las capas ZT



Fuente: Tomado de ¿QUÉ ES el modelo de Seguridad Zero Trust? [Anónimo]. Sealpath [página web]. [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://www.sealpath.com/es/blog/modelo-zero-trust-ciberseguridad/.

La estrategia es flexible y siempre puede ser modificada o mejorada. Cada tecnología constituye un factor pensado para la adopción del modelo de Zero Trust en la organización, abarcando desde el gobierno de los datos hasta todas las posibles capas que pueden ser evaluadas y revisadas.

8.5.3 Adaptación y Mejora

Con base en el monitoreo y la evaluación, es necesario realizar los cambios indicados, tanto en la estrategia como en las configuraciones. Esto puede llevar a la adopción de nuevas tecnologías, ya que se trata de un entorno cambiante que evoluciona, “Mejorar continuamente la postura de seguridad implica ajustar las

políticas y prácticas para tomar decisiones más rápidas y fundamentadas. Esta operación requiere una evaluación y ajuste constante de las políticas, acciones de autorización y tácticas de corrección, con el fin de adecuar el perímetro de cada recurso de manera efectiva"[154]. Mediante la actualización de políticas y la mejora de los diferentes procesos de seguridad. La adaptación y la mejora continua son necesarias para mantener una postura de Zero Trust sólida frente al panorama evolutivo de amenazas.

El panorama de amenazas está en constante evolución, por lo que es fundamental adoptar una mentalidad de adaptación y mejora continua en la postura de Zero Trust. Esto significa:

- Ser proactivo: Anticipar las nuevas amenazas y tendencias de seguridad e implementar medidas preventivas antes de que se materialicen.

- Realizar pruebas continuas: Llevar a cabo pruebas de penetración y otras evaluaciones de seguridad para identificar y abordar vulnerabilidades de forma proactiva.

- Aprender de los incidentes: Analizar los incidentes de seguridad para comprender sus causas fundamentales y mejorar las prácticas de seguridad.

- La adaptación y la mejora continua reducen el riesgo de posibles ataques o violaciones de datos, al ser una práctica diseñada para brindar una respuesta ante incidentes más rápida y eficaz, lo que se traduce en confianza organizativa para los usuarios, socios y clientes.

[154] ¿QUÉ es Zero Trust? | IBM. IBM - United States [página web]. [Consultado el 27, septiembre, 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust.

9. CONCLUSIONES

El enfoque Zero Trust, basado en su flexibilidad y capacidad de adaptación a cualquier organización, es el paso que debe seguir cualquier entidad colombiana que quiera estar a la vanguardia y aprovechar los beneficios de no estar limitada a un único perímetro "seguro". Este enfoque permite a las organizaciones abrir sus horizontes tanto para sus colaboradores como para el personal externo, brindando acceso controlado y medido a los recursos corporativos, lo que fomenta el crecimiento a largo plazo.

Zero Trust es una metodología cada vez más aceptada en las organizaciones colombianas, ya que permite que sus colaboradores puedan trabajar desde cualquier lugar accediendo de manera segura a los recursos corporativos. Dada la infraestructura limitada en muchas ciudades y municipios de Colombia, las organizaciones deben apoyarse en metodologías probadas internacionalmente que faciliten la adopción de Zero Trust. Es fundamental validar las metodologías existentes y adoptar aquellas que mejor se ajusten a las necesidades de cada organización, ya que algunas ofrecen una mayor facilidad de implementación según el tamaño y el sector de la entidad.

Este trabajo propone una guía para implementar la metodología Zero Trust en organizaciones colombianas, basándose en metodologías internacionales que han sido utilizadas en diversos países, especialmente aquellos que, impulsados por la necesidad del trabajo híbrido, surgida durante la pandemia, se vieron en la obligación de replantear su enfoque de seguridad. La guía abarca desde la definición de objetivos de seguridad y la evaluación del entorno actual, hasta el desarrollo e implementación de una estrategia Zero Trust, acompañada de un monitoreo y ajustes constantes para asegurar que la metodología esté siempre alineada con las necesidades de seguridad de las organizaciones colombianas que deseen implementar dicha metodología.

10. RECOMENDACIONES

Para realizar una correcta implementación de la confianza cero, se deben evaluar y planificar exhaustivamente los activos de información y los recursos de red, con el fin de identificar los puntos vulnerables y los riesgos que puedan traducirse en riesgos tangibles.

Es fundamental generar conciencia sobre el modelo de extremo a extremo que se pretende seguir, asegurando que los directores apoyen el proceso hasta su correcta ejecución en todas las áreas.

Las políticas son esenciales para la implementación del enfoque Zero Trust. Actualmente, se recomienda estudiarlas detenidamente y adaptarlas a las necesidades específicas de la organización.

Hoy en día, los estándares internacionales apoyan todo el proceso de ejecución del modelo de confianza cero. Se recomienda validar cuáles estándares son aplicables según las necesidades del negocio y la actividad económica que se ejerza.

Zero Trust es un enfoque moderno para cumplir con los diversos requisitos normativos y de cumplimiento. Se recomienda explicarlo con claridad y conectar con todas las áreas de la organización, especialmente con los líderes, para obtener una comprensión que motive la adopción temprana del modelo Zero Trust.

Las metodologías de seguridad Zero Trust ofrecen un apoyo importante para las organizaciones colombianas que contemplen implementar esta metodología. Es crucial evaluar cuál es la más adecuada para la organización, considerando factores como facilidad de comprensión, tamaño de la entidad y sector al que pertenece.

Existen metodologías que proporcionan un paso a paso detallado para la adopción de Zero Trust, mientras que otras hacen referencia a marcas y soluciones específicas. Por ello, es importante evaluar la disposición de la organización respecto a la metodología que se pretende adoptar internamente.

Es esencial programar y realizar pruebas de las tecnologías implantadas para el desarrollo de Zero Trust, evaluando su efectividad y ajustándolas según sea necesario.

Abordar la implementación de Zero Trust desde una perspectiva de mejora continua es clave para asegurar que lo implementado siga funcionando correctamente y se mantenga alineado con las necesidades y el entorno de la organización colombiana.

Mantenerse al día con la metodología Zero Trust permitirá ajustar enfoques y tecnologías implementadas, asegurando que estén al tanto de las últimas amenazas y que la metodología siga siendo eficaz para la organización.

En la presente monografía se ofrece una guía de implementación basada en diversas metodologías disponibles actualmente. Es importante estar al tanto de las variaciones y evoluciones de estas metodologías, así como de nuevas guías y enfoques que puedan ser implementados en las organizaciones colombianas.

11. BIBLIOGRAFÍA

A COMPREHENSIVE Framework for Migrating to Zero Trust Architecture [Anónimo]. IEEE Xplore [página web]. (10 de febrero de 2023). [Consultado el 20 de abril de 2024]. Disponible en Internet: http://ieeexplore.ieee.org/document/10052642.

AKAMAI. MODELO DE seguridad Zero Trust [Anónimo]. Akamai [página web]. [Consultado el 18 de septiembre de 2024]. Disponible en Internet: https://www.akamai.com/es/glossary/what-is-zero-trust.

APPLYING ZERO Trust Principles to Enterprise Mobility [Anónimo]. CISA [página web]. (Marzo de 2022). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.cisa.gov/sites/default/files/2023-01/Zero_Trust_Principles_Enterprise_Mobility_For_Public_Comment_508C.pdf.

ADOPTING A Zero Trust approach is a technology and business imperative [Anónimo]. Microsoft [página web]. (Marzo de 2022). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/adopting-zero-trust-infographic-final-5-business-scenarios.pdf?culture=es-co&country=co.

AUTENTICACION DE usuario [Anónimo]. Silverfort [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.silverfort.com/es/glossary/user-authentication/.

BALANCE DE CIBERSEGURIDAD 2022 [Anónimo]. Inicio | CAI Virtual [página web]. [Consultado el 27 de marzo de 2024]. Disponible en Internet: https://caivirtual.policia.gov.co/sites/default/files/observatorio/Balance%20anual%202022.pdf.

BEYONDCORP: SEGURIDAD empresarial con el modelo de confianza cero [Anónimo]. Google Cloud [página web]. (2023). [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://cloud.google.com/beyondcorp?hl=es.

BREVE HISTORIA de la confianza cero [Anónimo]. Líder en ciberseguridad y confianza cero | Zscaler [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.zscaler.es/resources/infographics/brief-history-zero-trust.pdf.

BIBLIOGUÍAS: REVISIONES sistemáticas: Definición: ¿qué es una revisión sistemática? [Anónimo]. Inicio - Biblioguías - BiblioGuías at Biblioteca Universidad

de Navarra [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://biblioguias.unav.edu/revisionessistematicas/que-es-una-revision-sistematica.

BIBLIOGUÍAS: REVISIONES sistemáticas: Pasos o Etapas para realizar una revisión sistemática [Anónimo]. Inicio - Biblioguías - BiblioGuías at Biblioteca Universidad de Navarra [página web]. (20 de septiembre de 2024). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://biblioguias.unav.edu/revisionessistematicas/pasos-realizar-revisionsistematica.

BALAOURAS, Stephanie. Zero Trust Security: The Business Benefits And Advantages. Forrester [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.forrester.com/zero-trust/.

BEYONDCORP | Run Zero Trust Security Like Google [Anónimo]. BeyondCorp [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.beyondcorp.com/.

CURSO DE ciberseguridad para profesionales de TI | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://www.fortinet.com/lat/training/cybersecurity-professionals.

CLOUDFLARE | Seguridad Zero Trust. [Anónimo]. Cloudflare [página web]. [Consultado el 22 de septiembre de 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

CAVASSA, Franca. 63% de las organizaciones han implementado Zero Trust. CTOPerú [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://ctoperu.pe/articulo/38767/63-de-las-organizaciones-han-implementado-zero-trust/?p=2.

COLOMBIA SIGUE siendo el país con más ataques de ciberseguridad en Latinoamérica, según IBM [Anónimo]. Forbes Colombia [página web]. (28 de febrero de 2024). [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://forbes.co/2024/02/28/tecnologia/colombia-es-el-pais-con-mas-ataques-de-ciberseguridad-en-latinoamerica.

CSIRT GOBIERNO [Anónimo]. Gobierno Digital 2020 [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/CSIRT-Gobierno.

COMPRENDER EL modelo de seguridad Zero Trust - SSL.com [Anónimo]. SSL.com [página web]. (7 de mayo de 2024). [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.ssl.com/es/artículo/Comprender-el-modelo-de-seguridad-de-confianza-cero./.

CONSIDERACIONES DE implementación para la autenticación multifactor de Microsoft Entra - Microsoft Entra ID [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (4 de octubre de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-mx/azure/active-directory/authentication/howto-mfa-getstarted#plan-user-rollout.

CISO ZERO Trust Perspectives: Balancing Influence and Complexity |… [Anónimo]. Appgate [página web]. (21 de noviembre de 2023). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.appgate.com/blog/ciso-zero-trust-perspectives-balancing-influence-complexity-and-business-objectives.

CIFRADO DE datos y cómo hacerlo [Anónimo]. Kaspersky [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/encryption?srsltid=AfmBOooR--1N7adyygTvPCZQLKAN-BkDRjIDWcUS9lKpJcreQCfS2s8O.

DECRETO 338 de 2022 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (8 de marzo de 2022). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866.

DEFINICIÓN Y explicación de confianza cero [Anónimo]. Kaspersky [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/zero-trust?srsltid=AfmBOoqDvyd9sKoItJjV0GloP6uHOmg26olR_MxZLvFL3Ip0D7a0S8XW.

DEPARTMENT OF DEFENSE Zero Trust Overlays [Anónimo]. (Junio de 2024). [Consultado el 4 de mayo de 2024]. Disponible en Internet: https://dodcio.defense.gov/Portals/0/Documents/Library/ZeroTrustOverlays.pdf.

DIRECTIVAS DE cumplimiento de dispositivos en Microsoft Intune [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (4 de julio de 2024). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/mem/intune/protect/device-compliance-get-started.

DECRETO 620 de 2020 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (2 de mayo de 2020). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=118337.

ESTUDIO GLOBAL del trabajo híbrido de Cisco, 2022 [Anónimo]. Cisco: Software, Network, and Cybersecurity Solutions - Cisco [página web]. [Consultado el 15 de noviembre de 2023]. Disponible en Internet: https://www.cisco.com/c/dam/global/es_mx/solutions/collateral/hybrid-work/hybrid-work-study-market-factsheet.pdf.

EVOLVING ZERO Trust [Anónimo]. Microsoft [página web]. (Noviembre de 2021). [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWJJdT.

EL PODER de la gobernanza del acceso basada en políticas: PBAC vs RBAC - SafePaaS [Anónimo]. SafePaaS [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.safepaas.com/es/articles/the-power-of-policy-based-access-governance/.

EXECUTIVE ORDER 14028: Improving the Nation's Cybersecurity [Anónimo]. U.S. General Services Administration [página web]. [Consultado el 19 de septiembre de 2024]. Disponible en Internet: https://www.gsa.gov/technology/it-contract-vehicles-and-purchasing-programs/information-technology-category/it-security/executive-order-14028.

ENHANCING SECURITY with Multi-Factor Authentication in Zero Trust Model [Anónimo]. ISMS.online [página web]. (9 de octubre de 2023). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.isms.online/knowledge/multifactor-authentication-and-zero-trust/.

EXECUTIVE ORDER on Improving the Nation's Cybersecurity | The White House [Anónimo]. The White House [página web]. (12 de mayo de 2021). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

¿EN QUÉ consiste el GRC? - Explicación sobre el enfoque de gobernanza, riesgo y cumplimiento - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/grc/.

GUÍA DE seguridad Zero Trust para la empresa digital - SafePaaS [Anónimo]. SafePaaS [página web]. [Consultado el 21 de septiembre de 2024]. Disponible en

Internet: https://www.safepaas.com/es/articles/zero-trust-security-guide-for-the-digital-enterprise/.

GUIJARRO, Alfonso; YEPEZ, Jesica. Defensa en profundidad aplicado a un entorno empresarial. Revista Espacios, 2018, núm. 42, pp. 19-28. ISSN 0798 1015.

GUÍA DE gestión de riesgos [Anónimo]. MINTIC [página web]. (2016). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://gobiernodigital.mintic.gov.co/692/articles-5482_G7_Gestion_Riesgos.pdf.

IBM MAXIMO Health, Safety and Environment version 8.1 and later, and SaaS [Anónimo]. IBM - United States [página web]. (25 de junio de 2024). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/docs/es/mhs-and-em/continuous-delivery?topic=permits-access.

IMPLEMENTING ZERO Trust Security in the Public Sector [Anónimo]. Gartner [página web]. (2023). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

IBM. ¿Qué es el análisis del comportamiento de usuarios y entidades (UEBA)? | IBM. IBM - United States [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/mx-es/topics/ueba.

IBM. ¿Qué es Zero Trust? | IBM. IBM - United States [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust.

IBM SECURITY Verify Access [Anónimo]. IBM - United States [página web]. [Consultado el 27 de junio de 2024]. Disponible en Internet: https://www.ibm.com/docs/es/sva/10.0.8?topic=administration-access-control-policies.

INCREMENTO DE ciberataques en Colombia demanda estrategia Zero Trust [Anónimo]. Tecnogus [página web]. [Consultado el 28 de febrero de 2023]. Disponible en Internet: https://www.tecnogus.com.co/incremento-de-ciberataques-en-colombia-demanda-estrategia-zero-trust/.

IBM. ¿Qué es ITIL? | IBM. IBM - United States [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/mx-es/topics/it-infrastructure-library.

ISO/IEC 27001:2022 [Anónimo]. ISO [página web]. (2022). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.iso.org/es/contents/data/standard/08/28/82875.html.

INFORMACIÓN GENERAL sobre el marco de adopción de Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (16 de abril de 2024). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/adopt/zero-trust-adoption-overview.

LA SEGURIDAD Zero-Trust como garantía del trabajo remoto e híbrido - Artículo para Asociación @aslan [Anónimo]. Asociación @aslan [página web]. [Consultado el 16 de mayo de 2023]. Disponible en Internet: https://aslan.es/la-seguridad-zero-trust-como-garantia-del-trabajo-remoto-e-hibrido/.

LÓPEZ AGUDELO, David. Universal Zero Trust: la estrategia clave para enfrentar la nueva realidad de ciberseguridad. Forbes Colombia [página web]. [Consultado el 22 de agosto de 2024]. Disponible en Internet: https://forbes.co/2024/08/22/negocios/universal-zero-trust-la-estrategia-clave-para-enfrentar-la-nueva-realidad-de-ciberseguridad.

LEY 1266 de 2008 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (31 de diciembre de 2008). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488.

LEY 1341 de 2009 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (30 de julio de 2009). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36913.

LEY 1581 de 2012 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (17 de octubre de 2012). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

LEY 1273 de 2009 - Gestor Normativo [Anónimo]. Inicio - Función Pública [página web]. (5 de enero de 2009). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492.

LAS CINCO fases de la adopción de zero trust: de la confianza implícita a la explícita - eSemanal - Noticias del Canal [Anónimo]. eSemanal - Noticias del Canal [página web]. (21 de diciembre de 2021). [Consultado el 23 de septiembre de 2024].

Disponible en Internet: https://esemanal.mx/2021/12/las-cinco-fases-de-la-adopcion-de-zero-trust-de-la-confianza-implicita-a-la-explicita.

Microsoft. (2023, noviembre 14). Proteger datos con Zero Trust. Microsoft Learn. [Consultado el 10 de junio de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/data.

MODELO de madurez del Department of Defense (DOD) [Anónimo]. LinkedIn [página web]. [Consultado el 07 de marzo de 2024]. Disponible en Internet: https://media.licdn.com/dms/image/C4E12AQFGtcUjYPFSkw/article-inline_image-shrink_1500_2232/0/1633999949954?e=1720051200&v=beta&t=jrwZoDAK1zA_zfZ0f1_BskWVZbz78DT9xraps-lirlY.

MERRITT, Rick. ¿Qué Es Zero-Trust? - Blog oficial de NVIDIA Latino América. Blog oficial de NVIDIA Latino América [blog]. [Consultado el 28 de octubre de 2022]. Disponible en Internet: https://la.blogs.nvidia.com/blog/que-es-zero-trust/.

METODOLOGÍA GRC [Anónimo]. GRC Total [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://grctotal.com/metodologia/.

METODOLOGÍA ZERO Trust: fundamentos y beneficios [Anónimo]. INCIBE [página web]. (9 de octubre de 2023). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.incibe.es/incibe-cert/blog/metodologia-zero-trust-fundamentos-y-beneficios.

MODELO ZERO Trust | Todo lo que debes saber [Anónimo]. Sealpath [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.sealpath.com/es/blog/modelo-zero-trust-ciberseguridad/.

MODELO DE madurez de confianza cero [Anónimo]. Agencia de Ciberseguridad y Seguridad de Infraestructura CISA [página web]. (Abril de 2023). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.cisa.gov/sites/default/files/2024-05/zero_trust_maturity_model_v2_508%20(1)_ES.pdf.

NORMA INTERNACIONAL ISO 31000 [Anónimo]. Rama Judicial de Colombia: Información y servicios para la justicia [página web]. (Febrero de 2018). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.ramajudicial.gov.co/documents/5454330/14491339/Norma.ISO.31000.2018.Espanol.pdf/cb482b2c-afd9-4699-b409-0732a5261486.

NEW MICROSOFT guidance for the DoD Zero Trust Strategy | Microsoft Security Blog [Anónimo]. Microsoft Security Blog [página web]. (16 de abril de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet:

https://www.microsoft.com/en-us/security/blog/2024/04/16/new-microsoft-guidance-for-the-dod-zero-trust-strategy/.

OBANDO, Jairo. Ciberseguridad en Colombia: panorama completo de su estado en 2023. Linktic [página web]. [Consultado el 22 de septiembre de 2024]. Disponible en Internet: https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia.

ORDEN EJECUTIVA sobre servicios de seguridad de ciberseguridad | IBM® [Anónimo]. IBM - United States [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/es-es/services/executive-order-cybersecurity.

ORDEN EJECUTIVA 14028 y la cadena de suministro de software - Lazarus Alliance, Inc. [Anónimo]. Leading IT Cyber Security Services | Lazarus Alliance, Inc. [página web]. (18 de julio de 2024). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://lazarusalliance.com/es/executive-order-14028-and-the-software-supply-chain/.

PROTECCIÓN DE la infraestructura crítica con el modelo Zero Trust [Anónimo]. Palo Alto Networks [página web]. [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cybersecurity-perspectives/zero-trust-for-critical-infrastructure.

PROTECCIÓN DE aplicaciones mediante la confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (30 de abril de 2024). [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/applications.

PROTECCIÓN DE puntos de conexión con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (17 de abril de 2024). [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/endpoints.

PROTECCIÓN DE puntos de conexión con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. [Consultado el 20 de febrero de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/endpoints.

P. PHIAYURA AND S. TEERAKANOK. A Comprehensive Framework for Migrating to Zero Trust Architecture. IEEE [página web]. (2023). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://ieeexplore.ieee.org/document/10052642.

PRATT, Mary K. History and Evolution of Zero Trust Security. WhatIs [página web]. (12 de octubre de 2022). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.techtarget.com/whatis/feature/History-and-evolution-of-zero-trust-security.

PÉREZ, Anna. Zero Trust: la nueva tendencia en estrategias de ciberseguridad. OBS Business School [página web]. (9 de abril de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.obsbusiness.school/blog/zero-trust-la-nueva-tendencia-en-estrategias-de-ciberseguridad.

PROTECCIÓN DE redes con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (16 de abril de 2024). [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/networks.

PELKEY, Laura. Protecting data with the principle of least privilege. Salesforce [página web]. (10 de mayo de 2023). [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://security.salesforce.com/es/blog/protecting-data-with-the-principle-of-least-privilege.

¿POR QUÉ el modelo Zero Trust es importante en las organizaciones? [Anónimo]. Red Seguridad [página web]. (6 de mayo de 2022). [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.redseguridad.com/actualidad/ciberseguridad/por-que-el-modelo-zero-trust-es-importante-en-las-organizaciones_20220506.html.

¿QUÉ ES el modelo de Seguridad Zero Trust? [Anónimo]. Sealpath [página web]. [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://www.sealpath.com/es/blog/modelo-zero-trust-ciberseguridad/.

¿QUÉ es Zero Trust? | IBM. IBM - United States [página web]. [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust.

¿QUÉ ES la gestión de identidad y acceso? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/access-management/what-is-identity-and-access-management/.

¿QUÉ ES identidad cero confianza? [Anónimo]. Silverfort [página web]. [Consultado el 16 de marzo de 2024]. Disponible en Internet: https://www.silverfort.com/es/glossary/identity-zerotrust.

¿QUÉ ES la gestión de dispositivos móviles (MDM)? | IBM. IBM - United States [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/mobile-device-management.

¿QUÉ ES un firewall de próxima generación (NGFW)? [Anónimo]. HPE Aruba Networking [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw/.

¿QUÉ ES un IPS (Sistema de Prevención de Intrusiones)? | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.fortinet.com/lat/resources/cyberglossary/what-is-an-ips.

¿QUÉ ES la confianza cero? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (15 de abril de 2024). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/zero-trust-overview.

¿QUÉ ES la seguridad zero trust? [Anónimo]. Netskope [página web]. [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://www.netskope.com/es/security-defined/what-is-zero-trust.

¿QUÉ ES la confianza cero? | Una guía completa de la seguridad de confianza cero [Anónimo]. Elastic — The Search AI Company [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.elastic.co/es/what-is/zero-trust.

QUÉ SON los activos informáticos y cómo se valoran [Anónimo]. Perito Informático - Peritaje informático [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://peritoinformatico.es/que-es-un-activo-informatico-y-como-se-valoran/.

¿QUÉ ES el análisis de datos? - Explicación del análisis de datos - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/data-analytics/.

¿QUÉ ES Microsoft Entra ID? - Microsoft Entra [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (28 de mayo de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/entra/fundamentals/whatis.

¿QUÉ ES Microsoft Defender for Cloud? - Microsoft Defender for Cloud [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (8 de agosto de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet:

https://learn.microsoft.com/es-es/azure/defender-for-cloud/defender-for-cloud-introduction.

¿QUÉ ES Microsoft Sentinel? [Anónimo]. Microsoft Learn: Build skills that open doors in tu carrera [página web]. (22 de mayo de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/azure/sentinel/overview?tabs=azure-portal.

¿QUÉ ES el principio del mínimo privilegio o zero trust? [Anónimo]. IDRIC [página web]. (21 de noviembre de 2022). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.idric.com.mx/blog/post/que-es-el-principio-del-minimo-privilegio-o-zero-trust.

¿QUÉ ES una revisión sistemática de la literatura? | Qué es, diferencias y cómo hacer una [Anónimo]. ATLAS.ti [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://atlasti.com/es/guias/revisiones-bibliograficas/revision-sistematica.

¿QUÉ ES una arquitectura Zero Trust (confianza cero)? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cyberpedia/what-is-a-zero-trust-architecture.

¿QUÉ ES GRC? Gobierno, riesgo y cumplimiento [Anónimo]. GlobalSuite Solutions [página web]. (28 de diciembre de 2023). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.globalsuitesolutions.com/es/que-es-grc-gobierno-riesgo-cumplimiento/.

¿QUÉ SON las Tecnologías Habilitadoras? [Anónimo]. Inndromeda [página web]. (13 de octubre de 2020). [Consultado el 03 de octubre de 2024]. Disponible en Internet: https://inndromeda.es/actualidad/que-son-las-tecnologias-habilitadoras.

¿QUÉ SON los puntos de referencia del CIS? - Explicación de los puntos de referencia del CIS - AWS [Anónimo]. Amazon Web Services, Inc. [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://aws.amazon.com/es/what-is/cis-benchmarks/.

¿QUÉ ES Zero Trust? [Anónimo]. Trend Micro [página web]. [Consultado el 22 de septiembre de 2024]. Disponible en Internet: https://www.trendmicro.com/es_es/what-is/what-is-zero-trust.html.

¿QUÉ ES la microsegmentación? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 21 de septiembre de 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cyberpedia/what-is-microsegmentation.

QUÉ PODEMOS esperar de un enfoque Zero Trust [Anónimo]. WatchGuard Technologies [página web]. [Consultado el 19 de junio de 2024]. Disponible en Internet: https://www.watchguard.com/es/wgrd-news/blog/que-podemos-esperar-de-un-enfoque-zero-trust.

¿QUÉ ES el principio de mínimos privilegios? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/access-management/principle-of-least-privilege/.

¿QUÉ ES la confianza cero? Google Cloud [Anónimo]. Google Cloud [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://cloud.google.com/learn/what-is-zero-trust?hl=es.

¿QUÉ ES la criticidad y cuál es su importancia? [Anónimo]. Euroinnova International Online Education [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.euroinnova.com/ingenieria/articulos/criticidad#definicion-de-activos-criticos.

¿QUÉ ES el Acceso a la red Zero Trust (ZTNA)? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 22 de septiembre de 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/access-management/what-is-ztna/.

¿QUÉ ES la arquitectura Zero Trust? [Anónimo]. Trend Micro [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.trendmicro.com/es_es/what-is/what-is-zero-trust/zero-trust-architecture.html.

¿QUÉ ES la ciberseguridad? [Anónimo]. Kaspersky [página web]. [Consultado el 03 de octubre de 2023]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security.

¿QUÉ ES la segmentación de la red? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 03 de octubre de 2024]. Disponible en Internet: https://www.paloaltonetworks.es/cyberpedia/what-is-network-segmentation.

¿QUÉ ES un firewall de próxima generación (NGFW)? [Anónimo]. HPE Aruba Networking [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.arubanetworks.com/latam/faq/que-es-un-ngfw.R
REGISTRO DE Publicaciones Técnicas de NIST SP 800-63A [Anónimo]. Instituto Nacional de Estándares y Tecnología [página web]. (Agosto, 2024). [Consultado el

25, septiembre, 2024]. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.ipd.pdf.

RAGGI, Nicolás. Qué es el modelo de seguridad Zero Trust y por qué creció su adopción. Award-winning news, views, and insight from the ESET security community [página web]. (14 de septiembre de 2020). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.welivesecurity.com/la-es/2020/09/14/zero-trust-que-es-modelo-seguridad-crecio-adopcion/.

REVISIONES SISTEMÁTICAS: definición y nociones básicas [Anónimo]. SCIELO [página web]. (diciembre de 2018). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-01072018000300184.

RAMIRO, Rubén. ¿Qué es Zero Trust en ciberseguridad? CIBERSEGURIDAD.blog [página web]. (14 de junio de 2019). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://ciberseguridad.blog/que-es-zero-trust-en-ciberseguridad/.

SEGURIDAD ZERO Trust | ¿Qué es una red Zero Trust? [Anónimo]. CLOUDFLARE [página web]. [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/.

SEGURIDAD ZERO Trust: Una guía completa [Anónimo]. ENTRUST [página web]. [Consultado el 22 de septiembre de 2024]. Disponible en Internet: https://www.entrust.com/es/resources/learn/zero-trust.

SEGURIDAD EMPRESARIAL de confianza cero de BeyondCorp [Anónimo]. Google Cloud [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://cloud.google.com/beyondcorp?hl=es-419.

SP 800-207, Zero Trust Architecture | CSRC [Anónimo]. NIST Computer Security Resource Center | CSRC [página web]. (agosto de 2020). [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://csrc.nist.gov/pubs/sp/800/207/final.

UNIVERSAL ZERO Trust: la estrategia clave para enfrentar la nueva realidad de ciberseguridad [Anónimo]. Forbes Colombia [página web]. (22 de agosto de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://forbes.co/2024/08/22/negocios/universal-zero-trust-la-estrategia-clave-para-enfrentar-la-nueva-realidad-de-ciberseguridad.

USAR REGLAS de reducción de la superficie expuesta a ataques para evitar la infección de malware - Microsoft Defender for Endpoint [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (2 de mayo de 2024). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/defender-endpoint/attack-surface-reduction.

VISIBILIDAD, AUTOMATIZACIÓN y orquestación con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (28 de mayo de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/visibility-automation-orchestration.

VERITAS TECHNOLOGIES. La importancia de la privacidad de datos y el cumplimiento: guía completa. The Leader in Enterprise Data Management | Veritas [página web]. [Consultado el 23, septiembre, 2024]. Disponible en Internet: https://www.veritas.com/es/mx/information-center/data-privacy.

VISIBILIDAD, AUTOMATIZACIÓN y orquestación con Confianza cero [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (28 de mayo de 2024). [Consultado el 27 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/es-es/security/zero-trust/deploy/visibility-automation-orchestration.

WHAT IS a Zero Trust Policy? [Anónimo]. Check Point [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.checkpoint.com/es/cyber-hub/network-security/what-is-zero-trust/what-is-a-zero-trust-policy/.

WHAT IS Zero Trust Architecture? | SANS Institute [Anónimo]. Cyber Security Training | SANS Courses, Certifications & Research [página web]. Disponible en Internet: https://www.sans.org/blog/what-is-zero-trust-architecture/.

WHAT IS BeyondCorp? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.paloaltonetworks.com/cyberpedia/what-is-beyondcorp.

WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your career [página web]. (12 de abril de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview.

WHAT IS Zero Trust Security? Principles of the Zero Trust Model [Anónimo]. crowdstrike.com [página web]. (17 de abril de 2023). [Consultado el 23 de

septiembre de 2024]. Disponible en Internet: https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/.

WHAT IS Zero Trust? [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (14 de abril de 2023). [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview#guiding-principles-of-zero-trust.

WHAT IS a Next-Generation Firewall? [Anónimo]. Líder en ciberseguridad y confianza cero | Zscaler [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.zscaler.es/resources/security-terms-glossary/what-is-next-generation-firewall.

WHAT IS Georeferencing? [Anónimo]. LocationIQ - API de geocodificación inversa gratuita, API de geocodificación, API de autocompletado [página web]. [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://es.locationiq.com/glossary/georeferencing.

ZERO TRUST Network Access (ZTNA) para controlar el acceso a las aplicaciones | Fortinet [Anónimo]. Fortinet [página web]. [Consultado el 23 de septiembre de 2024]. Disponible en Internet: https://www.fortinet.com/lat/solutions/enterprise-midsize-business/network-access/application-access.

ZERO TRUST adoption framework overview [Anónimo]. Microsoft Learn: Build skills that open doors in your carrera [página web]. (12 de abril de 2024). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview.

ZERO TRUST Blog Series - Blog 1: Adopting a Zero Trust Mindset | SANS Institute [Anónimo]. Cyber Security Training | SANS Courses, Certifications & Research [página web]. (22 de agosto de 2022). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://www.sans.org/blog/zero-trust-blog-1-adopting-zero-trust-mindset/.

ZERO TRUST Architecture [Anónimo]. NIST [página web]. (Agosto de 2020). [Consultado el 26 de septiembre de 2024]. Disponible en Internet: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.

Resumen Analítico Especializado -RAE

Tema	ZERO TRUST
Título	ZERO TRUST - UNA SOLUCIÓN PARA LA CIBERSEGURIDAD EN EMPRESAS COLOMBIANAS
Autor(es)	BRAYAN ARLEY CRUZ SENDOYA
Fuentes Bibliográficas	ADOPTING A Zero Trust approach is a technology and business imperative [Anónimo]. Microsoft [página web]. (Marzo de 2022). [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/adopting-zero-trust-infographic-final-5-business-scenarios.pdf?culture=es-co&country=co. CLOUDFLARE | Seguridad Zero Trust. [Anónimo]. Cloudflare [página web]. [Consultado el 22 de septiembre de 2024]. Disponible en Internet: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-zero-trust/. DEFINICIÓN Y explicación de confianza cero [Anónimo]. Kaspersky [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://latam.kaspersky.com/resource-center/definitions/zero-trust?srsltid=AfmBOoqDvyd9sKoItJjV0GloP6uHOmg26olR_MxZLvFL3Ip0D7a0S8XW. IBM. ¿Qué es Zero Trust? | IBM. IBM - United States [página web]. [Consultado el 25 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/es-es/topics/zero-trust. MERRITT, Rick. ¿Qué Es Zero-Trust? - Blog oficial de NVIDIA Latino América. Blog oficial de NVIDIA Latino América [blog]. [Consultado el 28 de octubre de 2022]. Disponible en Internet: https://la.blogs.nvidia.com/blog/que-es-zero-trust/. ORDEN EJECUTIVA sobre servicios de seguridad de ciberseguridad | IBM® [Anónimo]. IBM - United States [página web]. [Consultado el 24 de septiembre de 2024]. Disponible en Internet: https://www.ibm.com/es-es/services/executive-order-cybersecurity. ¿QUÉ ES una arquitectura Zero Trust (confianza cero)? [Anónimo]. Palo Alto Networks [página web]. [Consultado el 23 de septiembre de 2024]. Disponible en Internet:

	https://www.paloaltonetworks.es/cyberpedia/what-is-a-zero-trust-architecture.
Año	2024
Resumen	En los últimos años, diversas empresas pequeñas y medianas han enfrentado dificultades por la falta de profesionales, concienciación e inversión en ciberseguridad, lo que ha frenado la adopción del modelo de confianza cero (Zero Trust) en Colombia. Esta situación no coincide con el aumento de los ciberataques. Para reducir los riesgos organizacionales, se ha impulsado el crecimiento del enfoque Zero Trust, que emplea controles y principios de seguridad avanzados para prevenir amenazas. Con la desaparición de la distinción entre trabajo fijo y remoto, especialmente tras el auge del teletrabajo durante la pandemia, cada vez más empleados trabajan de forma distribuida. El modelo Zero Trust se aplica en diversas áreas de la empresa, abarcando dispositivos, datos y validación exhaustiva de la actividad de los usuarios, utilizando la microsegmentación de software para permitir una rápida modificación de políticas de seguridad, cumpliendo así con los requisitos de las empresas colombianas en su evolución cibernética. Esta monografía realiza una revisión sistemática sobre los principios de Zero Trust, brindando recomendaciones para empresas colombianas interesadas en su implementación, con el fin de minimizar amenazas internas y externas, y mantener la integridad y confidencialidad de la información y los sistemas. Además, ofrece información práctica para fortalecer la seguridad cibernética en estas organizaciones.
Palabras Clave	Ciberseguridad, Confianza Cero, Zero Trust, Empresas Colombianas, Teletrabajo, Microsegmentación, Amenazas internas, Amenazas externas, Protección de la información, Evolución de la ciberseguridad.
Contenido	El trabajo ofrece una estructura detallada que aborda el concepto de seguridad Zero Trust en profundidad. Inicia con la definición y justificación del problema, seguida por los objetivos generales y específicos. El marco referencial abarca los aspectos teóricos, conceptuales, históricos, científicos, tecnológicos y legales del modelo Zero Trust, destacando su evolución desde sus orígenes hasta su adopción actual. También se detalla el diseño metodológico, incluyendo revisiones sistémicas y el enfoque GRC. Los capítulos siguientes profundizan en la definición y funcionamiento de Zero Trust, las herramientas empleadas y las metodologías asociadas a marcos como NIST, Microsoft, Google y Forrester.

	Finalmente, se incluye una guía práctica para la implementación de estrategias Zero Trust, con un enfoque en la evaluación, desarrollo e implementación, seguido de monitoreo y ajustes, concluyendo con recomendaciones.
Descripción del problema de Investigación	En Colombia, la ciberseguridad se ha convertido en un tema crítico debido a ciberataques que han afectado a servicios hospitalarios, públicos, grandes y pequeñas empresas. Ejemplos notables incluyen el robo de datos del Grupo Keralty en noviembre de 2022 por Ransomhouse y el ataque a IFX Networks en septiembre de 2023, que impactó a cerca de 760 entidades. Según el Centro Cibernético de la Policía Nacional, en 2022 se registraron alrededor de 65.000 denuncias de ciberataques, reflejando un aumento de problemas de seguridad tras la pandemia. El auge del trabajo remoto y la modalidad híbrida ha resaltado la importancia de la ciberseguridad, y el modelo Zero Trust se presenta como una solución eficaz para mitigar riesgos y proteger los activos cibernéticos. Este modelo, que garantiza decisiones de acceso basadas en identidad, dispositivos y contexto, ha ganado relevancia a nivel global, incluso siendo adoptado por el gobierno de Estados Unidos en 2021. Sin embargo, en Colombia, la falta de profesionales y de inversión en ciberseguridad ha dificultado la adopción de Zero Trust en las empresas. ¿Cómo se puede implementar el enfoque de seguridad Zero Trust en las organizaciones colombianas para mejorar su postura de seguridad ante las amenazas cibernéticas?
Objetivo General	Proponer una guía del enfoque de seguridad Zero Trust, por medio de una revisión sistemática de literatura, facilitando la comprensión, planificación e implementación de Zero Trust en las organizaciones colombianas.
Objetivos Específicos	• Realizar una revisión sistemática de la literatura sobre el enfoque Zero Trust, metodologías, herramientas de seguridad informática. • Determinar las metodologías de seguridad Zero Trust existentes, identificando su aplicabilidad y efectividad en el contexto de las organizaciones colombianas, con el objetivo de recomendar las más adecuadas para su implementación. • Desarrollar una guía de implementación basada en conjunto de enfoques para orientar la implementación

	efectiva del modelo Zero Trust en las organizaciones colombianas, debió a la necesidad de fortalecer la postura de ciberseguridad en un entorno cada vez más complejo y vulnerable.
Metodología	Revisión Sistémica
Conclusiones	El enfoque Zero Trust, basado en su flexibilidad y capacidad de adaptación a cualquier organización, es el paso que debe seguir cualquier entidad colombiana que quiera estar a la vanguardia y aprovechar los beneficios de no estar limitada a un único perímetro "seguro". Este enfoque permite a las organizaciones abrir sus horizontes tanto para sus colaboradores como para el personal externo, brindando acceso controlado y medido a los recursos corporativos, lo que fomenta el crecimiento a largo plazo. Zero Trust es una metodología cada vez más aceptada en las organizaciones colombianas, ya que permite que sus colaboradores puedan trabajar desde cualquier lugar accediendo de manera segura a los recursos corporativos. Dada la infraestructura limitada en muchas ciudades y municipios de Colombia, las organizaciones deben apoyarse en metodologías probadas internacionalmente que faciliten la adopción de Zero Trust. Es fundamental validar las metodologías existentes y adoptar aquellas que mejor se ajusten a las necesidades de cada organización, ya que algunas ofrecen una mayor facilidad de implementación según el tamaño y el sector de la entidad. Este trabajo propone una guía para implementar la metodología Zero Trust en organizaciones colombianas, basándose en metodologías internacionales que han sido utilizadas en diversos países, especialmente aquellos que, impulsados por la necesidad del trabajo híbrido, surgida durante la pandemia, se vieron en la obligación de replantear su enfoque de seguridad. La guía abarca desde la definición de objetivos de seguridad y la evaluación del entorno actual, hasta el desarrollo e implementación de una estrategia Zero Trust, acompañada de un monitoreo y ajustes constantes para asegurar que la metodología esté siempre alineada con las necesidades de seguridad de las organizaciones colombianas que deseen implementar dicha metodología.