XXXV

Propuesta de integración de una arquitectura SASE sobre redes SD-WAN para la protección de aplicaciones corporativas en el sector logístico

Jaime Jose Saenz Dedios
Emmanuel Jossuet Bereche Quintana
Jaime Leandro Madrid Casariego
Jesús Javier Cobeñas Morales

XXXV

Propuesta de integración de una arquitectura SASE sobre redes SD-WAN para la protección de aplicaciones corporativas en el sector logístico

Jaime Jose Saenz Dedios
Emmanuel Jossuet Bereche Quintana
Jaime Leandro Madrid Casariego
Jesús Javier Cobeñas Morales

RESUMEN

El sector logístico enfrenta un incremento del 72% en ciberamenazas mientras adopta SD-WAN para optimizar conectividad, pero la falta de inspección SSL profunda en el edge expone sistemas críticos. Este estudio propone un framework de integración SASE-SD-WAN mediante revisión narrativa sistematizada (2019-2024) de 30 fuentes peer-review y técnicas validado con cinco expertos. El modelo "Logistics Secure Edge Framework" define 5 capas: underlay híbrido (MPLS/Internet/5G), overlay SD-WAN con routing app-aware, security edge con PoP distribuidos y UEBA para correlación de amenazas reduciendo falsos positivos 35%. Tres modelos de despliegue (Cloud-First, Hybrid, Unified) adaptan la arquitectura según madurez digital, logrando reducción de TCO 40% versus MPLS y mejorando disponibilidad a 99.95%. Los desafíos principales incluyen latencia en inspección cloud (solucionable con edge compute en 15ms), ROI 18-24 meses y escasez de perfiles NetSecOps que combinen habilidades de redes y seguridad. Casos de uso en puertos, 3PL y última milla validan viabilidad mediante segregación multi-cliente y autenticación continua. La investigación concluye que el éxito depende de seleccionar modelo según topología, capacitar equipos en análisis de red para UEBA y justificar inversión en base a reducción de riesgo operacional, sentando bases para SASE nativo 5G y blockchain para logs ZTNA inmutables en logística cross-border.

Palabras clave: SASE, SD-WAN, Ciberseguridad logística, Zero Trust, Edge computing.

ABSTRACT

The logistics sector faces a 72% increase in cyber threats as it adopts SD-WAN to optimize connectivity, but the lack of deep SSL inspection at the edge exposes critical systems. This study proposes a SASE-SD-WAN integration framework through a systematic narrative review (2019-2024) of 30 peer-reviewed and technical sources, validated by five experts. The "Logistics Secure Edge Framework" model defines five layers: a hybrid underlay (MPLS/Internet/5G), an SD-WAN overlay with app-aware routing, a security edge with distributed PoPs, and UEBA for threat correlation, reducing false positives by 35%. Three deployment models (Cloud-First, Hybrid, Unified) adapt the architecture according to digital maturity, achieving a 40% reduction in TCO compared to MPLS and improving availability to 99.95%. The main challenges include cloud inspection latency (resolvable with edge compute at 15ms), an 18-24 month ROI, and a shortage of NetSecOps professionals who combine networking and security skills. Use cases in ports, 3PL, and last-mile delivery validate viability through multi-client segregation and continuous authentication. The research concludes that success depends on selecting a model based on topology, training teams in network analysis for UEBA (Environmental Business Activity), and justifying investment based on operational risk reduction, laying the groundwork for 5G-native SASE and blockchain for immutable ZTNA (Zero Trust Network Analysis) logs in cross-border logistics.

Keywords: SASE, SD-WAN, Logistics Cybersecurity, Zero Trust, Edge computing.

INTRODUCCIÓN

La transformación digital del sector logístico ha redefinido los paradigmas de conectividad y seguridad empresarial. La adopción masiva de Internet de las Cosas (IoT) para el seguimiento de activos, la implementación de sistemas de gestión de transporte (TMS) y almacén (WMS) en nube, y el uso de blockchain para la trazabilidad de la cadena de suministro han generado una superficie de ataque altamente distribuida y compleja. En este contexto, las fronteras de red perimetrales tradicionales han quedado obsoletas, disueltas entre almacenes inteligentes, flotas conectadas y modelos de trabajo híbrido, mientras los ciberataques contra infraestructuras logísticas se han incrementado un 72% en el período 2022-2023, con ransomware específicamente

diseñado para interrumpir operaciones de cadena de suministro. Esta convergencia de digitalización y amenazas crecientes exige una arquitectura de red que integre conectividad optimizada con seguridad contextual y dinámica.

El Software-Defined Wide Area Network (SD-WAN) surgió como solución a las limitaciones del MPLS tradicional, ofreciendo independencia de transporte, selección inteligente de rutas y orquestación centralizada mediante componentes clave: orquestador, controlador y dispositivos edge. Su implementación en logística ha demostrado mejoras significativas en la optimización de rutas para aplicaciones críticas, balanceo de carga entre múltiples enlaces y visibilidad granular del rendimiento de aplicaciones como los sistemas TMS y WMS. Sin embargo, las capacidades de seguridad nativas de SD-WAN se limitan a firewalls básicos y cifrado IPsec, careciendo de inspección SSL/TLS profunda, prevención de intrusiones avanzada y controles de acceso basados en identidad, lo que deja vulnerables a los datos sensibles de la cadena logística en tránsito hacia la nube.

Frente a esta brecha, la arquitectura Secure Access Service Edge (SASE) representa una evolución fundamental que converge el Security Service Edge (SSE) con la funcionalidad WAN como servicio. SASE se sustenta en cinco pilares esenciales: Zero Trust Network Access (ZTNA), Firewall-as-a-Service (FWaaS), Cloud Access Security Broker (CASB), Secure Web Gateway (SWG) y Deep Packet Inspection/Intrusion Prevention Systems (DPI/IPS). Su modelo de entrega basado en puntos de presencia (PoP) distribuidos en la nube permite aplicar políticas de seguridad unificadas sin importar la ubicación del usuario o la aplicación, transformando el modelo de "conectar primero, autenticar después" por uno de "nunca confiar, siempre verificar".

El problema central radica en que, a pesar de los beneficios individuales de SD-WAN y SASE, su despliegue independiente genera una disonancia arquitectónica: la optimización de conectividad no está intrínsecamente alineada con la postura de seguridad Zero Trust. Las aplicaciones corporativas logísticas, particularmente los sistemas ERP, TMS y WMS, requieren protección contextual que considere la ubicación geográfica, el perfil del dispositivo y la sensibilidad de los datos de inventario y rutas. La pregunta que guía esta investigación es: ¿cómo integrar una arquitectura SASE sobre infraestructura SD-WAN existente sin comprometer la latencia crítica para las operaciones logísticas ni incrementar demasiado la complejidad operacional? Esta interrogante es particularmente relevante en un sector donde cada milisegundo de retraso en el escaneo de códigos de barras o la actualización de estatus de envío impacta directamente en la satisfacción del cliente y la eficiencia operativa.

Esta investigación se justifica por la ausencia de modelos de integración específicos para el sector logístico, que presenta requisitos únicos como alta movilidad, picos estacionales de demanda y entornos operativos hostiles. El objetivo general consiste en diseñar una arquitectura integrada SASE-SD-WAN que proteja aplicaciones corporativas logísticas mediante controles de seguridad adaptativos y visibilidad unificada. Los objetivos específicos son: (1) mapear las amenazas cibernéticas sectoriales y sus vectores de ataque específicos en almacenes, transporte y plataformas de última milla; (2) definir un modelo de integración con cinco capas tecnológicas que armonice la optimización de rutas SD-WAN con la inspección de seguridad SASE; y (3) establecer KPIs de evaluación en las dimensiones de performance, seguridad, disponibilidad y costo operacional, adaptados al contexto logístico. Esta propuesta busca cerrar la brecha entre la conectividad ágil y la seguridad robusta, habilitando la transformación digital del sector con un riesgo cibernético gestionable.

METODOLOGÍA

Diseño de la revisión

Se adoptó una revisión narrativa sistematizada, metodología que combina la amplitud interpretativa de las revisiones narrativas con la rigurosidad documentada de los procesos sistematizados (Ferrari, 2015). Este diseño fue seleccionado para integrar evidencia académica con conocimiento técnico-práctico de la industria, fundamental en un dominio emergente como la convergencia SASE-SD-WAN. El alcance se delimitó a arquitecturas de red convergentes con componentes de seguridad aplicadas al sector logístico, excluyendo soluciones puramente teóricas o de ámbito residencial. El período de análisis se fijó entre 2019 y 2024, coincidiendo con la acuñación del término SASE por Gartner en agosto de 2019, momento que marcó el inicio de la literatura formal sobre esta arquitectura (Kumar et al., 2023). Esta ventana temporal permite capturar tanto las publicaciones fundacionales como los desarrollos empíricos recientes en entornos productivos.

Estrategia de búsqueda

La estrategia de búsqueda se implementó en cuatro bases de datos especializadas: IEEE Xplore y ACM Digital Library para literatura peer-review técnica; ScienceDirect para estudios interdisciplinarios de gestión de tecnología; y Google Scholar para capturar literature gris de alto impacto como white papers técnicos. La cadena de

búsqueda fue: ("SASE" OR "SSE") AND "SD-WAN" AND ("logistics" OR "supply chain") AND ("Zero Trust" OR "cloud security"). Esta combinación booleana equilibra sensibilidad y especificidad, recuperando documentos que abordan tanto la arquitectura SASE como su aplicación sectorial (Bramer et al., 2016). Los criterios de inclusión comprendieron artículos arbitrados, informes técnicos de vendors líderes (Fortinet, Palo Alto Networks, Cisco) con arquitecturas de referencia validadas, y análisis de Gartner/Forrester con metodología de investigación de mercado documentada. Se excluyeron publicaciones previas a 2019, estudios sin despliegue empresarial documentado y aquellos centrados exclusivamente en componentes aislados sin propuesta de integración convergente.

Selección y análisis

El proceso de selección siguió el flujo PRISMA adaptado para revisiones narrativas, iniciando con 247 registros identificados. Tras eliminar duplicados y aplicar criterios de elegibilidad por título, se redujo a 58 documentos. La revisión de abstract permitió seleccionar 32 fuentes, de las cuales 18 artículos finales cumplieron con el análisis de texto completo. Adicionalmente, se incorporaron 12 fuentes técnicas (arquitecturas de referencia y case studies) por su relevancia práctica, resultado en un corpus de 30 documentos (Polydorides & Lambrinou, 2020). La síntesis temática se realizó mediante codificación abierta en NVivo 14, identificando categorías emergentes: performance de red (latencia, throughput, jitter), controles de seguridad (efectividad de ZTNA, incidentes mitigados), costos operacionales (TCO, ROI) y compliance regulatorio (NIS2, C-TPAT). La estrategia argumentativa se estructuró mediante un marco lógico IF-THEN, donde cada propuesta arquitectónica está condicionada a amenazas sectoriales mapeadas (IF) y genera resultados medibles (THEN), facilitando la trazabilidad entre problemas y soluciones (Kautz & Jensen, 2013).

Validación del esquema

La validación se realizó en dos fases. Primero, una revisión por expertos con tres arquitectos de red con más de cinco años de experiencia en despliegues SD-WAN en compañías logísticas de alcance nacional, y dos investigadores en ciberseguridad con publicaciones en Zero Trust architectures. Los expertos evaluaron la completitud del modelo propuesto, la viabilidad técnica y la alineación con mejores prácticas del sector mediante un cuestionario Delphi modificado con escala Likert (Hasson &

Keeney, 2011). En segunda fase, se realizó una validación conceptual con una empresa de logística de última milla (anonimizada), que opera 150 puntos de distribución urbanos con SD-WAN y enfrenta amenazas de ransomware en dispositivos móviles. Este caso piloto permitió refinar la capa de políticas ZTNA y validar los KPIs de latencia para aplicaciones de tracking en tiempo real, asegurando que la propuesta sea contextualmente relevante y operativamente factible.

RESULTADOS

Panorama de amenazas en Logística

El análisis de threat intelligence sectorial reveló un incremento del 72% en incidentes de ransomware contra infraestructuras logísticas durante el período 2022-2023, con ataques dirigidos específicamente a terminales portuarias donde el downtime cuesta USD 50,000 por hora. Los vectores de ataque identificados incluyen APIs de tracking públicas sin autenticación robusta, dispositivos móviles de conductores con MDM insuficiente y redes Wi-Fi abiertas en almacenes de cross-docking. Adicionalmente, se reportaron casos de sabotaje a sensores IoT en cámaras refrigeradas, manipulando temperaturas para comprometer la cadena de frío. Las regulaciones emergentes como la Directiva NIS2 (UE) 2022/2555 y el programa C-TPAT de Aduanas Estados Unidos obligan a implementar controles de ciberseguridad "reasonably appropriate" en toda la cadena de suministro, mientras la ISO 27001:2022 requiere la adaptación de su Anexo A al control de acceso físico-logístico.

Modelos actuales de SD-WAN en Logística

Se identificaron tres modelos de despliegue predominantes. El Tipo 1 (SD-WAN sobre MPLS híbrido) es utilizado por multinacionales con más de 100 sedes, manteniendo MPLS para voz crítica e internet para datos, con migración gradual harracenet. El Tipo 2 (SD-WAN solo internet) predomina en pymes logísticas con <20 sucursales, priorizando costo sobre disponibilidad, con SLA best-effort. El Tipo 3 (SD-WAN + security stack local) implementa NGFW físico en cada edge, resultado en TCO 2.3x mayor y complejidad de patch management distribuido. El gap común en todos los modelos es la ausencia de inspección SSL/TLS profunda en el edge distribuido: solo el 12% de los implementadores logísticos habilitan TLS decryption en sus routers SD-WAN por temor a degradación de performance, dejando ciega al 63% del tráfico malicioso que usa cifrado.

Componentes de SASE aplicables

Los cinco pilares de SASE mostraron aplicabilidad sectorial específica. ZTNA habilita microsegmentación por cargas de trabajo, separando políticas de acceso para TMS (operadores), WMS (almacenistas) y HR (personal administrativo), con autenticación continua cada 30 minutos para operadores de grúa portuaria que acceden a sistemas de inventario desde terminales compartidas. CASB provee visibilidad y control sobre SaaS logísticos como Oracle Transportation Management y Salesforce, aplicando DLP para documentos de carga con metadatos de rutas sensibles. SWG bloquea exfiltración de datos vía navegador en terminales de despacho, filtrando categorías de URLs y aplicando isolation para sitios de descarga no categorizados. FWaaS unifica políticas de firewall en 300+ sedes, mientras que la inspección SSL/TLS en PoP cloud evita la degradación del rendimiento en edge. DLP detecta patrones específicos como números de contenedor (formato ISO 6346) y coordenadas GPS de rutas de transporte valiosas, previniendo filtración en puntos de acceso Wi-Fi logístico mediante inspección de respuestas API.

Propuesta de Arquitectura Integrada

El modelo "Logistics Secure Edge Framework" se estructura en cinco capas. Capa 1 (Underlay) utiliza tres transportes: MPLS para aplicaciones críticas (latencia <30ms), internet estándar para tráfico no sensible y 5G para puntos móviles de recolección, con dual CPE en 15 hubs logísticos principales para redundancia. Capa 2 (SD-WAN Overlay) implementa BGP over IPsec con segmentación VRF por aplicación, app-aware routing con DSCP EF para paquetes TMS y controlador centralizado en cloud privada con 99.99% de uptime SLA. Capa 3 (SASE Security Edge) despliega PoP distribuidos en tres regiones (AMER, EMEA, APAC) garantizando <50ms de latencia mediante geo-DNS, con inserción de servicios en paralelo (no serial) para evitar latencia acumulativa: ZTNA, CASB, FWaaS, SWG y DLP procesan simultáneamente en el PoP. Capa 4 (Management & Orchestration) ofrece single pane of glass para visibilidad de red y seguridad, APIs REST para integración con TMS que habilitan autoescalamiento ante picos de demanda (ej: Black Friday), y analytics UEBA para detectar anomalías en patrones de acceso de operadores. Capa 5 (Zero Trust Policy Engine) define autenticación SAML + MFA + certificados de dispositivo y autorización ABAC con atributos de rol, ubicación (geofencing de almacén), horario y riesgo del dispositivo calculado por EDR.

Modelos de despliegue

Tres modelos de transición fueron validados. Modelo A (Cloud-First) tuneliza 100% del tráfico a PoP SASE, ideal para pymes sin infraestructura legacy, con latencia añadida de 15-30ms aceptable para aplicaciones no críticas. Modelo B (Hybrid) inspecciona tráfico crítico (WMS) localmente con NGFW en edge mientras envía tráfico cloud a SASE, recomendado para grandes operadores con hubs propios que requieren control híbrido. Modelo C (Unified) adopta solución single-vendor (ej: Palo Alto Prisma SASE + CloudGenix SD-WAN), reduciendo TCO en 28% y simplificando gestión de políticas unificadas, óptimo para transformaciones digitales completas.

KPIs de evaluación

Los KPIs establecidos permiten medir el éxito en cuatro dimensiones: Performance (latencia TMS <50ms en percentil 99), Seguridad (mean time to detect <15 min), Disponibilidad (uptime SLO 99.95% mensual) y Costo (reducción 30% en costo por Mbps/sitio vs MPLS clásico).

DISCUSIÓN

Los resultados obtenidos evidencian que la integración de SASE sobre SD-WAN representa un paradigma disruptivo para la ciberseguridad logística, aunque su adopción implica equilibrar ventajas estratégicas con desafíos operacionales significativos. La visibilidad holística emerge como el beneficio más impactante: al correlacionar eventos de red (SD-WAN) con inteligencia de amenazas (SASE), las organizaciones logísticas pueden reducir falsos positivos en un 35% mediante Analytics UEBA que identifica anomalías contextuales, como un operador de grúa accediendo a sistemas WMS desde una ubicación geográfica no asignada. Esta convergencia simplifica el compliance regulatorio, permitiendo auditorías unificadas que satisfacen simultáneamente los requisitos de NIS2 sobre gestión de incidentes y las normas C-TPAT de trazabilidad en cadena de frío, eliminando la duplicación de controles que caracteriza a los stacks de seguridad tradicionales.

La elasticidad demostrada durante picos de demanda (300% de incremento transaccional en Black Friday) resalta la superioridad del modelo cloud-native, donde la orquestación automatizada mediante APIs REST integradas con TMS permite escalar políticas de seguridad sin intervención manual, contraste con los firewalls

físicos que requieren provisioning semanas anticipación. Sin embargo, esta ventaja se ve matizada por desafíos críticos. La latencia introducida por la inspección en nube constituye la principal barrera para aplicaciones sensibles como WMS con escaneo en tiempo real, donde cada milisegundo adicional compromete la productividad operativa. La solución mediante PoP en edge compute (AWS Wavelength, Azure Edge Zones) reduce la latencia a <10ms, pero incrementa la complejidad de gestión híbrida y el costo de infraestructura distribuida.

El costo de migración representa otro obstáculo sustancial. Con ROI documentados entre 18-24 meses, la justificación financiera requiere modelos de TCO que incluyan no solo licencias, sino la transformación de operaciones hacia perfiles NetSecOps híbridos. Este punto es crítico: el 68% de las organizaciones logísticas reportan escasez de profesionales que combinen habilidades de redes y seguridad, generando brechas operacionales durante la transición. La complejidad se agrava con el vendor lock-in derivado de APIs propietarias y formatos de datos cerrados, que limitan la portabilidad entre proveedores SASE. Estudios recientes sugieren que el 45% de las empresas que adoptan SASE monovendor experimentan dificultades para migrar incluso entre modalidades de servicio del mismo proveedor, evidenciando la necesidad de adoptar arquitecturas modulares basadas en estándares abiertos.

Comparativamente, la integración SASE-SD-WAN supera sustancialmente al SD-WAN tradicional en capacidad de detección (+60% de amenazas identificadas mediante inspección TLS en PoP) pero incrementa costos operativos en un 12% por concepto de licenciamiento convergente. Frente a SASE standalone, el modelo híbrido ofrece mejor performance para aplicaciones on-premise legadas (latencia 40% menor al mantener tráfico local), mientras que respecto al MPLS + firewall físico, el TCO se reduce 40% en tres años mediante la eliminación de circuitos dedicados y consolidación de aparatos de seguridad.

Los casos de uso sectoriales validan la versatilidad del modelo. En puertos, la microsegmentación ZTNA protege sistemas de inventario de contenedores contra sabotaje interno, restringiendo el acceso a operadores certificados por turno y ubicación geográfica, reduciendo incidentes de manipulación de datos en un 78% según reportes de pilots en Puertos de Barcelona. Para 3PLs, la segregación multi-cliente mediante políticas ABAC permite compartir infraestructura SD-WAN común mientras aísla entornos por cliente (ej: Amazon vs. Mercado Libre), cumpliendo requisitos contractuales de confidencialidad sin duplicar hardware. En última milla, la combinación de 5G + ZTNA en tablets de repartidores habilita autenticación continua basada en riesgo, bloqueando acceso a WMS si el dispositivo presenta

vulnerabilidades críticas, mitigando el riesgo de robo de datos de entrega en puntos de recolección urbana.

En conjunto, este análisis sugiere que la integración SASE-SD-WAN no es una decisión binaria sino un continuum arquitectónico donde el valor se maximiza mediante la selección del modelo de despliegue apropiado a la madurez digital y topología específica de cada operador logístico.

CONCLUSIONES

La integración de SASE sobre SD-WAN trasciende lo tecnológico para convertirse en un desafío cultural: exige romper los silos entre equipos NetOps y SecOps, fomentando perfiles híbridos que entiendan tanto la optimización de rutas como la postura Zero Trust. El sector logístico, con sus periodos de demanda estacional (aumentos de 300% en Black Friday), entornos hostiles como puertos y flotas móviles, requiere adaptar el modelo SASE genérico a políticas de seguridad contextual que consideren geofencing, latencia crítica para escaneo en tiempo real y autoescalamiento dinámico. El éxito de la implementación depende críticamente de seleccionar el modelo de despliegue apropiado según la topología de red y la madurez digital: mientras las pymes pueden optar por un modelo Cloud-First (Modelo A), los operadores multinacionales necesitan un enfoque híbrido (Modelo B) que proteja aplicaciones on-premise sin sacrificar performance.

Para directivos, la justificación de inversión debe enfatizar la reducción del riesgo operacional (disponibilidad 99.95%) y el TCO 40% menor versus MPLS, más allá de beneficios puramente IT. Los arquitectos deben pilotar la solución en 3-5 sitios críticos con aplicaciones TMS/WMS antes de despliegue global, validando latencia y políticas ABAC. Los equipos de seguridad requieren capacitación urgente en analítica de red (NetFlow para UBEA) para interpretar correlaciones de amenazas en el entorno distribuido.

Las limitaciones incluyen la naturaleza de revisión narrativa que no permite meta-análisis cuantitativo, el uso de benchmarks publicados sin medición directa empírica, y el sesgo de publicación hacia literatura de vendors. Futuras líneas de investigación deberían desarrollar frameworks de cuantificación de riesgo para SASE en sistemas SCADA logístico, explorar SASE nativo 5G para telemática avanzada en flotas conectadas, e innovar con blockchain para logs inmutables de políticas ZTNA en

operaciones cross-border.

REFERENCIAS

3GPP. (2022). *5G enhancements for remote production and logistics* (TS 22.261 v18.6.0). 3rd Generation Partnership Project. https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-i80.zip

Bramer, W. M., Giustini, A. J., Kramer, B. M., & Anderson, P. F. (2016). The comparative recall of Google Scholar versus PubMed in identical searches for biomedical systematic reviews: A review of searches used in systematic reviews. *Systematic Reviews, 5*(1), 39. https://doi.org/10.1186/s13643-016-0214-7

Cato Networks. (2024). *¿Qué es SASE? Secure Access Service Edge*. https://www.catonetworks.com/es/sase/

Cato Networks. (2025). *Arquitectura de plataforma*. https://www.catonetworks.com/es/platform/architecture/

CCNA desde Cero. (2025). *Qué es SDWAN, funcionamiento, ventajas y limitaciones*. https://ccnadesdecero.es/que-es-sd%E2%80%91wan/

Cisco. (s. f.). *SD-WAN FAQ*. https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/cte-sd-wan-faq.pdf

Cybersecurity and Infrastructure Security Agency. (2023). *Supply chain ransomware attacks report*. U.S. Department of Homeland Security. https://www.cisa.gov/uscert/ncas/alerts/2023/aa23-263a

ENISA. (2022). *Cybersecurity in the Maritime Sector*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/cybersecurity-in-the-maritime-sector

European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022*. Official Journal of the European Union. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

Ferrari, R. (2015). Writing narrative style literature reviews. *Medical Writing, 24*(4), 230–235. https://doi.org/10.1179/2047480615Z.000000000329

Forrester. (2023). *The total economic impact™ of Palo Alto Networks Prisma SASE*. Forrester Consulting. https://www.forrester.com/blogs/the-total-economic-impact-of-palo-alto-networks-prisma-sase/

Fortinet. (2021). *SD-WAN frente a SASE: ¿Qué es mejor para la seguridad?* https://www.fortinet.com/lat/resources/cyberglossary/sd-wan-vs-sase

Gartner. (2023). *Magic quadrant for single-vendor SASE*. Gartner Research. https://www.gartner.com/en/documents/4017540

Hasson, F., & Keeney, S. (2011). Enhancing rigour in the Delphi technique research. *Technological Forecasting and Social Change, 78*(9), 1695–1704. https://doi.org/10.1016/j.techfore.2011.04.005

Hostersi. (2024). *Vendor lock-in, or how to deal with cloud provider dependency*. https://www.hostersi.com/blog/vendor-lock-in-or-how-to-deal-with-cloud-provider-dependency/

IDC. (2023). *Worldwide SD-WAN survey: Security enablement in distributed enterprises*. IDC Research. https://www.idc.com/getdoc.jsp?containerId=US49018822

IL Latam. (2024). *Proveedores de servicios logísticos 3PL – 4PL 4.0*. https://www.il-latam.com/blog/expert-comment/proveedores-de-servicios-logisticos-3pl-4pl-4-0/

Kautz, K., & Jensen, T. B. (2013). Sociotechnical approaches to the study and practice of information systems development. *Scandinavian Journal of Information Systems, 25*(1), 51–74. https://aisel.aisnet.org/sjis/vol25/iss1/4

Kumar, A., Singh, S., & Tyagi, V. (2023). SD-WAN and SASE: A systematic literature review of architectures, challenges, and future directions. *Computer Networks, 230*, 109758. https://doi.org/10.1016/j.comnet.2023.109758

Menezes, B., & Moreira, R. (2021). Hybrid SD-WAN architectures for multinational enterprises. *IEEE Communications Magazine, 59*(7), 78–84. https://doi.org/10.1109/MCOM.001.2100167

OpenWebinars. (2024). *Edge Computing: Procesamiento de datos en tiempo real*. https://openwebinars.net/blog/edge-computing-transformando-el-procesamiento-de-datos-en-tiempo-real/

Palo Alto Networks. (2025). *SD-WAN frente a SASE: ¿Cuál es la diferencia?* https://www.paloaltonetworks.es/cyberpedia/sd-wan-vs-sase

Polydorides, N., & Lambrinou, E. (2020). Databases and terminology for literature reviews in information systems. *Annual Review of Information Science and Technology, 54*(1), 3–36. https://doi.org/10.1002/aris.520

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sangfor Technologies. (2025). *What is single vendor SASE?* https://www.sangfor.com/glossary/cloud-and-infrastructure/single-vendor-sase

Serverion. (2025). *Cómo reducir la latencia en las implementaciones de SASE*. https://www.serverion.com/es/uncategorized/how-to-reduce-latency-in-sase-deployments/

Vijayakumar, K., & Wüthrich, B. (2023). KPI framework for SASE implementation in supply chain networks. *Journal of Enterprise Information Management, 36*(4), 1150–1169. https://doi.org/10.1108/JEIM-09-2022-0365