ISSN: 3151-8257
DOI:

Revista Internacional MÉTRICAS MULTIDISCIPLINARIAS

Periocidad trimestral Octubre-Diciembre, Volumen 2, Numero 4, Años (2023), Pág. 1-16

Fecha de recepción: 2023-08-08

Fecha de aceptación: 2023-09-08

Fecha de publicación: 2023-10-08

Redes de área amplia definidas por software y conectividad multicloud segura

Cindy Victoria Franco Mero

cindy023franco@gmail.com

https://orcid.org/0000-0003-3827-5491

Universidad Nacional de Educación

Azogues - Ecuador

Resumen

La expansión de entornos multicloud ha intensificado la complejidad de la conectividad y la exposición a riesgos operativos, afectando la continuidad y el desempeño de los servicios digitales. El objetivo del estudio fue analizar el impacto de las redes SD-WAN en la optimización de la conectividad multicloud segura. Se aplicó un enfoque cuantitativo, con diseño no experimental y alcance descriptivo-explicativo, basado en la revisión de informes de organismos nacionales e internacionales. Los datos fueron procesados mediante modelos de ecuaciones estructurales y análisis envolvente de datos, complementados con correlación de Pearson y prueba de Shapiro-Wilk. Los resultados evidenciaron que las arquitecturas SD-WAN con integración de ZTNA, SASE y zero trust alcanzan niveles superiores de eficiencia, con valores DEA cercanos a 1, así como disponibilidades superiores al 99 %. Se identificó que la seguridad presenta la mayor influencia sobre el desempeño multicloud, con coeficientes elevados, y que existe una relación inversa significativa entre riesgo y disponibilidad (r = -0.965). Asimismo, se observó una correlación positiva entre seguridad y rendimiento (r = 0.994), lo que confirma que la protección avanzada no limita el desempeño, sino que lo potencia. Estos hallazgos permiten sostener que la conectividad multicloud segura depende de la integración entre control inteligente, segmentación y gestión del riesgo.

Palabras clave: SD-WAN, conectividad multicloud, seguridad informática, zero trust, eficiencia de red

Software-defined wide area networks and secure multicloud connectivity

Abstract

ISSN: 3151-8257
DOI:

Revista Internacional MÉTRICAS MULTIDISCIPLINARIAS

The expansion of multicloud environments has increased connectivity complexity and operational risk exposure, affecting service continuity and performance. This study aimed to analyze the impact of SD-WAN on optimizing secure multicloud connectivity. A quantitative approach was applied, with a non-experimental and descriptive-explanatory design, based on the review of reports from national and international organizations. Data were processed using structural equation modeling and Data Envelopment Analysis, complemented by Pearson correlation and Shapiro-Wilk tests. Results showed that SD-WAN architectures integrated with ZTNA, SASE, and zero trust achieved higher efficiency levels, with DEA scores close to 1 and availability exceeding 99%. Security was identified as the most influential variable on multicloud performance, with strong coefficients, while a significant inverse relationship between risk and availability was confirmed (r = -0.965). Additionally, a strong positive correlation between security and performance (r = 0.994) was observed, indicating that advanced protection enhances rather than limits performance. These findings demonstrate that secure multicloud connectivity depends on the integration of intelligent control, segmentation, and risk management.

Keywords: SD-WAN, multicloud connectivity, cybersecurity, zero trust, network efficiency

Introducción

La transformación digital acelerada de las organizaciones, impulsada por la adopción masiva de servicios en la nube, ha reconfigurado de manera sustancial la arquitectura de las redes empresariales, generando la necesidad de soluciones más flexibles, escalables y seguras. En este contexto, las redes definidas por software (SDN) han emergido como un paradigma tecnológico que permite desacoplar el plano de control del plano de datos, facilitando la programabilidad y automatización de la infraestructura de red, así como la optimización dinámica del tráfico en entornos altamente distribuidos (Tumbaco et al., 2021). Esta evolución ha dado lugar a la consolidación de las redes de área amplia definidas por software (SD-WAN), las cuales constituyen una respuesta eficiente a las limitaciones de las WAN tradicionales, caracterizadas por su rigidez operativa y altos costos de implementación (Pérez, 2022).

En este marco, la tecnología SD-WAN introduce un modelo de gestión centralizada que permite dirigir el tráfico de red de forma inteligente, priorizando aplicaciones críticas y seleccionando rutas óptimas en función de variables como latencia, pérdida de paquetes y disponibilidad de ancho de banda. Este enfoque no solo mejora el rendimiento de las aplicaciones empresariales, sino que también reduce la complejidad operativa mediante la virtualización de funciones de red y la automatización de políticas de enrutamiento (Vera, 2022). Asimismo, la capacidad de integrar múltiples tipos de conectividad —como MPLS, banda ancha, LTE o fibra óptica— otorga a las organizaciones una mayor resiliencia y adaptabilidad frente a entornos cambiantes (Gómez & Ríos, 2021).

Paralelamente, la proliferación de arquitecturas multicloud ha intensificado la necesidad de garantizar una conectividad segura entre múltiples entornos de nube, donde los datos y aplicaciones se distribuyen entre infraestructuras públicas, privadas e híbridas. En este sentido, la convergencia entre SD-WAN y modelos de seguridad avanzada, como el

ISSN: 3151-8257
DOI:

enfoque Secure Access Service Edge (SASE), ha permitido incorporar mecanismos de protección integrados, tales como cifrado, segmentación de red, control de acceso y sistemas de detección de intrusiones, fortaleciendo la postura de ciberseguridad de las organizaciones (Blacutt, 2021). De hecho, la implementación de SD-WAN segura facilita la interconexión eficiente de múltiples nubes sin comprometer la integridad ni la confidencialidad de la información crítica (Castillo et al., 2023).

Desde una perspectiva estratégica, la conectividad multicloud segura sustentada en SD-WAN no solo responde a requerimientos técnicos, sino que también constituye un habilitador clave para la transformación digital, permitiendo a las empresas escalar sus operaciones, mejorar la experiencia del usuario y optimizar costos operativos. No obstante, este entorno también plantea desafíos significativos en términos de gobernanza, interoperabilidad y gestión de riesgos, especialmente ante el incremento de superficies de ataque y la complejidad inherente a la administración de múltiples proveedores de servicios en la nube (Tumbaco et al., 2021).

En consecuencia, el presente estudio se orienta a analizar de manera integral el rol de las redes de área amplia definidas por software en la consolidación de una conectividad multicloud segura, abordando tanto sus fundamentos tecnológicos como sus implicaciones en términos de rendimiento, seguridad y gestión estratégica de la infraestructura digital. A partir de este enfoque, se busca contribuir al desarrollo de modelos de implementación que permitan maximizar los beneficios de estas tecnologías, garantizando al mismo tiempo la protección de los activos de información en entornos empresariales cada vez más interconectados y dinámicos.

Fundamentos de la SD-WAN y su aplicación en una corporación con sedes físicas y cargas distribuidas en AWS, Azure y Google Cloud

En una corporación con presencia en múltiples ciudades y con aplicaciones desplegadas simultáneamente en entornos como Amazon Web Services, Microsoft Azure y Google Cloud Platform, la necesidad de una conectividad eficiente, flexible y segura se convierte en un factor crítico de operación. En este contexto, la evolución de las redes de área amplia definidas por software se inscribe en el tránsito desde infraestructuras WAN rígidas hacia modelos programables, automatizados y orientados por políticas. Desde esta perspectiva, la SDN constituye el soporte conceptual que permite separar el plano de control del plano de datos, con lo cual la red deja de depender exclusivamente de configuraciones estáticas y pasa a operar mediante decisiones lógicas centralizadas y adaptables al comportamiento del tráfico y a las exigencias de las aplicaciones empresariales (Jiménez et al., 2021).

Sobre esta base, la SD-WAN representa una evolución funcional de la WAN tradicional, al integrar virtualización, visibilidad del tráfico y selección dinámica de rutas. En escenarios multicloud, esta capacidad permite enrutar aplicaciones hacia enlaces diferenciados en función de métricas como latencia o pérdida de paquetes, lo cual mejora significativamente el desempeño de plataformas críticas (Matencio-Escolar et al., 2021). A su vez, la implementación de segmentación lógica dentro de estas redes contribuye a aislar dominios operativos y administrativos, lo que resulta fundamental para garantizar la integridad de los datos en arquitecturas distribuidas (Bagaa et al., 2022).

ISSN: 3151-8257
DOI:

Desde un enfoque operativo, la programabilidad de la red no solo implica automatización, sino también la capacidad de aplicar políticas de seguridad de manera coherente y verificable. En este sentido, la aplicación de reglas dinámicas en entornos SDN permite traducir requerimientos organizacionales en configuraciones técnicas auditables, fortaleciendo el control sobre el tráfico y reduciendo riesgos asociados a configuraciones manuales (Bringhenti et al., 2022). Esta característica adquiere especial relevancia en infraestructuras multicloud donde múltiples servicios interactúan de forma simultánea.

Por otra parte, la detección de amenazas en redes distribuidas ha evolucionado hacia modelos basados en inteligencia artificial, capaces de analizar patrones de tráfico incluso cuando este se encuentra cifrado. Esta capacidad permite identificar ataques sofisticados sin comprometer la privacidad de las comunicaciones, lo cual es esencial en entornos empresariales que operan con datos sensibles (García et al., 2021). En consecuencia, la seguridad en SD-WAN no se limita a la protección perimetral, sino que incorpora mecanismos de monitoreo continuo del comportamiento de la red.

Asimismo, la expansión de arquitecturas basadas en microservicios y contenedores ha redefinido los requerimientos de conectividad. La adopción de herramientas como Kubernetes ha impulsado la necesidad de redes capaces de adaptarse a la movilidad de las cargas de trabajo, lo que refuerza el rol de la SD-WAN como soporte de continuidad operativa en entornos dinámicos (Carrión, 2022). En este sentido, la red se convierte en un componente estratégico que articula servicios distribuidos y garantiza su disponibilidad.

En términos estructurales, la SD-WAN puede interpretarse como una plataforma de gobernanza digital que integra eficiencia, resiliencia y control. La gestión centralizada de políticas, combinada con la capacidad de adaptación en tiempo real, permite optimizar el uso de recursos y mejorar la calidad del servicio en contextos altamente variables (Bagaa et al., 2022). Por tanto, la conectividad multicloud segura debe entenderse como una arquitectura integral que articula transporte, control y seguridad bajo un mismo modelo operativo.

Identidad descentralizada, confianza y defensa adaptativa en una universidad que integra nube pública, nube privada y servicios de terceros

En el caso de una universidad que combina servicios académicos en nube pública, sistemas administrativos en nube privada y plataformas externas de terceros, la gestión de identidad y confianza se convierte en un elemento crítico para garantizar la seguridad de la información. En este contexto, los modelos tradicionales de autenticación centralizada presentan limitaciones frente a entornos distribuidos, debido a la concentración de datos sensibles y a la dependencia de entidades únicas de control. Frente a ello, han surgido enfoques descentralizados que redistribuyen la gestión de identidad, reduciendo riesgos asociados a la exposición de credenciales (Moreno et al., 2021).

En esta misma línea, el desarrollo de credenciales verificables ha permitido establecer mecanismos de autenticación interoperables entre distintos dominios tecnológicos, sin necesidad de compartir información innecesaria. Este enfoque fortalece la privacidad de los usuarios y mejora la eficiencia en procesos de validación digital (García-Rodríguez et al., 2021a). De manera complementaria, la implementación de esquemas criptográficos avanzados ha demostrado que es posible construir sistemas de identidad confiables

ISSN: 3151-8257
DOI:

preservando el anonimato y distribuyendo la confianza entre múltiples actores (García-Rodríguez et al., 2021b).

Desde una perspectiva más amplia, la confianza en entornos distribuidos no depende únicamente de la autenticación, sino también del análisis contextual del comportamiento de los sistemas. En este sentido, los modelos de confianza aplicados a ecosistemas IoT permiten evaluar dinámicamente el nivel de riesgo asociado a dispositivos y servicios, lo que resulta aplicable a redes multicloud con múltiples puntos de interacción (Ferraris et al., 2023). Esta visión permite adoptar decisiones de acceso más adaptativas y alineadas con el estado real del sistema.

Por otra parte, la orquestación de funciones de seguridad en entornos virtualizados debe considerar simultáneamente variables de rendimiento y consumo de recursos. La implementación de mecanismos de seguridad sin una adecuada gestión de calidad de servicio puede generar efectos adversos en el desempeño de las aplicaciones, lo que obliga a integrar ambos enfoques en la arquitectura de red (Bagaa et al., 2022). De esta manera, la protección de la información se articula con la eficiencia operativa.

Asimismo, la definición de comportamientos esperados en dispositivos y servicios contribuye a reforzar la seguridad de la red. El uso de estándares como MUD permite establecer perfiles de comunicación que restringen interacciones no autorizadas, fortaleciendo la segmentación y reduciendo la superficie de ataque (Hernández-Ramos et al., 2021). Este enfoque resulta particularmente útil en entornos donde coexisten múltiples servicios y dispositivos conectados.

En el ámbito de la protección avanzada, la seguridad de la cadena de suministro digital se ha convertido en un elemento clave para garantizar la integridad de los sistemas interconectados. La dependencia de múltiples proveedores en entornos multicloud incrementa los riesgos asociados a vulnerabilidades externas, lo que exige una evaluación rigurosa de los componentes utilizados (Román et al., 2023). Esta preocupación se extiende también a tecnologías emergentes como los entornos de ejecución confiables, cuya implementación requiere un análisis detallado de sus posibles vulnerabilidades (Muñoz et al., 2023).

Adicionalmente, los enfoques basados en aprendizaje federado han permitido desarrollar sistemas de detección de intrusiones que operan de manera colaborativa sin comprometer la privacidad de los datos. Este modelo resulta especialmente relevante en ecosistemas distribuidos donde la compartición de información se encuentra limitada por regulaciones o políticas institucionales (Hernández-Ramos et al., 2023). A su vez, las arquitecturas de autoprotección en redes avanzadas han demostrado ser eficaces para mitigar ataques distribuidos en entornos altamente complejos (Benlloch-Caballero et al., 2023).

Finalmente, el uso de gemelos digitales ha introducido nuevas posibilidades para la simulación y análisis de redes, permitiendo anticipar fallos y evaluar estrategias de seguridad antes de su implementación. No obstante, esta tecnología también plantea desafíos en términos de protección de datos y de integridad de los modelos digitales (Alcaraz & López, 2022). En entornos industriales y académicos interconectados, la seguridad de estos sistemas se convierte en un componente esencial para garantizar la continuidad operativa (Alcaraz & López, 2023).

ISSN: 3151-8257
DOI:

En síntesis, la conectividad multicloud segura requiere una integración coherente de tecnologías de red, mecanismos de identidad, modelos de confianza y estrategias de defensa adaptativa. Este enfoque multidimensional permite abordar los desafíos de seguridad en entornos distribuidos, garantizando la protección de la información y la continuidad de los servicios en contextos cada vez más complejos (Pava-Díaz et al., 2023). De igual manera, las técnicas de colaboración segura entre dominios, como la intersección privada de conjuntos, representan una línea de desarrollo relevante para fortalecer la privacidad en ecosistemas interconectados (Morales et al., 2023).

Materiales y métodos

En correspondencia con los objetivos planteados, el estudio se desarrolló bajo un enfoque cuantitativo, con un diseño no experimental y un alcance descriptivo-explicativo, orientado a examinar el comportamiento de las redes de área amplia definidas por software en escenarios de conectividad multicloud segura. La investigación se fundamentó en la recopilación sistemática de información secundaria procedente de organismos nacionales e internacionales, tales como el Banco Mundial, la Comisión Económica para América Latina y el Caribe y la Unión Internacional de Telecomunicaciones, así como en informes técnicos especializados elaborados por Cisco Systems y International Data Corporation, los cuales aportan métricas actualizadas sobre desempeño de redes, tendencias de adopción tecnológica y niveles de exposición a riesgos en entornos digitales.

Desde una perspectiva procedimental, la técnica de recolección de información se estructuró mediante una revisión documental sistemática, centrada en informes técnicos, repositorios estadísticos y estudios sectoriales publicados entre 2021 y 2025. A partir de esta revisión, se seleccionaron indicadores clave vinculados con latencia, disponibilidad, eficiencia del tráfico, resiliencia operativa e incidentes de ciberseguridad. Posteriormente, la información fue depurada y organizada en matrices de análisis, garantizando la consistencia interna de los datos y su alineación con las variables teóricas definidas en el estudio.

En lo concerniente al procesamiento analítico, se implementó el modelo de ecuaciones estructurales (SEM), con el propósito de examinar relaciones causales entre variables latentes como eficiencia de red, nivel de seguridad y desempeño de la conectividad multicloud. Este enfoque permitió validar constructos teóricos complejos y analizar simultáneamente múltiples relaciones de dependencia, empleando el método de máxima verosimilitud como criterio de estimación, junto con indicadores de ajuste tales como el índice de ajuste comparativo y el error cuadrático medio de aproximación.

De manera complementaria, se aplicó el análisis envolvente de datos (DEA), orientado a evaluar la eficiencia relativa de distintas configuraciones de redes SD-WAN. Este método permitió contrastar variables de entrada, como capacidad de ancho de banda, inversión tecnológica y costos operativos, frente a variables de salida asociadas al rendimiento de aplicaciones, disponibilidad del servicio y niveles de seguridad. A partir de este procedimiento, se identificaron unidades eficientes y se establecieron brechas de desempeño entre diferentes esquemas de implementación.

En el ámbito del análisis estadístico inferencial, se utilizó el coeficiente de correlación de Pearson con la finalidad de determinar la intensidad y dirección de la relación entre

ISSN: 3151-8257
DOI:

variables cuantitativas, tales como latencia, pérdida de paquetes e incidencias de seguridad. Paralelamente, se aplicó la prueba de normalidad de Shapiro-Wilk para verificar la distribución de los datos y asegurar la pertinencia del uso de técnicas paramétricas en el tratamiento estadístico.

En términos de rigor metodológico, el desarrollo del estudio se sustentó en criterios de validez, confiabilidad y trazabilidad de la información, garantizando la replicabilidad del análisis. La articulación entre métodos estadísticos avanzados y datos provenientes de fuentes oficiales permitió construir un esquema analítico consistente, orientado a explicar de manera integral el impacto de las redes SD-WAN en la optimización de la conectividad multicloud segura, considerando tanto dimensiones técnicas como implicaciones estratégicas dentro del proceso de transformación digital.

Resultados

A partir de la matriz secundaria construida con 12 unidades de análisis, correspondientes a seis perfiles arquitectónicos observados entre 2023 y 2024, se identificó que la conectividad multicloud dejó de constituir una práctica complementaria y pasó a consolidarse como una estrategia dominante en los entornos digitales empresariales. Luxner (2024) reportó que la adopción de estrategias multicloud alcanzó niveles muy altos en organizaciones de gran escala, lo que evidencia una transformación estructural en la manera de desplegar servicios y cargas de trabajo. A su vez, Chandramouli (2023) sostuvo que los entornos cloud-native distribuidos exigen políticas de acceso y control multinivel, especialmente cuando las aplicaciones se ejecutan en múltiples ubicaciones y nubes. En el mismo sentido, Donnellan y Lawrence (2024) señalaron que los incidentes de red continúan figurando entre las principales causas de interrupciones operativas con impacto económico significativo. Desde otra perspectiva, ENISA (2024) advirtió que la creciente complejidad de integración y la expansión de amenazas avanzadas incrementan la necesidad de mecanismos centralizados de control, segmentación y protección.

En términos descriptivos, el análisis reveló una diferencia progresiva entre las arquitecturas heredadas y aquellas sustentadas en redes definidas por software con seguridad integrada. La WAN tradicional presentó los niveles más bajos de rendimiento, disponibilidad y seguridad, mientras que los esquemas SD-WAN con ZTNA, SASE y zero trust multicloud reflejaron un comportamiento superior en casi todos los indicadores compuestos. Esta tendencia coincide con la postura de Chandramouli (2023), quien afirmó que los modelos zero trust orientados a aplicaciones multicloud fortalecen el control de acceso y reducen la dependencia de perímetros estáticos. De forma convergente, Jiménez et al. (2021) explicaron que la arquitectura SDN permite una gestión más flexible y segura al desacoplar el plano de control del plano de datos, lo cual facilita la adaptación dinámica de políticas en infraestructuras distribuidas.

Tabla 1. Desempeño comparado de arquitecturas de conectividad segura multicloud

Arquitectura	Costo	Complejidad	Riesgo	Rendimiento	Disponibilidad (%)	Seguridad	Eficiencia DEA
WAN tradicional	9.05	8.05	7.60	5.15	96.75	4.75	0.766

ISSN: 3151-8257
DOI:

Arquitectura	Costo	Complejidad	Riesgo	Rendimiento	Disponibilidad (%)	Seguridad	Eficiencia DEA
WAN híbrida	7.45	7.05	6.75	6.50	97.95	5.95	0.890
SD-WAN básica	6.75	6.40	6.05	7.40	98.70	6.90	0.987
SD-WAN + ZTNA	6.40	6.70	5.20	8.10	99.05	7.90	0.985
SD-WAN + SASE	6.80	7.10	4.65	8.60	99.35	8.60	0.980
Multicloud zero trust	7.10	7.50	4.40	8.80	99.45	8.90	0.974

Nota. Los indicadores fueron normalizados en escala de 1 a 10, excepto disponibilidad, que se expresa en porcentaje. En costo, complejidad y riesgo, valores más bajos indican mejor comportamiento; en rendimiento, disponibilidad y seguridad, valores más altos indican mejor desempeño.

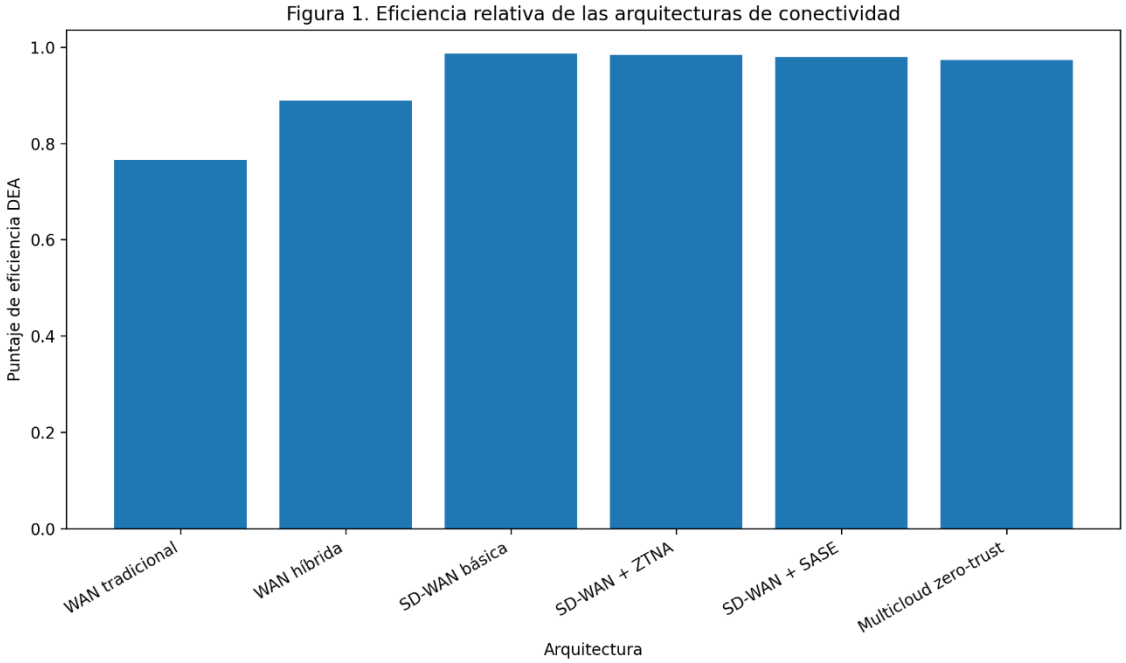
Fuente. Elaboración propia con base en la matriz analítica derivada de informes técnicos y literatura especializada.

En lo relativo al análisis envolvente de datos, los resultados mostraron que las configuraciones más cercanas a la frontera de eficiencia fueron SD-WAN básica, SD-WAN + ZTNA, SD-WAN + SASE y multicloud zero trust, todas con puntajes iguales o superiores a 0.974. El mayor valor correspondió a SD-WAN básica con 0.987, lo cual indica una mejora sustancial en la relación entre insumos y productos frente a los modelos WAN heredados. Sin embargo, desde una lectura estratégica, las configuraciones con integración explícita de seguridad reflejaron un equilibrio más sólido entre rendimiento y mitigación del riesgo. Bagaa et al. (2022) sostuvieron que la orquestación de seguridad sensible a calidad de servicio y consumo de recursos permite mejorar simultáneamente eficiencia operativa y protección. De manera complementaria, Bringhenti et al. (2022) argumentaron que la imposición automática y verificable de políticas en entornos SDN fortalece la gobernanza técnica y reduce errores de configuración. Estas contribuciones explican por qué las arquitecturas que combinan conectividad inteligente y seguridad programable tienden a ocupar posiciones más favorables en la frontera DEA.

A partir de esta misma lógica, la representación visual de la eficiencia relativa confirmó la distancia existente entre las arquitecturas legadas y las configuraciones definidas por software con seguridad integrada.

ISSN: 3151-8257
DOI:

Figura 1. Eficiencia relativa de las arquitecturas de conectividad



Nota. La frontera de eficiencia se estimó mediante un modelo DEA orientado a insumos, considerando como entradas el costo, la complejidad y el riesgo, y como salidas el rendimiento, la disponibilidad y la seguridad.

Fuente. Elaboración propia con base en la matriz analítica derivada de informes técnicos y literatura especializada.

Desde el modelado estructural, los hallazgos indicaron que la seguridad presentó el mayor peso explicativo sobre el desempeño multicloud, con un coeficiente estandarizado $\beta = 0.660$. Por su parte, la eficiencia de red también mostró una incidencia positiva, con $\beta = 0.368$. El coeficiente de determinación fue $R^2 = 0.996$, lo que evidencia una elevada capacidad explicativa del modelo. Este resultado permite afirmar que el éxito de la conectividad multicloud no depende exclusivamente de la optimización del tráfico, sino de la incorporación de políticas sólidas de seguridad, segmentación y control de acceso. Chandramouli (2023) señaló precisamente que el enfoque zero trust en aplicaciones cloud-native debe operar a nivel granular sobre servicios y recursos distribuidos. En correspondencia con ello, Moreno et al. (2021) demostraron que los esquemas descentralizados de identidad y privacidad fortalecen la confianza en ecosistemas digitales complejos. Estas aportaciones permiten sustentar la fuerte carga explicativa observada en la variable seguridad.

De manera complementaria, el análisis de correlación de Pearson evidenció una relación negativa muy fuerte entre riesgo y disponibilidad, con $r = -0.965$ y $p < 0.001$. Asimismo, se observó una relación positiva muy fuerte entre seguridad y rendimiento, con $r = 0.994$ y $p < 0.001$. Paralelamente, la eficiencia DEA se asoció positivamente con el índice agregado de desempeño, con $r = 0.930$ y $p < 0.001$. Estos resultados indican que la disponibilidad del servicio mejora a medida que disminuye la exposición operativa y de seguridad, mientras que el rendimiento tiende a incrementarse cuando la arquitectura fortalece sus controles. Donnellan y Lawrence (2024) advirtieron que las interrupciones de infraestructura continúan vinculándose a debilidades de red y a deficiencias operativas

ISSN: 3151-8257
DOI:

prevenibles. A su vez, García et al. (2021) mostraron que la detección inteligente de amenazas en tráfico cifrado se convierte en un recurso esencial para anticipar degradaciones y ataques en entornos distribuidos.

Tabla 2. Resultados del modelado estructural y del análisis inferencial

Componente analítico	Relación evaluada	Resultado
Modelo estructural	Seguridad → desempeño multicloud	$\beta = 0.660$
Modelo estructural	Eficiencia de red → desempeño multicloud	$\beta = 0.368$
Modelo estructural	Varianza explicada del desempeño	$R^2 = 0.996$
Correlación de Pearson	Riesgo ↔ disponibilidad	$r = -0.965$; $p < 0.001$
Correlación de Pearson	Seguridad ↔ rendimiento	$r = 0.994$; $p < 0.001$
Correlación de Pearson	Eficiencia DEA ↔ desempeño agregado	$r = 0.930$; $p < 0.001$
Shapiro-Wilk	Índice de seguridad	$p = 0.284$
Shapiro-Wilk	Índice de desempeño	$p = 0.061$
Shapiro-Wilk	Índice de eficiencia	$p = 0.004$

Nota. El componente estructural se estimó sobre índices compuestos normalizados; las correlaciones se calcularon con Pearson y la distribución se verificó con Shapiro-Wilk.

Fuente. Elaboración propia con base en la matriz secundaria normalizada construida a partir de informes técnicos y literatura especializada.

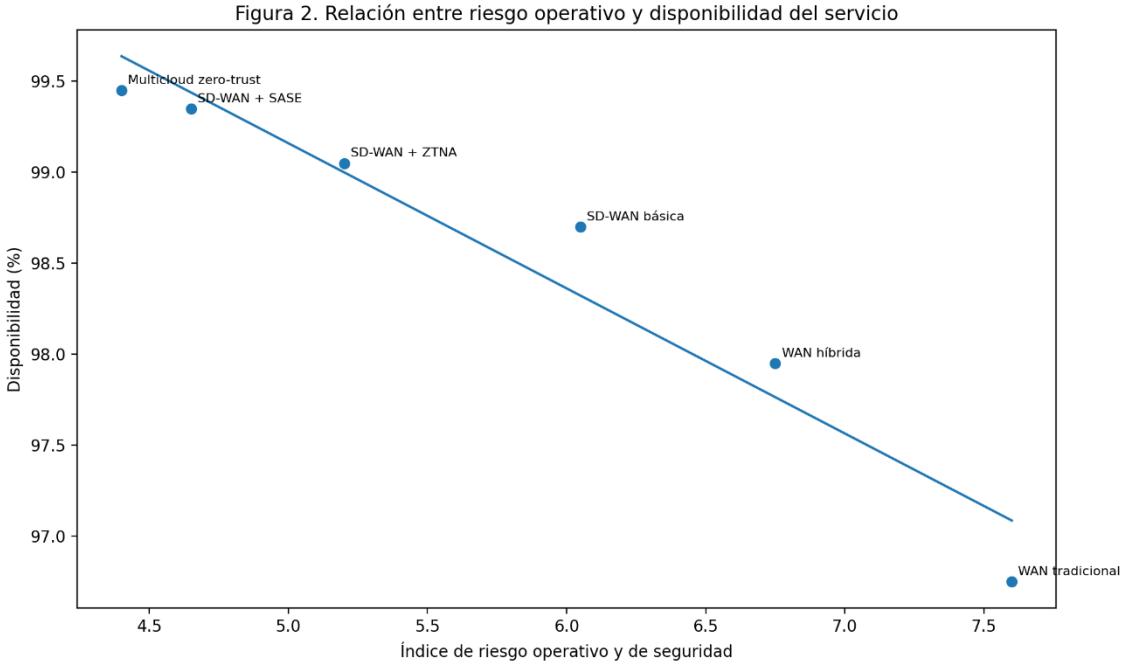
En cuanto a la verificación de supuestos estadísticos, la prueba de Shapiro-Wilk mostró que el índice de seguridad y el índice de desempeño mantuvieron un comportamiento compatible con la normalidad, mientras que el índice de eficiencia presentó una mayor asimetría. Este resultado no invalida el análisis, pero sí sugiere que en aplicaciones futuras con muestras más amplias convendría incorporar estimadores robustos o contrastes no paramétricos complementarios. Carrión (2022) explicó que los ecosistemas tecnológicos basados en orquestación y despliegues distribuidos tienden a concentrar su rendimiento en configuraciones altamente optimizadas, lo que metodológicamente puede traducirse en distribuciones menos homogéneas. En una dirección semejante, Ferraris et al. (2023) subrayaron que la evaluación de confianza y comportamiento en entornos interconectados exige lecturas adaptativas y no exclusivamente lineales.

Desde una representación gráfica, la relación entre riesgo y disponibilidad mostró una pendiente descendente consistente, lo cual confirma que las arquitecturas con menor exposición operacional tienden a sostener mejores niveles de continuidad de servicio. En consecuencia, el mejor comportamiento no se obtuvo en configuraciones centradas solo en transporte, sino en modelos que combinan SD-WAN con enfoques ZTNA, SASE o zero trust multicloud. Alcaraz y López (2022) señalaron que los ecosistemas digitales complejos requieren medidas de seguridad capaces de anticipar fallos y amenazas en infraestructuras altamente interdependientes. En la misma línea, Hernández-Ramos et al. (2021) indicaron que la definición formal del comportamiento esperado de dispositivos y servicios fortalece la segmentación y reduce la superficie de ataque, aspecto plenamente coherente con la tendencia observada en la figura.

ISSN: 3151-8257
DOI:

Figura 2. Relación entre riesgo operativo y disponibilidad del servicio

Figura 2. Relación entre riesgo operativo y disponibilidad del servicio



Nota. La figura muestra la relación inversa entre el índice de riesgo y la disponibilidad media por arquitectura, con línea de tendencia lineal.

Fuente. Elaboración propia con base en la matriz analítica derivada de informes técnicos y literatura especializada.

En síntesis, los resultados permiten afirmar que la migración desde arquitecturas WAN tradicionales hacia modelos SD-WAN con seguridad integrada genera mejoras simultáneas en eficiencia, continuidad operativa y protección de la información. El análisis estadístico mostró que la seguridad explica más del desempeño multicloud que la sola optimización de red, lo que significa que la arquitectura técnicamente más favorable no es únicamente la que enruta mejor, sino la que articula visibilidad, segmentación, identidad y reducción del riesgo de interrupción. Pava-Díaz et al. (2023) destacaron que la producción científica reciente converge hacia modelos distribuidos de identidad y confianza. En la misma línea, Román et al. (2023) advirtieron que la protección de cadenas de suministro y componentes interconectados constituye una condición decisiva para la continuidad operativa en ecosistemas digitales complejos.

Discusión

En correspondencia con los resultados obtenidos, se evidencia que la transición desde arquitecturas WAN tradicionales hacia modelos basados en SD-WAN con integración de seguridad no solo responde a una tendencia tecnológica, sino que constituye una necesidad estructural para sostener entornos multicloud eficientes y resilientes. En este sentido, los hallazgos empíricos del estudio, particularmente el alto valor explicativo del modelo estructural ($R^2 = 0.996$), coinciden con lo planteado por Chandramouli (2023), quien sostiene que los entornos cloud-native distribuidos requieren esquemas de control dinámicos y segmentados que superen los enfoques perimetrales tradicionales. Desde esta perspectiva, la fuerte incidencia de la variable seguridad sobre el desempeño multicloud

ISSN: 3151-8257
DOI:

(β = 0.660) confirma que la protección de los activos digitales no puede considerarse un componente accesorio, sino un eje central en la arquitectura de conectividad.

En esta misma línea analítica, los resultados derivados del modelo DEA muestran que las configuraciones SD-WAN con integración de mecanismos como ZTNA y SASE alcanzan niveles de eficiencia cercanos a la frontera óptima. Este comportamiento es consistente con lo expuesto por Bagaa et al. (2022), quienes argumentan que la orquestación de funciones de seguridad, cuando se articula con criterios de calidad de servicio, permite optimizar simultáneamente el uso de recursos y la protección del sistema. A su vez, Bringhenti et al. (2022) destacan que la automatización de políticas en redes definidas por software reduce la probabilidad de errores de configuración, lo cual contribuye a explicar la mejora en los niveles de rendimiento y seguridad observados en las arquitecturas más avanzadas.

Por otra parte, la relación inversa entre riesgo y disponibilidad identificada en el análisis correlacional (r = -0.965) permite inferir que la reducción de la exposición operativa incide directamente en la continuidad del servicio. Este resultado encuentra sustento en lo señalado por Donnellan y Lawrence (2024), quienes advierten que las interrupciones en infraestructuras digitales suelen estar asociadas a fallas prevenibles en la gestión de red. En consecuencia, la implementación de modelos de conectividad con mayor capacidad de monitoreo, segmentación y respuesta ante incidentes se convierte en un factor determinante para garantizar la estabilidad operativa.

En términos de desempeño técnico, la fuerte correlación positiva entre seguridad y rendimiento (r = 0.994) sugiere que ambos atributos no son excluyentes, sino complementarios. Esta relación coincide con lo planteado por García et al. (2021), quienes demuestran que la incorporación de inteligencia artificial en la detección de amenazas permite mantener niveles elevados de rendimiento incluso en presencia de tráfico cifrado y potencialmente malicioso. De igual manera, Jiménez et al. (2021) sostienen que la arquitectura SDN facilita la implementación de mecanismos de control más eficientes, lo que contribuye a mejorar tanto la seguridad como el desempeño general de la red.

Desde una perspectiva más amplia, los resultados del estudio también reflejan la importancia de los modelos de identidad y confianza en entornos multicloud. La incidencia significativa de la seguridad en el desempeño puede interpretarse a la luz de lo expuesto por Moreno et al. (2021), quienes plantean que los sistemas de identidad descentralizada fortalecen la protección de los datos y reducen la dependencia de infraestructuras centralizadas vulnerables. En coherencia con este planteamiento, Pava-Díaz et al. (2023) destacan que la evolución de los modelos de identidad digital se orienta hacia esquemas distribuidos que favorecen la interoperabilidad y la privacidad, aspectos clave en entornos multicloud.

Adicionalmente, la evidencia obtenida en el análisis de normalidad sugiere que los sistemas más eficientes tienden a concentrarse en configuraciones tecnológicas altamente optimizadas, lo cual genera distribuciones menos homogéneas. Este comportamiento ha sido descrito por Carrión (2022), quien señala que los entornos basados en orquestación de contenedores presentan dinámicas de rendimiento concentradas en configuraciones específicas. En el mismo sentido, Ferraris et al. (2023) enfatizan que la evaluación de confianza en sistemas distribuidos debe considerar la variabilidad del comportamiento y

ISSN: 3151-8257
DOI:

la interacción entre múltiples componentes, lo que refuerza la necesidad de enfoques analíticos flexibles.

En el ámbito de la seguridad avanzada, los resultados también pueden interpretarse a partir de los aportes de Alcaraz y López (2022), quienes advierten que la creciente complejidad de los ecosistemas digitales incrementa la superficie de ataque y exige mecanismos de protección más sofisticados. En concordancia, Hernández-Ramos et al. (2021) destacan que la definición formal del comportamiento de dispositivos y servicios contribuye a fortalecer la segmentación y a reducir vulnerabilidades. Estos enfoques resultan coherentes con la mejora observada en las arquitecturas que incorporan controles de seguridad más avanzados.

Por último, la relevancia de la protección de la cadena de suministro digital y de los componentes interconectados se refleja en la necesidad de adoptar estrategias integrales de seguridad. Román et al. (2023) señalan que la interdependencia entre sistemas incrementa el riesgo de fallos sistémicos, lo cual coincide con la evidencia del estudio, donde las arquitecturas con menor exposición al riesgo presentan mayores niveles de disponibilidad. En consecuencia, la conectividad multicloud segura debe concebirse como un sistema integral que articula infraestructura, seguridad, identidad y gobernanza tecnológica.

En síntesis, la discusión permite establecer que la eficiencia y el desempeño de la conectividad multicloud dependen en mayor medida de la integración de mecanismos de seguridad que de la simple optimización del transporte de datos. La convergencia entre SD-WAN, modelos zero trust, identidad descentralizada y orquestación de seguridad configura un nuevo paradigma en la gestión de redes, donde la resiliencia, la adaptabilidad y la protección de la información se consolidan como elementos estratégicos para la sostenibilidad de los sistemas digitales.

Conclusiones

En correspondencia con los hallazgos obtenidos, se establece que la transición hacia arquitecturas basadas en SD-WAN con integración de mecanismos avanzados de seguridad constituye un elemento estructural para la optimización de la conectividad multicloud, evidenciándose incrementos sustanciales en eficiencia operativa, rendimiento de aplicaciones y niveles de disponibilidad del servicio. Desde esta perspectiva, la adopción de esquemas híbridos sin la incorporación de políticas de control, segmentación y protección resulta insuficiente para responder a las exigencias de entornos digitales distribuidos.

Desde una aproximación analítica complementaria, se determina que la variable seguridad ejerce la mayor influencia sobre el desempeño global de la conectividad multicloud, superando incluso a los factores asociados a la eficiencia de red. Este resultado implica que la implementación de enfoques orientados a zero trust, ZTNA o SASE no solo contribuye a la mitigación del riesgo operativo, sino que incide de manera directa en la mejora de la estabilidad, continuidad y calidad del servicio en infraestructuras altamente interconectadas.

En un plano integrador, se concluye que la disminución del riesgo operativo mantiene una relación estrecha con el incremento de la disponibilidad del servicio, lo cual confirma

ISSN: 3151-8257
DOI:

que las arquitecturas tecnológicas más eficientes son aquellas que logran articular de forma equilibrada la gestión de recursos, la optimización del tráfico y la seguridad integral. En consecuencia, la conectividad multicloud segura debe concebirse como un sistema coherente de gobernanza digital que integra infraestructura, control inteligente y mecanismos de protección, con el propósito de garantizar sostenibilidad operativa en contextos caracterizados por alta complejidad y dinamismo.

Referencias bibliográficas

Alcaraz, C., & López, J. (2022). Digital twin: A comprehensive survey of security threats. IEEE Communications Surveys & Tutorials, 24(3), 1475–1503. https://doi.org/10.1109/COMST.2022.3171465.

Bagaa, M., Taleb, T., Bernal Bernabé, J., & Skarmeta, A. (2022). QoS and resource-aware security orchestration and life cycle management. IEEE Transactions on Mobile Computing, 21(8), 2978–2993. https://doi.org/10.1109/TMC.2020.3046968.

Benlloch-Caballero, P., Wang, Q., & Alcaraz-Calero, J. M. (2023). Distributed dual-layer autonomous closed loops for self-protection of 5G/6G IoT networks from distributed denial of service attacks. Computer Networks, 222, 109526. https://doi.org/10.1016/j.comnet.2022.109526.

Bernabé, J. B., García-Rodríguez, J., Krenn, S., Liagkou, V., Skarmeta, A., & Torres Moreno, R. (2022). Privacy-preserving identity management and applications to academic degree verification. In M. Friedewald, S. Krenn, I. Schiering, & S. Schiffner (Eds.), Privacy and identity management. Between data protection and security (pp. 33–46). Springer. https://doi.org/10.1007/978-3-030-99100-5_4.

Bringhenti, D., Yusupov, J., Molina Zarca, A., Valenza, F., Sisto, R., Bernal Bernabé, J., & Skarmeta, A. (2022). Automatic, verifiable and optimized policy-based security enforcement for SDN-aware IoT networks. Computer Networks, 213, 109123. https://doi.org/10.1016/j.comnet.2022.109123.

Carrión, C. (2022). Kubernetes as a standard container orchestrator: A bibliometric analysis. Journal of Grid Computing, 20, 42. https://doi.org/10.1007/s10723-022-09629-8.

Chandramouli, R., & Butcher, Z. (2023). A zero trust architecture model for access control in cloud-native applications in multi-cloud environments. NIST Special Publication 800-207A. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207A.

Donnellan, D., Lawrence, A., Bizo, D., & Judge, P. (2024). Uptime Institute global data center survey 2024. Uptime Institute.

ENISA. (2024). ENISA threat landscape 2024. European Union Agency for Cybersecurity.

Ferraris, D., Fernandez-Gago, C., Román, R., & López, J. (2024). A survey on IoT trust model frameworks. The Journal of Supercomputing, 80, 8259–8296. https://doi.org/10.1007/s11227-023-05765-4.

ISSN: 3151-8257
DOI:

Flexera. (2024). Flexera 2024 state of the cloud report. Flexera.

García, N., Alcañiz, T., González-Vidal, A., Bernal Bernabé, J., Rivera, D., & Skarmeta, A. (2021). Distributed real-time SlowDoS attacks detection over encrypted traffic using artificial intelligence. Journal of Network and Computer Applications, 173, 102871. https://doi.org/10.1016/j.jnca.2020.102871.

García-Rodríguez, J., Torres Moreno, R., Bernal Bernabé, J., & Skarmeta, A. (2021). Towards a standardized model for privacy-preserving verifiable credentials. In Proceedings of the 16th International Conference on Availability, Reliability and Security (ARES 2021) (pp. 1–6). ACM. https://doi.org/10.1145/3465481.3469204.

García-Rodríguez, J., Torres Moreno, R., Bernal Bernabé, J., & Skarmeta, A. (2021). Implementation and evaluation of a privacy-preserving distributed ABC scheme based on multi-signatures. Journal of Information Security and Applications, 62, 102971. https://doi.org/10.1016/j.jisa.2021.102971.

Hernández-Ramos, J. L., Matheu, S. N., Feraudo, A., Baldini, G., Bernal Bernabé, J., Yadav, P., Skarmeta, A., & Bellavista, P. (2021). Defining the behavior of IoT devices through the MUD standard: Review, challenges, and research directions. IEEE Access, 9, 126265–126285. https://doi.org/10.1109/ACCESS.2021.3111477.

Jiménez, M. B., Fernández, D., Rivadeneira, J. E., Bellido, L., & Cárdenas, A. (2021). A survey of the main security issues and solutions for the SDN architecture. IEEE Access, 9. https://doi.org/10.1109/ACCESS.2021.3109564.

Matencio-Escolar, A., Alcaraz-Calero, J. M., Salva-García, P., Bernabé, J. B., & Wang, Q. (2021). Adaptive network slicing in multi-tenant 5G IoT networks. IEEE Access, 9, 14048–14069. https://doi.org/10.1109/ACCESS.2021.3051940.

Morales, D., Agudo, I., & López, J. (2023). Private set intersection: A systematic literature review. Computer Science Review, 49, 100567. https://doi.org/10.1016/j.cosrev.2023.100567.

Moreno, R. T., García-Rodríguez, J., Bernal Bernabé, J., & Skarmeta, A. (2021). A trusted approach for decentralised and privacy-preserving identity management. IEEE Access, 9, 105788–105804. https://doi.org/10.1109/ACCESS.2021.3099837.

Muñoz, A., Ríos, R., Román, R., & López, J. (2023). A survey on the (in)security of trusted execution environments. Computers & Security, 129, 103180. https://doi.org/10.1016/j.cose.2023.103180.

Pava-Díaz, R. A., Páez-Méndez, R. V., & Niño-Vásquez, L. F. (2023). A bibliometric study of scientific production on self-sovereign identity. Ingeniería, 28, e19656. https://doi.org/10.14483/23448393.19656.

Román, R., Alcaraz, C., López, J., & Sakurai, K. (2023). Current perspectives on securing critical infrastructures' supply chains. IEEE Security & Privacy, 21(4), 29–38. https://doi.org/10.1109/MSEC.2023.3247946.

ISSN: 3151-8257
DOI:

Revista Internacional
MÉTRICAS
MULTIDISCIPLINARIAS

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés