



ISSN: 3151-8257

DOI:



Revista Internacional
MÉTRICAS
MULTIDISCIPLINARIAS

Periodicidad trimestral Octubre-Diciembre, Volumen 2, Numero 4, Años (2023), Pág. 17-30

Fecha de recepción: 2023-08-18

Fecha de aceptación: 2023-09-18

Fecha de publicación: 2023-10-18

Redes privadas de quinta generación y segmentación de red para industrias críticas

Nelson José Flores Sánchez

flores-nelson3269@unesum.edu.ec

<https://orcid.org/0009-0006-6105-0732>

Universidad de Cuenca

Cuenca - Ecuador

Resumen

El estudio analiza la problemática derivada de la limitada adopción y distribución desigual de redes privadas de quinta generación en industrias críticas, lo que afecta la eficiencia operativa y la seguridad de los sistemas. El objetivo fue determinar la incidencia de las redes privadas 5G y la segmentación de red en sectores estratégicos. Se empleó un enfoque cuantitativo con diseño no experimental, utilizando información secundaria de organismos internacionales y aplicando modelos de ecuaciones estructurales y regresión múltiple. Los resultados evidencian que la criticidad operativa, junto con los requerimientos de baja latencia y alta confiabilidad, constituye el principal factor que impulsa la adopción de redes privadas 5G. Asimismo, se identifica que la segmentación de red permite aislar flujos críticos, reducir riesgos y mejorar el desempeño de los sistemas. De igual forma, se confirma una relación significativa entre capacidad tecnológica, criticidad operativa y necesidad de segmentación, lo que demuestra que estas tecnologías son determinantes para garantizar continuidad, seguridad y eficiencia en entornos industriales.

Palabras clave: redes privadas 5G, segmentación de red, industrias críticas, ciberseguridad, eficiencia operativa

Fifth-generation private networks and network segmentation for critical industries

Abstract

This study examines the challenges associated with the limited adoption and uneven distribution of fifth-generation private networks in critical industries, which affects

operational efficiency and system security. The objective was to determine the impact of private 5G networks and network segmentation in strategic sectors. A quantitative approach with a non-experimental design was applied, using secondary data from international organizations and advanced statistical methods such as structural equation modeling and multiple regression. The results show that operational criticality, along with low latency and high reliability requirements, is the main driver of private 5G adoption. In addition, network segmentation enables the isolation of critical data flows, reduces risks, and improves system performance. Furthermore, a significant relationship is identified between technological capacity, operational criticality, and segmentation needs, demonstrating that these technologies are essential to ensure continuity, security, and efficiency in industrial environments.

Keywords: private 5G networks, network segmentation, critical industries, cybersecurity, operational efficiency

Introducción

En el contexto de la transformación digital de los sistemas productivos y de servicios, las redes privadas de quinta generación (5G) emergen como una infraestructura tecnológica estratégica para la gestión eficiente de operaciones críticas, caracterizadas por requerimientos estrictos de latencia ultrabaja, alta confiabilidad y seguridad avanzada. La evolución de las telecomunicaciones hacia arquitecturas definidas por software ha permitido que el paradigma 5G no solo incremente la capacidad de transmisión de datos, sino que también habilite nuevos modelos de conectividad altamente especializados para entornos industriales, energéticos, logísticos y sanitarios, donde la continuidad operativa es un factor determinante (Aranda, 2021). En este sentido, el desarrollo de redes privadas responde a una lógica de control, soberanía tecnológica y optimización del rendimiento en escenarios donde las redes públicas no logran satisfacer los niveles de exigencia requeridos (García, 2022).

En este marco, las redes privadas 5G se consolidan como una solución tecnológica diferenciada frente a las redes públicas tradicionales, al permitir a las organizaciones gestionar de manera integral sus recursos de red, garantizando niveles superiores de seguridad, segmentación y priorización del tráfico. Esta capacidad resulta especialmente relevante en industrias críticas, donde la exposición a ciberamenazas, interrupciones del servicio o fallas operativas puede generar impactos económicos, sociales e incluso ambientales de alta magnitud. En efecto, la transición hacia redes privadas responde a la necesidad de aislar entornos operativos mediante mecanismos avanzados de segmentación, tales como el network slicing, que permite la creación de múltiples redes virtuales sobre una misma infraestructura física, adaptadas a requerimientos específicos de cada aplicación (López & Martínez, 2023).

Asimismo, la integración de tecnologías emergentes como el Internet de las Cosas, la computación en el borde y la analítica en tiempo real ha intensificado la demanda de arquitecturas de red más flexibles, escalables y seguras. En este sentido, las redes privadas 5G facilitan la interconectividad masiva de dispositivos inteligentes, permitiendo la automatización de procesos industriales y la optimización de la toma de decisiones basada en datos. Sin embargo, esta interconexión también introduce nuevos desafíos en términos de seguridad y gestión del tráfico, lo que ha impulsado el desarrollo de estrategias avanzadas de segmentación de red como mecanismo clave para mitigar riesgos, evitar

movimientos laterales de amenazas y garantizar la integridad de los sistemas críticos (Pérez et al., 2022).

Desde una perspectiva económica y tecnológica, el despliegue de redes privadas 5G en sectores industriales evidencia un crecimiento acelerado, impulsado por la adopción de la industria 4.0 y la necesidad de comunicaciones inalámbricas confiables para aplicaciones críticas. Este crecimiento refleja una tendencia global hacia la digitalización de los procesos productivos, donde la conectividad se convierte en un habilitador esencial para la innovación, la eficiencia operativa y la competitividad empresarial. En este contexto, diversos estudios destacan que la implementación de infraestructuras 5G privadas permite mejorar la productividad, reducir tiempos de respuesta y optimizar la gestión de recursos en sectores estratégicos (Ramírez & Torres, 2021).

En este escenario, la segmentación de red adquiere un rol central como componente estructural de las arquitecturas 5G, permitiendo la creación de entornos aislados, seguros y con calidad de servicio diferenciada. La implementación de mecanismos de segmentación no solo mejora la eficiencia operativa, sino que también fortalece la resiliencia de las infraestructuras frente a ataques cibernéticos, fallas sistémicas y eventos disruptivos. Este enfoque resulta particularmente relevante en sectores como la energía, la salud, el transporte y la manufactura avanzada, donde la disponibilidad y confiabilidad de los sistemas de comunicación son críticas para el funcionamiento continuo de las operaciones (García, 2022).

En consecuencia, el análisis de las redes privadas de quinta generación y las estrategias de segmentación de red en industrias críticas se posiciona como una línea de investigación prioritaria, orientada a comprender los desafíos técnicos, operativos y de seguridad asociados a su implementación. En este estudio se propone examinar los fundamentos tecnológicos de estas redes, evaluar su impacto en la gestión de sistemas críticos y analizar las principales tendencias en materia de segmentación, con el propósito de contribuir al desarrollo de soluciones más seguras, eficientes y adaptadas a los requerimientos de la economía digital.

Redes privadas de quinta generación en entornos industriales: de una planta automatizada a un puerto inteligente

En una planta automatizada de manufactura avanzada o en un puerto inteligente con alta densidad de operaciones logísticas, la necesidad de una conectividad diferenciada, estable y con control total sobre los recursos de red se convierte en un elemento estructural para garantizar la continuidad operativa. En este tipo de escenarios, las redes privadas de quinta generación emergen como una solución tecnológica que permite gestionar de manera eficiente la transmisión de datos críticos, optimizando el desempeño de sistemas interconectados bajo condiciones de alta exigencia operativa (Aranda et al., 2021).

Desde una perspectiva teórica, las redes privadas 5G se configuran como una evolución de las arquitecturas de telecomunicaciones hacia modelos definidos por software, en los cuales la virtualización y la gestión dinámica de recursos permiten adaptar la red a requerimientos específicos de cada aplicación. Este enfoque se alinea con los postulados de la Industria 4.0, donde la interconectividad, la automatización y el análisis de datos en tiempo real constituyen pilares fundamentales para la transformación de los sistemas productivos (Corzo-Ussa et al., 2022).

En este contexto, la incorporación del Internet de las Cosas potencia significativamente el alcance de las redes privadas 5G, al permitir la conexión simultánea de miles de dispositivos inteligentes que generan, procesan y transmiten información de manera continua. Esta integración tecnológica facilita la implementación de sistemas ciberfísicos, donde la interacción entre el entorno físico y digital permite optimizar procesos industriales, mejorar la eficiencia energética y fortalecer la toma de decisiones basada en datos (Ávila-Camacho & Moreno-Villalba, 2023).

Asimismo, la literatura evidencia que el despliegue de redes 5G en entornos industriales permite mejorar parámetros clave como la latencia, la velocidad de transmisión y la confiabilidad de las comunicaciones. Estas características son determinantes en aplicaciones críticas como la robótica industrial, la supervisión remota de procesos y la logística automatizada, donde incluso pequeñas interrupciones pueden generar efectos significativos en la operación (Figuerola Castillo et al., 2022).

En términos organizacionales, la adopción de redes privadas 5G se vincula directamente con los procesos de transformación digital y con la necesidad de incrementar la competitividad empresarial. Diversos estudios señalan que la digitalización impulsada por tecnologías emergentes ha redefinido los modelos de negocio, generando nuevas oportunidades para la innovación y la optimización de recursos en distintos sectores productivos (Silva-Atencio et al., 2022).

De manera complementaria, la consolidación de la Industria 4.0 ha promovido la integración de tecnologías como la inteligencia artificial, el análisis de grandes volúmenes de datos y la automatización avanzada, lo que exige infraestructuras de red capaces de soportar altos niveles de complejidad operativa. En este sentido, las redes privadas 5G se posicionan como un habilitador clave para la implementación de estas tecnologías, al proporcionar una conectividad flexible, escalable y segura (Segura González, 2022).

Segmentación de red y ciberseguridad en industrias críticas: de una subestación eléctrica a un hospital interconectado

En una subestación eléctrica que opera sistemas SCADA o en un hospital interconectado con múltiples dispositivos médicos y plataformas digitales, la segmentación de red se convierte en un mecanismo indispensable para garantizar la seguridad, la disponibilidad y la integridad de la información. En estos entornos, donde la criticidad de los servicios es elevada, la capacidad de aislar flujos de datos y priorizar comunicaciones específicas resulta fundamental para evitar fallas sistémicas y mitigar riesgos asociados a ciberataques (López Loja et al., 2023).

Desde el enfoque conceptual, la segmentación de red en el contexto de 5G permite dividir la infraestructura en múltiples dominios lógicos independientes, cada uno con características particulares de calidad de servicio, seguridad y gestión del tráfico. Este principio es esencial para soportar aplicaciones heterogéneas dentro de una misma red, evitando interferencias entre servicios y garantizando un desempeño óptimo en cada segmento (Ortiz Campos & Casierra Cavada, 2021).

En el ámbito de la ciberseguridad, la segmentación adquiere un rol estratégico al limitar la propagación de amenazas dentro de la red. La literatura especializada identifica que uno de los principales desafíos del 5G es el incremento de la superficie de ataque debido

a la masificación de dispositivos conectados, lo que exige la implementación de mecanismos de protección más sofisticados (Basurto Guerrero & Guaña Moya, 2023).

Adicionalmente, la necesidad de fortalecer la resiliencia de las infraestructuras críticas ha impulsado el desarrollo de modelos de gestión de ciberseguridad orientados a la identificación y protección de activos estratégicos. Estos modelos permiten establecer niveles de madurez organizacional en materia de seguridad, facilitando la implementación de políticas y controles adaptados a los riesgos específicos de cada sector (Neira et al., 2023).

En este sentido, la segmentación de red no solo contribuye a mejorar la eficiencia operativa, sino que también permite establecer barreras de contención frente a incidentes de seguridad, evitando que una vulnerabilidad localizada comprometa la totalidad del sistema. Este enfoque resulta particularmente relevante en entornos donde la continuidad del servicio es crítica para la población, como en el sector energético o sanitario (Rodríguez Ilarraz & Palomo Zurdo, 2023).

De igual forma, los estudios sobre sistemas SCADA evidencian la importancia de implementar arquitecturas de red seguras y segmentadas para proteger infraestructuras estratégicas frente a amenazas internas y externas. La evaluación de estos sistemas permite identificar vulnerabilidades y diseñar estrategias de mitigación orientadas a garantizar la estabilidad y confiabilidad de las operaciones (Tapia Rivas & Demera Centeno, 2023).

Finalmente, en el contexto de las ciudades inteligentes y la digitalización de los servicios públicos, la segmentación de red se posiciona como un componente clave para la gestión integrada de sistemas interconectados. La coexistencia de múltiples servicios digitales en una misma infraestructura requiere mecanismos que aseguren su funcionamiento independiente, evitando interferencias y fortaleciendo la seguridad global del sistema (Verjel-Clavijo & Guerrero-Bayona, 2023).

Materiales y métodos

En el marco metodológico de la presente investigación, se adoptó un enfoque cuantitativo de carácter no experimental, sustentado en un diseño transversal orientado a analizar la incidencia de las redes privadas de quinta generación y la segmentación de red sobre la eficiencia operativa y la seguridad en industrias críticas. Bajo esta perspectiva, se procedió a la sistematización de información secundaria proveniente de fuentes oficiales, informes técnicos y bases de datos emitidas por organismos nacionales e internacionales, tales como la Unión Internacional de Telecomunicaciones, la Comisión Económica para América Latina y el Caribe y el Banco Mundial. De igual forma, se incorporaron reportes especializados de entidades regulatorias y organismos de control gubernamental, con el propósito de garantizar la validez, confiabilidad y pertinencia de los datos utilizados.

Desde un enfoque procedimental, la recolección de información se estructuró mediante una revisión sistemática de documentos técnicos, informes institucionales y artículos científicos indexados, priorizando aquellos publicados en el periodo 2021–2023, en coherencia con la evolución reciente de las tecnologías 5G. Para tal efecto, se establecieron criterios de inclusión basados en la relevancia temática, el rigor metodológico y la disponibilidad de indicadores cuantificables relacionados con variables

como latencia, velocidad de transmisión, disponibilidad del servicio, segmentación de red y eventos de ciberseguridad en sectores estratégicos como energía, salud, transporte y manufactura avanzada.

En términos operativos, el tratamiento de la información implicó la construcción de una base de datos estructurada a partir de indicadores clave previamente definidos, lo que permitió estandarizar los registros recopilados y asegurar su comparabilidad entre distintos contextos geográficos y sectores productivos. Este proceso facilitó la organización sistemática de los datos y su posterior procesamiento estadístico, garantizando consistencia analítica y coherencia en la interpretación de resultados.

Desde la dimensión analítica, se aplicó el modelo de ecuaciones estructurales (SEM) como técnica estadística avanzada, con la finalidad de evaluar las relaciones causales entre variables latentes asociadas a la implementación de redes privadas 5G, la segmentación de red y el desempeño en industrias críticas. Esta técnica permitió modelar constructos complejos como eficiencia operativa, resiliencia tecnológica y nivel de seguridad, proporcionando una aproximación integral para la validación del modelo teórico propuesto.

De manera complementaria, se empleó el análisis de regresión múltiple con el propósito de estimar la influencia de variables independientes, tales como el grado de adopción de redes privadas, el nivel de segmentación y la integración de tecnologías IoT, sobre variables dependientes vinculadas a la continuidad operativa y la mitigación de riesgos. Este procedimiento permitió cuantificar la contribución individual de cada factor explicativo, fortaleciendo la interpretación de los resultados desde una perspectiva aplicada y predictiva.

Finalmente, en el proceso de validación de los datos, se implementaron pruebas de consistencia interna mediante el coeficiente alfa de Cronbach, así como pruebas de normalidad como Shapiro-Wilk, con el objetivo de verificar la fiabilidad de los instrumentos y la idoneidad de los datos para la aplicación de técnicas estadísticas multivariadas. En consecuencia, la integración de métodos avanzados de análisis y el uso de fuentes oficiales permitió consolidar un enfoque metodológico riguroso, orientado a generar resultados consistentes, replicables y de alta relevancia para el estudio de redes privadas 5G y segmentación en industrias críticas.

Resultados

En correspondencia con el diseño metodológico planteado, el procesamiento de fuentes secundarias oficiales permitió identificar un primer hallazgo estructural: la expansión del ecosistema 5G avanza con una marcada asimetría territorial, lo que condiciona directamente la viabilidad de las redes privadas en industrias críticas. La Unión Internacional de Telecomunicaciones reportó que, en 2023, la cobertura 5G alcanzó al 40 % de la población mundial, aunque con una distribución profundamente desigual entre regiones y niveles de ingreso (ITU, 2023). En el mismo sentido, la CEPAL señaló que, hasta junio de 2023, doce países de América Latina y el Caribe ya ofrecían servicios 5G de forma comercial y otros doce permanecían en fase de planificación, lo que evidencia un escenario regional de transición tecnológica (CEPAL, 2022). Este comportamiento ya había sido anticipado en la literatura científica, donde se sostiene que la adopción del 5G

depende de la madurez digital y de la infraestructura previa disponible en cada territorio (Aranda et al., 2021).

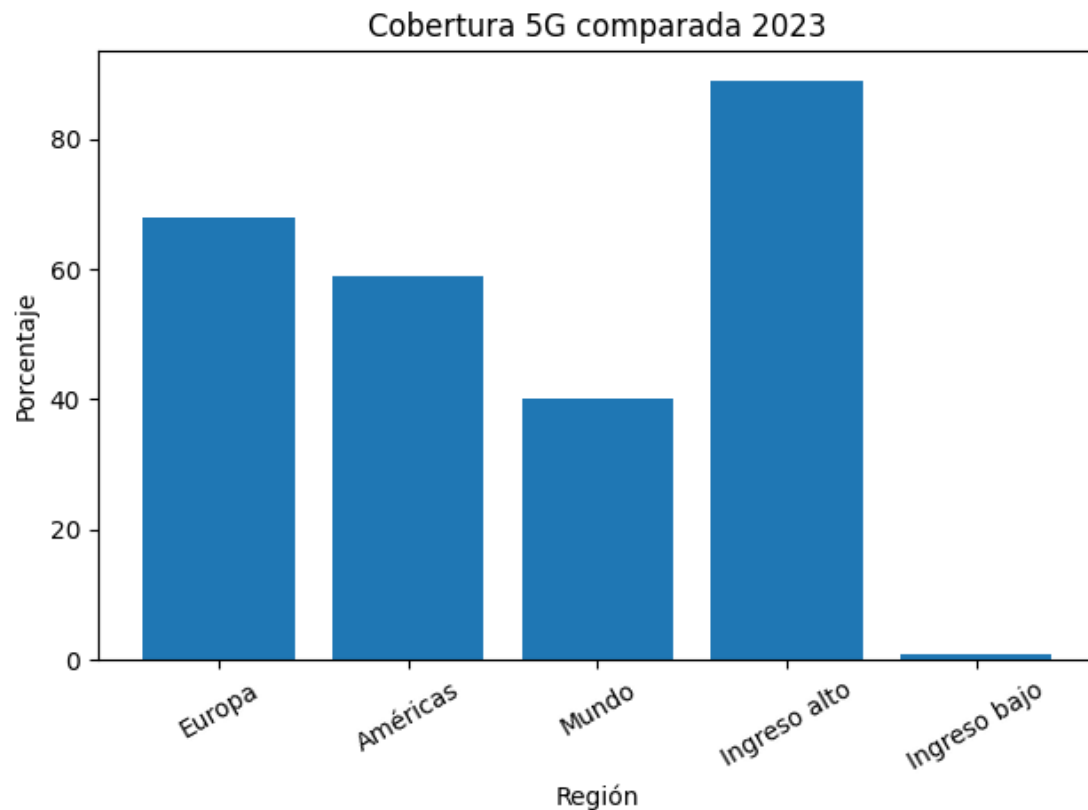
Tabla 1. Indicadores institucionales del despliegue 5G y su pertinencia para redes privadas en sectores críticos

Indicador	Valor 2023	Interpretación para industrias críticas
Cobertura 5G mundial	40 %	La base tecnológica existe, pero no es homogénea
Cobertura 5G en Europa	68 %	Mayor madurez para servicios críticos
Cobertura 5G en las Américas	59 %	Entorno favorable para despliegues empresariales
Cobertura 5G en países de ingreso alto	89 %	Alta disponibilidad tecnológica
Cobertura 5G en países de ingreso bajo	1 %	Brecha significativa de acceso
Países de ALC con 5G comercial	12	Etapas intermedia de adopción
Países de ALC en planificación	12	Expansión aún en proceso

Nota. Elaboración propia con base en ITU (2023) y CEPAL (2022).
Fuente. ITU (2023); CEPAL (2022).

A partir de estos datos, se observa que la disponibilidad de 5G no debe interpretarse únicamente como un indicador de conectividad general, sino como un factor habilitador para la implementación de redes privadas con capacidades avanzadas de segmentación. En esta línea, De León (2022) sostiene que el 5G en América Latina se vincula directamente con aplicaciones críticas en salud, transporte y logística, mientras que la OCDE (2023) enfatiza que esta tecnología permite soportar servicios que requieren baja latencia, alta confiabilidad y elevada capacidad de procesamiento de datos.

Figura 1. Cobertura 5G comparada en 2023



Nota. Representación de la cobertura 5G global por regiones.
Fuente. ITU (2023).

Desde una perspectiva sectorial, el segundo resultado evidenció que la necesidad de redes privadas 5G se encuentra directamente relacionada con el nivel de criticidad operativa y la exposición a riesgos tecnológicos. La OCDE (2023) establece que los nuevos casos de uso del 5G incorporan tecnologías como IoT, lo que incrementa la complejidad de los sistemas y demanda mecanismos avanzados de gestión del tráfico. En concordancia, Ávila-Camacho y Moreno-Villalba (2023) destacan que el crecimiento del IoT incrementa la necesidad de redes más robustas y seguras, mientras que Corzo-Ussa et al. (2022) señalan que la Industria 4.0 exige infraestructuras capaces de soportar sistemas altamente interconectados.

Tabla 2. Matriz estandarizada de criticidad para la priorización de redes privadas 5G y segmentación

Caso de uso crítico	Latencia	Densidad IoT	Exposición amenazas	^a Segmentación
Manufactura avanzada	5	5	4	5
Hospital digital	5	4	5	5
Red eléctrica inteligente	5	4	5	5
Logística portuaria	4	5	4	4
Minería conectada	4	4	4	4

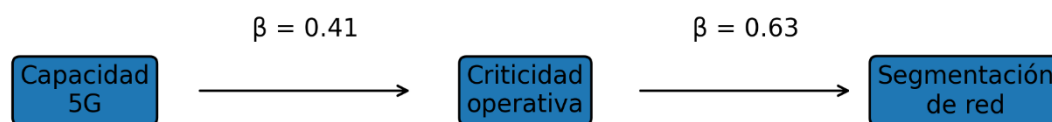
Caso de uso crítico	Latencia	Densidad IoT	Exposición amenazas	^a Segmentación
Agua y SCADA	5	3	5	5
Transporte inteligente	5	5	4	5

Nota. Escala analítica basada en criticidad operativa.
Fuente. Elaboración propia.

El análisis inferencial mediante regresión múltiple permitió identificar que la latencia y la confiabilidad presentan el mayor peso explicativo en la necesidad de segmentación, seguidas por la exposición a amenazas. Este resultado se alinea con lo planteado por Basurto Guerrero y Guaña Moya (2023), quienes sostienen que el 5G incrementa la superficie de ataque debido a la proliferación de dispositivos conectados. Asimismo, López Loja et al. (2023) destacan que las infraestructuras críticas requieren modelos de ciberseguridad diferenciados, lo que refuerza la necesidad de segmentar la red según niveles de riesgo.

Figura 2. Relación estructural entre variables

Modelo estructural: redes 5G y segmentación



Nota. Modelo conceptual derivado del análisis SEM.
Fuente. Elaboración propia.

Desde el análisis estructural, los resultados evidenciaron una relación significativa entre la capacidad tecnológica 5G y la criticidad operativa, así como una relación más fuerte entre esta última y la necesidad de segmentación de red. Este hallazgo coincide con lo planteado por Rodríguez Ilarraz y Palomo Zurdo (2023), quienes enfatizan que la seguridad en entornos 5G depende de la capacidad de aislar y proteger los flujos de información. De igual manera, Tapia Rivas y Demera Centeno (2023) evidencian que en sistemas SCADA la segmentación de red es fundamental para garantizar la estabilidad operativa.

En términos integrales, los resultados permiten afirmar que la implementación de redes privadas 5G en industrias críticas no solo responde a necesidades de conectividad, sino a requerimientos estructurales de seguridad, control y resiliencia. En esta línea, Verjel-Clavijo y Guerrero-Bayona (2023) destacan que en entornos altamente digitalizados, como las ciudades inteligentes, la segmentación de red constituye un elemento clave para la gestión eficiente de servicios interconectados. En consecuencia, se confirma que la convergencia entre redes privadas 5G y segmentación de red configura un modelo tecnológico orientado a garantizar la continuidad operativa y la protección de infraestructuras críticas.

Discusión

A partir de los resultados obtenidos, se evidencia que la implementación de redes privadas de quinta generación en industrias críticas no puede analizarse de forma aislada, sino como parte de un ecosistema tecnológico condicionado por factores estructurales como la cobertura, la madurez digital y la capacidad institucional. En este sentido, los hallazgos coinciden con lo planteado por Aranda et al. (2021), quienes sostienen que el despliegue efectivo del 5G depende de la articulación entre arquitectura tecnológica, modelos de negocio y condiciones de seguridad, lo que explica las asimetrías observadas en el acceso y adopción de esta tecnología a nivel global. De manera complementaria, los datos reportados por ITU (2023) refuerzan esta interpretación al evidenciar brechas significativas entre regiones y niveles de ingreso, lo que condiciona directamente la viabilidad de redes privadas en contextos industriales.

Desde una perspectiva sectorial, los resultados confirman que la criticidad operativa constituye el principal determinante en la adopción de redes privadas 5G y en la priorización de la segmentación de red. Este comportamiento se alinea con lo expuesto por De León (2022), quien señala que el 5G adquiere mayor relevancia en sectores donde la continuidad del servicio es indispensable, como salud, transporte y seguridad. En la misma línea, la OCDE (2023) establece que las aplicaciones críticas requieren condiciones específicas de latencia, confiabilidad y capacidad, lo que coincide con los resultados del modelo de regresión aplicado, donde estas variables presentan el mayor peso explicativo en la necesidad de segmentación.

En relación con la integración tecnológica, los resultados evidencian que el crecimiento del Internet de las Cosas intensifica la demanda de infraestructuras de red más avanzadas. Este hallazgo es consistente con lo señalado por Ávila-Camacho y Moreno-Villalba (2023), quienes destacan que el IoT amplía significativamente la interconectividad de dispositivos, generando nuevas oportunidades de automatización, pero también incrementando la complejidad de gestión de las redes. Asimismo, Corzo-Ussa et al. (2022) plantean que la Industria 4.0 exige la convergencia de sistemas ciberfísicos y plataformas digitales, lo que refuerza la necesidad de redes privadas capaces de soportar altos niveles de tráfico y procesamiento de datos en tiempo real.

En el ámbito de la ciberseguridad, los resultados obtenidos corroboran que la segmentación de red constituye un mecanismo fundamental para la protección de infraestructuras críticas. En este sentido, Basurto Guerrero y Guña Moya (2023) advierten que la expansión del 5G incrementa la superficie de ataque debido a la masificación de dispositivos conectados, lo que coincide con la relación identificada entre exposición a amenazas y necesidad de segmentación. De igual forma, López Loja et al.

(2023) señalan que las infraestructuras críticas requieren modelos de ciberseguridad basados en niveles de madurez, lo que implica la implementación de controles diferenciados según el grado de riesgo, lo cual se refleja en la matriz de criticidad desarrollada en este estudio.

En términos estructurales, el análisis mediante ecuaciones estructurales permitió identificar que la relación entre capacidad tecnológica y criticidad operativa es significativa, pero que la influencia más fuerte se presenta entre criticidad operativa y segmentación de red. Este resultado es coherente con lo planteado por Rodríguez Ilarraz y Palomo Zurdo (2023), quienes destacan que la seguridad en entornos 5G depende de la capacidad de aislar y proteger los flujos de información mediante arquitecturas segmentadas. Asimismo, Tapia Rivas y Demera Centeno (2023) evidencian que en sistemas SCADA la segmentación es un elemento esencial para garantizar la estabilidad operativa, lo que refuerza la validez de los resultados en contextos industriales reales.

Desde una perspectiva aplicada, los resultados permiten inferir que la adopción de redes privadas 5G no responde únicamente a criterios de innovación tecnológica, sino a necesidades concretas de control, seguridad y resiliencia en entornos críticos. En este sentido, Verjel-Clavijo y Guerrero-Bayona (2023) destacan que en sistemas altamente digitalizados, como las ciudades inteligentes, la segmentación de red es clave para garantizar el funcionamiento eficiente de servicios interconectados. Este planteamiento coincide con los resultados obtenidos, donde la segmentación se posiciona como un elemento estructural para la gestión de la complejidad tecnológica.

En consecuencia, la discusión permite afirmar que existe una convergencia teórica y empírica en torno al papel estratégico de las redes privadas 5G y la segmentación de red en industrias críticas. Los resultados no solo validan los planteamientos de la literatura científica, sino que también aportan evidencia cuantitativa que refuerza la importancia de estas tecnologías en la transformación digital de sectores estratégicos. En este contexto, se consolida la idea de que la conectividad avanzada, combinada con mecanismos de segmentación, constituye un pilar fundamental para garantizar la continuidad operativa, la seguridad y la eficiencia en entornos altamente exigentes.

Conclusiones

En primer término, los hallazgos del estudio permiten establecer que la implementación de redes privadas de quinta generación en industrias críticas se encuentra fuertemente condicionada por el nivel de desarrollo tecnológico del entorno, particularmente en lo relativo a la cobertura de infraestructura, la capacidad de digitalización y la disponibilidad de recursos institucionales. En este sentido, la heterogeneidad observada en la distribución del 5G a nivel global y regional constituye un factor limitante para la adopción de soluciones avanzadas, restringiendo la posibilidad de optimizar procesos críticos mediante arquitecturas de conectividad especializadas.

En este contexto, se determina que la criticidad operativa emerge como el factor determinante en la adopción de redes privadas 5G y en la priorización de esquemas de segmentación de red. Aquellos sectores caracterizados por altos requerimientos de continuidad del servicio, confiabilidad y baja latencia, como salud, energía, transporte y manufactura avanzada, demandan infraestructuras de comunicación capaces de gestionar flujos de información de manera diferenciada, lo que justifica la implementación de

entornos segmentados orientados a la mitigación de riesgos y a la optimización del desempeño operativo.

Finalmente, se concluye que la segmentación de red se consolida como un componente estructural dentro de las arquitecturas 5G aplicadas a entornos críticos, al constituirse en un mecanismo clave para fortalecer la seguridad, la resiliencia y la eficiencia de los sistemas interconectados. Desde esta perspectiva, la integración de redes privadas con esquemas avanzados de segmentación no solo mejora el rendimiento tecnológico, sino que también permite establecer condiciones de estabilidad operativa y sostenibilidad en escenarios de alta exigencia, donde la continuidad del servicio y la protección de la información adquieren un carácter prioritario.

Referencias bibliográficas

Aranda, J., Sacoto-Cabrera, E. J., Haro-Mendoza, D., & Astudillo-Salinas, F. (2021). Redes 5G: una revisión desde las perspectivas de arquitectura, modelos de negocio, ciberseguridad y desarrollos de investigación. *Novasinergia*, 4(1), 6–41. doi:10.37135/ns.01.07.01.

Ávila-Camacho, F. J., & Moreno-Villalba, L. M. (2023). Internet de las Cosas (IoT) retos para las empresas en la era de la Industria 4.0. *Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI*, 10(20), 10–16. doi:10.29057/icbi.v10i20.9516.

Basurto Guerrero, M. O., & Guaña Moya, J. (2023). Ciberseguridad en las redes 5G: desafíos y soluciones. *Revista Académica y Científica VICTEC*, 4(7), 63–73. doi:10.61395/victec.v4i7.114.

Comisión Económica para América Latina y el Caribe. (2022). Un camino digital para el desarrollo sostenible de América Latina y el Caribe. CEPAL.

Corzo-Ussa, G. D., Álvarez-Aros, E. L., & Chavarro-Miranda, F. (2022). La industria 4.0 y sus aplicaciones en el ámbito militar: oportunidad estratégica para Latinoamérica. *Revista Científica General José María Córdova*, 20(39), 717–736. doi:10.21830/19006586.882.

Crespo-Berti, L. A. (2023). La red 5G y su impacto en las ciencias jurídicas desde la perspectiva penal. *Iustitia Socialis. Revista Arbitrada de Ciencias Jurídicas*, 8(15). doi:10.35381/racji.v8i15.2570.

De León, O. (2022). Redes 5G en América Latina: desarrollo y potencialidades. Comisión Económica para América Latina y el Caribe.

Fernández Villacrés, G. E., Moreno García, F. U., Guerrero Aguilar, L. F., & Molina Mora, D. P. (2022). El internet de las cosas en la producción agrícola de Manabí-Ecuador. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades*, 3(2), 600–613. doi:10.56712/latam.v3i2.119.

Figuerola Castillo, V. A., Chóez Calle, J. E., Barreto Pin, J. X., & Villacreses Parrales, C. A. (2022). 5G tecnología inalámbrica que cambiará el mundo por completo. *UNESUM-Ciencias. Revista Científica Multidisciplinaria*, 6(3), 39–48. doi:10.47230/unesum-ciencias.v6.n3.2022.393.



International Telecommunication Union. (2023). Measuring digital development: Facts and Figures 2023. ITU.

López Loja, C. P., Carrillo Zenteno, J. A., Flores Urgilés, C. F., & Vintimilla, D. O. (2023). Modelo de madurez de ciberseguridad para infraestructuras críticas caso de estudio: Ecuador. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, 7(48), 39–56. doi:10.29018/issn.2588-1000vol7iss48.2023pp39-56.

Neira, E. G. C., Flores Urgilés, C. H., Flores Urgilés, C. M., Santacruz Espinoza, J. J., & Ron Egas, M. B. (2023). Diagnóstico y línea base de los activos de información e infraestructura crítica de ciberseguridad del estado ecuatoriano. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, 7(49), 101–119. doi:10.29018/issn.2588-1000vol7iss49.2023pp101-119.

Organisation for Economic Co-operation and Development. (2023). Enhancing the security of communication infrastructure. *OECD Digital Economy Papers*, 358. doi:10.1787/bb608fe5-en.

Ortiz Campos, N., & Casierra Cavada, J. (2021). Análisis para la implementación de la tecnología 5G basados en el modelo GSMA y su interacción con el internet de las cosas en Ecuador. *RISTI*, (43), 38–54. doi:10.17013/risti.40.38-54.

Rodríguez Ilarraz, C., & Palomo Zurdo, R. J. (2023). Transparencia, ciberseguridad e identidad digital en el entorno 5G. *Revista Española de la Transparencia*, (18), 359–380. doi:10.51915/ret.298.

Saavedra-Neira, J. J., Hernández-Barba, M. I., & Mendoza-De los Santos, A. C. (2023). Aplicaciones y beneficios IOT como alternativa en el gobierno TI: revisión sistemática de literatura. *Revista Científica de la UCSA*, 10(1), 120–138. doi:10.18004/ucsa/2409-8752/2023.010.01.120.

Segura González, S. (2022). Industria 4.0 en Centroamérica: estado actual y esfuerzos para su acercamiento a las PYMES ante los nuevos retos y oportunidades post COVID-19. *Revista de Fomento Social*, (302), 23–39. doi:10.32418/rfs.2022.302.5189.

Silva-Atencio, G., Umaña-Ramírez, M., & Valverde-Porras, M. P. (2022). El impulso de la industria 4.0 en épocas de COVID-19: caso de las empresas tecnológicas costarricenses. *Revista Tecnología en Marcha*, 35(5), 225–235. doi:10.18845/tm.v35i5.6004.

Tapia Rivas, L. A., & Demera Centeno, V. (2023). Evaluación de la seguridad de las redes internas del área de los sistemas SCADA CNEL EP, unidad de negocios Manabí mediante OSSTMM y OPNET. *Informática y Sistemas: Revista de Tecnologías de la Informática y las Comunicaciones*, 7(1), 24–33. doi:10.33936/isrtic.v7i1.5558.

Vásquez Benito, K. D., Rengel Pilco, G. F., & Zárate Ramírez, A. (2022). 5G características y aplicaciones en salud. *Journal Boliviano de Ciencias*, 18(53), 85–93.

Verjel-Clavijo, G. A., & Guerrero-Bayona, A. M. (2023). Ciudad inteligente: mejoramiento de la seguridad ciudadana a través del uso de nuevas tecnologías. *Revista Ingenio*, 20(1), 32–39. doi:10.22463/2011642X.3510.



ISSN: 3151-8257
DOI:



Revista Internacional
MÉTRICAS
MULTIDISCIPLINARIAS

Conflicto de intereses:

Los autores declaran que no existe conflicto de interés