Analizar las vulnerabilidades de seguridad en redes 5G y su impacto en la privacidad de datos y la exposición a ciberataques en pagos digitales

Alan Edimmer Jimenez Chica

Directora

Yina Alexandra González Sanabria

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Monografía presentada como requisito para optar al título de:

Ingeniera de sistemas

Marzo 2026

Dedicatoria

Este proyecto se lo dedico a mi padres que siempre me han apoyado siempre en este proceso, a mis abuelitos que siempre han confiado en mi para estudiar y graduarme de mi carrera, a mis tíos por siempre estar disponibles para ayudarme a resolver cualquier problema que he tenido en mi carrera, a mis hermanos por siempre ser una motivación para nunca rendirme sin importar lo difícil que sea, a mí por siempre seguir adelante sin importar lo difícil del proceso, el tiempo para entregar buenos trabajos, revisar las fuentes bibliográficas y coordinar los trabajos con mis compañeros para que todos logremos aprender y realizar aportes significativos

Agradecimientos

Quiero agradecer a mis padres por siempre impulsarme a perseguir mis sueños y hoy estar realizado este trabajo para cumplir un objetivo de vida que es tener mi carrera, a toda mi familia por siempre apoyarme cuando lo he necesitado y a mí por dar siempre lo mejor de mis todos los días para ser un mejor estudiante y aprender mucho más

Resumen

Las redes 5G, quinta generación de tecnología móvil, ofrecen velocidades de hasta 10 Gbps (100 veces más rápidas que 4G), latencia de 1-5 ms y capacidad para conectar hasta 1 millón de dispositivos por km². Operan en bandas de frecuencia baja, media y alta, utilizando tecnologías como *network slicing* (redes virtuales independientes), *edge computing* (procesamiento cercano al usuario) y virtualización de funciones. Esto habilitas aplicaciones como cirugías remotas, vehículos autónomos y pagos digitales seguros. Sin embargo, estas innovaciones introducen nuevos riesgos de seguridad.

En Colombia, el despliegue de 5G promete avances económicos y sociales (Bowen, 2022), pero también vulnerabilidades. Su arquitectura basada en software, computación al borde y segmentación de red amplía la superficie de ataque (Tulsa, 2024). La descentralización del procesamiento en el borde debilita las defensas tradicionales, aumentando riesgos de sabotaje cibernético. La integración masiva de dispositivos IoT, muchos con seguridad débil, facilita ataques como botnets y DDoS. Además, el modo no autónomo de 5G, que depende de la infraestructura 4G/3G, hereda vulnerabilidades de protocolos como SS7 y Diameter, permitiendo intercepción de SMS y elusión de autenticación de dos factores. Fallos en el protocolo 5G-AKA, como el "5G AKA Bypass", habilitan suplantaciones y mensajes maliciosos. La cadena de suministro global de 5G también introduce riesgos, como componentes falsificados o software malicioso, explotables por actores estatales o cibercriminales.

Estas vulnerabilidades amenazan la privacidad. El cifrado débil, el aislamiento deficiente en la segmentación de red y los dispositivos de borde comprometidos exponen datos sensibles (Owoko, 2024). La mayor capacidad de recopilación de datos de 5G, junto con la densificación de antenas, facilita el seguimiento de ubicaciones y la elaboración de perfiles detallados. Los dispositivos LoT con poca seguridad agravan la exposición de datos

personales. En pagos digitales, el compromiso de datos biométricos, irreversibles por naturaleza, aumenta el riesgo de robo de identidad financiera. Para mitigar estos riesgos, es crucial abordar proactivamente las vulnerabilidades, fortaleciendo la seguridad de la infraestructura y los dispositivos conectados.

Palabras clave**:** Redes 5G, Quinta generación, Velocidad, Latencia, Conectividad, Segmentación de red, Computación al borde, Virtualización, Aplicaciones críticas, Seguridad, Ciberataques, Privacidad, Internet de las cosas (LoT), Vulnerabilidades, Economía digital

Abstract

5G networks, the fifth generation of mobile technology, offer speeds up to 10 Gbps (100 times faster than 4G), ultra-low latency of 1-5 ms, and the ability to connect up to 1 million devices per km². They operate across low, mid, and high-frequency bands, leveraging technologies like network slicing (independent virtual networks), edge computing (processing near the user), and function virtualization. This enables critical applications such as remote surgeries, autonomous vehicles, and secure digital payments. However, these innovations introduce new security risks.

In Colombia, 5G deployment promises significant economic and social advancements (Bowen, 2022), but it also brings vulnerabilities. Its software-based architecture, edge computing, and network slicing expand the attack surface (Tulsa, 2024). Decentralized edge processing weakens traditional defenses, increasing risks of cyber sabotage. The massive integration of IoT devices, many with weak security, facilitates attacks like botnets and DDoS. Additionally, 5G's non-standalone mode, reliant on existing 4G/3G infrastructure, inherits vulnerabilities from protocols like SS7 and Diameter, enabling SMS interception and bypassing two-factor authentication. Flaws in the 5G-AKA protocol, such as the "5G AKA Bypass," allow impersonation and malicious message injection. The global 5G supply chain also introduces risks, including counterfeit components or malicious software, exploitable by state actors or cybercriminals.

These vulnerabilities threaten privacy. Weak encryption, poor network slicing isolation, and compromised edge devices expose sensitive data (Owoko, 2024). The increased data collection capacity of 5G, combined with antenna densification, facilitates location tracking and detailed profiling. IoT devices with inadequate security further amplify exposure of personal data. In digital payments, the compromise of biometric data, irreversible by nature, heightens the risk of financial identity theft. To mitigate these risks, proactively addressing

vulnerabilities is critical, strengthening the security of infrastructure and connected devices

Keywords**:** 5G networks, fifth generation, Speed, Latency, Connectivity, Network slicing, Edge computing, Virtualization, Critical applications, Security, Cyberattacks, Privacy, Internet of Things (IoT), Vulnerabilities, Digital economy

Tabla de contenido

Lista de tablas

Lista de Figuras

Introducción

En la actualidad, el desarrollo de las redes móviles de quinta generación(5G) representan un avance significativo en la conectividad global, permitiendo velocidades de transmisión de datos sin precedentes, baja latencia y una mayor capacidad de dispositivos conectados. Esta tecnología promete transformar sectores clave como la salud, la educación, el transporte y, especialmente, los servicios financieros. Sin embargo, junto con sus beneficios, emergen preocupaciones criticas relacionadas con la seguridad de la información, la privacidad de los usuarios y la exposición a ciberataques, especialmente en contextos donde la infraestructura tecnológica y la legislación aún están en proceso de consolidación, como es el caso de Colombia.

Las redes 5G, al estar basadas en arquitecturas virtualizadas y distribuidas, presentan nuevas superficies de ataque que no estaban presentes en generaciones anteriores. Estas vulnerabilidades pueden ser explotadas por actores maliciosos para interceptar comunicaciones, manipular datos o comprometer sistemas críticos. Según Diaz (2023), en un estudio publicado por la revista Trilogía Ciencia Tecnología Sociedad, el uso de tecnologías de la información ha traído consigo un aumento en los delitos informáticos y otras problemáticas sociales asociadas, lo que evidencia la necesidad de fortalecer los mecanismos de seguridad en entornos digitales.

Además, la creciente dependencia de plataformas digitales para realizar pagos y transferencias ha generado una nueva forma de vulnerabilidad: la monetización de los datos personales. En muchos casos, los usuarios entregan información sensible sin conocer los riesgos asociados ni las políticas de tratamientos de datos. Como advierte Quiros García (2021), los datos personales se han convertido en el “oro del siglo XXI”, y su uso indebido puede derivar en prácticas ilegales como la extorsión digital o robo de identidad

Por tanto, resulta fundamental analizar de manera critica las implicaciones de la

tecnología 5G en la seguridad digital y la privacidad de los usuarios, especialmente en un país como Colombia, donde la transformación digital avanza rápidamente pero aún enfrenta brechas significativas en términos de regulación, educación digital y ciberseguridad. Esta monografía busca aportar a ese análisis, identificando las principales vulnerabilidades de las redes 5G y su impacto en los pagos digitales, con el fin de proponer recomendaciones que contribuyan a un desarrollo tecnológico más seguro y ético.

Planteamiento del problema

La implementación de las redes 5G (redes de quinta generación) en Colombia marca un punto de inflexión en la evolución tecnológica del país. Esta nueva generación de conectividad promete revolucionar la forma en que las personas interactúan con los servicios digitales, especialmente en el ámbito financiero. La velocidad, la baja latencia y la capacidad de conectar múltiples dispositivos simultáneamente abren la puerta a una digitalización más profunda de los pagos y transacciones cotidiana.

Sin embargo, este avance también trae consigo una serie de riesgos que no pueden ser ignorados. Las redes 5G, al estar basadas en arquitecturas que pueden ser aprovechadas por grupos maliciosos. Esto incluye la posibilidad de interceptar comunicaciones, manipular datos en tránsito y acceder a sistemas críticos sin autorización. Uno de los principales focos de preocupaciones es la seguridad de los pagos digitales.

A medida que más colombianos adoptan plataformas de pago móvil, billeteras digitales y servicios bancarios en línea, aumenta también la exposición a amenazas como la suplantación de identidad, el robo de credenciales y el fraude financiero. La velocidad de las redes 5G, aunque beneficiosas, también puede dificultar la detección temprana de actividades sospechosas.

Además, las interfaces de programación de aplicaciones (APIs) utilizados por bancos Fintech para integrar servicios financieros son especialmente vulnerables si no se implementan con protocolos de seguridad robustos. En un entorno 5G, donde la conectividad es constante y ubicua, cualquier brecha en estas interfaces de las transacciones. En Colombia, aunque existen regulaciones como la circular 029 de la Superintendencia Financiera, estas normativas no abordan de manera específica los desafíos técnicos que plantea la tecnología 5G. La regulación actual se enfoca en aspectos generales de seguridad de la información,

pero no contempla los nuevos vectores de ataque introducidos por la virtualización de funciones de red, el edge computing o la conectividad masiva.

Este vacío normativo deja a las instituciones financieras y a los usuarios en una posición vulnerable. La falta de lineamientos claros sobre cómo proteger los sistemas en un entorno 5G puede traducirse en una implementación insegura de tecnologías que, aunque innovadoras requieren un enfoque más riguroso en términos de ciberseguridad.

La educación digital tiene un papel fundamental en este contexto. Muchos usuarios no están plenamente informados sobre los riesgos que se encuentran asociado al uso de servicios financieros digitales, lo que los hace más susceptibles a caer en trampas como el phishing (ciberataque donde roban información confidencial o datos personales de un usuario), el malware (programa maligno) o las aplicaciones falsas. La falta de conciencia sobre la protección de datos personales agrava aún más el problema.

En este escenario, es fundamental desarrollar estrategias de mitigación que se adapten al contexto colombiano. Estas estrategias deben considerar tanto las capacidades tecnológicas del país como sus limitaciones regulatorias y sociales. La implementación de soluciones de seguridad basadas en inteligencia artificial, autenticación multifactor y cifrado extremo a extremo pueden ser claves para reducir los riesgos.

Asimismo, es necesario fomentar la colaboración entre el gobierno, el sector privado y la academia para generar conocimiento de estándares técnicos, protocolos de respuesta ante incidentes y campañas de concientización ciudadana que fortalezcan la confianza en los sistemas digitales.

Para finalizar, la llegada del 5G a Colombia representa una oportunidad única para modernizar el sistema financiero, pero también plantea desafíos urgentes en materia de seguridad y privacidad.

Justificación

La implementación de las redes 5G marca un punto de inflexión dentro de la evolución tecnología en Colombia. Este tipo de avance tecnológico no solo promete mejorar la velocidad de conexión y reducir la latencia, sino que también habilita nuevas formas de interacción digital, especialmente en el ámbito económico y financiero. Sin embargo, este avance no está exento de riesgos. La complejidad técnica del 5G introduce nuevas vulnerabilidades que, si no se abordan adecuadamente financieras.

Uno de los principales motivos para desarrollar esta investigación es la falta de preparación normativa frente a los desafíos que plantea esta red de quinta generación (5G). Aunque exististe regulaciones generales sobre seguridad de la información, como la circular 029 de la Superintendencia intendencia Financiera, estas no contemplan las amenazas específicas que surgen con la virtualización de funciones de red, el edge computing y la conectividad masiva. Esta laguna regulatoria deja a los usuarios expuestos a riesgos como el fraude por SIM swapping (suplantación de tarjeta SIM), el robo de datos financieros y los ataques a plataformas bancarias.

En este contexto, el sistema financiero colombiano enfrenta una paradoja: por un lado, se impulsa la digitalización de los servicios para mejorar la inclusión financiera; por otro lado, no se han establecido mecanismos de protección suficientemente robustos para garantizar la seguridad de estas operaciones. Esta contradicción puede minar la confianza de los usuarios y frenar el avance de la transformación digital.

También, la infraestructura tecnología de Colombia presenta desigualdades significativas. Mientras algunas entidades financieras cuentan con recursos para implementar soluciones avanzadas de ciberseguridad, otras, especialmente la más pequeñas o regionales, enfrentan limitaciones técnicas y presupuestarias. Esta disparidad crea un

ecosistema financiero fragmentado, donde los niveles de protección varían considerablemente entre instituciones.

La mayoría de los estudios se centran en los beneficios económicos del 5G dejando de lado los riesgos asociados a la seguridad y la privacidad. Esta investigación busca llenar ese vacío, proporcionando un análisis técnico y contextualizado que pueda servir de referencia para futuras políticas públicas y estrategias de mitigación en el sector financiero colombiano.

Por ejemplo, el estudio de Muños Hernández et al. (2019) sobre riesgos informáticos en Colombia evidencia como la evolución tecnológica ha incrementado la necesidad de proteger la información almacenada digitalmente. Los autores destacan que las amenazas informáticas afectan a todos los aspectos de las organizaciones (Muñoz Hernández et al., 2019).

Así mismo, Rojas-Diaz y Yepes-Londoño (2022) advierten que el uso irreflexivo de las tecnologías de la información ha generado un aumento en los delitos informáticos en América Latina. Su revisión sistemática revela que, a pesar del impacto de estas problemáticas, existe un déficit investigativo que impide acciones de intervención eficaces (Rojas-Díaz & Yepes-Londoño,2022).

Otro aspecto relevante es la falta de conciencia ciudadana sobre los riesgos digitales. Muchos usuarios no comprender como sus datos pueden ser utilizados o comprometidos, lo que los hace más vulnerables a ataques y fraudes. Esta situación se ve agravada por la escasa adopción de buenas prácticas de ciberseguridad, como el uso de autenticación multifactor o la verificación de legitimidad de las plataformas de pago.

La educación digital, por tanto, se convierte en un componente esencial para mitigar los riesgos asociados al 5G. Es necesario implementar campañas de concientización que informan a los usuarios sobre los peligros del entorno digital y les enseñen a proteger su

información personal. Esta tarea debe ser asumida tanto por el estado como por las entidades financieras educativas.

Además, la confianza en el sistema financiero digital depende de gran medida de la percepción de seguridad. Si los usuarios sienten que sus datos no están protegidos o que las plataformas son susceptibles a ataques, es probable que reduzcan su uso de estos servicios, afectando negativamente la inclusión financiera y el desarrollo económico. Por ello, garantizar la seguridad en redes 5G no es solo una cuestión técnica, sino también social y económica.

Como lo plantea el artículo de la revista venezolana de gerencia, las organizaciones deben adoptar estrategias integrales de seguridad informática que incluyan tanto medidas técnicas como procesos de capacitación y cultura organizacional. Este enfoque es especialmente relevante en contexto del 5G, donde la velocidad de adopción tecnológica supera muchas veces la capacidad de respuesta institucional (C (Muñoz Hernández, Zapata Cantero, Requena Vidal, & Ricardo, 2019).

Esta investigación busca convertirse en una herramienta útil para el sector financiero colombiano. Al identificar las principales amenazas técnicas asociadas al 5G y proponer soluciones concretas, se espera contribuir a una adopción más segura de esta tecnología, protegiendo tanto a las instituciones como a los usuarios. Este aporte es esencialmente valioso en un momento en que el país se encuentra en plena transición hacia una economía digital.

Para finalizar, el desarrollo y la finalidad de este proyecto es responder a una necesidad urgente de fortalecer la seguridad digital en Colombia ante la llegada del 5G. La falta de regulación específica, la escasa literatura loca, la desigualdad tecnológica y la baja conciencia ciudadana hacen imprescindible una investigación que aborde estos desafíos de

manera integral. Solo así será posible garantizar que la transformación digital del país se realice de forma segura, inclusiva y sostenible.

Objetivos

Objetivo general

Analizar las vulnerabilidades de seguridad en redes 5G y su impacto en los sistemas de pagos digitales en Colombia, para proponer estrategias de mitigación que fortalezcan la protección de datos y transacciones financieras

Objetivos específicos

Identificar las principales vulnerabilidades técnicas de las redes 5G que afectan la seguridad de los pagos digitales en el contexto colombiano

Evaluar el nivel de exposición a ciberataques en las plataformas de pagos digitales causado por la implementación del 5G

Comparar los estándares de seguridad actuales con los riesgos identificados, determinando sus brechas de protección

Proponer un conjunto de medidas técnicas y normativas adaptadas al ecosistema financiero colombiano para reducir los riesgos de seguridad en pagos digitales con 5G

Marco Referencial

Transformación Digital y Potencial de las Redes 5G

La transformación digital cobro fuerza en la última década, impulsada por la necesidad de modernizar los servicios públicos y privados. En este contexto, la llegada de las redes 5G representa una oportunidad para acelerar procesos de innovación, especialmente en sectores como el financiero, donde la conectividad es clave para el funcionamiento de plataformas de pago, banca móvil y servicios digitales.

El 5G no es simplemente una mejora de velocidad al respecto al 4G; implica una reconfiguración completa de la arquitectura de redes. Esta tecnología permite la conexión simultanea de millones de dispositivos, lo que habilita el desarrollo de ciudades inteligentes, vehículos autónomos y sistemas financieros más agiles. Sin embargo, esta misma complejidad técnica introduce nuevos desafíos en materia de seguridad.

Desafíos de Ciberseguridad en el Entorno 5G

Uno de los principales riesgos asociados al 5G son la descentralización de los nodos de red, lo que dificulta la supervisión centralizada y aumenta la superficie de ataque. En redes tradicionales, los puntos de control eran más limitados, pero en el 5G, cada dispositivo puede convertirse en un punto vulnerable si no se implementan medidas de protección adecuadas.

En el caso colombiano, la infraestructura tecnología aún presenta brechas significativas. Aunque se han realizado pilotos de 5G en ciudades como Bogotá y Medellín, la cobertura nacional es limitada y la preparación institucional para enfrentar los riesgos de ciberseguridad es desigual. Esto plantea un reto importante para la adopción segura de esta tecnología. La ciberseguridad en Colombia ha sido abordada principalmente desde una perspectiva reactiva. Las políticas públicas, como la Política Nacional de Seguridad Digital, han avanzado en la identificación de amenazas, pero aún falta una integración efectiva con

sectores estratégicos como el financiero. Esta desconexión puede ser critica en un entorno 5G, donde los ataques pueden propagarse rápidamente.

Pagos Digitales y Seguridad en el Sector Financiero

En el ámbito financiero, los pagos digitales crecieron de forma exponencial. Según datos del Banco de la República, el uso de billeteras digitales y transferencias electrónicas aumento más del 60% entre 2020 y 2023. Este crecimiento, aunque positivo, también vino acompañado por un incremento en los fraudes eléctricos y el robo de identidad.

La investigación de Rodríguez y Castañeda (2021) sobre seguridad en plataformas de pago en Colombia señalo que muchas Fintech carecen de protocolos robustos de protección de datos, lo que las convierte en blancos fáciles para los ciberdelincuentes (Vargas, 2021).

Esta situación se agrava con la llegada del 5G, que puede facilitar ataques más sofisticados y difíciles de rastrear.

Otro estudio relevante es el de Martínez y Gómez (2022), quienes analizaron la percepción de seguridad en usuarios de banca móvil. Su investigación revelo que la confianza del usuario está directamente relacionada con la transparencia en el manejo de datos y la capacidad de respuesta ante incidentes (Rojas-Díaz J. J.-L., 2022). Esto sugirió que la ciberseguridad en un componente esencial. Muchos usuarios no comprenden los riesgos asociados al uso de servicios financieros digitales, lo que los hace más vulnerables a fraudes como el phishing o el SIM swapping, la alfabetización digital debe ser parte fundamental dentro de cualquier estrategia de implementación de 5G. La interoperabilidad entre plataformas también representa un riesgo. A medida que los servicios financieros se integran con redes sociales, Marketplace y otras aplicaciones, se multiplican los puntos de entrada

para posibles ataques. La estandarización de protocolos de seguridad es fundamental para mitigar estos riesgos.

Desde el punto de vista técnico, el 5G requiere un enfoque de seguridad basado en capas. Esto incluye desde la protección del hardware hasta la supervisión del tráfico de red mediante inteligencia artificial. La detección temprana de anomalías puede marcar la diferencia entre un incidente menor y una brecha de seguridad masiva.

La experiencia internacional ofrece lecciones valiosas en países como Estonia y Finlandia, la implementación del 5G ha estado acompañada de marcos regulatorios estrictos y una de fuerte inversión del 5G. Colombia puede adaptar estas experiencias a su contexto, priorizando la protección de los datos personales y la integridad de las transacciones.

Gobernanza y Confianza para una Adopción Segura del 5G

La colaboración entre el sector público, privado y académico es clave. Universidades como la Nacional y la Javeriana desarrollaron líneas de investigación en ciberseguridad, pero aún falta una mayor articulación del sector financiero. Esta sinergia es esencial para generar soluciones adaptadas al entorno colombiano.

En cuanto a la regulación, la Ley 1581 de 2012 sobre protección de datos personales es un avance importante, pero no contempla los desafíos específicos del 5G. Es necesario actualizar el marco normativo para incluir aspectos como la protección de datos en redes virtualizadas, la responsabilidad de los proveedores de servicios y los mecanismos de auditoría. La percepción de seguridad en los usuarios de plataformas digitales es un factor determinante para su adopción y su uso continuo. En el contexto colombiano, donde el acceso a servicios financieros digitales ha crecido rápidamente, la confianza del usuario se convierte en un activo estratégico. Según Salas- Rubio y Abrego-Alzaman (2023), la seguridad percibida y la confianza son antecedentes clave en la aceptación del comercio

electrónico, y su ausencia puede generar resistencia al uso de estas tecnologías. Los autores destacaron que la implementación de mecanismos de autenticación, el cifrado de datos y la transparencia en las políticas de privacidad son los elementos esenciales para fortalecer la confianza del consumidor. En un entorno potenciado por redes 5G, donde las transacciones se realizan a mayor velocidad y con mayor volumen de datos, estos factores adquieren aún más relevancia para garantizar la integridad del sistema financiero (Ábrego-Almazán, 2023).

En el plano operativo, las entidades financieras deben adoptar una cultura de seguridad que vaya más allá del cumplimiento normativo. Esto implica capacitar al personal, realizar auditorías periódicas y establecer protocolos de respuesta ante incidentes. La improvisación ante un ciberataque puede tener consecuencias irreversibles.

Finalmente, el marco referencial de esta investigación se sustenta en la necesidad de comprender el 5G como un ecosistema complejo que requiere una gobernanza sólida, una regulación adaptativa y una cultura de seguridad digital. Solo así será posible aprovechar todo su potencial sin comprometer la privacidad y la confianza de los usuarios.

Marco Conceptual

Características y Potencial de las Redes 5G

Las redes 5G, o redes móviles de quinta generación, representan una evolución tecnología que supera ampliamente las capacidades de sus predecesoras. Esta tecnología se caracteriza por ofrecer velocidades de transmisión de datos significativamente más altas, una latencia ultra baja y una capacidad de conexión masiva de dispositivos. Estas características permiten habilitar aplicaciones avanzadas como la automatización industrial, la telemedicina, los vehículos autónomos y, especialmente, los servicios financieros digitales en tiempo real. En el contexto colombiano, el despliegue de 5G ha sido impulsado por la necesidad de modernizar la infraestructura digital y cerrar brechas de conectividad, aunque aún enfrenta desafíos regulatorios y técnicos.

Desde una perspectiva técnica, el 5G se basa en una arquitectura más compleja que incluye tecnologías como el network slicing, el edge computing y la virtualización de funciones de red. Estas innovaciones permiten una mayor flexibilidad y eficiencia en la gestión del tráfico de datos, pero también introducen nuevas superficies de ataque que deben ser consideradas desde el diseño de la red. Según un estudio publicado en la revista Redalyc, el avance de las Tecnologías de la Información y la Comunicación (TIC), incluyendo el 5G, ha transformado profundamente la forma en que se accede a la información y se gestionan los servicios digitales, lo que exige una adaptación institucional y técnica para garantizar su uso seguro y eficiente.

Despliegue del 5G en Colombia: Avances y Desafíos

En Colombia, el ministerio TIC ha promovido pilotos de 5G en ciudades como Bogotá, Medellín y Cali, con el objetivo de evaluar su viabilidad técnica y su impacto en sectores estratégicos. Sin embargo, expertos advierten que la adopción de esta tecnología debe ir acompañada de políticas públicas claras en materia de ciberseguridad, protección de datos y gobernanza digital. La literatura académica nacional aún es limitada en cuanto al análisis de riesgos específicos del 5G, lo que refuerza la necesidad de investigaciones que aborden estos desafíos desde una perspectiva local y contextualizada.

Pagos Digitales: Innovación y Confianza en el Sector Financiero

Los pagos digitales son transacciones financieras que se realizan a través de medios electrónicos, sin necesidad de dinero en efectivo o contacto físico. Estos incluyen el uso de aplicaciones móviles, plataformas bancarias en línea, billeteras digitales, código QR y transferencias electrónicas. Su principal ventaja radica en la rapidez, comodidad y trazabilidad que ofrecen, lo que ha impulsado su adopción tanto por parte de consumidores como de empresas. En Colombia, el crecimiento de los pagos digitales ha sido notable en los últimos años, especialmente tras la pandemia, que acelero la digitalización de servicios financieros y el comercio electrónico.

Desde una perspectiva académica, los pagos digitales nos representan una innovación tecnológica, sino también un cambio en los hábitos de consumo y en la estructura del sistema financiero. Según Salas-Rubio y Abrego-Almazán (2023), la aceptación de estos medios de pago está fuertemente influenciada por la percepción de seguridad y la confianza del usuario en las plataformas utilizadas (Ábrego-Almazán, 2023). Los autores destacan que la implementación de mecanismos de autenticación, el cifrado de datos y la transparencia en las políticas de privacidad son factores determinantes para fomentar el uso de estas tecnologías

en contextos emergentes como el colombiano.

Los ciberataques se pueden entender como acciones deliberadas y maliciosas ejecutadas a través de redes y sistemas informáticos, con el propósito de comprometer la seguridad de la información o la funcionalidad de los activos digitales. Estas ofensivas buscan, fundamentalmente, la explotación de vulnerabilidades en el hardware, software o incluso en los procesos humanos para lograr acceso no autorizado, manipulación o interrupción de operaciones (Schneier, 2015). A diferencia de simples fallos técnicos, un ciberataque implica una intención hostil, donde un actor (individuo, grupo u organización) persigue un objetivo específico, ya sea el robo de datos, el sabotaje, la extorsión o la interrupción de servicios críticos, impactando severamente a gobiernos, empresas e individuos a nivel global (Kshetri, 2014).

La morfología de los ciberataques es sorprendentemente variada, abarcado desde técnicas relativamente sencillas hasta operaciones de alta sofisticación. Por ejemplo, los ataques de phishing siguen siendo una de las vías más comunes para el robo de credenciales, donde los atacantes suplantan identidades legitimas para engañar a las víctimas (ENISA, ENISA (European Union Agency for Cybersecurity, 2017). Los programas maliciosos como el ransomware, que secuestran datos o sistemas exigiendo un rescate, han escalado en frecuencia y agresividad, paralizando organizaciones enteras (Broadcom, 2019). También destacan los ataques de denegación de servicio distribuido (DDoS), que buscan saturar la capacidad de un servidor o red, impidiendo que usuarios legítimos acceden a los servicios. A esto se suman las amenazas persistentes avanzadas, caracterizadas por su sigilo y

persistencia, a menudo respaldadas por estados, y la inyección de código malicioso como SQL injectios o cross-site scripting (XSS) en aplicaciones web (Foundation, 2021).

Ciberataques y Vulnerabilidades en el Ecosistema 5G

Un caso real en Bogotá con el exsecretario de seguridad Hugo Acero fue víctima de la modalidad de suplantación a través de su tarjeta SIM.

Los delincuentes lograron robarle la portabilidad numérica de su línea telefónica. Una vez que tuvieron el control de su número, intentaron sustraer dinero sus cuentas y realizar transacciones con sus tarjetas de crédito.

Este caso demuestra que incluso figuras públicas con conocimiento en seguridad no son inmunes a este tipo de ataques, lo que subraya la sofisticación de los cibercriminales y la vulnerabilidad de la autenticación basadas en mensajes de texto Noticias Caracol, (2024, febrero 24). Le hicieron millonario fraude tras ser víctima de suplantación, Youtube, https://www.youtube.com/watch?v=lWNLe8Q7ANs.

Las repercusiones de un ciberataque exitoso son multifacéticas y pueden ser devastadoras. Económicamente, las empresas enfrentan costos significativos por la remediación de daños, la restauración de sistemas, las multas por incumplimiento de normativas de privacidad y la pérdida de ingresos debido a la interrupción del negocio (Institute., 2023). Mas irreparablemente la reputación de una marca y en casos críticos,incluso comprometer la seguridad nacional o la infraestructura critica (Ventures, 2023). La interconexión de sistemas y la dependencia global de la tecnología digital significan que un incidente en una entidad puede tener un efecto domino, afectando a múltiples sectores y países.

El concepto de “vulnerabilidad de seguridad” en el ámbito de la ciberseguridad se refiere a una debilidad o fallo en un sistema, aplicación, protocolo o incluso en los procedimientos humanos, que puede ser explotados por una amenaza para comprometer la confidencialidad, integridad o disponibilidad de la información o de los activos del sistema.

Como lo define el Instituto Nacional de Ciberseguridad, una vulnerabilidad es un “fallo técnico o deficiencia de un programa que puede permitir que un usuario no legitimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota” (INCIBE, 2020). Estas debilidades son inherentes a la complejidad de los sistemas y pueden surgir por errores de diseño, implementación, configuración o mantenimiento.

Las vulnerabilidades pueden manifestarse en diversas formas. Por ejemplo, pueden ser errores en el software, configuraciones incorrectas de sistemas o redes, falta de parches o actualizaciones en sistemas operativos y aplicaciones, o la utilización de credenciales débiles o predeterminadas. También pueden ser fallas en los controles de acceso, la gestión de permisos o falta de validación de entradas de datos, lo que abre puertas a los atacantes para ejecutar código arbitrario o acceder a información sensible (Hackmetrix., 2023). Incluso el factor humano, a través de la falta de concientización o capacitación en seguridad, puede introducir vulnerabilidades significativas en una organización (Hacknoid, 2023).

El impacto de una vulnerabilidad de seguridad puede ser devastador para una organización, independientemente de su tamaño. La explotación exitosa de una vulnerabilidad puede llevar a la interrupción de operaciones, perdida de datos sensibles, daños a la reputación, multas regulatorias por incumplimiento de normativas de protección de datos como GDPR, y significativas pérdidas financieras debido a los costos de remediación y la interrupción del negocio (Xygeni, 2025). Por ello la identificación evaluación y mitigación proactiva de las vulnerabilidades son pilares fundamentales de una estrategia de ciberseguridad robusta (Seguridad, 2023).

Protección de Datos y Educación Digital: Pilares para un Ecosistema Seguro

La protección de datos personales se erige como un derecho fundamental y un pilar esencial en la sociedad digital contemporánea, refiriéndose al conjunto de principios,

normativas y mecanismos técnicos y organizativos destinados a salvaguardar la información que identifica o puede identificar a una persona física. Su propósito primordial es garantizar la privacidad individual y el control sobre la información, evitando el uso indebido, el acceso no autorizado sobre el derecho a la intimidad (Solove, 2008). Este concepto se basa en la idea de que los individuos deben tener la capacidad de decidir cómo se recogen, almacenan, utilizan y comparten sus datos, promoviendo la transparencia y la responsabilidad por parte de quienes los procesan (EDPB, 2025).

Para materializar este derecho este derecho, se han desarrollado marcos regulatorios complejos a nivel global y regional. Un ejemplo paradigmático es el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que ha establecido estándares rigurosos sobre la legitimidad del tratamiento, la minimización de datos, la exactitud, la limitación del plazo de conservación, la integridad y confidencialidad y la rendición de cuentas (RGPD, 2016). Estas normativas no solo imponen obligaciones a las organizaciones que tratan datos, sino que también otorgan a los individuos una serie de derechos específicos, como el derecho de acceso, rectificación, suspensión, limitación del tratamiento, portabilidad y oposición (ICO, 2025). La implementación efectiva de estos principios requiere no solo de un marco legal robusto, sino también de medidas técnicas de seguridad y políticas internas rigurosas.

La relevancia de la protección de datos personales se magnifica en un mundo crecientemente interconectado, donde la información es un activo valioso y las violaciones de datos pueden tener consecuencias severas. Una protección inadecuada puede derivar en fraudes de identidad, discriminación, exposición a ciberataques dirigidos, o incluso la manipulación de comportamientos (Zuboff, 2019). Por tanto, es vital para mantener la confianza en los servicios digitales, fomentar la innovación responsable y asegurar la autonomía de los individuos frente al poder de las grandes corporaciones y los estados. La

falta de un régimen de protección de datos solido puede acarrear no solo sanciones económicas para las empresas, sino también in detrimento significativo en la reputación y la relación con los usuarios.

La educación digital se refiere al proceso integral de enseñanza y aprendizaje que incorpora y aprovecha las tecnologías de la información y la comunicación (TIC) para enriquecer las experiencias educativas, desarrollar competencias digitales y preparar a los individuos para desenvolverse eficazmente en un entorno cada vez más digitalizado. No se limita simplemente al uso de dispositivos tecnológicos en el aula, sino que implica una transformación pedagógica profunda que fomenta nuevas metodologías, recursos y formas de interacción (Sangrà, 2012). Este concepto abarca desde la adquisición de habilidades técnicas básicas hasta el pensamiento crítico, La resolución de problemas y la ciudadanía digital responsable, fundamentales para la participación plena en la sociedad del conocimiento.

Este paradigma educativo se manifiesta en diversas formas y niveles. Incluye la enseñanza a distancia y en línea (e-learning), el uso de plataformas virtuales de aprendizaje, recursos educativos abiertos y herramientas colaborativas, que facilitan el acceso al conocimiento y personalizan el proceso de aprendizaje (Siemens, 2005). Además, la educación digital impulsa el desarrollo de lo que se conoce como competencias digitales, que van más allá del manejo de herramientas e implican la capacidad de buscar, gestionar y producir información de forma critica, como comunicarse de manera efectiva en entornos virtuales y comprender las implicaciones éticas y de seguridad del uso de la tecnología (Ala-Mutka, 2011). Fomenta, asimismo, la autonomía del estudiante y su capacidad de autoaprendizaje continuo en un mundo en constante cambio.

La trascendencia de la educación digital es innegable en el siglo XXI, dado que prepara a individuos y sociedades para afrontar los desafíos y aprovechar las oportunidades de la era digital. Es crucial para el desarrollo profesional, la inclusión social y la reducción de

la brecha digital, ya que permite a las personas adquirir las habilidades necesarias para el mercado laboral y para participar activamente en la vida pública y privada (García-Peñalvo, 2018). Además, contribuye a una mayor equidad en el acceso a la educación y a la construcción de sociedades más resilientes y adaptables. En un contexto donde la tecnología avanza rápidamente, la educación digital se convierte en un imperativo para garantizar que todos puedan prosperar y contribuir de manera significativa.

Colombia se encuentra inmersa en un proceso acelerado de transformación digital, impulsado por políticas gubernamentales y la creciente adopción de tecnologías emergentes que buscan optimizar la eficiencia económica y social. En este escenario, el despliegue de las redes de quinta generación representa un hito crucial, prometiendo no solo una conectividad sin precedentes -caracterizada por su alta velocidad, baja latencia y masiva capacidad de conexión-, sino también la habilitación de un vasto ecosistema de servicios avanzados, incluyendo soluciones financieras más agiles e innovadoras (GSMA, 2023) La promesa del 5G para el sector financiero es particularmente atractiva, ya que facilitará transacciones instantáneas, impulsará el internet de las cosas (loT) financiero y permitirá el desarrollo de nuevos modelos de negocio basados en datos en tiempo real, lo que se alinea con la estrategia de inclusión financiera y modernización del país (Asobancaria, Superintendecia Financiera de Colombia, 2023).

Sin embargo, esta rápida adopción tecnológica no está exenta de desafíos significativos, especialmente en lo que respecta a la seguridad y la privacidad. La arquitectura subyacente de 5G, basada en software y con una mayor superficie de ataque debido a la densificación de nodos y la virtualización de funciones de red, introduce inherentemente nuevos vectores de amenaza que no existían en generaciones anteriores de telecomunicaciones (ENISA, ENISA Threat Landscape for 5G Networks, 2020). En el contexto colombiano, estas vulnerabilidades se ven exacerbadas por una infraestructura

tecnología que aún presenta brechas significativas en términos de madurez y resiliencia. A pesar de los avances, la disparidad en la calidad de la conectividad, la limitada adopción de estándares de seguridad robustos en algunas capas de la infraestructura y la falta de talento especializado en ciberseguridad continúan siendo puntos débiles que pueden ser explotados por actores maliciosos (CAF, 2020).

Adicionalmente, el marco regulatorio vigente en Colombia no ha evolucionado a la misma velocidad que la disrupción tecnológica. Las leyes y normativas existentes en materia de ciberseguridad y protección de datos, aunque fundamentales, no contemplan completamente la complejidad y los desafíos específicos que plantean las redes 5G y la exposición de los pagos digitales (SIC, Informe sobre Protección de Datos Personales en el Sector Financiero, 2023). Esta brecha regulatoria genera incertidumbre y puede dejar vacíos legales que comprometan la capacidad del Estado y las empresas para proteger la información de los usuarios y garantizar la integridad del sistema financiero. La ausencia de marcos claros sobre la responsabilidad ante incidentes en entornos 5G o la falta de normativas específicas para la seguridad de transacciones habilitadas por la loT financiera, por ejemplo, incrementan el riesgo para la privacidad de los datos y la exposición a ciberataques dirigidos (BID, La Ciberseguridad en América Latina y el Caribe: Nuevos Retos y Oportunidades, 2022).

En este desarrollo del proyecto, resulta imperativo un análisis exhaustivo de como estas innovaciones tecnológicas, particularmente las redes 5G y la proliferación de los pagos digitales, impactan directamente la seguridad de los usuarios y la integridad del sistema y la masificación de los datos del sistema financiero colombiano. La interconexión de sistemas y la masificación de los datos sensibles en tránsito hacen que cualquier vulnerabilidad en la infraestructura 5G pueda ser un vector de ataque para comprometer la privacidad de datos personales y financieros, exponiendo a los usuarios y a las instituciones a ciber ataques de

mayor sofisticación y escala (Forum, 2023). Un estudio riguroso sobre estos riesgos es esencial para proponer estrategias de mitigación efectivas y construir un ecosistema digital seguro y confiable para todos los actores involucrados

Marco Teórico

Fundamentos de la Ciberseguridad Adaptativa

La ciber seguridad adaptativa representa un paradigma avanzado en la protección de sistemas y datos, que se distancia significativamente de los enfoques de seguridad tradicionales. Mientras que la ciberseguridad convencional se basa predominante mente en modelos estáticos de defensa perimetral y detección de amenazas conocidas mediante firmas, la ciberseguridad adaptativa adopta una postura proactiva y dinámica. Su esencia radica en la capacidad de evolucionar y ajustarse continuamente a un panorama de amenazas en constante cambio, aprendiendo de cada interacción y anticipando posibles ataques, en lugar de reaccionar únicamente a incidentes ya ocurridos (Mak, 2017). Este enfoque reconoce que las organizaciones operan en un entorno de riesgo persistente y que la prevención absoluta es inalcanzable, por lo que la resiliencia y la capacidad de respuesta son primordiales.

Marcos Teóricos de la Ciberseguridad Adaptativa

Los principios clave que rigen la ciberseguridad adaptativa incluyen detección proactiva, que utiliza análisis predictivos y comportamientos para identificar anomalías antes de que escalen a incidentes; la respuesta dinámica, que permite a los sistemas ajustar sus defensas y contramedidas en tiempo real basándose en la inteligencia de amenazas y con defensa. ataque; y el aprendizaje automático, que es fundamental para que el sistema mejore su efectividad con el tiempo, reconociendo patrones emergentes y optimizando las estrategias de defensa. Otros principios importantes son la segmentación para contener los ataques y la automatización de tareas repetitivas para acelerar la respuesta. Frameworks como el defens`s

Adaptive Security Architecture proponen un ciclo continuo de predecir, prevenir, detectar y responder, integrando inteligencia de amenazas, análisis de comportamiento y orquestación de seguridad (HARBOR, 2014). De manera similar, el NIST Cybersecurity Framework, aunque no es exclusivamente adaptativo, proporciona una estructura que facilita la implementación de un enfoque más dinámico a través de sus funciones de identificar, proteger, detectar, responder y recuperar, permitiendo a las organizaciones madurar sus capacidades para reaccionar a amenazas evolutivas (NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2018).

Aplicaciones de la Ciberseguridad Adaptativa en Redes 5G

La aplicación de la ciberseguridad adaptativa es especialmente critica en entornos tecnológicamente avanzados como las redes 5G, donde la baja latencia y la vasta interconexión de dispositivos (loT) multiplican exponencialmente la superficie de ataque y la velocidad a la que pueden propagarse las amenazas. En este contexto, un modelo de seguridad estático es insostenible. La ciberseguridad adaptativa permite monitorear continuamente el comportamiento de miles de millones de dispositivos conectados, identificar patrones anómalos de tráfico en tiempo real y desplegar contramedidas automatizadas para aislar dispositivos comprometidos o segmentos de red antes de que un ataque se propague por toda la infraestructura (Ericsson, 5G Security: Security Architecture and Solutions, 2021). En el sector financiero, por ejemplo, se ha implementado para proteger transacciones digitales en tiempo real, detectando fraudes basados en anomalías de comportamiento del usuario o de la red que no se ajustarían a reglas predefinidas, incluso en ecosistemas de pagos móviles (Ward & Subramanian, 2022). Esto permite una protección continua y una resiliencia superior ante ciber ataques sofisticados que evaden las defensas tradicionales

Arquitectura y Vulnerabilidades de las Redes 5G

La quinta generación de redes móviles representa un salto cualitativo respecto a sus predecesoras, no solo en términos de velocidad y capacidad, sino también en su arquitectura fundamental, que introduce nuevas complejidades y consecuentemente, nuevos vectores de vulnerabilidad. A diferencia de las redes 4G, que se basan en una arquitectura de hardware más monolítica, 5G adopta un enfoque definido por software, virtualizando y altamente distribuido. Sus componentes técnicos clave incluyen el **Núcleo 5G**, que es el cerebro de la red y gestiona la movilidad, el acceso y la calidad del servicio, adoptando una arquitectura nativa de la nueve con funciones de red virtualizada; la **Red de Acceso Radio** (RAN), que conecta los dispositivos de usuario a la red central a través de antenas y estaciones base, evolucionando hacia la RAN virtualizada; el **Slicing de Red** (Network Slicing), que permite la creación de múltiples redes lógicas y personalizadas sobre una misma infraestructura física, adaptándose a necesidades específicas de servicio; y el **edge computing**, que acerca el procesamiento de datos y la capacidad de almacenamiento al punto de origen, reduciendo la latencia y facilitando aplicaciones de tiempo real (ETSI, ETSI EN 303 644: Cybersecurity for 5G - Security Requirements and Evaluation, 2020).

La implementación de estas innovaciones arquitectónicas, si bien es ventajosa para el rendimiento, genera un conjunto de nuevas vulnerabilidades que requieren atención especializada. La virtualización y el SDN son tecnologías fundamentales para el 5G, introducen riesgos derivados de posibles configuraciones erróneas, fallos en el aislamiento entre máquinas virtuales, o ataques dirigidos a las capas de orquestación y gestión que controlan toda la red (Penttinen & GSMA, 2021). La **exposición de interfaces de programación de aplicaciones** (APIs) entre los distintos componentes virtualizados y los

servicios de terceros amplia la superficie de ataque, haciéndolas susceptibles a inyecciones de código, accesos no autorizados o ataque de denegación de servicio (DoS/DDoS) (Citaristi, 2022). Además, la promesa de conectar un numero masivo de dispositivos loT en la red 5G multiplica exponencialmente los posibles puntos de entrada para los atacantes, ya que muchos de estos dispositivos carecen de medidas de seguridad robustas inherentes y pueden ser utilizados como nodos para lanzar ataques distribuidos o exfiltrar datos (ERICSSON, 2021).

Seguridad en Redes 5G vs. 4G: Mejoras y Desafíos

En comparación con las redes 4G, la seguridad en 5G presenta tanto mejoras como nuevos desafíos. Si bien 5G incorpora protocolos de cifrado más fuertes y una autenticación mutua mejorada entre el dispositivo y la red (3GPP, Specification #33.501, 2018), la naturaleza descentralizada y el uso intensivo de tecnologías en la nube y virtualización cambian el paradigma de seguridad de un perímetro relativamente fijo a uno más difuso. En 4G, la seguridad se centraba más en la red central y los enlaces de radio; en 5G, la seguridad debe ser inherente cada “slice” de red, en el edge, y en cada nuevo servicio o dispositivo conectado. Estudios técnicos e informes de organismos como la ETSI (European Telecommunications Standards Institute) y el 3GPP (3rd generation Partnership Project) han detallado extensamente estas consideraciones, delineando arquitecturas de seguridad y requisitos para mitigar riesgos. Por ejemplo, el 3GPP especifica mecanismos para la privacidad de la identidad del suscriptor y la protección de la señalización (3GPP TS33.501), mientras que la ETSI ha publicado un análisis sobre la seguridad de NFV y SDN (ETS NFV SEC 001)

Protección de Datos en Pagos Digitales

La proliferación de los pagos digitales ha revolucionado la forma en que las transacciones financieras se llevan a cabo, ofreciendo comodidad y eficiencia, pero también elevado la complejidad de la protección de la información sensible. Los **tipos de datos sensibles** que se manejan en este ecosistema son variados y altamente atractivos para los ciberdelincuentes. Incluyen **credenciales** de acceso a plataformas bancarias (nombre de usuario, contraseñas), los tokens de autenticación generados para transacciones específicas, y cada vez más, los datos biométricos (huellas dactilares, reconocimiento facial) utilizados para la verificación de identidad. Además, se gestiona información transaccional detallada, números de tarjetas de crédito/debito, códigos de seguridad (CVV) e incluso datos de geolocalización asociados a las operaciones, cuya exposición podría derivar en fraudes masivos y suplantación de identidad (Europol, 2023).

Para mitigar estos riesgos, el sector financiero y tecnológico ha implementado diversas tecnologías de protección robustas. El **cifrado de extremo a extremo** (E2EE) asegura que los datos se transformen en un formato ilegible desde el punto de origen hasta su destino final, impidiendo que terceros no autorizados accedan a la información en tránsito. La tokenizacion reemplaza los datos sensibles de la tarjeta de pago (o credenciales) por un valor único, no sensible (no token), que no tienen valor fuera del contexto especifico de la transacción, reduciendo así el riesgo en caso de una brecha de datos (Council, 2022). Por su parte, la **autenticación multifactor (MFA)** exige que los usuarios verifiquen su identidad a través de al menos dos métodos de seguridad distintos (por ejemplo, contraseña y código enviado al celular), lo que añade una capa significativa de protección contra accesos no autorizados, incluso si una credencial es comprometida (Grassi, Garcia, & Fenton, NIST

Special Publication 800-63-3: Digital Identity Guidelines, 2017).

A pesar de estas defensas, persisten **amenazas comunes** que evolucionan constantemente. El skimming digital busca interceptar datos de tarjetas de crédito directamente desde los formularios de pago en línea de sitios web comprometidos. El **malware financiero**, como troyanos bancarios, se especializa en robar credenciales y datos de transacciones directamente desde los dispositivos de los usuarios. Los **ataques Man in the Middle (MitM)**, por su parte, permiten a los atacantes interceptar y alterar la comunicación entre dos partes sin que estas lo perciben, facilitando el robo de información o la manipulación de transacciones. Para contrarrestar estas amenazas, existen normativas relevantes y estándares de cumplimiento a nivel global, como el **PCI-DSS (Payment Card Industry Data Security Standard)**, que establece un conjunto de requisitos para las organizaciones que procesan, almacenan o transmiten datos de tarjetas de crédito, y la **ISO/IEC 27001**, un estándar internacional para sistemas de gestión de seguridad de la información (ISMS). En Colombia, la **Circular Externa 007 de 2019** de la Super Intendencia Financiera, junto con la Ley 1581 de 2012 de Protección de Datos Personales, establecen el marco regulatorio para la gestión de riesgos de ciber seguridad y la protección de información sensible en el sector financiero, adaptando principios globales a la realidad nacional (Colombia S. F., 2019).

Un ejemplo práctico de estas amenazas y la necesidad de una seguridad robusta se observa en **casos reales de fraudes en billeteras digitales** como Nequi, Bancolombia a la mano o Daviplata en Colombia. Estos servicios, aunque convenientes, han sido blanco de estafas de phishing y smishing (phishing vía SMS) donde los atacantes suplantan la identidad

de las plataformas para engañar a los usuarios y obtener sus credenciales o tokens de acceso, resultado en el vaciado de cuentas (Torres, 2024). Estos incidentes demuestran que más allá de las tecnologías de protección, la **concienciación del usuario y la educación**

digital son elementos cruciales para fortalecer la cadena de seguridad en el ecosistema de pagos digitales

Marco Normativo y Estrategias de Ciberseguridad en Colombia

El panorama de la ciberseguridad en Colombia se configura mediante una articulación de entidades especializadas y un marco normativo en constante evolución, diseñado para tanto a ciudadano como a la infraestructura critica del país. Una de las figuras centrales en esta estrategia es el ColCERT (Centro Cibernético de Colombia), que opera como el Computer Emergency Response Team nacional. Sus Funciones principales incluyen el monitoreo proactivo de la ciberseguridad a nivel nacional, la emisión de alertas sobre vulnerabilidades y amenazas emergentes, y la coordinación de la respuesta a incidentes cibernéticos de gran envergadura que afectan a entidades públicas y privadas. ColCERT actúa como un punto de contacto clave para la cooperación nacional e internacional en materia de ciberseguridad, facilitando el intercambio de información y la mitigación de riesgos (ColCERT., 2025).

Este enfoque institucional no solo fortalece la capacidad de respuesta ante incidentes, sino que también promueve una cultura de prevención y colaboración entre actores públicos y privados. La labor del ColCERT es especialmente relevante en un entorno digital cada vez más interconectado, donde amenazas como el ransomware, el phishing y los ataques a infraestructuras criticas requieren una vigilancia constante y coordinada. Además, su rol como puente entre Colombia y organismos internacionales permite al país mantenerse

actualizado frente a tendencias globales en ciberseguridad, adaptando buenas prácticas y tecnologías emergentes a su contexto normativo y operativo.

Los informes recientes de ColCERT y otras entidades muestran una escalada preocupante en las estadísticas de ciber ataques en Colombia durante los últimos dos años. Si

bien las cifras exactas varían, las tendencias generales apuntan a un aumento significativo en la frecuencia y sofisticación de los ataques, con un impacto creciente en sectores como el financiero, gubernamental y de telecomunicaciones. Según el Reporte de Cibercrimen 2023 de la Policía Nacional de Colombia, las denuncias por delitos informáticos continúan al alza, destacando el fraude por medios informáticos, la violación de datos personales y la suplantación de identidad como los incidentes más recurrentes (DIGITAL, 2023). Estos datos subrayan la persistencia de las amenazas y la necesidad de fortalecer las capacidades de defensa del país ante un entorno digital cada vez más hostil.

El marco normativo colombiano busca establecer un pilar legal para la seguridad digital y la protección de la información. La ley 1581 de 2012 es la piedra angular para la protección de datos personales, estableciendo los principios y derechos que rigen el tratamiento de datos en el país, similar en espíritu al GDPR europeo, aunque con diferencias especificas en su alcance y sanciones (Comercio, 2023). Por otro lado, la Ley 1273 de 2009 tipifica los delitos informáticos, endureciendo las penas para acciones como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, el daño informático, el fraude por medios informáticos y la suplantación de sitios web. Mas recientemente, el Decreto 338 de 2022 consolida la Política Nacional de Seguridad Digital, proporcionando directrices estratégicas para la gestión de riesgos de ciberseguridad, la protección de infraestructuras críticas y la promoción de una cultura de seguridad digital en el sector público y privado (Colombia P. d., 2022).

Estas normativas e iniciativas del gobierno se complementan con documentos de política como la Política Nacional de Confianza digital y el CONPES 3995 de 2020, que busca fortalecer la resiliencia digital y la ciberseguridad. Dicha política promueve un enfoque integral, abordando la gobernanza, la gestión de riesgos, la respuesta a incidentes y la cooperación público-privada (DNP, Documento CONPES 3995: Política Nacional de

Confianza Digital, 2020). Al comparar este andamiaje normativo con estándares internacionales como el NIST Cybersecurity Framework o el GDPR (Reglamento General de Protección de Datos) de la unión europea, se observa que Colombia ha adoptado muchos principios y mejores prácticas globales. Aunque la Ley 1581 de 2012 comparte la esencia de garantizar el control del individuo sobre sus datos, el GDPR, por ejemplo, impone requisitos de cumplimiento más estrictos y multas significativamente mayores. El NIST Framework, por su parte, ofrece una guía más flexible y basada en el riesgo para la implementación de programas de ciberseguridad, y las empresas colombianas a menudo lo utilizan como referencia para sus propias estrategias de seguridad (MinTIC, 2023). Este marco regulatorio, aunque en desarrollo continuo, es crucial para sentar las bases de un entorno digital seguro en un país en plena transformación tecnológica.

Desarrollo de Objetivos Específicos

Vulnerabilidades técnicas de las redes 5G

La tecnología **5G** representa la quinta generación de redes móviles, marcando una evolución significativa y una ruptura tecnológica fundamental respecto a su predecesora, la 4G LTE. Mas allá de ser una simple mejora de velocidad, 5G se diseñó para habilitar un nuevo universo de servicios y aplicaciones que demandan capacidades de red sin precedentes. Sus **características clave** distintas incluyen una **alta velocidad** de transmisión de datos (con picos teóricos de hasta 10 Gbps), una **baja latencia** (inferior a 1ms), lo que permite respuestas casi instantáneas criticas para aplicaciones de control remoto y vehículos autónomos, y una **mayor densidad de dispositivos conectados** (hasta 1 millón de dispositivos por kilómetro cuadrado). Esta evolución permite la convergencia de tecnologías como el Internet de las Cosas (loT), la inteligencia digital en múltiples sectores (ITU, 2020).

La arquitectura técnica del 5G es intrínsecamente más compleja y flexible que la de 4G, diseñada para ser nativa de la nube y programable. Se compone de dos elementos

principales: la **Red de Acceso Radio (RAN)** y la **Red central (Core)**. La RAN en 5G, conocida como New Radio (NR), se ha desagregado y virtualizado, permitiendo una mayor flexibilidad y eficiencia en el despliegue y gestión de las estaciones base. La **Red Central (5GC)**, por su parte, se ha reconstruido desde cero con un enfoque de microservicios, operando sobre plataformas de **virtualización de funciones de red (NFV)**. Esto significa que las funciones de red que antes requerían hardware propietario ahora pueden ejecutarse como software en servidores estándar (ETSI, MEC security Status of standards support, 2022). Complementando esto, las **Redes Definidas por Software (SDN)** desacoplan el plano de control (inteligencia de la red) del plano de datos (transmisión de tráfico), permitiendo una gestión centralizada y programable de la red, lo que facilita la automatización y la optimización del rendimiento (3GPP, 3GPP TS 23.501: System Architecture for the 5G System (5GS), 2018).

En la siguiente tabla encontraremos una comparación entre las redes 4G y las 5G donde se evidencian las formas diferentes en las que ha evolucionado esta red, como su arquitectura, identidad de usuario y sus ataques más comunes

Tabla 1

Comparación de la seguridad entre las redes 4G y 5G

Redes	**Arquitectura**	Identidad Usuario	Ataques más comunes
4G	La arquitectura está basada en hardware, con una red centralizada conocida Envolved Packet Core (EPC). Esta estructura se basa en equipos físicos que realizan funciones de control y procesamiento de datos	La identidad del usuario IMSI (Internacional Mobile Subscriber Identity), se transmite en texto plano al inicio de la conexión. Este proceso es vulnerable a un ataque, donde un atacante puede interceptar esta identidad para rastrear la ubicación del usuario	Los ataques más comunes en 4G se centran en la intercepción de la comunicación, como los ataques de intermediario y los ataques de degradación, que obligan al dispositivo a conectarse a redes menos seguras para poder espiar la comunicación. El rastreo de la ubicación a través del IMSI era un riesgo conocido
5G	Su arquitectura se basa en software, lo	La identidad del usuario introduce	Dentro de

Redes	**Arquitectura**	Identidad Usuario	Ataques más comunes
	que se conoce como redes virtualizadas y definidas por software. Esto permite una arquitectura modular y descentralizada por software	una mejora de seguridad significativa al remplazar el IMSI por el SUCI (Subscription Concealed Identifier). El SUCI se cifra utilizando una clave publica antes de ser enviado, lo que protege la identidad del suscriptor desde el inicio y dificulta enormemente el rastreo por parte de otros	los ataques más comunes están atacar a los servidores de la red central, infectar equipos tecnológicos con baja seguridad para obtener datos a gran escala, interconexión con otras redes y objetivos de transmisión de datos con posibles robos de datos

*(*Subscriber Identity), se transmite en texto plano al inicio de la conexión. Este proceso es vulnerable a un

(3GPP, *5G Security Architecture and Procedures*, 2020) *(*ENISA, *ENISA Threat Landscape for 5G Networks*, 2020) (Kaspersky, 2025)

Además de estos componentes fundamentales, 5G introdujo conceptos transformadores como el **edge Computing** y el **Network Slicing**. El edge computing traslado la capacidad de procesamiento y almacenamiento de datos desde la nube centralizada hacia el "borde" de la red, más cerca de donde se generaron los datos (por ejemplo, en las estaciones base 5G). Esto es crucial para reducir aún más la latencia en aplicaciones críticas y para procesar grandes volúmenes de datos localmente, optimizando la eficiencia (Group, 2022).

Por su parte, el Network Slicing permitió a los operadores crear múltiples redes lógicas virtuales e independientes sobre una única infraestructura física 5G. Cada "slice"

puede ser optimizada y personalizada para cumplir con los requisitos específicos de diferentes servicios o clientes, como, por ejemplo, una slice dedicada a vehículos autónomos con ultra baja latencia, o una slice para loT masivo con alta densidad de conexiones (Ericsson, Network Slicing: Building the 5G Enterprise, 2021). Estas innovaciones proporcionaron una **ventaja técnica** sustancial sobre 4G en términos de flexibilidad y capacidad de adaptación a diversos casos de uso, pero también introdujeron **desafíos técnicos** complejos, particularmente en la gestión de la seguridad, la orquestación de servicios y la interoperabilidad entre las múltiples capas y slices de la red.

Estas innovaciones no solo representaron un salto tecnológico respecto a generaciones anteriores, sino que también redefinieron la manera en que se conciben y gestionan las redes móviles. El **edge computing**, al acercar el procesamiento a los dispositivos finales, no solo mejora la latencia, sino que también plantea nuevas oportunidades para servicios sensibles al tiempo, como pagos digitales en tiempo real o aplicaciones de salud remota. Sin embargo, esta descentralización también implico que los puntos de procesamiento se multiplicaran, lo que puedo aumentar la complejidad en la protección de datos y en la detección de amenazas.

Por otro lado, el network slicing ofrece una flexibilidad sin precedentes, permitiendo adaptar la red a las necesidades específicas de cada servicio. Esto es especialmente valioso en sectores como el financiero, donde se lograron crear slices con altos estándares de seguridad para proteger transacciones digitales. No obstante, esta segmentación también exige una gestión rigurosa de los límites entre slices, ya que una mala configuración o una brecha en un slice podría comprometer la integridad de toda la red. Por tanto, aunque estas tecnologías abren la puerta a una era de conectividad personalizada, también requieren un enfoque más sofisticado y dinámico en materia de ciberseguridad.

La arquitectura del 5G, con su énfasis en la flexibilidad y el software, introdujo un conjunto de vulnerabilidades que difieren en naturaleza y escala de las encontradas en

generaciones de red anteriores. Entender estos puntos débiles es crucial para desarrollar estrategias de seguridad robustas.

La adopción masiva de la virtualización de funciones de red y las redes definidas por software en el núcleo 5G y, cada vez más, en la RAN, introduce una capa de abstracción y programabilidad que, si bien optimiza la operación, también genero nuevos vectores de ataque. Los riesgos por software mal configurado o comprometido son significativos, ya que un fallo en la configuración de una función de red virtualizada podrirá exponer datos o permitir el acceso no autorizado a componentes críticos (Mishra, 5G Security Challenges & Solutions: A Comprehensive, 2024). Un ataque a hipervisores y controladores SDN es particularmente devastador. El hipervisor, que gestiona múltiples máquinas virtuales en un mismo hardware, se convierte en un punto único de fallo; un compromiso de este podría permitir a un atacante acceder a todos los VNFs que aloja (Hu, 2020). De manera similar, los controladores SDN, al centralizar la lógica de control de la red, son objetivos de alto valor: un ataque exitoso podría permitir a los adversarios manipular el tráfico, desviar datos o denegar servicios a gran escala (ONF, 2015). Finalmente, el acceso no autorizado a funciones virtualizadas a través de APIs expuestas o credenciales débiles podría a las atacantes modificar la configuración de la red, inyectar malware o lanzar ataques Man in the Middle.

El edge computing acerco el procesamiento de datos y la capacidad de cómputo al borde de la red, reduciendo la latencia y facilitando aplicaciones de tiempo real. Sin embargo, esta distribución tiene implicaciones de seguridad considerables. Al procesar datos en el borde de la red, se genera menos control centralizado y una mayor cantidad de puntos de exposición físicos y lógicos. Los nodos de edge pueden estar en ubicaciones menos seguras físicamente que un centro de datos tradicional, aumentando el riesgo de manipulación de datos en nodos locales a través de accesos físicos no autorizados o ataques

de software específicos contra estos entornos distribuidos y a menudo con recursos limitados (Shi, 2016). Además, la dificultad para aplicar políticas de seguridad uniformes en una infraestructura tan distribuida y heterogénea es un desafío crítico. Cada nodo edge podría tener diferentes versiones de software, configuraciones o parches, creando inconsistencias que los atacantes pueden explotar para eludir las defensas de seguridad generales.

El network slicing es una característica definitoria del 5G que permite la creación de múltiples redes lógicas (slices) sobre una infraestructura física compartida, cada una optimizada para un caso de uso específico (ej. loT masivo, comunicaciones de misión crítica). No obstante, esta compartimentación introdujo desafíos de seguridad únicos. El principal riesgo es que cada "slice" puede tener diferentes niveles de seguridad basados en sus requisitos de servicio. Por ejemplo, una slice para loT de baja seguridad podría tener menos protecciones que una para servicios bancarios. Un ataque a un slice puede escalar a otros si no hay un aislamiento adecuado entre ellos, lo que se conoce como "slice hopping". Si un atacante logra comprometer una slice de menor seguridad, podría potencialmente usar esa brecha para moverse lateralmente a una slice más crítica si la virtualización o la orquestación del slice no garantiza una separación estricta y segura (Taloba, 2021). Esto representa un riesgo significativo de propagación de ataques y de acceso no autorizado a datos o servicios sensibles.

La promesa del 5G de conectar miles de millones de dispositivos loT es un arma de doble filo para la seguridad. Un gran número de estos dispositivos son inherentemente inseguros: muchos dispositivos no tienen protocolos de seguridad robustos debido a limitaciones de hardware, costo o ciclo de vida de desarrollo. Carecen de capacidades de cómputo para cifrado avanzado, no reciben actualizaciones de seguridad regulares y a menudo vienen con contraseñas predeterminadas o configuraciones débiles (ENISA, Baseline Security Recommendations for IoT in the context of Critical Information

Infrastructures, 2017). Esto los convierte en blancos fáciles para ser comprometidos y utilizados en ataques DDoS desde dispositivos comprometidos. Ejemplos históricos como Mirai (que usó cámaras IP y DVRs) muestran el potencial devastador de estas redes de dispositivos zombis para paralizar servicios esenciales (Kolias, 2017). El riesgo en dispositivos de pago como datafonos, relojes inteligentes o wearables habilitados para transacciones es particularmente alto, ya que su compromiso podría llevar directamente al robo de credenciales financieras, fraude transaccional o espionaje de hábitos de consumo (Futuras Amenazas Cibernéticas, 2021).

A pesar de las mejoras en el cifrado de 5G en comparación con 4G, la intercepción y manipulación de datos sigue siendo una preocupación primordial. Los ataques tipo “man in the Middle” continúan siendo una amenaza persistente, donde los atacantes se posicionan entre dos partes que se comunican para interceptar o alterar la información sin que ninguna de las partes lo sepa (Singh, 2020). Aunque 5G introduce una autenticación de vulnerabilidades en la implementación pueden abrir la puerta a este tipo de ataques, especialmente en la capa de acceso radio o en la interconexión con redes legadas. Las vulnerabilidades en el plano de controlo del 5GC son especialmente criticas; si los atacantes logran comprometer las funciones que gestionan la señalización y la configuración de la red, podrían redirigir el tráfico, inyectar comandos maliciosos o manipular los datos de facturación y ubicación, afectando directamente la confidencialidad y la integridad de las comunicaciones y transacciones financieras (Huawei, 2021).

El avance de las redes 5G en Colombia y la expansión de los pagos digitales se insertaron en un contexto nacional particular, que presenta tanto oportunidades como desafíos inherentes a la seguridad.

El estado actual del despliegue 5G en Colombia vio avances significativos tras la subasta del espectro a finales de 2023. Operadores como Claro, Tigo-Une, Movistar y WOM

iniciaron el despliegue de sus redes, con ciudades piloto como Bogotá, Medellín, Cali y barranquilla siendo las primeras en experimentar la cobertura. Si bien la cobertura inicial se concentró en zonas urbanas densamente pobladas, se espera una expansión progresiva en los próximos años, lo que permitirá la masificación de servicios avanzados (Santa, 2024). Este despliegue es fundamental para la modernización de la infraestructura digital del país.

En el siguiente grafico se evidenciará una representación clara de cómo en Colombia siguen los avances en cada una de las empresas que ofrecen servicios de internet además de que ya están llegando a muchas más partes del país incluyendo las primeras ciudades piloto, estoy muy importante para el desarrollo del país a nivel tecnológico

Figura 1
Cobertura de redes 5G en Colombia

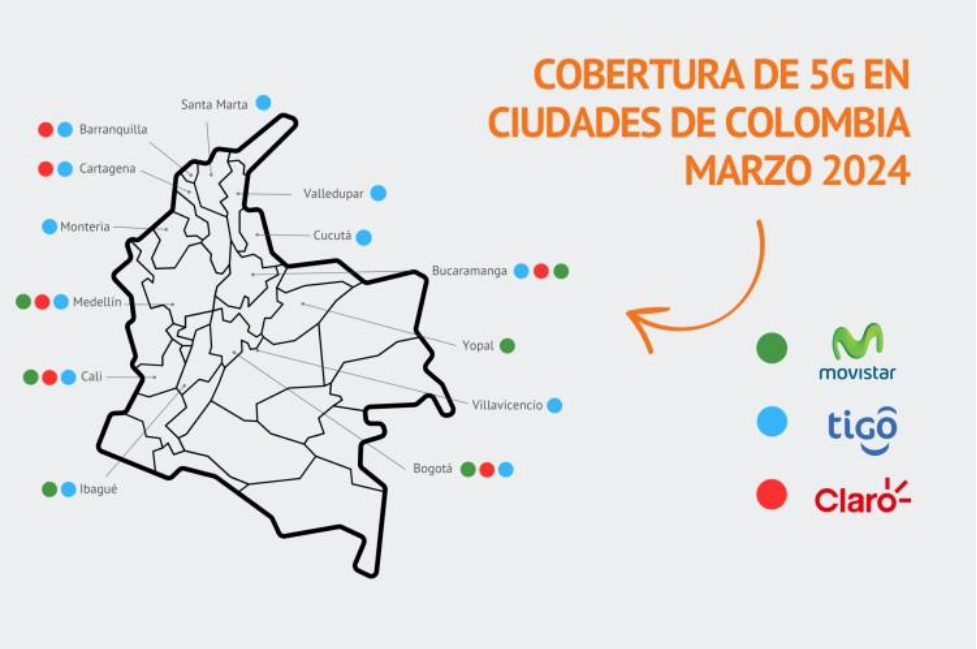


Gráfico: Dayanne González, *vía La República* Publicado: jueves 21 de marzo de 2024 (https://dfsud.com/dfsud/site/artic/20240320/pags/20240320160958.html)

Paralelamente, Colombia ha experimentado una explosión en la adopción de plataformas de pago digital, que se han convertido en herramientas esenciales para la

inclusión financiera y la economía diaria. Las más utilizadas incluyen billeteras móviles como Nequi (filial de Bancolombia) y Daviplata (de Davivienda), que permiten transacciones P2P, pagos de servicios y compras en comercios. Además, plataformas como PS (Pagos Seguros en Línea), que facilita débitos directos desde cuentas bancarias, otras billeteras móviles y soluciones de pago sin contacto han transformado el panorama transaccional (González, 2025).

No obstante, este dinamismo digital se enfrenta a riesgos específicos en Colombia. La infraestructura tecnología del país, aunque en desarrollo, aún presenta brechas en términos de madurez y resiliencia. La disparidad regional en la conectividad, la falta de inversión en ciberseguridad en ciertos sectores y la escasez de talento especializado pueden crear puntos débiles que los ciberdelincuentes pueden explotar (BID, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, 2016). Un factor crítico es el bajo nivel de ciberhigiene en los usuarios. La falta de conocimiento sobre amenazas comunes como el phishing, el uso de contraseñas débiles o la descarga de aplicaciones maliciosas, convierte a los usuarios en el eslabón más vulnerable de la cadena de seguridad, especialmente en un contexto de rápida adopción de nuevas tecnologías (DIGITAL, 2023). Esto se refleja en los casos de ataques recientes a entidades financieras y a los usuarios de plataformas de pago digital, donde los fraudes por suplantación de identidad, smishing y phishing son recurrentes, afectando la confianza en el sistema (Bermudez, 2023).

Las vulnerabilidades inherentes a la arquitectura 5G, combinadas con el contexto de ciberseguridad colombiano, tuvieron un impacto directo y significativo en la seguridad de los pagos digitales.

Las vulnerabilidades del 5G pueden afectar las transacciones móviles de diversas maneras. Por ejemplo, un ataque exitoso a una slice de red dedicada a servicios financieros podría comprometer la disponibilidad del servicio de pago, impidiendo que los usuarios

realicen transacciones. Un compromiso en la capa de edge computing podría permitir la manipulación de datos transaccionales antes de que lleguen a los sistemas centrales, alterando montos o beneficiarios. Además, la masiva interconexión de dispositivos loT en 5G, incluyendo wearables y otros dispositivos de pago comprometido se conecta a la red 5G, podría ser utilizado como un punto de entrada para el robo de información o la inyección de malware (ENISA, ENISA Threat Landscape for 5G Networks, 2020).

La autenticación biométrica, cada vez más utilizada en pagos digitales (ej., reconocimiento facial o huella dactilar en smartphones), también se vio expuesta a riesgos en el entorno 5G. Si bien la biométrica ofrece conveniencia, las vulnerabilidades en la red (como ataques MitM o manipulación del plano de control) podrían, en teoría, interceptar o alterar los datos biométricos en tránsito o incluso los tokens de autenticación derivados de ellos, comprometiendo la integridad del proceso de verificación de identidad (Huawei, 2021). Esto podría llevar a riesgos de suplantación de identidad, donde un atacante se hace pasar por el usuario legitimo para realizar transacciones fraudulentas.

La integridad de datos financieros es otro punto crítico. Las vulnerabilidades en virtualización y SDN, si son explotadas, podrían permitir a los atacantes acceder a funciones de red que gestionan el tráfico de pagos, lo que podría resultar en la manipulación de pago (alteración de montos o destinatarios) o el robo de credenciales y tokens de transacción. Los ataques a dispositivos loT de pago (como datafonos conectados a 5G en comercios) pueden facilitar el skimming digital o la interceptación de datos de tarjetas en el punto de venta. En última instancia, la combinación de una infraestructura 5G en desarrollo con un bajo nivel de ciberhigiene en los usuarios colombianos crea un caldo de cultivo para que los riesgos de suplantación, robo de credenciales y manipulación de pagos se materialicen con mayor facilidad, requiriendo un enfoque de ciberseguridad adaptativa y una fuerte educación digital para mitigar estas amenazas.

En este capítulo se han establecido las bases teóricas de las redes 5G, la virtualización de funciones de red y las redes definidas por software. Estos conceptos, que convierten el hardware en software y centralizan el control de la red, son fundamentales para comprender el entorno técnico en el que operan los pagos digitales. Al definir estos pilares hemos logrado dar el primer paso para cumplir el objetivo 1, que buscar analizar las vulnerabilidades de seguridad inherentes a estas arquitecturas.

Nivel de exposición a ciberataques en las plataformas de pagos digitales

Colombia ha experimentado una transformación digital acelerada, particularmente impulsada por la pandemia de COVID-19, que catapulto el crecimiento de los pagos digitales. La necesidad de transacciones sin contacto y la búsqueda de mayor eficiencia llevaron a un aumento masivo en el uso de plataformas como Nequi, Daviplata, PSE, y diversas billeteras móviles y aplicaciones bancarias (Asobancaria, Superintendecia Financiera de Colombia, 2023). Estas herramientas se han consolidado como pilares de la inclusión y modernización financiera, facilitando desde pequeños pagos persona a persona hasta compras en comercios y el acceso a servicios bancarios desde dispositivos móviles, lo que reconfiguro los hábitos de consumo y las operaciones económicas en el país (Fintech, 2024).

Paralelamente a esta evolución financiera, el despliegue del 5G en Colombia está tomando forma a pasos agigantados. Tras la Resolución 3947 de 2023 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que sentó las bases para la licitación del espectro, la subasta de 2024 asigno bloques a los principales operadores (MinTIC, 2023). Como resultado, operadores como Claro, Tigo, y Movistar están liderando la cobertura, concentrándose inicialmente en las grandes urbes. Reportes recientes indican que hay más de 1.100 estaciones base activas en al menos 22 ciudades del país, marcando un hito en la infraestructura de conectividad nacional y prometiendo transformar múltiples

sectores, incluyendo el financiero y de servicios (Economia, 2024).

La introducción de la tecnología 5G modifico fundamentalmente el panorama de ciberseguridad para los pagos digitales, alterando la naturaleza de los riesgos y las estrategias de defensa necesarias.

Primero la mayor velocidad y menor latencia del 5G implican la capacidad de procesar más transacciones menos tiempo. Si bien esto mejoro la eficiencia operativa y la experiencia del usuario, también significo que los atacantes pueden ejecutar y propagar activades maliciosas (como fraudes o exfiltración de datos) a una velocidad mucho mayor, reduciendo las ventanas de tiempo para la detección y respuesta (ITU, 2020). Un ataque automatizado que antes tardaría minutos en afectar a miles de usuarios podría ocurrir en segundos en un entorno 5G, intensificando la presión sobre los sistemas de detección de anomalías y prevención de fraude.

Segundo, la mayor densidad de dispositivos conectados, facilitada por el 5G (particularmente en el ámbito del internet de las cosas, loT) se traduce en más puntos de entrada para los atacantes. Cada dispositivo loT, desde sensores industriales hasta wearables habilitados para pagos, representa un potencial vector de ataque (ENISA, 2017). Si estos dispositivos carecen de medidas de seguridad robustas, pueden ser fácilmente comprometidos para formar parte de botnets masivas, capaces de lanzar ataques de denegación de servicio distribuido (DDoS) que podrían paralizar infraestructuras críticas de pagos o actuar como pivotes para acceder a redes más sensibles, comprometiendo datos financieros o interrumpiendo servicios.

Tercero, la adopción del edge Computing y la virtualización condujo a una descentralización del procesamiento, lo que complica la protección de datos. Al mover el procesamiento de datos más cerca del usuario final o del dispositivo loT, se dispersaron los puntos de control y se introdujeron nuevos nodos que deben ser asegurados. Esto represento

un desafío para aplicar políticas de seguridad uniformes y monitorear la integridad de los datos en toda la red, especialmente cuando la información financiera sensible se procesa en estos entornos distribuidos. Los atacantes podrían apuntar a estos nodos de borde, que a menudo tienen menos recursos de seguridad que los centros de datos centrales, para manipular transacciones o interceptar datos antes de que sean cifrados por completo.

Finalmente, el Network Slicing, una característica distintiva del 5G, introduce un nuevo paradigma de riesgo. Aunque cada "slice" es una red lógica aislada, diseñada con requisitos de servicio específicos, un ataque en un slice puede afectar a otros si no hay un aislamiento adecuado (Taloba, 2021). Si un atacante compromete un slice de menor seguridad (por ejemplo, para loT básico), podría buscar la forma de saltar a un slice de mayor seguridad, como uno dedicado a servicios financieros o de pagos. Este riesgo de "salto de slice" o de "escape" entre entornos virtuales, si no se gestiona con arquitecturas de seguridad de confianza cero y segmentación estricta, podría permitir a los ciberdelincuentes acceder a datos financieros críticos o manipular transacciones que operan en diferentes segmentos de la misma infraestructura física 5G.

En la siguiente tabla como las redes 5G tienen nuevas vulnerabilidades y el impacto que tienen integridad, confidencialidad y disponibilidad dentro de los usuarios

Tabla 2

Vulnerabilidades del 5G y su impacto en la confidencialidad, integridad y disponibilidad

Vulnerabilidades	**Network Slicing**	**Virtualización y SDN/NFV**	**Expansión de la superficie de ataque**	**Ataque de Denegación de servicios (DDoS)**	**Robo de credenciales**	**Puntos de entrada**	**Creación de Botnets**
Definición	Una vulnerabilidad en un segmento (slice) de red bajo nivel podría permitir a	Una configuración errónea o un fallo de codificación en el software	La interconexión masiva de dispositivos, la compatibilidad con	Un atacante puede aprovechar la baja latencia y la capacidad de	Los atacantes pueden explotar vulnerabilidades en dispositivos o software	Un dispositivo loT con una contraseña débil o un firmware desactual	Los dispositivos loT comprometidos son usados por los ciberdelincuentes para

Vulnerabilidades	Network Slicing	Virtualización y SDN/NFV	Expansión de la superficie de ataque	Ataque de Denegación de servicios (DDoS)	Robo de credenciales	Puntos de entrada	Creación de Botnets
	un atacante moverse lateralmente para comprender un segmento más crítico, como el dedicado a transacciones financieras, afectando la confidencialidad y la integridad de los datos totales del servicio. Esto afecta la disponibilidad y genera desconfianza en los usuarios	que maneja las funciones de red (NFV) podría ser explotado para la interrupción de servicio, afectando directamente la disponibilidad de la red	diferentes tecnologías y la conexión con redes de terceros incrementan el riesgo de una brecha de seguridad	conectar miles de dispositivos para orquestar un ataque DDoS a gran escala, sobrecargando los servidores de un banco o una plataforma de pago y provocando la interrupción	para interceptar comunicaciones, robar credencias les de acceso, numero de tarjeta de crédito y otra información personal, comprometido la confidencialidad de los datos del usuario	izado puede ser fácilmente compro metido. Una vez dentro, el atacante usa este dispositivo como puente para acceder a la red domestica o empresarial, buscando la forma de llegar a los dispositivos que manejan información financiera	construir redes masivas de dispositivos botnets. Estas botnets son la herramienta principal para lanzar ataques DDoS masivos contra bancos, plataformas de comercio electrónico y otras infraestructuras críticas que gestionan los pagos digitales.

(Teldat, 2024) (Tecnologías, 2024) (Topaz, 2025)

La intercepción de datos, siguen siendo una amenaza fundamental en al ámbito de los pagos digitales, y las redes 5G, a pesar de sus mejoras de seguridad, no son inmunes. Los ataques tipo Man in the Middle (MitM) en redes públicas Wi-Fi, o incluso en configuraciones 5G mal aseguradas, permiten a un atacante situarse entre el dispositivo del usuario y el servidor de pago para capturar o modificar el tráfico sin ser detectado (Fang et al., 2017). El riesgo es aún mayor en aplicaciones de pago que no implementan un cifrado de extremo a extremo (E2EE) robusto, dejando la información financiera vulnerable durante su

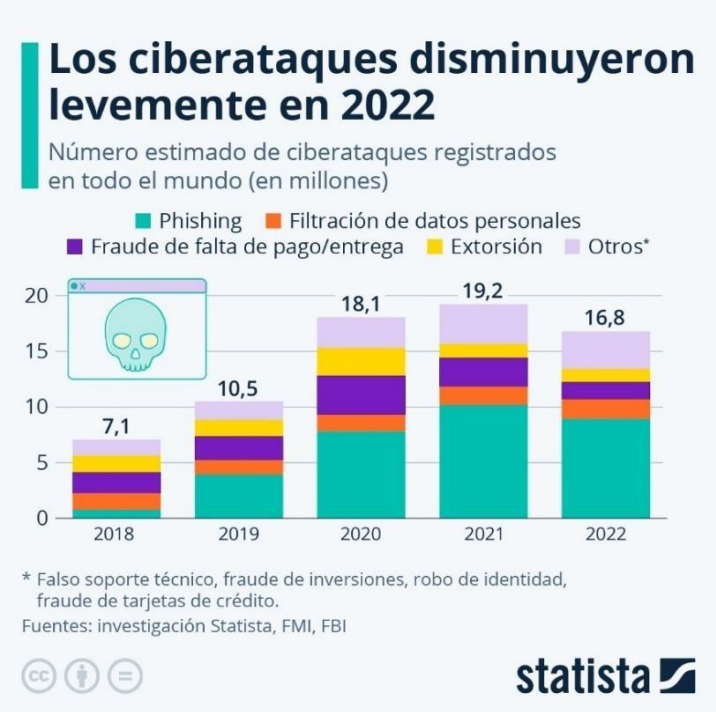
tránsito. Esto es especialmente preocupante en entornos donde las slices de red pueden tener diferentes niveles de seguridad o donde la virtualización introduce puntos de control menos centralizados, facilitando que un atacante establezca un punto de control menos centralizados, facilitando que un atacante establezca un punto de intercepción antes o después de las capas de seguridad de la aplicación (Mishra & Rathore, 5G Security Challenges & Solutions: A Comprehensive Survey, 2024).

Los ataques de suplantación de identidad se vuelven más sofisticados y efectivos gracias a la velocidad y la capacidad del 5G. El phishing y el smishing (phishing por SMS) pueden ser orquestados a una escala y con una rapidez sin precedentes, distribuyendo enlaces maliciosos o mensajes engañosos a un vasto número de usuarios en cuestión de segundos (Sahni, 2022) Esto facilita el robo de credenciales bancarias y tokens de autenticación, ya que la alta velocidad del 5G permite que los sitios web falsos carguen instantáneamente y que las redirecciones sean imperceptibles para el usuario común. Además, la proliferación de dispositivos loT conectados a 5G puede ser utilizada para campañas de phishing dirigidas, donde los mensajes maliciosos se entregan a través de canales menos esperados, aumentado la credibilidad del engaño y la vulnerabilidad del usuario (J. P. Mohan, 2022).

En la siguiente imagen se encuentra una relación entre los ciberataques más comunes y el aumento desde el 2018 hasta el 2022 de esta manera encontramos los ataques más comunes y su porcentaje con otros años

Figura 2

Ciber ataques más comunes y su estadística por años



María Florencia Melo,11 mayo 2023 (https://es.statista.com/grafico/29964/ciberataques-registrados-en-todo-el-mundo/)

El enorme volumen de dispositivos loT conectados a las redes 5G representa una vasta y a menudo vulnerable superficie de ataque para los pagos digitales. Dispositivos como datafonos, relojes inteligentes, asistente de voz o wearables, que ahora pueden facilitar transacciones, son blancos atractivos. Muchos de estos dispositivos tienen limitaciones de hardware y software que impiden la implementación de protocolos de seguridad robustos, no reciben actualizaciones de seguridad regulares, o son configurados con credenciales predeterminadas (Y. Yang, 2017). Esto los hace susceptibles a ser comprometidos, lo que puede llevar al robo directo de datos de pago almacenados en el dispositivo, a la intercepción de transacciones o a su uso como punto de pivote para acceder a la red del usuario o de la institución financiera (Asim, Khan, & Tariq, 2021). Un dispositivo loT comprometido en la red 5G podría convertirse en una puerta trasera silenciosa para el fraude.

La velocidad y el ancho de banda del 5G facilitan la propagación y el funcionamiento del malware financiero. Los troyanos bancarios que infectan dispositivos móviles o computadoras pueden comunicarse con servidores de comando y control de manera más rápida y sigilosa, exfiltrando datos sensibles o automatizando transacciones fraudulentas sin despertar sospechas (H. Rõigas, 2017). Un riesgo creciente son las aplicaciones falsas que simulan ser plataformas de pago legitimas. Los atacantes pueden diseñarlas para que se vean idénticas a las aplicaciones reales, utilizando la capacidad de las redes 5G para descargar rápidamente estos malware a los dispositivos de los usuarios. Una vez instaladas, estas apps falsas pueden robar credenciales, interceptar códigos de autenticación de dos factores o incluso iniciar transacciones sin el consentimiento del usuario (SAFA J. ALTAHA, 2024).

Los ataques de denegación de servicio distribuido (DDoS) se vuelven más potentes y difíciles de mitigar en el entorno 5G debido a su inmensa capacidad de ancho de banda y la alta densidad de dispositivos conectados. Los atacantes pueden aprovechar botnets compuestas por miles o millones de dispositivos loT comprometidos (muchos de ellos inyectados a través de vulnerabilidades en la red 5G), para generar un volumen masivo de tráfico malicioso (Sangwan, 2022). Esta capacidad permite lanzar ataques DDoS de tal magnitud que pueden sobrecargar incluso la infraestructura robusta de plataformas de pago o bancos, interrumpiendo servicios esenciales. La baja latencia del 5G también podría permitir un control más preciso y coordinado de estas botnets, haciendo que los ataques sean más adaptativos y persistentes, afectando gravemente la disponibilidad de los servicios financieros digitales y la confianza del usuario (Cherry Manglaa, 2022).

Evaluar el nivel de exposición de los pagos digitales en el entorno 5G colombiano implico analizar los factores que aumentan el riesgo frente a aquellos que lo mitigan. Este balance fue crucial para comprender la vulnerabilidad general del sistema.

Factores que aumentan la exposición

Varis elementos contribuyen a un mayor nivel de exposición en el panorama de pagos digitales sobre 5G en Colombia. Uno de los más significativos es la baja cultura de ciberseguridad en los usuarios. A pesar del auge de las herramientas digitales, muchos usuarios carecen del conocimiento básico para identificar amenazas como el phishing, el smishing o las aplicaciones falsas, lo que los convierte en el eslabón más débil de la cadena de seguridad (Hassan & Shukur, 2023). Esta falta de conciencia facilita la ingeniería social y el robo de credenciales. Otro factor crítico es la falta de actualizaciones en dispositivos móviles. Un porcentaje significativo de usuarios no mantiene sus sistemas operativos y aplicaciones de pago actualizados, dejando sus dispositivos vulnerables a exploits conocidos que podrían ser utilizados para instalar malware financiero o acceder a información sensible (Archibong et al., 2024). Finalmente, el uso de redes Wi-Fi públicas para transacciones financieras amplifica el riesgo. Estas redes, a menudo sin cifrado adecuado o con configuraciones de seguridad débiles, son caldo de cultivo para ataques Man in the Middle y la intercepción de datos, comprometiendo la confidencialidad de las transacciones de pagos digitales (Marat, 2023).

Factores que mitigan la exposición

Afortunadamente, existen factores y tecnologías que ayuda a mitigar la exposición, fortaleciendo la seguridad de los pagos digitales sobre 5G. La implementación generalizada de la autenticación multifactor es una defensa poderosa. Al requerir dos o más formas de verificación de identidad (como una contraseña y un código enviado al teléfono), MFA reduce drásticamente probabilidad de acceso no autorizados, incluso si las credenciales primarias son robadas (Archibong, Stephen, & Asuquo, 2024). Un atacante necesario no solo la contraseña, sino también acceso físico o lógico al segundo factor de autenticación, lo que eleva considerablemente la barrera de entrada. El cifrado de datos robusto es otro pilar

fundamental. El cifrado de extremo a extremo, aplicando tanto a los datos en tránsito (por ejemplo, mediante TLS en aplicaciones de pago) como a los datos almacenados en dispositivos o servidores, asegura que la información sensible permanezca ilegible para atacantes, incluso si logran interceptarla o acceder a los sistemas (Kasiyanto, 2016). Por último, el monitoreo en tiempo real por parte de bancos y Fintech juega un rol crucial. Estas instituciones invierten en sistemas avanzados de detección de fraudes que utilizan inteligencia artificial y análisis de comportamiento para identificar patrones sospechosos de transacciones o accesos. La capacidad de detectar anomalías y bloquear transacciones fraudulentas de forma casi instantánea es vital para contener el daño de un ciberataque, aprovechando la velocidad y capacidad de análisis que las redes 5G pueden facilitar para procesar grandes volúmenes de datos transaccionales (Borketey, 2024).

Este capítulo ha profundizado en las vulnerabilidades específicas de las redes 5G, incluyendo fallos en la autenticación, la arquitectura Edge Computing y los desafíos del Networ Slicing. Al identificar y explicar cómo estas vulnerabilidades pueden ser explotadas, se ha logrado el objetivo 2, que consiste en evaluar el impacto de estas amenazas en la privacidad y seguridad de los datos de los usuarios, especialmente en el contexto de los servicios financieros.

Estándares de seguridad actuales con los riesgos identificados

La seguridad en el ecosistema 5G de pagos digitales se sustenta en una combinación de estándares internacionales y normativas nacionales, que buscan establecer un marco de protección robusto.

Los estándares internacionales proporcionan un lenguaje y mejores prácticas para gestionar la seguridad de la información. La norma ISO/IEC 27001 es un sistema de gestión de la seguridad de la información (SGSI) reconocido globalmente que establece los requisitos para implementar, establecer, mantener y mejorar continuamente un sistema de gestión de

riesgos de seguridad. Es fundamental para organizaciones que manejan datos sensibles, incluyendo las del sector financiero y las operadoras de redes 5G (ISO, 2022). El NIST Cybersecurity Framework ofrece un enfoque flexible y basado en el riesgo para gestionar y reducir los riesgos de ciberseguridad. Sus cinco funciones clave (identificar, proteger, detectar, responder recuperar) proporcionan una hoja de ruta para la mejora continua de la ciberseguridad, siendo adaptable a la complejidad de las redes 5G y los sistemas de pago (NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2018).

Para la seguridad de las transacciones con tarjera, el PCI DSS (Payment Card Industry Data Security estándar) es un conjunto de requisitos de seguridad diseñado para garantizar que todas las empresas que procesan almacenan o transmiten información diseñado para garantizar que todas las empresas que procesan almacenan o transmiten información de tarjetas de crédito mantengan un entorno seguro. Es crucial para las plataformas de pago digital y las entidades financieras (SSC, 2022). En el ámbito especifico 5G, el estándar 3GPP TS 33.501 es vital; esta especificación técnica define la arquitectura y los procedimientos de seguridad para el Sistema 5G, cubriendo aspectos como la autenticación, la privacidad de la identidad del suscriptor y la seguridad de la señalización, siendo la referencia técnica principal para los fabricantes de equipos y operadores (3GPP, Specification # 33.501, 2018). Finalmente, el concepto de Zero Trust Architecture (ZTA), aunque no es un estándar normativo, es un modelo estratégico de ciberseguridad que asume que ninguna entidad (usuario, dispositivos, red) debe ser inherente confiable. Requiere una verificación estricta de cada solicitud de acceso, sin importar su origen, lo que es esencial para entornos dinámicos y distribuidos como 5G y edge computing (Rose, Borchert, Mitchell, & Connelly, 2020).

A nivel nacional, Colombia ha avanzado en la construcción de un marco regulatorio para la protección de datos y la ciberseguridad. La ley 1581 de 2012 es la ley general de protección de datos personales, que establece los principios y disposiciones de los titulares de

la información fundamental para la operación segura de los pagos digitales (SIC, Informe sobre Protección de Datos Personales en el Sector Financiero, 2023). La ley 1273 de 2009 tipifica los delitos informáticos, creando un marco penal para sancionar conductas como el acceso abusivo a sistemas informáticos, la interceptación de datos, el daño informático y el fraude por medios electrónicos, ofreciendo herramientas legales contra los ciberataques (Publica, 2009).

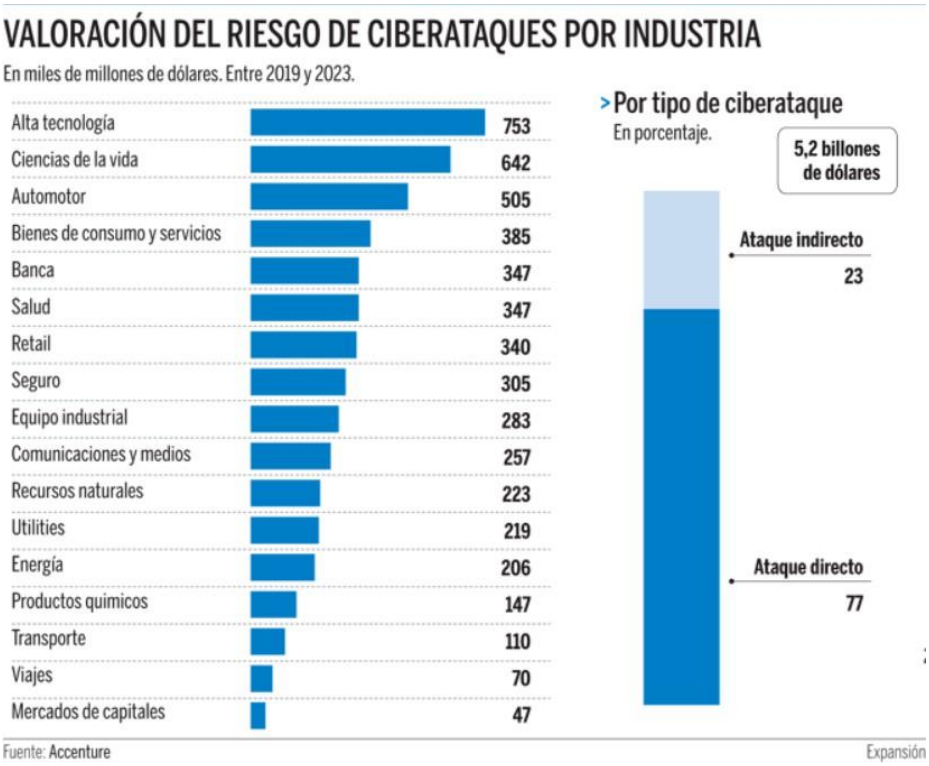
Más recientemente, el decreto 338 de 2022 complementa este marco al fortalecer la gobernanza de la seguridad digital a nivel nacional, estableciendo lineamiento para la gestión de riesgos, la protección de la infraestructura crítica y la promoción de una cultura de ciberseguridad en entidades públicas y privadas. En el sector financiero, el Sistema BRE- (Banca de la república – Ecosistema de pagos de bajo valor) es una iniciativa clave que busca garantizar la interoperabilidad, la seguridad y la eficiencia en los pagos digitales en Colombia, estableciendo reglas claras para los participantes y fomentado la innovación controlada en este ámbito (Özyilmaz, 2025). Estas normativas e iniciativas son cruciales para el desarrollo de un ecosistema de pagos digitales seguro sobre la infraestructura 5G.

La integración de las redes 5G con los sistemas de pagos digitales introdujeron y amplificaron una serie de riesgos de ciberseguridad, muchos de los cuales derivan de las características arquitectónicas del 5G de la superficie de ataque extendida.

En la siguiente grafica se encuentra los datos de los sectores más afectados por ataques cibernéticos lo cual nos da una idea los puntos débiles que tiene el sector financiero y en donde se debe dar prioridad y más atención para ayudar a mitigar este tipo de ataque

Figura 3

Amenazas de ciberseguridad que enfrenta el sector de servicios financieros



WordPress, *valoración del riesgo de ciberataques por industria*, octubre 29 2020 (https://blog.nivel4.com/noticias/amenazas-de-ciberseguridad-que-enfrenta-el-sector-de-servicios-financieros)

Los ataques a la virtualización representan una amenaza significativa, ya que la manipulación de funciones de red virtualizadas o los ataques a los controladores SDN pueden comprometer la integridad y disponibilidad de toda la red. Un compromiso en estas capas subyacentes podría permitir a los atacantes controlar el flujo de datos financieros, redirigir transacciones o interrumpir los servicios de pagos (Patel et al., 2021).

Las fallas en el aislamiento de slices de red son otro riesgo crítico. Si las participaciones lógicas del 5G no están adecuadamente separadas, un ataque exitoso en un slice de menor seguridad (por ejemplo, la utilizada por dispositivos loT básicos) podría escalar y afectar slices de alta seguridad que manejan pagos digitales, resultando en acceso no autorizados o interrupciones de servicios financieros críticos (Bhushan et al., 2023).

La intercepción de datos en edge computing es una preocupación creciente. Al acercar el procesamiento de datos al usuario ya los dispositivos loT, los nodos de edge se convierten en nuevos puntos de vulnerabilidad. Un atacante podría interceptar o manipular datos financieros sensibles antes de que sean completamente cifrados o procesados por la red central, especialmente si la seguridad física o lógica en estos nodos distribuidos es deficiente (Ahmad, y otros, 2018).

Los ataques a dispositivos loT conectados a plataformas de pago constituyen un vector de ataque masivo. Muchos de estos dispositivos (datafonos, wearables, etc.) carecen de medidas de seguridad robustas, lo que hace fáciles de comprometer, Una vez infectados, pueden ser utilizados para el robo directo de credenciales de pago, la inyección de programa maligno o como parte de botnets para ataques amplios (Sun:, Wan et al.,2024).

Además, el panorama de amenazas incluye el phishing y malware financiero más sofisticado. La velocidad y capacidad el 5G pueden facilitar la entrega y ejecución de campañas de phishing a gran escala o la rápida propagación de troyanos bancarios, haciendo que sean más difíciles de detectar y mitigar antes de que causen daños significativos. Finalmente, los ataques DDoS se vuelven más potentes por el ancho de banda del 5G. La capacitación de orquestar botnets masivas a través de dispositivos loT conectados a 5G permite lanzar ataques de denegación de servicio de una magnitud sin precedentes, capaces de paralizar la infraestructura de pagos digitales y afectar gravemente la disponibilidad de servicios esenciales (Valdovinos, Choo, Pérez, & Botero, 2021).

A pesar del marco normativo y la existencia de estándares internacionales, Colombia enfrenta varias brechas en la protección de sus redes 5G y sistemáticas de pago digitales que exacerban su vulnerabilidad.

Uno de los desafíos más significativos es la baja adopción de estándares internacionales como ISO/IEC 27001 o el NIST, particularmente en el PYMEs y Fintech

(Gordillo-Gaitán, 2024). Aunque las grandes instituciones financieras y operadores de telecomunicaciones pueden invertir en estas certificaciones, muchas empresas más pequeñas, que son cruciales para el ecosistema de pagos digitales, carecen de los recursos o el conocimiento para implementar y mantener estos estándares rigurosos. Esta disparidad crea puntos débiles en la cadena de suministro digital que los atacantes puedan explotar.

Relacionado con esto, la falta de auditorías obligatorias y regulares en muchas plataformas digitales agrava la situación. Si bien algunas normativas sectoriales exigen auditorias, no todas las plataformas que manejan datos financieros, especialmente las emergentes o aquellas con menor regulación, están sujetas a revisiones de seguridad periódicas y exhaustivas por parte de terceros independientes (Zuluaga & Moreno, 2024). Esto significa que las vulnerabilidades pueden persistir detectadas y corregidas, aumentando el riesgo de brechas de seguridad.

La desactualización tecnología en la infraestructura pública también representa un riesgo considerable. Aunque el despliegue del 5G avanza, existen sistemas legados y componentes de infraestructura crítica a nivel gubernamental o en servicios esenciales que no han sido modernizados a la misma velocidad. Estos sistemas antiguos pueden presentar vulnerabilidades conocidas que son fácilmente explotables, sirviendo como “puertas traseras” para ataques más amplios que podrían impactar indirectamente los servicios financieros (Cohen, Rojas, & Barrera, 2025).

Además, persiste una escasa cultura de ciberseguridad en usuarios y empleados. Mas allá de la falta de conocimiento básica sobre phishing en usuarios finales, muchos empleados de empresas que manejan información sensible no reciben captación adecuada y continua en ciberseguridad. Esto los hace susceptibles a ataques de ingeniería social o a cometer errores que exponen datos o sistemas (Almagro et al., 2020). Las políticas de “Bring Your Own Device” o en el teletrabajo sin medidas de seguridad estrictas pueden magnificar este riesgo.

Finalmente, la limitada interoperabilidad entre sistemas de seguridad en diferentes entidades y sectores dentro de Colombia obstaculiza una respuesta coordinada y efectiva ante ciberataques. A menudo, las agencias gubernamentales, el sector financiero y los operadores

de telecomunicaciones utilizan herramientas y plataformas de seguridad que no se comunican eficiente mente entre sí (ÁLZATE, 2024). Esta fragmentación puede retrasar la detección de amenazas, la comparación de inteligencia sore incidentes y la implementación de contramedidas a nivel nacional, dejando a Colombia más expuesta a ataques sofisticados y de gran escala.

A lo largo de este capítulo, se analizó el crecimiento del fraude digital en Colombia, presentando los riesgos de estas nuevas tecnologías. Hemos establecido una conexión directa entre las vulnerabilidades de la autenticación 5G-AKA y la facilidad con la que los delincuentes pueden suplantar la identidad de los usuarios para realizar ataques como el SIM swapping. Con esta conexión, se cumplió el objetivo 3, al examinar la relación entre las vulnerabilidades de la tecnología 5G y los ataques financieros que afectan a los usuarios

Conjunto de medidas técnicas y normativas adaptadas al ecosistema financiero colombiano

La necesidad de implementar medidas de ciberseguridad robustas y especificas en Colombia es más apremiante que nunca, impulsada por la confluencia de dos fenómenos tecnológicos transformadores: el auge de los pagos digitales y el despliegue de las redes 5G. El crecimiento exponencial de los pagos digitales ha sido una constante en el país, con plataformas como Nequi, Daviplata y PSE experimentando un uso desde la pandemia, convirtiéndose en herramientas esenciales para la vida cotidiana y la inclusión financiera (Asobancaria, Superintendecia Financiera de Colombia, 2023). Esta digitalización ha expuesto a millones de usuarios y transacciones a un entorno en línea que, por su propia

naturaleza, es vulnerable a ciberataques.

Simultáneamente, el despliegue del 5G en Colombia promete una mayor velocidad y conectividad, habilitando un sinfín de nuevas aplicaciones y mejorando la eficiencia de las transacciones digitales. Sin embargo, esta avanzada tecnología también introduce más vectores de ataque debido a su arquitectura basada en software, su alta densidad de dispositivos conectados y su naturaleza distribuida (Mishra, 5G Security Challenges & Solutions: A Comprehensive, 2024).

La combinación de estos factores ha resultado en riesgos identificados que van desde la suplantación de identidad (facilitada por phishing y smishing cada vez más sofisticados), el malware financiero (que puede propagarse más rápido en redes de alta velocidad), y los ataques a dispositivos loT (muchos de ellos con seguridad deficiente) hasta fallas en el aislamiento de slices de red que podrían permitir la propagación de ataques entre servicios críticos (PWC, 2024). Este escenario de lata adopción digital y nuevas complejidades tecnológicas exige una acción coordinada y la implementación de medidas de seguridad que vayan más allá de los enfoques tradicionales.

Para fortalecer la seguridad de los pagos digitales en el entorno 5G, es fundamental adoptar un conjunto de medidas técnicas avanzadas y adaptativas.

En la siguiente tabla encontramos las diferentes estrategias que posee la nueva red de quinta generación, buscando mostrar un avance para proteger los pagos digitales

Tabla 3

Estrategias de ciberseguridad en redes 5G

Estrategias	**Segmentación de red y Microsegmentación**	**Autenticación y Cifrado de Extremo a Extremo**	**Seguridad de la cadena de Suministro**
Definición	Se utiliza el Networ Slicing no solo para optimizar el rendimiento, sino para aislar los servicios de pago en segmentos de red	A pesar de las mejoras de seguridad inherentes al 5G, las plataformas de pago deben implementar sus propias capas de	Dado que la arquitectura 5G depende de múltiples proveedores de software y hardware, las empresas financieras deben

Estrategias	Segmentación de red y Microsegmentación	Autenticación y Cifrado de Extremo a Extremo	Seguridad de la cadena de Suministro
	dedicados y con fuertes controles de seguridad. Dentro de estos segmentos, la microsegmentación crea barreras entre los componentes de la aplicación, lo que impide que un atacante que logra entrar en una parte del sistema se mueva libremente por toda la red en un entorno 5G	seguridad. Esto incluye el cifrado de datos desde el dispositivo del usuario hasta el servidor del banco, así como el uso de la autenticación multifactor o la biometría, que son más rápidas y fiables	auditar y garantizar que sus socios tecnologías cumplan con los estándares de seguridad más altos para evitar puntos débiles

(Asobancaria, *Guía de buenas prácticas para auditar la ciberseguridad*, 2022) (Liderazgo, 2023) (Teldat, 2024)

La tokenizacion es una técnica de seguridad que sustituye los datos sensibles, como números de tarjeta de crédito o información bancaria, por un valor único y no sensible llamado token. Este token carece de significado fuera del contexto especifico de la transacción o sistema, lo que reduce drásticamente el riesgo de robo de información en tránsito o almacenamiento (Council, 2022). Si un atacante intercepta un token, no obtendrá datos financieros reales, La implementación de la tokenizacion es crucial para todas las plataformas de pago digital y debe extenderse a los dispositivos loT que manejan transacciones, garantizando que la información del cliente nunca se almacene de forma legible en puntos de venta o dispositivos edge.

El cifrado de extremo a extremo garantiza que los datos se cifren en el punto de origen y solo se descifren en el destino final. Esto protege los datos desde el origen hasta el destino, impidiendo que cualquier intermediario no autorizado, incluyendo la red, pueda leer la información (Abie, 2024). Es esencial en entornos de edge computing y redes públicas 5G, donde los datos pueden pasar por múltiples nodos distribuidos antes de llegar a los

servidores centrales de pago. Hay que asegurar que las aplicaciones de pago, las billeteras digitales y las comunicaciones entre dispositivos y servidores utilicen siempre cifrado de extremo a extremo con algoritmos criptográficos robustos es una capa de defensa fundamental contra la intercepción y manipulación de datos.

La autenticación multifactor (MFA) requiere que los usuarios verifiquen si identidad a través de la combinación de al menos dos factores de autenticación independientes: algo que el usuario sabe (una contraseña), algo que el usuario tiene (un token de hardware o un código enviado al teléfono) y/o algo que el usuario es (biometría como huella dactilar o reconocimiento facial) (Grassi, Fenton, Newton, & Perlner, 2023). La MFA es altamente recomendada para todas las plataformas de pago, ya que eleva significativamente la barrera para los atacantes. Incluso si una contraseña es comprometida a través de phishing o malware, el atacante no podrá acceder a la cuenta sin el segundo factor, reduciendo drásticamente los riesgos de suplantación de identidad.

La capacidad de monitoreo en tiempo real y detección de fraudes es crítica en el entorno de alta velocidad del 5G. Esto implica el uso de inteligencia artificial y machine learning para identificar patrones sospechosos en las transacciones que se desvíen del comportamiento normal del usuario o de las normas de la red (garibay, Alaghband, & Yousefi, 2023). Los algoritmos de IA pueden analizar volúmenes masicos de datos a la velocidad del 5G, detectando anomalías que un sistema manual no podría. Es crucial que los bancos y las Fintech implementen sistemas que envíen notificaciones instantáneas al usuario ante movimientos inusuales o intentos de accesos sospechosos, permitiendo una acción rápida para bloquear transacciones fraudulentas y protegerlas cuentas.

Para mitigar los riesgos inherentes a la arquitectura 5G, es vital implementar una segmentación de red estricta y un fuerte aislamiento de slices. Esto implica diseñar la red de manera que cada slice tenga políticas de seguridad independientes y estrictas, minimizando

las interacciones innecesarias y el acceso entre ellas (Alwis, Porambage, Dev, Gadekallu, & Liyanage, 2024). El objetivó es evitar que un ataque en un slice de menor seguridad afecte a otros servicios críticos, como los pagos digitales, que residen slices de mayor seguridad. Un modelo de confianza ceo aplicado a la inter-slice la comunicación es fundamental para asegurar que los permisos sean mínimos estrictamente monitoreados.

Una práctica de ciberhigiene fundamental es la actualización y gestión de parches. Es imperativo que los usuarios mantengan actualizados los sistemas operativos, las aplicaciones y el firmware de todos los dispositivos conectados a la red 5G que utilicen para pagos (smartphones, wearables, datafonos, etc.) (Sheng, Zhicheng Chen, Huang, Gu, & Huang, 2025). De la misma forma, los operadores de telecomunicaciones y las entidades financieras deben tener procesos robustos para la gestión de vulnerabilidades y la aplicación de parches en su infraestructura 5G y sus plataformas de pago, asegurándose de que las debilidades conocidas sean corregidas proactivamente para cerrar posibles vectores de ataque.

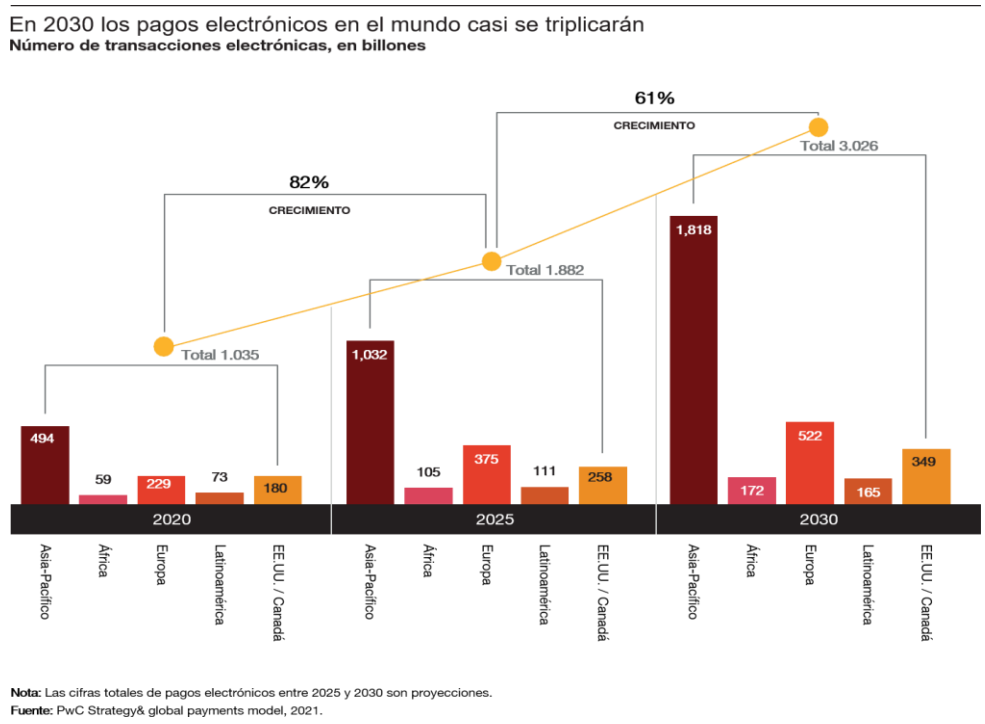
Para construir un ecosistema de pagos digitales seguro en el contexto 5G, las medidas técnicas deben estar respaldados por un marco normativo y regulatorio robusto y adaptado a los desafíos actuales.

Colombia ya cuenta con un base legal importante, pero su fortalecimiento y aplicación rigurosa son esenciales. La ley 1581 de 2012 (Protección de datos personales) debe seguir siendo el pilar fundamental, exigiendo a todas las entidades que manejan datos financieros y transacciones digitales un cumplimiento estricto de los principios de seguridad, confidencialidad y veracidad. Su alcance debe ser explícitamente extendido y adaptado a las complejidades del 5G y el edge computing, donde los datos se procesan en múltiples puntos (SIC, Informe sobre Protección de Datos Personales en el Sector Financiero, 2023). La ley 1273 de 2009 (Delitos Informáticos) debe ser revisada y actualizada periódicamente para incluir nuevas modalidades de ciberdelincuencia que emergen con el 5G, como ataques a

network slicing o firmware de dispositivos loT (Publica, 2009). Finalmente, el decreto 338 de 2022 (Gobernanza de la Seguridad Digital) sienta las bases para una política de seguridad digital cohesiva. Este decreto debe ser el punto de partida para desarrollar regulaciones más específicas que obliguen a los operadores de 5G y alas fintechs a implementar controles de seguridad basados en riesgos y a reportar incidentes de manera estandarizada (Colombia P. d., 2022).

La siguiente grafica nos muestra el crecimiento por año de los ataques cibernéticos desde el año 2020 hasta una proyección del 2030 esta proyección es a nivel mundial donde vemos países con mayor capacidad de conexión y avances tecnológicos son más propensos a ataques cibernéticos

Figura 4
Medios de pago: 2025 y más allá



Fuente PwC *Strategy global payments model*, 2021 (https://www.pwc.es/es/financiero/medios-pago-2025-mas-alla.html)

El sistema BRE-B (Banca de la Republica – Ecosistemas de Pagos de Bajo Valor) es una iniciativa prometedora para la seguridad de los pagos digitales en Colombia. Su rol

clave es promover la interoperabilidad y seguridad en pagos digitales de bajo monto, lo cual es vital para el crecimiento de billeteras móviles y transacciones cotidianas. Al monto, lo cual es

vital para el crecimiento de billeteras móviles y fintechs, el BRE-B facilita la implementación de prácticas de seguridad uniformes, la prevención del fraude y la resolución de disputas. Es crucial que este sistema se adapte y contemple los riesgos emergentes del 5G, asegurando que los estándares de seguridad que impone sean compatibles con las nuevas arquitecturas y velocidades de red, y que promueva la adopción de tecnología de protección como la tokenizacion y el E2EE en todas las transacciones que lo atraviesen.

Más allá de la normativa existente, se necesitan acciones regulatorias específicas. Es imperativo exigir el cumplimiento de estándares internaciones como PCI DSS para toda entidad que procese pagos con tarjeta y la certificación ISO/IEC 27001 para la gestión de la seguridad de la información en bancos, fintechs y operadores 5G (Council, 2022). La obligatoriedad de auditorías periódicas de ciberseguridad en plataformas de pago, realizadas por terceros independientes, es fundamental para identificar vulnerabilidades y asegurar la mejora continua. Además, se requiere una regulación específica para los dispositivos loT usados en pagos (como datafonos móviles o wearables). Esta regulación debería establecer requisitos mínimos de seguridad para su hardware, firmware y conectividad 5G, incluyendo la necesidad de actualizaciones de seguridad regulares y el uso de cifrado fuerte, para evitar que se conviertan en puntos débiles en el ecosistema financiero (ENISA, ENISA Threat Landscape for 5G Networks, 2020).

Para complementar las medidas técnicas y normativas, es vital implementar propuestas específicas que aborden las particularidades del contexto colombiano. Las campañas de educación digital masivas son esenciales para usuarios y comerciantes. Estas

campañas, lideradas por entidades gubernamentales, financieras y operadores, deben enfocarse en buenas prácticas de ciberhigiene: como identificar phishing y smishing, la importancia de las contraseñas fuertes y el MFA, y los riesgos de las redes Wi-Fi públicas. Educar al usuario final es la primera línea de defensa contra la ingeniera social (Varalakshmi, S, Baheti, & Dugar, 2024).

Se deben crear incentivos fiscales para fintechs que implementen tecnologías seguras. El gobierno podría ofrecer beneficios tributarios a aquellas empresas que inviertan en tokenizacion, cifrado de extremo a extremo, sistemas avanzados de detección de fraude basados en IA, y que obtengan certificaciones de seguridad reconocidas internacionalmente. Esto fomentaría la adopción de medidas de seguridad que van más allá de lo básico (BID, Ciberseguridad ¿Estamos preparados en América Latina y el Caribe?, 2016).

El establecimiento de alianzas público-privada para compartir inteligencia sobre amenazas es crucial. Un modelo de colaboración donde ColCERT, la Superintendencia Financiera, bancos, fintechs y operadores 5G compartan información en tiempo real sobre nuevas amenazas, vulnerabilidades y tácticas de ataque permitiría una respuesta más rápida y coordinada a nivel nacional, anticipando y neutralizando ciberataque de manera más eficiente (IBM, 2024).

Finalmente, la creación de una certificación nacional de ciberseguridad para aplicaciones de pago podría elevar la confianza del usuario. Un sello o certificación oficial, otorgado por una entidad independiente reconocida, que valide que una aplicación de pago cumple con estándares mínimos de seguridad rigurosos, les daría a los usuarios una garantía de confianza al elegir plataformas digitales y fomentaría la sana competencia en seguridad entre los proveedores de servicios (Asobancaria, Superintendencia Financiera de Colombia, 2023).

En este último capítulo, se exploró las estrategias de mitigación, como el uso de la

autenticación de dos factores mejorada, la educación en ciberhigiene y las regulaciones más estrictas. Al proponer estas soluciones, se logró el Objetivo 4, que consistía en proponer estrategias para mitigar los riesgos y aumentar la seguridad de los pagos digitales. Estas recomendaciones no solo abordan los desafíos actuales, sino que también sientan las bases para futuras investigaciones en el campo de la ciberseguridad financieras.

Líneas de trabajo futuro

1. Evaluación de la Infraestructura de Entidades Financieras Colombianas: Lecciones y Vulnerabilidades

Imagina un panorama donde los bancos y fintechs colombianas, como Bancolombia, Davivienda o Nequi, adoptan redes 5G para acelerar sus plataformas de pago. Esta línea de investigación propone un análisis profundo, tanto cualitativo como cuantitativo, de la infraestructura tecnológica actual de estas entidades. Nos preguntamos: ¿cómo están integrando el 5G? ¿Qué vulnerabilidades emergen en esta transición?

El estudio examinará casos reales de ciberataques que han explotado debilidades en redes financieras, comparando las medidas de seguridad adoptadas por diferentes instituciones. Por ejemplo, podríamos analizar cómo un ataque de phishing o un exploits en una red 4G afectó a una Fintech colombiana y qué lecciones se pueden aprender para el 5G. Al identificar brechas de seguridad y destacar mejores prácticas, esta investigación proporcionará una hoja de ruta para que el sector financiero colombiano esté mejor preparado.

Riesgo futuro: Sin una evaluación proactiva, las vulnerabilidades en la implementación temprana del 5G podrían exponer a millones de usuarios a robos de datos o interrupciones en servicios críticos. En un país donde los pagos digitales están en auge, un solo incidente podría minar la confianza de los consumidores y frenar la adopción tecnológica.

2. Diseño de un Marco Regulatorio para la Ciberseguridad 5G en Colombia

El despliegue del 5G en Colombia no es solo una oportunidad tecnológica, sino también un desafío regulatorio. Basándonos en estándares globales, como la "Caja de Herramientas de Ciberseguridad 5G" de la Unión Europea y las guías del NIST, esta propuesta busca desarrollar un marco regulatorio adaptado al contexto colombiano. Este marco sería una herramienta clave para entidades como el Ministerio de TIC, la CRC o la Superintendencia Financiera.

El trabajo incluiría:

Requisitos de seguridad obligatorios para proveedores de infraestructura 5G, garantizando que cumplan con estándares técnicos robustos.

Certificaciones para dispositivos LoT utilizados en el sector financiero, asegurando que no se conviertan en puntos débiles de la red.

Guías de ciberhigiene dirigidas a usuarios de pagos digitales, fomentando prácticas seguras en un entorno cada vez más conectado.

Este enfoque no solo protegerá la infraestructura crítica, sino que también posicionará a Colombia como un referente en ciberseguridad en América Latina.

Riesgo futuro: Sin regulaciones claras, los proveedores de 5G podrían priorizar costos sobre seguridad, dejando la red vulnerable a ataques sofisticados, como los de denegación de servicio distribuido (DDoS) o la explotación de dispositivos LoT inseguros. Esto podría tener consecuencias devastadoras para la economía digital colombiana.

3. Inteligencia Artificial para Combatir el Fraude en Pagos Digitales Colombianos

En un país donde plataformas como PSE, Nequi y Daviplata son parte del día a día de millones de usuarios, la inteligencia artificial (IA) y el aprendizaje automático (ML)

pueden marcar la diferencia en la lucha contra el fraude. Esta línea de investigación propone analizar los tipos de fraude más comunes en estas plataformas, desde phishing hasta transacciones no autorizadas, y evaluar cómo los modelos de IA actuales detectan anomalías.

El estudio irá más allá, proponiendo un modelo predictivo que identifique patrones sospechosos en transacciones, utilizando datos anonimizados para proteger la privacidad. Por ejemplo, podríamos desarrollar un sistema que alerte en tiempo real sobre actividades inusuales, como transferencias masivas desde una cuenta nueva. Este enfoque no solo reducirá pérdidas financieras, sino que también fortalecerá la confianza de los usuarios en el ecosistema digital.

Riesgo futuro: A medida que los ciberdelincuentes adopten técnicas más avanzadas, como el uso de IA para generar ataques de phishing hiper personalizados, las plataformas que no integren modelos predictivos robustos quedarán rezagadas. Esto podría traducirse en pérdidas millonarias y una menor adopción de servicios digitales en Colombia.

Conclusiones

1. El análisis detallado sobre la arquitectura 5G nos indica que tecnología como la virtualización de funciones de red (NFV), las redes definidas por software (SDN), el edge computing y el networking slicing, aunque fundamentales para la eficiencia del sistema, introducen nuevas superficies de ataque. Estas vulnerabilidades, especialmente en entornos financieros, pueden ser explotadas para comprometer la integridad de las transacciones, interceptar datos sensibles o facilitar ataques de denegación de servicio. En el contexto colombiano, donde la infra estructura aún está en expansión, estas debilidades representan un riesgo crítico para la seguridad de los pagos digitales.

2. Se logro evidenciar que la implementación del 5G incrementa significativamente la exposición a ciberataques debido a la mayor velocidad, densidad de dispositivos conectados y descentralización del procesamiento de datos. Factores como el bajo nivel de ciberhigiene de los usuarios, el uso de redes públicas y la falta de actualizaciones en dispositivos móviles agravan esta situación. Las plataformas de pago digital en Colombia, aunque en crecimiento, enfrentan amenazas como el phishing, el malware financiero y los ataques a dispositivos loT, lo que exige una respuesta más proactiva y coordinada.

3. La comparación entre los estándares internacionales y los riesgos específicos del entorno 5G evidencio que, si bien existen marcos sólidos, persisten brechas importantes en su implementación, especifica en pequeñas fintechs y plataformas emergentes. En Colombia, la falta de auditorías obligatorias, la desactualización tecnológica y la escasa cultura de ciber seguridad ante amenazas sofisticadas.

4. Se reconocieron las medidas propuestas, como la tokenizacion, el cifrado de extremo a extremo, la autenticación multifactor y la segmentación segura de red, se presentan como soluciones viables y necesarias para mitigar los riesgos identificados. A nivel normativo se destaca la necesidad de actualizar leyes como la 1581 de 2012 y la 1273 de 2009, así como fortalecer incentivos para la adopción de tecnologías seguras y crear una certificación nacional de ciberseguridad par plataformas de pago. Estas acciones permitirán construir un ecosistema financiero más seguro, resiliente y confiable en el contexto colombiano del 5G.

Glosario

5G (Quinta Generación): Estándar de tecnología de redes celulares de última generación, diseñado para proporcionar velocidades de transmisión significativamente superiores, latencia ultra-baja y capacidad para soportar una conexión masiva de dispositivos simultáneamente, optimizando aplicaciones como LoT, vehículos autónomos y realidad aumentada.

4G (Cuarta Generación): Estándar de tecnología móvil precedente al 5G, caracterizado por ofrecer conectividad de banda ancha de alta velocidad, soporte para aplicaciones multimedia y una mejora sustancial en la eficiencia de red respecto a generaciones anteriores.

Amenaza Persistente Avanzada (APT): Tipo de ciberataque sofisticado y prolongado, en el que un actor malicioso establece una presencia encubierta y persistente en una red, con el objetivo de exfiltrar datos sensibles o estratégicos durante un período extendido, empleando técnicas avanzadas de infiltración y evasión.

Ancho de Banda: Capacidad máxima de transmisión de datos a través de una conexión de red en un intervalo de tiempo específico, medida típicamente en bits por segundo (bps). En 5G, el ancho de banda es significativamente superior al de 4G, permitiendo mayor volumen y velocidad de transferencia.

Autenticación de Dos Factores (2FA): Método de seguridad que refuerza la protección de acceso al requerir dos formas de verificación independientes, como una contraseña y un código temporal enviado a un dispositivo asociado, reduciendo el riesgo de accesos no autorizados.

Autenticación Multifactor (MFA): Sistema de seguridad avanzado que exige la presentación de dos o más factores de verificación (como algo que el usuario sabe, posee o

es) para autenticar el acceso a recursos protegidos, incrementando la robustez frente a posibles vulneraciones.

Biometría: Tecnología de autenticación que emplea características físicas o conductuales únicas, como huellas dactilares, reconocimiento facial o patrones de voz, para verificar la identidad de un usuario con alta precisión y seguridad.

Botnets: Red de dispositivos infectados por malware, controlados remotamente por un actor malicioso para ejecutar actividades ilícitas, como ataques de denegación de servicio distribuido (DDoS), envío de spam o robo de datos, sin el conocimiento de los propietarios de los dispositivos.

Ciberhigiene: Conjunto de prácticas y políticas implementadas por usuarios y organizaciones para mantener la seguridad de sus sistemas y datos, incluyendo la actualización regular de software, el uso de contraseñas seguras y la monitorización de actividades sospechosas.

Cifrado (Encriptación): Proceso técnico de transformación de datos legibles en un formato codificado mediante algoritmos criptográficos, garantizando que solo las partes autorizadas con la clave correspondiente puedan acceder a la información original.

Confidencialidad: Principio fundamental de la seguridad de la información que asegura que los datos sean accesibles únicamente por las personas o sistemas autorizados, protegiéndolos contra accesos no permitidos.

Costo del Cibercrimen: Impacto económico derivado de actividades delictivas en el entorno digital, incluyendo pérdidas por robo de datos, interrupciones operativas, costos de mitigación y recuperación, y daños reputacionales.

Ciberseguridad: Disciplina dedicada a la protección de sistemas, redes, dispositivos y datos contra amenazas digitales, accesos no autorizados y ataques maliciosos, mediante la

implementación de tecnologías, procesos y políticas de seguridad.

Denegación de Servicio (DoS): Tipo de ciberataque que busca interrumpir la disponibilidad de un servicio o recurso en línea, sobrecargando los sistemas con un volumen excesivo de tráfico o solicitudes, impidiendo el acceso a usuarios legítimos.

Denegación de Servicio Distribuido (DDoS): Variante avanzada de un ataque DoS que utiliza una red coordinada de múltiples dispositivos (generalmente una botnet) para generar un volumen masivo de tráfico malicioso, saturando los recursos del objetivo.

Disponibilidad: Principio de seguridad que garantiza que los sistemas, aplicaciones y datos estén operativos y accesibles para los usuarios autorizados en el momento en que se requieran, minimizando interrupciones por fallos o ataques.

Estrategia de Cero Confianza (Zero Trust): Modelo de seguridad que adopta el principio de "nunca confiar, siempre verificar", exigiendo autenticación y autorización estrictas para cada solicitud de acceso a recursos de red, independientemente de la ubicación o el origen del usuario.

Fraude Digital: Actividad delictiva realizada en entornos digitales con el propósito de obtener beneficios económicos o estratégicos mediante engaño, como el robo de identidad, la suplantación de sitios web o el uso indebido de datos financieros

Identificador Internacional de Suscriptor Móvil (IMSI): Código único asignado a cada suscriptor de una red móvil para identificarlo de manera inequívoca. En redes 4G, el IMSI se transmitía en texto plano, lo que representaba una vulnerabilidad de seguridad al permitir la interceptación de datos de identidad por actores maliciosos.

Integridad: Principio fundamental de la seguridad de la información que asegura que los datos no han sido modificados, alterados o comprometidos de forma no autorizada, garantizando su exactitud y confiabilidad durante todo su ciclo de vida.

Internet de las Cosas (LoT): Ecosistema de dispositivos físicos integrados con sensores,

software y tecnologías de conectividad que permiten la recolección, intercambio y procesamiento de datos a través de redes de Internet, habilitando aplicaciones como hogares inteligentes, ciudades conectadas y automatización industrial.

Latencia: Intervalo de tiempo que transcurre desde que un paquete de datos es enviado desde su origen hasta que llega a su destino, medido en milisegundos. Las redes 5G están diseñadas para reducir significativamente la latencia, optimizando aplicaciones en tiempo real como cirugía remota y vehículos autónomos.

Ley de Ciberseguridad 5G (UE): Marco normativo establecido por la Unión Europea para regular la seguridad de las redes 5G, definiendo requisitos estrictos para proteger la infraestructura crítica, garantizar la confidencialidad de los datos y mitigar riesgos asociados con proveedores y tecnologías de red.

Malware: Software malicioso diseñado específicamente para infiltrarse, dañar o tomar control de sistemas informáticos, exfiltrar datos sensibles o interrumpir operaciones, abarcando diversas formas como virus, gusanos y ransomware.

Virtualización de Funciones de Red (NFV): Tecnología que permite la ejecución de funciones de red, tradicionalmente implementadas en hardware propietario, como software virtualizado en servidores estándar, mejorando la flexibilidad, escalabilidad y eficiencia de las redes.

Segmentación de Red (Network Slicing): Característica avanzada de las redes 5G que permite la creación de múltiples redes virtuales independientes sobre una única infraestructura física, cada una optimizada para cumplir requisitos específicos de servicios o aplicaciones, como LoT masivo, banda ancha mejorada o comunicaciones de baja latencia.

Instituto Nacional de Estándares y Tecnología (NIST): Entidad estadounidense responsable de desarrollar estándares, directrices y mejores prácticas en múltiples disciplinas tecnológicas, incluyendo ciberseguridad, con Frameworks ampliamente adoptados como el

NIST Cybersecurity Framework.

Phishing: Técnica de ingeniería social que utiliza correos electrónicos, mensajes de texto o llamadas fraudulentas para inducir a los usuarios a divulgar información confidencial, como credenciales de acceso o datos financieros, bajo pretextos engañosos.

Ransomware: Variante de malware que cifra los datos de un sistema o dispositivo, impidiendo el acceso a los archivos de la víctima y exigiendo un pago, generalmente en criptomonedas, para proporcionar la clave de descifrado, representando una amenaza significativa para organizaciones y usuarios.

Redes Definidas por Software (SDN): Arquitectura de red que desacopla el plano de control del plano de datos, permitiendo la gestión centralizada y programable de la infraestructura de red, lo que facilita la configuración dinámica y la optimización del tráfico.

Identificador de Suscriptor Cifrado (SUCI): Identificador en redes 5G que reemplaza al IMSI, cifrando la identidad del suscriptor desde el dispositivo para proteger su privacidad y mitigar riesgos de interceptación o suplantación en la red.

Suplantación de Identidad: Delito en el que un atacante se hace pasar por una entidad legítima, como una persona o institución, para obtener beneficios ilícitos, como acceso no autorizado a sistemas, robo de datos o fraude financiero.

Superficie de Ataque: Conjunto de todos los puntos de entrada potenciales en un sistema o red que un atacante podría explotar, incluyendo vulnerabilidades en software, configuraciones débiles o credenciales expuestas, cuya gestión es crítica para reducir riesgos de seguridad.

Telefonía Móvil: Sistema de comunicación inalámbrica que permite a los usuarios realizar llamadas, enviar mensajes y acceder a servicios de datos a través de redes celulares, evolucionando desde generaciones analógicas hasta las actuales redes 5G de alta capacidad.

Troyano (Caballo de Troya): Tipo de malware que se presenta como software legítimo para

engañar a los usuarios y lograr su instalación, permitiendo a los atacantes ejecutar acciones maliciosas como el robo de datos, la vigilancia remota o la creación de puertas traseras en el sistema.

Referencias Bibliográficas

3GPP. (2018). 3GPP TS 23.501: System Architecture for the 5G System (5GS). https://www.3gpp.org/DynaReport/23501.htm

3GPP. (23 de Marzo de 2018). Specification # 33.501. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

3GPP. (2018). Specification #33.501. https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

3GPP. (2020). 5G Security Architecture and Procedures. https://www.google.com/search?q=https://www.3gpp.org/technologies/5g/5g-security

9th International Conference on Cyber Conflict: Defending the Core. (2017). IEEE Advancing Technology for humanity , 54-67.

Abie, H. (2024). Autonomous Adaptive Security Framework for 5G-Enabled IoT. Norwegian Computing Center.

Ábrego-Almazán, M. I.-R. (2023). Influencia de la seguridad y la confianza como antecedentes de la.

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2018). Overview of 5G Security Challenges and Solutions. IEEE.

Ala-Mutka, K. (2011). Mapping Digital Competence: Towards a Conceptual Understanding. Joint Research Centre, Institute for Prospective Technological Studies.

Almagro, L., Gómez, S. C., Urrutia, F. D., & Treppel, A. A. (2020). Estado de la ciberseguridad en el sistema financiero Colombiano . Asobancaria, 50-112.

Alwis, C. D., Porambage, P., Dev, K., Gadekallu, T. R., & Liyanage, M. (2024). A Survey on Network Slicing Security: Attacks,. IEEE, 2-25.

ÁLZATE, J. D. (2024). repository unad. https://repository.unad.edu.co/bitstream/handle/10596/65294/jdosorioal.pdf?sequence=1&isAllowed=y

Archibong, E. E., Stephen, B. U.-A., & Asuquo, P. (2024). Analysis of CybersecurityVulnerabilities in MobilePayment Applications. Advanced Engineering Science, 1-10.

Asim, M., Khan, F. A., & Tariq, N. (2021). Security Challenges and Requirements for Smart Internet of Things. International Workshop on Cyber Security and Digital Investigation, 1-6.

Asobancaria. (2022). Guía de buenas prácticas para auditar la ciberseguridad. https://www.asobancaria.com/wp-content/uploads/2022/06/Guia_de_Buenas_Practicas_para_Auditar_la_Ciberseguridad_2022_V1.pdf

Asobancaria. (2023). Superintendecia Financiera de Colombia. Informe de Tendencias en la Banca Digital Colombia: https://www.superfinanciera.gov.co/publicaciones/10115193/reporte-de-inclusion-financiera-2023-avances-y-retos-en-colombia/

Banguero Melo, H. R.-M. (2019). Efectividad de un programa de intervención psicoeducativa para el fortalecimiento de las habilidades sociales en personas privadas de la libertad.

Bermudez, D. A. (17 de Junio de 2023). Billeteras digitales: ¿cómo protegerse de estafas? Esto dicen las entidades financieras. El Tiempo: https://www.eltiempo.com/bogota/billeteras-digitales-como-protegerse-de-estafas-esto-dice-nequi-daviplata-y-dale-778599

Bhushan, B. (2018). Security Attacks and Countermeasures in 5G Enabled Internet of Things.

Bhushan, B., Sharma, S. K., Kumar, R., & Priyadarshini, I. (2023). 5G and Beyond. Springer

Tracts in Electrical and Electronics Engineering.

BID. (2016). Ciberseguridad ¿Estamos preparados en América Latina y el Caribe? . Organization of American States.

BID. (2022). La Ciberseguridad en América Latina y el Caribe: Nuevos Retos y Oportunidades. Organization of American States.

Board, E. D. (2024). Guías y recomendaciones del EDPB. Edpb.europa.eu: https://www.google.com/search?q=https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations_en

Borketey, B. (2024). Real-Time Fraud Detection Using Machine Learning. Journal of Data Analysis and Information Processing , 12(02):189-209.

Bowen, M. (12 de Diciembre de 2022). Intelligent -CIO-. https://www.intelligentcio.com/latam/2022/12/12/myths-and-benefits-of-5g-before-its-implementation-in-colombia/

Broadcom. (2019). Internet Security Threat Report (ISTR). Symantec.

CAF. (2020). Brechas Digitales en América Latina y el Caribe: Una Visión desde la Conectividad. https://www.google.com/search?q=https://www.caf.com/es/conocimiento/publicaciones/2020/09/brechas-digitales-en-america-latina-y-el-caribe/

Cherry Manglaa, S. R. (2022). Mitigating 5G security challenges for next-gen industry using quantumcomputing. Journal of King Saud University –Computer and Information Sciences, 1-13.

Citaristi, I. (2022). International Telecommunication Union—ITU. Routledge.

Cohen, S. K., Rojas, D. M., & Barrera, P. P. (2025). Estrategia Nacional de Seguridad digital de colombia 2025-2027. Gobierno de colombia, 4-32.

ColCERT. (26 de Noviembre de 2025). Acerca de ColCERT.

https://www.colcert.gov.co/800/w3-article-198657.html

Colombia, P. d. (2022). Decreto 338 de 2022.

Colombia, S. F. (2019). Circular Externa 007.

Comercio, S. d. (2023). Guía para el Tratamiento de Datos Personales.

Council, P. S. (2022). PCI DSS Quick Reference Guide. PCI Security Standards Council, LLC.

Diaz, M. F. (18 de Septiembre de 2023). Universidad nacional del litoral. https://www.redalyc.org/journal/6559/655977607008/

DIGITAL, P. N. (2023). Informe de Cibercrimen 2023.

DNP. (2020). Documento CONPES 3995: Política Nacional de Confianza Digital.

DNP. (2020). Guía de Ciberseguridad para Entidades Públicas y Privadas.

Economia, R. (23 de Febrero de 2024). Despliegue de redes 5G comienza en Colombia: ¿cómo impacta a los usuarios. EL ESPECTADOR: https://www.elespectador.com/economia/despliegue-de-redes-5g-comienza-en-colombia-como-impacta-a-los-usuarios/

EDPB. (9 de octubre de 2025). European Data Protection Board. Guías y recomendaciones del EDPB.: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_es

EDPB. (4 de Diciembre de 2025). European Data Protection Board. Guías y recomendaciones del EDPB: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2025/joint-guidelines-interplay-between-digital_en

El campesinado colombiano . (2019).

ENISA. (2017). Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. European Union Agency For Network And Information

Security.

ENISA. (Enero de 2017). ENISA (European Union Agency for Cybersecurity. ENISA Threat Landscape Report: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

ENISA. (2020). ENISA Threat Landscape for 5G Networks. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Ericsson. (2021). Network Slicing: Building the 5G Enterprise: https://www.google.com/search?q=https://www.ericsson.com/en/reports-and-papers/white-papers/network-slicing-building-the-5g-enterprise

ERICSSON. (2021). 5G security - enabling a trustworthy 5G system. http://ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system

Ericsson. (2021). 5G Security: Security Architecture and Solutions. https://www.google.com/search?q=https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security-architecture-and-solutions

Esnoz, I. (28 de Septiembre de 2023). Teldat. Teldat: https://www.teldat.com/es/blog/5g-tecnologia-conectividad-ciberseguridad/

ETSI. (2020). ETSI EN 303 644: Cybersecurity for 5G - Security Requirements and Evaluation. European standard.

ETSI. (2022). MEC security Status of standards support.

Europol. (2023). Internet organised crime. European Union Agency for Law Enforcement Cooperation,.

Fang, D., Qian, Y., & Hu, R. Q. (2017). Security for 5G Mobile Wireless Networks. IEEE Access, 1-21.

Fintech, C. (2024). Fintech Snapshot 2024.

https://colombiafintech.co/lineaDeTiempo/articulo/fintech-snapshot-2024-

Forum, W. E. (2023). Global Cybersecurity Outlook 2023. Accenture.

Foundation, O. (2021). OWASP Foundation. OWASP Top 10 - 2021.: https://owasp.org/www-project-top-ten/

Futuras Amenazas Cibernéticas. (2021). https://www.accenture.com/content/dam/accenture/final/a-com-migration/manual/r3/pdf/pdf-157/Accenture-Future-Cyber-Threats-Argentina-2021.pdf

García-Peñalvo, F. J.-G. (2018). Critical thinking and creativity in computational thinking. En F. J.-G. García-Peñalvo, Critical thinking and creativity in computational thinking (págs. 595-602). Technological Ecosystems for Enhancing Multiculturality.

garibay, I., Alaghband, M., & Yousefi, N. (2023). A Comprehensive Survey on Machine Learning Techniques and User Authentication Approaches for Credit Card Fraud Detecti. Cornell University, 5-25.

Givant. (2017). Relation algebras. In Introduction to Relation Algebras. . Springer.

González, J. M. (2025). Tendencias de innovación DEI en sector bancario.

Gordillo-Gaitán, A. (2024). Cybersecurity Strategies for SMEs in the Tertiary. European Public & Social Innovation, 1-18.

Grassi, P. A., Fenton, J. L., Newton, E. M., & Perlner, R. A. (2023). Digital Identity Guidelines. NIST.

Grassi, P. A., Garcia, M. E., & Fenton, J. L. (2017). NIST Special Publication 800-63-3: Digital Identity Guidelines. U.S Department of commerce.

Group, M. I. (2022). MEC (Multi-access Edge Computing) in 5G: Benefits and Challenge.

GSMA. (2023). https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/latam/. The Mobile Economy Latin America 2023:

https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/latam/

H. Rõigas, R. J. (2017). 9th International Conference on Cyber Conflict:. IEEE Advance Technology for Humanity , 54-67.

Hackmetrix. (17 de Marzo de 2023). Hackmetrix. Conoce los principales tipos de explotación de vulnerabilidades.: https://blog.hackmetrix.com/principales-tipos-de-explotacion-de-vulnerabilidades/

Hacknoid. (31 de Octubre de 2023). Hacknoid. Cómo impactan las vulnerabilidades en la continuidad del negocio: https://www.hacknoid.com/hacknoid/como-impactan-las-vulnerabilidades-en-la-continuidad-del-negocio/

HARBOR, N. (2014). Gartner. Gartner Identifies the Top 10 Security Technologies for 2014: https://www.gartner.com/en/newsroom/press-releases/2014-06-24-gartner-identifies-the-top-10-technologies-for-information-security-in-2014

Hassan, M. A., & Shukur, Z. (2023). A systematic review of user authentication security in electronic payment system . Proceedings of International Conference on Data Science.

Hu, F. Y. (2020). Security analysis of 5G network slicing and its countermeasures. Journal of Network and Computer Applications, 166.

Huawei. (2021). Huawei 5G Security White Paper. Huawei: https://www.huawei.com/en/trust-center/5g-cyber-security

IBM. (2024). The Road Ahead for Cybersecurity - 2024 and Beyond Trends. https://mediacenter.ibm.com/media/IBM+Z+Day+2023%3A+The+Road+Ahead+for+Cybersecurity+-+2024+and+Beyond+Trends/1_d5iaws7l

ICO. (19 de Junio de 2025). Information Commissioner's Office. Individual rights: https://ico.org.uk/for-organisations/law-enforcement/guide-to-le-processing/individual-rights/

INCIBE. (15 de Enero de 2020). INCIBE. Vulnerabilidad: https://www.incibe.es/aprendeciberseguridad/vulnerabilidad

Institute., P. (2023). IBM Security. Cost of a Data Breach Report: https://www.ibm.com/reports/data-breach

ISO. (2022). Information security, cybersecurity. INTERNATIONAL STANDARD, 1-26.

ITU. (2020). IMT-2020 (5G) Overview. https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx

J. P. Mohan, N. S. (2022). Cyber Security Threats for 5G Networks. IEEE International Conference on Electro Information Technology, 446-454.

Kasiyanto, S. (2016). END-TO-END ENCRYPTION IN ON-LINE PAYMENT SYSTEMS: THE INDUSTRY RELUCTANCE AND THE ROLE OF LAWS. Tilburg University Legal advisor, 101-121.

Kaspersky. (2025). Amenazas cibernéticas en aumento: Kaspersky revela el panorama. https://impactotic.co/tecnologia/amenazas-ciberneticas-en-aumento-kaspersky-revela-el-panorama/

Kolias, C. K. (2017). DDoS in the IoT: A survey of techniques for attack detection and mitigation. ournal of Network and Computer Applications, 89, 130-154.

Kshetri, N. (2014). The cybercrime economy in the global South. Journal of Cybersecurity, 22-35.

Liderazgo, I. C. (2023). La tecnología 5G china y los riesgos para Colombia: análisis comparado y recomendaciones de política. https://icpcolombia.org/wp-content/uploads/2023/12/La-tecnologia-5G-china-y-los-riesgos-para-Colombia.pdf

López, J. &. (2023). Vulnerabilidades en redes 5G: Un análisis crítico. SIC.

Mak, J. P. (2017). The Forrester Wave™: Automated Malware Analysis Solutions. Forrester.

Marat, A. (2023). Risks of using Public Wi-Fi. International Journal of Innovative Science

and Research Technology, 1-4.

MinTIC. (2023). Guía de Ciberseguridad para Entidades Públicas y Privadas.

Mishra, S. (2024). 5G Security Challenges & Solutions: A Comprehensive. https://ijrti.org/papers/2405076.pdf

Mishra, S., & Rathore, P. (2024). 5G Security Challenges & Solutions: A Comprehensive Survey. IJRTI, 1-15.

Muñoz Hernández, H., Zapata Cantero, L. G., Requena Vidal, D. M., & Ricardo. (2019). Redalyc. Riesgos informáticos y alternativas para: https://www.redalyc.org/articulo.oa?id=29063446029

NIST. (2018). Framework for Improving. National Institute of Standards and Technology, 1-55.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. National Institute of Standards and Technology, 2-50.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity. https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

ONF. (2015). SDN & NFV Security Solutions. https://opennetworking.org/news-and-events/press-releases/the-open-networking-foundation-and-the-open-networking-summit-announce-sdn-solutions-showcase-categories-and-participants/

Owoko, W. (24). Exploring the technological advancements and security issues of 5G . World Journal of Advanced Research and Reviews, 2-4.

Özyilmaz. (2025). Lineamientos Educativos de Bre-B. Banco de la republica .

Patel, Y., Rawal, B. S., & Rahman, L. (2021). Security and Privacy Challenges in 5G-enabled Technology. IEE CSCLOUD.

Penttinen, J., & GSMA. (2021). 5G Security: Use Cases y Best Practices. T-ISAC.

Publica, F. (2009). Ley 1273 de 2009. Funcion publica: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

PWC. (2024). Global Digital Trust Insights de 2024 de PwC Colombia. PricewaterhouseCoopers.

Quirós-García, E. (21 de Junio de 2021). Universidad de costa rica. La huella digital y la protección de datos: su impacto en las culturas de alto contexto y alto control de incertidumbre en Latinoamérica: https://www.redalyc.org/journal/666/66671361007/

RGPD. (2016). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. Harvard University Press.

Rojas-Díaz, J. J.-L. (2022). Panorama de riesgos por el uso de la tecnología en América Latina. Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Rojas-Díaz, J. S., & Yepes-Londoño, J. J. (2022). Panorama de riesgos por el uso de la tecnología en América Latina. Trilogia ciencia tecnologia sociedad.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture. National Institute of Standatd and technology.

SAFA J. ALTAHA, A. A. (2024). A Survey on Android Malware Detection. IEEE Access, 1-24.

Sahni, I. (2022). A Systematic Literature Review on 5G Security. arvix, 1-8.

Sangrà, A. V. (2012). Hacia una definición de blended learning: Revisión fundamental de la literatura. En A. V. Sangrà, Hacia una definición de blended learning: Revisión fundamental de la literatura (págs. 1-26). Universities and Knowledge Society Journal.

Sangwan, A. A. (2022). A Comprehensive Review of DDoS Attack, Types and Mitigation Techniques in the Internet of Things Network. International Journal for Modern

Trends in Science and Technology, 72-79.

Santa, R. (2024). Colombia entregó espectro para despliegue del 5G. https://www.tvyvideo.com/novedades/ultimas-noticias/21-empresas/21102-colombia-entrego-espectro-para-despliegue-del-5g.html

Schneier, B. (2015). Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. W. W. Norton & Company. New york Times.

Seguridad, R. (8 de Septiembre de 2023). Red Seguridad. Amenaza, vulnerabilidad y riesgo: Diferencias en ciberseguridad: https://www.redseguridad.com/actualidad/diferencias-vulnerabilidad-amenaza-riesgo-seguridad-ti_20230908.html

Sheng, Z., Zhicheng Chen, S. G., Huang, H., Gu, G., & Huang, J. (2025). LLMs in Software Security: A Survey of Vulnerability Detection Techniques and Insights. Cornel Univesity, 2-30.

Shi, W. &. (2016). Edge computing: Vision and challenges. IEEE Internet of Things Journal, 3(5), 637-646.

SIC. (2023). Guía para el Tratamiento de Datos Personales.

SIC. (2023). Informe sobre Protección de Datos Personales en el Sector Financiero. https://www.sic.gov.co/content/sobre-la-protecci%C3%B3n-de-datos-personales

Siemens, G. (2005). Connectivism: A Learning Theory for the Digital Age. International Journal of Instructional Technology and Distance Learning.

Singh, R. K. (2020). A comprehensive survey on 5G security: Current status and future challenges. Journal of Network and Computer Applications, 155.

Solove. (2008). Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos . Harvard University Press.

SSC, P. (2022). Payment Card Industry Estándar de Seguridad de Datos. PCI Security Standards Council, LLC.

Sun:, P., Wan, Y., Fang, Z., & Li, Q. (2024). Una encuesta sobre cuestiones de privacidad y seguridad en entornos basados en IoT: tecnologías, medidas de protección y direcciones futuras. Computers & Security.

Taloba, A. E.-S.-K. (2021). Security aspects in 5G network slicing: A survey. Future Generation Computer Systems.

Tecnologías, T. (2024). Ciberseguridad e IoT. https://blog.tenea.com/ciberseguridad-e-iot/

Teldat. (2024). Redes 5G – Amenazas y Soluciones de Ciberseguridad. https://www.teldat.com/es/blog/redes-5g-amenazas-en-ciberseguridad/

Topaz. (2025). https://www.topazevolution.com/es/blog/ciberataques-bancarios-en-latinoamerica?hsLang=es

Torres, T. A. (05 de 11 de 2024). Emprendedor denuncia nueva modalidad de estafa por Transfiya de la que casi fue víctima: ‘Uno no se da ni cuenta’. EL TIEMPO: https://www.eltiempo.com/cultura/gente/emprendedor-denuncia-nueva-modalidad-de-estafa-por-transfiya-de-la-que-casi-fue-victima-uno-no-se-da-ni-cuenta-3396993

TransUnion. (24 de Octubre de 2024). TransUnion. 43.5% crecen los intentos de fraude digital en Colombia.

Tulsa, U. d. (22 de Enero de 2024). Tulsa University : https://online.utulsa.edu/blog/5g-security-risks-and-solutions/

UDELAR, F. (2014). Bases de datos.

Valdovinos, I. A., Choo, K.-K. R., Pérez, J. a., & Botero, J. F. (2021). Emerging DDoS attack detection and mitigation strategies in software-defined networks: Taxonomy, challenges and future directions. Journal of Network and Computer Applications .

Varalakshmi, D., S, A., Baheti, A., & Dugar, P. (2024). Cyber security in digital payments: An empirical study. Asian Journal of Management and Commerce , 305-310.

Vargas, M. Á. (2021). Ciberseguridad en las redes móviles de telecomunicaciones y su gestión de riesgos. Redalyc.

Ventures, C. (2023). Cybersecurity Ventures. de Cybercrime Magazine: The Official Cybersecurity Magazine: https://cybersecurityventures.com/

Ward, M., & Subramanian, S. (2022). Deloitte. Cybersecurity Study: https://www2.deloitte.com/us/en/insights/industry/public-sector/2022-deloitte-nascio-study-cybersecurity-post-pandemic.html

Xygeni. (7 de Febrero de 2025). Xygeni. Razones por las que se producen vulnerabilidades de seguridad en el software: https://xygeni.io/es/blog/reason-why-security-vulnerabilities-in-software-occur/

Y. Yang, L. W. (2017). "A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journa.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Zuluaga, J. A., & Moreno, S. D. (2024). Desafíos Regulatorios, Financieros y Tecnológicos que enfrentan las Fintech en el. Universidad EAN, 18-35.