# La tecnología 5G, amenazas para la seguridad y oportunidades para los sistemas de información.

**Autor: Fernández Fernández, Francisco Jesús.**

**Director/es: Fernández Gavilanes, Milagros y Fondo Ferreiro, Pablo.**

Contacto: mfgavilanes@cud.uvigo.es/externo.pfondo@cud.uvigo.es/jesusfdez609@outlook.com

---

**Resumen:** El estudio desarrolla las amenazas para la seguridad que supone el uso de la tecnología 5G, tanto para usuarios particulares como de las organizaciones, para después proponer medidas que las mitiguen. También se describen las oportunidades de uso que supone el empleo de esta tecnología.

El organismo de estandarización 3GPP (3rd Generation Partnership Project) desarrolla los estándares de comunicación móvil incluyendo la tecnología 5G, detallando el acceso al espectro radio, la estructura de la red de comunicaciones y las capacidades de los servicios, a fin de definir un sistema completo para estas comunicaciones. El estándar 5G no solo es desarrollado por este organismo, sino que también se ve modificado periódicamente, puesto que es un estándar en constante evolución. Otro organismo, el ETSI (European Telecommunications Standards Institute) publica los estándares de 5G aplicables que deben cumplirse cuando se despliegan estas redes en ámbito europeo.

Adicionalmente, las amenazas para la seguridad derivadas de su uso pueden ser explotadas con fines delincuenciales, estableciendo una desventaja tecnológica con los usuarios desconocedores de las vulnerabilidades. Este desajuste debe ser enmendado por los diferentes actores, pues podría llegar un momento en el que las capacidades de la tecnología sean tan superiores que si la gestión de la seguridad sigue basada en sistemas tradicionales, demostraría ser ineficiente e insegura.

Pero el uso de 5G supone una mejora en las capacidades de uso de las comunicaciones de las organizaciones, lo que implica el aprovechar una serie de oportunidades para proporcionar nuevas funcionalidades a los sistemas de información dedicados a la Seguridad y Defensa, así como los utilizados por el resto de la sociedad.

Por todo ello, los datos masivos de comunicación, ya sea entre dispositivos industriales M2M (machine to machine), IoT (internet of things), o las comunicaciones entre dispositivos

móviles de uso generalizado (smartphones, tablets, portátiles, etc.), van a cambiar el escenario de los grandes volúmenes de datos que se pueden explotar para diferentes propósitos, además de mejorar las comunicaciones.

**Palabras clave:** 5G, Seguridad, IoT. Amenazas, Oportunidades.

---

## 1. Introducción

La tecnología 5G representa un avance significativo en las comunicaciones móviles, pero su cambio hacia infraestructuras virtualizadas y su previsible impacto en actividades críticas hacen que la gestión de la seguridad sea crucial. Un estudio sobre las implicaciones de seguridad en 5G y sus aplicaciones en sistemas de información se vuelve esencial, dada la rápida expansión de esta tecnología en comparación con generaciones anteriores de redes móviles. La importancia radica en garantizar la correcta gestión de la seguridad de la información para evitar riesgos que podrían afectar los desarrollos que utilicen 5G.

El despliegue de esta tecnología presenta diversos desafíos y riesgos de seguridad que deben abordarse de manera integral. La capacidad mejorada de conectividad y la densidad de dispositivos aumentan la superficie de ataque, especialmente con la incorporación masiva de dispositivos IoT. La relevancia crítica de 5G en infraestructuras esenciales como redes eléctricas y sistemas de transporte implica que cualquier ataque o vulnerabilidad podría tener consecuencias graves. Además, las nuevas tecnologías introducidas, como la NFV (virtualización de funciones de red) y la segmentación de red, brindan beneficios, pero también plantean desafíos de seguridad que deben abordarse.

La dependencia de software y las interfaces abiertas aumentan el riesgo de vulnerabilidades y ataques. La protección de la privacidad de los datos se vuelve crucial, dada la cantidad y sensibilidad de la información transmitida. El cumplimiento de regulaciones y normativas, como el Real Decreto-Ley 7/2022 en España [1], es esencial para mitigar riesgos. Finalmente, los riesgos de seguridad de 5G no solo afectan la esfera tecnológica, sino que también tienen implicaciones a nivel nacional, requiriendo un enfoque estratégico y coordinado para abordarlos desde una perspectiva de Seguridad Nacional.

Por todas estas razones, es fundamental que la industria, los organismos reguladores, los gobiernos y los investigadores de seguridad continúen colaborando para identificar, evaluar y mitigar los riesgos de seguridad asociados con las redes 5G.

La especificación del standard está desarrollada por el consorcio 3GPP (3rd Generation Partnership Project) [2], utiliza un método estructurado denominado “Release” [3] para desarrollar y lanzar actualizaciones y mejoras en la tecnología 5G. Cada Release representa un conjunto coherente de especificaciones técnicas y estándares que definen las capacidades, características y mejoras de la tecnología móvil. En el momento del desarrollo de este trabajo, la última versión cerrada del estándar es la Release 18, se está trabajando en fijar la Release 19 para el 2024.

La Agencia de la Unión Europea para la Ciberseguridad-ENISA publica el informe “Enisa Threat Landscape for 5G Networks” [4], dentro de la hoja de ruta de gestión del riesgo en 5G, tras analizar las amenazas. En 2020 se publica la 5G toolbox, orientada a mitigar los riesgos derivados de estas amenazas.

### *1.1. Hipótesis*

La hipótesis enuncia que el estado actual de la seguridad en los desarrollos de redes actuales es insuficiente para implantar soluciones 5G de forma sólida y robusta. Es necesario contar con el probable desarrollo de paquetes de amenazas que puedan atacar a estas nuevas soluciones, así como paquetes de medidas que las puedan mitigar. Además, existe una oportunidad de mejora en los sistemas de información para la Defensa y la Seguridad.

### *1.2. Objetivos.*

Proporcionar una comprensión detallada de las redes de comunicación, centrándose en las redes 5G, delineando su operación, beneficios y aplicaciones. Además, se debe realizar un estudio exhaustivo sobre las amenazas de seguridad vinculadas a la tecnología 5G, proponiendo medidas efectivas de mitigación. Simultáneamente, se busca identificar oportunidades para enriquecer los sistemas de información dedicados a la Seguridad y Defensa mediante la integración de nuevas funcionalidades.

### *1.3. Relación entre Hipótesis y Objetivos*

Los objetivos específicos, derivados de la contextualización de la tecnología 5G y sus futuros desarrollos, constituyen la base esencial para comprender el ecosistema completo, identificar oportunidades y amenazas, y finalmente confirmar la hipótesis planteada. La relación intrínseca entre los objetivos y la hipótesis se destaca al estudiar amenazas específicas del 5G, demostrando la insuficiencia de las medidas de seguridad móvil previas y la necesidad de nuevas estrategias de mitigación. Asimismo, partiendo de los sistemas de información actuales de Defensa y Seguridad, se busca respaldar la idea de posibles oportunidades de mejora en dichos sistemas.

### *1.4. Importancia de la Investigación*

Un estudio como el presente trabajo es esencial para anticipar y mitigar riesgos de seguridad en la tecnología 5G, que está rápidamente convirtiéndose en el estándar para la comunicación móvil, impactando principalmente en los sectores de Seguridad y Defensa. La investigación sobre la seguridad en redes 5G es crucial debido a la interconexión más amplia y compleja de dispositivos, aumentando la superficie de ataque y exigiendo garantías de integridad, confidencialidad y disponibilidad de datos. La implementación de tecnologías emergentes, como IoT y la inteligencia artificial, intensifica la importancia de la seguridad, especialmente para dispositivos conectados, como vehículos autónomos y dispositivos médicos. Desde una perspectiva económica, la confianza en las redes 5G es crucial para fomentar la inversión y el desarrollo, ya que las brechas de seguridad podrían afectar negativamente a la adopción de la tecnología, desacelerando el progreso y teniendo un impacto devastador en la economía global.

## 2. Desarrollo

El trabajo comienza con el estudio de las diferentes tecnologías, resumidas en la Figura 1, donde se observa la evolución en la capacidad del ancho de banda de descarga de datos [6].

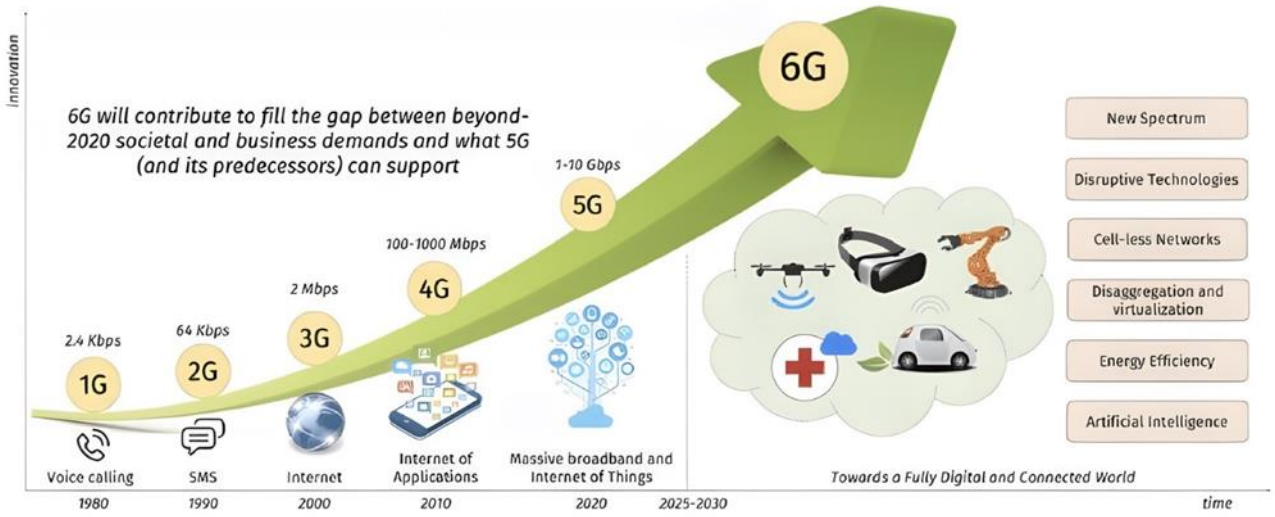


Figura 1. Evolución de las tecnologías de comunicación móviles [6].

Como se observa, las distintas generaciones han experimentado una evolución significativa a lo largo del tiempo, desde sus primeras formas hasta las tecnologías avanzadas actuales. Este desarrollo ha sido impulsado por la demanda creciente de mayor velocidad, capacidad y eficiencia en la transmisión de datos.

El estándar 5G tiene como objetivo principalmente el mejorar la calidad del servicio, especialmente en situaciones donde la latencia es crítica, lo que permite nuevos flujos de datos. Se establece una nueva arquitectura en la que las instancias cercanas a los clientes funcionan como una red local mediante la tecnología Edge Computing. Estas instancias utilizan el núcleo de red del operador, para facilitar comunicaciones a larga distancia.

En las redes 5G, el modelo de confianza se fundamenta en dos elementos esenciales: el SUPI (Subscription Permanent Identifier) y el SUCI (Subscription Concealed Identifier). El SUPI, un identificador único permanentemente asociado a la suscripción del usuario, contiene información crucial para la autenticación y configuraciones de seguridad, actuando como identificador principal durante las comunicaciones con la red. En contraste, el SUCI, un identificador temporal, salvaguarda la privacidad del usuario al ocultar el SUPI real, especialmente en la etapa inicial de conexión. Este enfoque protege la privacidad al limitar la exposición de información sensible en transacciones específicas, reduciendo así el riesgo de seguimiento no autorizado.

El proceso de confianza implica la interacción entre la USIM (Universal Subscriber Identity Module), donde se almacenan los parámetros necesarios para configurar el SUPI y el SUCI, y el núcleo de la red en el UDM (Unified Data Management), con autenticación de credenciales o ARPF (Authentication Credential Repository and Processing Function).

Como resultado de los parámetros de confianza, el proyecto SMARTER del 3GPP, iniciado en 2015, se centró en definir aplicaciones clave para la tecnología 5G, generando más de 70 casos de uso categorizados en tres grupos. Estos grupos incluyen eMBB (Enhanced Mobile Broadband) para aplicaciones basadas en datos con altas velocidades de datos y amplia cobertura, URLLC (Ultra-Reliable and Low Latency Communications) para casos de uso críticos que requieren baja latencia y alta confiabilidad, como cirugía a distancia y vehículos autónomos, y mMTC/MIoC (Massive Machine Type/Inernet of Things Communications) para soportar un gran número de dispositivos en un área

pequeña, típicamente asociados con IoT. Los casos de uso se caracterizan por los atributos de rendimiento necesarios para cada categoría.

Posteriormente ENISA en su Threat Landscape for 5G Networks Report [7] listó una serie de vulnerabilidades encontradas a partir de los puntos descritos anteriormente con detalles de cada una de las vulnerabilidades y los sistemas que afecta. También se intentó describir cómo estas vulnerabilidades se pueden explotar en ciberamenazas y cómo se pueden mitigar estas amenazas a través de controles de seguridad.

El informe de ENISA destaca las consideraciones de seguridad para diversos conjuntos de activos en redes 5G. Se señala que en la RAN (Radio Access Network), es esencial asegurar la latencia para aplicaciones críticas, aunque persiste la vulnerabilidad a ataques de denegación de servicio basados en perturbación de señales (jamming), y presenta una exposición significativa a ataques físicos. En el núcleo de red, los componentes hardware y software, junto con los procesos, son fuentes inherentes de vulnerabilidad, subrayando la importancia de la integración y la cadena de suministro como fuentes de riesgo. Para NFV (Network Function Virtualization), se destaca que la virtualización puede brindar una falsa sensación de seguridad, ya que el equipo donde se ejecuta el software de virtualización, dicho software y el hipervisor, pueden comprometerse si se descubren vulnerabilidades.

En SDN (Software-Defined Networking), se resalta que, además de los riesgos asociados con la virtualización, la alta exposición de estos sistemas debe manejarse cuidadosamente, especialmente cuando están ubicados en instancias de terceros. Finalmente, en NSI (Network Slicing Instance), se subraya la seguridad proporcionada por la segmentación, pero se advierte sobre la importancia de prestar atención a las interfaces de gestión, las tecnologías de cifrado y la gestión de claves.

## 3. Resultados y discusión

Se ha concluido que las aplicaciones finales más importantes que ya se están desplegando sobre redes 5G, y que se agrupan dentro de los casos de uso definidos por 3GPP son las mostradas en la Figura 2 [5].


Figura 2. Workplan de aplicaciones basadas en 5G según el 3GPP [5].

La tecnología 5G promete transformar diversos sectores con sus aplicaciones innovadoras. En el ámbito de los vehículos autónomos, la comunicación casi instantánea se vuelve esencial para reacciones en tiempo real a su entorno. En ciudades inteligentes, la infraestructura y la gestión del tráfico se beneficiarán de la comunicación bidireccional entre vehículos y la infraestructura, mejorando la seguridad en el transporte. En la automatización industrial, 5G posibilitará una automatización completamente inalámbrica, permitiendo fábricas más eficientes y el control de máquinas en tiempo real.

Para la realidad aumentada y virtual, 5G mejorará la inmersión y participación, siendo aplicable en sectores industriales para tareas como reparación y mantenimiento. En el ámbito de los drones, 5G ampliará los límites en alcance e interactividad, impactando en áreas como búsqueda y rescate, seguridad fronteriza y servicios de entrega mediante drones. La integración de inteligencia artificial se acelerará gracias a 5G, siendo esencial para servicios como seguridad inteligente y predicciones por máquinas tras ejecutar autoaprendizaje.

La conexión masiva de dispositivos IoT permitirá la recopilación y análisis de datos a gran escala. Además, 5G será crucial para servicios que requieren comunicación confiable y rápida, como los servicios de emergencia. Para el entretenimiento y formación, 5G ofrecerá experiencias de juego más inmersivas y aplicaciones de realidad virtual innovadoras. En aplicaciones industriales diversas, como salud, comercio, agricultura, manufactura y logística, 5G desempeñará un papel transformador, permitiendo desde dispositivos portátiles de alerta médica hasta la automatización de fábricas y la gestión en tiempo real de inventarios y procesos industriales.

Los resultados fundamentales derivados del análisis son diversos y destacan aspectos clave en la implementación del 5G. En primer lugar, se resalta el impacto transformador del 5G, considerándolo como una evolución crítica en las redes de comunicación, con el potencial de alterar significativamente la sociedad y la economía. Sin embargo, se subraya la necesidad de equilibrar las oportunidades que ofrece con nuevos desafíos de seguridad, señalando la importancia de abordar estos riesgos de manera proactiva y con estrategias bien definidas, como requisito fundamental para aprovechar plenamente los beneficios del 5G y mitigarlos.

Por ello, se subraya el papel del 5G como catalizador de la innovación y la transformación digital en diversos sectores, especialmente en áreas críticas como la Defensa y la Seguridad. Para una implementación exitosa, destaca la necesidad de estrategias de seguridad sólidas, la adopción de mejores prácticas y un enfoque en la capacitación y concienciación sobre los desafíos y oportunidades inherentes al 5G.

## 4. Conclusiones

Las conclusiones destacadas del análisis sobre el 5G enfatizan su impacto transformador en las redes de comunicación, presentando capacidades innovadoras que pueden remodelar la sociedad y la economía. Sin embargo, se subraya la necesidad de abordar los desafíos asociados con estas oportunidades, la importancia del equilibrio entre las oportunidades y la seguridad se destaca resaltando que la implementación exitosa del 5G requerirá estrategias proactivas y bien definidas. Se enfatiza la colaboración continua entre la industria, la academia y los reguladores, así como la adopción de estándares de seguridad globales.

El 5G se identifica como un catalizador para la innovación y la transformación digital, especialmente en sectores críticos como Defensa y Seguridad. Como recomendaciones estratégicas, se aconseja la implementación de sistemas basados en 5G mediante estrategias de seguridad sólidas, adopción de mejores prácticas y un enfoque en la capacitación y concienciación sobre los desafíos y oportunidades asociados con esta tecnología.

Finalmente, se detallan una serie de recomendaciones propuestas por el autor, clasificadas en varias categorías. Para garantizar la *seguridad en la implementación de redes 5G*, se enfatiza la adopción de estándares y buenas prácticas de seguridad, siguiendo directrices de organizaciones como 3GPP, ENISA, ETSI y la legislación nacional. La evaluación y gestión de riesgos se considera crucial,

abordando vulnerabilidades en hardware, software, interfaces y la infraestructura de red mediante evaluaciones regulares.

La actualización constante de sistemas y dispositivos con las últimas medidas de seguridad es esencial, dado la dinámica de los vectores de amenazas. Se insta a desarrollar una estrategia de resiliencia de red, implementando redundancia y sistemas de detección y respuesta a intrusiones. La capacitación y concienciación del personal se identifican como defensas clave contra ciberataques. Integrar la seguridad desde el diseño, monitorizar y analizar el tráfico de red en tiempo real, así como colaborar en redes de intercambio de información, son recomendaciones adicionales para fortalecer la seguridad.

La planificación de la continuidad del negocio y la recuperación ante desastres se destaca como medida esencial para minimizar interrupciones en caso de incidentes de seguridad o fallos de red. Siguiendo estas recomendaciones, las administraciones e instituciones pueden fortalecer su seguridad y aprovechar plenamente las capacidades avanzadas que ofrece la tecnología 5G en los sistemas de información.

Para una *exitosa y eficiente implantación de sistemas de información*, se enfatiza la necesidad de realizar una evaluación exhaustiva de las necesidades y requisitos específicos del sistema de información, considerando factores clave como volumen de datos, velocidad requerida y latencia. El diseño cuidadoso de la infraestructura basada en 5G es crucial, seleccionando hardware y software apropiados, planificando la cobertura y considerando la integración con redes existentes. Se sugiere la realización de pruebas piloto y un despliegue gradual para identificar posibles problemas y facilitar una transición escalonada.

La capacitación del personal, tanto en tecnologías 5G como en nuevas aplicaciones, es esencial, incluyendo a los usuarios finales. La integración sin problemas con sistemas existentes y la gestión robusta de seguridad y privacidad de datos son aspectos críticos. Se recomienda establecer un sistema de monitorización y soporte continuo para resolver rápidamente problemas y garantizar la alta disponibilidad. Mantener una evaluación y actualización continua del rendimiento de la red y las aplicaciones es clave para identificar áreas de mejora y adaptarse a nuevas tecnologías y estándares, asegurando la relevancia y eficacia del sistema a lo largo del tiempo.

Para maximizar las oportunidades que ofrece el 5G en *sistemas de información con aplicaciones de Defensa y Seguridad*, se enfatiza el desarrollo de sistemas de comunicación seguros y encriptados que capitalicen la alta velocidad y baja latencia del 5G, especialmente para operaciones tácticas y estratégicas en defensa, seguridad ciudadana y gestiones de crisis. La ciberseguridad se identifica como un elemento crucial, dada la apertura a nuevos posibles ataques cibernéticos dirigidos especialmente a estas estructuras por parte de actores interesados en fines de desestabilización o amenazas híbridas. La colaboración entre el sector público y privado se subraya para desarrollar soluciones innovadoras aprovechando el 5G. Asegurarse de que las implementaciones cumplan con estándares internacionales es esencial para garantizar la compatibilidad y seguridad.

Se destaca la importancia de la capacitación y concienciación del personal integrante de los colectivos de Defensa y Seguridad sobre los riesgos y beneficios del 5G. La integración del 5G con tecnologías emergentes como inteligencia artificial, drones y vehículos autónomos se propone para mejorar la vigilancia, reconocimiento y capacidad de respuesta en situaciones de conflicto, gestión de crisis o de mantenimiento de la seguridad. Utilizar la capacidad del 5G para programas de

entrenamiento avanzado, simulaciones realistas, y mejoras en la logística y gestión de recursos militares y civiles se considera vital. También se resalta el potencial del 5G para mejorar los servicios de emergencia, facilitando comunicaciones más rápidas y efectivas en gestión de crisis, así como su aplicación en sistemas de transporte inteligente para mejorar la seguridad vial y movilidad urbana.

Para finalizar, la hipótesis de este trabajo, que enfatiza la insuficiencia de la seguridad en las soluciones de redes actuales para la implantación robusta de tecnologías 5G, ha sido comprobada a través de un análisis del estado de tecnologías actuales y planteadas en redes que utilizarán éste estándar. Se han identificado y analizado las lagunas existentes en los sistemas de seguridad actuales, evidenciando la necesidad de implantar nuevas estrategias y enfoques para enfrentar los desafíos únicos que presenta el 5G. Este resultado resalta la importancia de una evolución continua dada la evolución de las amenazas, y los desarrollos para mitigarlas, especialmente en el contexto de la Seguridad y Defensa Nacional.

## Referencias


1. Jefatura del Estado, Real Decreto-Ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación, vol. BOE-A-2022-4973. 2022, pp. 41546-41564. [En línea]. Disponible en: https://www.boe.es/eli/es/rdl/2022/03/29/7
2. «3GPP – The Mobile Broadband Standard», 3GPP. [Internet]. [8 Nov 2023]. https://www.3gpp.org/
3. «The 3GPP's System of Parallel Releases», 3GPP. [Internet]. [8 Nov 2023] https://www.3gpp.org/specifications-technologies/releases
4. «ENISA Threat Landscape for 5G Networks Report», ENISA. [Internet]. [12 Nov 2023] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks
5. «5G Applications and Use Cases». [Internet]. [12 Nov 2023] https://www.digi.com/blog/post/5g-applications-and-use-cases
6. K. Vaigandla, S. Bolla, y R. Karne, «A Survey on Future Generation Wireless Communications-6G: Requirements, Technologies, Challenges and Applications», International Journal of Advanced Trends in Computer Science and Engineering, vol. 10, pp. 3067-3076, oct. 2021, doi: 10.30534/ijatcse/2021/211052021.
7. «ENISA Threat Landscape for 5G Networks Report», ENISA. [Internet]. [10 Nov 2023] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks