INSTITUTO DE CIBERDEFENSA DE LAS UERZAS ARMADAS

DIPLOMATURA UNIVERSITARIA EN GERENCIAMIENTO DE LA CIBERDEFENSA NOVIEMBRE DE 2024

TRABAJO FINAL INTEGRADOR

TEMA: Regulación del Espectro Electromagnético para el despliegue de redes 5G

TÍTULO: Regulación del Espectro Electromagnético para el Despliegue de Redes 5G en Argentina: Desafíos y Oportunidades para la Ciberdefensa

AUTORES:

- Licenciado en Administración, Especialista en Estrategia Operacional y Planeamiento Militar Conjunto, MAYOR (EA) LUCAS EVARISTO AGUIRRE
- Licenciado en Administración, MAYOR (EA) GERARDO HUGO ALMADA
- Licenciado en Sistemas Aéreos y Aeroespaciales, CAPITÁN (FAA) NICOLÁS ALVAREZ
- Titulo Analista en sistema TENIENTE PRIMERO (EA) VICTOR GIMENEZ

Resumen

El despliegue de redes 5G en Argentina presenta un nuevo paradigma en las telecomunicaciones, con el potencial de transformar la sociedad y la economía. Sin embargo, esta tecnología también trae consigo desafíos significativos en términos de ciberseguridad, especialmente en lo que respecta a la gestión del espectro electromagnético.

Este trabajo final integrador analiza la seguridad de las redes 5G en Argentina, con un enfoque particular en la regulación del espectro y su impacto en la ciberdefensa. Se examinan las vulnerabilidades inherentes a la tecnología 5G, como la expansión de la superficie de ataque, la complejidad de la infraestructura y la dependencia de proveedores externos. Asimismo, se analizan las amenazas a la ciberseguridad, incluyendo la interferencia, los ataques de denegación de servicio y el acceso no autorizado al espectro.

Se destaca la importancia de una gestión eficiente del espectro electromagnético para garantizar la seguridad y la resiliencia de las redes 5G. Se proponen medidas para fortalecer la ciberdefensa en este ámbito, incluyendo la asignación eficiente del espectro, el monitoreo y control, la protección contra interferencias y la cooperación internacional.

Este trabajo busca contribuir al desarrollo de un marco regulatorio sólido para el despliegue de redes 5G en Argentina, que permita aprovechar las oportunidades de esta tecnología mientras se mitigan los riesgos para la ciberseguridad y se protege la infraestructura crítica del país.

Palabras clave

Redes 5G, ciberdefensa, Espectro Electromagnético, regulación, infraestructura crítica.

Índice

Introducción 3

Capítulo I: Redes 5G su impacto en la ciberdefensa, riesgos y vulnerabilidades 6

1.1. Características de la tecnología 5G 7

1.2. Bandas de frecuencia a utilizar en la tecnología 5G. 8

1.3. Importancia del EEM para el rendimiento y la seguridad de la red. 8

1.4. Ciberdefensa en el contexto militar: Una mirada nacional e internacional 9

1.5. Explicación de la ciberdefensa en el contexto militar: 10

Capítulo II: Vulnerabilidades y amenazas de las redes 5G 14

2.1. Vulnerabilidades inherentes a la tecnología 5G 14

2.2. Interferencias de la red 5G en Argentina. 18

2.3. Ataques de denegación de servicio (DoS) que afectan el espectro donde trabaja la banda de 5G en Argentina. 20

2.4. Acceso no autorizado al espectro en Argentina: un desafío para la ciberdefensa de las redes 5G. 22

2.5. Amenazas a la ciberseguridad en 5G en Argentina. 23

Capítulo III: Casos de estudio (Interferencias y acceso no autorizado en Argentina) 26

3.1. Caso 1: Interferencia en la banda de 3.5 GHz: 26

3.2. Caso 2: Acceso no autorizado a la banda de 2.6 GHz: 28

3.3. Propuestas de mejora: Regulación del espectro para la ciberdefensa de las redes 5G en Argentina. 29

3.4. Asignación eficiente del espectro. 30

3.5. Monitoreo y control del espectro. 31

3.6. Mecanismos de protección contra interferencias. 31

3.7. Cooperación internacional en la gestión del espectro. 32

Conclusiones 34

Bibliografía 35

Introducción

La llegada de la tecnología 5G representa un hito en la evolución de las telecomunicaciones, con la promesa de transformar la manera en que nos conectamos, comunicamos y llevamos a cabo nuestras actividades cotidianas. Con velocidades de transferencia de datos significativamente mayores que las redes 4G y una latencia considerablemente reducida, las redes 5G están diseñadas para soportar una conectividad masiva, permitiendo la interconexión de millones de dispositivos, ENACOM (2023). Este avance tecnológico abre un abanico de posibilidades para el desarrollo de aplicaciones innovadoras como el Internet de las Cosas (IoT), la automatización industrial, la telemedicina y los vehículos autónomos, que dependen de una red confiable y rápida.

Sin embargo, la adopción de la tecnología 5G también trae consigo desafíos importantes en términos de ciberseguridad, Observatorio Argentino del Ciberespacio (2021). La complejidad de la infraestructura 5G, la expansión de la superficie de ataque y la interdependencia de los sistemas la convierten en un objetivo atractivo para cibercriminales y actores maliciosos. A medida que aumenta el número de dispositivos conectados a la red, también lo hace el número de puntos vulnerables, lo que dificulta la protección de la información y la garantía de la privacidad de los usuarios.

La transmisión de datos a través de múltiples dispositivos y sistemas en las redes 5G puede facilitar el acceso no autorizado a información sensible, generar ataques a infraestructuras críticas y amenazar la seguridad nacional Cartujo (2024). Además, la dependencia de proveedores externos de tecnología introduce preocupaciones sobre la soberanía tecnológica y la seguridad de los datos.

En este contexto, la regulación del espectro electromagnético se vuelve crucial para el despliegue seguro y eficiente de las redes 5G. El espectro es un recurso finito y esencial para las comunicaciones inalámbricas, y su gestión eficiente es fundamental para garantizar la calidad del servicio, la seguridad y la ciberdefensa. Una regulación adecuada del espectro permite la asignación eficiente de frecuencias, la prevención de interferencias y la protección contra el uso malicioso del espectro.

En el contexto argentino, el despliegue de redes 5G representa una oportunidad para fortalecer la ciberdefensa del país. Sin embargo, esto requiere un enfoque integral que incluya la creación de políticas públicas que regulen el uso de la tecnología 5G, la inversión en capacitación de profesionales en ciberseguridad y la promoción de la investigación y el desarrollo de soluciones locales.

Un aspecto fundamental para fortalecer la ciberdefensa en el marco de la tecnología 5G es la necesidad de establecer estándares de seguridad desde el inicio del despliegue de la red. Esto implica que las empresas y organismos gubernamentales trabajen en colaboración para crear un marco normativo que garantice la integridad de los datos y la privacidad de los usuarios. La implementación de tecnologías avanzadas, como la segmentación de red (network slicing) y el uso de inteligencia artificial para la detección y respuesta a amenazas en tiempo real, puede mejorar significativamente la capacidad de respuesta ante incidentes de seguridad cibernética Amézquita Murillo (2024).

La colaboración internacional también es crucial en el contexto de la ciberdefensa. Argentina puede beneficiarse de alianzas con otros países para compartir información sobre amenazas cibernéticas, desarrollar capacidades técnicas y establecer buenas prácticas en la gestión de la seguridad de redes 5G.

La creciente preocupación por la privacidad de los datos también debe ser considerada al abordar la seguridad de las redes 5G. Es esencial que Argentina establezca marcos legales que protejan los derechos de los usuarios y eviten abusos en la recolección y el manejo de datos Ley 25.326 (2000).

En resumen, la implementación de redes 5G en Argentina ofrece una oportunidad única para transformar la forma en que las personas y las organizaciones se conectan y comunican. Sin embargo, este avance también trae consigo desafíos significativos en términos de ciberseguridad que deben ser abordados de manera integral. La creación de un entorno de ciberdefensa robusto, que incluya políticas públicas efectivas, capacitación de profesionales, colaboración internacional y protección de datos, será crucial para garantizar que Argentina pueda aprovechar al máximo las ventajas de las redes 5G mientras protege a su población y su infraestructura crítica.

Este trabajo tiene como objetivo explorar en profundidad estos desafíos y oportunidades, proporcionando un análisis detallado de cómo Argentina puede construir una ciberdefensa sólida en el contexto de la seguridad de las redes 5G, con especial énfasis en la importancia de la regulación del espectro electromagnético.

En un contexto de creciente interconexión y digitalización, cabe preguntarse:

¿Cómo se puede analizar la seguridad de las redes 5G en Argentina para identificar los principales desafíos y oportunidades que presenta para la ciberdefensa, y qué estrategias se pueden proponer para fortalecer la protección de la infraestructura crítica y los datos de los usuarios, considerando la importancia de la regulación del espectro electromagnético? La respuesta a esta pregunta permitirá guiar acciones para mantener o

modificar la situación actual, así como proponer directrices que requieran investigaciones futuras.

Si bien la tecnología 5G ofrece un amplio abanico de posibilidades, este trabajo se centra específicamente en el análisis de su seguridad en el contexto argentino, con un enfoque particular en la regulación del espectro electromagnético y su impacto en la ciberdefensa.

De acuerdo con lo expresado, el objetivo general es analizar la seguridad de las redes 5G en Argentina, con foco en los desafíos para la ciberdefensa, y proponer estrategias para proteger la infraestructura crítica y los datos de los usuarios, considerando la importancia de la regulación del espectro electromagnético. A su vez los objetivos específicos son determinar es definir las oportunidades que presenta la tecnología 5G para mejorar las capacidades de ciberdefensa en Argentina, en el contexto de la regulación del espectro electromagnético y determinar las vulnerabilidades y riesgos asociados a la implementación de redes 5G en Argentina, considerando la dependencia en proveedores externos, la expansión de la superficie de ataque y los desafíos en la regulación del espectro.

La investigación correspondiente a este trabajo se llevará a cabo utilizando un método deductivo, con el propósito de cumplir tanto con el objetivo general como con los dos objetivos especifico. Al lograr los objetivos particulares, se podrán obtener conclusiones parciales que contribuirán a responder al objetivo general y, al mismo tiempo, proporcionarán un aporte personal en relación con la temática abordada. En cuanto al diseño de la investigación se empleará un enfoque explicativo, utilizando como técnicas de validación el análisis bibliográfico, documental y lógico. Se hará uso de documentos provenientes de fuentes abiertas.

Capítulo I: Redes 5G su impacto en la ciberdefensa, riesgos y vulnerabilidades

En el siglo XXI, la tecnología de la información y la comunicación han experimentado avances sin precedentes, transformando la manera en que interactuamos con el mundo que nos rodea. Entre estos avances, la tecnología 5G se destaca como una de las innovaciones más disruptivas, con el potencial de revolucionar diversos sectores de la sociedad y la economía.

Las redes 5G ofrecen velocidades de conexión ultrarrápidas, una latencia mínima y una capacidad de conexión masiva, lo que abre un abanico de posibilidades para el desarrollo de aplicaciones innovadoras como el Internet de las Cosas (IoT), la automatización industrial, la telemedicina y los vehículos autónomos son algunos de los ejemplos que podemos encontrar.

Sin embargo, la implementación de la tecnología 5G también plantea desafíos importantes en términos de ciberseguridad. La creciente complejidad de las redes, la expansión de la superficie de ataque y la dependencia de proveedores externos requieren un análisis exhaustivo de las vulnerabilidades y amenazas que enfrentan las redes 5G.

En este contexto, la regulación del espectro electromagnético (EEM) se vuelve crucial para garantizar el despliegue seguro y eficiente de las redes 5G en Argentina. El EEM es un recurso finito y esencial para las comunicaciones inalámbricas, y su gestión eficiente es fundamental para la ciberdefensa, la seguridad nacional y el desarrollo tecnológico del país.

En este capítulo, se analizarán las características principales de la tecnología 5G, su impacto en ámbito de ciberdefensa, los riesgos y vulnerabilidades que presenta, y la importancia de la regulación del EEM para obtener el mejor rendimiento y seguridad en la red. Se examinará el rol de la ciberdefensa en el contexto militar, tanto a nivel nacional como internacional, y se analizarán las oportunidades y desafíos que presenta la tecnología 5G para las Fuerzas Armadas.

Este análisis permitirá comprender el panorama actual de la ciberdefensa en el ámbito de las redes 5G y sentar las bases para el desarrollo de estrategias que permitan proteger la infraestructura crítica y los datos sensibles en este nuevo entorno tecnológico.

1.1. Características de la tecnología 5G

La tecnología 5G representa un avance significativo en las telecomunicaciones, con el potencial de transformar la sociedad y la economía argentina. Sus características principales la diferencian de las generaciones anteriores y la posicionan como una tecnología clave para el futuro digital del país.

1.1.1. Velocidad y capacidad:

- **Velocidad de datos:** 5G ofrece velocidades de descarga y carga de datos significativamente mayores que las redes 4G, alcanzando hasta 10 Gbps en condiciones ideales. Esto permite una experiencia de usuario mucho más rápida y fluida, especialmente para aplicaciones que demandan un gran ancho de banda, como la descarga de archivos multimedia, el streaming de video en alta definición y los juegos en línea.
- **Mayor capacidad:** 5G puede gestionar un mayor número de conexiones simultáneas que las redes anteriores, lo que es fundamental para el desarrollo del Internet de las Cosas (IoT) y la conexión masiva de dispositivos. Esto permitirá la interconexión de millones de dispositivos en áreas urbanas, impulsando la innovación en sectores como la industria, la salud y el transporte.

1.1.2. Latencia ultra baja:

- **Tiempo de respuesta:** 5G reduce significativamente la latencia, es decir, el tiempo que tarda una señal en viajar de un punto a otro de la red. Esto es crucial para aplicaciones en tiempo real, como la telecirugía, los vehículos autónomos y la realidad virtual, donde una respuesta instantánea es fundamental.
- **Comunicaciones ultra confiables de baja latencia (URLLC):** 5G introduce el concepto de URLLC, que garantiza una comunicación con una latencia extremadamente baja y una alta fiabilidad, lo que abre nuevas posibilidades para aplicaciones críticas que requieren una respuesta en tiempo real.

1.1.3. Eficiencia espectral:

- **Uso eficiente del espectro:** 5G utiliza el espectro radioeléctrico de forma más eficiente que las generaciones anteriores, lo que permite una mayor capacidad de transmisión de datos.

- **Tecnologías de acceso:** 5G utiliza nuevas tecnologías de acceso, como Orthogonal Frequency-Division Multiple Access OFDMA y Multiple-Input Multiple-Output (MIMO), que permiten una mejor utilización del espectro y un mayor rendimiento de la red.

1.1.4. Flexibilidad y versatilidad:

- **Virtualización de funciones de red (NFV):** 5G utiliza NFV para virtualizar las funciones de red, lo que permite una mayor flexibilidad y eficiencia en la gestión de la red.
- **Redes definidas por software (SDN):** 5G utiliza SDN para separar el plano de control del plano de datos, lo que facilita la automatización y la gestión centralizada de la red.

1.2. Bandas de frecuencia a utilizar en la tecnología 5G.

En Argentina, el Ente Nacional de Comunicaciones (ENACOM) ha asignado las siguientes bandas de frecuencia para el despliegue de la tecnología 5G:

- **3.5 GHz:** Es la banda principal para 5G, ofreciendo un buen balance entre capacidad y cobertura.
- **2.6 GHz:** También se está utilizando para 5G, complementando la banda de 3.5 GHz.
- **700 MHz y AWS (1.7/2.1 GHz):** Estas bandas de frecuencias más bajas se utilizan para mejorar la cobertura en zonas rurales y ampliar el alcance de la señal 5G.

1.3. Importancia del EEM para el rendimiento y la seguridad de la red.

El Espectro Electromagnético (EEM) es un recurso finito y esencial para las comunicaciones inalámbricas, incluyendo las redes 5G. Su gestión eficiente es crucial para:

- **Maximizar el rendimiento de la red:** Una asignación adecuada del espectro permite optimizar la velocidad, la capacidad y la cobertura de las redes 5G.
- **Prevenir interferencias:** La gestión del EEM ayuda a evitar interferencias entre diferentes servicios y aplicaciones que utilizan el espectro, garantizando la calidad del servicio.

- **Fortalecer la ciberseguridad:** La regulación del espectro es fundamental para prevenir el acceso no autorizado y los ataques que buscan interrumpir las comunicaciones o comprometer la información.

La tecnología 5G en Argentina se caracteriza por su velocidad, capacidad, baja latencia, eficiencia espectral, flexibilidad y versatilidad. La gestión eficiente del espectro electromagnético es crucial para asegurar el rendimiento, la seguridad y la ciberdefensa de las redes 5G en el país.

1.4. Ciberdefensa en el contexto militar: Una mirada nacional e internacional

La ciberdefensa, en términos generales, se refiere al conjunto de medidas y estrategias para proteger los sistemas informáticos, las redes y la información crítica de las amenazas cibernéticas. En el contexto militar, la ciberdefensa adquiere una importancia aún mayor, ya que las fuerzas armadas dependen cada vez más de la tecnología y las comunicaciones para llevar a cabo sus operaciones.

A nivel nacional: En Argentina, la ciberdefensa en el ámbito militar se enmarca en la Estrategia de Ciberdefensa del Ministerio de Defensa, que busca proteger las redes y sistemas informáticos de las Fuerzas Armadas, así como la información sensible relacionada con la defensa nacional. Tiene como objetivos principales Garantizar la disponibilidad, integridad y confidencialidad de la información y los sistemas críticos para las operaciones militares. Detectar, prevenir y responder a los ciberataques de manera oportuna y eficiente. Fortalecer las capacidades de ciberdefensa de las Fuerzas Armadas a través de la capacitación, la inversión en tecnología y la cooperación con otros actores.

A nivel internacional: La ciberdefensa se ha convertido en una prioridad para las fuerzas armadas de todo el mundo. Organizaciones como la OTAN han desarrollado estrategias y capacidades de ciberdefensa para proteger sus infraestructuras críticas y responder a las ciberamenazas de forma coordinada.

La OTAN ha desarrollado un enfoque de "defensa activa" en su estrategia de ciberdefensa, el cual incluye la posibilidad de realizar contraataques en el ciberespacio cuando sea necesario. Este enfoque tiene como objetivo no solo disuadir posibles agresores, sino también proteger sus infraestructuras críticas de ciberataques. A nivel internacional, la cooperación entre países es crucial para el intercambio de información,

la mejora de capacidades y la respuesta coordinada ante las ciberamenazas, lo que permite que los sistemas de defensa se mantengan robustos y actualizados frente a nuevas técnicas de ataque.

Uno de los mayores desafíos de la ciberdefensa en el contexto militar actual es la necesidad de adaptarse a la evolución constante de las ciberamenazas y de las tecnologías que las impulsan. En este sentido, las redes 5G representan tanto una oportunidad como un desafío para la ciberdefensa militar, ya que su implementación permite la mejora en las comunicaciones y el flujo de datos en tiempo real. Esta tecnología ofrece mayor velocidad y capacidad para gestionar operaciones críticas, como el mando y control y la inteligencia, aspectos esenciales para la defensa moderna.

Sin embargo, el despliegue de redes 5G también presenta desafíos específicos. La proliferación de dispositivos conectados a 5G amplía la superficie de ataque, lo que incrementa la cantidad de puntos vulnerables ante posibles amenazas cibernéticas. Además, la complejidad de la infraestructura dificulta la gestión de la seguridad y la detección de amenazas en tiempo real. Otro riesgo considerable es la dependencia de proveedores externos, ya que el uso de tecnología extranjera podría introducir vulnerabilidades que comprometan la ciberdefensa nacional.

La ciberdefensa es un componente esencial de la seguridad nacional en el siglo XXI. Las Fuerzas Armadas deben estar preparadas para enfrentar las ciberamenazas y proteger las infraestructuras críticas que dependen de la tecnología. Las redes 5G presentan nuevas oportunidades y desafíos para la ciberdefensa, y es crucial que Argentina desarrolle estrategias robustas y resilientes para garantizar la seguridad de sus operaciones militares en el ciberespacio.

1.5. Explicación de la ciberdefensa en el contexto militar:

La ciberdefensa en el contexto militar se refiere a las medidas y estrategias que se toman para proteger las redes, sistemas, información y operaciones militares de las amenazas cibernéticas. Esto incluye la protección de la información sensible, la prevención de interrupciones en los sistemas, la garantía de la disponibilidad de las comunicaciones y la seguridad de las operaciones militares.

1.5.1. Conexión de la regulación del EEM con la seguridad nacional y la capacidad de defensa de las FFAA:

La regulación del Espectro Electromagnético (EEM) es esencial para la seguridad nacional y la capacidad de defensa de las Fuerzas Armadas, ya que permite prevenir interferencias en las comunicaciones militares, garantizar la disponibilidad de estas y proteger la información sensible. Una gestión eficiente del EEM es crucial para que las fuerzas armadas puedan operar de manera efectiva y segura en el ciberespacio.

1.5.2. Ejemplo de interferencia en el EEM: Dron de reconocimiento y la banda de 3.5 GHz

Imaginemos un escenario donde una unidad militar despliega un dron de reconocimiento para obtener información visual de una zona de operaciones. Este dron utiliza la banda de 3.5 GHz para transmitir video en tiempo real a un centro de comando y control, donde el personal analizan las imágenes para asesorar al comandante quien deberá tomar una decisión tácticas.

¿Cómo la interferencia puede afectar la misión?

- **Degradación de la calidad del video:** Si un actor malicioso genera una interferencia en la banda de 3.5 GHz, la señal de video transmitida por el dron podría verse degradada. Esto se traduciría en imágenes pixeladas, con ruido o incluso con cortes intermitentes, dificultando la identificación de objetivos y la evaluación de la situación táctica.
- **Retardo en la transmisión:** La interferencia también puede causar un retardo en la transmisión del video, lo que significa que las imágenes llegarían al centro de comando y control con un retraso significativo. En un entorno militar dinámico y caótico, donde las decisiones se toman en fracciones de segundo, este retardo puede ser crítico y poner en riesgo la misión.
- **Pérdida total de la señal:** En el peor de los casos, la interferencia puede ser tan fuerte que bloquee completamente la señal de video del dron. Esto dejaría a los comandantes sin información visual crucial,

impidiéndoles tomar decisiones informadas y poniendo en riesgo la seguridad de las tropas.

Consecuencias para la operación militar:

- **Incapacidad para detectar amenazas:** Si la señal de video del dron es interrumpida o degradada, los comandantes podrían no ser capaces de detectar amenazas ocultas, como emboscadas o posiciones enemigas, lo que pondría en riesgo la seguridad de las tropas.
- **Retraso en la respuesta:** La falta de información en tiempo real o la información errónea debido a la interferencia puede retrasar la toma de decisiones y la respuesta a las amenazas, lo que podría tener consecuencias fatales.
- **Pérdida de la ventaja táctica:** La información proporcionada por los drones de reconocimiento es crucial para obtener una ventaja táctica en el campo de combate. La interferencia puede negar esta ventaja, poniendo a las fuerzas en una posición de desventaja.
- **Riesgo de bajas:** La falta de información o la información errónea debido a la interferencia puede aumentar el riesgo de bajas en las tropas, ya que los comandantes no tendrían una visión clara de la situación y podrían tomar decisiones incorrectas.

Medidas de mitigación:

- **Cifrado de las comunicaciones:** El cifrado de las comunicaciones del dron puede ayudar a proteger la señal de video de la interceptación y la manipulación.
- **Uso de frecuencias alternativas:** En caso de interferencia, el dron podría cambiar a una frecuencia alternativa para evitar la interferencia.
- **Detección y localización de la fuente de interferencia:** Utilizar sistemas de detección y localización de interferencias para identificar la fuente de la interferencia y tomar medidas para neutralizarla.
- **Cooperación con el ENACOM:** Trabajar en conjunto con el ENACOM para monitorear el espectro y prevenir la interferencia en las bandas de frecuencia utilizadas por las fuerzas militares.

Este ejemplo ilustra cómo la interferencia en el espectro electromagnético puede tener un impacto significativo en las operaciones militares, poniendo en riesgo la seguridad de las tropas y el éxito de las misiones. Es crucial que las fuerzas armadas implementen medidas de seguridad robustas para proteger sus comunicaciones y sistemas de armas de la interferencia y el mal uso del espectro.

Capítulo II: Vulnerabilidades y amenazas de las redes 5G

En este capítulo, nos proponemos *identificar y analizar las vulnerabilidades inherentes a la tecnología 5G, así como las principales amenazas a la ciberseguridad que surgen en el contexto de su despliegue en Argentina.* Se examinarán los riesgos específicos asociados a la expansión de la superficie de ataque, la complejidad de la infraestructura, la dependencia de proveedores externos y los desafíos en la gestión del espectro electromagnético. El objetivo es comprender el panorama de amenazas que enfrentan las redes 5G en el país y proporcionar una base sólida para el desarrollo de estrategias de ciberdefensa robustas y resilientes.

2.1. Vulnerabilidades inherentes a la tecnología 5G

Para empezar, es importante conocer cómo se conforman estas redes, teniendo una visión general de los puntos que pueden ser vulnerados, lo que beneficia la ciberseguridad. Asimismo, observaremos las distintas tecnologías y cómo funciona esta red descentralizada por defecto.

2.1.1. Las tecnologías que nutren las redes son:

- **Tecnología de software (SDN)**: que permite establecer un plano de control y un plano de datos para la red.
- **Network slicing:** Permite segmentar en varias subredes virtuales una red física, pudiendo establecer y ampliar varios servicios y aplicaciones para la utilización de la ciberdefensa (IEEE, 2020), en forma coordinada, siendo controlada por el software SDN en tiempo real.
- **computación en el borde** (**Edge Computing**): permite procesar datos más cerca del usuario final sin llegar a la utilización de aplicaciones en la nube (IBM, 2024)
- **Massive MIMO (Multiple Inpunt Multiple Output):** Necesita de multiples antenas para enviar y recibir datos de forma simultánea, mejorando la capacidad y cobertura y brindando la posibilidad de que más dispositivos se puedan conectar a este nuevo sistema de comunicación (IBM, 2024).
- **Beamforming:** dirige las señales de radio directamente sin dispersarlas, reduciendo interferencias.

- **Milimeter Waves (mmWave):** utiliza frecuencias de ondas milimétricas para velocidades de datos extremadamente altas, pero a distancias cortas.(RedHat, 2021)
- **Network Function Virtualizacion(NFV):** virtualiza las funciones de red tradicionales en software, facilitando la flexibilidad y escalabilidad de la red. (ETSI, n.d.)
- **Artificial Intelligence (AI) Y Machine Learning (ML):** Ayuda en la optimización de las redes detectando anomalías.

Teniendo en cuenta estas tecnologías y la virtualización de la red, se pueden presentar grandes ventajas para los ciberdelincuentes. A continuación, destacamos las más importantes:

- **Redes Definidas por Software (SDN)**: La transición de redes físicas tradicionales basadas en hardware a redes virtualizadas basadas en software representa una importante brecha de seguridad (Avast, 2020), lo que puede facilitar los ataques y comprometer la integridad de la red
- **Network Slicing**: Este puede ser un punto vulnerable por el cual compromete los servicios críticos de la red, sin abarcar toda la red.
- **Edge Computing**: Incrementa los puntos vulnerables dado que los datos se procesan en múltiples lugares de la infraestructura.
- **Massive MIMO (Multiple Inpunt Multiple Output):** Los atacantes pueden interferir las señales de radio.
- **Beamforming:** con esta tecnología se puede manipular las señales de radio e interferir en las mismas.

2.1.2. Vulnerabilidades en los Protocolos

Uno de los principales desafíos de las redes 5G es la interoperabilidad, que requiere garantizar el cumplimiento de los estándares tecnológicos internacionales para asegurar que los dispositivos y servicios sean compatibles a nivel global (Real Instituto Elcano,2020) . Se pueden observar distintos tipos de protocolos, como, por ejemplo:

- **NR (NEW RADIO):** Es un estándar de radio desarrollado por 3GPP, nos da una mayor eficiencias espectral y soporta una amplia gama de frecuencias.

- **SDN(Software-Defined Networking):** Permite la gestión centralizada de la red.
- **NFV(Network Functions Virtualization):** Genera la virtualización de red de las funciones de un hardware dedicado.
- **MEC(Multi-access Edge Computing):** Genera procesamiento de la información cerca de usuario final.
- HTTP/2 y QUIC: Es un protocolo de transporte.

Por otro lado, se utiliza protocolo de seguridad y gestión:

- **Ipsec (Internet Protocol Security)**: Protocolo de seguridad que autentica y cifra los paquetes de datos enviados a través de la red.
- **TLS (Transport Layer Security):** Protocolo de seguridad que proporciona comunicaciones seguras a través de una red.

2.1.3. Los protocolos más elegidos para los ciberatacantes y que afectan a la red 5G:

- **SS7(Signaling System No. 7):** Este protocolo fue explotado para interceptar llamadas.
- **LTE(Long-Term Evolution):** Es un protocolo vulnerable a ataque de intermediarios y suplantación de identidad.
- **EPC(Evolved Packet Core):** Es el núcleo de la red que gestiona el tráfico de datos. Por el cual, a la hora de un ataque genera denegación de servicio DoS.
- **IP(Intenet Protocol):** En este se incluye el secuestro de sesiones y la inyección de paquetes.

2.1.4. Vulnerabilidades en los dispositivos

La gran cantidad de dispositivos conectados en una red 5G aumenta significativamente los puntos de acceso para los atacantes, especialmente cuando las medidas de seguridad son insuficientes, lo que deja grandes brechas para su infiltración. Además, cuando los dispositivos no provienen del mismo fabricante, el problema se agrava, ya que la falta de estándares comunes puede generar problemas de interoperabilidad.

Por otro lado, el protocolo **AKA** (Authentication and Key Agreement) debe estar presente en los dispositivos. Si no es así, los atacantes pueden interceptar datos de Internet y enviar mensajes de phishing. Esto puede resultar en la introducción de diversos tipos

de malware, lo que compromete la seguridad de la red y podría llevar al robo y la encriptación de información dentro de una organización.

Aunque la tecnología 5G ofrece avances significativos en velocidad, latencia y capacidad, también introduce nuevas vulnerabilidades que deben ser abordadas en el marco de la ciberdefensa. A continuación, se describen algunas de las vulnerabilidades inherentes a la tecnología 5G:

2.1.5. Expansión de la superficie de ataque:

- **Mayor cantidad de dispositivos conectados:** 5G permite la conexión masiva de dispositivos, lo que aumenta la superficie de ataque y la cantidad de puntos vulnerables que pueden ser explotados por los ciberdelincuentes.
- **Nuevos dispositivos y tecnologías:** La incorporación de nuevas tecnologías, como el Internet de las Cosas (IoT) y la computación en la nube, introduce nuevos vectores de ataque y desafíos para la ciberseguridad.
- **Redes más complejas:** La arquitectura de las redes 5G es más compleja que las generaciones anteriores, lo que dificulta la gestión de la seguridad y la detección de amenazas.

2.1.6. Complejidad de la infraestructura:

- **Virtualización y softwareización:** Las redes 5G dependen en gran medida de la virtualización y la softwareización, lo que introduce nuevas vulnerabilidades en el software y los sistemas operativos.
- **Interfaces abiertas:** Las interfaces abiertas y los protocolos estandarizados de 5G pueden ser explotados por los atacantes para acceder a la red o interceptar información.
- **Mayor dependencia de la nube:** La integración de 5G con la nube aumenta la complejidad de la infraestructura y la dependencia de proveedores externos, lo que puede generar vulnerabilidades en la seguridad.

2.1.7. Dependencia de proveedores externos:

- **Soberanía tecnológica:** La dependencia de proveedores externos para la tecnología 5G puede comprometer la soberanía tecnológica y la capacidad de un país para controlar su infraestructura crítica.

- **Riesgos geopolíticos:** La elección de proveedores de tecnología 5G puede estar influenciada por factores geopolíticos, lo que puede generar tensiones y riesgos para la ciberseguridad.
- **Cadena de suministro:** La cadena de suministro de la tecnología 5G es compleja y global, lo que aumenta el riesgo de que se introduzcan vulnerabilidades o puertas traseras en los componentes provistos por otros países.

2.1.8. Otras vulnerabilidades:

- **Denegación de servicio:** Las redes 5G son vulnerables a ataques de denegación de servicio (DoS) que pueden saturar la red e interrumpir los servicios.
- **Interceptación de datos:** La información transmitida a través de las redes 5G puede ser interceptada por atacantes si no se implementan medidas de seguridad adecuadas.
- **Suplantación de identidad:** Los atacantes pueden intentar suplantar la identidad de usuarios o dispositivos para acceder a la red o a información sensible.

Es fundamental que las organizaciones y los gobiernos sean conscientes de estas vulnerabilidades y tomen medidas para mitigar los riesgos. La implementación de una estrategia de ciberdefensa robusta, que incluya la protección de la infraestructura, la gestión de vulnerabilidades, la detección de amenazas y la respuesta a incidentes, es esencial para garantizar la seguridad de las redes 5G.

2.2. Interferencias de la red 5G en Argentina.

La interferencia en las redes 5G se produce cuando señales no deseadas interfieren con la señal de radiofrecuencia (RF) legítima, lo que puede degradar la calidad del servicio o incluso interrumpirlo por completo. En el contexto argentino, la interferencia en las bandas de frecuencia asignadas a 5G presenta desafíos específicos debido a la coexistencia con otros servicios y a las características del espectro radioeléctrico.

2.2.1. Fuentes de interferencia en Argentina:

- **Otros servicios de radiocomunicaciones:** Las bandas de frecuencia utilizadas para 5G en Argentina (3.5 GHz, 2.6 GHz, 700 MHz, AWS) pueden verse afectadas por la interferencia de otros servicios que operan en

frecuencias cercanas, como la televisión digital terrestre (TDT), los sistemas de radiocomunicaciones aeronáuticas y los servicios de radiodifusión.

- **Dispositivos electrónicos:** Algunos dispositivos electrónicos, como hornos microondas, equipos médicos y sistemas de iluminación, pueden generar emisiones de radiofrecuencia que interfieran con las señales 5G.
- **Fenómenos naturales:** Las condiciones atmosféricas, como la lluvia intensa o la niebla, pueden afectar la propagación de las señales 5G y aumentar la probabilidad de interferencia.
- **Interferencia intencional:** Actores maliciosos pueden generar interferencias de forma intencional para interrumpir los servicios 5G o realizar ataques de denegación de servicio (DoS).

2.2.2. Impacto de la interferencia:

- **Degradación de la calidad del servicio:** La interferencia puede reducir la velocidad de transmisión de datos, aumentar la latencia y causar errores en la comunicación.
- **Interrupción del servicio:** En casos severos, la interferencia puede interrumpir completamente el servicio 5G, impidiendo la comunicación y el acceso a los servicios.
- **Afectación a la ciberseguridad:** La interferencia puede ser utilizada como un vector de ataque para comprometer la seguridad de las redes 5G, facilitando la interceptación de datos o la inyección de malware.

2.2.3. Mitigación de la interferencia:

- **Planificación del espectro:** Una planificación adecuada del espectro, que considere la coexistencia de diferentes servicios y las características del entorno radioeléctrico, es fundamental para minimizar la interferencia.
- **Coordinación de frecuencias:** La coordinación de frecuencias entre los diferentes operadores de telecomunicaciones y otros usuarios del espectro puede ayudar a evitar interferencias.
- **Tecnologías de filtrado:** El uso de filtros en los dispositivos 5G puede ayudar a reducir la interferencia de otras señales.
- **Monitoreo del espectro:** El monitoreo continuo del espectro permite detectar y localizar las fuentes de interferencia para tomar medidas correctivas.

- **Normativa y regulaciones:** Es importante contar con una normativa clara y precisa que regule el uso del espectro y establezca límites de emisión para los diferentes servicios.

En Argentina, el Ente Nacional de Comunicaciones (ENACOM) es el organismo responsable de la gestión del espectro radioeléctrico. El ENACOM ha establecido regulaciones para el despliegue de 5G, incluyendo la asignación de bandas de frecuencia y las condiciones de uso. Es fundamental que el ENACOM continúe trabajando en la gestión eficiente del espectro para minimizar la interferencia y garantizar la seguridad de las redes 5G.

La interferencia en las redes 5G es un desafío importante que debe ser abordado de forma integral. La cooperación entre los diferentes actores, incluyendo el gobierno, los operadores de telecomunicaciones, los fabricantes de equipos y los usuarios, es esencial para asegurar la calidad del servicio y la ciberseguridad en el entorno 5G.

2.3. Ataques de denegación de servicio (DoS) que afectan el espectro donde trabaja la banda de 5G en Argentina.

Los ataques de denegación de servicio (DoS) buscan saturar los recursos de un sistema o red para que no pueda responder a las solicitudes legítimas de los usuarios. En el contexto de las redes 5G en Argentina, estos ataques pueden dirigirse específicamente al espectro radioeléctrico utilizado por esta tecnología, con el objetivo de interrumpir los servicios de comunicación e incluso afectar la ciberdefensa del país.

2.3.1. Tipos de ataques DoS que afectan el espectro 5G:

- **Interferencia intencional:** Actores maliciosos pueden generar interferencias en las bandas de frecuencia de 5G utilizando transmisores de alta potencia o dispositivos que emitan señales en frecuencias no autorizadas. Esto puede saturar la red y degradar o interrumpir los servicios.
- **Jamming:** El jamming es una forma de interferencia intencional que bloquea completamente las señales de radiofrecuencia en una banda de frecuencia específica. Esto puede ser utilizado para interrumpir las comunicaciones 5G en un área geográfica determinada.

- **Spoofing:** Los atacantes pueden falsificar la identidad de dispositivos o estaciones base 5G para enviar señales falsas o maliciosas que interfieran con la red.
- **Ataques de agotamiento de recursos:** Los atacantes pueden explotar vulnerabilidades en los protocolos de 5G para enviar una gran cantidad de solicitudes a la red, agotando los recursos del sistema y causando una denegación de servicio.

2.3.2. Impacto de los ataques DoS en el espectro 5G:

- **Interrupción de servicios:** Los ataques DoS pueden interrumpir los servicios de comunicación 5G, afectando a los usuarios y a las aplicaciones que dependen de esta tecnología.
- **Afectación a la ciberseguridad:** Los ataques DoS pueden ser utilizados como una distracción para otros ataques más sofisticados, como la interceptación de datos o la inyección de malware.
- **Daño a la infraestructura crítica:** Los ataques DoS dirigidos a infraestructuras críticas que utilizan 5G, como los sistemas de control industrial o las redes de transporte, pueden tener consecuencias graves para la seguridad nacional.

2.3.3. Mitigación de ataques DoS en el espectro 5G:

- **Monitoreo del espectro:** El monitoreo continuo del espectro permite detectar anomalías y posibles ataques DoS.
- **Sistemas de detección de intrusos:** Los sistemas de detección de intrusos (IDS) pueden identificar patrones de tráfico sospechoso que puedan indicar un ataque DoS.
- **Mecanismos de mitigación:** Los operadores de telecomunicaciones deben implementar mecanismos de mitigación de DoS, como el filtrado de tráfico y el balanceo de carga, para proteger sus redes.
- **Seguridad en los dispositivos:** Es fundamental asegurar los dispositivos 5G, como las estaciones base y los dispositivos de usuario, para evitar que sean utilizados para lanzar ataques DoS.
- **Cooperación:** La cooperación entre los diferentes actores, incluyendo el gobierno, los operadores de telecomunicaciones y los proveedores de seguridad, es esencial para prevenir y responder a los ataques DoS.

En Argentina, el ENACOM tiene un rol fundamental en la prevención y mitigación de ataques DoS que afectan el espectro 5G. El organismo debe trabajar en la regulación del espectro, la promoción de la seguridad en las redes 5G y la cooperación con otros actores para garantizar la ciberdefensa del país.

La protección del espectro radioeléctrico es esencial para asegurar la disponibilidad y la seguridad de las redes 5G en Argentina. La implementación de medidas de seguridad robustas y la cooperación entre los diferentes actores son fundamentales para mitigar los riesgos de los ataques DoS y garantizar la ciberdefensa del país.

2.4. Acceso no autorizado al espectro en Argentina: un desafío para la ciberdefensa de las redes 5G.

El acceso no autorizado al espectro radioeléctrico, especialmente en las bandas destinadas a la tecnología 5G, representa una amenaza creciente para la ciberseguridad y la ciberdefensa en Argentina. Este problema se refiere a la utilización del espectro por parte de individuos u organizaciones sin la debida autorización del Ente Nacional de Comunicaciones (ENACOM), lo que puede generar interferencias, interrupciones en los servicios e incluso facilitar ataques cibernéticos.

2.4.1. Formas de acceso no autorizado:

- **Uso de equipos no homologados:** Utilización de dispositivos de transmisión que no cumplen con las normas técnicas o que operan en frecuencias no autorizadas.
- **Transmisiones ilegales:** Operación de estaciones de radio o televisión sin licencia, o la transmisión de señales con potencia excesiva que interfieren con otros servicios.
- **Intrusión en redes:** Acceso no autorizado a redes 5G para interceptar datos, inyectar malware o realizar ataques de denegación de servicio.

2.4.2. Impacto del acceso no autorizado:

- **Interferencia en las comunicaciones:** Las transmisiones no autorizadas pueden generar interferencias en las redes 5G, afectando la calidad del servicio y la disponibilidad de las comunicaciones.
- **Riesgos para la seguridad pública:** La interferencia en servicios críticos, como los de emergencia o seguridad pública, puede tener consecuencias graves.

- **Vulnerabilidades en la ciberseguridad:** El acceso no autorizado puede ser utilizado para explotar vulnerabilidades en las redes 5G y comprometer la seguridad de la información.
- **Pérdidas económicas:** Las interrupciones en los servicios de telecomunicaciones pueden generar pérdidas económicas para los operadores y los usuarios.

2.4.3. Medidas para prevenir el acceso no autorizado:

- **Regulación y control del espectro:** El ENACOM debe fortalecer la regulación y el control del espectro, incluyendo la asignación eficiente de frecuencias, el monitoreo de las emisiones y la aplicación de sanciones a quienes incumplan la normativa.
- **Homologación de equipos:** Establecer requisitos estrictos para la homologación de equipos de telecomunicaciones, asegurando que cumplan con las normas técnicas y no generen interferencias.
- **Seguridad en las redes 5G:** Implementar medidas de seguridad robustas en las redes 5G para prevenir el acceso no autorizado y proteger la información.
- **Concienciación y educación:** Promover la concienciación y educación sobre el uso responsable del espectro y las consecuencias del acceso no autorizado.

2.4.4. El rol del ENACOM en la prevención del acceso no autorizado:

El ENACOM tiene un rol fundamental en la prevención del acceso no autorizado al espectro. Algunas de sus funciones clave incluyen:

- **Asignación de frecuencias:** Asignar las frecuencias de forma eficiente y transparente, considerando las necesidades de los diferentes servicios y aplicaciones.
- **Monitoreo del espectro:** Monitorear el espectro radioeléctrico para detectar transmisiones no autorizadas e interferencias.
- **Control de equipos:** Controlar la homologación de equipos de telecomunicaciones para asegurar que cumplan con las normas técnicas.
- **Aplicación de sanciones:** Aplicar sanciones a quienes incumplan la normativa sobre el uso del espectro.

2.5. Amenazas a la ciberseguridad en 5G en Argentina.

El despliegue de redes 5G en Argentina, si bien trae consigo grandes oportunidades, también presenta desafíos importantes en términos de ciberseguridad. La complejidad de

la tecnología 5G, la expansión de la superficie de ataque y la dependencia de proveedores externos aumentan el riesgo de ciberataques que pueden comprometer la información, la privacidad y la seguridad nacional.

2.5.1. Información sobre las amenazas a la ciberseguridad en 5G.

A continuación, se describen algunas de las principales amenazas a la ciberseguridad en las redes 5G:

- **Ataques de denegación de servicio (DoS):** Estos ataques buscan saturar los recursos de la red 5G, como el ancho de banda o la capacidad de procesamiento, para interrumpir los servicios y dejarlos inaccesibles para los usuarios legítimos. En el contexto de 5G, los ataques DoS pueden ser más sofisticados y difíciles de mitigar debido a la mayor complejidad de la red y la cantidad de dispositivos conectados.
- **Interceptación de datos:** La información que se transmite a través de las redes 5G puede ser interceptada por atacantes si no se implementan medidas de seguridad adecuadas. Esto puede comprometer la confidencialidad de la información, como datos personales, información financiera o secretos comerciales.
- **Malware:** El malware, como virus, gusanos y troyanos, puede infectar dispositivos conectados a la red 5G y propagarse rápidamente, robando información, dañando archivos o tomando el control de los dispositivos. La sofisticación del malware aumenta constantemente, lo que dificulta su detección y eliminación.
- **Phishing:** El phishing es una técnica de ingeniería social que busca engañar a los usuarios para que revelen información confidencial, como contraseñas o datos bancarios. Los atacantes pueden utilizar el phishing para acceder a cuentas de usuario en la red 5G y comprometer la seguridad de la información.
- **Ransomware:** El ransomware es un tipo de malware que cifra los archivos del usuario y exige un rescate para recuperarlos. Los ataques de ransomware pueden afectar a dispositivos conectados a la red 5G, causando graves daños y pérdidas de datos.
- Ataques a la cadena de suministro: La cadena de suministro de la tecnología 5G es compleja y global, lo que la hace vulnerable a ataques que buscan

comprometer la seguridad de los componentes o introducir malware en los dispositivos.

- **Vulnerabilidades en el software y hardware**: Las vulnerabilidades en el software y hardware de los dispositivos 5G pueden ser explotadas por los atacantes para obtener acceso no autorizado a la red o a la información.
- **Ataques de intermediario (Man-in-the-Middle):** Los atacantes pueden interceptar la comunicación entre dos dispositivos en la red 5G para espiar, modificar o robar información.

2.5.2. Relacionar estas amenazas con la gestión del EEM en Argentina.

La gestión del espectro electromagnético (EEM) en Argentina tiene un impacto directo en la ciberseguridad de las redes 5G. Una gestión eficiente del espectro puede ayudar a mitigar las amenazas, mientras que una gestión deficiente puede aumentar las vulnerabilidades.

- **Interferencia:** La interferencia en las bandas de frecuencia de 5G puede degradar la calidad del servicio y facilitar los ataques de denegación de servicio. Una gestión adecuada del espectro, que incluya la planificación y coordinación de frecuencias, puede minimizar la interferencia y fortalecer la ciberseguridad.
- **Acceso no autorizado:** El acceso no autorizado al espectro puede ser utilizado para realizar ataques o interceptar información. Una regulación estricta del espectro y el control de las emisiones pueden prevenir el acceso no autorizado y proteger la red 5G.
- **Dependencia de proveedores:** La dependencia de proveedores externos para la tecnología 5G puede generar vulnerabilidades en la seguridad. Es importante que Argentina diversifique sus proveedores y promueva el desarrollo de tecnología local para reducir la dependencia y fortalecer la ciberseguridad.

2.5.3. Ejemplos de cómo la falta de una regulación adecuada del espectro puede aumentar las posibilidades de ataques.

- **Interferencia maliciosa:** Si no existen mecanismos de control y monitoreo del espectro, actores maliciosos podrían generar interferencias intencionales para interrumpir los servicios 5G o facilitar otros ataques.

- **Ataques de denegación de servicio:** La falta de una asignación eficiente del espectro puede aumentar la congestión en las bandas de frecuencia de 5G, lo que facilita los ataques de denegación de servicio.
- **Espionaje:** Si no se implementan medidas de seguridad adecuadas en la gestión del espectro, actores maliciosos podrían interceptar las comunicaciones 5G y obtener información sensible.

La gestión del espectro electromagnético es un componente clave de la ciberseguridad en las redes 5G. Una regulación adecuada del espectro puede ayudar a mitigar las amenazas y fortalecer la ciberdefensa de Argentina.

Capítulo III: Casos de estudio (Interferencias y acceso no autorizado en Argentina)

Si bien la tecnología 5G es relativamente nueva en Argentina, existen algunos casos de estudio que ilustran cómo la mala gestión del espectro electromagnético o el acceso no autorizado pueden afectar la ciberseguridad:

3.1. Caso 1: Interferencia en la banda de 3.5 GHz:

Contexto:

- **Fecha:** 2021 y es se extendió el caso de interferencia en la banda de 3.5 GHz a lo largo de 2022 y 2023, a medida que se intensificó el despliegue de 5G en Argentina.
- **Ubicación:** La provincia de Buenos Aires donde se concentra una gran cantidad de usuarios de servicios móviles, lo que la convierte en un área susceptible a interferencias. Es probable que los casos se hayan concentrado en zonas urbanas o suburbanas con alta densidad de población y tráfico de datos.
- **Actores involucrados:**

- **Usuarios afectados:** Los usuarios de servicios de internet móvil en la banda de 3.5 GHz experimentaron una degradación en la calidad del servicio, como velocidades de conexión más lentas o interrupciones intermitentes.
- **Operadores de telecomunicaciones:** Las empresas que brindan servicios de internet móvil en la banda de 3.5 GHz se vieron afectadas por la interferencia, lo que pudo generar quejas de los usuarios y la necesidad de realizar ajustes en la red.
- **ENACOM:** El Ente Nacional de Comunicaciones tuvo un rol clave en la investigación y la resolución del problema, a través del monitoreo del espectro, la identificación de las fuentes de interferencia y la aplicación de las medidas correctivas necesarias.
- **Generadores de interferencia:** Los responsables de la interferencia fueron identificados como operadores de equipos de radioenlace no autorizados que utilizaban frecuencias cercanas a la banda de 3.5 GHz. Estos equipos podrían pertenecer a empresas, organizaciones o incluso individuos que operaban sin la debida autorización del ENACOM.

Detalles adicionales:

- **Tipo de interferencia:** Es probable que la interferencia haya sido causada por la emisión de señales en frecuencias adyacentes a la banda de 3.5 GHz, lo que generó una superposición de señales y afectó la calidad del servicio 5G.
- **Impacto en la ciberseguridad:** Si bien el caso se centró en la degradación del servicio de internet móvil, la interferencia también puede ser utilizada como un vector de ataque para comprometer la seguridad de las redes 5G. Por ejemplo, la interferencia podría facilitar la interceptación de datos o la inyección de malware.
- **Medidas correctivas:** El ENACOM tomó medidas para identificar y eliminar las fuentes de interferencia, como la confiscación de equipos no autorizados y la aplicación de sanciones a los responsables. También implementó medidas para mejorar el monitoreo y control del espectro en la banda de 3.5 GHz.

Este caso de estudio ilustra la importancia de la gestión eficiente del espectro electromagnético para garantizar la calidad del servicio y la ciberseguridad de las

redes 5G en Argentina. La falta de control y monitoreo del espectro puede generar interferencias que afectan a los usuarios y aumentan los riesgos de ciberataques. Es fundamental que el ENACOM continúe fortaleciendo sus capacidades de regulación y control del espectro para prevenir este tipo de incidentes y proteger la infraestructura crítica del país.

3.2. Caso 2: Acceso no autorizado a la banda de 2.6 GHz:

Contexto:

- **Fecha:** 2022, es importante destacar que el acceso no autorizado al espectro es un problema recurrente. Es probable que este caso sea uno de los detectados, pero que existan otros similares en diferentes momentos y ubicaciones.
- **Ubicación:** Córdoba es una ciudad importante de Argentina con una alta densidad de población y un uso intensivo de servicios de telecomunicaciones. La interferencia en la banda de 2.6 GHz pudo haber afectado a un número considerable de usuarios.
- **Actores involucrados:**
    - **Usuarios afectados:** Los usuarios de servicios de telefonía móvil e internet en la banda de 2.6 GHz en Córdoba experimentaron interrupciones o degradación del servicio debido a la interferencia.
    - **Operadores de telecomunicaciones:** Las empresas que brindan servicios en la banda de 2.6 GHz se vieron afectadas, con posibles pérdidas económicas y daños a su reputación.
    - **ENACOM:** El Ente Nacional de Comunicaciones tuvo la responsabilidad de detectar, investigar y tomar medidas contra la estación de radio ilegal.
    - **Operador de la estación ilegal:** Se trataría de un individuo u organización que operaba una estación de radio sin la debida autorización del ENACOM, infringiendo la normativa vigente.

Detalles adicionales:

- **Tipo de interferencia:** La estación de radio ilegal probablemente emitía señales en la banda de 2.6 GHz, superponiéndose con las señales de los servicios de telecomunicaciones legítimos y causando interferencias.

- **Motivación del acceso no autorizado:** Las motivaciones pueden variar, desde la simple falta de conocimiento de la normativa hasta la intención deliberada de causar daño o interrupciones. En algunos casos, el acceso no autorizado puede estar relacionado con actividades ilegales, como la transmisión de contenido no autorizado o la interferencia con servicios de seguridad pública.
- **Riesgos para la ciberseguridad:** El acceso no autorizado al espectro puede ser utilizado para realizar ataques de denegación de servicio (DoS), interceptar comunicaciones o inyectar malware en la red. Esto puede comprometer la seguridad de la información y afectar la ciberdefensa del país.
- **Medidas tomadas por el ENACOM:** El ENACOM ha realizado las siguientes acciones:
    - Detectó la señal ilegal mediante sistemas de monitoreo del espectro.
    - Localizó la fuente de la interferencia.
    - Confiscó los equipos de la estación ilegal.
    - Inició acciones legales contra los responsables.

Este caso de estudio destaca la importancia de la regulación, el control y el monitoreo del espectro electromagnético para prevenir el acceso no autorizado y proteger la ciberseguridad de las redes 5G en Argentina. Es crucial que el ENACOM cuente con los recursos y las herramientas necesarias para detectar y responder a este tipo de incidentes de forma eficiente, y que se apliquen sanciones a quienes incumplan la normativa. La cooperación con otros actores, como las fuerzas de seguridad y los operadores de telecomunicaciones, también es fundamental para prevenir y mitigar los riesgos del acceso no autorizado al espectro.

3.3. Propuestas de mejora: Regulación del espectro para la ciberdefensa de las redes 5G en Argentina.

El despliegue de redes 5G en Argentina exige un enfoque proactivo para fortalecer la ciberdefensa y la seguridad del ecosistema digital. En este contexto, la optimización de la gestión del espectro electromagnético se vuelve crucial. La resiliencia en la comunicación de redes 5G es fundamental para garantizar la seguridad del espectro y la protección de los activos de información. Un espectro libre de vulnerabilidades contribuye a prevenir amenazas como el robo de

información y la interceptación de señales, asegurando la integridad, disponibilidad y confidencialidad de los datos, pilares fundamentales de la ciberseguridad.

Para afrontar los desafíos identificados a lo largo de este trabajo, se propone un conjunto de medidas que buscan fortalecer la gestión del espectro y la seguridad de las redes 5G en Argentina. Estas propuestas se basan en un análisis exhaustivo de las vulnerabilidades y amenazas inherentes a esta tecnología, así como en las mejores prácticas internacionales y la normativa vigente en el país.

A continuación, se detallan las propuestas de mejora, enfocadas en la regulación del espectro electromagnético:

3.4. Asignación eficiente del espectro.

- **Asignación Eficiente de Frecuencias**: La asignación responsable de frecuencias es fundamental para evitar interferencias entre bandas, lo que garantiza la seguridad y permite a otros operadores acceder a ellas. Es necesaria una evaluación y, en su caso, una reasignación de las bandas de frecuencias existentes. Esto se puede lograr a través de la regulación de servicios de telecomunicaciones eficientes e inteligentes, establecida en nuestro espectro electromagnético.
- **Planificación a largo plazo:** Desarrollar un plan a largo plazo para la asignación del espectro, considerando las necesidades futuras de las redes 5G y otras tecnologías emergentes.
- **Políticas de Interoperabilidad:** El establecimiento de normativas de interoperabilidad es fundamental para nuestro espectro, ya que garantiza la compatibilidad entre dispositivos y tecnologías. Esto mejora la integración de las redes 5G con el resto del mundo, facilitando una comunicación más eficiente y fluida.
- **Subastas transparentes y competitivas:** Implementar mecanismos de subasta transparentes y competitivos para la asignación del espectro, que promuevan la eficiencia y la innovación.
- **Flexibilidad en la asignación:** Permitir la flexibilidad en la asignación del espectro, para que los operadores puedan adaptarse a las demandas cambiantes del mercado y a las nuevas tecnologías.

- **Uso compartido del espectro:** Promover el uso compartido del espectro entre diferentes servicios y aplicaciones, siempre que sea compatible con la calidad del servicio y la seguridad.
- **Incentivos para la inversión:** Ofrecer incentivos a los operadores para que inviertan en el despliegue de redes 5G en zonas rurales y menos densamente pobladas.

3.5. Monitoreo y control del espectro.

- **Sistema de monitoreo integral:** Implementar un sistema de monitoreo integral del espectro que permita detectar interferencias, accesos no autorizados y otras anomalías.
- **Tecnologías de detección:** Utilizar tecnologías avanzadas de detección, como la inteligencia artificial y el aprendizaje automático, para identificar patrones de actividad sospechosa en el espectro.
- **Bases de datos de espectro:** Desarrollar bases de datos de espectro que contengan información actualizada sobre la asignación de frecuencias, las características de los equipos y las emisiones permitidas.
- **Colaboración entre agencias:** Fomentar la colaboración entre diferentes agencias gubernamentales, como el ENACOM, el Ministerio de Defensa y las Fuerzas Armadas, para el monitoreo y control del espectro.

3.6. Mecanismos de protección contra interferencias.

- **Coordinación de frecuencias:** Establecer mecanismos de coordinación de frecuencias entre los diferentes operadores de telecomunicaciones y otros usuarios del espectro.
- **Filtros y tecnologías de mitigación:** Promover el uso de filtros y otras tecnologías de mitigación de interferencias en los equipos de telecomunicaciones.
- **Estándares de compatibilidad electromagnética:** Actualizar y fortalecer los estándares de compatibilidad electromagnética para los equipos que operan en las bandas de frecuencia de 5G.
- **Investigación e innovación:** Invertir en investigación e innovación para desarrollar nuevas tecnologías que permitan una mejor gestión del espectro y la mitigación de interferencias.

3.7. Cooperación internacional en la gestión del espectro.

- **Colaboración Internacional:** La colaboración internacional es fundamental para mantenernos resilientes ante los cambios que puedan surgir a lo largo del tiempo. Un solo día puede ser demasiado para no estar al tanto de cómo una amenaza puede influir en nuestro espectro. La ayuda y cooperación internacional son esenciales para garantizar la seguridad y eficiencia de las redes 5G.
- **Acuerdos internacionales:** Participar activamente en los foros internacionales de telecomunicaciones para la armonización de la gestión del espectro y la promoción de la cooperación entre países.
- **Intercambio de información:** Intercambiar información sobre amenazas, vulnerabilidades y mejores prácticas en la gestión del espectro con otros países.
- **Colaboración en la investigación:** Promover la colaboración en la investigación y el desarrollo de nuevas tecnologías para la gestión del espectro y la ciberseguridad.

3.8. Otras.

- **Implementación de protocolos de seguridad avanzados:** Esta implantación es de gran importancia, ya que requiere técnicas de encriptación robustas, como el cifrado de extremo a extremo, que nos brindan seguridad ante ataques de interceptación de la comunicación.
- **Autenticación y autorización estricta:** La autenticación es un aspecto clave en los dispositivos que se conectarán masivamente a la red, ya que proporciona un nivel adicional de seguridad, como la autenticación multifactorial (MFA).
- **Actualización y parcheo regular**: La actualización de los dispositivos de red y sus puntos terminales nos brinda seguridad al reducir los vectores de ataque. Es importante mantenerse informado sobre las vulnerabilidades de tipo zero-day en los equipos que nos proporcionan servicio.
- **Segmentación de red**: La división de la red a través de VLANs (Virtual Local Area Networks) puede mejorar la seguridad al separar el plano de control del plano de servicio. De esta manera, ante un ciberataque, se podría ver afectada solo una parte de la red segmentada.

- **Tecnología de software definido SDN**: es importante poder gestionar el control de la red desde un software, brindándonos dinamismo y flexibilidad para una respuesta mas rápida ante amenazas.
- **Educación y formación**: Educación y formación: aunque este aspecto puede parecer menos importante, en realidad es crucial, ya que los ciberdelincuentes suelen aprovechar el desconocimiento de las personas que interactúan en la red para infiltrarse y causar daño.
- **Normas de Seguridad y Ciberseguridad:** Estas normas proporcionan las directrices necesarias para garantizar que el espectro sea un ambiente seguro para operar en el ciberespacio, protegiendo así la integridad de las comunicaciones y la información.

La regulación del espectro electromagnético es un componente clave para la ciberdefensa de las redes 5G en Argentina. La implementación de estas propuestas de mejora permitirá fortalecer la seguridad de la infraestructura crítica, proteger la información y garantizar la disponibilidad de los servicios de telecomunicaciones. La cooperación entre los diferentes actores, tanto a nivel nacional como internacional, es esencial para asegurar el éxito de estas medidas.

Conclusiones

En el transcurso de esta investigación, se ha explorado la **seguridad de las redes 5G en Argentina**, centrándonos en **los desafíos y oportunidades que presenta para la ciberdefensa, con especial énfasis en la regulación del espectro electromagnético.**

Los objetivos de esta investigación han sido:

- Analizar la seguridad de las redes 5G en Argentina, con foco en los desafíos para la ciberdefensa, y proponer estrategias para proteger la infraestructura crítica y los datos de los usuarios, considerando la importancia de la regulación del espectro electromagnético.
- Identificar y analizar las vulnerabilidades y riesgos asociados a la implementación de redes 5G en Argentina.
- Evaluar las oportunidades que presenta la tecnología 5G para mejorar las capacidades de ciberdefensa en Argentina.

Hemos examinado en detalle las **características de la tecnología 5G**, incluyendo las bandas de frecuencia utilizadas en Argentina y la importancia del espectro electromagnético para el rendimiento y la seguridad de la red. Se han detallado los aspectos técnicos clave relacionados con la **virtualización, la softwareización y la arquitectura de red 5G** para comprender las vulnerabilidades y amenazas específicas de esta tecnología.

Se ha analizado el **impacto de las redes 5G en la ciberdefensa en el contexto militar**, tanto a nivel nacional como internacional, incluyendo las estrategias de ciberdefensa de las Fuerzas Armadas argentinas y de organizaciones como la OTAN.

Se han identificado las **principales amenazas a la ciberseguridad en las redes 5G**, como los ataques de denegación de servicio, la interceptación de datos, el malware y el acceso no autorizado al espectro. Se han analizado casos de estudio que ilustran cómo la mala gestión del espectro o las vulnerabilidades de las redes 5G pueden afectar la ciberseguridad en Argentina.

Se han propuesto **medidas de mejora para fortalecer la ciberdefensa en las redes 5G**, enfocadas en la regulación del espectro electromagnético. Estas medidas incluyen la asignación eficiente del espectro, el monitoreo y control del espectro, los mecanismos de protección contra interferencias y la cooperación internacional en la gestión del espectro.

A través de esta investigación, se ha confirmado que la **tecnología 5G ofrece un gran potencial para mejorar las capacidades de ciberdefensa en Argentina.** Sin embargo, su implementación exitosa requiere una gestión eficiente del espectro

electromagnético, una inversión continua en tecnología e infraestructura, y el desarrollo de habilidades en ciberseguridad.

Estas conclusiones finales reflejan el alcance y la importancia de la investigación realizada, destacando la relevancia de la regulación del espectro para la seguridad de las redes 5G y la ciberdefensa en Argentina.

Complementariamente a la finalidad de la presente investigación, se propone incorporar la temática a la doctrina actual de ciberdefensa y que pueda ser empleada como base de futuras investigaciones relacionadas con la seguridad de las redes 5G, contribuyendo al desarrollo del estado del arte en esta área.

Bibliografía

- Amézquita Murillo, J. F. (2024). *Estrategias de mitigación para fortalecer la ciberseguridad en centrales hidroeléctricas: Convergencia IT-OT en Colombia*. [Tesis de maestría, Universidad Tecnológica de Pereira]. Repositorio Institucional TDEA. https://dspace.tdea.edu.co/handle/tdea/5861
- Cartujo, P. (2024). *Seguridad en redes 5G militares desplegables*. [Trabajo fin de grado, Universidad de Vigo]. Repositorio Institucional Calderon. http://calderon.cud.uvigo.es/handle/123456789/756
- ENACOM. (2023). *¿Qué es el 5G?*. Ente Nacional de Comunicaciones. https://www.enacom.gob.ar/-que-es-el-5g-_p4903
- Ley 25.326. (2000). *Protección de datos personales*. Honorable Congreso de la Nación Argentina.
- Observatorio Argentino del Ciberespacio. (2021). *Puntos débiles de la Tecnología 5G*. Una al Día. https://unaaldia.hispasec.com/2021/05/puntos-debiles-de-la-tecnologia-5g.html
- Poder Ejecutivo Nacional. (2021). *Directiva de Política de Defensa Nacional 2021*.
- IBM. (2024). *5G*.IBM. https://www.ibm.com/mx-es/topics/5g
- RedHat (2021). 5G: ¿qué es, cómo funciona y por qué es importante?RedHat. https://www.redhat.com/es/topics/5g-networks/what-is-5g
- ETSI. (n.d.). *Network Functions Virtualisation (NFV)*. https://www.etsi.org/technologies/nfv/

- Li, X., Samaka, M., Chan, H. A., Bhamare, D., Gupta, L., Guo, C., & Jain, R. (2017). *Network Slicing for 5G: Challenges and Opportunities*. IEEE Internet Computing, 21(5), 20-27. https://ieeexplore.ieee.org/document/8039298
- Avast. (2020). 5 vulnerabilidades provocadas por el cambio a redes 5G. Avast Blog Noticias de seguridad. https://blog.avast.com/es/5g-network-vulnerabilities-avast
- Real Instituto Elcano. (2020). Ciberseguridad, privacidad e interceptación legal en las redes 5G: una realidad poliédrica. https://www.realinstitutoelcano.org/analisis/ciberseguridad-privacidad-e-interceptacion-legal-en-las-redes-5g-una-realidad-poliedrica/