Gestión de riesgos cibernéticos por uso de las antenas satelitales en el Ejército Nacional

Mayor (EJC) Fabian Esteban Cano Jaime

Artículo para optar al título profesional:

Magister en Ciberseguridad y Ciberdefensa

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2025

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

DATOS GENERALES		
Nombre del estudiante	**:**	Mayor (EJC) Fabian Esteban Cano Jaime
Identificación	**:**	80041435
Programa académico	**:**	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	**:**	Nubia Edith Céspedes Prieto
Tutor temático	**:**	Nubia Edith Céspedes Prieto
Fecha de entrega	**:**	24 de agosto de 2025
Extensión	**:**	7.820 palabras

DECLARACIÓN DE ORIGINALIDAD Y CESIÓN DE DERECHOS

El autor declara que este artículo fue escrito de acuerdo con la normatividad de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) y no existe ningún potencial conflicto de interés relacionado con este. Las posturas y aseveraciones presentadas son resultado de un ejercicio académico e investigativo que no representan la posición oficial ni institucional de la ESDEG, las Fuerzas Militares de Colombia o el Ministerio de Defensa Nacional.

Este artículo es enteramente mi propio trabajo y no ha sido presentado para la obtención de un título en esta u otra Institución de Educación Superior. Se han referenciado todos los trabajos y puntos de vista de otros autores, así como los datos de otras fuentes utilizadas. No se emplearon herramientas de generación de contenido por Inteligencia Artificial para su elaboración.

El autor acepta ceder los derechos de publicación en favor de la ESDEG y su Sello Editorial de acuerdo con los términos de la licencia Creative Commons: Reconocimiento-NoComercial-SinObrasDerivadas.

AUTORIZACIÓN DE PUBLICACIÓN

El autor no autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto. Porque se esta gestionando la publicación en revista indexada internacional.

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia

Gestión de riesgos cibernéticos por uso de las antenas satelitales en el Ejército Nacional

Cyber Risk Management Associated with the Use of Satellite Antennas in the National Army

My. Fabian Esteban Cano Jaime[1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: La conectividad digital es actualmente esencial para la eficiencia y seguridad en operaciones militares. Sin embargo, el Ejército Nacional de Colombia enfrenta problemas debido a la limitada cobertura y baja calidad de su red interna (INTRANET), lo que obliga al personal a recurrir a soluciones comerciales como antenas satelitales. Aunque estas alternativas aportan ventajas como cobertura global y alta velocidad, introducen riesgos cibernéticos importantes, incluyendo la posible interceptación a las comunicaciones comprometiendo la seguridad nacional. Este artículo analiza los sistemas SATCOM y su papel en la infraestructura tecnológica militar, describiendo su uso estratégico y táctico. Se identifican vulnerabilidades inherentes a estas tecnologías como el jamming, spoofing o ataques al segmento terrestre que exigen la evaluación y fortalecimiento de estrategias de ciberdefensa, así como la adopción de técnicas y estándares adecuados para mitigar los riesgos y proteger las comunicaciones militares frente a amenazas crecientes.

Palabras clave: antenas satelitales, riesgos cibernéticos, ciberespacio, ciberdefensa, ciberseguridad.

- **Abstract:** Digital connectivity is now essential for efficient and secure military operations. However, the Colombian National Army faces significant challenges due to the limited coverage and low quality of its internal network (INTRANET), forcing personnel to rely on commercial solutions such as satellite antennas. While these alternatives provide advantages like global coverage and high speed, they introduce considerable cyber risks, including communication interception that could compromise national security. This article analyzes SATCOM systems and their role as technological infrastructure within the military, detailing their strategic and tactical applications. It identifies inherent vulnerabilities in these technologies such as

[1] Mayor del Ejército Nacional de Colombia. Maestrante en ciberseguridad y ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Magister en Gestion del Riesgo y Desarrollo, Escuela de Ingenieros Militares. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0000-0002-6645-9303 - Contacto: Fabian.cano@esdeg.edu.co.

jamming, spoofing, or attacks targeting ground segments which highlight the urgency of evaluating and strengthening cyber defense strategies. The adoption of appropriate techniques and standards is crucial to mitigate risks and protect military communications against emerging cyber threats. **Keywords:** satellite antenas, cyber risks, cyberspace, cyber defense, cybersecurity.

Introducción

Actualmente la transformación digital ha potenciado la importancia de la conectividad en el entorno militar, donde la eficiencia y la seguridad dependen en gran medida de la capacidad para mantener comunicaciones estables y seguras. El Ejército Nacional de Colombia se enfrenta al reto de una red institucional con cobertura y calidad insuficientes, lo que ha llevado, en la práctica, a que numerosas unidades opten por soluciones comerciales como las antenas satelitales comerciales (Ejército Nacional de Colombia. 2021. Informe de gestión del Comando de Apoyo Operacional de Comunicaciones y Ciberdefensa (CAOCC)). Esta elección, aunque resuelve vacíos inmediatos de conectividad, incluye una serie de riesgos cibernéticos: desde la interceptación de información y accesos no autorizados hasta la exposición generalizada a amenazas en el ciberespacio. A raíz de esta problemática, el presente artículo tiene como objetivo aplicar una metodología que permita gestionar y mitigar las vulnerabilidades y amenazas cibernéticas derivadas del uso de antenas satelitales comerciales en el desarrollo de las operaciones militares (Santamarta, n.d.). Para esto se utilizó una metodología mixta, combinando métodos cualitativos y cuantitativos con un enfoque proyectivo a través de encuestas al personal militar, donde se realizó el análisis de los datos mediante la aplicación de la herramienta estadística JASP.

Los resultados obtenidos evidencian que solo el 52% de las unidades cuentan con cobertura de red institucional, mientras que el resto recurre a soluciones comerciales para cumplir sus funciones. Más aún, cerca del 45% de estas conexiones alternativas se emplean en tareas administrativas, el 33% en operaciones y el 22% en capacitación, lo que pone en evidencia el riesgo operativo asociado. Las principales razones para utilizar estas redes

externas son la búsqueda de una mejor conectividad (44%), una cobertura más amplia (48%) y mayor velocidad (17%). Resulta preocupante que más del 80% del personal recomienda el uso de estas soluciones y que el 60%, aproximadamente, no implementa ninguna medida de seguridad ni percibe los riesgos inherentes al uso de redes comerciales, un hecho que se explica en parte el desconocimiento o la falta de capacitación en ciberseguridad y ciberdefensa. Analizando el mercado de las comunicaciones satelitales, se identificó que, pese a la existencia de más de 18 proveedores de internet satelital en Colombia, únicamente cuatro concentran la mayor parte de la demanda institucional, destacando Starlink de SpaceX por sus ventajas en costo, facilidad de uso y cobertura (Shaengchart & Kraiwanit, 2023).

El estudio resalta la urgencia de aumentar la conciencia sobre riesgos cibernéticos y mejorar las estrategias de ciberdefensa, promoviendo la adopción de medidas de seguridad y el desarrollo de capacidades institucionales para salvaguardar la integridad de las comunicaciones y la información en las operaciones militares.

Metodología

La metodología aplicada en esta investigación se basó en un método mixto, integrando técnicas cualitativas y cuantitativas, y se caracterizó por su enfoque proyectivo en relación con la gestión de riesgos cibernéticos asociados al empleo de antenas satelitales en las operaciones del Ejército Nacional de Colombia. En primer lugar, se diseñó y aplicó un instrumento de recolección de datos tipo encuesta dirigido al personal militar presente en varias zonas del país logrando una cobertura mayor al 80%, con el propósito de explorar las condiciones de conectividad, prácticas de uso, percepciones de seguridad y medidas de

protección implementadas en el manejo de redes satelitales comerciales. Las preguntas abordaron variables como cobertura institucional, actividades vinculadas al empleo de medios alternativos, motivos de adopción de estas soluciones y el conocimiento sobre vulnerabilidades y amenazas.

El enfoque proyectivo permitió orientar la investigación hacia la identificación de estrategias futuras para la gestión y mitigación de los riesgos detectados, promoviendo una visión proactiva en la toma de decisiones institucionales. La recolección de información se realizó con un istrumento validado por pares expertos, bajo criterios de anonimato y voluntariedad, asegurando la validez de los datos. El análisis cuantitativo fue desarrollado con la herramienta estadística JASP, complementado por un análisis cualitativo que interpretó las experiencias y percepciones del personal, logrando integrar ambas perspectivas. Esta metodología permitió determinar el problema y su impacto operacional, así como proponer acciones para fortalecer las capacidades de ciberdefensa y ciberseguridad en la institución.

La Realidad de las Comunicaciones Militares en Colombia

Durante varios años el Ejército Nacional ha tenido que desarrollar operaciones en una de las áreas geografías más complejas. Debido a esto, desde hace algún tiempo, las antenas satelitales se han convertido en las mejores aliadas para garantizar la comunicación y el control de las unidades militares, permitiendo que aquellas que se encuentran en las áreas más remotas o en las montañas más altas puedan comunicarse. Sin estas herramientas, simplemente no se podría llevar a cabo el desarrollo de las diferentes actividades que se realizan a diario. El problema es que, con el tiempo, se ha llegado a depender ellas para

todo, desde procesos administrativos o logísticos, capacitación y hasta en el área de operaciones, convirtiéndose en el punto débil que los enemigos conocen bien.

El conflicto en el que actualmente Colombia viene enfrentando, ya no solo se trata de combates en el área de operaciones, ahora, el mismo conflicto ha evolucionado a la par con las tecnologías actuales, incursionando en el domino del ciberespacio. Diferentes grupos con intenciones maliciosas, tanto de otros países como internos, tienen la capacidad de lanzar ataques cibernéticos contra la infraestructura. Y, como es de esperarse, las comunicaciones militares son uno de sus objetivos preferidos. Se identifica que, a nivel mundial, se pueden interferir las señales de satélite, engañar a los receptores con información falsa o, en el peor de los casos, tomar el control de los equipos. Esta nueva realidad muestra las debilidades de cómo se están defendiendo las herramientas vitales.

El Ejército Nacional de Colombia ha generado mecanismos de atención y protección a las redes de comunicación y a las bases de datos, pero los resultados muestran que para la protección de equipos físicos ha sido insuficiente para el desarrollo de las actividades que se requieren en el servicio, uno de estos son las antenas satelitales. Se tienen protocolos para el manejo y gestión de medios de comunicación como lo establece la Directiva Permanente N° 0118000010005/2018 "Lineamientos para el Direccionamiento de las Tecnologías de la Información de las Fuerzas Militares" es el que regula el empleo de antenas satelitales y medios de comunicación personal o alternos para la protección de la información, a su vez existe la directiva permanente 101 del Comando General de las Fuerzas Militares "Lineamientos de Ciberseguridad y Ciberdefensa para las FF.MM." la cual se enfoca en políticas y directrices para la protección en el ciberespacio, pero no regula ni detalla el uso físico de antenas, ni de medios alternos o personales. La normativa vigente

deja un vacío significativo, frente a los riesgos digitales específicos para los dispositivos y las nuevas alternativas de comunicación relacionadas con la tecnología 4G y 5G, una brecha que se necesita cerrar con urgencia.

Es precisamente por esta razón que surge esta investigación. Con el propósito de estudiar cuáles son esas vulnerabilidades que presentan las antenas empleadas a diario para el cumplimiento de las actividades, tanto operacionales como administrativas. La idea es sentar las bases para crear un plan claro y práctico que facilite la gestión de estos nuevos riesgos. El objetivo es asegurar que las comunicaciones sigan siendo seguras y confiables para que el Ejército pueda cumplir con su misión sin importar los desafíos que se presenten en el terreno o en el mundo cibernético.

El atractivo de las soluciones comerciales

La evolución de las nuevas tecnologías en las cuales diferentes empresas han invertido billones de dólares, hace de la comunicación satelital un sistema innovador con mayor capacidad y menor latencia en las redes terrestres y aéreas, optimizando factores como el ancho de banda, la latencia, la seguridad y la disponibilidad, garantizando una comunicación sin interrupciones incluso en las áreas más remotas(Comunicación Vía Internet Sobre La Plataforma Satelital, n.d.).

Empresas como Starlink de SpaceX, se han posicionado en el planeta por su servicio y su infraestructura, sus sistemas son más avanzados, económicos y rápidos que la tecnología con la que actualmente cuenta el Ejercito. Se caracteriza por su gran constelación, que al mes de julio de 2025 cuenta con 7.885 satélites en órbita (https://www.space.com/spacex-starlink-satellites.html), Musk (2021) había prometido cobertura global con latencias menores que los sistemas tradicionales, con una distancia de

500 km desde la superficie de la tierra con un rendimiento similar al de la fibra óptica que alcanzaría un aumento de hasta 100 veces el ancho de banda si la comparamos con los sistemas satelitales geoestacionarios (GEO).

Por otro lado, en Colombia empresas como HughesNet, Skynet, GlobalTT entre otras, emplean satélites geoestacionarios (GEO), lo que significa que se encuentran a 36.000 km de distancia desde la superficie de la tierra lo que implica una mayor latencia y con ello otras desventajas frente a Starlink, sin mencionar la parte física en cuanto su infraestructura y su operación.

La facilidad en el empleo de las antenas Starlink como la portabilidad también es un punto a favor. Pues cualquier persona puede aprender a operar uno de estos dispositivos en menos de una hora. No requiere de años de entrenamiento técnico o capacitación, ni conocimientos especializados en este tipo de dispositivos. Simplemente enciende el equipo, apunta hacia el cielo y ya cuenta con el servicio de internet. Es tan simple como usar un celular. Esta simplicidad operacional contrasta drásticamente con los sistemas militares tradicionales que requieren de personal especializado, certificado y con procedimientos complejos de instalación y mantenimiento.

En cuanto a costos, también favorecían estas soluciones, teniendo en cuenta que los planes y los equipos son asequibles económicamente en el mercado de estas tecnologías, resaltando que los equipos son propiedad del usuario y no exige una cláusula de permanencia (https://www.starlink.com/co/service-plans), todos estos factores hacen que sean más atractivos y como una posible alternativa más precisa para garantizar la calidad y la conectividad de las comunicaciones.

Establecer una red de internet de alta velocidad significa poder transmitir video en tiempo real, descargar imágenes de satélite de alta resolución y usar aplicaciones modernas para el desarrollo de las operaciones militares (Logic Fruit Technologies. (2024). Secured Communication Solutions in Defense & Military) . Las nuevas capacidades permiten integrar sistemas de información geográfica avanzados, comunicaciones multimedia y plataformas en que se planean y ejecutan las operaciones.

Países que emplean satélites StarLink en operaciones militares

País	Empleo
Ucrania	Como herramienta esencial para comunicaciones de mando, coordinación de drones, logística, internet en bases avanzadas y respaldo en zonas donde la infraestructura convencional fue destruida. https://www.dw.com/es/qu%C3%A9-pasar%C3%ADa-si-eeuu-desconectara-starlink-en-ucrania/a-71839124
Estados Unidos	Soporte a bases aéreas y navales, demostraciones de conectividad, y pruebas de interoperabilidad entre sistemas de mando y control durante maniobras https://danielmarin.naukas.com/2024/06/30/la-megaconstelacion-militar-starshield-de-spacex-toma-forma/
Brasil	Para mantener conectividad en zonas aisladas, particularmente en la Amazonía y zonas marítimas, facilitando ejercicios de patrulla, adiestramiento y operaciones logísticas. https://apublica.org/2024/10/starlink-militares-usam-internet-via-satelite-de-elon-musk-sem-teste-de-seguranca-da-rede/#

Los Peligros Ocultos

Cuando Rusia atacó a Ucrania

Los eventos de febrero de 2022 cambiaron todo. Los ataques rusos contra las redes de Viasat no fueron accidentes ni efectos colaterales. Fueron ataques deliberados y bien planeados contra infraestructura civil que apoyaba operaciones militares (CISA, 2022). Los rusos sabían exactamente lo que estaban haciendo: cortar las comunicaciones para sembrar caos antes de la invasión. La precisión y sincronización de estos ataques demostró un nivel de planificación que había estado en desarrollo durante meses, posiblemente años, sugiriendo que las capacidades antisatélite formaban parte integral de la doctrina militar rusa moderna.

Lo más preocupante fue la sofisticación de los ataques. No fueron simples bloqueos de señales. Los rusos lograron ingresar en sus sistemas, manipular el software y causar daños permanentes a miles de terminales. Esto demostró que tenían capacidades técnicas específicamente desarrolladas para atacar sistemas satelitales comerciales. Los análisis posteriores revelaron que los atacantes habían estudiado detalladamente las vulnerabilidades específicas de cada sistema, desarrollando herramientas personalizadas para explotar debilidades que los fabricantes desconocían. Esta preparación sugiere programas de investigación especializados en guerra antisatélite que habían estado operando en secreto durante años.

Luego vinieron los ataques contra Starlink. Grupos asociados con la inteligencia rusa, especialmente uno conocido como Secret Blizzard, comenzaron a atacar dispositivos militares ucranianos que usaban estas antenas (TheSIGN, 2024). No atacaban los satélites directamente, sino que usaban técnicas más sutiles: infiltraban dispositivos móviles de los

soldados, instalaban software malicioso y robaban información sobre las ubicaciones y actividades de las tropas. Esta aproximación indirecta mostró comprensión sofisticada de cómo funcionan realmente las operaciones militares modernas, donde los sistemas satelitales se integran con múltiples dispositivos y redes locales.

La Agencia de Seguridad de Ucrania descubrió un programa malicioso específicamente diseñado para atacar sistemas Starlink, al que llamaron "Malware 4.STL" (Cyber Defense Magazine, 2024). Este programa usaba los teléfonos de los soldados para recopilar información sobre las antenas: dónde estaban ubicadas, qué tipo de datos transmitían y cuándo estaban más activas. Era una forma inteligente de atacar: en lugar de bloquear las señales directamente, recopilaban inteligencia para ataques futuros más efectivos. El malware demostraba conocimiento detallado del protocolo de comunicaciones interno de Starlink y capacidad de operar sin detección durante períodos extendidos.

Las Vulnerabilidades Técnicas

Los investigadores de seguridad habían estado advirtiendo sobre estos problemas durante años. Santamarta (2018) había documentado vulnerabilidades serias en terminales satelitales que incluían puertas traseras aparentes, contraseñas fijas en el software y protocolos de comunicación inseguros. Pero la industria no prestó mucha atención hasta que empezaron los ataques reales. La resistencia de la industria a implementar mejoras de seguridad se debió parcialmente a consideraciones de costo y la percepción de que las amenazas eran teóricas más que prácticas. Esta situación cambió después de los eventos en Ucrania, cuando quedó claro que las vulnerabilidades académicas se habían convertido en vectores de ataque operacionales.

Lennert Wouters, especialista en ciberseguridad de la Universidad KU Leuven (Lovaina), Bélgica, demostró algo particularmente alarmante en una conferencia de seguridad. Con un chip modificado que costaba apenas 25 dólares, pudo hackear un terminal StarLink y evadir todas sus medidas de seguridad. Esto mostró que los ataques no requerían recursos enormes ni tecnología militar avanzada. Un atacante inteligente con conocimientos básicos de electrónica podía comprometer estos sistemas. La demostración fue especialmente impactante porque usó componentes disponibles comercialmente y técnicas documentadas en literatura académica, sugiriendo que cualquier adversario con recursos modestos podía replicar el ataque.

Las investigaciones posteriores fueron aún más preocupantes. Liu et al. (2024) encontraron evidencia de que más de 8,675 terminales Starlink habían sido usados para actividades maliciosas, incluyendo ataques automatizados contra otros sistemas. Esto significaba que la red no solo era vulnerable a ataques externos, sino que también podía ser usada como plataforma para atacar otros objetivos. Los terminales comprometidos formaban una red distribuida (botnet) que podía ser controlada remotamente para lanzar ataques coordinados, convirtiendo la infraestructura de comunicaciones en un arma cibernética dirigida contra otros sistemas.

El estudio identificó más de 8,700 vulnerabilidades de seguridad en la red, desde problemas menores hasta fallas críticas que podían permitir control total de los terminales. Lo más preocupante era que muchas de estas vulnerabilidades existían por diseño: los sistemas estaban optimizados para facilidad de uso y costo, no para seguridad militar. La arquitectura fundamental priorizaba accesibilidad y escalabilidad sobre protección,

reflejando las prioridades del mercado comercial donde la seguridad militar no era una consideración primaria.

Las Amenazas Específicas

Interceptación y Espionaje

Escuchar conversaciones militares ajenas es una práctica tan vieja como la guerra misma. Lo que ha cambiado es qué tan fácil se ha vuelto hacerlo. Graham et al. (2020) explican que cualquier persona con equipos de radioaficionado puede interceptar señales satelitales básicas. Aunque descifrar el contenido requiere más recursos, simplemente saber cuándo y desde dónde se comunican las tropas ya es información valiosa. Las técnicas de análisis de tráfico permiten extraer inteligencia significativa incluso de comunicaciones cifradas, mediante el estudio de patrones, volúmenes y sincronización de transmisiones. Los sistemas modernos de interceptación automatizada pueden procesar miles de comunicaciones simultáneamente, identificando patrones que serían imposibles de detectar mediante análisis manual.

Los patrones de comunicación revelan mucho sin necesidad de entender las conversaciones. Si una unidad aumenta súbitamente su tráfico de comunicaciones, probablemente está planeando algo importante. Si las comunicaciones se concentran en ciertas horas, eso indica rutinas que pueden ser explotadas. Si el volumen de datos transmitidos cambia, puede significar que están recibiendo nuevas órdenes. Los algoritmos de aprendizaje automático pueden identificar correlaciones sutiles entre patrones de comunicación y actividades operacionales, permitiendo predicciones sobre operaciones futuras basadas únicamente en metadatos de tráfico (Ministerio de Defensa de España.

2024. *La inteligencia artificial como factor de transformación de las operaciones militares en el nivel operacional*)

Los analistas pueden rastrear terminales específicos y crear mapas detallados de movimientos militares. Cada terminal tiene características únicas, como una huella digital electrónica, que permite seguirlo a través del tiempo y el espacio. Esto es especialmente peligroso para las unidades especiales que dependen del secreto para sus operaciones. Las técnicas de fingerprinting electrónico han evolucionado para detectar diferencias mínimas en componentes de hardware, configuraciones de software y patrones de uso que hacen único cada terminal. Esta individualización permite seguimiento persistente incluso cuando se cambian identificadores superficiales como números de serie o direcciones de red.

Nogueira et al. (2019) documentan cómo esta información puede usarse para anticipar operaciones militares. Si los patrones muestran que una unidad se está moviendo hacia una zona específica con comunicaciones intensas, es probable que estén planeando una operación en esa área. Los grupos criminales pueden usar esta información para abandonar laboratorios de drogas, preparar emboscadas o simplemente evitar el contacto. La capacidad predictiva de estos análisis ha mejorado significativamente con el uso de inteligencia artificial que puede correlacionar múltiples fuentes de información para generar predicciones operacionales con precisión alarmante.

Bloqueo e Interferencia

Bloquear comunicaciones militares ha sido una táctica de guerra durante décadas. Lo nuevo es qué tan sofisticadas se han vuelto estas técnicas. Ya no se trata simplemente de transmitir ruido para saturar las frecuencias. Los sistemas modernos pueden adaptar sus ataques en tiempo real, seguir cambios de frecuencia e imitar señales legítimas para

confundir a los receptores. Los jammers modernos incorporan algoritmos de seguimiento adaptativo que pueden identificar y contrarrestar automáticamente las técnicas anti-interferencia que usan los sistemas objetivo. Esta competencia electrónica armamentista ha llevado a sistemas de interferencia cada vez más sofisticados que pueden operar autónomamente durante períodos extendidos.

El bloqueo de enlaces ascendentes es particularmente efectivo porque se puede hacer desde tierra, relativamente cerca de las tropas objetivo. Un transmisor de interferencia bien posicionado puede silenciar fácilmente a una unidad militar que depende de un terminal satelital de baja potencia. Esto es especialmente preocupante para patrullas pequeñas o unidades especiales que operan lejos de apoyo. Los transmisores portátiles de interferencia ahora son mucho más pequeños, permitiendo que algunos grupos atacantes los transporten y posicionen estratégicamente cerca de unidades militares sin ser detectados. La geografía montañosa de Colombia proporciona múltiples posiciones ventajosas desde donde es posible lanzar ataques de interferencia efectivos.

In Compliance Magazine (2024) describe técnicas de interferencia adaptativa que pueden seguir automáticamente los intentos del sistema de cambiar frecuencias o protocolos. Estos sistemas "inteligentes" aprenden de los intentos de defensa y se adaptan para mantener la interferencia efectiva. Es como un juego de gato y ratón, pero automatizado y a velocidad electrónica. Los sistemas más avanzados incorporan capacidades de aprendizaje automático que pueden predecir las respuestas defensivas y preparar contramedidas antes de que se implementen, creando un ciclo de interferencia persistente que es extremadamente difícil de romper.

Engaños y Señales Falsas

Enviar señales falsas para confundir al enemigo es otra táctica antigua que se ha modernizado considerablemente. Los ataques de "spoofing" pueden hacer que un terminal militar piense que está recibiendo órdenes legítimas cuando en realidad está siendo manipulado por el enemigo. Falco y Boschetti (2021) documentan casos donde estos ataques han logrado engañar incluso a sistemas militares sofisticados. La efectividad de estos ataques ha aumentado dramáticamente con el desarrollo de sistemas de inteligencia artificial que pueden analizar y replicar patrones de comunicación legítimos con precisión extraordinaria.

El caso más famoso ocurrió en 2011, cuando Irán logró derribar un drone estadounidense RQ-170 usando señales GPS falsas. Los iraníes no dispararon ningún misil ni usaron jamming tradicional. Simplemente enviaron señales GPS falsas que hicieron que el drone pensara que estaba volando sobre Afganistán cuando en realidad estaba sobre territorio iraní. El drone aterrizó "suavemente" en Irán, creyendo que había regresado a su base. Este incidente demostró que los ataques de spoofing podían ser más efectivos que las contramedidas tradicionales, ya que explotaban la confianza de los sistemas en sus propios sensores.

En el contexto de las comunicaciones, estos ataques pueden ser usados para insertar información falsa en los canales militares. Un atacante sofisticado podría enviar órdenes falsas que parezcan venir de comandos superiores, reportes de inteligencia modificados o incluso coordenadas incorrectas para ataques aéreos. La clave está en hacer que la información falsa sea lo suficientemente convincente para pasar desapercibida. Los sistemas modernos de spoofing pueden replicar no solo el contenido de las comunicaciones

sino también los patrones técnicos, tiempos de transmisión y características de señal que los operadores usan para verificar autenticidad.

Massimi et al. (2023) explican cómo estos ataques se pueden combinar con ingeniería social para ser más efectivos. Los atacantes pueden usar información obtenida de fuentes abiertas (redes sociales, noticias, etc.) para crear mensajes falsos que sean creíbles. Si saben que una unidad está operando en cierta área y que hay reportes de actividad enemiga, pueden enviar alertas falsas que causen confusión o desvíen recursos. La proliferación de información en fuentes abiertas ha facilitado enormemente la construcción de engaños convincentes, ya que los atacantes pueden correlacionar múltiples fuentes de información pública para crear narrativas falsas pero verosímiles.

Impacto en las Operaciones Militares

Perder comunicaciones durante una operación militar es como quedar ciego en medio del combate. Los comandantes pierden visibilidad sobre lo que está pasando en el terreno. Las unidades en el área no pueden recibir órdenes actualizadas ni reportar novedades a tiempo. La coordinación se vuelve imposible y cada unidad tiene que improvisar basándose en información desactualizada. Esta fragmentación de comando y control puede convertir rápidamente una operación coordinada en múltiples acciones independientes que pueden interferir entre sí o duplicar esfuerzos, lo que disminuye notablemente la efectividad general.

Lewis (2014) describe cómo la manipulación de comunicaciones puede ser peor que simplemente perderlas. Si los comandantes reciben información incorrecta pero creíble, pueden tomar decisiones que activamente perjudican la operación. Las unidades pueden ser enviadas a lugares equivocados, los recursos pueden ser desaprovechados en objetivos

falsos y el elemento sorpresa puede perderse completamente. La información falsa puede propagarse a través de múltiples niveles de comando antes de ser detectada, amplificando sus efectos destructivos y creando confusión que puede durar horas o días.

Problemas Logísticos

Las operaciones logísticas modernas son increíblemente complejas y dependen totalmente de comunicaciones confiables. Rastrear inventarios, coordinar movimientos de suministros y gestionar la cadena de abastecimiento requiere información actualizada constante. Cuando las comunicaciones fallan, toda la máquina logística puede colapsar rápidamente. Los sistemas de gestión logística automatizada procesan miles de transacciones diarias, desde solicitudes de municiones hasta programación de mantenimiento de equipos. La interrupción de estos flujos de información puede crear efectos en cascada que se extiende mucho más allá de las unidades inmediatamente afectadas.

Los sistemas automatizados de gestión logística son especialmente vulnerables porque dependen de datos precisos y actualizados. Si los sistemas reportan ubicaciones incorrectas de suministros o inventarios falsos, las decisiones logísticas serán incorrectas. Recursos escasos pueden ser enviados a lugares equivocados mientras unidades que los necesitan urgentemente se quedan sin apoyo. La automatización que hace más eficientes las operaciones también crea vulnerabilidades centralizadas donde errores o ataques pueden tener efectos multiplicados a través de toda la red logística.

La coordinación de evacuaciones médicas representa un caso especialmente crítico. Los sistemas de telemedicina que permiten consultas médicas remotas dependen de comunicaciones de alta calidad. Si estas comunicaciones son interrumpidas o

comprometidas durante una emergencia médica, las consecuencias pueden ser fatales. Coordenadas incorrectas para evacuación pueden enviar helicópteros médicos a lugares equivocados. Los protocolos de evacuación médica en Colombia involucran coordinación compleja entre unidades terrestres, de aviación, hospitales de campaña y frecuentemente instalaciones civiles. La falla de comunicaciones en cualquier punto de esta cadena puede resultar en retrasos que comprometen la supervivencia de heridos.

Los ataques dirigidos específicamente contra sistemas logísticos pueden ser usados para debilitar las capacidades militares sin enfrentamientos directos. Si se puede interrumpir el suministro de municiones, combustible o alimentos, las tropas se ven forzadas a reducir operaciones o abandonar posiciones. Es una forma de guerra económica que puede ser muy efectiva con recursos relativamente limitados. Los grupos criminales en Colombia han mostrado un entendimiento de estos principios, atacando frecuentemente movimientos motorizados de suministros e instalaciones logísticas para degradar capacidades militares indirectamente.

Estrategias de Protección

La lección más importante es no depender de un solo sistema para algo tan crítico como las comunicaciones militares. Diversificar significa usar múltiples proveedores, diferentes tecnologías y varios métodos de respaldo. Si un sistema falla o es atacado, los otros pueden mantener las operaciones funcionando. La diversificación real requiere comprensión profunda de las arquitecturas fundamentales de diferentes sistemas para asegurar que no compartan vulnerabilidades comunes que podrían ser explotadas simultáneamente. Los planificadores militares deben considerar no solo diversidad técnica

sino también diversidad geográfica, política y económica en sus proveedores de comunicaciones.

Esto no significa simplemente comprar antenas de diferentes marcas. Significa usar tecnologías fundamentalmente diferentes que no comparten las mismas vulnerabilidades. Los sistemas geoestacionarios tradicionales funcionan de manera muy diferente a las constelaciones como Starlink. Aunque pueden ser menos modernos, también son menos vulnerables a ciertos tipos de ataques. La diversificación técnica efectiva debe incluir sistemas que operen en diferentes bandas de frecuencia, usen diferentes protocolos de comunicación y dependan de infraestructuras de control terrestres geográficamente dispersas.

Los sistemas terrestres siguen siendo importantes como respaldo. Las radios HF pueden ser anticuadas, pero son independientes de infraestructura espacial que puede ser atacada. Las comunicaciones por microondas pueden tener alcance limitado, pero son difíciles de interceptar desde lejos. Las redes celulares tácticas pueden ser lentas, pero están bajo control nacional. Cada tecnología tiene ventajas específicas que pueden ser críticas en circunstancias particulares. La integración efectiva de múltiples sistemas de comunicación requiere desarrollo de protocolos y procedimientos que permitan transición rápida entre sistemas cuando sea necesario.

Protección Adicional

Usar sistemas comerciales no significa aceptar sus niveles de seguridad comerciales. Las comunicaciones militares necesitan protección adicional que vaya más allá de lo que ofrecen los proveedores. Esto significa agregar capas extra de cifrado, autenticación más robusta y monitoreo continuo de la integridad de las comunicaciones.

Los sistemas comerciales están diseñados para amenazas comerciales típicas, no para adversarios sofisticados con recursos estatales y motivaciones militares o criminales específicas.

El cifrado independiente es especialmente importante. En lugar de confiar solo en la protección que proporciona el proveedor comercial, las Fuerzas Militares deben agregar su propio cifrado antes de transmitir información sensible. Esto significa que incluso si los sistemas comerciales son comprometidos, la información militar sigue protegida por sistemas controlados por la institución. Los sistemas de cifrado militar deben usar algoritmos y llaves completamente independientes de cualquier sistema comercial, asegurando que el compromiso de un sistema no afecte la seguridad del otro.

La autenticación debe verificar no solo quién está enviando mensajes, sino también que los mensajes no han sido alterados en tránsito. Esto requiere sistemas que puedan detectar manipulación sutil de comunicaciones, no solo ataques obvios. Los métodos deben incluir verificación de identidad de dispositivos además de usuarios individuales. Los protocolos de autenticación para uso militar deben ser más robustos que los estándares comerciales, incorporando múltiples factores de verificación y técnicas de validación continua durante sesiones de comunicación.

El monitoreo continuo debe detectar anomalías que puedan indicar ataques en progreso. Esto incluye cambios en patrones de tráfico, interferencias inusuales y comportamientos extraños de los sistemas. Los analistas necesitan herramientas especializadas para reconocer indicadores de ataques contra sistemas satelitales específicamente. Los sistemas de monitoreo deben incorporar inteligencia artificial capaz

de detectar desviaciones sutiles de patrones normales que podrían indicar infiltración o manipulación por adversarios sofisticados**.**

Colombia necesita desarrollar capacidades internas para entender, evaluar y proteger sistemas de comunicación satelital. Esto no significa necesariamente construir satélites propios inmediatamente, sino desarrollar el conocimiento y las habilidades necesarias para ser menos dependiente de proveedores externos. El desarrollo de capacidades internas debe seguir un enfoque progresivo que comience con comprensión básica de tecnologías satelitales y evolucione gradualmente hacia capacidades de diseño y construcción independientes.

Los centros de operaciones cibernéticas necesitan personal especializado en tecnologías satelitales. Esto requiere entrenamiento específico que va más allá de la ciberseguridad tradicional. Los analistas necesitan entender cómo funcionan las comunicaciones satelitales, qué tipos de ataques son posibles y cómo detectar y responder a amenazas específicas. El entrenamiento debe incluir aspectos técnicos de sistemas satelitales, pero también comprensión de las implicaciones operacionales y estratégicas de diferentes tipos de vulnerabilidades.

Los programas de investigación y desarrollo pueden crear soluciones adaptadas a necesidades específicas. Empezando por el Comando de Apoyo Tecnológico del Ejercito Nacional, el Ministerio de Defensa de Colombia, en coordinación con las Fuerzas Militares, impulsa la "Fuerza Innovación", un hub nacional multisectorial de colaboración entre Estado, universidades y sector productivo. Las universidades pueden contribuir con investigación fundamental, mientras que la industria privada puede desarrollar aplicaciones prácticas. La cooperación con países aliados puede acelerar el desarrollo mientras se

mantiene control nacional sobre tecnologías críticas. Los programas de investigación deben enfocarse en problemas específicos que enfrenta Colombia, como comunicaciones en ambientes de selva tropical o protección contra amenazas asimétricas de grupos no estatales.

El desarrollo de capacidades satelitales propias debe verse como una inversión a largo plazo en soberanía tecnológica. Aunque los costos iniciales son altos, el control nacional sobre comunicaciones críticas justifica la inversión. Un programa puede empezar con capacidades básicas y expandir gradualmente según sea factible económicamente. La cooperación regional con otros países latinoamericanos puede hacer más viable el desarrollo de capacidades satelitales compartidas que serían demasiado costosas para cualquier país individual.

Recomendaciones Prácticas

Avanzar hacia un sistema integral para la gestión de riesgos e incidentes que utilice inteligencia artificial, pero desde una perspectiva cercana y práctica: lo ideal es combinar herramientas inteligentes que ayuden a vigilar y proteger las infraestructuras y servicios tecnológicos, detectando rápidamente cualquier comportamiento extraño para responder sin demoras. El uso de estos recursos, más allá de la automatización, permite anticipar problemas, documentar los incidentes de manera ordenada y tomar mejores decisiones frente a las crisis. Apostar por la inteligencia artificial en este proceso no solo mejora la capacidad de reacción y protección, sino que facilita el trabajo diario de las personas y aporta tranquilidad, sabiendo que cuentan con el respaldo de soluciones que se adaptan y aprenden de cada situación.

Fomentar la innovación y establecer centros de excelencia en ciberseguridad para impulsar el desarrollo de nuevas soluciones y mejores prácticas en la protección digital. Estos centros deben ser espacios colaborativos donde expertos, académicos y profesionales puedan trabajar juntos, compartir conocimientos y experimentar con tecnologías de vanguardia. Promover la innovación en este ámbito no solo fortalece las defensas frente a amenazas actuales, sino que también prepara a las organizaciones y al país para enfrentar los desafíos futuros con creatividad y eficacia. Así se construye una comunidad sólida y continuamente actualizada que aporta seguridad, confianza y crecimiento sostenible en el entorno digital.

Impulsar la ciberdefensa a través de simulaciones y el uso de tecnologías emergentes, partiendo de una visión práctica y cercana, incorporando ejercicios simulados ayuda a preparar mejor a las personas para afrontar situaciones reales, permite aprender de los errores en entornos controlados y fortalecer la reacción ante posibles amenazas. Aprovechar herramientas innovadoras y nuevas tecnologías como entornos virtuales, sensores inteligentes y análisis avanzado contribuye a anticipar riesgos y adaptar las respuestas. De esta manera, se crea una cultura de prevención y mejora continua que facilita el trabajo cotidiano y brinda mayor confianza, al saber que la defensa tecnológica evoluciona constantemente frente a los desafíos modernos.

Desarrollar e implementar un programa de formación en gestión de incidentes pensado para fortalecer las capacidades de respuesta de todas las personas involucradas. Este programa debe ofrecer herramientas claras, ejercicios prácticos y espacios de aprendizaje colaborativo, de modo que cada participante sepa cómo actuar ante situaciones inesperadas y pueda aportar con confianza en la resolución de problemas. Capacitar y

sensibilizar de manera continua, adaptando los contenidos a las necesidades reales y fomentando el intercambio de experiencias, contribuye no solo a mejorar el manejo de incidentes, sino también a crear un ambiente de trabajo más seguro y preparado ante cualquier desafío digital.

Una propuesta de adquisición de nuevos portafolios de seguridad en la nube como el proyecto de AWS (Amazon Web Service), integra los principios clave para el diseño y operación de una arquitectura espacial híbrida de soporte militar en el contexto del "AWS Proyecto KUIPER". Enumera los cuatro pilares principales que deben ser garantizados en una solución tecnológica satelital y de nube para apoyo militar: seguridad, desempeño, confiabilidad y escalabilidad. En esencia esta infraestructura prioriza la protección ante riesgos y amenazas, ofrecer alto rendimiento en comunicaciones y operaciones, asegurar que los sistemas funcionen de manera continua y confiable, y estar preparada para crecer y adaptarse a diferentes necesidades y volúmenes de usuarios. Estos factores son fundamentales tanto en entornos militares como en aplicaciones críticas que requieren conectividad segura y robusta, aprovechando tecnologías satelitales (como Kuiper de AWS) y plataformas digitales avanzadas**.**

Acciones Inmediatas (Primeros 6 Meses)

El Ejército debe comenzar inmediatamente a implementar cifrado adicional en todas las comunicaciones sensibles. Esto puede hacerse con dispositivos portátiles que se conectan entre los terminales Starlink y los equipos de comunicación militar. Estos dispositivos deben usar algoritmos aprobados para información clasificada y deben ser independientes de cualquier sistema comercial. La implementación debe incluir protocolos

estrictos para gestión de llaves criptográficas y procedimientos para verificación regular de integridad de los sistemas de cifrado.

Los procedimientos operacionales deben cambiar para incluir verificación de información crítica a través de canales independientes. Los mensajes importantes deben confirmarse usando métodos alternativos como radio HF o comunicaciones terrestres cuando sea posible. Esto puede ser más lento, pero proporciona verificación independiente de que la información no ha sido manipulada. Los procedimientos deben especificar qué tipos de información requieren verificación independiente y establecer tiempos límite para confirmación que no comprometan la efectividad operacional.

El entrenamiento del personal debe incluir concientización sobre amenazas específicas contra comunicaciones satelitales (ciberseguridad). Los operadores deben aprender a reconocer señales de interferencia, ataques de bloqueo y comportamientos anómalos en los sistemas. Los procedimientos de reporte deben establecer canales claros para notificar incidentes sospechosos rápidamente. El entrenamiento debe ser práctico e incluir ejercicios que simulen diferentes tipos de ataques para que el personal pueda practicar respuestas apropiadas en ambientes controlados.

Deben establecerse inventarios completos de todos los terminales satelitales en uso, incluyendo ubicaciones, configuraciones y aplicaciones específicas. Esta información es necesaria para evaluación de riesgos y planificación de respuesta a incidentes. Los terminales deben auditarse regularmente para detectar modificaciones no autorizadas o comportamientos extraños. Los inventarios deben incluir también información sobre cadenas de suministro e historiales de mantenimiento para facilitar investigaciones forenses si se detectan compromisos.

Mejoras a Mediano Plazo (6 Meses a 2 Años)

Implementar centros de operaciones cibernéticas para desarrollar capacidades especializadas en el monitoreo de comunicaciones satelitales. Esto requiere equipos específicos para análisis de espectro, personal entrenado en tecnologías satelitales y procedimientos adaptados para amenazas contra sistemas espaciales. Las capacidades de monitoreo deben incluir detección de interferencias, análisis de anomalías en patrones de tráfico e identificación de señales de spoofing. Los centros deben establecer conexiones con organizaciones internacionales que monitorizan amenazas contra sistemas satelitales para intercambio de información sobre amenazas emergentes.

Los sistemas de respaldo deben mejorarse significativamente para proporcionar alternativas confiables cuando los sistemas comerciales no estén disponibles. Esto puede incluir actualización de redes radio existentes, implementación de comunicaciones por microondas tácticas y desarrollo de capacidades satelitales militares básicas. Los sistemas de respaldo deben ser testeados regularmente en condiciones realistas para asegurar que funcionarán cuando sean necesarios. La transición entre sistemas primarios y de respaldo debe ser practicada frecuentemente para minimizar interrupciones durante emergencias.

Los acuerdos con múltiples proveedores deben negociarse para reducir dependencia en un solo sistema. Estos acuerdos deben incluir garantías de disponibilidad durante crisis y acceso prioritario para aplicaciones militares. Los contratos deben especificar niveles de servicio y penalidades por incumplimiento. Los acuerdos deben también incluir provisiones para acceso a información técnica necesaria para operación independiente y mantenimiento de sistemas críticos. La negociación de contratos debe considerar implicaciones geopolíticas e incluir cláusulas que protejan intereses nacionales.

Los programas de desarrollo de personal deben crear expertos en tecnologías satelitales y ciberseguridad especializada. Esto puede incluir intercambio con organizaciones internacionales, entrenamiento avanzado y colaboración con universidades. La retención de personal especializado debe ser prioridad para evitar pérdida de conocimientos críticos. Los programas deben incluir tanto entrenamiento técnico como educación sobre implicaciones operativas y estratégicas de decisiones tecnológicas. El desarrollo de experiencia interna debe ser sistemático y sustentable a largo plazo.

Objetivos a Largo Plazo (2 a 5 Años)

Considerar el desarrollo de capacidades satelitales nacionales o regionales. Esto no significa necesariamente construir y lanzar satélites inmediatamente, sino desarrollar las capacidades técnicas necesarias para reducir la dependencia extranjera a largo plazo. El desarrollo de capacidades satelitales requiere una fuerte inversión en educación técnica, desarrollo industrial y cooperación internacional. Los beneficios a largo plazo de independencia tecnológica justifican los costos iniciales significativos.

La cooperación regional puede ser una alternativa más factible que el desarrollo completamente nacional. Países como Brasil, México y Argentina tienen experiencia en tecnologías satelitales. Una cooperación regional podría crear capacidades compartidas que sean más efectivas y económicas que esfuerzos nacionales aislados. La cooperación regional debe estructurarse para asegurar que Colombia mantenga control sobre aspectos críticos de seguridad nacional.

Los programas de investigación y desarrollo deben enfocarse en contramedidas específicas contra amenazas identificadas. Esto incluye tecnologías anti-interferencia, sistemas de detección de ataques y métodos mejorados de autenticación y cifrado. La

investigación debe involucrar centros de investigación, universidades, industria privada y cooperación internacional. Los programas de investigación deben equilibrar la investigación fundamental con el desarrollo de aplicaciones prácticas que puedan implementarse en plazos realistas.

Las regulaciones nacionales deben evolucionar para abordar amenazas emergentes y nuevas tecnologías. El marco legal debe ser lo suficientemente flexible para adaptarse a cambios rápidos en tecnología y amenazas, pero lo suficientemente específico para proporcionar orientación clara a usuarios y proveedores. Las regulaciones deben desarrollarse en coordinación con las partes interesadas relevantes y deben considerar implicaciones económicas además de consideraciones de seguridad. El proceso regulatorio debe incluir mecanismos para la actualización periódica de estándares y requisitos basados en lecciones aprendidas y evolución de amenazas.

Lecciones de otros países

Experiencias Internacionales

Estados Unidos aprendió lecciones valiosas durante conflictos en Iraq y Afganistán sobre vulnerabilidades en comunicaciones militares. Los drones militares en Iraq transmitían video sin cifrado, permitiendo que insurgentes interceptaran las transmisiones usando software comercial básico. Esto llevó a mejoras significativas en protocolos de seguridad y procedimientos operacionales. Las experiencias estadounidenses demostraron que incluso sistemas diseñados para uso militar pueden tener vulnerabilidades graves cuando se implementan sin consideración adecuada de amenazas específicas del ambiente operacional.

La OTAN ha desarrollado estándares específicos para uso de tecnologías comerciales en aplicaciones militares. Estos estándares reconocen que las tecnologías comerciales son inevitables debido a su superioridad técnica y ventajas de costo, pero establecen requisitos mínimos de seguridad y procedimientos de evaluación de riesgos. Los estándares de la OTAN equilibraron la necesidad práctica con los requisitos de seguridad, proporcionando un modelo para otros países que enfrentan desafíos similares.

Israel ha desarrollado un enfoque híbrido que combina tecnologías comerciales con capacidades nacionales especializadas. Usan sistemas comerciales para aplicaciones no críticas pero mantienen sistemas nacionales independientes para comunicaciones más sensibles. Esta aproximación permite aprovechar beneficios comerciales mientras se protegen capacidades críticas. El modelo israelí demuestra que es posible mantener la independencia estratégica mientras se benefician de la innovación comercial.

Los países europeos han comenzado a desarrollar capacidades satelitales independientes específicamente por preocupaciones de seguridad sobre dependencia en sistemas estadounidenses. El programa IRIS2 (Infrastructure for Resilience, Interconnectivity and Security by Satellite) de la Unión Europea busca crear alternativas europeas para comunicaciones gubernamentales críticas. Casaril y Galletta (2024) analizan cómo estas iniciativas equilibran cooperación internacional con soberanía tecnológica. Las iniciativas europeas demuestran que Incluso aliados cercanos pueden decidir que la independencia tecnológica merece una inversión sustancial para su desarrollo.

Análisis y resultados

Para establecer claramente los elementos de relación y análisis de resultados, se parte conceptualizando dos elementos de correlación, la **superficie de ataque** que corresponde al conjunto total de puntos de entrada, vulnerabilidades y vectores de ataque que un atacante podría aprovechar para acceder de forma no autorizada a los sistemas, datos o redes de una organización según el NIST (National Institute of Standards and Technology, 2018), en la medida de la magnitud y la complejidad de la arquitectura que configura una superficie de ataque, las probabilidades de riesgo de sufrir incidentes de seguridad también aumentan, en cuanto al **tiempo de exposición**, este término hace referencia al periodo durante el cual una vulnerabilidad está presente y un sistema es susceptible a ataques (ISACA, 2023). Partiendo de estas definiciones se hace la relación con los resultados encontrando que la relación en un sistema SATCOM respecto al tiempo de exposición es directamente proporcional a la probabilidad de recibir intentos de ataques, explotación de vulnerabilidades y riesgos de interceptación entre otros, relacionándose directamente con los elementos que integran la superficie de ataque, haciendo más vulnerable el sistema en la medida en que la arquitectura de la superficie de ataque se mantenga, aumentando el riesgo de vulnerabilidad, por lo tanto se debe trabajar en los análisis de riegos conjuntos e independientes para establecer matrices de riesgos.

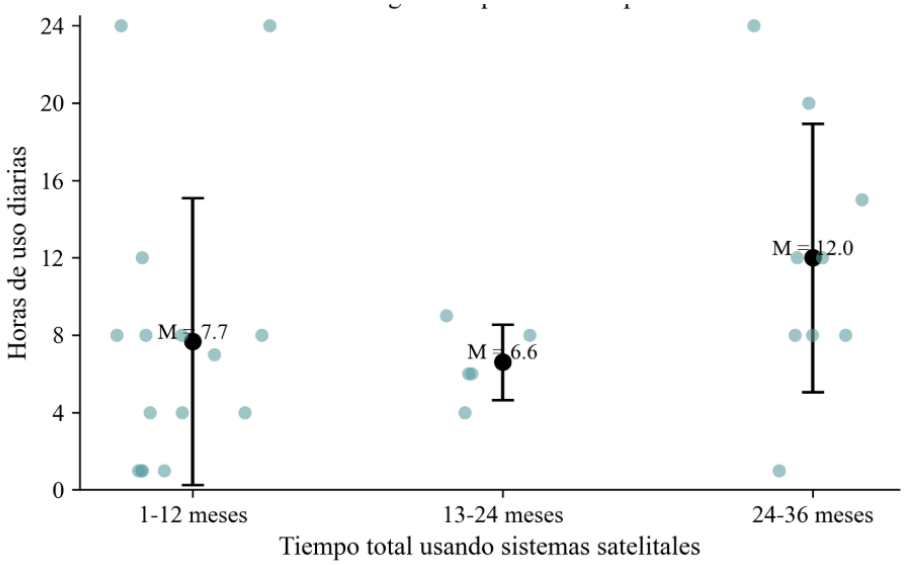
Sin embargo, al mantener el control y monitoreo constante de los elementos que conforman la superficie de ataque (digitales, físicos y social o humana) en relación con el tiempo de exposición o ventana de exposición, puede impactar en la reducción de las vulnerabilidades sin necesidad de limitar el tiempo de empleo, si bien es cierto las

vulnerabilidades son inevitables, no solo se trata de pensar en protección sino en desarrollar maneras de detección y respuesta.

Por lo anterior una consideración que resalta el estudio realizado el empleo de las antenas satelitales comerciales reducen esa ventana de exposición, teniendo en cuenta que si el usuario desea realizar una descarga de un archivo del tamaño de 1gb, este tardara aproximadamente 54 segundos, a diferencia de una red institucional que puede tardar hasta 34 minutos, aumentando el tiempo de exposición frente a las vulnerabilidades que un sistema pueda tener, lo cual genera una tendencia creciente a la exposición de:

- Más oportunidades para ataques de denegación de servicio (DoS) o jamming.
- Más tiempo disponible para que un adversario intente explotar vulnerabilidades de la red satelital o del terminal.
- Mayor probabilidad de que los datos sean interceptados o que se intente una inyección de código malicioso.

Figura 1. Frecuencia de uso según tiempo total de experiencia satelital

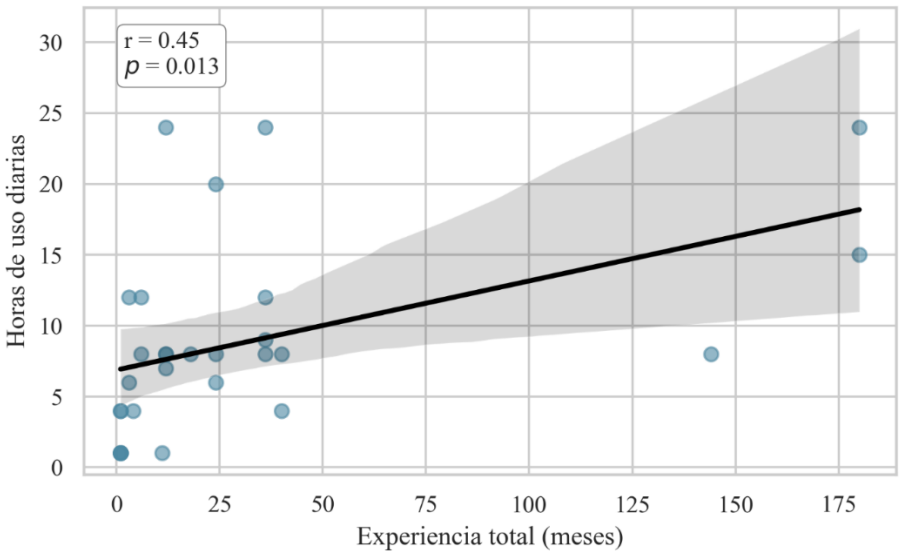


Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

La relación entre la experiencia total (en meses) y la frecuencia diaria de uso (en horas) para las unidades que hicieron parte de estudio, demuestra que, aunque existe una tendencia positiva: a mayor experiencia total, aumentan las horas de uso diarias. Este patrón se ve reflejado en la línea de regresión ajustada con una pendiente ascendente.

El coeficiente de correlación de Pearson (r = 0,45) indica una correlación moderada y positiva entre ambas variables, lo que sugiere que los individuos con más meses de experiencia tienden a utilizar el sistema o tecnología con mayor frecuencia diaria. El valor p = 0,013, muestra que esta asociación es estadísticamente significativa con una tendencia que representa el aumento de confianza y con ello un crecimiento en el riesgo.

Figura 2. Relación entre experiencia total y frecuencia diaria de uso



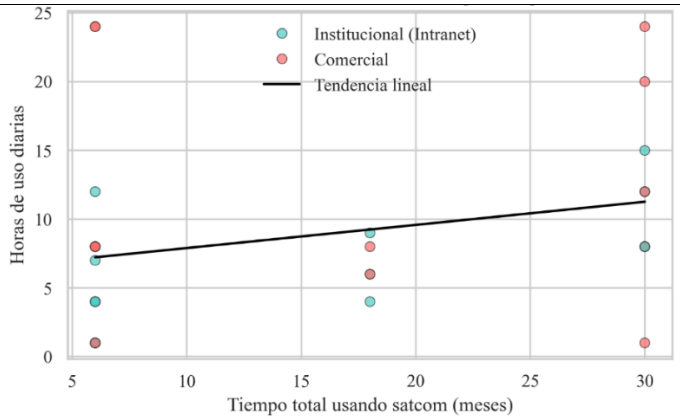
Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

El uso frecuente de sistemas SATCOM tanto institucionales como comerciales ante diversos niveles de experiencia, evidencia la diversidad en el conocimiento y cumplimiento de protocolos de seguridad por parte de los usuarios. Los resultados obtenidos demuestran que, incluso personas con experiencia significativa pueden llegar a usar redes comerciales, las cuales suelen presentar mayores vulnerabilidades frente a interceptaciones, manipulación de tráfico y ataques de ingeniería social.

El incremento en la frecuencia de uso diaria expone de manera proporcional mayores volúmenes de información, aumentando el riesgo de filtraciones o compromisos de datos críticos si no se adoptan medidas robustas de protección y monitoreo. Además, la alternancia entre redes institucionales y comerciales puede dificultar la estandarización de políticas de seguridad, generando brechas que pueden ser aprovechadas por actores maliciosos.

Estos hallazgos resaltan la necesidad de fortalecer la educación en ciberseguridad, promover las prácticas de acceso y uso de SATCOM. Esto implica el desarrollo y aplicación de estrategias de gestión de riesgos, autenticación y capacitación constante del personal, junto con el monitoreo activo de las redes utilizadas en todas las operaciones militares.

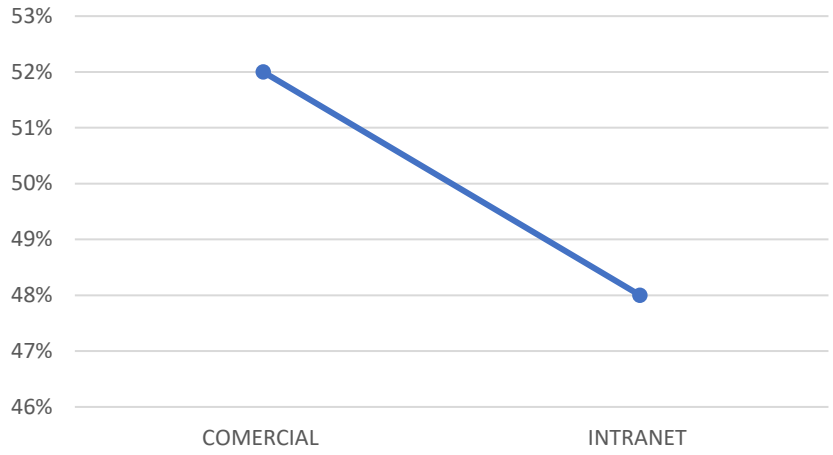
Figura 2. Tendencia de la frecuencia diaria vs tiempo de experiencia



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Se evidencio que solo el 48% de las unidades cuentan con una cobertura de red de datos institucional (intranet) que permite la ejecución de las diferentes actividades propias de la fuerza, el restante 52% corresponde al personal que por sus medios emplea otros medios comerciales con el propósito de dar cabal cumplimiento las tareas propias e inherentes de cada funcionario

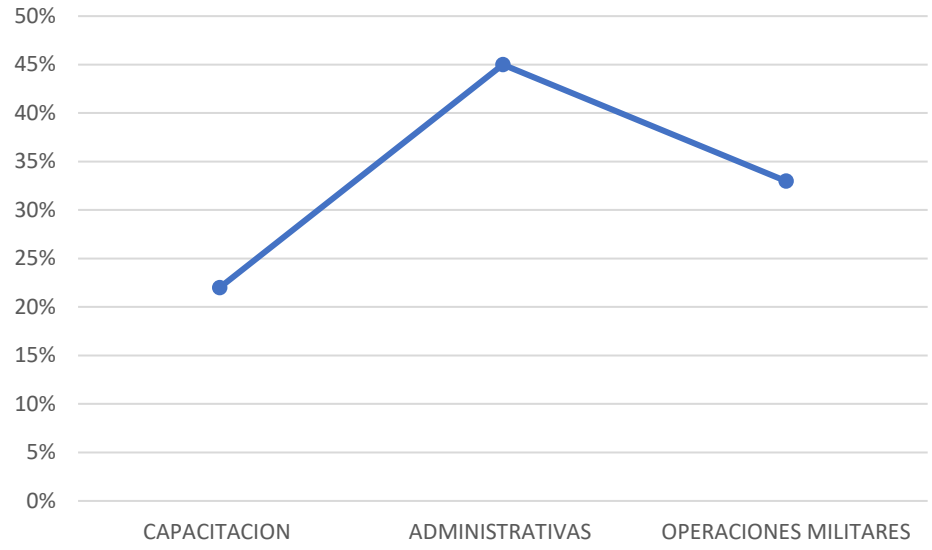
Figura 1. Comparación cobertura de datos en las unidades del Ejercito Nacional



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Una vez se determina que casi el 50% de las unidades gestiona la conectividad de datos a través de otros medios a los institucionales, se logra establecer en que tipo de actividades son empleados, observando el mayor porcentaje en funciones administrativas con un 45%, el 33% en operaciones militares lo cual genera una vulnerabilidad para las mismas y por último el 22% son utilizadas en procesos de capacitación o formación.

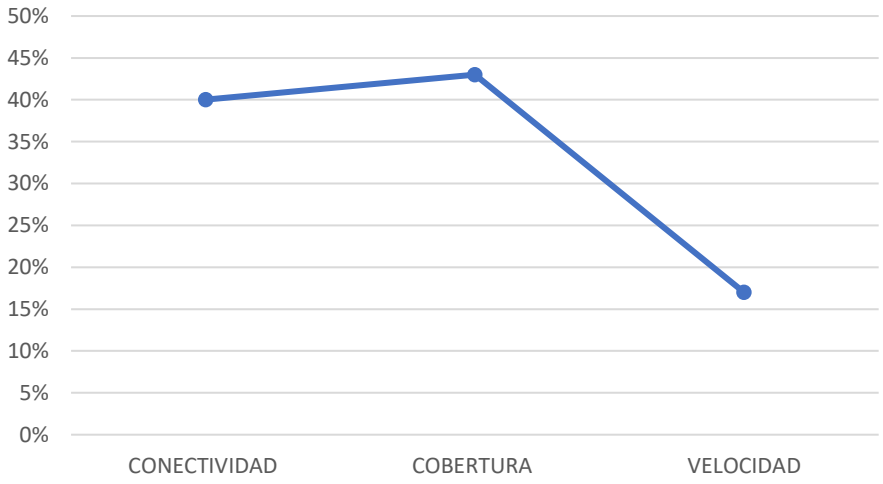
Figura 2. Empleo de las comunicaciones satelitales comerciales en el Ejercito Nacional



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Los motivos expuestos por el personal que emplean las comunicaciones comerciales, están relacionados con variables que no encuentran en la red institucional como lo son la conectividad en un 40%, la cobertura con un 43% y la velocidad con 17%.

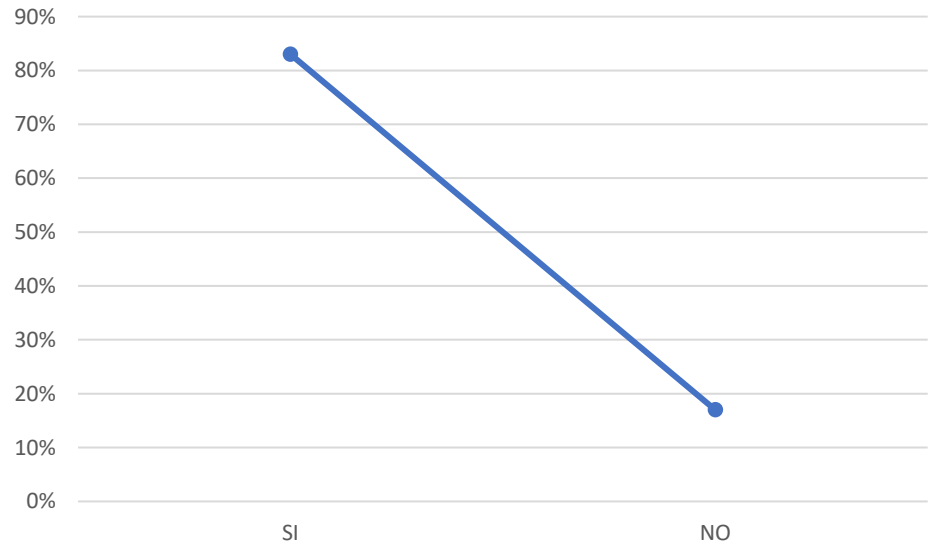
Figura 3. Motivos por los cuales se emplean las antenas satelitales comerciales



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Teniendo en cuenta los temas analizados anteriormente, se puede evidenciar que una solución aplicada en un término inmediato por sus ventajas es el empleo de medios alternos a los institucionales, y se marca en la tendencia al aumento de estos medios a través de las recomendaciones que hace el personal que las está utilizando, se encontró que más del 80% del personal que las emplea recomienda utilizarlas como solución al problema de conectividad.

Figura 4. ¿Recomienda el uso de las antenas satelitales comerciales en las unidades del Ejercito?

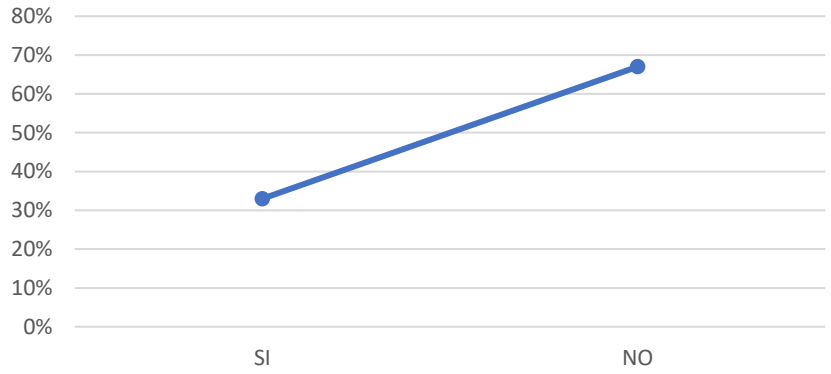


Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Se encontró que más del 60% del personal que emplea estos medios alternos, no aplica alguna medida de seguridad en el manejo de la información, exponiendo la misma a una variedad de amenazas de las cuales pueden ser víctimas, se podría deducir que esto sucede por desconocimiento de las nuevas amenazas en el medio cognitivo o por falta de concientización en el factor humano, por lo cual es necesario medidas de desarrollo de

capacidades que impacten en la educación, capacitación y concientización a todo el personal de la institución.

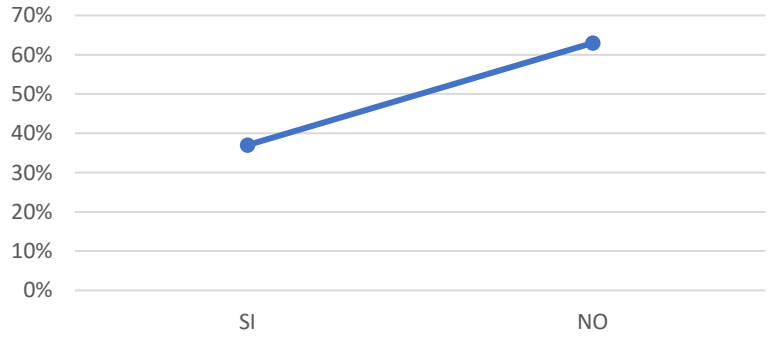
Figura 5. Implementa medidas de seguridad durante el empleo de las antenas satelitales comerciales



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Complementando el punto anterior, también se encontró que mas del 60% desconoce que el empleo de estos medios hace vulnerable la gestión de la información y que no representa algún tipo de riesgos.

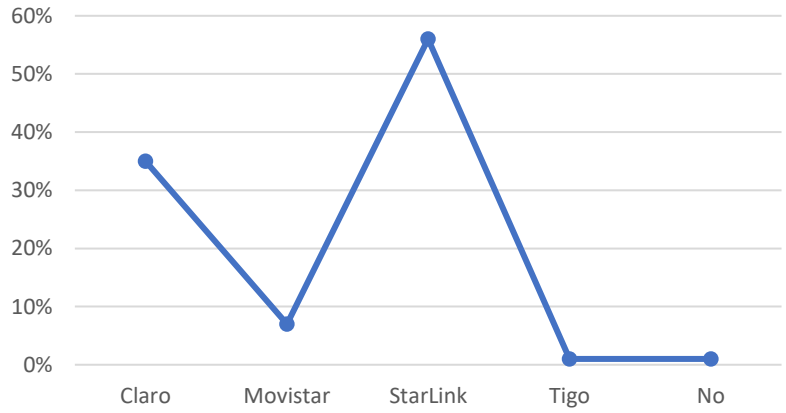
Figura 6. Considera que el uso de antenas satelitales comerciales representa riesgos



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Se encontró que en Colombia, existen mas de 18 proveedores de servicio de internet satelital, notando que solo cuatro de ellas son las mas empleadas en la institución para la solución a la problemática, resaltando entre ellas que la empresa de Starlink de SpaceX, que presenta la tendencia mas alta en el empleo, esto se debe a varios factores como los valores de adquisición y servicio que son mas económicos, es fácil de instalar y operar, su velocidad y cobertura tiene mayor ventaja frente a los demás, son dispositivos portátiles de fácil transporte y que no requiere de personal técnico especializado para su instalación o cambio de ubicación.

Figura 6. Considera que el uso de antenas satelitales comerciales representa riesgos



Fuente: elaboración propia con base en los datos recolectados por el instrumento de evaluación

Los resultados del estudio muestran que existe una baja frecuencia en la ejecución de auditorías técnicas, lo que ha permitido el incremento de vulnerabilidades que al momento podrían estar sin resolver. Estos hallazgos se ven reflejados en indicadores de

riesgo, evidenciando la necesidad de fortalecer los procesos de gestión de riesgos cibernéticos y aplicar un plan de monitoreo.

Es recomendable implementar una estrategia de evaluación fundamentada en indicadores de riesgo y en el fortalecimiento del cumplimiento regulatorio. Esta medida permitiría mejorar la resiliencia del sistema y reducir la superficie efectiva de ataque, optimizando la seguridad integral de la infraestructura.

Los indicadores de riesgo desempeñan un rol fundamental al permitir una medición objetiva del nivel de exposición y facilitar una evaluación continua de la seguridad. Para que estos sean efectivos, deben complementarse con auditorías periódicas, pruebas de penetración (pentesting) y sistemas de monitoreo de amenazas. Estas medidas permiten ajustar controles y protección. Siguiendo metodologías reconocidas como ISO 2001:2022, NIST RMF y Magerit, que proporcionan marcos sólidos para la gestión y mitigación de riesgos.

Magerit es tomado de la norma española une 71504:2008, que lo define como "un componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización e incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos".

En respuesta a los resultados obtenidos, se propusieron algunos indicadores que podrían ayudaran a monitorear la eficacia de las medidas de seguridad. Aplicando el análisis de la gestión del control, tal como lo define el marco MAGERIT, sugieren que los

controles existen, pero no son completamente efectivos ni están documentados de forma rigurosa.

La integración de estos indicadores aplicando marcos de referencia internacionales valida la robustez de la metodología empleada. La medición del TPDA (tiempo promedio de detección y alerta) y el TMRS (tiempo medio de respuesta y solución) es evidencia directa del cumplimiento de las funciones "Detectar" y "Responder" del Marco de Ciberseguridad NIST. De manera similar, la evaluación de la gestión del control es fundamental para la adhesión a las cláusulas de seguridad de la información de la norma ISO/IEC 27001. Esta alineación estratégica demuestra que la gestión de riesgos no solo es un ejercicio interno, sino una actividad que posiciona al Ejército Nacional dentro de un esquema de defensa globalmente reconocido y auditable, transformando las mediciones de riesgo en una herramienta estratégica de alto nivel, aplicando como base algunas de las clasificaciones de la teoría de la clasificación MAGERIT

Tabla 1. Escala de valoración del impacto de los riesgos

Impacto		
MA	Muy alto	5
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy bajo	1

Tabla 2. Escala de valoración de probabilidad de vulneración

Probabilidad de vulneración	
5	Prácticamente seguro
4	Probable
3	Posible
2	Poco probable
1	Muy raro

Valencia Duque, F. J., Marulanda Echeverry, C. E., & López Trujillo, M. (2024). *Modelos y marcos de referencia de gestión de riesgos en entornos digitales*

Tabla 3. Escala de valoración de gestión del control

Calificación de gestión del control	
1	Control no existente
2	Existe, pero no efectivo
3	Efectivo, pero no documentado
4	Efectivo y documentado

Tabla 4. Escala de valoración de impacto probabilidad y riesgo

Escalas					
Impacto			Probabilidad		Riesgo
5	MA	Muy alto	5	Prácticamente seguro	Crítico
4	A	Alto	4	Probable	Importante
3	M	Medio	3	Posible	Apreciable
2	B	Bajo	2	Poco probable	Bajo
1	MB	Muy bajo	1	Muy raro	Despreciable

Teniendo en cuenta lo anterior se presenta una tabla adicional con indicadores de riesgos específicos que podría ayudar a reducir el riesgo en el empleo de sistemas de comunicación satelital, enfocada

Tabla 5. Indicadores de riesgo.

Indicador de riesgo	Métrica
Número de puntos de entrada y servicios expuestos	Inventario actualizado de interfaces; porcentaje con control de acceso
Incidentes críticos detectados por periodo	Nº de incidentes / trimestre; tendencia trimestral
Vulnerabilidades sin solucion	% de vulnerabilidades críticas abiertas más de X días
Tiempo promedio de respuesta a incidentes	Horas entre detección y mitigación

Indicador de riesgo	Métrica
Auditorías y tests de penetración periódicos	Nº auditorías realizadas al año; resultados agrados
Cumplimiento de marcos regulatorios internacionales	% de controles alineados a UIT, NIST, ISO, FCC, IFT, CONPES
Registro de licencias, plataformas y servicios	Nº plataformas en cumplimiento; Nº registros y actualizaciones
Coordinación y reporte de incidentes entre organismos	Nº de incidentes reportados y gestionados en colaboración
Tasa de Vulnerabilidades Corregidas (TVC)	TVC=Vulnerabilidades IdentificadasVulnerabilidades Cerradas
Tiempo Promedio de Restauración del Servicio (TMRS)	TMRS=Nu´mero de Incidentes∑Tiempo de Indisponibilidad
Índice de Clics de Phishing Simulados (ICPS)	ICPS=Total de Personal ObjetivoNu´mero de Clicks×100
Índice de No Conformidad con Políticas de Seguridad (INCS)	INCS=Controles VerificadosHallazgos en Auditorı´as×100
Índice de Amenazas Cibernéticas (IAC)	N° de amenazas detectadas / N° de escaneos realizados X100
Tiempo Promedio de Detección de Amenazas (TPDA) y Tiempo Promedio de Restauración del Servicio (TMRS)	∑(Hora de Deteccion - Hora de Inicio del Incidente)/N° total de incidentes
Tasa de Parcheo y Actualización (TPA) y Tasa de	Vulnerabilidades Cerradas/ vuelnerabilidades identificadas

Indicador de riesgo	Métrica
Vulnerabilidades Corregidas (TVC)	
Nivel de Vulnerabilidad del Software del Terminal (VS)	Vulnerabilidades crıticas no Parcheadas/ total de dispositivos X100
Índice de Clics de Phishing Simulados (ICPS) y Índice de Confianza del Personal (ICP)	Numero de clics en correos falsos / Total de perosnal que recibio el correo
Nivel de Exfiltración de Datos (ED)	Volumen de Datos anómalos saliente/volumen de datos promedio salientes
Costo de Recuperación de Incidentes (CRI) y Retorno de Inversión en Ciberseguridad (ROI-C)	Perdidas Evitadas - Costo de Medidas de Seguridad/ costo de medidas de seguridad
Tasa de capacitación y sensibilización del personal	% empleados capacitados en seguridad satelital por semestre

Esta situación se encuentra relacionada con las falencias observadas en el cumplimiento normativo frente a marcos internacionales reconocidos. Particularmente los estándares establecidos por NIST y las directrices de la Unión Internacional de Telecomunicaciones (UIT) sugieren la implementación de ciclos más estrictos de monitoreo.

En este sentido el marco normativo colombiano (CONPES 3701; Ley 1273/09; Resolución 5569/18), mexicano (LFTR, IFT, coordinación UIT) y estadounidense (FCC, ITU-R, NIST) muestran diferencias en requerimientos de protección, licenciamiento y obligación de proceso de auditoría periódica. Mientras Colombia enfatiza la protección de infraestructura crítica y la integración civil-militar, México prioriza la coordinación internacional y el registro de frecuencias, en Estados Unidos predominan políticas de cielos abiertos y regulación flexible para fomentar la competencia, por consiguiente se presenta una tabla comparativa sobre el marco regulatorio en materia de ciberseguridad y telecomunicaciones para Colombia, México y Estados Unidos, que destaca las dimensiones normativas más relevantes y vigentes de cada país.

Tabla 6. análisis comparativo marco regulatorio regional.

Dimensión normativa	Colombia	México	Estados Unidos
Estructura nacional	colCERT (Incidentes) y CSIRT Gobierno (Gobierno Digital)	IFT (regulador autónomo); CSIRTs sectoriales	NIST (normas y marcos); FCC (regulación y licencias)
Leyes de ciberataques	Ley 1273/2009 (delitos informáticos); Decreto 620/2019–2020	Ley federal de protección de datos; política general de ciberseguridad IFT	FISMA; CMMC; HIPAA; leyes sectoriales (defensa, salud, energía)

Dimensión normativa	Colombia	México	Estados Unidos
Protección de datos	Ley 1581/2012 (protección de datos personales)	Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Leyes estatales y sectoriales; "Privacy Act"; GDPR referencia
Infraestructura Crítica	Guía ICC (2015); CONPES 3995/2020; Decreto 338/2022	Lineamientos técnicos del IFT e integración con CONATEL	Listado federal y sectorial, integración con CISA, NIST
Gestión de riesgos	Políticas CONPES 3995/2020 y Decreto 338/2022 de Seguridad Digital	Políticas y acciones IFT; requisitos para operadores y concesionarios	NIST Cybersecurity Framework (CSF); RMF obligatorio en gobierno federal
Normas técnicas	Adopción progresiva de estándares NIST, ISO 27001, UIT-R	Cumplimiento con UIT, transición IPv6, requisitos de categoría y acceso	NIST SP 800-53/171; referencia internacional para industria y gobierno

Dimensión normativa	Colombia	México	Estados Unidos
Sanciones y cumplimiento	Sanciones penales y administrativas, obligaciones a operadores	Supervisión técnica y legal del IFT, revisiones periódicas	Sanciones regulatorias, pérdida de contratos federales, investigaciones del DHS y FCC
Mecanismos de reporte	Reporte obligatorio a colCERT; atención a ICS/SCADA	Requisito para concesionarios y operadores sectoriales, y coordinación con IFT	Incidentes deben reportarse a CISA, DHS o sectores regulados según línea normativa

Conclusiones

Colombia enfrenta un dilema real con sus comunicaciones militares. Los sistemas tradicionales no funcionan lo suficientemente bien para operaciones modernas, pero las alternativas comerciales traen riesgos de seguridad de mucha atención. No hay soluciones perfectas, solo compromisos entre diferentes tipos de riesgos y beneficios. El desafío para el Ejercito es encontrar el balance óptimo que maximice capacidades operacionales mientras reduce vulnerabilidades estratégicas. Este equilibrio debe reevaluarse continuamente a medida que evolucionan el entorno de amenazas y las capacidades tecnológicas.

La experiencia internacional, especialmente los ataques documentados contra sistemas satelitales en Ucrania, demuestran que estas amenazas son reales y actuales, no problemas teóricos para el futuro. Existe grupos que han desarrollado capacidades específicas para atacar sistemas comerciales y han demostrado disposición para usarlas. La evidencia de Ucrania debería servir como un llamado de atención para todas las fuerzas militares que dependen de sistemas satelitales comerciales, demostrando que la superioridad tecnológica no garantiza protección contra adversarios determinados. Y que la tendencia de crecimiento en desarrollo tecnología en el marco de la 5G, exige mayor preparación y desarrollos que prevengan situaciones que comprometan la seguridad del estado.

Los grupos armados y organizaciones criminales tienen razones para interferir las comunicaciones militares, y algunos han mostrado capacidades tecnológicas crecientes. La geografía del país hace que las comunicaciones satelitales sean especialmente importantes, pero también crea dependencias que pueden ser explotadas. La combinación de terreno desafiante, adversarios adaptativos y recursos limitados crean un entorno particularmente vulnerable a la interrupción de los sistemas de comunicación.

Los beneficios operacionales de sistemas como Starlink son innegables. Han mejorado significativamente las capacidades de comunicación y coordinación del Ejército. El problema no es que estas tecnologías sean inherentemente malas, sino que son vulnerables por lo tanto deben ser entendidas, atendidas y mitigadas apropiadamente. El reconocimiento de estas vulnerabilidades no debería conducir al abandono de estas tecnologías, sino a una implementación más reflexiva que aborde los riesgos asociados.

El equilibrio entre beneficios operacionales y riesgos de seguridad requiere evaluación continua y ajustes basados en amenazas cambiantes y capacidades evolucionantes.

La ciberseguridad en sistemas satelitales requiere enfoques especializados que van más allá de la seguridad informática tradicional. Las amenazas son diferentes, las vulnerabilidades son diferentes y las contramedidas deben ser adaptadas específicamente para estos entornos únicos.

Colombia tiene la oportunidad de aprender de las experiencias de otros países y desarrollar enfoques que equilibren apropiadamente beneficios operacionales con imperativos de seguridad nacional. El costo de no actuar puede ser mucho mayor que el costo de implementar protecciones apropiadas.

Referencias

Anderson, C., & Johnson, M. (2003). The impressive psychology paper. Lucerne Publishing.

Ansong, S., Rankothge, W., & Ghorbani, A. A. (2024). Role of cybersecurity for a secure global communication eco-system: A comprehensive cyber risk assessment for satellite communications. Computers & Security, 128, 103-118.

Casaril, F., & Galletta, L. (2024). Securing SatCom user segment: A study on cybersecurity challenges in view of IRIS2. Computers & Security, 139, 103-115.

Castillo, J. (2018). Soberanía tecnológica y seguridad nacional en América Latina. Editorial Universitaria.

CISA - Cybersecurity and Infrastructure Security Agency. (2022, March 17). Strengthening cybersecurity of SATCOM network providers and customers. Cybersecurity Advisory AA22-076A.

CISA - Cybersecurity and Infrastructure Security Agency. (2022, May 10). U.S. government attributes cyberattacks on SATCOM networks to Russian state-sponsored malicious cyber actors.

CONPES 3854. (2016). Política Nacional de Ciberseguridad y Ciberdefensa. Consejo Nacional de Política Económica y Social, República de Colombia.

Cyber Defense Magazine. (2024, March 23). Cybersecurity threats in global satellite internet. Diálogo Américas. (2022, April 7). Colombia rises to the cyber challenge.

Directiva Permanente 300-28. (2018). Lineamientos de ciberseguridad y ciberdefensa para las Fuerzas Militares. Ministerio de Defensa Nacional, República de Colombia.

Espinosagiralt, J. (2023). Antenas satelitales y sus aplicaciones en comunicaciones críticas. Revista de Ingeniería de Telecomunicaciones, 45(3), 78-95.

Falco, G., & Boschetti, A. (2021). Commercial satellite vulnerabilities: A comprehensive analysis. International Journal of Critical Infrastructure Protection, 32, 100-115.

Foro Económico Mundial. (2021). The Global Risks Report 2021. World Economic Forum Press.

Graham, J., Smith, L., & Patel, R. (2020). Satellite communications and cybersecurity: Emerging threats. Journal of Space Technology, 45(2), 56-72.

Guerrero, R. (2011). Fundamentos de comunicaciones satelitales militares. Editorial Técnica Militar.

Guevara Julca, J. Z. (2002). Sistemas de comunicaciones orientadas a la descentralización de las entidades públicas del país. Universidad Nacional Mayor de San Marcos.

Hierro Alcántara, J. L. (2023). Aplicaciones militares de los satélites de navegación en el siglo XXI. Revista de Defensa y Tecnología, 48(4), 112-128.

Housen-Couriel, D. (2016). Commercial off-the-shelf vulnerabilities in space systems. Space Policy, 38, 128-135.

Huidobro, J. M. (2013). Tecnología de antenas: Principios y aplicaciones. Editorial Ra-Ma.

In Compliance Magazine. (2024, March 5). Electronic warfare and cyber defense of satellites.

IOActive. (2022, March 25). Missed calls for SATCOM cybersecurity: SATCOM terminal cyberattacks open the war in Ukraine.

ISO 27001:2022. (2022). Information security management systems - Requirements. International Organization for Standardization.

Kareem, K. M. (2024). Cyber threat landscape analysis for Starlink: Assessing risks and mitigation strategies in the global satellite internet infrastructure. arXiv preprint arXiv:2406.07562.

Latina Ecuador Sacristán Romero, M. (2005). Evolución de las comunicaciones satelitales. Editorial Universidad Central.

Lewis, J. A. (2014). Conflict and negotiation in cyberspace. Center for Strategic and International Studies.

Liu, Y., Zhang, X., & Wang, L. (2024). Characterizing and analyzing LEO satellite cyber landscape: A Starlink case study. ResearchGate.

Llanso, E., & Pearson, M. (2016). Cybersecurity challenges in satellite communications. Communications of the ACM, 59(11), 44-51.

Massimi, F., Tedeschi, P., & Di Pietro, R. (2023). Advanced persistent threats in satellite networks. IEEE Network, 37(2), 78-85.

MDPI Sensors. (2024). A survey on satellite communication system security. Sensors, 24(9), 2897.

MinTIC Colombia. (2022). Regulación de las tecnologías satelitales en Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones.

Morales, P., & Hernández, D. (2021). Tecnologías satelitales y defensa nacional: Un análisis jurídico. Revista de Derecho Espacial, 18(1), 34-49.

Musk, E. (2021). Starlink constellation deployment and military applications. Space Technology Review, 28(5), 234-247.

NATO STANAG 4774. (2023). Cybersecurity requirements for military communication systems. North Atlantic Treaty Organization.

NIST Cybersecurity Framework 2.0. (2024). Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, U.S. Department of Commerce.

Nogueira, R., Silva, M., & Torres, F. (2019). Cybersecurity challenges in military satellite systems. Defense Systems Journal, 67(4), 89-104.

NSA Cybersecurity Advisory. (2022). Protecting VSAT communications. National Security Agency, United States.

Pinto, R., Medina, C., & Vargas, L. (2023). Tecnologías emergentes en comunicaciones satelitales. Ingeniería y Competitividad, 25(2), 234-251.

Resolución 7870. (2022). Lineamientos para la ciberseguridad en servicios satelitales.

Ministerio de Tecnologías de la Información y las Comunicaciones, República de Colombia.

Sacristán, P. (2005). Historia de las comunicaciones espaciales. Editorial Espacio.

Santamarta, R. (2018). Last call for SATCOM security. Black Hat Technical Conference Proceedings. Las Vegas, NV.

Smith, M. (2001). Writing a successful paper. The Trey Research Monthly, 53, 149-150.
SpaceX. (2022). Starlink technology overview. Retrieved from www.spacex.com

Tedeschi, P., Sciancalepore, S., & Di Pietro, R. (2022). Satellite-based communications security: A survey of threats, solutions, and research challenges. Computer Networks, 216, 109-125.

TheSIGN. (2024). Uncovering potential vulnerabilities in Starlink: Russian hackers' persistent attempts.

U.S. Trade.gov. (2024). Colombia - Defense & Security.

Wang, K., Li, M., & Chen, S. (2022). Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. Journal of Cybersecurity, 8(1), tyac008.

White, J., & Mauldin, K. (2020). Military applications of commercial satellite systems. Defense Technology Quarterly, 33(4), 67-82.

Yang, Z., Liu, H., & Zhang, W. (2024). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. Acta Astronautica, 198, 447-458.

Zetter, K. (2023). Geopolitical implications of commercial satellite dependencies. International Security Review, 45(3), 123-145.

Zhao, H. (2019). The next generation of satellite services: Challenges and opportunities. Telecommunications Policy, 43(8), 654-668.

Ministerio de Defensa de España. 2024. *La inteligencia artificial como factor de transformación de las operaciones militares en el nivel operacional.*