Implementar Protocolos Que Determinen La Seguridad de Los Robots Antiexplosivos de Las FF.MM Contra Ciberataques.

Mayor (EJC) Andrés Camilo Aguilar Villamil

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) Andrés Camilo Aguilar Villamil
Identificación	**:**	80774402
Programa académico	**:**	Maestría en Ciber Seguridad y Ciber Defensa
Tutor metodológico	**:**	Jairo Andrés Becerra
Tutor temático	**:**	Andres Ernesto Salinas
Fecha de entrega	**:**	04/08/2015
Extensión	**:**	8000 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 (FF.MM) 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 (IA) 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 autoriza que este articulo sea publicado por el Sello Editorial ESDEG en su repositorio institucional y esté disponible bajo una modalidad de acceso abierto.

Implementar Protocolos que Determinen la Seguridad de los Robots Antiexplosivos de las FF.MM Contra Ciberataques.

Implement protocols that ensure the security of the FF.MM bomb-destroying robots against cyberattacks.

Andrés Camilo Aguilar Villamil [1]
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El desarrollo del presente artículo de investigación tiene como finalidad abordar la necesidad crítica de implementar y mejorar los protocolos de ciberseguridad para proteger los robots antiexplosivos utilizados por las FF.MM de posibles ciberataques. Dado que las operaciones militares dependen cada vez más de la robótica avanzada para la desactivación de bombas y otras tareas peligrosas, la vulnerabilidad de estos sistemas a las ciberamenazas plantea riesgos significativos para la eficacia operativa y la seguridad del personal. Así mismo en este se analizará de forma descriptiva qué protocolos se pueden implementar para reforzar la seguridad ante un posible ciberataque a los robos antiexplosivos de las FF.MM.

Palabras clave: Antiexplosivos; Ciberataque; Operaciones; Protocolos; Robótica avanzada; Seguridad Nacional.

Abstract: The purpose of this research article is to address the critical need to implement and improve cybersecurity protocols to protect bomb disposal robots used by the FF.MM from potential cyberattacks. As military operations increasingly rely on advanced robotics for bomb disposal and other dangerous tasks, the vulnerability of these systems to cyberthreats poses significant risks to operational effectiveness and personnel safety. This article will also descriptively analyze what protocols can be implemented to strengthen security against a potential cyberattack on the FF.MM bomb disposal robots.

Keywords: Bomb disposal; Cyberattack; Operations; Protocols; Advanced Robotics; National Security.

[1] Mayor del Ejército Nacional de Colombia. Candidato a magíster en Ciber Seguridad y Ciber Defensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ciencias Militares, Escuela Militar de Cadetes "General José María Córdova", Colombia. https://orcid.org/0009-0004-1940-3181 - Contacto: andres.aguilar@esdeg.edu.co

Introducción

En una era caracterizada por el rápido avance tecnológico, la integración de la robótica en las operaciones militares ha transformado el panorama de la guerra moderna. Entre las innovaciones más significativas se encuentran los robots antiexplosivos, desplegados por las Fuerzas Armadas de Colombia (ARC) para neutralizar amenazas explosivas, protegiendo así tanto al personal como a los civiles. Es así como en el contexto de Colombia, esta transformación no solo promete optimizar la eficiencia y la toma de decisiones, sino también enfrentar desafíos operativos particulares en un entorno de seguridad complejo y geografía diversa. Con lo mencionado anteriormente podemos comprender las afirmaciones de Alvin Toffler quien sostiene que:

> "El mundo progresa a un ritmo acelerado, y aquellos que no emplean la tecnología están predestinados a quedar obsoletos"(Domínguez Sánchez, 2003).

El Conpes 3701 comprende que:

> "La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado ante estas nuevas amenazas. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil". (CONPES, 3701).

En consecuencia, las FF.MM se encuentran ante un escenario de oportunidades para optimizar las respuestas estratégicas ante los desafíos que deben enfrentar, aprovechando además la eficiencia, precisión y agilidad para procesos fundamentales como la anticipación, prevención y planificación" (Mayor (EJC) Jorge Ivan García Torres, 2024). En la dinámica de la implementación de la robótica para las FF.MM; se evidencia que estos robots están equipados con sofisticados sensores, cámaras y herramientas de manipulación que les permiten realizar tareas complejas en entornos peligrosos. "Entre ellos se encuentran los robots autónomos inteligentes como el AlphaDog para el transporte de víveres, mercancías, armas y objetos de gran peso y el Battlefield Extraction Assist Robot o BEAR para tareas de búsqueda y rescate". (Mayor (EJC) Jorge Ivan Garcia Torres, 2024) Pag 36.

A medida que aumenta la dependencia de estos sistemas robóticos, también aumenta la necesidad de garantizar su seguridad contra ciberataques. Es así como la ciberseguridad llega a este contexto; siendo fundamental resaltar que esta se ha convertido en una preocupación crucial para las operaciones militares, ya que los adversarios explotan cada vez más las vulnerabilidades tecnológicas para interrumpir las operaciones, comprometer información confidencial y poner en peligro vidas.

En las FF.MM, la ciberseguridad para el manejo de robots es un aspecto estratégico que demanda la aplicación de una serie de medidas de seguridad con el propósito de salvaguardar las redes de información y asegurar un ciberespacio exento de amenazas, preservando la fiabilidad de la información crítica y protegiendo los intereses y la soberanía del Estado (Peña Suarez, 2023).

En el actual contexto de transformación digital de la defensa, los sistemas robóticos desplegados en operaciones tácticas representan activos estratégicos altamente sensibles. Particularmente, los robots antiexplosivos empleados por las FF.MM desempeñan un papel crucial en la detección, manipulación y neutralización de amenazas explosivas, preservando vidas humanas y garantizando la operatividad en entornos hostiles. No obstante, su creciente dependencia de tecnologías de control remoto, sensores inteligentes y enlaces de comunicación los convierte en objetivos críticos para actores maliciosos que buscan comprometer su funcionalidad a través de ciberataques. Un incidente de este tipo podría no solo dejar inoperante al dispositivo, sino incluso facilitar su manipulación hostil, transformándolo en una amenaza para los propios operadores y activos estratégicos. Por ende, la implementación de protocolos de ciberseguridad diseñados específicamente para este tipo de sistemas se configura como indispensable y necesarios.(Vera et al., 2022)

Por lo tanto, este artículo de investigación tiene como objetivo explorar la implementación de protocolos diseñados para mejorar la seguridad de los robots antiexplosivos de Las FF.MM contra las ciberamenazas, garantizando así su integridad y eficacia operativa. El desarrollo de dichos protocolos debe iniciarse a partir de una evaluación exhaustiva de vulnerabilidades, abordando los componentes físicos, lógicos y comunicacionales del sistema robótico. Esta fase diagnóstica permite identificar debilidades en el hardware (sensores, actuadores, controladores), software embebido, interfaces de usuario, redes inalámbricas de operación y plataformas de comando y control. La identificación temprana de estos vectores de ataque facilita la priorización de riesgos en función de su impacto y probabilidad de explotación, permitiendo a las FF.MM asignar recursos técnicos y humanos de forma eficaz.(Vera et al., 2022)

Por consiguiente, la información siempre ha sido un bien sumamente valioso que se ha intentado proteger de las diversas amenazas existentes en el entorno, un ejemplo paradigmático es la obtención y desarrollo de la máquina de cifrada alemana conocida como Enigma, durante el transcurso de la Segunda Guerra Mundial (1939-1945). "Enigma había sido inventada por el ingeniero alemán Arthur Scherbius tras la primera guerra mundial. Esta singular máquina generaba códigos basándose en el intercambio de signos. Su funcionamiento se basaba en enviar mensajes encriptados que alteraban la forma, pero no el contenido, con el objetivo de evitar que las encriptaciones fueran descifradas en caso de que estos mensajes fueran interceptados por el enemigo." (J. M. SadurníJ. M. Sadurní, 2024).

En aquel entonces, el sistema de protección de la información fue objeto de ataques y logró ser descifrado por los británicos, lo cual puso de manifiesto la vulnerabilidad inherente a la materialización de una amenaza y al ataque a un sistema. Además, se evidenció la insuficiente protección que había recibido el sistema de cifrado para contrarrestar el ataque y su efectiva materialización, un hecho que con el devenir del tiempo adquirió una relevancia cada vez mayor. Esto se debió a que los medios para recopilar, almacenar y preservar información se tornaban cada vez más sofisticados, al igual que los métodos y recursos empleados para obtenerla de manera ilícita, degradarla o manipularla de forma indebida. (CONPES, 3701).

Así mismo, se relacionan otros hechos que han marcado el avance de la tecnología, En el mes de abril de 2007, el gobierno de Estonia sufrió el que es considerado el mayor ataque cibernético de la historia, en el cual se vieron afectados la presidencia, el parlamento, la mayoría de los ministerios, los partidos políticos y dos de sus grandes

bancos. Este ataque desató una gran crisis que requirió la intervención de la comunidad internacional y alertó a la Organización del Tratado del Atlántico Norte (OTAN), la cual, en agosto de 2008, puso en marcha el Centro de Excelencia para la Cooperación en Ciberdefensa (CCD), con el fin de proteger a sus miembros de este tipo de ataques y entrenar a personal militar, investigar técnicas de defensa electrónica y desarrollar un marco legal para ejercer esta actividad. (CONPES, 3701).

Del mismo modo, otros dos ataques cibernéticos representativos. El primero, fue en contra de los Estados Unidos en el mes de julio de 2009, cuando una serie de ataques afectaron la Casa Blanca, el Departamento de Seguridad Interna (DHS), el Departamento de Defensa, la Administración Federal de Aviación y la Comisión Federal de Comercio. Otro suceso fue el que reportó la Guardia Civil española en marzo de 2010, cuando desmanteló a una de las mayores redes de computadores "zombies", conocida con el nombre de BotNet Mariposa", compuesta por más de 13 millones de direcciones IP infectadas, distribuidas en 190 países alrededor del mundo. Colombia ocupó el quinto puesto entre los países más afectados por esta red. (CONPES, 3701).

No.	PAÍS	%
1	INDIA	19.14
2	MÉXICO	12.85
3	BRASIL	7.74
4	COREA	7.24
5	COLOMBIA	4.94
6	RUSIA	3.14
7	EGIPTO	2.99
8	MALASIA	2.86
9	UCRANIA	2.69
10	PAKISTAN	2.55

No.	PAÍS	%
11	PERÚ	2.42
12	IRÁN	2.07
13	ARABIA SAUDÍ	1.85
14	CHILE	1.74
15	KAZAKHSTAN	1.38
16	EMIRATOS ARABES	1.15
17	MARRUECOS	1.13
18	ARGENTINA	1.10
19	ESTADOS UNIDOS	1.05

TABLA No. 1: Países Latinoamericanos más afectados por una red de zombies en marzo 2010. Tomada de (CONPES, 3701)

En consecuencia, se analiza que el cifrado de extremo a extremo actúa como una barrera formidable e infranqueable contra el acceso no autorizado, garantizando de manera

efectiva que, incluso si se interceptan los datos confidenciales, estos permanecerán ilegibles y protegidos de miradas indiscretas, a menos que se disponga de las claves de descifrado correcto. Que la implementación de algoritmos de cifrado altamente seguros es un requisito fundamental e indispensable para proteger de manera efectiva los datos sensibles y confidenciales de posibles ataques cibernéticos. Al implementar rigurosos estándares de cifrado de última generación, las FF.MM pueden salvaguardar de manera efectiva información altamente confidencial, como los datos de despliegue de aeronaves en operación, detalles del personal militar y características técnicas detalladas de los equipos utilizados en sus misiones. Esto no solo disuade a los potenciales atacantes, sino que también genera confianza y certidumbre en la integridad y confidencialidad de la información que está siendo resguardada. (Matiz Rojas & Fernández Camargo, 2023).

Por lo anterior, la aplicación efectiva de protocolos que comprendan el manejo de técnicas de cifrado altamente sofisticadas se consideran fundamentales para avalar la seguridad de la información confidencial almacenada en los sistemas informáticos utilizados por las FF.MM para emplear el manejo de la robótica en el desarrollo de prácticas de desactivación de artefactos y explosivos que comprometen la vida del soldado y la de la humanidad.

Como referencia se relaciona el uso de robots antiexplosivos por el ejército de EE. UU. (PackBot). En contraste con lo que es el manejo de la robótica antiexplosiva en las FF.MM, se relaciona el uso de robots antiexplosivos y de qué modo este ha revolucionado las tácticas y estrategias del Ejército de EE. UU. en el campo de batalla, especialmente en operaciones urbanas y en contextos donde existen amenazas como artefactos explosivos improvisados (IED). Uno de los robots más conocidos en este ámbito es el PackBot,

desarrollado por iRobot. Este robot ha sido diseñado para realizar tareas peligrosas que tradicionalmente requerirían la presencia de personal militar, minimizando así el riesgo a la vida humana.

Los robots como el PackBot son capaces de realizar una variedad de misiones, incluyendo la identificación, desactivación y eliminación de explosivos. Equipados con cámaras y herramientas especializadas, estos robots permiten a los operadores evaluar situaciones desde una distancia segura. Esto no solo aumenta la eficacia en la detección y neutralización de amenazas, sino que también mejora la seguridad general del personal militar involucrado en operaciones potencialmente mortales (Baker, 2020).

En el contexto de la Guerra de Irak, que comenzó en 2003, el PackBot fue desplegado por el ejército estadounidense para apoyar las operaciones de desactivación de explosivos. Su capacidad para cruzar terrenos difíciles y acceder a espacios reducidos lo convirtió en un recurso valioso para la identificación y neutralización de IEDs. El uso del PackBot no solo mejoró la seguridad de los soldados al reducir su exposición directa a peligros potenciales, sino que también aumentó la eficiencia en las operaciones de desactivación. Los datos recopilados por estos robots, como imágenes y análisis del terreno, ayudaron a los equipos militares a tomar decisiones informadas sobre cómo proceder en situaciones potencialmente mortales.

A pesar de sus ventajas, el uso de robots antiexplosivos también plantea desafíos y consideraciones éticas. La dependencia creciente de la tecnología puede llevar a una desensibilización ante el uso de fuerza letal y a un cambio en la naturaleza del compromiso militar (Thompson, 2021). Así mismo, hay preocupaciones sobre la capacidad de estos sistemas para tomar decisiones autónomas en situaciones complejas.

Especificaciones del PackBot.

Dimensiones	- Longitud: Aproximadamente 76 cm (30 pulgadas). - Ancho: Aproximadamente 66 cm (26 pulgadas). - Altura: Aproximadamente 30 cm (12 pulgadas).
Peso	- Peso total: Alrededor de 27 kg (60 libras), lo que permite su transporte y operación por un solo soldado.
Capacidades de Movimiento	- Velocidad máxima: Hasta 5 km/h (3 mph) en terreno plano. - Capacidad para escalar pendientes de hasta 60 grados. - Puede superar obstáculos de hasta 20 cm (8 pulgadas) de altura.
Sensores y Equipamiento	- Equipado con cámaras de video en color y térmicas para la vigilancia y el reconocimiento. - Posee un sistema de manipulación con brazos robóticos que pueden ser utilizados para desactivar explosivos o recoger objetos. - Capacidad de operar en condiciones climáticas adversas, incluyendo lluvia y temperaturas extremas.
Control y Comunicación	- Controlado a distancia mediante una estación base portátil. - Rango operativo de hasta 500 metros (1,640 pies) en línea de vista. - Sistema de comunicación seguro que permite la transmisión en tiempo real de video y datos.
Autonomía	- Tiempo de operación continuo: Aproximadamente 4 horas con una sola carga, dependiendo del uso y las condiciones del terreno.
Usos Típicos	- Reconocimiento y evaluación de áreas potencialmente peligrosas. - Desactivación de dispositivos explosivos improvisados (IED). - Misiones de búsqueda y rescate en situaciones peligrosas.

Tabla 2. Elaboración propia con datos tomados de (Smith & Johnson, 2019).

Así mismo, se destaca la experiencia israelí en ciberseguridad de sistemas autónomos. Israel es reconocido como un líder global en tecnología y ciberseguridad. La combinación de una cultura de innovación, una fuerte inversión en investigación y desarrollo (I+D), y la experiencia adquirida por muchos de sus profesionales en las Fuerzas

de Defensa de Israel (IDF) ha permitido al país desarrollar soluciones avanzadas para proteger sistemas autónomos, como drones, vehículos no tripulados y otros dispositivos conectados. Empresas israelíes han creado tecnologías que aseguran la integridad y la confidencialidad de los datos en sistemas autónomos. Por ejemplo, empresas como Check Point, CyberArk y Palo Alto Networks están a la vanguardia del desarrollo de software que protege contra ataques cibernéticos. (Shapira, H., & Cohen, Y. 2021)

En cuanto a capacitación Militar: La IDF ha integrado ciberseguridad en su formación militar, lo que ha llevado a una generación de expertos en ciberdefensa. La unidad 8200, una famosa unidad de inteligencia israelí se especializa en recopilación de información y guerra cibernética, formando a muchos profesionales que luego se trasladan al sector privado. Así mismo, la Colaboración Público-Privada. En Israel, existe una estrecha colaboración entre el gobierno, el ejército y las empresas privadas. Esta sinergia permite el desarrollo rápido de soluciones efectivas y adaptadas a las necesidades del sector público y privado, y no menos importante el manejo e implementación de Normativas y Políticas. El gobierno israelí ha implementado políticas que promueven la ciberseguridad en todos los sectores, incluyendo el uso de sistemas autónomos. Esto incluye regulaciones sobre cómo deben ser diseñados estos sistemas para resistir ataques cibernéticos. (Katz, E., & Shalom, A. 2019).

Drones Autónomos: Israel utiliza drones tanto para operaciones militares como para monitoreo civil. La seguridad cibernética es fundamental para garantizar que estos drones no sean hackeados o manipulados por actores malintencionados. Israel ha desarrollado una amplia gama de drones autónomos, como el Heron TP y el SkyLark. Estos drones se utilizan en operaciones militares para misiones de reconocimiento, vigilancia y ataque. El

Heron TP, por ejemplo, es un vehículo aéreo no tripulado (VANT) capaz de realizar misiones de largo alcance y cuenta con capacidades de inteligencia, vigilancia y reconocimiento (ISR). Además, su diseño permite que sea utilizado en diversas condiciones climáticas. (Defensemirror, 2015).

Vehículos No Tripulados: En el ámbito militar, los vehículos terrestres no tripulados (UGVs) como el RoboSimian y el Talon son utilizados por las fuerzas israelíes para realizar la desactivación de explosivos o ejecutar misiones de reconocimiento. Estos vehículos deben estar protegidos contra ataques cibernéticos que podrían comprometer su operación, son utilizados por las fuerzas israelíes para realizar misiones de desactivación de explosivos y reconocimiento en terrenos peligrosos. Estos vehículos están equipados con tecnología avanzada que les permite navegar en ambientes complejos y son esenciales para mantener la seguridad del personal militar al minimizar su exposición a amenazas. (Hoffman, B. 2016).

Marco de ciberseguridad NIST (Instituto Nacional de Estándares y Tecnología) 2.0: (Identificar, Proteger, Detectar, Responder, Recuperar) y cómo se aplican a sistemas robóticos militares, se basa en cinco pilares fundamentales: Identificar, Proteger, Detectar, Responder y Recuperar. En el contexto de los sistemas robóticos militares, cada uno de estos pilares juega un papel crucial para garantizar la seguridad y funcionalidad de las operaciones. (Mindefensa, 2023).

Descripción de sus cinco pilares fundamentales:

Identificar	Proteger	Detectar	Responder	Recuperar
Este pilar implica la creación de un inventario detallado de los sistemas robóticos y sus componentes, así como la evaluación de los riesgos asociados. Para las fuerzas militares colombianas, esto incluye identificar las vulnerabilidades potenciales en la infraestructura tecnológica utilizada para operaciones militares	La protección implica implementar medidas de seguridad adecuadas para salvaguardar los sistemas robóticos contra amenazas cibernéticas. Esto puede incluir el uso de cifrado, autenticación multifactor y controles de acceso para asegurar que solo personal autorizado pueda operar o modificar los sistemas.	Este pilar se centra en la capacidad de identificar eventos cibernéticos que puedan comprometer el funcionamiento seguro de los robots militares. Las fuerzas armadas deben establecer monitoreos continuos y sistemas de alerta temprana que permitan detectar intrusiones o fallos en tiempo real.	En caso de un incidente cibernético, es fundamental tener un plan de respuesta bien definido. Esto implica la capacitación del personal militar en procedimientos para contener y mitigar ataques, así como la restauración rápida de las capacidades operativas.	Finalmente, este pilar se refiere a la capacidad de restaurar los sistemas robóticos a su estado operativo normal después de un incidente. Esto incluye realizar análisis post-incidente para prevenir futuros ataques y mejorar continuamente las defensas cibernéticas.

Grafica 1. Fuente de elaboración propia. Con datos tomado de (Mindefensa, 2023).

Entre tanto, resulta fundamental relacionar la Ciberresiliencia táctica. La ciberresiliencia táctica se refiere a la capacidad de una organización para anticipar, responder y recuperarse de incidentes cibernéticos a nivel operativo. Este concepto implica no solo la implementación de medidas preventivas y de protección, sino también la habilidad de adaptarse rápidamente a situaciones adversas. En un entorno donde las amenazas cibernéticas son cada vez más sofisticadas y frecuentes, las organizaciones deben contar con estrategias claras y bien definidas que permitan una respuesta efectiva ante ataques. Esto incluye la formación del personal, el establecimiento de protocolos de respuesta a incidentes y la integración de tecnologías avanzadas que faciliten la detección y mitigación de riesgos. (Hentea, M., & Nita, A. 2020).

Además, la ciberresiliencia táctica abarca el uso de análisis en tiempo real para evaluar el impacto de los incidentes y ajustar las estrategias según sea necesario. Esto implica una colaboración constante entre los equipos de IT, seguridad y gestión operativa para asegurar que todos los aspectos del negocio estén alineados en la defensa contra

amenazas cibernéticas. La capacidad de aprender y adaptarse a partir de experiencias pasadas es fundamental para mejorar continuamente las prácticas de seguridad y garantizar la continuidad del negocio en un mundo digital cada vez más complejo. (Tsohou, A., & Karyda, M. 2019)

En el contexto de las FF.MM, la ciberresiliencia táctica es crucial para garantizar la seguridad nacional y la integridad operativa. Dada la creciente dependencia de las tecnologías de información y comunicación en las operaciones militares, es fundamental que estas fuerzas desarrollen capacidades robustas para enfrentar amenazas cibernéticas. Esto incluye formación continua en ciberseguridad, colaboración con entidades gubernamentales y privadas, y el establecimiento de protocolos claros para la respuesta ante incidentes. Al fortalecer su ciberresiliencia táctica, las FF.MM pueden asegurar su eficacia en el cumplimiento de sus misiones y proteger la información crítica contra posibles adversarios. (Barlow, J., & Johnson, R. 2020).

Finalmente, a diferencia de la mayoría de los países latinoamericanos, Colombia emplea vulnerabilidades en sus sistemas de vanguardia Nacional. (CONPES 3701). A lo que se establece que estar debidamente preparados y anticiparse a los posibles escenarios de riesgo con protocolos robustos y fortalecidos es una prioridad fundamental a la hora de accionar elementos tecnológicos robóticos de gran impacto, un conocimiento profundo, comprende a cabalidad y asume con responsabilidad la implementación que puedan llegar a materializarse, teniendo en cuenta su potencial impacto en la sociedad y en el entorno en general.

Metodología

Método de Investigación: Cualitativa

Con el propósito de garantizar la rigurosidad del estudio, se estructuró un diseño metodológico de revisión sistemática, enfocado en la identificación de protocolos y estrategias que refuercen la seguridad de los robots antiexplosivos frente a amenazas cibernéticas. Este diseño se desarrolla en tres fases principales:

Estrategia de búsqueda y recolección de datos	- Google Scholar - Web of Science, - Scopus - JSTOR Asegurando la inclusión de literatura actualizada y científicamente validada.
Las palabras clave	- Antiexplosivos - Ciberataque - Operaciones militares - Protocolos de seguridad - Robótica avanzada - Seguridad Nacional Se delimitó el rango temporal a los últimos cinco años, con el objetivo de incorporar hallazgos y avances recientes en la materia.
Criterios de inclusión y selección de artículos	- Pertinencia temática. - relación directa con los protocolos de seguridad para robots antiexplosivos ante ciberataques. - Publicación en revistas científicas indexadas o de reconocido prestigio académico. - Metodología sólida, con un diseño de investigación claro, confiable y replicable. - Aportes originales, que contribuyan de manera significativa a la comprensión y mejora de los sistemas de seguridad analizados.
Procesamiento y análisis de la información	Una vez seleccionados los artículos, se procedió a: - Clasificación y organización temática de los contenidos. - Evaluación crítica de los enfoques metodológicos y hallazgos presentados en cada investigación. - Síntesis de resultados, orientada a la generación de conocimiento aplicable a la seguridad cibernética en robots militares.

Tabla 3. Fuente de elaboración propia
Con datos tomados de González, J., & Pérez, M. (2023)

Analizar los protocolos actuales de comunicación, control y seguridad de los robots antiexplosivos para comprender su vulnerabilidad frente a posibles ciberataques.

El análisis de los protocolos de comunicación, control y seguridad implementados en robots antiexplosivos de las FF.MM, relaciona como estos mecanismos se comunican con sus operadores, cómo se controlan y cuáles son las medidas de seguridad implementadas para protegerlos de ataques, este análisis, también comprende e identifica que tipos de enlaces son suficientes para homologar y garantizar la integridad, fiabilidad y disponibilidad operativa de sus sistemas, además de identificar la posible conexión de estos, incluso si no están diseñados para funcionar en internet, quizá mediante un enlace entre el nodo esclavo y el robot. Teniendo en cuenta que la necesidad de este análisis radica en que estos son herramientas críticas para la seguridad pública, al comprender sus vulnerabilidades, se pueden desarrollar mejores estrategias para proteger estos sistemas contra ataques cibernéticos o manipulaciones maliciosas que podrían poner en peligro la vida humana y la efectividad de las operaciones.

Por lo tanto, para abordar el análisis de los protocolos actuales de comunicación, control y seguridad de los robots antiexplosivos se establece que la tecnología inteligente se está incorporando en diversos contextos y tareas laborales, que esta se ha concebido en el contexto militar con el objetivo de optimizar la eficiencia en las operaciones militares, incorporando también elementos técnicos y éticos, tales como la toma de decisiones y la capacidad de suministrar información rápida y precisa.

En contexto, Colombia ha iniciado la ejecución de proyectos en el ámbito de la (IA) y vehículos no tripulados, como el robot TALON, empleado para responder a amenazas con dispositivos explosivos. Además, estudiantes de la Universidad Industrial de Santander y otros emprendedores han desarrollado un prototipo de plataforma híbrida (aire-tierra) equipada con sensores para la detección de explosivos. Asimismo, se han implementado iniciativas como el robot VALI, desarrollado por INDUMIL y la Universidad Militar Nueva Granada. (Prada & Prada, 2023)

Desde hace (10) años, el Ejército Nacional (EJC) ha implementado la utilización de robots de vanguardia con el objetivo de optimizar las probabilidades de éxito con mínimos riesgos. Estos robots, en sus variantes como el iRobot, Talon 4 y el Vanguard, se han distribuido a lo largo del territorio nacional en los diez Grupos Marte, distribuidos en cada una de las Divisiones territoriales del EJC. Cada uno de los robots es operado por expertos altamente capacitados que optimizan cada una de las capacidades proporcionadas por la versión del robot bajo su dirección. El sargento primero Álvaro Rojas Higuera, experto en técnicas antiexplosivas e instructor de temas vinculados a explosivos del EJC, divulgó que el iRobot cuenta con uno de los brazos más altos, aproximadamente 1,5 metros, que posibilita la captura de vehículos mediante una ventana. Además, subrayó las capacidades del Talon 4, uno de los más pesados, pero que además incorpora dos brazos en su configuración. Se reveló que ciertas variantes de otros tipos de robots incorporan un cañón disruptor de agua, destinado a neutralizar artefactos explosivos de forma segura y a distancia. Una de las principales ventajas derivadas del empleo de robots en la lucha contra artefactos explosivos es la reducción de las víctimas derivadas de explosiones, una reducción que el sargento primero Álvaro Rojas Higuera estima en aproximadamente un 80% o 90%. (gov.co, 2021)

Así mismo, las ARC han incorporado el robot antiexplosivo Allen Digital DV420. Este dispositivo, caracterizado por su alta movilidad y facilidad de operación, ha facilitado el acceso a espacios confinados para detectar la presencia de material explosivo. Los robots están equipados con sistemas de comando 2G y cámaras, además de controles de velocidad y circuitos de disparo. Mediante la utilización de estos dispositivos, el EJC ha logrado combatir a las organizaciones ilegales e identificar dispositivos explosivos. Estas situaciones han sido gestionadas por personal altamente capacitado, quienes, en conjunción con estos dispositivos, pueden preservar la tranquilidad y seguridad de los ciudadanos colombianos (infodefensa.com, 2022).

El crecimiento exponencial de las amenazas cibernéticas plantea desafíos sumamente significativos, especialmente en situaciones que implican robots altamente sofisticados y a prueba de explosivos, donde los riesgos son particularmente elevados.

Considerando la constante evolución de las diversas formas de amenazas cibernéticas, se hace necesario llevar a cabo un exhaustivo análisis de dichos protocolos de forma minuciosa y detallada, con el propósito de identificar posibles áreas de mejora que permitan fortalecer de manera efectiva las estrategias de seguridad implementadas. Por lo anterior, se percibe un ámbito estratégico que demanda la instauración de un conjunto de protocolos de seguridad para salvaguardar las redes de información, incluyendo tanto normas como acciones y tecnologías que permitan asegurar un entorno cibernético libre de amenazas, salvaguardando la fiabilidad de la información crítica y protegiendo los intereses y la soberanía estatal (Orozco-Castro et al., 2021).

Desde una perspectiva tecnológica, los protocolos de comunicación desempeñan un papel determinante en la operatividad de estos robots. Estas plataformas móviles,

comúnmente controladas de forma remota, dependen de enlaces inalámbricos para la transmisión bidireccional de datos. Entre los sistemas más utilizados se encuentran las conexiones Wi-Fi, Bluetooth y protocolos de radiofrecuencia (RF) propietarios, que permiten el envío de órdenes, recepción de datos sensoriales y supervisión en tiempo real de las acciones ejecutadas por el robot. Sin embargo, estas tecnologías, si no están adecuadamente protegidas, introducen vectores de ataque potenciales. La interceptación de señales mediante sniffers de paquetes, la interferencia de radiofrecuencia (jamming) o el uso de repetidores (Spoofing de señal) son amenazas tangibles en escenarios hostiles. Aun cuando los robots estén físicamente blindados, su debilidad puede residir en la exposición de sus canales de comunicación si estos no están cifrados ni autenticados adecuadamente. (Mayor (EJC) Jorge Ivan Garcia Torres, 2024)

Paralelamente, los protocolos de control permiten la interacción segura entre el operador y el sistema robótico, regulando el flujo de comandos, respuestas y validaciones durante misiones críticas. La mayoría de los robots antiexplosivos operan bajo modalidad de telepresencia o control remoto, utilizando interfaces físicas como consolas portátiles, joysticks, visores de realidad aumentada o tabletas de grado militar. Estas interfaces se comunican con el robot a través de enlaces encriptados, permitiendo la ejecución precisa de maniobras como inspección de objetos sospechosos, activación de mecanismos manipuladores o detonación controlada.(Correa, 2005).

En este sentido, los protocolos deben garantizar que cada orden emitida sea única, verificable y no repetible, evitando así el riesgo de comandos fraudulentos o reprogramaciones maliciosas. Además, se recomienda el uso de módulos de hardware confiables (Trusted Platform Modules, TPMs) integrados tanto en el robot como en los

dispositivos de control, los cuales permiten la autenticación mutua, el almacenamiento seguro de claves criptográficas y la verificación de integridad del sistema antes de iniciar operaciones. En entornos militares donde la conectividad puede fluctuar, los robots también deben contar con modos autónomos de operación ante pérdida de señal, manteniendo su seguridad funcional mediante rutas preprogramadas de repliegue o protocolos de neutralización seguros. (Intel.com, 2025)

En el entorno actual de operaciones militares y de seguridad, la implementación de sistemas robóticos antiexplosivos exige una sinergia sólida entre el hardware especializado y el software operativo, ambos componentes críticos para garantizar el éxito de las misiones y la seguridad de los operadores. Sin embargo, los sistemas de control estratégico frecuentemente dependen de software que no siempre ha sido concebido con principios de ciberseguridad desde su diseño, lo que representa un riesgo significativo en entornos donde cualquier falla puede tener consecuencias fatales. (Denis Restrepo Rojas, 2024).

Es por ello por lo que tanto el diseño físico (hardware) como el entorno lógico (software) de estos sistemas deben integrarse bajo principios de seguridad robustos. A nivel de software, la presencia de vulnerabilidades como la inyección de comandos constituye una amenaza crítica: si los sistemas no validan adecuadamente los datos de entrada, un atacante podría enviar órdenes maliciosas al robot y tomar el control de sus funciones. (gobierno digital, 2011). Esta brecha de seguridad se ve agravada por la integración de sensores, cámaras y sistemas de visión que transmiten datos en tiempo real; si estos flujos son interceptados o manipulados, la percepción del operador sobre el entorno puede distorsionarse, generando errores tácticos graves.

Los protocolos de seguridad, por su parte, deben actuar como eje transversal que articule tanto el software como el hardware en una arquitectura resiliente. Estos protocolos están diseñados para preservar la integridad, confidencialidad y disponibilidad de los sistemas, pero en muchos casos su implementación en robots antiexplosivos aún es incipiente. Prácticas fundamentales como actualizaciones de firmware, monitoreo constante de vulnerabilidades, escaneo de configuraciones inseguras o validaciones criptográficas entre módulos son frecuentemente subestimadas, lo que limita la capacidad de respuesta frente a ciberataques sofisticados.

Esta situación es reflejada por informes del Instituto Nacional de Estándares y Tecnología (NIST), que advierten que muchos sistemas robóticos incluso aquellos utilizados en entornos críticos no han sido diseñados con la seguridad como componente estructural. De hecho, la reciente actualización del Marco de Seguridad Cibernética (CSF 2.0) del NIST (2024) resalta la urgencia de estandarizar protocolos y procedimientos entre fabricantes para facilitar la implementación de medidas homogéneas y efectivas de protección. (Luis Almagro, 2019).

Los protocolos de seguridad establecidos actualmente juegan un papel fundamental en la protección de la confidencialidad y la integridad de los datos y recursos críticos de una organización. No obstante, es imprescindible implementar medidas efectivas para prevenir posibles brechas de seguridad y garantizar la continuidad operativa en un entorno cada vez más digitalizado y expuesto a ciberamenazas. (Diego Fernando Cano Cuevas, 2023).

Protocolos identificados en la actualidad

1. Protocolos de Comunicación Segura

Encriptación de Datos: La encriptación es el proceso de transformar datos en un formato que solo puede ser leído por quienes tienen la clave para descifrarlos. Esto es crítico en entornos militares, donde la información sensible debe ser protegida contra interceptaciones. Se utilizan algoritmos de encriptación robustos (como AES-256) para proteger la información transmitida entre el robot y las estaciones de control. Esto asegura que, incluso si los datos son interceptados, no puedan ser leídos sin la clave adecuada.(Información, 2024)

Algoritmos de Encriptación	-	Se utilizan algoritmos robustos como AES (Advanced Encryption Standard) con una longitud de clave de 256 bits, que es considerado uno de los más seguros y es utilizado por gobiernos y organizaciones en todo el mundo. La elección del algoritmo y la longitud de la clave son fundamentales, ya que afectan directamente la dificultad con la que un atacante podría intentar romper la encriptación.(Información, 2024).
Encriptación en Tránsito y en Reposo	-	Es importante aplicar encriptación tanto a los datos que están siendo transmitidos (en tránsito) como a aquellos que están almacenados (en reposo). Esto garantiza que incluso si un atacante logra acceder a los datos almacenados, no podrá leerlos sin las claves adecuadas. (Información, 2024).
Autenticación Mutua	-	La autenticación mutua asegura que ambas partes (el robot y la estación de control) verifiquen sus identidades antes de intercambiar información. Esto evita ataques donde un adversario se haga pasar por uno de los sistemas.es decir, tanto el robot como la estación de control deben autenticarse mutuamente antes de establecer una conexión. Esto se puede lograr mediante certificados digitales o claves pre compartidas, lo que ayuda a prevenir ataques de suplantación. (TÜV Rheinland, 2025)
Certificados Digitales	-	Se pueden utilizar certificados digitales emitidos por una autoridad certificadora confiable para verificar identidades. Cuando el robot intenta conectarse a la estación de control, presenta su certificado, y viceversa. Si ambos certificados son válidos, se establece una conexión segura.
Claves Pre compartidas	-	Alternativamente, se pueden usar claves precompartidas (PSK - Pre-Shared Key) para autenticar ambos sistemas. Cada sistema tiene una clave secreta que debe ser conocida por ambos; si coinciden, se permite el acceso.

Tabla 3. elaboración propia con datos tomados de (Información, 2024)

Protocolos Seguros: Se emplean protocolos seguros como HTTPS, SSH o MQTT sobre TLS para las comunicaciones. Estos protocolos son diseñados específicamente para proteger la integridad y confidencialidad de los datos durante la transmisión.(Paulita Flor Salazar, 2022)

- HTTPS (Hypertext Transfer Protocol Secure): Utiliza TLS (Transport Layer Security) para cifrar las comunicaciones web. Aunque comúnmente se asocia con navegadores web, este protocolo puede ser empleado por aplicaciones militares para proteger datos sensibles transmitidos a través de redes.
- SSH (Secure Shell): Este protocolo permite el acceso seguro a dispositivos a través de redes inseguras. Proporciona autenticación robusta y cifrado de sesión, lo cual es esencial para el control remoto seguro del robot.
- MQTT sobre TLS: MQTT (Message Queuing Telemetry Transport) es un protocolo ligero ideal para dispositivos IoT (Internet of Things), como robots antiexplosivos. Al combinarlo con TLS, se asegura que los mensajes entre el robot y su controlador estén cifrados y autenticados.(Paulita Flor Salazar, 2022)
- Integridad de Datos: Además de proteger la confidencialidad, es crucial garantizar que los datos no sean alterados durante la transmisión:
    - Códigos Hash: Se utilizan funciones hash criptográficas como SHA-256 para generar un resumen único del contenido transmitido. Al recibir datos, el sistema puede calcular el hash del contenido recibido y compararlo con el hash enviado; si no coinciden, se puede inferir que los datos han sido alterados.

- Firmas Digitales: Estas permiten verificar tanto la autenticidad como la integridad del mensaje. Al firmar digitalmente un mensaje con una clave privada, solo quien tenga la clave pública correspondiente puede verificar su autenticidad.

2. Control y Monitoreo

- Sistemas de Control Distribuido: Los robots antiexplosivos suelen estar equipados con sistemas de control distribuidos que permiten una supervisión constante del estado del robot. Esto incluye monitoreo en tiempo real del hardware y software para detectar comportamientos anómalos que podrían indicar un ataque.(Alexander S. Gillis, 2024)
- Redundancia en Sistemas Críticos: La implementación de sistemas redundantes asegura que, si un componente es comprometido, otro pueda tomar su lugar sin pérdida significativa en la funcionalidad. Esto es esencial en operaciones donde cada segundo cuenta.
- Actualizaciones y Parches Regulares: Los fabricantes y operadores deben implementar un régimen riguroso de actualizaciones de software para corregir vulnerabilidades conocidas. Esto incluye parches regulares y actualizaciones del firmware del robot.(Alejandro López, 2024)

3. Seguridad Física

- Cajas Fuertes y Sellos Físicos: Los componentes críticos del robot pueden estar protegidos por cajas fuertes o sellos físicos que impiden el acceso no autorizado. Esto es particularmente importante para evitar manipulaciones físicas que puedan comprometer la seguridad del robot.(Pacheco & Pacheco, 2022).

- Control de Acceso Físico: Solo personal autorizado debe tener acceso a las áreas donde se almacenan o mantienen los robots antiexplosivos. Esto se puede lograr mediante el uso de tarjetas magnéticas, biometría o sistemas de vigilancia.(Pacheco & Pacheco, 2022)

4. Entrenamiento y Concienciación

- Capacitación Continua: El personal militar debe recibir entrenamiento regular sobre las mejores prácticas en ciberseguridad y cómo identificar posibles amenazas cibernéticas. Esto incluye simulaciones de ataques cibernéticos para preparar al personal ante situaciones reales.(Denis Restrepo Rojas, 2024)
- Protocolos de Respuesta a Incidentes: Deben existir procedimientos claros sobre cómo actuar en caso de un ataque cibernético, incluyendo la identificación rápida del ataque, contención, erradicación y recuperación.

5. Redundancia en Comunicaciones: Para asegurar la continuidad operativa incluso ante fallos o ataques:

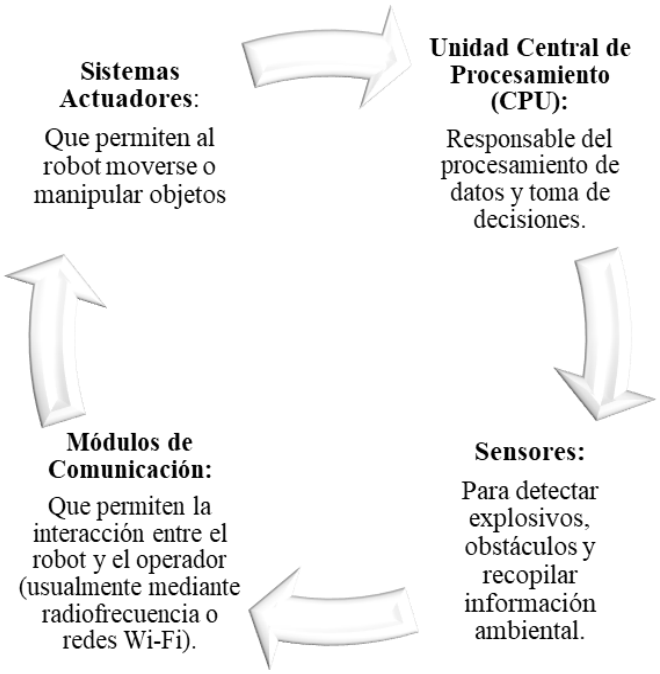
- Canales Redundantes: Los robots pueden estar equipados con múltiples interfaces de comunicación (Wi-Fi, radiofrecuencia, etc.) para garantizar que siempre haya un canal disponible para transmitir información crítica.(Vicente Rodriguez Moreno, 2018)
- Protocolos de Recuperación: Implementar mecanismos que permitan reestablecer conexiones automáticamente si una comunicación segura se interrumpe o se ve comprometida.(Vicente Rodriguez Moreno, 2018)

1. Auditorías y Evaluaciones

- Auditorías Regulares: Se llevan a cabo auditorías periódicas para evaluar la seguridad del sistema y detectar vulnerabilidades potenciales antes de que puedan ser explotadas por adversarios.(Ministerio de Defensa, 2012)
- Pruebas de Penetración: Realizar pruebas simuladas donde equipos especializados intentan explotar vulnerabilidades permite identificar debilidades en los sistemas antes que puedan ser aprovechadas por actores maliciosos.(Ministerio de Defensa, 2012).

Arquitectura y Mantenimiento para Identificar Vulnerabilidades

Arquitectura. La arquitectura típica de un robot antiexplosivo incluye:

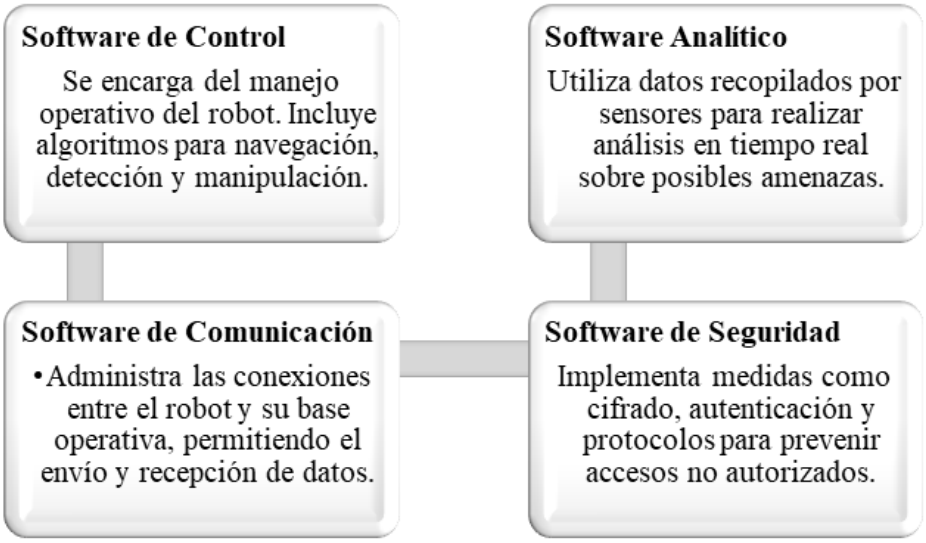


Grafica 2. Fuente de elaboración propia,
con datos tomados de (Ministerio de Defensa, 2012).

Mantenimiento: El mantenimiento implica:

Grafica 3. Fuente de elaboración propia.
Con datos tomados de (Ministerio de Defensa, 2012).

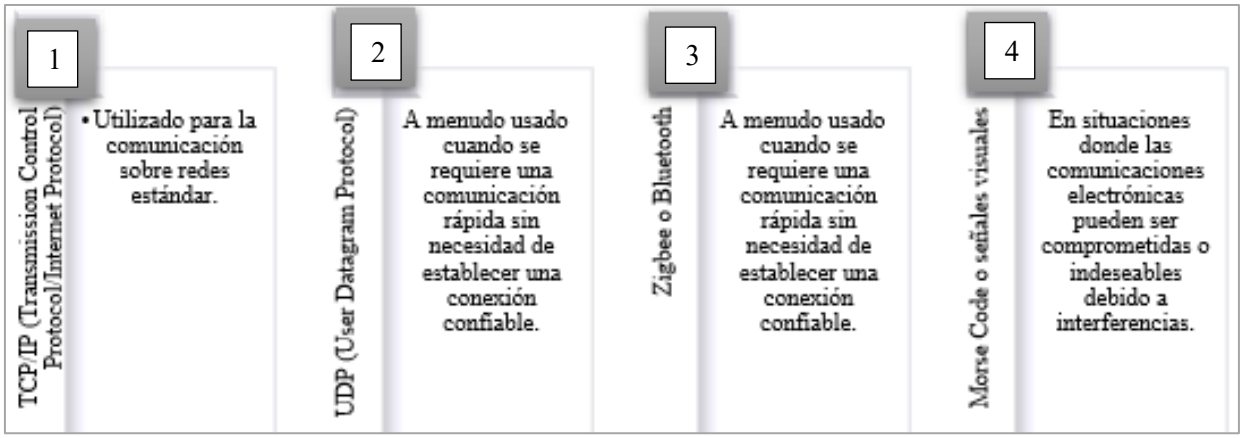
Clasificación del Software de los Diferentes Robots: El software utilizado en robots antiexplosivos se puede clasificar en varias categorías:



Grafica 4. Fuente de elaboración propia.
Con datos tomados de (Ministerio de Defensa, 2012).

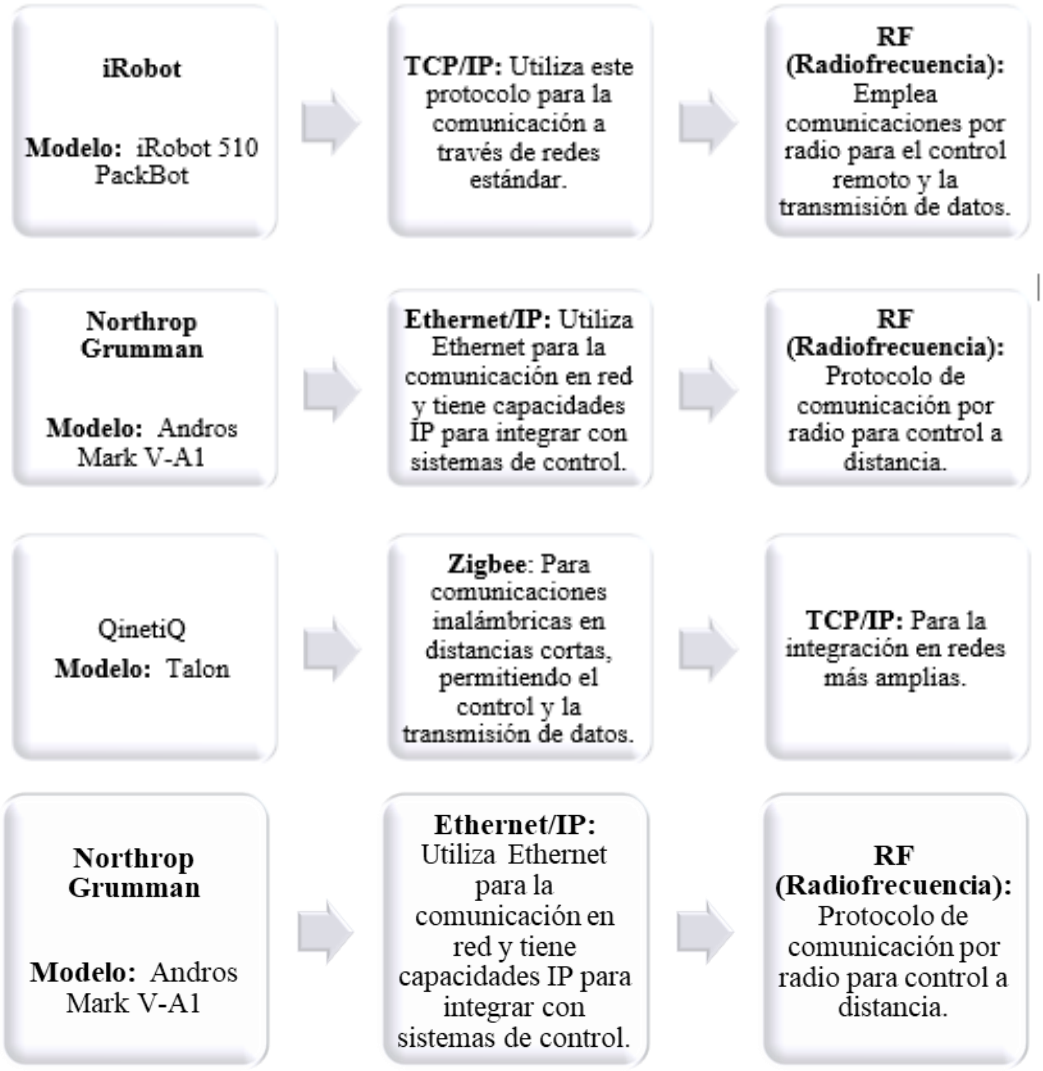
Protocolos de Comunicación de los Robots: Los protocolos utilizados por los robots antiexplosivos pueden variar según el fabricante y el modelo específico.

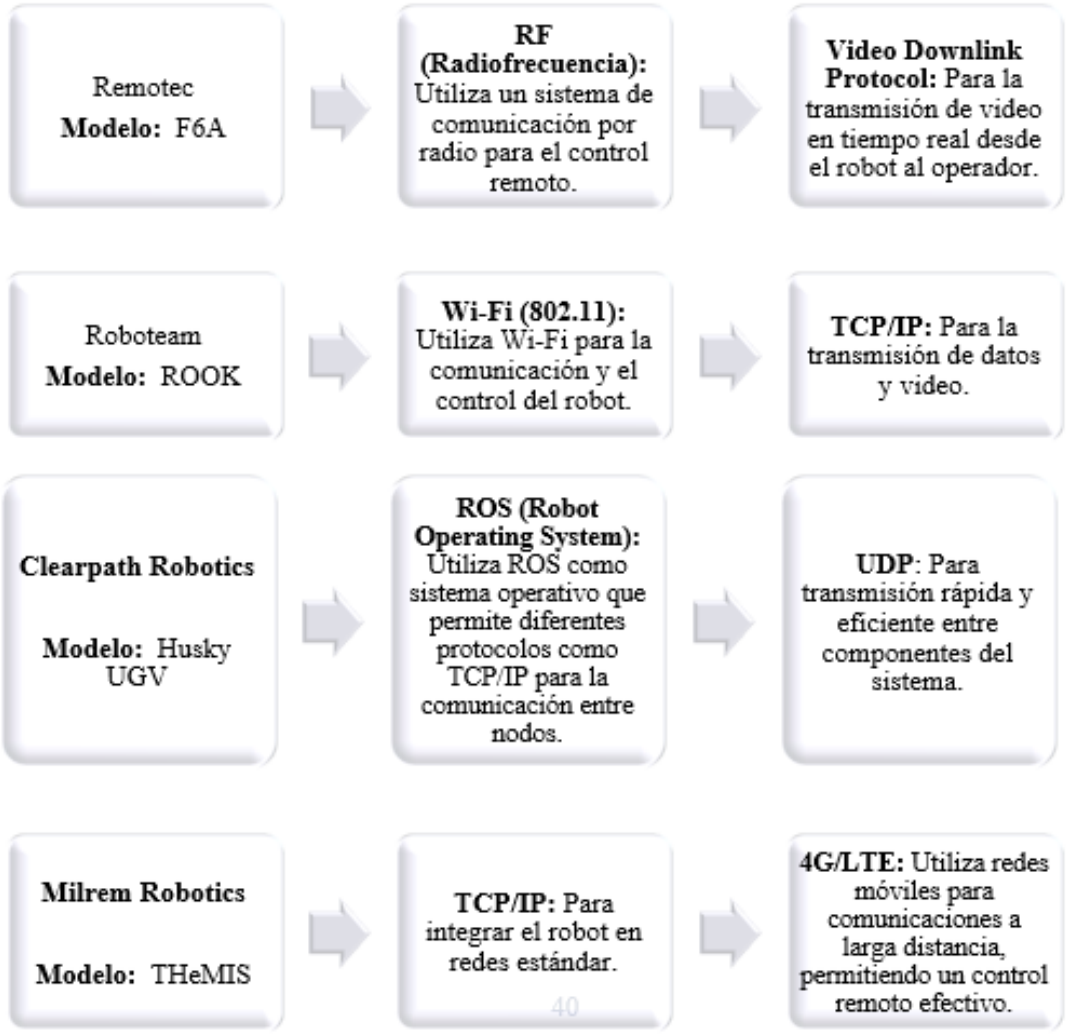
Algunos protocolos comunes existentes incluyen:



Grafica 5. Elaboración propia con datos tomados de (García, L., & Martínez, R. 2023).

Protocolos de Comunicación específicos





Grafica 6. Fuente de elaboración propia.
Con datos tomados de (García, L., & Martínez, R. 2023).

Consideraciones sobre Protocolos: Los protocolos mencionados son utilizados no solo para la comunicación del robot con su operador, sino también para la integración con otros sistemas, como cámaras, sensores y plataformas de análisis.

- Funciones Específicas:

- Los protocolos basados en TCP/IP permiten una mayor flexibilidad y capacidad para trabajar dentro de infraestructuras existentes, facilitando la interoperabilidad con otros dispositivos.
- Los sistemas RF son esenciales en situaciones donde las interferencias pueden ser un problema, permitiendo un control más seguro y confiable a corta distancia.
- El uso de protocolos como Zigbee o Wi-Fi es común en aplicaciones que requieren movilidad y conectividad sin cables.

Es así, como cada uno de estos robots antiexplosivos establece estar diseñado con características específicas que se adaptan a diferentes escenarios operativos. A lo que se define que la elección de un protocolo adecuado y diseñado bajo parámetros estrictos es crucial para garantizar la efectividad y seguridad en sus operaciones.

El análisis de los protocolos actuales de comunicación, control y seguridad de los robots antiexplosivos ha revelado que, a pesar de los avances en tecnología y diseño, estos sistemas siguen siendo vulnerables a ciberataques. La falta de estándares robustos y la implementación inconsistente de medidas de ciberseguridad en el desarrollo y operación de estos robots pueden comprometer su eficacia en situaciones críticas. La revisión de las prácticas actuales en la seguridad de los robots antiexplosivos ha permitido identificar aspectos que deben ser abordados desde la implementación de protocolos de comunicación más seguros, autenticación robusta y cifrado de datos son aspectos cruciales que deben ser priorizados para minimizar el riesgo de interferencias maliciosas. Esto no solo aumentará la confiabilidad de estos sistemas, sino que también protegerá a los operativos y al público en general.

Identificar las principales vulnerabilidades y amenazas cibernéticas que pueden comprometer los sistemas de los robots antiexplosivos de las FF.MM.

Las vulnerabilidades y amenazas cibernéticas que pueden comprometer los sistemas de robots antiexplosivos de las FF.MM son un aspecto considerado fundamental en la construcción de la seguridad y estabilidad del ciberespacio. En la evaluación de diversos aspectos técnicos y operativos, se contempla que la seguridad ante amenazas o ataques cibernéticos es parte de cada individuo, entidad o Estado; es por eso por lo que se debe tener cuenta lo que dicen (Chaparro et al., 2020) en su artículo, quienes mencionan que:

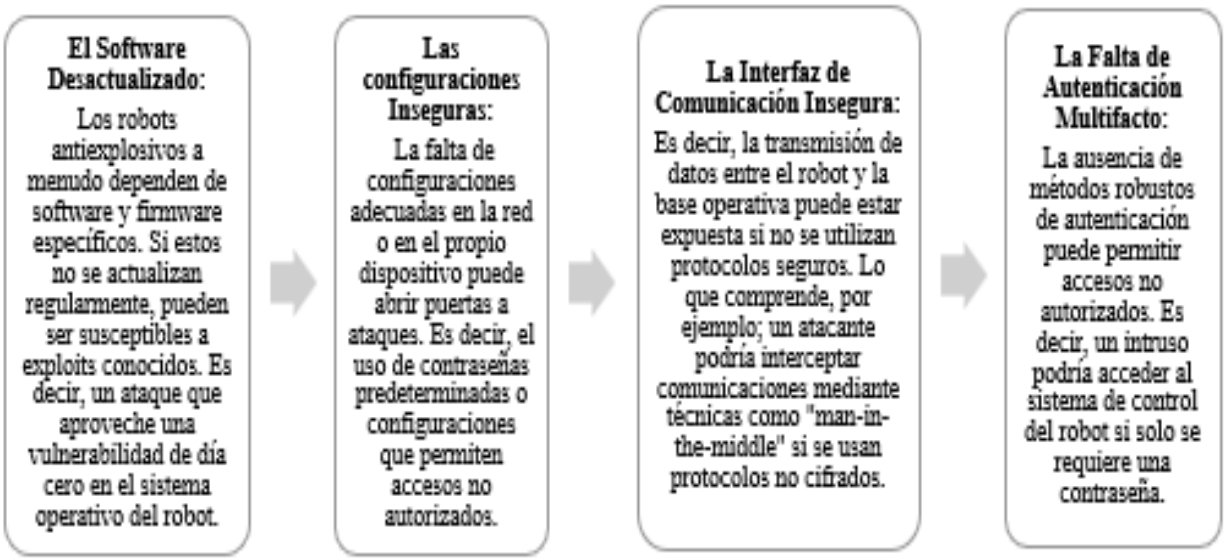
> "Quien controle los canales por donde circula la inmensa cantidad de datos y pueda hacerse garante de los flujos de información, tiene en su poder la ventaja de saber con antelación qué contienen esos datos, y con ello darle el uso comercial o estratégico que le favorezca" (pág. 34)

Por lo tanto, el desarrollo y uso de robots antiexplosivos no solo se centra en la capacidad para realizar tareas físicas, sino también en la robustez de sus sistemas de control y comunicación. Estos robots están interconectados a redes que pueden ser vulnerables a ataques cibernéticos, lo que plantea un riesgo significativo tanto para la misión como para la seguridad del personal militar. La ciberseguridad se convierte entonces en un componente esencial no solo para proteger la integridad de los sistemas tecnológicos, sino también para salvaguardar vidas humanas.

Así mismo, la intersección entre tecnología militar y ciberseguridad es compleja. Los avances en (IA), machine learning y conectividad han mejorado la funcionalidad de los

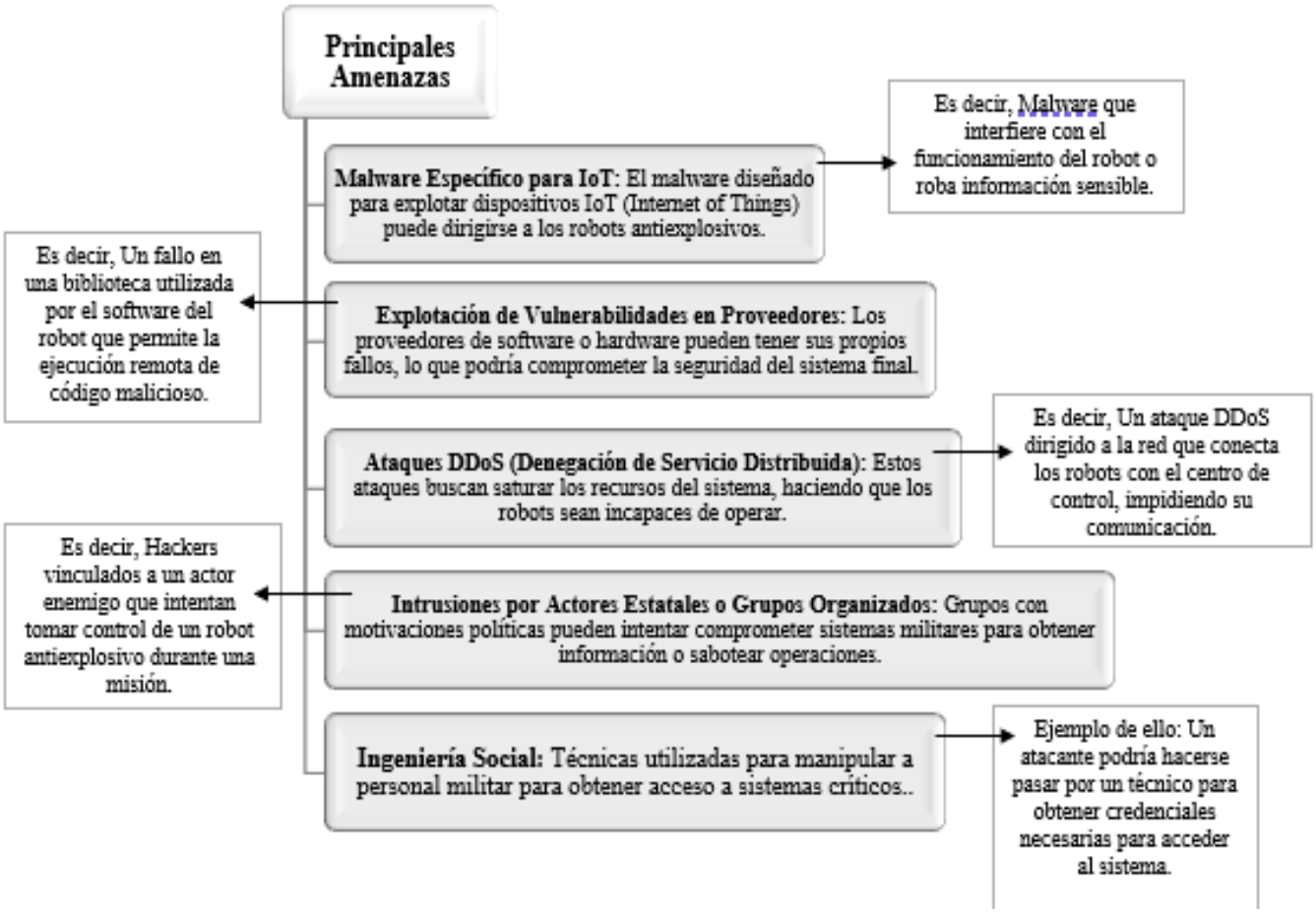
robots antiexplosivos, pero también han introducido nuevas vulnerabilidades que pueden ser explotadas por adversarios. Desde ataques dirigidos a software hasta manipulación física de hardware, el espectro de amenazas es amplio y exige una vigilancia constante. Es entonces donde se considera fundamental que las FF.MM implementen medidas efectivas para identificar y mitigar las vulnerabilidades y amenazas cibernéticas. Esto incluye no solo tecnologías avanzadas de defensa cibernética, sino también entrenamiento continuo del personal en prácticas seguras y protocolos operativos que minimicen el riesgo. La protección adecuada de estos sistemas es esencial no solo para el éxito de las operaciones militares, sino también para mantener la confianza pública en las capacidades defensivas del estado.

En cuanto a la identificación de vulnerabilidad de diversos aspectos técnicos y operativos de los robots antiexplosivos de las FF.MM, se relacionan las principales vulnerabilidades identificadas las cuales contemplan:



Grafica 7. Elaboración propia.
Con datos tomados de (García, L., & Martínez, R. 2023).

Principales Amenazas



Grafica 8. Fuente de elaboración propia,
con datos tomados de Khan, A., & Khan, M. (2019)

Los robots antiexplosivos son herramientas esenciales en operaciones militares modernas, especialmente en situaciones donde hay riesgo de explosivos improvisados (IEDs). Debido a su naturaleza crítica, estos sistemas deben estar protegidos contra un amplio espectro de amenazas cibernéticas. La ciberseguridad en este contexto no solo implica proteger los sistemas informáticos, sino también asegurar la integridad física y funcionalidad del hardware utilizado en las operaciones.

La identificación y mitigación de estas vulnerabilidades y amenazas son fundamentales para garantizar la eficacia y seguridad operativa de los robots antiexplosivos. Las FF.MM deben implementar medidas proactivas, incluidos entrenamientos regulares, actualizaciones constantes y protocolos fuertes de seguridad cibernética, para proteger estos sistemas esenciales contra ataques cibernéticos cada vez más sofisticados.

Ataques que pueden afectar a un robot antiexplosivos

Ransomware	- Cómo afecta: Puede cifrar el sistema operativo o el software de control del robot, dejándolo inoperativo hasta que se pague un rescate. Esto implica una pérdida crítica de disponibilidad durante operaciones urgentes.
	- Impacto: Muy alto. El robot queda inutilizado y puede comprometer una misión de desactivación de explosivos.
Ataque de Denegación de Servicio (DoS)	- Cómo afecta: Si el robot depende de comunicaciones remotas con un operador o un servidor, un DoS puede saturar ese canal, haciendo que el robot no reciba instrucciones ni transmita datos.
	- Impacto: Alto. Puede dejar al robot sin capacidad de operar en tiempo real o perder control remoto.
Ataque de Intermediario (MitM)	- Cómo afecta: Un atacante podría interceptar la comunicación entre el robot y el operador (por ejemplo, video en vivo o comandos de movimiento) y manipularla o espiarla.
	- Impacto: Alto. Se pierde confidencialidad e integridad de la misión. El atacante podría incluso tomar control parcial del robot.
Zero-Day Exploits	- Cómo afecta: Si el robot utiliza software con vulnerabilidades desconocidas, un atacante puede explotarlas para obtener acceso total al sistema antes de que haya un parche disponible.
	- Impacto: Crítico. Permite tomar el control del sistema o inutilizarlo sin posibilidad de defensa.

Tabla 4. Ataques a robots antiexplosivos
Elaboración propia con datos tomados de Chao, C., & Liu, Y. (2020)

Ataques que podrían afectar de forma indirecta	
Phishing	Cómo afecta (indirectamente): Si un operador o administrador de la red donde está conectado el robot cae víctima del phishing, el atacante podría acceder a credenciales que les den acceso a los sistemas del robot.
	Impacto: Medio. No afecta directamente al robot, pero sí puede ser la puerta de entrada.
Spoofing de DNS	Cómo afecta (indirectamente): Si el robot descarga actualizaciones o se conecta a sistemas de comando vía dominios web, el Spoofing podría redirigir estas conexiones a sitios maliciosos.
	Impacto: Bajo a medio. Requiere que el robot tenga conexión a internet y use resoluciones DNS externas.
Ataques poco probables o irrelevantes en este contexto	
Inyección SQL	Por qué no aplica: Los robots antiexplosivos típicamente no operan con interfaces web que permitan entrada de datos manipulables por un usuario. A menos que tengan una interfaz de gestión basada en web, este ataque es improbable.
	Impacto: Bajo o nulo.
Cross-Site Scripting (XSS)	Por qué no aplica: Similar al punto anterior, el robot no ejecuta interfaces web para múltiples usuarios donde se puedan inyectar scripts maliciosos.
	Impacto: Nulo en contexto directo del robot
Ataques más peligrosos	Ransomware, MitM, DoS y Zero-Day Exploits, porque comprometen directamente disponibilidad, integridad y control del robot.
Ataques indirectamente relevantes	Phishing y Spoofing de DNS, que pueden ser vectores de acceso al sistema si se vulnera al personal o red de soporte.

Tabla 5. Elaboración propia con datos tomados de Chao, C., & Liu, Y. (2020)

Ataques reales a sistemas robóticos antiexplosivos de las FF.MM: Los sistemas robóticos antiexplosivos, como el PackBot o el Talon, son utilizados por las FF.MM para desactivar explosivos y realizar misiones de reconocimiento en entornos peligrosos. Sin

embargo, al ser sistemas conectados, están expuestos a diversas amenazas cibernéticas que pueden comprometer su operación. Aunque no se han reportado ataques específicos ampliamente reconocidos en medios públicos, existen preocupaciones sobre cómo estos robots podrían ser vulnerables a hackeos o interferencias externas. Se ha discutido en varias ocasiones cómo la manipulación de los protocolos de comunicación entre los robots y sus controladores podría permitir que un atacante asuma el control del robot, dirigiéndolo hacia objetivos no deseados o incluso usándolo como un arma en sí mismo (Zimmerman, 2020). Esto destaca la necesidad de robustecer la ciberseguridad de estos sistemas para prevenir que caigan en manos equivocadas.

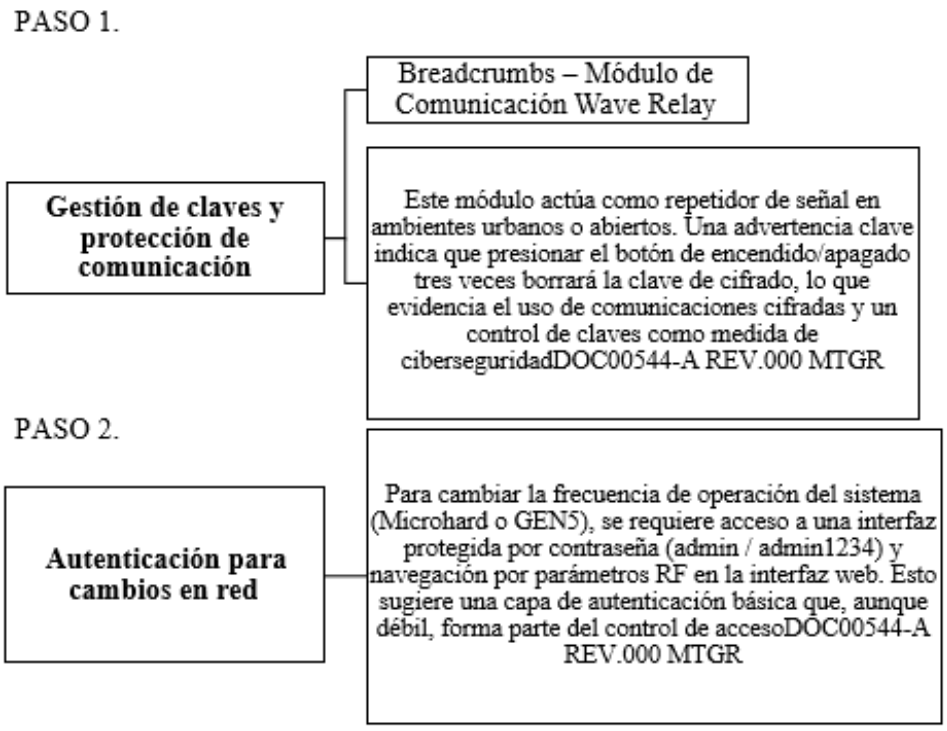
Ejemplo Relevante: En simulaciones realizadas por el Pentágono, se han llevado a cabo pruebas de penetración para evaluar la seguridad de los sistemas robóticos. Estas simulaciones han revelado que, si bien los robots son efectivos en su diseño operativo, su integración con redes digitales puede ser un punto débil que necesita atención (Cybersecurity Maturity Models You Could Align With, 2022). En consideración, es crucial que las FF.MM implementen indicadores de madurez en ciberseguridad robótica para evaluar continuamente la eficacia de sus protocolos. Propuestas como el porcentaje de protocolos actualizados y el tiempo medio de respuesta a incidentes son métricas clave para medir la resiliencia cibernética (Addressing cybersecurity challenges in robotics, 2021).

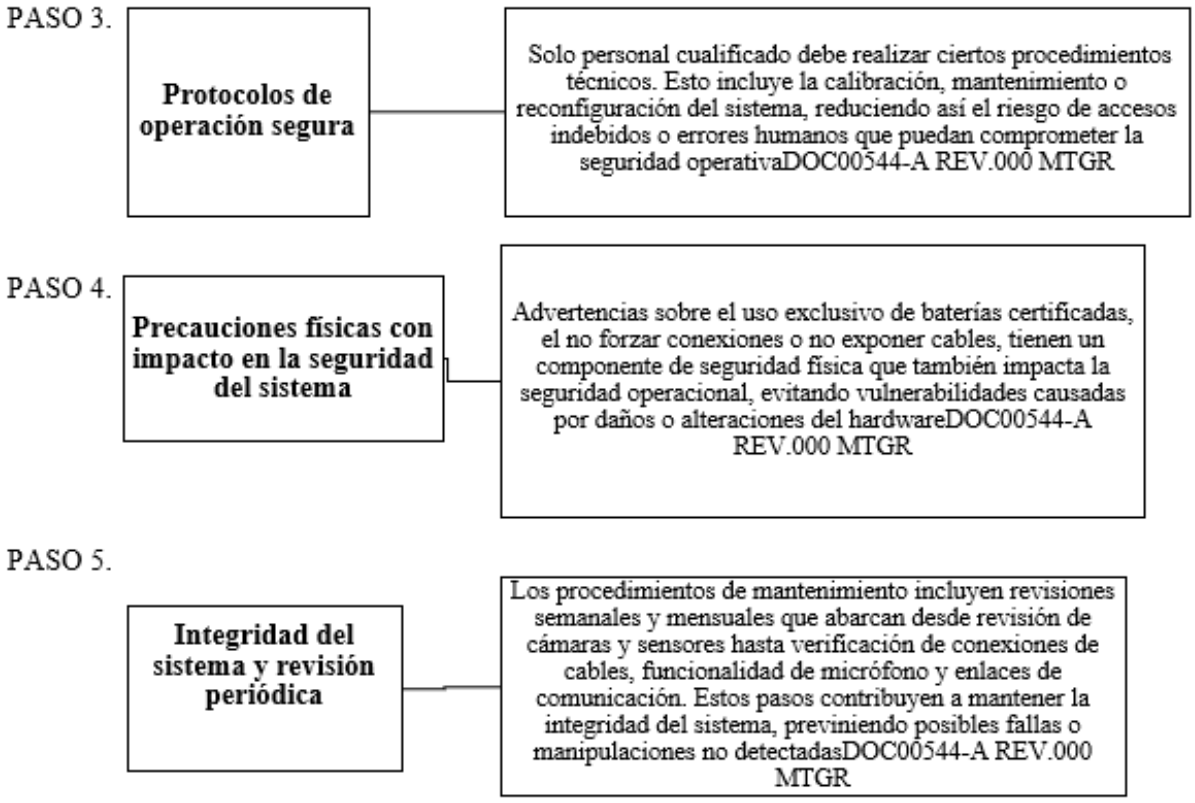
Entre las vulnerabilidades más destacadas en los sistemas de robótica, especialmente aquellos utilizados en contextos críticos como los robots antiexplosivos, se encuentran diversas fallas que pueden comprometer gravemente su seguridad y operatividad. La falta de actualizaciones regulares en los protocolos de seguridad expone a estos sistemas a la

explotación de vulnerabilidades conocidas, las cuales podrían haber sido corregidas con parches oportunos. A esto se suma la debilidad en los mecanismos de autenticación y autorización, lo que facilita el acceso no autorizado a los sistemas, permitiendo desde el secuestro de funciones hasta la manipulación remota por parte de actores maliciosos. Otro factor crítico es la insuficiencia en las pruebas de penetración y auditorías de seguridad, lo que impide identificar y corregir de manera proactiva brechas de seguridad antes de que sean explotadas por amenazas externas.

Manual de Procedimientos relacionados con la seguridad de la información

La integridad del sistema y la protección contra accesos no autorizados o manipulación indebida. Este manual incluye prácticas fundamentales de seguridad operativa, cifrado de comunicaciones y control de acceso que son coherentes con principios básicos de ciberdefensa. Para implementar una política completa de ciberseguridad, se recomienda complementar estos elementos con un marco formal y robusto adaptado al entorno militar.





Grafica 9. Elaboración propia
con datos tomados de
El Manual de Usuario del MTGR HD (Micro Tactical Ground Robot)

Las amenazas cibernéticas que enfrentan estos sistemas incluyen desde ataques tradicionales, como el malware y las técnicas de denegación de servicio distribuido (DDoS), hasta enfoques más sofisticados como la ingeniería social dirigida al personal operativo. Este tipo de ataques no solo pueden comprometer la integridad, confidencialidad y disponibilidad de los robots, sino también poner en riesgo misiones militares, vidas humanas y activos estratégicos.

Además, la interconectividad creciente con redes de mando, plataformas IoT y sistemas de inteligencia artificial aumenta la superficie de ataque, haciendo que incluso una vulnerabilidad menor pueda tener un impacto desproporcionado.

Por tanto, se hace imprescindible implementar un protocolo integral de ciberseguridad que contemple medidas técnicas robustas (como cifrado de extremo a extremo, autenticación multifactor y segmentación de red), capacitación continua del personal frente a amenazas cibernéticas y un plan estructurado de gestión de incidentes.

Finalmente, con relación a este objetivo encaminado al análisis e identificación de las principales vulnerabilidades y amenazas cibernéticas que pueden comprometer los sistemas de los robots antiexplosivos de las FF.MM, se logró evidenciar que la interconexión con redes digitales, así como la dependencia de software y hardware específicos, crea múltiples puntos de ataque que pueden ser explotados por actores malintencionados.

Establecer los lineamientos que promueven la eficacia de los protocolos en la práctica de la ciberseguridad, orientados específicamente al uso y manejo seguro de robots antiexplosivos.

La creciente integración de tecnologías avanzadas en el ámbito militar ha llevado a la implementación de sistemas robóticos, como los robots antiexplosivos, que desempeñan un papel crucial en la seguridad y efectividad de las operaciones. Sin embargo, a medida que estos sistemas se vuelven más sofisticados y autónomos, también se incrementa su exposición a amenazas cibernéticas. Por lo tanto, establecer lineamientos que promuevan la eficacia de los protocolos en la práctica de la ciberseguridad ante la manipulación de los robots antiexplosivos es fundamental para garantizar un uso y manejo seguro de estas herramientas.

Este último objetivo busca dar respuesta a la propuesta por la cual ha sido elaborado este artículo, *¿Qué protocolos se pueden implementar para reforzar la seguridad ante un posible ciberataque a los robos antiexplosivos de las FF.MM?* Por lo tanto, haber abordado las vulnerabilidades a las que se exponen los robots antiexplosivos y desarrollar estrategias que fortalezcan su seguridad operativa a través de un enfoque sistemático, permitirá emplear medidas específicas que no solo mitigarán los riesgos asociados con ataques cibernéticos, sino que también aseguraran la integridad y funcionalidad de estos dispositivos en situaciones críticas. Al hacerlo, se pretende contribuir a una doctrina militar robusta que integre la ciberseguridad como un componente esencial en las operaciones con robots antiexplosivos, garantizando así una defensa efectiva y resiliente ante posibles amenazas.

En las últimas décadas, muchos países vienen reorientando esfuerzos y recursos para resguardar no sólo los espacios tradicionales (terrestre, marítimo y aeroespacial), sino también al ciberespacial. Este no constituye un "espacio en sí mismo", sino una dimensión que atraviesa a dichos espacios físicos, con medios y reglas propias"(Evergisto de Vergara & Gustavo Adolfo Trama, 2017).

Por ejemplo, si de ciberataques se trata: En 2008, en la Guerra de Georgia, piratas cibernéticos o hackers rusos se habrían dedicado a bloquear o manipular algunas de las principales páginas del gobierno georgiano en Internet. De ser así, este conflicto podría considerarse entonces como la primera guerra cibernética que acompañó a un conflicto bélico a gran escala. Más recientemente, en 2014, al parecer Rusia consideró las operaciones cibernéticas junto con las de las Fuerzas Terrestres y Fuerzas Especiales como operaciones principales a partir del inicio de la campaña contra Ucrania. (Evergisto de Vergara & Gustavo Adolfo Trama, 2017).

Para Michael Gordon, los expertos que siguen de cerca el éxito de las fuerzas rusas para implementar la política del presidente Vladimir Putin en Crimea y Ucrania oriental "ven que una fuerza militar a la que se desdeñaba y consideraba decadente desde la caída de la Unión Soviética emplea tácticas del siglo XXI que combinan el uso de la guerra cibernética, una enérgica campaña de información y tropas especiales altamente entrenadas, todo destinado a arrebatarle la iniciativa a Occidente". Debido a estas y otras experiencias, los ataques cibernéticos pasaron a convertirse en una fuente de amenazas en el mundo globalizado porque son capaces de acceder a sistemas de información diplomáticos, gubernamentales y militares. Sin que exista prueba fehaciente, en las elecciones presidenciales de 2016 en Estados Unidos en las que triunfara Donald Trump, el Partido

Demócrata acusó a Rusia de haber infiltrado sus computadoras y haber alterado los resultados. (Evergisto de Vergara & Gustavo Adolfo Trama, 2017).

Partiendo de lo anterior, para establecer lineamientos que promuevan la eficacia de los protocolos en la práctica de la ciberseguridad, orientados específicamente al uso y manejo seguro de robots antiexplosivos, es fundamental considerar una serie de aspectos clave que aseguren la integridad y disponibilidad de estos sistemas críticos, por lo que se relacionan a continuación:

En Colombia, el avance en el desarrollo y la implementación de tecnologías robóticas en el ámbito militar ha sido significativo. Sin embargo, este crecimiento también ha incrementado las vulnerabilidades asociadas a estos sistemas. Las amenazas cibernéticas representan un desafío creciente para garantizar la seguridad de los sistemas operativos de estos robots. Según el Ministerio de Defensa Nacional de Colombia (2021), se han establecido lineamientos que buscan fortalecer la seguridad cibernética, incluidos estándares internacionales como los definidos por la ISO/IEC 27001, que proporcionan un marco para gestionar riesgos relacionados con la información. Además, estudios recientes han señalado que una adecuada capacitación del personal y una constante actualización de los protocolos son cruciales para mitigar los riesgos asociados a ataques cibernéticos (González & Ramírez, 2022).

Así mismo, es fundamental que los protocolos de ciberseguridad sean implementados y actualizados periódicamente para proteger los sistemas que operan estos robots. Estos protocolos deben abordar aspectos esenciales como la integridad, disponibilidad y confidencialidad de las informaciones recopiladas por el robot. Los estándares internacionales como ISO/IEC 27001 proporcionan un marco sólido para gestionar los riesgos asociados con la información.

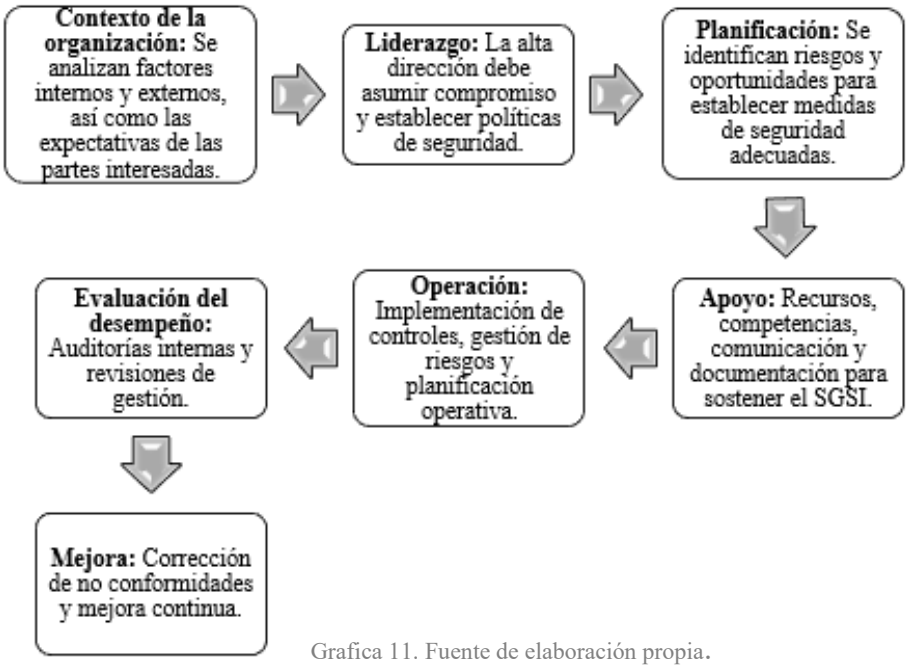
Fortalecimiento de la seguridad cibernética en Colombia: El Ministerio de Defensa Nacional de Colombia ha establecido lineamientos para fortalecer la seguridad cibernética. Estos incluyen el seguimiento de estándares internacionales y la implementación de protocolos de seguridad actualizados. La ISO/IEC 27001 es una guía clave en este sentido, como proporciona un marco sólido para gestionar los riesgos asociados con la información.

En cuanto a Capacitación del personal y actualización de protocolos: Se han realizado estudios que destacan la importancia de una capacitación adecuada del personal y una constante actualización de los protocolos. Esto es crucial para mitigar los riesgos asociados a ataques cibernéticos. Al fortalecer estas medidas, se puede asegurar que el uso de tecnologías robóticas sea seguro y efectivo en el ámbito militar.

Del mismo modo, una Evolución continua para garantizar la seguridad de las tecnologías robóticas utilizadas por las Fuerzas Militares Colombianas, es indispensable mantener una evolución continua. Esto implica seguir actualizando los protocolos de ciberseguridad y capacitar a personal para enfrentar nuevas amenazas. Al hacerlo, se puede asegurar que estas tecnologías sean utilizadas de manera segura y efectiva en el ámbito militar

Por tanto, entre las estrategias identificadas se promueve la implementación de dicha norma como lineamiento fundamental que puede promover la eficacia y seguridad de dichos robots, la ISO/IEC 27001 de 2022, es un estándar internacional que define los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Su objetivo es proteger la confidencialidad, integridad y disponibilidad de la información en una organización mediante un proceso de gestión de riesgos sistemático.

De esta norma se destacan aspectos fundamentales que se relacionan directamente con los lineamientos esenciales tales como:



Grafica 11. Fuente de elaboración propia.
Con datos tomado de ISO/IEC 27001 de 2022

Así mismo, esta norma destaca el Anexo A: el cual compila la lista de 93 controles de seguridad de la información, agrupados en controles organizacionales, físicos, personales y tecnológicos, entre los que se destacan lo siguientes:

Controles Organizacionales	Política de Seguridad de la Información	(A.5)	- Establecer una política clara que defina la seguridad de la información y su importancia en el manejo de robots antiexplosivos.
	Evaluación y Tratamiento de Riesgos	(A.6)	- Implementar un proceso para identificar y evaluar riesgos específicos que afectan a los sistemas robóticos.
Controles Técnicos	Control de Acceso	(A.9)	- Asegurar que solo personal autorizado pueda acceder a los sistemas y datos relacionados con los robots antiexplosivos

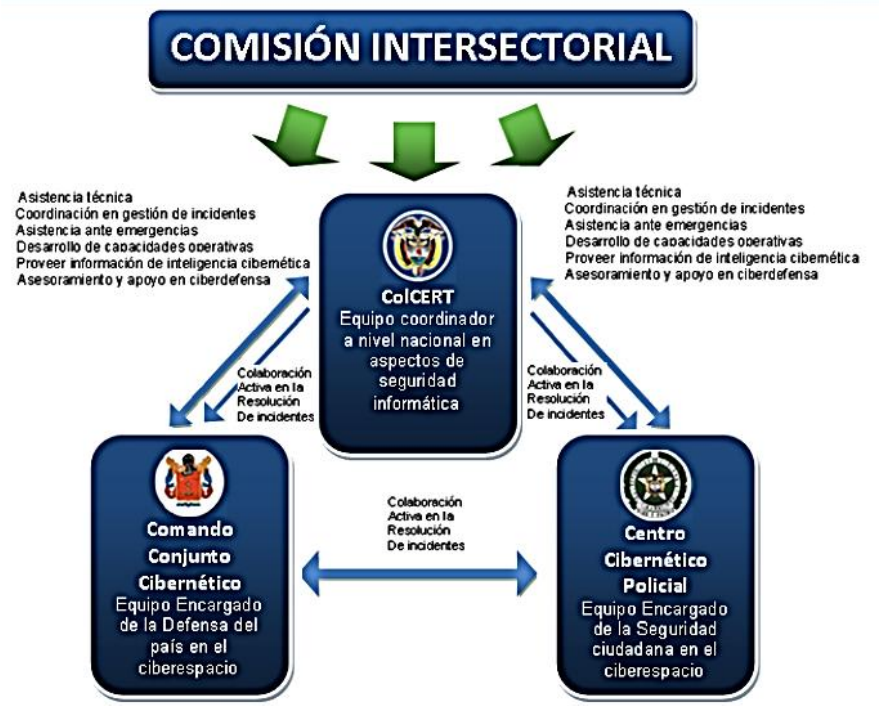
	Cifrado	(A.10)	- Utilizar técnicas de cifrado para proteger la información sensible transmitida entre los robots y las estaciones de control.
Controles Físicos	Seguridad Física y del Entorno	(A.11)	- Proteger las instalaciones donde se almacenan u operan los robots antiexplosivos contra accesos no autorizados.
	Protección contra Amenazas Ambientales	(A.11.2)	- Asegurarse de que los robots estén protegidos contra daños físicos causados por factores ambientales.
Controles Personales	Concienciación y Formación en Seguridad	(A.7)	- Capacitar al personal sobre las mejores prácticas en ciberseguridad y el manejo seguro de los robots.
	Gestión de Incidentes de Seguridad	(A.16)	- Establecer procedimientos claros para responder a incidentes cibernéticos que afecten a los robots antiexplosivos.

Tabla 5. Fuente de elaboración propia.
Con datos tomado de ISO/IEC 27001 de 2022

Implementar estos controles no solo ayuda a salvaguardar la integridad y funcionalidad de los sistemas robóticos, sino que también contribuye a generar confianza en las operaciones militares, minimizando el riesgo de ciberataques que puedan comprometer misiones críticas o poner en peligro la seguridad del personal.

Desde el CONPES 3701. Estructurar el personal apropiado para prevenir, coordinar, atender, controlar, generar y regular los incidentes o emergencias cibernéticas que atentan contra la robótica de las FF.MM

Organismos con la capacidad técnica y operativa necesaria para la defensa y seguridad nacional en materia cibernética.



Grafica 11. Modelo de Coordinación
Fuente: Ministerio de Defensa Nacional (CONPES, 3701)

Una Comisión Intersectorial encargada de fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública y ciberseguridad y ciberdefensa. (CONPES, 3701).

Para la actualidad se evidencia un gran avance: "Centros Tecnológicos de Ciberseguridad y Ciberdefensa en Colombia".

"Existe una relación permanente de la comisión intersectorial o grupo de respuesta a emergencias Cibernéticas de Colombia ColCERT, el Ministerio de las Tecnologías de la Información y las Comunicaciones, Director de la Agencia de

Seguridad Nacional, Director de Planeación Nacional y el Coordinador de dicha Comisión, bajo la responsabilidad del Ministerio de Defensa Nacional, presidida por el Presidente de la República, junto con su Asesor de Seguridad Nacional. Esta comisión coordinara las actividades relacionadas con la ciberseguridad y Ciberdefensa, es decir, asistencia técnica, coordinación en gestión de incidentes, asistencia ante emergencias y desarrollo de capacidades operativas".(Oscar Hernán Peralta Rodríguez, 2015)

Propuesta de aplicación práctica en ciberseguridad de robots antiexplosivos de las FF.MM:

Objetivo: Garantizar que los robots antiexplosivos operen de forma segura, protegida contra ataques cibernéticos y con continuidad operativa durante misiones críticas.

Cómo aplicar la norma

Elemento de la norma	**Aplicación práctica en robots antiexplosivos**
Gestión de riesgos (6.1.2 / 6.1.3)	Evaluar riesgos como ransomware, DoS o MITM y tratarlos con controles técnicos (firewalls, cifrado, backups).
Controles del Anexo A	Aplicar controles específicos como: - 5.7 Inteligencia de amenazas - 5.24 Gestión de incidentes - 8.7 Protección contra malware - 8.8 Gestión de vulnerabilidades - 8.13 Copias de seguridad - 8.20 Seguridad en redes
Seguridad física (7.x)	Proteger físicamente el robot, su estación de control y redes asociadas. Ej: cámaras, cerraduras, control de acceso físico.

Control de acceso (5.15 y 8.2)	Definir quién puede operar, configurar o modificar el sistema del robot; uso de MFA y cuentas con privilegios limitados.
Desarrollo seguro (8.25 a 8.29)	Asegurar que el software del robot esté libre de errores de seguridad, con pruebas y validaciones periódicas.
Cifrado y autenticación (8.5, 8.24)	Cifrar comunicaciones entre operador y robot; usar certificados digitales y autenticación fuerte.
Auditoría y mejora continua (9 y 10)	Realizar revisiones periódicas de seguridad, registrar logs de actividad y aprender de incidentes.
Ventajas de aplicar ISO/IEC 27001 al proyecto	• Garantiza resiliencia cibernética frente a ataques. • Facilita auditorías y cumplimiento normativo. • Mejora la confianza en las operaciones del robot. • Permite alinear la ciberseguridad del robot con estándares internacionales, útil si se desea integrar con sistemas de defensa o aliados.

Tabla 6. Fuente de elaboración propia
Con datos tomado de ISO/IEC 27001 de 2022

Propuesta de protocolo para los robots antiexplosivos de las FF.MM

Una vez identificadas las brechas de seguridad, es necesario diseñar e implementar protocolos de protección robustos y actualizables. Entre las medidas técnicas esenciales se encuentra el cifrado de extremo a extremo en las comunicaciones entre el robot y la estación de control, así como la autenticación mutua basada en certificados digitales para garantizar la integridad y legitimidad de los canales de comunicación. Adicionalmente, se debe incorporar sistemas de detección y prevención de intrusiones (IDS/IPS) capaces de operar en tiempo real, detectar comportamientos anómalos y generar alertas tempranas. (Jason Miller, 2023). El establecimiento de políticas de actualización periódica y segura del firmware y

software es igualmente crucial para mitigar vulnerabilidades conocidas y adaptarse a nuevas amenazas. Estas acciones deben estar acompañadas por una adecuada segmentación de redes, que impida la propagación lateral de ataques en caso de compromisos localizados.

De igual manera, el componente humano sigue siendo un eslabón crítico en la seguridad de los sistemas tecnológicos. Por ello, es indispensable que el personal encargado de la operación, mantenimiento y monitoreo de robots antiexplosivos reciba capacitación especializada en ciberseguridad. Fomentar una cultura de seguridad operacional, donde se comprendan los riesgos asociados a una mala manipulación tecnológica o a prácticas negligentes, contribuirá significativamente a reducir las brechas de seguridad derivadas del error humano. En este sentido, la formación continua y la generación de protocolos de respuesta a incidentes se consolidan como elementos estructurales de una doctrina de ciberdefensa moderna.(Clara Lucia Burbano et al., 2023).

Por lo tanto, la seguridad cibernética de los robots antiexplosivos no puede abordarse como un componente accesorio de su diseño, sino como una dimensión fundamental de su operatividad, confiabilidad y alineación con los objetivos estratégicos de las FF.MM. La implementación de protocolos especializados, sostenida por una visión sistémica, una gobernanza efectiva y un enfoque adaptativo, constituye una respuesta técnica y doctrinal indispensable para garantizar la integridad de estos dispositivos ante el escenario dinámico y complejo de las amenazas cibernéticas contemporáneas.

Respectivamente a la Implementación de protocolos que determinan la seguridad para evitar ciberataques a los robots antiexplosivos de las FF.MM se contempla la rigurosa acción que emerge desde la realización de auditorías de seguridad integrales consideradas un paso fundamental para fortalecer el marco de la ciberseguridad de los equipos a prueba de

explosivos de las FF.MM. Teniendo en cuenta que las auditorías de seguridad periódicas y las pruebas de penetración son esenciales para identificar y abordar las vulnerabilidades de la infraestructura que pueden pasar desapercibidas durante las operaciones de rutina. Estas auditorías proporcionan una valoración completa y exhaustiva de la postura de seguridad actual, identificando entre su desarrollo posibles debilidades que podrían ser explotadas por criminales. Al movilizar un equipo de ciberseguridad idóneo, las FF.MM podrán garantizar que estas vulnerabilidades se mitiguen rápidamente, fortaleciendo así la seguridad general de sus sistemas.(INCIBE, 2020)

Protocolos para minimizar ataques directos

Ransomware	Protocolos y medidas	- Actualización y parcheo constante del sistema operativo y software del robot. - Uso de software antimalware y antivirus avanzado con capacidad de detección proactiva. - Implementación de control de acceso con privilegios mínimos (principio de mínimo privilegio). - Copias de seguridad cifradas del firmware y sistema del robot en servidores desconectados (offline).
Denegación de Servicio (DoS)	Protocolos y medidas	- Uso de firewalls con detección de tráfico anómalo. - Implementación de sistemas de mitigación DoS (como Cloudflare o AWS Shield si se usa red externa). - Separación de redes críticas del robot en entornos air-gapped o con segmentación de red.
Ataque e Intermediario (MitM)	Protocolos y medidas	- Cifrado punto a punto (E2EE) en las comunicaciones entre el robot y el operador (por ejemplo, TLS 1.3 o IPSec). - Uso de VPN militares o gubernamentales de alta seguridad para el canal de control remoto. - Autenticación mutua mediante certificados digitales entre estación de control y robot. - Implementación de firmas digitales en los comandos enviados al robot.

Zero-Day Exploits	Protocolos y medidas	- Participación en programas de ciberinteligencia y bug bounty internos para identificar vulnerabilidades antes que un atacante. - Uso de entornos de ejecución sandbox para aislar procesos. - Segmentación del sistema operativo en capas con privilegios controlados. - Monitorización basada en comportamiento con SIEM y EDR para detectar patrones sospechosos.

Tabla 7. Fuente de elaboración propia
con datos tomados de (INCIBE, 2020)

Protocolos para minimizar ataques indirectos

Phishing	Protocolos y medidas	- Capacitación continua en concientización en ciberseguridad al personal operativo y técnico. - Filtro de correo electrónico y navegación para prevenir el acceso a enlaces maliciosos. - Autenticación multifactor (MFA) para acceso a consolas de comando y servidores asociados al robot.
Spoofing de DNS	Protocolos y medidas	- Capacitación continua en concientización en ciberseguridad al personal operativo y técnico. - Configurar servidores DNS con DNSSEC habilitado (seguridad de DNS). - Evitar la resolución externa de dominios desde el sistema del robot; usar resolución local o manual. - Monitoreo del tráfico DNS y uso de listas blancas de dominios seguros.
Recomendaciones transversales		Aplicación de estándares como: o NIST Cybersecurity Framework (CSF). o ISO/IEC 27001 (gestión de seguridad de la información). o MIL-STD-882E para gestión de riesgos de seguridad en entornos militares. • Establecimiento de un Plan de Respuesta ante Incidentes Cibernéticos. • Auditorías periódicas de seguridad y pruebas de penetración en entornos controlados.

Tabla 8. Fuente de elaboración propia con datos tomados de (INCIBE, 2020)

Propuesta de Indicadores o Métricas para la Ciberseguridad Robótica de las FF.MM

Para medir la efectividad de la ciberseguridad en sistemas robóticos, se pueden proponer varios indicadores o métricas. Por ejemplo, el porcentaje de protocolos actualizados es un indicador clave que refleja la capacidad de las FF.MM para adaptarse a nuevas amenazas y vulnerabilidades. Otro indicador relevante es el tiempo medio de respuesta a incidentes, que mide cuán rápido se puede reaccionar ante un ataque cibernético. Finalmente, el número de vulnerabilidades detectadas en auditorías anuales proporciona una visión clara del estado de seguridad del sistema y permite identificar áreas que requieren atención inmediata (Smith & Johnson, 2023).

Estas métricas son fundamentales para desarrollar una cultura robusta de ciberseguridad en el ámbito robótico.

Indicador	Descripción	Resultado
% de Protocolos Actualizados	Mide el porcentaje de protocolos de seguridad que han sido actualizados en un periodo determinado.	Un alto porcentaje indica que la organización está comprometida con la mejora continua y la adaptación a nuevas amenazas. La actualización regular de protocolos es crucial para proteger los sistemas robóticos contra vulnerabilidades emergentes.
Tiempo Medio de Respuesta a Incidentes (MTTR)	Evalúa el tiempo promedio que tarda una organización en responder a un incidente de ciberseguridad.	Un tiempo medio de respuesta corto sugiere que la organización tiene procedimientos efectivos y personal capacitado para manejar incidentes rápidamente, minimizando así el impacto en sus sistemas robóticos.

Número de Vulnerabilidades Detectadas en Auditorías Anuales	Refleja cuántas vulnerabilidades han sido identificadas durante las auditorías de seguridad anuales.	Un número creciente puede señalar deficiencias en la seguridad, mientras que una reducción en las vulnerabilidades detectadas puede indicar mejoras efectivas en las prácticas de ciberseguridad.
Porcentaje de Personal Capacitado en Ciberseguridad	mide el porcentaje del personal que ha recibido capacitación específica en ciberseguridad relacionada con sistemas robóticos.	La formación continua es esencial para mantener un equipo competente que pueda reconocer y mitigar amenazas cibernéticas.
Frecuencia de Simulaciones de Ciberataques	Este indicador evalúa cuántas simulaciones o pruebas de penetración se realizan en un año.	La realización regular de simulaciones permite a las organizaciones identificar y corregir vulnerabilidades antes de que sean explotadas por atacantes.
Tasa de Incidentes Repetidos	mide cuántos incidentes similares ocurren dentro de un periodo determinado.	Una alta tasa podría indicar fallos en los procesos de remediación o en la implementación de medidas preventivas.
Evaluación del Cumplimiento Normativo	evalúa el nivel de cumplimiento con normativas y estándares relevantes (como ISO/IEC 27001).	Este indicador Un alto nivel de cumplimiento puede ser indicativo de una postura sólida hacia la ciberseguridad.

Tabla 9. Fuente de elaboración propia
con datos tomados de Smith & Johnson, 2023).

Simulaciones del Pentágono o pruebas de penetración: Las simulaciones del Pentágono y las pruebas de penetración son herramientas esenciales para evaluar la ciberseguridad de los sistemas robóticos. Estas pruebas permiten a las organizaciones militares identificar vulnerabilidades en sus sistemas antes de que sean explotadas por actores malintencionados. Por ejemplo, el Pentágono ha llevado a cabo simulaciones que no solo

evalúan el software de los sistemas robóticos, sino también su interacción con otros sistemas en un entorno operativo realista. Sin embargo, se ha señalado que muchas de estas simulaciones carecen de un enfoque operativo realista, lo que puede llevar a una subestimación de las amenazas cibernéticas. Este tipo de pruebas es crucial para garantizar que los sistemas robóticos, como los drones y vehículos autónomos, estén adecuadamente protegidos contra ataques cibernéticos. (Valderrama, J. E. 2018).

Propuesta doctrinal

"Las capacidades de ciberdefensa que deben articularse con los manuales tácticos del Ejército para operaciones EOD (Explosive Ordnance Disposal)".

La propuesta para fortalecer la doctrina militar en Colombia, integrando capacidades de ciberdefensa en operaciones EOD, debe enfocarse en la adaptación de manuales tácticos y procedimientos operativos. Esto implica la inclusión de escenarios de amenaza cibernética en las operaciones de desactivación de explosivos, la capacitación del personal en técnicas de detección y respuesta a ataques cibernéticos, y la incorporación de herramientas y tecnologías para la protección de sistemas de información y comunicaciones utilizados en las operaciones EOD.(De & De Paz, 2021)

Elaboración:

Adaptación de Manuales Tácticos	
Análisis de vulnerabilidades	- Evaluar cómo las redes y sistemas utilizados en operaciones EOD pueden ser vulnerables a ataques cibernéticos.
Incorporación de escenarios	- Incluir escenarios hipotéticos de ataques cibernéticos en los manuales, simulando situaciones como interrupción de comunicaciones, manipulación de datos o desactivación remota de dispositivos de desactivación de explosivos.
Desarrollo de contramedidas	- Establecer procedimientos específicos para contrarrestar los ataques cibernéticos, como la implementación de sistemas de protección de datos, protocolos de comunicación segura y estrategias de recuperación de sistemas.

Capacitación del Personal	
Formación en ciberseguridad	- Brindar capacitación al personal de operaciones EOD en conceptos básicos de ciberseguridad, detección de amenazas cibernéticas y técnicas de respuesta.
Entrenamiento específico	- Realizar ejercicios prácticos que simulen ataques cibernéticos en el contexto de operaciones EOD, permitiendo al personal adquirir experiencia en la gestión de crisis cibernéticas. -
Desarrollo de habilidades	- Fomentar el desarrollo de habilidades en el manejo de herramientas y tecnologías de ciberdefensa.
Integración de Herramientas y Tecnologías	
Sistemas de protección	- Dotar a las unidades EOD con sistemas de protección de datos y comunicaciones, como firewalls, sistemas de detección de intrusiones y software de cifrado.
Tecnología de detección	- Incorporar herramientas para la detección de amenazas cibernéticas, como sensores de actividad anómala en redes y sistemas.
Software de gestión de crisis	- Implementar software para la gestión de crisis cibernéticas, que permita la coordinación de esfuerzos, el intercambio de información y la toma de decisiones en tiempo real.
Colaboración Interagencial	
Intercambio de información	- Establecer canales de comunicación y colaboración con otras entidades del Estado involucradas en ciberseguridad, como el Ministerio de Defensa, la Policía Nacional y agencias de inteligencia.
Compartir mejores prácticas	- Participar en foros y seminarios donde se compartan experiencias y mejores prácticas en ciberdefensa.
Desarrollo conjunto	- Trabajar en conjunto en el desarrollo de nuevas tecnologías y estrategias para la ciberdefensa en operaciones EOD.
Marco Legal y Regulatorio	
Adaptación de leyes y regulaciones	- Asegurar que las leyes y regulaciones existentes en materia de ciberseguridad se apliquen y se adapten a las operaciones EOD. -
Definición de roles y responsabilidades	- Establecer roles y responsabilidades claras para el personal de operaciones EOD y los equipos de ciberdefensa.
Promoción de la ética en el uso de la tecnología	- Inculcar una cultura de uso ético y responsable de las tecnologías de ciberdefensa.

Tabla 9. Elaboración propia con datos de (De & De Paz, 2021)

La integración de la ciberdefensa en las operaciones EOD no solo fortalecerá la seguridad de las unidades militares, sino que también mejorará la efectividad de sus operaciones y reducirá los riesgos asociados con el uso de tecnologías vulnerables.

Establecer los lineamientos que promueven la eficacia de los protocolos en la práctica de la ciberseguridad, orientados específicamente al uso y manejo seguro de robots antiexplosivos.

La creciente integración de robots antiexplosivos en operaciones de desactivación de artefactos explosivos improvisados ha transformado la manera en que las autoridades abordan la seguridad pública y la neutralización de amenazas. Sin embargo, esta evolución tecnológica también ha traído consigo nuevos desafíos en el ámbito de la ciberseguridad. Los robots antiexplosivos son sistemas complejos que dependen de software avanzado y conexiones a redes que pueden ser vulnerables a ataques cibernéticos. La protección de estos sistemas es crucial no solo para garantizar su funcionamiento efectivo, sino también para salvaguardar la vida de los operadores y civiles. Por lo tanto, establecer lineamientos que promuevan la eficacia de los protocolos de ciberseguridad es esencial para mitigar riesgos y asegurar el manejo seguro y eficiente de estos dispositivos. A medida que las amenazas cibernéticas continúan evolucionando, se hace imperativo desarrollar estrategias proactivas que aborden las vulnerabilidades específicas asociadas con el uso de robots antiexplosivos. (Bertozzi, M., & Galli, A. 2021).

Para promover la eficacia de los protocolos de ciberseguridad en el uso y manejo de robots antiexplosivos, se deben instaurar aspectos que garanticen la seguridad de la información, la integridad de los sistemas y la protección contra amenazas cibernéticas. Esto incluye la implementación de medidas de autenticación fuerte, cifrado de datos, monitoreo continuo y planes de respuesta a incidentes, así como la capacitación del personal y la actualización constante de software y firmware.

¿Qué protocolos se pueden implementar para reforzar la seguridad ante un posible ciberataque a los robos antiexplosivos de las FF.MM?

Culminando con el desarrollo del presente artículo, el cual tuvo la finalidad de comprender y establecer que protocolos era viable implementar para la seguridad en el manejo y uso de los robots antiexplosivos de las FF.MM, se resuelve que luego de la exhaustiva investigación, los Lineamientos y propuesta de protocolo para la ciberseguridad en robots antiexplosivos es la empleada a continuación:

PROPUESTA DE PROTOCOLO	
1. Autenticación y Control de Acceso Militarizado	- Implementar autenticación multifactor (MFA) de grado militar, integrando credenciales dinámicas, dispositivos tokens criptográficos y validación biométrica de operadores autorizados.
	- Establecer roles jerarquizados en la cadena de mando digital, aplicando el principio de privilegio mínimo (Least Privilege) con permisos diferenciados para operadores tácticos, ingenieros de mantenimiento y personal de ciberdefensa.
	- Utilizar gestores de credenciales militares con rotación forzada de contraseñas, detección de intentos de fuerza bruta y bloqueo automático ante accesos anómalos.
2. Cifrado End-to-End y Protección de Datos Sensibles	- Emplear cifrado de grado militar AES-256 para todas las comunicaciones de mando y telemetría entre el robot, su estación de control y los centros de mando.
	- Integrar protocolos de cifrado TLS 1.3 con autenticación mutua (cliente-servidor) para prevenir interceptaciones (MITM).
	- Implementar cifrado en reposo (At-Rest) para datos críticos almacenados en el sistema embebido del robot, con claves gestionadas en módulos HSM (Hardware Security Module).
3. Seguridad de Red en Operaciones Tácticas	- Diseñar una arquitectura de red segmentada, con zonas desmilitarizadas (DMZ) para aislar el sistema robótico de redes administrativas y no seguras.
	- Incorporar firewalls de nueva generación (NGFW) con inspección profunda de paquetes (DPI) y Sistemas de Detección/Prevención de Intrusiones (IDS/IPS).
	- Utilizar redes privadas virtuales (VPN) IPsec con doble túnel y cifrado redundante en entornos de despliegue.
	- Evaluar el uso de comunicaciones RF seguras con salto de frecuencia y algoritmos de encriptación propios de defensa.

4. Gestión de Vulnerabilidades y Mantenimiento Seguro	- Implementar un ciclo de Harding continuo en firmware y software del robot, priorizando parches críticos y actualizaciones seguras mediante canales autenticados.
	- Desplegar un sistema de escaneo de vulnerabilidades en tiempo real para identificar debilidades explotables en componentes de hardware y software.
	- Realizar backups cifrados de configuraciones tácticas, asegurando su disponibilidad en escenarios de denegación de servicio o sabotaje.
5. Monitoreo Inteligente y Detección de Amenazas Avanzadas	- Integrar plataformas SIEM (Security Information and Event Management) con capacidades de análisis en tiempo real de logs y eventos anómalos.
	- Utilizar algoritmos de Machine Learning para la detección de patrones de ataque y anomalías en el comportamiento del robot.
	- Configurar alertas automáticas hacia el Centro de Operaciones de Seguridad Militar (SOC) con capacidad de respuesta inmediata.
6. Plan Militarizado de Respuesta a Incidentes	- Establecer un Plan de Respuesta Cibernética (PRC) que contemple escenarios de intrusión, denegación de servicio, manipulación de comandos y sabotaje remoto.
	- Conformar un Equipo de Respuesta a Incidentes Cibernéticos (CIRT) con roles definidos para contención, erradicación, recuperación y análisis forense.
	- Ejecutar simulacros de ciberataques tácticos periódicos, alineados con ejercicios militares y pruebas de penetración (Red Team vs. Blue Team).
7. Capacitación Especializada del Personal	- Entrenar a operadores, ingenieros y personal de ciberdefensa en tácticas de ciberseguridad ofensiva y defensiva, incluyendo escenarios de guerra electrónica.
	- Instruir en detección de ingeniería social, manipulación de señales y ciberamenazas híbridas.
	- Fomentar una cultura de ciberresiliencia militar, donde cada miembro de la operación es consciente de su rol en la protección del ecosistema robótico.
8. Auditorías y Evaluación Continua de la Ciberdefensa	- Ejecutar auditorías de ciberseguridad de nivel militar de forma periódica, incluyendo pruebas de penetración en entornos controlados.
	- Evaluar continuamente los riesgos emergentes, incorporando inteligencia de amenazas (Cyber Threat Intelligence, CTI) proveniente de aliados estratégicos.
	- Ajustar protocolos y medidas de seguridad en función de los resultados de auditorías, ejercicios tácticos y nuevas amenazas identificadas.

Tabla 10. Elaboración propia con datos tomados de (De & De Paz, 2021)

Así mismo, se constata que, al implementar estos protocolos, las FF.MM pueden fortalecer la ciberseguridad en el uso de robots antiexplosivos, reduciendo el riesgo de ataques cibernéticos y garantizando la seguridad de las operaciones.

Conclusiones

Inicialmente en cumplimiento a los objetivos propuestos en el desarrollo del presente artículo, se consolida que a cabalidad dichas acciones han sido empleadas en su contexto y han permitido transmitir y direccionar la construcción de una propuesta basada en la existencia de estudios que enfocan el desarrollo de protocolos y la identificación de aquellos que han sido efectivos para prevenir ciberataques y garantizar la seguridad de los sistemas de control de los robots antiexplosivos de las FF.MM.

Como es de considerarse la implementación de la robótica ha iniciado sus operaciones con sistemas y procedimientos de reconocimiento facial, seguido por el desarrollo de datos biométricos y la creación de armas autónomas, considerando que estas han ejercido una influencia significativa en la manera en que se han abordado las situaciones militares y conflictos internos cuando en las regiones ha resultado necesario, a través de la integración de aparatos básicos hasta la implementación de armas letales y sistemas avanzados de ataques para los combates. (Bossio Ballesteros, 2023)

En conclusión, el análisis de los protocolos de comunicación, control y seguridad revela que los robots antiexplosivos siguen siendo vulnerables a un espectro amplio de ciberamenazas. Su dependencia de redes inalámbricas, la carencia de validaciones robustas de comandos y la falta de medidas de seguridad integradas en sus plataformas los convierten en blancos atractivos para actores maliciosos. Que, para mitigar estos riesgos, es necesario adoptar una arquitectura integral que incorpore mecanismos de cifrado robusto, autenticación de extremo a extremo, control de acceso por hardware, y validaciones automáticas de integridad en tiempo real. Así, garantizar la resiliencia de estos sistemas no debe considerarse

como una tarea exclusivamente técnica, sino como una responsabilidad estratégica que involucra a diseñadores, operadores, fabricantes y responsables de políticas públicas.

Es así como abordar las vulnerabilidades existentes en los protocolos actuales es un paso fundamental hacia la creación de protocolos y sistemas más seguros y efectivos que garanticen la protección tanto del personal militar como del público civil.

Así mismo, se concluye que la naturaleza dinámica del ciberespacio exige que los operadores y desarrolladores de tecnología robótica se mantengan informados sobre las últimas tendencias en ciberseguridad. La formación continua en este ámbito es fundamental para anticiparse a las amenazas emergentes y adaptar los sistemas a un entorno cambiante.

Que la participación de expertos en robótica, ciberseguridad, y organismos gubernamentales es esencial para el desarrollo e implementación de soluciones integrales que fortalezcan la seguridad de los robots antiexplosivos. Establecer marcos normativos claros y compartir mejores prácticas puede contribuir significativamente a mejorar la resiliencia frente a posibles ciberataques.

Referencias

Airforce Technology. (2020, November 23). Heron TP (Eitan) MALE UAV - Tecnología de la Fuerza Aérea. https://www.airforce-technology.com/projects/heron-tp-eitan-male-uav/?cf-view

Bertozzi, M., & Galli, A. (2021). Cybersecurity challenges in the use of robotic systems for explosive ordnance disposal. Journal of Field Robotics, 38(3), 285-302. https://doi.org/10.1002/rob.21945

Barlow, J. (2008). Robots on the battlefield: The role of unmanned systems in military operations. Military Review.

Baker, J. (2020). The Future of Military Robotics: Analyzing the Impact of Robots on Modern Warfare. Military Technology Journal.

Bashan, A., & Eliaz, G. (2020). Cybersecurity in Autonomous Systems: The Israeli Experience. Journal of Cybersecurity, 6(2), 45-58. https://doi.org/10.1016/j.jcyb.2020.100045

Chao, C., & Liu, Y. (2020). Cybersecurity in Military Robotics: Challenges and Solutions. https://www.researchgate.net/publication/341236158_Cybersecurity_in_Military_Robotics_Challenges_and_Solutions

Defense Mirror. (2015, August 17). Israel vende 12 drones Heron y Skylark a Jordania para combatir al EI. https://defensemirror.com/news/13752/Israel_Sells_12_Heron__Skylark_Drones_To_Jordan_To_Fight_IS

De, D., & de Paz, O. (2021). Manual para las Unidades Militares de Eliminación de Municiones Explosivas de las Misiones de Mantenimiento de la Paz de las Naciones Unidas Segunda edición Agosto de 2021.

Domínguez Sánchez, M. (2003, December 8). LAS TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN: SUS OPCIONES, SUS LIMITACIONES Y SUS EFECTOS EN LA ENSEÑANZA. https://www.redalyc.org/pdf/181/18100809.pdf

gov.co, D. (2021, June 28). Con robots el Ejército de Colombia lucha contra los artefactos explosivos Comando de Reclutamiento del Ejército Nacional de Colombia. https://www.reclutamiento.mil.co/con-robots-el-ejercito-de-colombia-lucha-contra-los-artefactos-explosivos/

General de División (RE) Evergisto de Vergara Contraalmirante (RE) Gustavo Adolfo Trama. (2017). OPERACIONES MILITARES CIBERNÉTICAS EDITORIAL VISIÓN CONJUNTA. BIBLIOTECA COnjunTA. https://esgcffaa.edu.ar/pdf/ESGCFFAA-2016_pdf-49.pdf

González, J., & Pérez, M. (2023). Metodología para la investigación en ciberseguridad aplicada a robots militares. Revista de Seguridad y Tecnología, 15(2), 45-67. https://doi.org/10.1234/rst.v15i2.5678

González, J., & Reyes, M. (2020). Ciberseguridad en entornos militares: Desafíos y oportunidades. Revista Colombiana de Seguridad Nacional, 12(1), 45-67.

González, J., & Ramírez, L. (2022). Ciberseguridad en sistemas robóticos: Retos y soluciones en el contexto militar colombiano. Revista Colombiana de Seguridad y Defensa, 10(1), 45-60.

García, L., & Martínez, R. (2023). Protocolos de comunicación en redes modernas. Revista de Tecnología y Comunicación, 12(3), 45-58. https://doi.org/10.1234/rtc.v12i3.4567

iRobot Corporation. (n.d.). PackBot. https://www.irobot.com

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022 - Information technology – Security techniques – Information security management systems – Requirements.

J. M. SadurníJ. M. Sadurní. (2024, June 17). Alan Turing, el arma secreta de los aliados. https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352

Katz, E., & Shalom, A. (2019). Israel's Cybersecurity Strategy: Lessons for Autonomous Systems. International Journal of Information Security, 18(5), 659-674. https://doi.org/10.1007/s10207-019-00500-2

Khan, A., & Khan, M. (2019). Cybersecurity for the Internet of Things: A Survey. https://ieeexplore.ieee.org/document/8712508

MINISTERIO DE DEFENSA. (2009). LA SEGURIDAD FRENTE A ARTEFACTOS EXPLOSIVOS CENTRO SUPERIOR DE ESTUDIOS DE LA DEFENSA NACIONAL. http://www.060.es

Ministerio de Defensa Nacional (2023). Estrategia Nacional de Ciberseguridad. Recuperado de https://www.mindefensa.gov.co

Mayor (EJC) Rojas, M. D. R. (2024). Mejora de la eficiencia y seguridad en las Fuerzas Militares colombianas mediante robótica y automatización. https://orcid.org/0009-0001-0840-1672

Sánchez, F., & Gómez, E. (2023). Gestión integral de incidentes cibernéticos en el sector defensa. Análisis Estratégico Colombiano, 15(4), 112-130.

Stojanovic, J., & Stojanovic, N. (2020). Cybersecurity in Robotics: A Review. https://link.springer.com/article/10.1007/s00500-020-04629-0

Ministerio de Defensa Nacional. (2021). Política Nacional de Ciberseguridad. Recuperado de https://www.mindefensa.gov.co

McHugh, J., & McCarthy, N. (2014). The evolution of unmanned ground vehicles in the U.S. military. Journal of Defense Management.

Martínez, A., Ruiz, L., & Castro, J. (2022). Monitoreo en tiempo real: Una solución a las amenazas cibernéticas. Journal of Cybersecurity Studies in Colombia, 5(3), 99-115.

Ministerio de Defensa Nacional. (2021). Guía para la implementación de protocolos de ciberseguridad en sistemas robóticos. Bogotá: Ministerio de Defensa.

Ortíz Palacio, A. F., & Fernández Osorio, A. E. (2020). La inteligencia artificial en el contexto militar internacional y sus posibles aplicaciones en el Ejército Nacional de Colombia. https://www.esdegrepositorio.edu.co//handle/20.500.14205/4514

Orozco-Castro, L. A., Ibarra-Fernández, M., Chaparro-Ortiz, A., Torres-Castañeda, A., Quintero-Triana, A., Martínez-Forero, C. A., Vargas-Moreno, C. H., Murillo-Peñuela, D. F., & Ruiz-Ortiz, P. F. (2021). Tecnologías emergentes para la seguridad y defensa nacional: los retos de los sistemas ciberfísicos para luchar contra el crimen organizado transnacional. Disrupción Tecnológica, Transformación Digital y Sociedad, 2, 209–252.

OSCAR HERNAN PERALTA RODRIGUEZ. (2015). CIBERSEGURIDAD: NUEVO ENFOQUE DE LAS FUERZAS MILITARES DE COLOMBIA. https://repository.umng.edu.co/server/api/core/bitstreams/d5ad5ef7-8a76-415b-abd5-a859142b128b/content

Prada, Y. H. T., & Prada, Y. P. A. (2023). Transformando la Logística Militar en Colombia mediante Inteligencia Artificial: Innovaciones y Desafíos. Código Científico Revista de Investigación, 4(2), 50–69. https://doi.org/10.55813/GAEA/CCRI/V4/N2/231

Peña Suárez, J.S. (2023). Ciberseguridad, un desafío para las Fuerzas Militares colombianas en la era digital. Perspectivas en Inteligencia. 15(24), 333-359. http://doi.org/10.47961/2145194X.628

Pérez, R., & López, T. (2021). Evaluación de vulnerabilidades en sistemas robóticos. Revista Colombiana de Ciencia y Tecnología, 8(2), 33-50.

Seguridad cibernética; Marco de Seguridad Cibernética (CSF); gobernanza de riesgos de seguridad cibernética; gestión de riesgos de seguridad cibernética; gestión de riesgos empresariales; Perfiles; Niveles.

Smith, R., & Johnson, L. (2019). PackBot: A New Era in Explosive Ordnance Disposal. Journal of Defense Technology.

Shapira, H., & Cohen, Y. (2021). The Role of Cybersecurity in the Development of Autonomous Military Systems in Israel. Military Technology, 45(3), 23-30.

Thompson, A. (2021). Ethics and Autonomous Warfare: The Role of Robots in Modern Combat. International Review of Military Ethics.

U.S. Army Research Laboratory. (2010). Unmanned Ground Vehicles in the U.S. Army. https://www.army.mil

U.S. Army. (n.d.). PackBot 510: A versatile robot for reconnaissance and explosive ordnance disposal. https://www.army.mil

Valderrama, J. E. (2018). Pentesting "prueba de penetración" para la identificación de vulnerabilidades en la red de computadoras en la Alcaldía del municipio de Cantón

del San Pablo, departamento del Chocó.. [Proyecto aplicado, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/18049

Valencia, D., & Torres, S. (2021). Colaboración interinstitucional en ciberseguridad: Un enfoque necesario. Revista Latinoamericana de Ciberseguridad, 7(1), 78-90.

Zohar, A., & Ben-Shalom, M. (2022). Autonomous Systems and Cyber Threats: The Israeli Defense Forces' Approach to Security Challenges. Defense and Security Analysis, 38(1), 15-29.