Integración e interoperabilidad de los sistemas de comunicaciones de las Fuerzas Militares empleando tecnología digital.

Capitán de Corbeta Juan Sebastián Ospina Arango

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	:	CC Juan Sebastián Ospina Arango
Identificación	:	16078707
Programa académico	:	Maestría en Ciberseguridad y Ciberdefensa
Tutor metodológico	:	Jairo Andrés Becerra
Tutor temático	:	Giovanni Alberto Gómez Rodríguez
Fecha de entrega	:	25/08/2025
Extensión	:	7786 palabras

Integración e interoperabilidad de los sistemas de comunicaciones de las Fuerzas Militares empleando tecnología digital.

Integration and interoperability of the Armed Forces' communication systems using digital technology.

Juan Sebastián Ospina Arango[1]

Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este trabajo analiza la situación actual de los sistemas de comunicación digital utilizados por el Ministerio de Defensa Nacional y las Fuerzas Militares de Colombia (FFMM), identificando brechas críticas en interoperabilidad, soberanía de datos y seguridad cibernética. Desde una perspectiva cualitativa con enfoque inductivo, se evaluaron plataformas empleadas para correo electrónico y mensajería instantánea, así como su arquitectura (on-premise o tercerizada) y mecanismos criptográficos. El análisis revela que las tecnologías actuales presentan vulnerabilidades explotables por actores maliciosos, tales como phishing, pérdida de integridad y falta de cifrado extremo a extremo. Frente a ello, se propone la adopción de tecnologías open-source como Rocket.Chat y Mattermost, bajo despliegues on-premise, por su capacidad de hardening, cifrado integral, control de metadatos y cumplimiento de estándares militares. El estudio concluye que, para garantizar comunicaciones seguras, resilientes y soberanas, es imperativo que las FFMM adopten soluciones integradas, estandarizadas y con control total sobre infraestructura, usuarios y datos. Se recomienda una migración progresiva hacia arquitecturas Zero Trust, fortaleciendo la ciberdefensa nacional frente a amenazas híbridas y persistentes avanzadas (APT).

---

[1] Capitán de Corbeta de la Armada Nacional de Colombia. Candidato a magíster en Ciberseguridad y Ciberdefensa, Escuela Superior de Guerra "General Rafael Reyes Prieto", Colombia. Profesional en Ingeniería Industrial, Universidad Nacional de Colombia, Colombia. Contacto: juan.ospina@armada.mil.co

Palabras clave: ciberdefensa, interoperabilidad, comunicaciones militares, hardening, soberanía digital, Zero Trust, encriptación, plataformas on-premise

Abstract: This research analyzes the current state of digital communication systems used by the Colombian Ministry of National Defense and the Armed Forces (FFMM), identifying critical gaps in interoperability, data sovereignty, and cyber resilience. Using a qualitative methodology with an inductive approach, the study evaluates the platforms employed for email and instant messaging, their infrastructure architecture (on-premise or outsourced), and the encryption mechanisms in place. Findings indicate that current systems are vulnerable to phishing, integrity loss, and lack end-to-end encryption, posing significant operational risks. As a strategic solution, the paper proposes the adoption of open-source platforms such as Rocket.Chat and Mattermost, deployed under on-premise models, for their enhanced hardening capabilities, integrated encryption, metadata control, and alignment with military-grade cybersecurity standards. The research concludes that achieving secure, resilient, and sovereign communications demands an integrated and standardized communication framework with full control over infrastructure, users, and data. A progressive migration toward Zero Trust architectures is recommended to strengthen national cyberdefense capabilities against hybrid and advanced persistent threats (APT).

Keywords: cyberdefense, interoperability, military communications, hardening, digital sovereignty, Zero Trust, encryption, on-premise platforms.

Tabla de contenido

INTRODUCCIÓN

En los escenarios contemporáneos de conflicto, donde los dominios tradicionales de la guerra han sido ampliados con la inclusión del ciberespacio, garantizar la protección de la información sensible del Estado se ha convertido en un factor decisivo para la defensa nacional. Las Fuerzas Militares de Colombia (FFMM), en su misión de salvaguardar la soberanía y seguridad del país, requieren sistemas de comunicación digital que no solo sean funcionales, sino que respondan a estándares elevados de confidencialidad, integridad y disponibilidad de la información. En este contexto, el Ministerio de Defensa Nacional (MDN) se enfrenta al reto de fortalecer su arquitectura tecnológica para enfrentar las crecientes amenazas cibernéticas y garantizar una operación conjunta, interoperable y resiliente.

Actualmente, las FFMM emplean diversas plataformas de correo electrónico y mensajería instantánea como Outlook, Zimbra y servicios de buzón institucionaL que, si bien permiten el intercambio de información entre dependencias, carecen de estandarización, interoperabilidad y mecanismos robustos de cifrado extremo a extremo. Aún más preocupante es la adopción informal de aplicaciones comerciales como WhatsApp o Signal para la transmisión de datos operacionales, lo cual expone a las unidades tácticas y estratégicas a serios riesgos de seguridad, dado que se desconoce el tratamiento y destino final de los mensajes enviados a través de dichas plataformas.

La falta de un sistema unificado y soberano de comunicaciones digitales pone en evidencia una superficie de ataque ampliada que puede ser explotada por actores hostiles, tanto estatales como no estatales, interesados en acceder a datos sensibles de carácter militar. Las amenazas

persistentes avanzadas (APT), el espionaje cibernético, la ingeniería social y las técnicas de phishing han evolucionado al punto de comprometer sistemas enteros mediante una única brecha mal gestionada. Por tanto, resulta indispensable repensar el modelo actual y adoptar soluciones que permitan al MDN y a las FFMM ejercer control total sobre su entorno operativo, desde el hardware hasta los datos y usuarios que lo componen.

El presente artículo propone un análisis técnico y doctrinal sobre los medios digitales empleados por las Fuerzas para la transmisión de información clasificada, evaluando sus debilidades y contrastándolas con alternativas tecnológicas disponibles en el mercado. A partir de una metodología cualitativa e inductiva, sustentada en revisión documental y análisis comparativo, se plantean recomendaciones orientadas a fortalecer la ciberresiliencia institucional mediante el uso de plataformas open-source desplegadas bajo arquitecturas on-premise. Soluciones como Rocket.Chat y Mattermost, la cuales, al ser gestionadas de forma interna, ofrecen un nivel superior de seguridad, personalización y gobernanza de los datos.

En suma, este trabajo busca contribuir al diseño de un modelo de comunicaciones digitales militarizadas, interoperables y seguras, que respondan a las exigencias actuales del campo de batalla moderno, donde la supremacía informacional se traduce en una ventaja estratégica tan decisiva como la potencia de fuego o la maniobra táctica.

Metodología

La presente investigación se desarrolló bajo un enfoque cualitativo, orientado a la descripción y análisis de prácticas de seguridad digital en las Fuerzas Militares de Colombia. Se adoptó un diseño de investigación documental y bibliográfica, sustentado en la revisión de manuales institucionales, literatura académica y artículos indexados que abordan la protección de datos en el ámbito de la defensa. Pudiendo manifestar que "La investigación cualitativa implica el uso y la recopilación estudiada de una variedad de materiales empíricos, estudio de caso, experiencia personal, introspección, historia de vida, entrevista, artefactos, **textos culturales y** producciones", (Denzin & Lincoln, 2011, p. 3)

A partir de la revisión, se identificaron diversas soluciones tecnológicas presentes en el mercado seleccionando dos para un análisis comparativo en profundidad, atendiendo a criterios de relevancia como la integridad, confidencialidad y la disponibilidad de la información en el contexto militar. cabe precisar que no se realizaron pruebas técnicas ni experimentales de software, dado que la investigación se centró exclusivamente en el estudio documental, normativo y académico, lo que permitió establecer conclusiones fundamentadas en evidencia literaria y normativa, más no en validaciones empíricas.

De esta manera. La metodología se alinea con un enfoque descriptivo y analítico, garantizando rigor en la identificación de brechas y posibles alternativas de solución frente al problema planteado, sin pretender agotar todas las opciones tecnológicas existentes. Es así que ""La investigación descriptiva tiene como objetivo describir algunas características fundamentales de conjuntos homogéneos de fenómenos, utilizando criterios sistemáticos que permiten establecer la estructura o el comportamiento de los fenómenos en estudio, proporcionando información sistemática y comparable con otras fuentes." (Guevara et al., 2020, p. 166)

1. Documentar medios de comunicación digital para tránsito de información sensible entre MDN, CGFM, Ejército, Armada, Fuerza Aeroespacial. (Buzón Ejército, Zimbra, Outlook), desde el ambiente ciber

En el mundo actual donde los dominios de la guerra han cambiado al incluir el dominio ciberespacial, las Fuerzas Militares a nivel mundial han puesto su lente en la forma cómo se comunica su información, cómo fluyen las órdenes y cómo la digitalización se convierte en una tecnología habilitante para prácticamente todos los seres humanos, con un carácter ampliamente decisivo en el resultado de la guerra, ya que permitir que un enemigo penetre las barreras digitales de la información sensible de un país puede traducirse en resultados catastróficos, es por ello que el Ministerio de Defensa Nacional de Colombia y sus instituciones adscritas deben contar con medios digitales de transmisión de información con altos niveles de seguridad con el fin de evitar que sus planes sean conocidos por enemigos

internos o externos. Siendo así detallaremos que medios se usan actualmente para mover información sensible y trataremos de determinar si estos son suficientes para suplir las necesidades de la defensa nacional. Siendo preocupante escuchar noticias como, "Militares colombianos destacados en zonas de conflicto están recurriendo a Whatsapp como medio principal de comunicación, compartiendo información sensible como estrategias, ubicaciones en tiempo real y reportes de combates." (Reyes, 2025)

1.1. Plataformas para el tránsito de información tipo E-MAIL y CHAT de las FFMM.

En el ámbito del intercambio de información las organizaciones estatales en especial aquellas involucradas en el ambiente de la seguridad y defensa, son llamadas a establecer controles cada vez más estrictos debido al nivel de confidencialidad de los datos que procesan y transfieren, actualmente estas organizaciones hacen amplio uso de documentos digitales que deben viajar de un lugar a otro cumpliendo con parámetros para mantener su confidencialidad, integridad y disponibilidad requiriendo sistemas especializados para tal fin, como lo manifiesta Landwehr podríamos considerar que los sistemas seguros son aquellos que a través de medidas de control establecidas no permiten la difusión no autorizada de la información, impiden su modificación así como la retención de la misma por personal sin las debidas credenciales. (Landwehr et al., 1984, p. 198).

En la actualidad el Ministerio de defensa Nacional y las Fuerzas Militares no cuentan con un sistema estándar que permita llevar a cabo la transmisión segura de información entre todas sus dependencias y unidades, lo que amplía la superficie de ataque para aquellas personas, organizaciones no estatales y estados que desean acceder a los datos privilegiados del sector defensa. Podemos observar que el Ejército Nacional usa mayormente el servicio de correo electrónico buzón ejército, la Armada Nacional el sistema de correo Zimbra y la Fuerza Aeroespacial Colombiana utiliza el sistema de correo Outlook con el fin de mantener comunicaciones digitales, así mismo a pesar de que está prohibido por las políticas de seguridad de la información el tránsito de información de tipo militar a través de plataformas como WhatsApp y Signal está ampliamente difundido mayormente por la accesibilidad de

dichas plataformas, su fácil uso y el nivel de penetración social con el que cuentan, dichas prohibiciones se evidencian en la Armada Nacional donde a través de la señal 20250025140767133/MDN-COGFM-COARC-SECAR-JEMAF-JOLAN-DITIC-OATIC-38.1 la cual prohíbe el uso de sistemas de mensajería no institucionales acuerdo el Manual de seguridad digital ARC T6.15-1 CAPITULO IV NUMERAL IV, así mismo en el Plan de Seguridad y Privacidad de la Información del Comando General de las Fuerzas Militares establece en su numeral 7 Seguridad de Comunicaciones, literal b Transferencias de información establece que "todo funcionario es responsable por proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de diferentes medios para el intercambio de información que pueden generar una divulgación o modificación no autorizada así mismo se deben usar canales cifrados" (Comando General de Las Fuerzas Militares, 2020, p. 35). Este tipo de sistemas tanto de chat como E-mail presentan ciertas vulnerabilidades pudiendo afirmar que, el correo no es un medio diseñado en su génesis para ser seguro contra ciberataques lo que lo hace un objetivo de interés para los actuales ciberatacantes que conocen estas debilidades, demostrado esto ya que para el 2021 el 83% de las empresas a nivel mundial han sufrido ataques de phishing. (Nunes, 2023, p. 221). Así mismo es de anotar que el MDN y las Fuerzas Militares carecen de una plataforma segura de tipo chat que esté protegida bajo protocolos de seguridad de nivel militar, atendiendo a que el surgimiento de aplicaciones de chat cifrado garantiza en gran medida una óptima seguridad y privacidad, destacando el almacenamiento cifrado de chat en bases de datos (Singh et al., 2024, p. 1).

Es innegable que las instituciones que hacen parte del Ministerio de Defensa Nacional deben contar con sistemas propios que les garanticen capacidad de respuesta ante incidentes y riesgos de ciberseguridad, así como un amplio control sobre los datos y el hardware para el almacenamiento de los mismos, la estandarización de un sistema único de comunicación para todas las unidades del Ministerio de Defensa Nacional facilitaría el control de la información, la interoperabilidad y la conjuntés, reduciendo el riesgo de que amenazas internas o externas puedan tener acceso a información privilegiada debido al uso de

plataformas comerciales inseguras motivado por la falta de medios dentro de la misma institución (chats de descarga libre).

> "Las fuerzas conjuntas requieren altos niveles de interoperabilidad y sistemas que son conceptualizados y diseñados con arquitecturas y estrategias de adquisición conjuntas. Este nivel de interoperabilidad reduce las barreras técnicas, doctrinales y culturales que limitan la capacidad de los CDTUC para alcanzar los objetivos". (Centro de Doctrina Conjunta de las Fuerzas Militares de Colombia - CEDCO, 2018, p. 27).

Como vimos anteriormente los correos electrónicos y los chats comerciales presentan debilidades que han ocasionado incidentes de ciberseguridad en las diferentes fuerzas y el Ministerio de Defensa Nacional, especialmente en cuanto a los email "al ser atacados y que se presenten Business Email Compromise (BEC) se pueden afectar las cadenas de suministro, así como generar un gran daño reputacional a las organizaciones" (Ogwo-Ude, 2023, p. 809).

Un ejemplo del peligro al cual se encuentran expuestas las fuerzas en sus e-mail podemos encontrarlo en la plataforma Zimbra de uso masivo en la Armada Nacional como se muestra a continuación.

> "Un equipo de investigación descubrió una campaña masiva de phishing activa desde al menos abril de 2023, destinada a recolectar credenciales de cuenta de usuarios de Zimbra Collaboration. La campaña se está difundiendo masivamente y sus objetivos son una variedad de pequeñas y medianas empresas, como también entidades gubernamentales." (Díaz Reyes, 2025, p. 9)

Por último, es importante mencionar que hay esfuerzos aislados en las diferentes fuerzas para

> proteger parcialmente la sectores de la información así la Fuerza Aeroespacial colombiana usa el sistema HERMES (sistema de gestión documental), Ejercito cuenta con el sistema 13X o HERMES (el cual es para unidades especializadas de inteligencia), y la Armada Nacional además del Zimbra para trámite de documentación de inteligencia cuenta con el sistema de correo THOT y Rocketchat. Pero es de mencionar que dichos sistemas no están irrigados al nivel de todas las

fuerzas, ni estandarizados para lograr una interoperabilidad generalizada que las asegure.

1.2. Tipos de plataformas de hardware (on-premise o tercerizadas) utilizadas para soportar el tránsito de información e-mail y chat del Ministerio de Defensa Nacional y las FFMM.

Después de haber identificado los medios en términos de software que son utilizados por el Ministerio de Defensa Nacional y sus FFMM es menester conocer cuál es la arquitectura de hardware utilizada para soportar mencionadas plataformas de software, la primera pregunta que debe asaltarnos es si ella está basada en servicios de hardware de terceros o es tecnología On-premise (tecnología propia controlada y administrada por las instituciones), el fin de lo anterior es poder entender que tanto control sobre los datos y los servicios poseen las instituciones.

Claramente al tercerizar servicios el cliente puede desmarcarse de actividades como el mantenimiento de servidores, su actualización en términos de software y hardware así como la garantía de funcionamiento desde el punto de vista del gasto energético etc. Lo anterior se considera una gran ventaja, pero así mismo ello nos lleva a plantear interrogantes como, ¿Quién tiene acceso a las instalaciones donde esta nuestra información?, ¿puede acceder una o varias personas?, ¿En qué lugar se encuentran las instalaciones y los servidores que contienen nuestra información y qué leyes aplican a mencionados datos?, ¿Nuestros datos pueden ser copiados debido a que personal no autorizado tiene acceso físico a los servidores, donde reside nuestra información? y muchas más que evidencian los riesgos a los cuales se expone una organización al tercerizar el manejo de su software y su hardware. Es de anotar que esta situación sucede tanto para los sistemas de buzón de correo como para los sistemas de mensajería instantánea tipo chat. Algunos de los riesgos relacionados pueden ser la dependencia de proveedores en términos de servicios lo que hace vulnerable la organización a una denegación de servicio, nuestro acceso siempre dependerá de una conexión a internet siendo susceptible a filtraciones, la pérdida o robo de nuestros datos sensibles, así mismo algunos servicios especiales podrían tardar en su despliegue al depender de las condiciones

de una red tercerizada, y como la información debe hacer tránsito a través de nodos hasta su destino final se hace vulnerable a interceptaciones. (Goyas & Vargas, 2014, pág. 2).

Ejemplo de lo anterior esta evidenciado en el contrato de menor cuantía 148 del Comando General de las Fuerzas Militares DIAF del año 2022, cuyo objeto era "contratar el servicio de nube híbrida, el cual incluye, migración, instalación, configuración y puesta en funcionamiento de los servidores del CGFM" (Comando General de las Fuerzas Militares, 2022, p. 1), generando preocupación debido a que la información del instrumento del poder nacional que tiene que ver con el campo militar podría verse comprometida al permitir que terceros tengan interacción con ella. Debemos entender que una nube híbrida es aquella donde se mezclan servicios de almacenamiento privados on premise con servicios de almacenamiento público con el fin de gestionar en ella todos nuestros datos, para el CGFM encontramos que "en la actualidad el Comando General de las Fuerzas militares cuenta con una estructura tecnológica basada en productos y servicios de nube Microsoft la cual apalanca procesos críticos de tecnologías de la información los cuales son utilizados por todos sus funcionarios" (Comando General de las Fuerzas Militares, 2022, p. 1). Permitiéndonos comprender como funciona la arquitectura para almacenamiento y tránsito de información al interior de las Fuerzas Militares.

2. Catalogar los medios digitales de aseguramiento de la información sensible con los que cuentan Ministerio de Defensa Nacional, CGFM, Ejercito Nacional, Armada de Colombia y Fuerza Aeroespacial.

Es importante tener claro que no solo se debe contar con medios seguros de transmisión de la información sino que también se debe contar con medios de cifrado que sirvan como segundo anillo de defensa ante las intrusiones de terceros interesados, que aseguren que la información es almacenada en los servidores de manera cifrada, viaja de manera cifrada y solo puede ser vista por la persona a quien es dirigida la misma, así como que las organizaciones cuentan con Forward secrecy siendo este el protocolo donde

> "Se añaden claves efímeras **(DHE)**, que permite llegar a un acuerdo de clave, pero sin utilizar los parámetros estáticos de los certificados. Se consigue Forward Secrecy porque se evitan los ataques basados en la obtención de certificados, y una tercera parte malintencionada no puede descifrar la información de los datos capturados anteriormente. Esta versión puede considerarse segura." (Barreda , 2022, p. 18)

garantizando que se usan claves de cifrado diferentes para cada mensaje enviado, a continuación, evaluaremos cual es el estado actual en este sentido y determinaremos si son suficientes o no las medidas tomadas para protegernos dentro de nuestras instituciones de defensa.

2.1. Medios de encriptación usados por el Ministerio de Defensa Nacional y las FFMM en sus aplicaciones de E-MAIL y CHAT.

Es muy importante para el público interesado por el tema de la seguridad en el transporte de información digital conocer los modelos en los cuales se basan las tecnologías E-mail, "podemos resumirlo explicando que hay dos tipos de formas para manejar este tipo de servicio, los modelos de clientes de servicios web y los modelos de cliente de e-mail" (Hernandez , 2020, p. 25) siendo su principal diferencia que para los primeros no se requiere instalar aplicaciones ya que los servicios se gestionan a través de un navegador web, mientras en el segundo se debe instalar una aplicación de manera local en el dispositivo para gestionar los mensajes. En el caso del MDN, CGFM y las FFMM, contamos con agentes de los dos tipos ya que por ejemplo Zimbra usado por la Armada Nacional se basa en el modelo cliente de e-mail mientras Outlook en la Fuerza Aérea se basa en un soporte de cliente web. Así mismo los anteriores sistemas cuentan con mecanismos para proteger la información con ciertas ventajas y desventajas, los principales protocolos son el protocolo TLS (cifrado en tránsito), cifrado en reposo y cifrado de extremo a extremo, algunos de los servicios mencionados no están directamente disponibles en las plataformas y algunos deben ser configurados e instalados haciendo que se presenten brechas que pueden ser utilizadas de

manera eventual por los ciberatacantes, para el caso del protocolo TLS podemos afirmar que "los ataques se pueden dividir en dos categorías: pasivos y activos. Los ataques pasivos implican espiar conexiones para conocer identidades y capacidades criptográficas de clientes y servidores. Los ataques activos, por otro lado, cambian los mensajes que se envían". (Polanía, 2024, p. 14). En el caso del cifrado en reposo es una opción que asumen las organizaciones con el fin de que los mensajes de correo electrónico se guarden de manera cifrada en el servidor con el fin de que no puedan ser extraídos de manera local por personal no autorizado, en el caso de Outlook este tipo de cifrado se hace por defecto en los servidores de Microsoft pero el inconveniente es que las claves de cifrado pertenecen a Microsoft y no son conocidas por el dueño de la información lo cual representa un riesgo potencial, sin embargo podemos afirmar que este sistema "protege la información almacenada en bases de datos o sistemas de archivos. Utilizando algoritmos como AES, los datos permanecen seguros incluso si el sistema es comprometido. Esto asegura que la información confidencial no pueda ser accesada o manipulada" (Martínez et al., 2023, p. 3).

En el caso del cifrado de extremo a extremo este no viene por defecto en los sistemas de correo electrónico en la mayoría de las veces por lo cual debe ser instalado y configurado por los diferentes administradores lo que impide crear un entorno seguro de manera a priori, este sistema de cifrado es considerado uno de los más seguros ya que ni el proveedor de servicio de correo ni el administrador conocen las claves ya que son únicas para el emisor y el receptor protegiendo ampliamente contra ciberataques enfocados en espionaje estatal y corporativo, "este sistema de comunicación debe asegurar que solo el emisor y receptor puedan leer lo que es enviado, y que ningún tercero; ni siquiera el servicio o aplicación que lo implementa lo puedan leer" (Belén, 2021, p. 7).

Así mismo existen esfuerzos con el fin de proteger la información considerada sensible a través del uso de programas licenciados como el PGP, el cual garantiza el movimiento encriptado de la información a través de los correos institucionales, pero estos son esfuerzos aislados debido a que no se encuentran masificados a nivel institucional y solo algunas unidades cuentan con ellos "La seguridad en las conversaciones con tus fuentes anónimas son tu responsabilidad. Aplicaciones como Signal, Wire, el uso de PGP, de Https Everywhere

y las SecureDrop, entre otras, ofrecen una fuerte encriptación" (Rivero Pérez, 2020, p. 38)., así mismo es un error común pensar que solamente la información operacional o de inteligencia es de interés para terceros interesados, debido a que para conocer el apresto operacional de una unidad los datos acerca de su parte de personal, parte de su armamento, guardias, órdenes del día, cantidad de vehículos etc. en ocasiones considerados de rutina son cruciales con el fin de establecer su nivel de alistamiento en caso de un conflicto. La criptografía de clave pública siempre permitirá a los usuarios un mayor acceso a los beneficios de la ciberseguridad, al utilizar un cifrado de extremo a extremo se asegura la integridad de los datos y se evita que estos sean alterados en su viaje hacia el destinatario final. Sin requerir terceros en el proceso, pudiendo enmarcar en este marco aplicaciones como Openpgp y S/MIME [4]. (Andrade , 2020, p. 17).

En el caso de las aplicaciones de mensajería instantánea comercial de descarga libre usadas de manera masiva en las fuerzas, es de especial preocupación como se expresó ya, que no son controladas por las instituciones debido a que carecen de exclusividad operacional y aunque ofrecen una presunta encriptación end to end, nunca es posible conocer cómo funciona la misma y que pasa con los mensajes una vez son presuntamente desencriptados en el equipo del usuario final, creando un halo de incertidumbre que puede abrir la puerta a vulnerabilidades explotables por terceros interesados.

2.2. Comparación de las capacidades y debilidades de los diferentes medios de encriptación utilizados por el MDN y las FFMM en sus aplicaciones E-MAIL y CHAT.

Característica	Outlook	Zimbra	PGP / OpenPGP	WhatsApp
Cifrado en tránsito (TLS)	✅ TLS/SSL	✅ TLS/SSL	❌ Manual	❌ Incluido
Cifrado extremo a extremo	S/MIME u OME	S/MIME / OpenPGP	✅ Completo	✅ Completo, pero sin

				posibilidad de verificación.
Forward secrecy	❌ No	❌ No	❌ No	✅ Sí
Usabilidad	Media	Media-baja	Baja	Muy alta
Seguridad	Alta si está bien configurado	Depende de su configuración	Criptografía sólida pero obsoleta	Presuntamente Muy sólida pero no es verificable
Deficiencias	Ciertos parámetros de seguridad no están establecidos por defecto	Ciertos parámetros de seguridad no están establecidos por defecto	No utiliza llaves efímeras, desbloqueo de información en bloque	metadatos expuestos

Fuente: elaboración propia

Para desarrollar este punto debemos empezar por el entendido de que todos los medios de encriptación y aseguramiento de la información presentan ventajas, desventajas y debilidades para lo cual evaluaremos cada uno de los casos. Inicialmente verificaremos el cifrado en tránsito TLS (Transfer layer security) que como ya se explicó anteriormente consiste en crear un túnel o ducto virtual desde el emisor hasta el receptor por donde los datos viajarán cifrados asegurando la capa de transporte de la información, si al usar un servicio de correo o aplicación vemos al inicio de su URL, https, la s (secure) del final nos indica que se hace uso del Protocolo TLS, en nuestro caso de estudio podemos observar qué los servicios de correo cuentan con este tipo de protección por defecto pero este ha sido vulnerado en varias ocasiones debido a una mala gestión de versiones abriendo puertas a ciberatacantes que los han aprovechado a través de técnicas como Man in the Middle el cual consiste en insertar un canal fraudulento entre las dos partes por parte del ciberatacante obteniendo la llave pública tanto del cliente como del servidor, imitando cada una de las partes, accediendo así a la información compartida a través de diferentes técnicas, ya que el cliente cree que está

enviando y recibiendo información al servidor (Polanía, 2024, p. 14), así mismo el uso de técnicas como el phishing hacen que el protocolo TLS pueda ser esquivado debido a que a través de un mensaje que puede contener malware de diferentes tipos camuflados en archivos aparentemente confiables el ciberatacante toma el control del equipo del usuario por lo cual el protocolo es burlado en su totalidad. "los casos más populares de esta amenaza se tienen a los ciberdelincuentes que se hacen pasar por alguna persona conocida o alguna entidad importante, desde la cual envían un mensaje de correo a la víctima objetivo" (Pardo, 2018, p. 4), es así que para nuestro caso podemos ver que los servicios de correo utilizados por las fuerzas poseen esta vulnerabilidad la cual puede ser explotada ampliando la superficie de ataque.

Teniendo en cuenta que no existe un servicio de mensajería instantánea institucional como ya se afirmó se tiende al uso de las plataformas comerciales las cuales manifiestan contener en sus modos de transmisión el protocolo anterior, pero esto no es verificable.

Característica	**Outlook (FAC)**	**Zimbra (ARMADA**	**Buzón Ejército**	**PGP / OpenPGP**	**WhatsApp /Signal**
Cifrado en tránsito (TLS)	✅ TLS/SSL	✅ TLS/SSL	✅TLS/SSL	❌ Manual	❌Incluido supuestamente pero no es posible verificarlo
Principal vulnerabilidad	Phishing e ingeniería social	Phishing e ingeniería social	Phishing e ingeniería social	Phishing e ingeniería social, en caso de una penetración al no tener fordwar	No autorizado por el mando militar, se desconocen sus políticas de manejo de la información

				security todos los mensajes pueden ser revelados.	y el destino y manejo de los mensajes. Phishing y spoofing

Ahora entraremos a analizar el protocolo S/MIME (Secure/Multipurpose Internet Mail Extensions) el cual hace parte de los protocolos de seguridad de los sistemas de correo electrónico usados por las fuerzas, consistente en colocar los mensajes dentro de contenedores blindados, con una clave privada que solamente podrá ser usada por el destinatario final, además de ello el mensaje va firmado de manera digital por el emisor del mismo para que el sistema receptor del mensaje pueda comprobar que el mensaje efectivamente viene de la fuente especificada. "S/MIME proporciona dos servicios de seguridad: Firmas digitales y Cifrado de mensajes, estos dos servicios son el núcleo de la seguridad de los mensajes basada en S/MIME. Todos los demás conceptos relacionados con la seguridad de los mensajes sirven de apoyo a estos dos servicios. Si bien todo el ámbito de la seguridad de los mensajes puede parecer complejo, estos dos servicios son la base de dicha seguridad" (Puetate, 2009, p. 82).

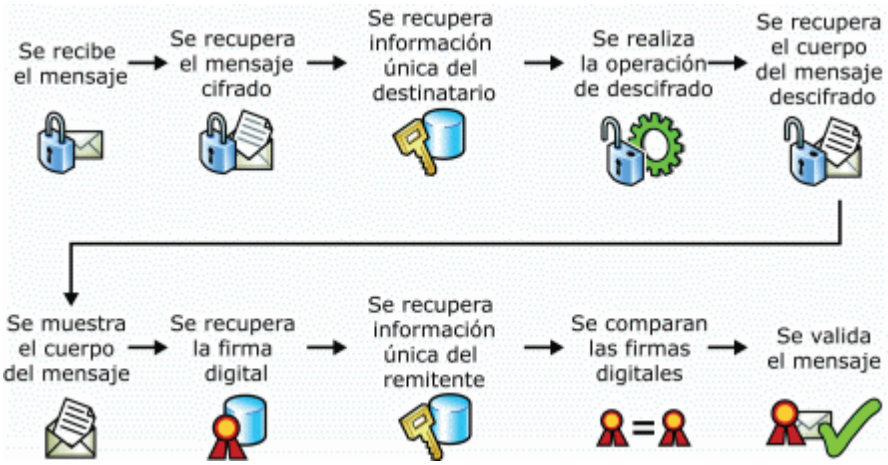


Figura 1: tomado de (Puetate, 2009, p. 92)

Ahora bien, continuando con el análisis podemos verificar cuales vulnerabilidades pueden afectar este protocolo. Si bien este protocolo puede protegernos contra ataques como MITM (man in the middle), también es vulnerable a riesgos como la ingeniería social y el phishing, debido a que estas técnicas usadas por los ciberatacantes buscan llegar al control de la maquina como tal abriendo puertas traseras en el sistema para monitorear de manera total las actividades de la organización, pudiendo afirmar que este sistema asegura el tránsito pero no protege contra ataques de malware embebidos en archivos tipo troyano, como comúnmente sucede (fotografías, archivos ofimáticos etc.).

Característica	**Outlook**	**Zimbra**	**PGP / OpenPGP**	**WhatsApp**
Cifrado extremo a extremo	S/MIME u OME	S/MIME / OpenPGP	✅ Completo	❌ presuntamente Completo
Seguridad/deficiencias	Alta si está bien configurado, pero solo protege en tránsito	Alta si está bien configurado, pero solo protege en tránsito	Criptografía sólida pero obsoleta	Aparentemente Muy sólida, metadatos expuestos, jamás recomendado para uso militar por desconocimiento en el manejo de política de datos.
Principal vulnerabilidad	Phishing e ingeniería social	Phishing e ingeniería social	Phishing e ingeniería social, en	No autorizado por el mando militar, se

			caso de una penetración al no tener fordwar security todos los mensajes pueden ser revelados.	desconocen sus políticas de manejo de la información y el destino y manejo de los mensajes

Fuente: elaboración propia

Otra de las deficiencias en los sistemas para intercambio de correo dentro de las Fuerzas Militares es que estos no tienen de manera intrínseca el sistema de seguridad Forward Secrecy (Seguridad hacia adelante), explicando este sistema de una manera simple podríamos decir que este genera para cada mensaje una llave pública y privada nueva, esto con el fin de que si las llaves de cualquier tipo caen en manos de un ciber atacante solamente podrá descifrar el mensaje para el cual fueron diseñadas las claves únicas, pero no podrá comprometer el resto de la información, un sistema que no cuente con mencionada tecnología se ve avocado a una vulnerabilidad crítica en caso de la pérdida de una de sus llaves, pues estas darán acceso a toda la información almacenada. Con este sistema se garantiza tanto seguridad hacia el frente como hacia atrás (mensajes antiguos y futuros) generando automáticamente un backward secrecy garantizando que las claves son útiles una sola vez y su pérdida no compromete ni los mensajes pasados ni los futuros, este tipo de llaves se consideran claves efímeras (ephemeral keys) (Khandpur, 2018, p. 34). Lo anterior minimiza el impacto de una obtención ilegal de claves de cifrado para mensajes de correo electrónico por parte de ciberatacantes haciendo más difícil su actividad ilegal, de igual manera, aunque este sistema es fuerte no va más allá de la capa de transporte de la información por ello, no hardeniza el sistema contra ataques enfocados en phishing, ingeniería social y malware de infección para la obtención de un control total de un equipo con el propósito de escalar privilegios.

Las debilidades vistas en caso de ser explotadas de manera exitosa por parte de un ciberatacante pueden permitir que este obtenga control total de un equipo y así leer los mensajes entrantes y salientes desde un correo institucional, controlar los sistemas, examinar carpetas, enviar mensajes falsos, espiar y escalar privilegios de manera vertical y lateral con el fin de acceder a información clasificada para sus intereses delictivos. Por lo cual se requiere de sistemas más cerrados que cierren aún más la brecha que representan.

3. Determinar mediante vigilancia tecnológica la disponibilidad y oferta de aplicaciones y tecnologías que puedan ser instaladas en el Ministerio de Defensa Nacional, CGFM y la FFMM para la transmisión segura de información entre los mismos.

Después de determinar el estado actual en el que se encuentran los sistemas del Ministerio de Defensa Nacional especialmente las FFMM y habiendo analizado sus vulnerabilidades es menester determinar opciones que permitan mitigar estas vulnerabilidades permitiendo una operación segura y que agreguen valor a la información desde el entendido que todo dato es relevante para el enemigo externo e interno ya que todo aquello que permita conocer nuestro nivel de alistamiento en cualquiera de las funciones de conducción de la guerra es de valor al momento de que nuestras fuerzas enfrenten una amenaza, "las funciones de conducción de la guerra son seis grupos básicos de capacidades y actividades relacionadas (mando y control, inteligencia, fuegos, movimiento y maniobra, protección y sostenimiento) que ayudan a los CDTUC a integrar, sincronizar y dirigir operaciones conjuntas." (Centro de Doctrina Conjunta de las Fuerzas Militares de Colombia - CEDCO-CGFM, 2018, p. 46)

3.1. Diferencias, ventajas y desventajas entre la arquitectura on-premise y arquitecturas tercerizadas para entidades que manejan información clasificada.

En el ecosistema digital actual los administradores y propietarios de los sistemas están cada vez más tentados a la utilización de servicios de computación en la nube sobre las tecnologías de arquitectura On-premise. Con el avance del internet y el crecimiento de

empresas como GOOGLE, AMAZON y WINDOWS, quienes descubrieron que podían ofertar superficie de almacenamiento, procesamiento y actualización a empresas de cualquier tamaño incluyeron esta línea de negocio dentro de sus portafolios dando origen a lo que hoy en día llamamos cloud computing o coloquialmente como la nube.

Para ser concretos empezaremos por establecer la diferencia entre las tecnologías On premise y la tecnología de la nube, en si su diferencia no es compleja, la tecnología On-premise se basa en la soberanía del dato y su gobierno por parte de la organización, aunque ello implique que la matriz de costos del negocio aumente por temas de actualización de hardware y software, mientras que la tecnología de la nube se basa en el manejo federado de los datos otorgando ciertos privilegios a un tercero que generalmente es dueño de la tecnología de hardware y software, reduciendo los costos operacionales en actualizaciones pero aumentando los riesgos de seguridad al tener que hacer concesiones de control como permitir al tercero escoger en qué lugar del mundo se guardan los datos y los sistemas de seguridad física para proteger las instalaciones donde residen los mismos, así como la gestión de claves de administración etc.

> "La atracción de la computación en la nube no se limita únicamente a las grandes empresas, sino que también los emprendedores, las startups, las medianas y pequeñas empresas se beneficiarían enormemente, ya que tendrán una nueva alternativa y oportunidades que antes no estaban a su alcance, lo cual les permitiría ahorrar millones de dólares. Con la computación en la nube, podrán optar por alquilar únicamente la potencia de cómputo, el espacio de almacenamiento y la capacidad de comunicación necesarios, proporcionados por un gran proveedor de servicios en la nube que cuenta con todos estos activos conectados a Internet." (Bisong & Rahman, 2001, p. 33).

Es innegable que la computación en la nube presenta grandes ventajas para las empresas, pero si analizamos estas desde el punto de vista de las instituciones de seguridad y defensa se avizoran en el horizonte riesgos que pueden comprometer el desempeño de las mismas y la defensa de la nación, podríamos en esta línea de análisis listar riesgos como:

- **Falta o nula accesibilidad de usuario:** si durante el proceso de contratación las empresas o instituciones no establecen líneas claras acerca de temas como la administración privilegiada de los datos, controles exclusivos de acceso a la información exigiendo que no deben ser conocidos por el prestador del servicio, así como el cifrado de los datos en los repositorios a través de sistemas no conocidos por el prestador, se puede presentar un alto riesgo de denegaciones de servicio e intrusiones abusivas por parte de personal no autorizado.

- **Aplicación Normativa (auditorías):** si no se establecen de manera clara en la contratación puede presentarse el riesgo de que el prestador de servicios no esté dispuesto a recibir auditorías de campo por parte de la institución que toma el servicio, estas auditorías tendrían como fin el verificar físicamente la soberanía y la residencia de los datos, lo cual es complejo debido a que no es común que las empresas de computación en la nube autoricen este tipo de interventorías de seguridad y no se considera seguro aquello que no se puede revisar.

- **Residencia de los datos (ubicación):** debe ser exigible al proveedor de servicios que almacene y procese los datos en jurisdicciones territoriales específicas y que estos no puedan ser copiados o movidos territorialmente sin consentimiento de la institución tomadora del servicio, ya que como es bien sabido los datos se apegan a las leyes del territorio en el cual son almacenados y no es un riesgo asumible por parte de las instituciones de seguridad perder la soberanía sobre sus datos, pero este tipo de exigencias pueden ser difíciles debido a que los proveedores de servicios en la nube generalmente creen tener cierta autoridad sobre todas estas cuestiones considerando que no son de incumbencia del tomador de servicios

- **Segregación de los datos:** es común que las empresas de servicios en la nube almacenen grandes volúmenes de datos de sus clientes en diferentes lugares y

servidores, es importante que el tomador del servicio sepa cómo fueron segregados los datos y que tipo de cifrado se maneja para ello, esto representa un riesgo alto de impacto debido a que no es posible mantener la integridad de la matriz de información, y en caso de requerirse la devolución de los datos de manera rápida esto tomará una cantidad de tiempo considerable.

- **Programa de resiliencia ante desastres**: se debe exigir al proveedor de servicios en la nube cómo se protegerán los datos en el momento de presentarse un desastre y cuál es el plan de resiliencia verificable por parte del prestador del servicio y la ubicación de los backups, así como la posibilidad de verificación de estos últimos.

Analizando los anteriores riesgos podemos manifestar que para el Ministerio de Defensa Nacional y sus instituciones adscritas estos riesgos pueden ser de un alto nivel y no serían asumibles debido al tipo de información de inteligencia y operacional que se maneja por ello no se debe tener un alto apetito al riesgo en esta situación y es notorio que las desventajas podrían superar a las ventajas por parte de la computación en la nube frente a la soberanía y gobernanza de los datos que ofrece la tecnología On-premise.

"Es de suma importancia proteger la información almacenada en la "nube", sabiendo que los sistemas en red están expuestos a diversos tipos de amenazas. Un ejemplo de esto es la **falta de conectividad**, dado que toda la información crítica se encuentra alojada en un servidor web. Teniendo en cuenta la gran cantidad de datos que residen en la computación en la nube, esta se convierte en un blanco para los ataques, comprometiendo los **principios fundamentales de la seguridad de la información: integridad, confidencialidad y disponibilidad**." (Pianoski et al., 2018, p. 70)

Aspecto	On-premise	Cloud (tercerizada)
Control de los datos	**Ventaja:** Control absoluto de la información y claves de acceso. **Desventaja:** Mayor responsabilidad interna de gestión y seguridad.	**Ventaja:** Delegación de parte de la gestión en expertos del proveedor. **Desventaja:** Pérdida de soberanía y posible acceso indebido por terceros.
Residencia de la información	**Ventaja:** Datos bajo jurisdicción nacional y normativas propias. **Desventaja:** Limitaciones en redundancia geográfica.	**Ventaja:** Posibilidad de redundancia en múltiples países. **Desventaja:** Riesgo de sometimiento a leyes extranjeras.
Seguridad física	**Ventaja:** La entidad define y controla accesos y custodia. **Desventaja:** Altos costos de infraestructura física.	**Ventaja:** Centros de datos del proveedor con altos estándares de seguridad física certificados. **Desventaja:** La entidad no controla directamente las instalaciones.

Escalabilidad	**Ventaja:** Control del crecimiento según presupuesto. **Desventaja:** Escalabilidad lenta y costosa (compra e instalación de hardware).	**Ventaja:** Escalabilidad inmediata y flexible (bajo demanda). **Desventaja:** Dependencia completa del proveedor para ampliar capacidad.
Costos iniciales y operación	**Ventaja:** Inversión única en hardware propio. **Desventaja:** Altos costos iniciales y de mantenimiento (CAPEX).	**Ventaja:** Costos iniciales bajos, modelo de pago por uso (OPEX). **Desventaja:** Posibles costos crecientes a largo plazo si el uso es intensivo.
Auditorías y cumplimiento normativo	**Ventaja:** La institución puede auditar sin restricciones. **Desventaja:** Requiere más recursos internos para auditoría.	**Ventaja:** Algunos proveedores cumplen normas internacionales de seguridad (ISO 27001, FedRAMP, etc.). **Desventaja:** Pocas veces permiten auditorías físicas;

		confianza obligada en certificaciones del proveedor.
Disponibilidad y resiliencia	**Ventaja:** Depende de planes internos, control total sobre backups. **Desventaja:** Menor redundancia si no hay inversión suficiente en continuidad.	**Ventaja:** Alta disponibilidad gracias a redundancia global y SLA (Acuerdos de Nivel de Servicio). **Desventaja:** Dependencia de conectividad a internet y del plan de resiliencia del proveedor.
Segregación y recuperación de datos	**Ventaja:** Datos gestionados y segregados de acuerdo con las políticas internas. **Desventaja:** Recuperación lenta si no se tienen planes de contingencia bien implementados.	**Ventaja:** Recuperación de datos rápida en entornos preparados. **Desventaja:** Riesgo de mezcla de datos con otros clientes y limitaciones de segregación.
Riesgos estratégicos	**Ventaja:** Minimiza la exposición a	**Ventaja:** Acceso a innovación

	espionaje y extraterritorialidad. **Desventaja:** Riesgo de obsolescencia tecnológica si no se actualiza.	tecnológica continua (IA, Big Data, etc.). **Desventaja:** Mayor exposición a espionaje, ciberataques y dependencia del proveedor.

Fuente: elaboración propia

3.2. Aplicaciones comerciales que pueden ser adaptadas para uso privado por el MDN y las FFMM en sus aplicaciones de E-MAIL y CHAT.

En el mercado actual existen opciones para el intercambio de información digital con mejoras con el fin de fortalecer y hardenizar las vulnerabilidades críticas en el proceso que presentan tanto los correos electrónicos como las aplicaciones de mensajería instantánea para instituciones con requerimientos especiales de seguridad. Dos de las mejores opciones que se encuentran en el mercado son Rocketchat y Mattermost, inicialmente empezaremos por explicar que son estas aplicaciones y porque se consideran útiles en el proceso de hardenizar la estructura de intercambio de información. Estas aplicaciones hibridan las funciones del correo electrónico y una aplicación de mensajería instantánea similar a Whatsapp o Signal, pero permitiendo que esta sea manejada de manera on-premise (control total por parte de la organización), así mismo estas aplicaciones permiten configurar los filtros de seguridad agregando valores que no son posibles dentro de los ambientes de correo y chat más conocidos de manera comercial.

> "Rocket.Chat Es una plataforma de comunicaciones diseñada con un profundo conocimiento de la necesidad de sus usuarios de contar con sólidos controles de seguridad, protección de datos y privacidad. Ofrece un conjunto completo de

funciones de seguridad y configuraciones personalizables para proteger los espacios de trabajo contra posibles amenazas. Estos controles de seguridad permiten a los administradores optimizar la plataforma para cumplir con los requisitos específicos de la organización, garantizando la protección de la información confidencial" (Rocketchat, 2025).

Algunas de las características especiales y configurables para el caso de Rocketchat son:

- Content Security Policy (CSP) esta funcionalidad de seguridad permite a los administradores controlar, limitar y neutralizar la carga de scripts que contengan malwares permitiendo solo la ejecución de scripts altamente confiables.

- CORS (Intercambio de recursos de origen cruzado), esto hace referencia a evitar que desde la aplicación instalada on-premise se intercambie información con sitios externos manteniendo aislado el sistema y cerrando las puertas a ciberatacantes que hacen uso de sitios web maliciosos como trampa para atraer incautos y penetrar sistemas de alto valor.

- TLS (transfer layer security) o cifrado de datos en tránsito, si bien rocketchat no cuenta con este cifrado de manera automática se apoya en proxys que pueden ser configurados por el administrador del sistema que realiza la actividad de encriptar la información en tránsito y de esta forma protegerla, así como también identificar a cada usuario evitando que sujetos maliciosos ingresen al sistema y puedan realizar ataques de denegación de servicios.

- DLP (Data loss Prevent) o prevención de pérdida de datos "La prevención de pérdida de datos (DLP) es un mecanismo de seguridad diseñado para garantizar que los datos confidenciales no se compartan, utilicen indebidamente, se pierdan o sean accedidos por personas no autorizadas". (Rocketchat, 2025), esta es otra aplicación descargable la cual complementa las funciones de seguridad de Rocketchat que aumenta aún más la seguridad evitando que los usuarios compartan información confidencial

bloqueando este tipo de mensajes a través de su DLP. Un ejemplo de ello es que si el usuario intenta enviar contraseñas a través del sistema Rocketchat el DLP prohibirá la operación y bloqueará el mensaje.

- Metadatos EXIF, este sistema permite que el administrador active la funcionalidad de seguridad de eliminar los metadatos de los archivos como la geolocalización previniendo ciberataques para seguimiento de posiciones. "Hay que tener en cuenta que las imágenes suelen guardar metadatos (EXIF), que incluyen información valiosa como la localización GPS, fecha de captura, y otros datos que pueden probar la presencia del dispositivo en una localización y momento del tiempo." (Gonzales Fernandez, 2018, p. 69).

- Carga de Archivos esta funcionalidad permite al administrador del sistema configurar cómo será la carga de archivos, pudiendo restringir, tamaños, tipos de archivos, limitar el acceso a los archivos gestionando que solo los usuarios autorizados puedan verificarlos y modificarlos lo cual robustece la ciberseguridad y dificulta acciones intrusivas al sistema por medio del uso de software embebido con malwares ocultos en archivos aparentemente inofensivos.

- Así mismo el sistema le permite al administrador la gestión de política de contraseñas según las necesidades de la organización pudiendo establecer el número de caracteres, tipos de caracteres, lo cual protege la organización y dificulta los procesos de secuestro de sesión o hijaking, el cual se puede definir como "tentativa de tomar una sesión ya activa entre dos equipos. Es diferente del IPSPOOFING en el cual se suplanta una dirección IP o una dirección MAC de otro equipo" (Verdesoto Gaibor, 2007, p. 52).

- Esta aplicación cuenta con una plataforma configurable que aplica los principios de mínimo privilegio, configurando las capacidades de los usuarios dentro de sus perfiles evitando que accedan a funciones administrativas no autorizadas, limitando la

superficie de ataque a un espacio cada vez más pequeño previniendo escalamientos en caso de un ciberataque.

- Es importante también mencionar que esta aplicación entrega la posibilidad de generar un doble factor de autenticación al momento de ingresar a sesiones lo cual previene y dificulta aún más que los ciberatacantes puedan tener un acceso completo al sistema en caso de que este se vea comprometido.

  "La autenticación de dos factores proporciona una capa secundaria de seguridad que hace que sea más difícil para los piratas informáticos acceder a los dispositivos y las cuentas en línea de una persona para robar información personal. Con la autenticación de dos factores habilitada, incluso si el pirata informático conoce la contraseña de su víctima, la autenticación seguirá fallando y evitará el acceso no autorizado" (Reyes Riveros et al., 2023).

- Por ultimo por razones de seguridad es muy importante también dar a conocer que el sistema ROCKET CHAT exige al usuario antes de ingresar a la aplicación loggearse con un usuario y contraseña como ya se mencionó, y también le permite cerrar la sesión en caso de que tenga que realizar tránsitos por lugares donde pueda ser abordado por la amenaza y su terminal celular o pc pueda ser susceptible de una revisión, incluso podría desinstalar la aplicación y su información no se perdería pues puede abrir la sesión en cualquier momento, protegiendo así la vida del usuario final. Asi mismo Se pueden activar configuraciones de seguridad adicionales como auto-logout por inactividad, cifrado local de caché, y bloqueo por PIN o biometría**.**

Analizaremos un segundo sistema llamado Mattermost que al igual que Rocketchat nace debido a las necesidades de asegurar los sistemas de comunicación digital ante las crecientes amenazas cibernéticas para las instituciones del ámbito de la seguridad y la defensa que requieren una amplia soberanía digital sobre sus datos entendiendo esta como "una forma de referirse a una esfera digital ordenada, basada en valores, regulada y, por lo tanto, razonable

y segura" (Phole & Thorsten, 2022, p. 12) muy vinculada con la independencia tecnológica, la resiliencia digital y la autonomía operacional.

Es de destacar que también cumple con las condiciones de hibridar los servicios de transmisión de información en correo y los sistemas de mensajería instantánea, de igual manera este sistema cuenta con altos estándares de seguridad que no son posibles de desplegar en los anteriores además que puede ser desplegado en la modalidad On-premise.

> "Mattermost es una plataforma de colaboración de código abierto diseñada para equipos que operan en ambientes donde la seguridad, la soberanía de datos y el control operativo son prioritarios. Ofrece un conjunto completo de controles de seguridad, configuraciones avanzadas y capacidades de integración que permiten a las organizaciones proteger la confidencialidad, integridad y disponibilidad de su información crítica." (Mattermost, 2025)

Así mismo Mattermost además de contar con las mismas funcionalidades descritas anteriormente para Rocketchat también cuenta con funcionalidades resaltables como.

- admite cifrado en tránsito
- Admite cifrado en reposo
- Fortalecimiento de la red y la seguridad
- Monitoreo del sistema
- Pruebas de penetración anuales
- Revisiones de código fuente manuales y automatizadas
- Actualizaciones de seguridad periódicas entregadas a la comunidad antes de su divulgación pública
- Compromiso continuo con los principios del RGPD y la CCPA lo cual hace referencia a que según el Reglamento General de Protección de Datos de la Unión Europea (RGPD) las organizaciones están obligadas a reforzar el consentimiento explícito de

los usuarios para la recopilación de datos personales. Además, se reconocen derechos fundamentales como el acceso, la rectificación, la cancelación, la oposición, el derecho al olvido y la portabilidad de los datos, garantizando mayor control sobre la información personal (Bahillo Ortego, 2018, p. 16), y la CCPA la Ley de Privacidad del Consumidor de California (CCPA) la cual destaca la necesidad de mayor transparencia, opciones de privacidad más amplias y consideran que la CCPA debería ser tan aplicable como lo es el RGPD en Europa. (Baik, 2020)

- Autoridad de numeración CVE (CNA)
- Programa de recompensas por errores y política de divulgación responsable.

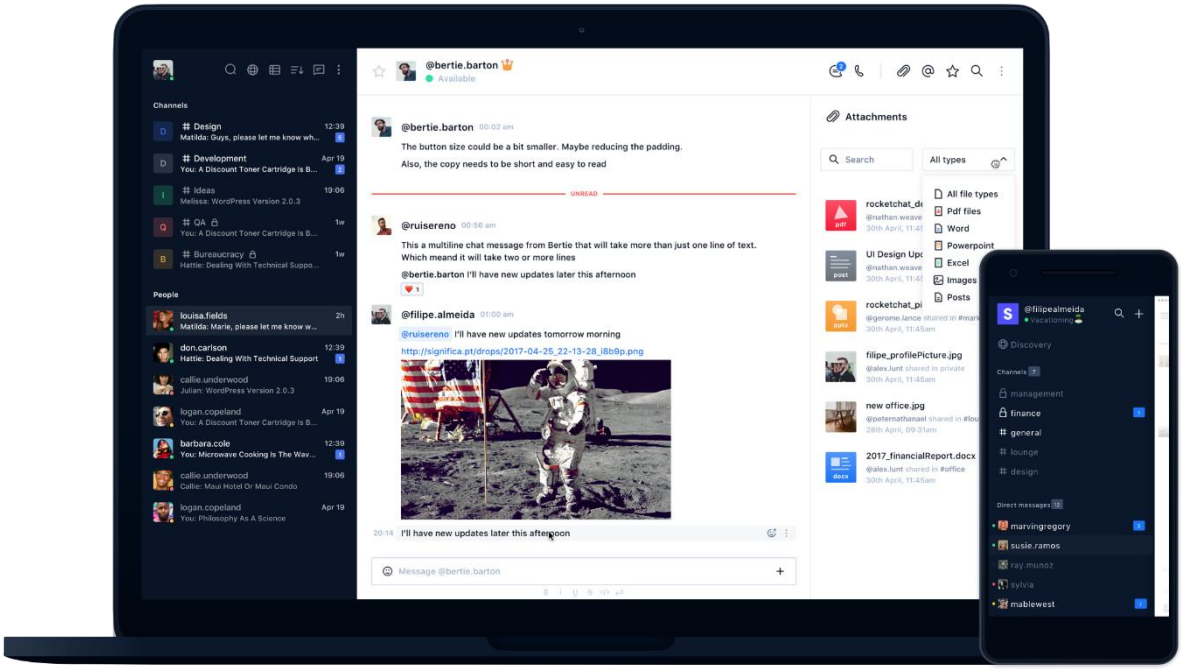
Por último y con el fin de soportar de manera clara el por qué se enfoca el análisis en estas dos opciones es que su selección se sustenta en evidencia documental verificable. En el caso e Rocket chat posee certificaciones internacionales como ISO/IEC 27001(International Organization for Standardization / International Electrotechnical Commission, norma de gestión de seguridad de la información) y auditorias SOC 2 (System and organization Controls 2, control de seguridad y confidencialidad) lo que confirma su idoneidad para uso en entornos críticos. Mattermost, por su parte, además de ofrecer despliegue on-premise con controles de seguridad avanzados, ha sido adoptado por la Fuerza Aérea de los Estados Unidos en el *618th Air Operations Center* lo que evidencia su madurez tecnológica y confiabilidad en operaciones militares.

Proponer los sistemas que con tecnología digital permiten la protección de la información y una alternativa de aplicación de intercambio de datos para la comunicación, del MDN, CGFM, Ejército, Armada y Fuerza Aeroespacial para una transmisión de información segura entre los mismos

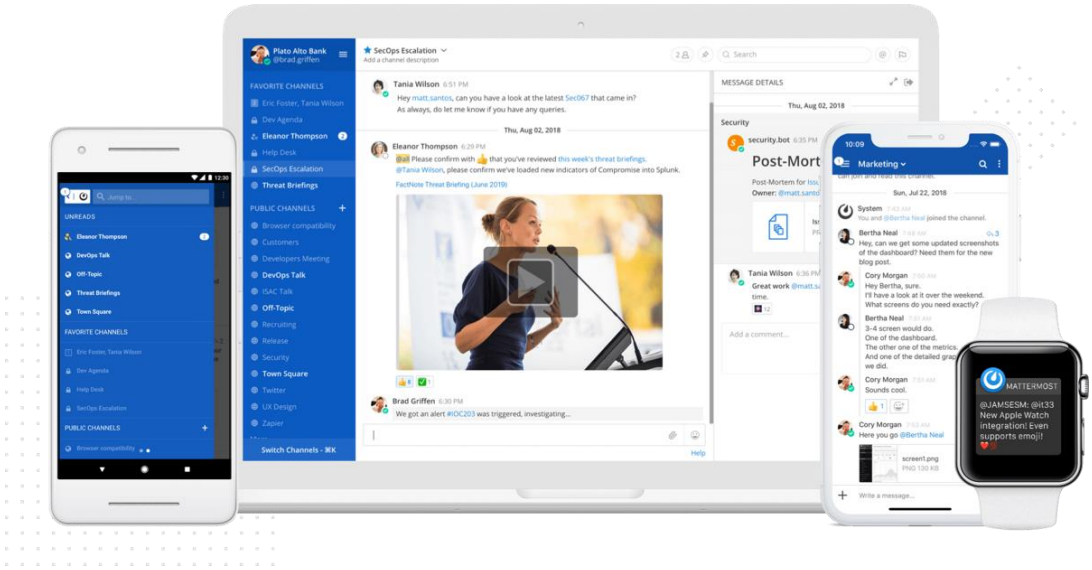
4. Proponer los sistemas que con tecnología digital permiten la protección de la información en el intercambio de datos para la comunicación entre MDN, CGFM, Ejército, Armada y Fuerza Aeroespacial para la transmisión de datos entre los mismos.

En el marco de las operaciones militares modernas, donde la guerra de información, la ciberdefensa y las operaciones multidominio (terrestre, marítimo, aéreo, ciberespacio y espacial) exigen garantizar la **supervivencia de la información**, la capacidad de mantener las comunicaciones seguras, soberanas y resistentes frente a amenazas cibernéticas es un elemento crítico para la conducción de la guerra.

Ambas plataformas **Rocket.Chat** y **Mattermost** representan soluciones tácticas y estratégicas de comunicaciones internas seguras, capaces de reemplazar y superar en seguridad a los canales tradicionales como correo electrónico o aplicaciones comerciales (WhatsApp, Telegram, Signal), las cuales representan vulnerabilidades operativas inaceptables en un entorno militar.



Fuente: página oficial de Rocket chat



Fuente: página oficial de Mattermost

4.1 Análisis comparativo entre las tecnologías actuales de que disponen el MDN y las FFMM en sus entornos de E-MAIL y CHAT y las alternativas que ofrece el mercado con el fin de determinar la mejor opción en términos de seguridad y rendimiento.

Criterios Operacionales de Evaluación Militar

- Soberanía de la Información.
- Ciberresiliencia ante amenazas híbridas y APT.
- Control total del entorno operativo (infraestructura, usuarios, datos).
- Capacidad de hardening y defensa perimetral interna.
- Escalabilidad para estructuras desde una compañía hasta un teatro operacional.
- Capacidad de sostener operaciones en ambientes degradados, contestados o denegados.
- Resistencia frente a inteligencia de señales (SIGINT) e inteligencia de fuentes abiertas (OSINT).

Comparativo Técnico-Militar Rocket.Chat vs. Mattermost

Parámetro Militar	Rocket.Chat	Mattermost
Soberanía de Datos	100% On-Premise. Control total del entorno físico y lógico.	100% On-Premise. Con mayor madurez en interoperabilidad con sistemas militares y mayor capacidad de integración con estándares de ciberseguridad de defensa.
Arquitectura Operacional	Microservicios escalables. Despliegue flexible (bare metal, contenedores, nube privada).	Arquitectura distribuida reforzada. Despliegue nativo en Kubernetes, Docker o infraestructura física. Mejor adaptado para operaciones de alta disponibilidad y continuidad operacional en escenarios militares.
Modelo de Seguridad	Fuerte. CSP, CORS, TLS por proxy, DLP externo. Protección avanzada con controles configurables por el administrador.	Modelo **Zero Trust nativo.** Seguridad desde el diseño. TLS obligatorio, DLP vía API, cifrado en reposo y en tránsito, eliminación de EXIF, RBAC granular a nivel de organización, equipo y canal.
Resistencia a SIGINT y OSINT	Moderada. Protección contra metadatos EXIF y cifrado en tránsito.	Alta. Eliminación avanzada de metadatos, cifrado completo, logs auditables, control de trazabilidad, protección contra geolocalización y fingerprinting digital, ideal para operaciones especiales y ambientes no permisivos.

Gestión de Crisis (Compromiso Físico)	Logout manual, borrado local posible, datos seguros en servidor.	Logout manual + logout remoto + cifrado de caché + bloqueo por PIN o biometría. Resistente a escenarios donde el operador es capturado o su dispositivo confiscado.
Prevención de Escalada (Hardening Interno)	Políticas de contraseñas robustas, RBAC por perfiles, MFA opcional.	Hardening extremo. MFA obligatorio, RBAC multi-nivel (organización, equipo, canal, función), restricciones IP, API Gateway con autenticación y limitación, Zero Trust, segmentación de tráfico y control total de superficie de ataque.
Integración con Infraestructura Militar	LDAP, SAML, OAuth. Buen nivel de integración, pero requiere configuraciones adicionales para estándares militares avanzados.	Integración avanzada con LDAP, SAML, OpenID, SIEM, EDR, XDR, IAM militar, con APIs abiertas para interconectar con plataformas C4ISR, sistemas de mando y control (C2) y centros de operaciones cibernéticas.
Capacidad de Escalabilidad Operacional	Alta. Hasta decenas de miles de usuarios.	Muy alta. Escalabilidad nativa en clústeres Kubernetes, balanceo de carga, alta disponibilidad. Capaz de escalar desde una unidad táctica hasta un comando conjunto.
Control de Archivos y Riesgos de Malware	Control de tipos y tamaños, carga segura, eliminación de EXIF básica.	Control avanzado de archivos, sandboxing externo posible, escaneo antivirus integrado, restricción extrema de formatos, eliminación

		automática de metadatos, control sobre retención y acceso.
Logs, Auditoría y Forense	Logs básicos y exportables, necesita integración manual con SIEM para auditoría forense completa.	Logs detallados, exportables en tiempo real, trazabilidad total. Integración con SIEMs de nivel militar (Splunk, QRadar, Elastic), con capacidad de soporte para operaciones de contrainteligencia y análisis de intrusiones.
Supervivencia Operacional	Alta. Operación asegurada en infraestructura propia, independiente de la nube pública.	Muy alta. Pensado desde el diseño para ambientes degradados, contestados, aislados o denegados. Puede operar en entornos sin acceso a internet o bajo redes militares aisladas, con alta resiliencia ante ciberataques y ataques físicos.

Fuente: elaboración propia

Ventajas Operacionales en Ambiente Militar

Rocket.Chat	Mattermost
• Más sencillo de desplegar. • Interfaz intuitiva. • Buen balance entre seguridad y simplicidad.	• Seguridad de nivel militar. • Mayor hardening. • Arquitectura Zero Trust. • Más integración con SIEM y sistemas C4ISR. • Operación robusta en escenarios degradados o aislados.

Fuente: Elaboración propia

Conclusión Militar y Recomendación Operativa

- **Rocket.Chat** es una excelente solución para niveles tácticos, brigadas, comandos intermedios o dependencias administrativas, donde se requiere una plataforma segura, flexible, fácil de implementar y con niveles de seguridad elevados, pero con menor complejidad técnica.
- **Mattermost**, en cambio, es la plataforma recomendada para ambientes de operaciones críticas, comandos conjuntos, centros de ciberdefensa, fuerzas especiales, unidades de inteligencia y operaciones multidominio, donde la prioridad absoluta es la supervivencia de la información, la ciberresiliencia avanzada, el control total sobre datos y la resistencia operacional ante amenazas híbridas complejas.

COMPARACIÓN CON LOS MEDIOS USADOS ACTUALMENTE

Cualitativo	Valor numérico (sugerido) = P
Muy baja	1
Baja	2
Media	3
Alta	4
Muy alta	5

CRITERIO EVALUADO	PESO (%)	TECNOLOGÍAS ACTUALES (OUTLOOK, ZIMBRA, ETC.)	P	%	ROCKET.CHAT	P	%	MATTERMOST	P	%
1. Soberanía de la Información	13%	Bajo. Datos alojados en nubes públicas como	2	**0,26**	Alta. 100% On-premise.	4	**0,52**	Muy Alta. 100% On-premise con arquitectura	5	**0,65**

		Microsoft. O nubes híbridas						reforzada y control granular.		
2. Ciberresiliencia ante amenazas APT (amenazas avanzadas persistentes) e híbridas	13%	Media. Falta de Forward Secrecy, cifrados incompletos, políticas débiles.	3	**0,39**	Alta. CSP (cloud services provider), DLP (data loss prevent), hardening.	4	**0,52**	Muy Alta. Zero Trust, MFA obligatorio, cifrado en tránsito y reposo, segmentación de red.	5	**0,65**
3. Control Operativo Total (infraestructura, datos, usuarios)	8%	Bajo. Tercerización y dependencia tecnológica.	2	**0,16**	Alta. Admin local, control granular.	4	**0,32**	Muy Alta. Control operativo multicapas (infraestructura, canal, equipo, rol).	5	**0,4**
4. Hardening y Defensa Perimetral Interna	8%	Bajo. Configuraciones débiles, sin monitoreo SIEM nativo (gestión de información y eventos de seguridad).	2	**0,16**	Medio. MFA opcional, filtros de archivos. (autenticación multifactor)	3	**0,24**	Alta. RBAC (Control de Acceso Basado en Roles) detallado, integración SIEM (gestión de información y eventos de seguridad), sandboxing, Zero Trust.	4	**0,32**
5. Escalabilidad Operacional (desde compañía hasta teatro de operaciones)	8%	Limitada. Pensadas para entornos civiles y administrativos.	2	**0,16**	Alta. Escalable hasta decenas de miles de usuarios.	4	**0,32**	Muy Alta. Escalable en Kubernetes, Docker, balanceo de carga.	5	**0,4**
6. Operatividad en Ambientes Degradados o Denegados	8%	Muy Baja. Requiere conexión externa constante.	1	**0,08**	Alta. Puede operar localmente.	4	**0,32**	Muy Alta. Diseñado para redes aisladas, militares, sin internet.	5	**0,4**
7. Resistencia a SIGINT / OSINT (anonimato, metadatos, trazabilidad)	7%	Muy baja. EXIF no eliminado, metadatos accesibles.	1	**0,07**	Media. Eliminación EXIF básica.	3	**0,21**	Alta. Eliminación avanzada, control de fingerprinting, logs auditables.	4	**0,28**
8. Gestión de Crisis (pérdida de	7%	Muy Baja. Sin logout remoto, sin cifrado de caché.	1	**0,07**	Media-Alta. Logout manual,	3	**0,21**	Alta. Logout remoto, cifrado	4	**0,28**

dispositivo, infiltración física)					cifrado en servidor. Logout automatico programable			local, bloqueo por biometría/PIN.		
9. Auditoría y Capacidad Forense	10%	Baja. Requiere herramientas externas.	2	**0,2**	Media. Logs básicos exportables.	3	**0,3**	Alta. SIEM (gestión de información y eventos de seguridad) integrado, trazabilidad completa.	4	**0,4**
10. Interoperabilidad con Infraestructura Militar (LDAP Protocolo Ligero de Acceso a Directorios), C2, SIEM, etc.)	10%	Limitada. Integración parcial con Active Directory.	2	**0,2**	Media. LDAP, OAuth, SAML.	3	**0,3**	Alta. APIs abiertas, integración nativa con C4ISR, SIEMs, IAM militar.	4	**0,4**
11. COSTOS	8%	**COSTO MEDIO**: pagado vía licencias existentes. Vulnerabilidades elevadas.	3	**0,24**	**COSTO MEDIO**: implementación on-premise, código abierto, sin licencias por usuario.	3	**0,24**	**Costo alto inicial**: despliegue complejo, requiere infraestructura robusta y equipo técnico especializado, pero sin licencias por usuario.	4	**0,32**
TOTAL	**100%**		**1,99**			**3,5**			**4,5**	

Fuente: elaboración propia

Recomendación Estratégica Militar

Para un **Teatro de Operaciones Conjunto**, un comando de fuerzas especiales, unidades de inteligencia, o un Cibercomando Militar Nacional, la recomendación táctica es:

- Si se cuenta con el presupuesto implementar **Mattermost** como plataforma base para comunicaciones críticas, operaciones clandestinas, mando y control en ambientes secretos, y manejo de información clasificada.
- Mantener e implementar **RocketChat** como solución inicial para comunicaciones operacionales, tácticas, administrativas, soporte, logística o ambientes donde se priorice facilidad de uso y un nivel aceptable de hardening pero que sus costos de adquisición sean esbeltos ideal para el inicio de una hardenización estable en organizaciones militares.
- A través de lo documentado se observa que las ingeniería social y el phishing especialmente, se perfilan como la amenaza más persistente para lo cual estos sistemas crean un anillo cerrado de comunicación que impiden que terceros no autorizados ingresen al sistema sin antes ser validados y dados de alta en el ambiente digital propuesto lo que garantiza compartimentación y ante todo sostiene los tres aspectos de la información (disponibilidad, integridad y confiabilidad).
- Con la nueva política de creación de nubes de batalla propuestas por el Comando Conjunto Cibernético la implementación de un sistema interoperable de seguridad garantiza aún más la seguridad de la información de carácter militar haciendo más compleja una intrusión al ciberespacio militar.

CONCLUSIONES

1. El Ministerio de Defensa Nacional y las FFMM a pesar de que poseen sistemas de comunicación digital tipo e-mail, estos no están estandarizados, ni son interoperables entre fuerzas lo que no aporta a la conjuntes. Lo anterior afecta la capacidad de respuesta ante situaciones de conflicto cinético a gran escala. Así mismo estos medios podrían ser hardenizados a un nivel de tipo militar que asegure las comunicaciones.

2. El ministerio de Defensa y las FFMM no cuentan con medios de cifrado estándar que garanticen la interoperabilidad y el tránsito seguro de información entre las diferentes fuerzas afectando la conjuntes y abriendo vulnerabilidades a ciberatacantes que

trabajen para terceros interesados en la información de las instituciones de defensa nacional.

3. Si bien el uso del correo electrónico es ampliamente difundido y se considera primario en el Ministerio de Defensa Nacional y las FFMM este no es un medio concebido para el tránsito de información clasificada, así mismo es una mala práctica permitir que las unidades usen este medio y sistemas de mensajería comerciales tipo chat para transitar información clasificada debido a las vulnerabilidades que los mismos presentan y el desgobierno que se presenta sobre los datos.

4. Con el fin de obtener un gobierno sobre los datos enfocado en controlar parámetros como, su lugar de residencia, la dinámica de usuarios, sus sistemas de cifrado tanto en tránsito como en reposo en los servidores, el control de claves efímeras con el fin de evitar pérdidas masivas de información, se recomienda basar el sistema de comunicaciones digital en tecnologías on-premise aunque su costo sea más elevado y adquirir o diseñar un sistema que cumpla con estos parámetros con el fin estandarizarlo para todas las fuerzas y lograr una hardenizacion del sistema a nivel militar.

5. La interoperabilidad y estandarización de los sistemas de comunicaciones digitales de las Fuerzas Militares trascienden el ámbito técnico para convertirse en un factor decisivo del poder militar. La supremacía informacional, en un escenario de guerra multidominio, solo puede garantizarse si las comunicaciones seguras y soberanas se integran como un pilar estratégico a todos los niveles. En este sentido, la implementación de las plataformas propias on-premise y bajo arquitecturas Zero Trust, no deben entenderse únicamente como una medida de ciberseguridad, sino como un requisito indispensable para la conducción de la capacidad efectiva del mando y control (C2), la protección de la inteligencia militar y la preservación de la capacidad de decisión del Estado. En un conflicto futuro la fuerza que asegure sus flujos de información y niegue al adversario la explotación de sus comunicaciones,

habrá ganado una ventaja estratégica equiparable al control del espacio aéreo o marítimo. Por tanto, la consolidación de un sistema de comunicación unificado, seguro y resiliente debe ser asumida como una prioridad estratégica nacional y no como una solución tecnológica aislada.

5. Bibliografía

Denzin, N., & Lincoln, Y. (2011). *The SAGE Handbook of Qualitative Research.* SAGE publications.

Ogwo-Ude, O. (2023). Business Email Compromise Challenges to Medium and Large-Scale Firms in USA: An Analysis. *Scientific Research Publishing, 13*, 803-812. https://doi.org/DOI: 10.4236/ojapps.2023.136064

Rivero Pérez, C. (2020). *Los susurros encriptados del siglo XXI.* Trabajo de grado, Universidad de la Laguna.

Andrade , F. R. (2020). *interoperabilidad de mensajes protegidos con criptografía utilizando el protocolo PGP.* Tesis de Grado, Pontificia Universidad Católica del Ecuador Sede Esmeraldas.

Bahillo Ortego, R. (2018). *Extensión de FIWARE para soporte de privacidad acorde a las nuevas reglas del RGPD relativas a la gestión del flujo de datos personales.* Trabajo de Grado, Escuela de Ingeniería informática.

Baik, J. (2020). Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *Telematics and Informatics*, 1-34. https://doi.org/https://doi.org/10.1016/j.tele.2020.101431

Barreda , C. (2022). *ESTUDIO PRELIMINAR SOBRE TLS POST-CUÁNTICO.* Trabajo de grado, Escuela de Estudios de Postgrado Universidad de Laguna.

Belén, J. (2021). *Medios de comunicacion virtual durante la pandemia: "Un mapeo sistemático".* Trabajo de Grado, Universidad Politécnica Salesiana sede Guayaquíl.

Bisong, A., & Rahman, S. (2001). Una visión general de las preocupaciones de seguridad en la computación en la nube empresarial. *International Journal of Network Security & Its Applications (IJNSA), 3*(1), 30-45.

Centro de Doctrina Conjunta de las Fuerzas Militares de Colombia - CEDCO. (2018). *Manual Fundamental Conjunto 1.0.* Área imprenta y publicaciones COGFM.

Centro de Doctrina Conjunta de las Fuerzas Militares de Colombia - CEDCO-CGFM. (2018). *Manual fundamental Conjunto MFC 1.0 Doctrina Conjunta.* Área imprenta y publicaciones COGFM.

Comando General de Las Fuerzas Militares. (2020). *Plan de Seguridad y Privacidad de la Información.*

Comando General de las Fuerzas Militares. (2022). Proceso de selección abreviada menor cuantía 184 CGFM-DIAF 2022 (estudio previo). *Proceso de selección abreviada menor cuantía 184 CGFM-DIAF 2022 (estudio previo)*. COLOMBIA.

Díaz Reyes, A. (2025). *Desarrollo de un plug-in con inteligencia artifical para minimizar ataques de ingenieria social en un navegador.* Universidad Estatal de la Península de Santa Helena.

Gonzales Fernandez, A. (2018). *Análisis de riesgos, de vulnerabilidades y auditorías de dispositivos.* Tesis de Grado, Universidad Oberta de Catalunya.

Goyas, M. A., & Vargas, J. D. (2014). *Almacenamiento en la Nube.* Resumen de Tesis .

Guevara, G. P., Verdesoto , A. E., & Castro , N. E. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *RECIMUNDO, 4*(3), 163–173. https://doi.org/10.26820/recimundo/4.(3).julio.2020.163-173

Hernandez , Y. (2020). *Análisis y diseño de un mecanismo de cifrado de correo electrónico para garantizar y proteger la información enviada por las PYMES.* Tesis de Especialización, Universidad Nacional Abierta y a Distancia - Facultad de Ciencias Básicas e Ingeniería.

Khandpur, A. (2018). *Estudio de la herraienta Criptográfica Signal.* Trabajo de grado, universidad de la Laguna.

Landwehr, C., Heitmeyer, C., & McLean, J. (1984). A Security Model for Military Message Systems. *ACM Transactions on Computer Systems, 2*, 198-222.

Martínez, S., Gómez, J., López, C., & Moreno, A. (2023). Fortalecimiento de la seguridad en aplicaciones web mediante criptografía avanzada: métodos y técnicas. *Revista Vínculos: Ciencia, tecnología y sociedad, 20*.

Mattermost. (2025, 06 1). *Mattermost*. https://mattermost.com/security/

Nunes, E. (2023). *Trends in Data Protection and Encryption Technologies.* https://doi.org/https://doi.org/10.1007/9

Pardo, C. (2018). *Amenazas en la Red: Entrando al Mundo de los Ciberataques Ingenieria social, Phishing y Malware.* Trabajo de Grado.

Phole, J., & Thorsten, T. (2022). Soberanía Digital-Revista Latinoamericana de Economía y Sociedad Digital. *ECONSTOR*, 1-22. https://doi.org/10.53857/OLMH2516

Pianoski , E., Fernandez, C., & Farragoni, R. (2018). *REVISTA FATEC SEBRAE EM DEBATE, 5*(9), 70-80. https://doi.org/ISSN: 2358-9817

Polanía, C. R. (2024). Determinación de actividades, vulnerabilidades SSL/TLS y de encriptación. *Revista Agunkuyâa, 14*. https://doi.org/ 10.33132/27114260.2432

Puetate, J. M. (2009). *Estudio de los Protocolos de seguridad del Servicio de Correo Electrónico para implementar un webmail en HCPCH.* Tésis de Grado.

Reyes Riveros, A., Mendoza de los Santos , A., & Salinas Meza, J. (2023). Modelo de Autentificación de Doble Factor. *Innovación y Software, 4*, 82-95. https://doi.org/ 2708-0935

Reyes, D. E. (2025, 05 13). *INFOABE*. INFOABE: https://www.infobae.com/colombia/2025/05/13/militares-colombianos-recurren-a-whatsapp-en-operaciones-por-inoperancia-de-equipos-de-comunicacion-del-ejercito/

Rocketchat. (2025, 06 11). *Rocketchat*. Rocketchat: https://docs.rocket.chat/docs/security-guidelines

Singh, P., Mangaonkar, A., Patil, B., & Patale, K. (2024). Encrypted Chat Application. *International Journal of Scientific Research in Engineering and Management (IJSREM), 8*, 1. https://doi.org/10.55041/IJSREM35388

Verdesoto Gaibor, A. (2007). *Utilizacion de kacking ético para diagnosticar analizar y mejorar la seguridad informatica en la intranet de via celular comunicaciones y representaciones.* Trabajo de Grado, Escuela Politécnica Nacional, Quito.