PERSPECTIVAS EN INTELIGENCIA 2022

Revista Científica en Ciencias Sociales e Interdisciplinaria
Bogotá D.C., Colombia
Volumen 14, N° 23, Enero–Diciembre 2022, pp. 63-95
http://doi.org/10.47961/2145194X.333

El fenómeno de las ciberamenazas: afectaciones a la ciberseguridad del Ejército nacional de Colombia

The phenomenon of cyberthreats: cyber-security implications for the Colombian national Army

Oswaldo Mozo Rivera[1] y Jeisyl Valentina Ardila Contreras[2*]

(1) Universidad Militar Nueva Granada, Bogotá, D. C. – Colombia,
✉ oswaldo.mozo@buzonejercito.mil.co
(2) Universidad Santo Tomás, Bogotá, D. C. – Colombia,
✉ jeisylardila@usantotomas.edu.co
* Autor a quien se dirige la correspondencia

Resumen

El objetivo de este trabajo es analizar las ciberamenazas con capacidad de afectar la seguridad de la información del Ejército nacional de Colombia entre enero del año 2019 a junio de 2020, poniendo en riesgo los intereses nacionales y, por lo tanto, la defensa nacional. Para ello se ha recurrido a fuentes de información primaria, apoyadas en técnicas de investigación cualitativa, obtenidas de documentos científicos y académicos, donde se evaluaron los niveles de riesgos derivados de ataques cibernéticos, estableciendo las causas que comprometieron la integridad en la seguridad de la información y el impacto generado en la Institución. Por lo cual, se hace imperativo integrar capacidades y especialidades cibernéticas con la participación de actores del sector privado y público, civil y militar, para contrarrestar las vulnerabilidades a las cuales se expone el Ejército nacional de Colombia con uno de sus principales activos estratégicos: "La información".

Clasificación JEL: H56, O33

Palabras clave: Ciberdefensa; ciberseguridad; ciberespacio; seguridad de la información; Ejército nacional.

Fecha de recepción: 06/07/2022 | Fecha de aprobación: 24/10/2022

Abstract

The objective of this work is to analyse the cyber threats with the capacity to affect the information security of the Colombian National Army between January 2019 and June 2020, putting national interests and, therefore, national defence at risk. For this purpose, primary information sources have been used, supported by qualitative research techniques, obtained from scientific and academic documents, where the levels of risks derived from cyber attacks were evaluated, establishing the causes that compromised the integrity of information security and the impact generated in the institution. Therefore, it is imperative to integrate cybernetic capacities and specialties with the participation of actors from the private and public, civilian and military sectors, to counteract the vulnerabilities to which the Colombian National Army is exposed with one of its main strategic assets, "Information".

Keywords: Cyber defence; cybersecurity; cyberspace; information security; National Army.

Introducción

La revolución tecnológica de la información y las comunicaciones, producto de la globalización, ha encaminado al mundo hacia nuevos riesgos y amenazas. Los retos del futuro, desde la disciplina de la Ciberinteligencia, exigen analizar este fenómeno de manera transversal, con una visión holística, en busca de responder a los desafíos y proteger uno de los principales activos estratégicos del Ejercito nacional de Colombia: "la información". La sociedad actual, las instituciones, los Estados, empresas, gobiernos, entre otros actores, se han vuelto dependientes del internet. Cada día hay una mayor interconectividad entre computadoras y sistemas de información de cara a las múltiples oportunidades que brinda esta red informática, convirtiendo a los múltiples actores en objetivos para las amenazas emergentes (Guguyener, 2017). Lo anterior se relaciona a lo mencionado por Pirateque (2021), en su libro de Comunicaciones Estratégicas (STRATCOM) y Social Media: su aplicabilidad para el mundo Postwesfaliano.

> *En el mundo posmoderno, donde la globalización se replantea en sus alcances, la democratización y expansión de la Tecnología de la Información y las Comunicaciones estructura múltiples y complejas amenazas, así como actores atomizados y micropoderes con capacidades de desestabilización por parte de cualquier actor, bien sea estatal o no estatal. Este marco de acción gira en lo que expertos han determinado como la "Guerra de Quinta Generación" que se desarrolla en lo cognitivo, con la manipulación de los sistemas de creencias de los ciudadanos, donde la victoria o derrota se define en el campo de la legitimidad.*

Es importante tener presente cómo a través del crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia se ha

permitido de la mano de sus ciudadanos consolidar un Estado cada vez más competitivo, proactivo e innovador en el entorno digital, con capacidades diferenciales en procesos y procedimientos para ser más eficientes en la gestión pública al servicio de la sociedad (Política de Gobierno Digital, 2018). Es por ello que, dentro de los retos y estrategias del actual Gobierno nacional, se ha buscado impulsar la transformación y modernización digital con mejores tecnologías, transversal a los sectores económicos y sociales, que permitan emprendimiento, productividad, mejor educación, entre otros objetivos, para lograr una mejor calidad de vida y bienestar del pueblo colombiano (Plan Nacional de Desarrollo, 2018). Sin embargo, el incremento en la participación en el entorno digital de los ciudadanos y la adopción de nuevas tecnologías trae consigo nuevas y más sofisticadas formas para atentar contra la seguridad de las personas y la defensa del Estado (Conpes 3995, 2020).

Lo anterior es de gran preocupación, principalmente para los actores del Ministerio de Defensa, y las autoridades civiles del sector público, encargados de garantizar la seguridad del Estado colombiano, por lo cual se ha buscado crear y promover una cultura de generación de conocimiento e investigación para innovación, desarrollo en ciencia y tecnología, fortaleciendo las capacidades de las Fuerzas Militares y de la Policía nacional, para interpretar las diversas modalidades de las amenazas, y de esta manera, poder estar a la vanguardia de las mismas (Política de Defensa y Seguridad, 2019). Para ello, no solo se ha tomado como referente las potencias de primer orden (Estados Unidos, Rusia, China, Alemania, Inglaterra, entre otras), sino que, además, Colombia ha buscado crear sus propias políticas y lineamientos que garanticen la seguridad y defensa en el ciberespacio.

Con el Conpes 3701 de 2011, se crearon los lineamientos de ciberseguridad y ciberdefensa, con el fin de diseñar una estrategia nacional y un marco jurídico que les permita a los organismos que llevan a cabo estas actividades actuar de manera legal para contrarrestar las amenazas existentes en el ciberespacio, reduciendo la probabilidad de que estas sean efectivas y fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo, situación que exige la estructuración de una política de seguridad digital y la participación de multiplicidad de actores que intervienen en el espacio cibernético. (Conpes 3854, 2016).

Aunado a lo anterior, mediante un trabajo dinámico, liderado por personal experto en el tema, se han identificado barreras que no han permitido una transformación digital exitosa, por lo que se busca crear las condiciones habilitantes en el sector público y privado, que garanticen su desarrollo y transformación; para ello, el capital humano juega un papel preponderante, ya que garantiza no solo su aprovechamiento, sino que además, mediante sus capacidades y competencias distintivas, con la participación de diversos sectores, enfrenta los retos que la cuarta revolución industrial exige (Conpes 3975, 2019).

Ante este escenario, el Ministerio de Defensa de Colombia admite que la protección de la soberanía y los ciudadanos depende en gran medida de la lucha contra la delincuencia

cibernética y de la defensa de las Infraestructuras Críticas Cibernéticas Nacionales ICCN, (Comando Conjunto Cibernético, 2017; Ministerio de Defensa, 2016). Es así como diferentes académicos han buscado explorar el desarrollo institucional del dominio del ciberespacio en Colombia y su incidencia sobre las relaciones cívico-militares en el país, que permita involucrar tanto a los actores de la Fuerza Pública, como a miembros del sector civil (académicos, empresarios, sector financiero, ministerios, entre otros), para fortalecer capacidades y diseñar estrategias que generen confianza y seguridad en el entorno digital, mediante la investigación, el desarrollo y la innovación (Cujabante et al., 2020).

Teniendo en cuenta lo anterior, el propósito de este trabajo es analizar las ciberamenazas con capacidad de afectar la seguridad de la información del Ejército nacional de Colombia entre enero del año 2019 a junio de 2020 mediante ataques cibernéticos que haya causado fuga de información, poniendo en riesgo los intereses nacionales y, por lo tanto, la defensa nacional. Toda vez que, debido al avance de la globalización, se han diseñado elementos tecnológicos cada vez más avanzados que le permiten a diferentes actores, tanto legales como ilegales, del orden nacional e internacional, desde el ciberespacio obtener información sensible. Dicho lo anterior, es pertinente hacer la siguiente pregunta de investigación ¿Cómo las ciberamenazas afectaron la seguridad de la información del Ejército nacional de Colombia entre enero del año 2019 a junio de 2020? De esta manera, el presente trabajo identificará los tipos de ataques cibernéticos con capacidad de afectar los pilares de seguridad de información en el Ejército Nacional de Colombia, evaluará los riesgos informáticos derivados de los ataques cibernéticos y establecerá las causas que dieron lugar a los ciberataques comprometiendo la seguridad de la información en el Ejército nacional de Colombia entre enero del año 2019 a junio de 2020. Finalmente, se elaborarán conclusiones que permitirán seguir abordando el presente tema en estudio para futuras investigaciones.

Diseño metodológico

Se realizó un estudio de un enfoque cualitativo con diseño descriptivo de tipo documental, con el que se seleccion**ó** rigurosamente aquella información que resultó pertinente para los objetivos de la investigación, a partir de criterios de búsqueda y mediante el uso de motores de búsqueda como Bibliometrix, Scopus, Google académico, Redalyc, Base-Search, Janes, Clacso, Scielo, entre otros. Se encontraron cerca de 220 registros relacionados con la investigación, a los cuales se les realizó un estudio sistemático de acuerdo con la técnica exploratoria y analítica para la recolección y revisión de información determinada para este tipo de artículo (Calle, 2016).

El tipo de revisión adoptada es de carácter sistemático, ya que permitió descartar rápidamente los artículos de revisión que son de poco interés o científicamente dudosos, y detectar potenciales de error. Es así como de los 220 registros encontrados se obtuvo un aproximado de 43 registros con un alto nivel de confiabilidad a partir de una evaluación

sistemática de las investigaciones publicadas (Vera, 2009). Es decir que, los resultados obtenidos fueron filtrados y procesados de tal forma que permitieron analizar cómo las ciberamenazas están en la capacidad de afectar la integridad de la información del Ejército nacional de Colombia mediante ataques cibernéticos.

Marco conceptual

El internet surgió de estudios e investigaciones de tipo militar, con el ánimo de garantizar las comunicaciones en caso de un ataque nuclear en el marco del planeamiento de la Guerra Fría (1969) por parte del Departamento de Defensa de los Estados Unidos; de manera específica, por la Agencia de Investigación Avanzada de Proyectos de Defensa. Sin embargo, la utilidad para el resto del mundo se arraigaría con la creación del protocolo conocido hasta el momento como TCP/IP, brindando con esto un lenguaje genérico para todos los computadores y con el cual serían capaces de comunicarse, surgiendo así el World Wide Web (WWW) y en esencia el internet como es conocido en nuestros días.

Hoy el internet enlaza y gestiona servicios esenciales en un país, entendiendo como servicios vitales los siguientes: medios de comunicación, redes de repartición (agua, electricidad, gas, petróleo), medios de transporte, servicios de gobierno y Fuerzas Armadas; también se consideran servicios vitales las entidades financieras, universidades, entre otros, llevándonos a inferir con lo anterior que la economía y la seguridad nacional dependen de las Tecnologías de la Información y la logística de las comunicaciones.

En la actualidad se considera el ciberespacio como el nuevo integrante del global common, en conjunto con los habituales: terrestres, marítimos, aéreo y espacial, siendo objeto común de reflexión y publicación por parte de estudiosos y numerosas agencias e instituciones públicas y privadas nacionales e internacionales, incluyendo la Organización del Tratado del Atlántico Norte (OTAN), Unión Europea, Organización para la Seguridad y Cooperación en Europa (OSCE) (Centro superior de estudios de la defensa nacional. 2012).

El ciberespacio hace que las fronteras pierdan su vigencia haciendo que la información se propague por canales políticos, étnicos, religiosos, entre otros. Todo lo relacionado con las tecnologías de la información se desarrolla genéricamente en software, hardware e implantación de protocolos de seguridad, los cuales son creados por organizaciones que se estandarizan bajo el concepto de interoperabilidad; consecuente a ello las vulnerabilidades son expuestas y disponibles para ser explotadas de manera cada vez más sofisticadas.

Existen diversos tipos de ciberamenazas en el basto universo digital; para el caso específico del Ejercito nacional de Colombia es lógico que todas puedan llegar a afectar, pero de manera directa, y conforme se establecerá en el desarrollo de este trabajo, que existen dos ciberamenazas con un alto nivel de impacto, activos de valor estratégico, estas son Ciberespionaje y Ciberterrorismo.

Para explicar lo anterior, se debe tener en cuenta el concepto de seguridad de la información, el cual se trata de las medidas preventivas y de reacción del individuo, la organización y las tecnologías para proteger la información, buscando mantener en esta la confidencialidad, la autenticidad y la integridad. Hay que tener claro que los términos seguridad de la información y seguridad informática son diferentes. La segunda trata solamente de la seguridad en el medio informático, mientras que la primera es para cualquier tipo de información, sea esta digital o impresa. La seguridad de la información abarca muchas cosas, pero todas estas giran en torno a la información. Por ejemplo, la disponibilidad, la comunicación, la identificación de problemas, el análisis de riesgos, la integridad, la confidencialidad y la recuperación de los riesgos (Universidad Libre, 2015).

Ahora, el Ciberespionaje se puede definir de diversas maneras; para efectos de este trabajo se considera apropiada la siguiente: "En tiempo de paz, los adversarios pueden realizar reconocimientos de los sistemas de información de gobiernos, universidades y compañías privadas, identificando los objetivos clave, buscando vulnerabilidades para su empleo en tiempos de crisis o confrontación" (Maroto, 2009).

Con esta realidad expuesta, un primer modelo de negocio utilizado en el Ciberespionaje es soportado directamente en los gobiernos en los que se apoyan de manera oculta o poco conocida actividades que conllevan a obtener información que eventualmente permita obtener ventajas estratégicas. Análogamente se evidencia, y como segundo concepto a considerar, que las organizaciones están dispuestas a invertir grandes cantidades de dinero en la preparación y realización de sus acciones bajo la acción denominada "CaaS Cybercrime-As-A Service" (Cibercrimen como servicio), percibiéndose gran competencia entre los mismos ciberdelincuentes y obligando a prestar un servicio cada vez más fiable para sus clientes, donde ofrecen paquetes que permiten la explotación, búsqueda y vulneración de sistemas informáticos (Karake, 2019).

Las compañías de seguridad invierten en tratar de medir las pérdidas que genera esta actividad, por ejemplo, McAffe expone, en su informe titulado "The Economic Impact of Cibercrime and Ciberespionaje", que las pérdidas económicas por actividades relacionadas por Ciberespionaje suponen entre 0,5 y el 2 % del PIB de una nación, pero adicional a esto, y muy lógico, el principal daño no se puede medir en términos económicos, pues se considera más importante la pérdida de confianza, iniciativa, oportunidad y, en el caso de entidades de gobierno, la pérdida de legitimidad (Studies, 2013).

Por otra parte, el Ciberterrorismo es la forma de terrorismo que utiliza las tecnologías de la información para intimidar, coaccionar o para causar daños a grupos sociales con fines político-religiosos; como característica principal, este no requiere la presencia física del atacante, indicando así que el nivel de resiliencia es alto y sin múltiples amenazas. En este concepto se pueden enmarcar tres formas de ciberterrorismo: 1. Los ataques realizados desde computadoras hacia centros tecnológicos, 2. La propaganda como forma de enviar

sus mensajes y para promover el daño ocasionado por sus ataques y, 3. La planificación logística de atentados tradicionales, biológicos o tecnológicos (Martínez, 2009).

Una amenaza importante que puede derivarse del ciberterrorismo es la ciberdelincuencia; esta no funcionaría de manera tercerizada o tipo outsourcing prestando sus servicios a gobiernos y Estados, sino actuando de manera propietaria, utilizando todas sus capacidades y aplicándolas a entidades de gobiernos mediante la utilización de técnicas y herramientas especializadas.

Luego de identificar las dos amenazas con mayor nivel de impacto y afectación para el Ejército nacional de Colombia, se debe precisar otro tipo de actividades o ataques derivados de las dos amenazas anteriormente mencionadas, que afectan de manera importante a las Fuerzas Militares, como lo es el Hacktivismo, el cual es la mezcla de la política y la tecnología, es decir, realizar actividades de Hacking por una causa política. Siguiendo este hilo, el término hacker se define como "una persona que disfruta explorando los detalles de la programación de sistemas y la forma de estirar sus capacidades" y una persona que es capaz de "superar o burlar creativamente limitaciones". Y el activismo se define como "una política de tomar acción directa y militante para conseguir una meta política o social" (Santiago, 2018).

Otras técnicas y herramientas especializadas son el Spearphishing, la cual consiste en estafas por medio de correos electrónicos o comunicaciones dirigida a personas, organizaciones o empresas específicas. Aunque su objetivo a menudo es robar datos para fines maliciosos, los cibercriminales también pueden tratar de instalar malware en la computadora de la víctima. Funciona de manera simple, llega un correo electrónico, aparentemente de una fuente confiable, que dirige al destinatario incauto a un sitio web falso con gran cantidad de malwares (Kaspersky, 2020).

Los malwares son cualquier tipo de software malicioso creado para causar daño o explotar cualquier dispositivo, servicio o red programable, uno de los más utilizados es el Ransomware, que es un programa de software malicioso que infecta la computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. Este tipo de malware es un sistema criminal para ganar dinero, que se puede instalar a través de enlaces engañosos incluidos en un mensaje de correo electrónico, mensaje instantáneo o sitio web (Kaspersky, 2020). Y, finalmente, otra herramienta frecuentemente utilizada por los ciberdelincuentes es el Exploits, Exploit-Kits Y Exploit Drive-By, la cual es una vía definida para romper la seguridad de un sistema aprovechando una vulnerabilidad. Un exploit se refiere a una parte de software, herramienta o técnica que se vale de una vulnerabilidad para obtener privilegios dentro de un sistema, hacerle perder la integridad y, si es el caso, denegar servicios en el sistema atacado (Moral, 2014).

Estado del arte

El estudio de las ciberamenazas ha recobrado el interés de investigadores, los cuales están conscientes de que es un riesgo inminente a nivel global; es una actividad que tiene por objeto comprometer la seguridad de un sistema de información alterando la disponibilidad, integridad o confidencialidad de un sistema o de la información que contiene. Este tema ha tomado gran relevancia a partir de finales del siglo XX, mostrando que la llegada de la tecnología ha amplificado este tipo de ataques que cuentan cada vez con una capacidad más desarrollada de expansión, por lo que afectan a instituciones, gobiernos y diferentes usuarios. A continuación se expondrán algunas de las teorías de las Relaciones Internacionales que logran vincularse al concepto de seguridad, enfocado a las ciberamenazas, así como también se tendrán en cuenta diversos estudios y perspectivas realizadas sobre este tema, que serán útiles para el desarrollo y análisis de esta investigación.

Para dar paso al análisis de la ciberamenazas en la disciplina de las Relaciones Internacionales es pertinente mencionar la concepción del concepto de seguridad como objeto de estudio. Ante la llegada de la globalización, la inmersión de nuevos actores en el Sistema Internacional ha generado una preocupación para los Estados, por lo que necesitan implementar estrategias que contengan los efectos en las ciberamenazas; es en este punto donde se debe plasmar el anterior concepto de seguridad que estaba inmerso en las intenciones de los Estados para proteger su soberanía y enfocarlo a las nuevas dinámicas internacionales.

Para el realismo clásico, Hans Morgenthau explica que el Sistema Internacional es conflictivo por naturaleza y es explicado a partir de dos fenómenos importantes: la maldad es inherente a la naturaleza humana y el Sistema Internacional permanece en anarquía (Morgenthau, 1948), por lo que la seguridad de los Estados se ve afectada por las acciones de las pequeñas organizaciones o de otros actores, haciendo que exista "Una identificación y comprensión de los procesos de "securitización", que remitan al modo en que los temas ingresan de las agendas de seguridad y se interroguen sobre el rol que desempeñan en este marco los actos discursivos gubernamentales" (Waever, 1999).

Esta securitización es un paso de los Estados para enfrentar las ciberamenazas, pues al no existir ninguna autoridad supranacional que regule este tipo de acciones, los Estados son esa unidad básica unitaria que busca maximizar su seguridad creando estrategias que aumenten su poder en tres aspectos: *i)* militares, con nuevas armas; *ii)* tecnológicos, enfocados a la seguridad informática; y *iii)* humanos, con la constante capacitación de los ejércitos para poder asegurar su supervivencia en el sistema. No obstante, esta securitización desata en los demás actores una inseguridad llamada dilema de seguridad, haciendo que se aumente la desconfianza debido a la percepción de amenaza entre los Estados.

Sin embargo, para el liberalismo el Sistema Internacional cuenta con una serie de instituciones que manejan los conflictos por medio de la cooperación entre países que logran acciones colectivas para combatir las ciberamenazas. La ciberdelincuencia, al poder traspasar las fronteras nacionales, obliga a los Estados a actuar bajo el nivel normativo, tratados y diferentes alianzas que mitiguen las amenazas.

Los Estados a nivel interno han creado redes de apoyo entre sus instituciones para afrontar este tipo de inconveniente. En Colombia, el Ejército nacional creó el Grupo de Apoyo de Comunicaciones y Ciberdefensa; en la Armada Nacional se cre**ó** la Dirección Cibernética Naval y en la Fuerza Aérea Colombiana se cre**ó** la Dirección Cibernética Aérea; así mismo, de manera coordinada y conjunta realizan operaciones para la Defensa y Seguridad Nacional (Realpe, 2012).

A nivel externo, en el año 2011 los organismos de la ONU se unieron con una empresa de ciberseguridad para fortalecer la Unión Internacional de Comunicaciones (UIT), que tiene como objetivo

> *"la detección, el análisis y la respuesta eficaz de las ciberamenazas. Esta coalición, que es particularmente interesante para los países en desarrollo y pequeños Estados que no disponen de la capacidad ni los recursos indispensables para desarrollar sus propios centros avanzados de ciberrespuesta, también es beneficiosa para los países técnicamente avanzados, ya que les da una visión mundial de las amenazas en línea potenciales y reales"* (ITU.IN, 2011).

Otro ejemplo es el Convenio de Budapest, elaborado por el Consejo de Europa, el cual entró en vigor en el año 2004; fue el primer y principal tratado internacional que se propuso asociar a los Estados respecto a delitos informáticos. Distintos países se adhirieron al convenio para aplicar una política penal común en materia de cibercrimen (Council of Europe Portal, 2019).

Los postulados del realismo y del liberalismo demuestran que aún siguen teniendo vigencia en el Sistema Internacional, pues aunque los conflictos y las amenazas sean diferentes y evolucionen, los Estados van a preservar esos principios de seguridad, poder y cooperación para sobrevivir en el sistema.

La teoría de la interdependencia, de Josep Nye, afirma que el orden internacional está definido por una jerarquía en términos de que el país más fuerte, con mayor influencia y recursos será el hegemón de la región o del mundo. Los Estados bajo esta teoría actuarán por interés propio en los siguientes factores: *i)* las estrategias de vinculación en las que los Estados con gran capacidad militar y alto nivel de crecimiento económico son quienes predominan sobre los organismos internacionales y sirven como condicionante, en virtud de la asociación de sus propias políticas, sobre las relaciones e intereses de otros Estados; *ii)* el establecimiento de la agenda en la que se prioricen y se concentren

cuestiones políticas, militares y socioeconómicas que definan su discusión e intereses dentro del Sistema Internacional y; *iii)* la definición de las relaciones transnacionales y trasgubernamentales en donde las coaliciones políticas no se encuentran limitadas por las fronteras nacionales que establecerán los temas principales de la agenda y los demás Estados harán caso o se enfrentarán a diversas sanciones económicas o intervenciones (Cardona, 2016).

En el caso de la seguridad y las ciberamenazas, Estados Unidos, al ser el hegemón, es el que presenta la agenda con respecto a las nuevas amenazas, por lo que, en Naciones Unidas, este tema ha tenido mayor trascendencia, pues al ser uno de los países con mayores amenazas cibernéticas en el mundo, debe implementar estrategias para identificar y mitigar estas.

Villalba y Corchado, en el texto análisis de las ciberamenazas, hablan acerca de las nuevas tecnologías y el uso extensivo del internet, el cual genera nuevos retos para los Estados; entre estos aparece la protección y recuperación de los sistemas de infraestructura crítica que se ven afectados dentro del ciberespacio como medio para interferir en actividades de los ciudadanos y de las demás instituciones. Los autores muestran un estudio del caso de España y los ciberincidentes gestionados por el CERT Gubernamental Nacional, que tratan de mitigar el robo de información y diversos aspectos de la seguridad, llegando a verse comprometidos servicios críticos y otros aspectos que afectan a la seguridad nacional.

Este tipo de situaciones ha generado una cierta pérdida de confianza en los servicios electrónicos entre los usuarios, debido a constantes y alarmantes informaciones sobre brechas de seguridad. Las razones más importantes por las que los usuarios se han manifestado son por las inadecuadas garantías de privacidad, lo que ha llevado a que determinados proveedores de servicios de mensajería hayan empezado a ofrecer a sus usuarios un cifrado extremo a extremo de forma que ni siquiera tales proveedores puedan acceder a los mensajes intercambiados. Por lo que, desde el Centro Nacional de Inteligencia, la Oficina Nacional de Seguridad y el Centro Criptológico Nacional, se generan los elementos de prevención y recuperación de los sistemas de las Tecnologías de la Información y las Comunicaciones para que España y los españoles puedan desarrollarse en el entorno digital de forma segura (Fernández, 2017).

Ruiz, en su artículo ciberamenazas ¿el terrorismo del futuro?, define a las ciberamenazas como aquellas actividades presentes en el ciberespacio que suelen estar vinculadas en delitos mediante su utilización, manipulación, control o sustracción. Para el Departamento de Defensa de los EE. UU., el ciberespacio sería «Un dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos y controladores. Ante esto, los Estados han optado por concientizar a la población de tener cuidado con

los virus informáticos, así como también se han realizado modificaciones legislativas que, llevadas a cabo, tienen el objetivo de enmarcar las actuaciones de las fuerzas de seguridad, apoyándose en la ampliación de los delitos de terrorismo y en la prevención de la ciberdelincuencia (Díaz, 2016).

Dammert y Núñez, en el artículo Enfrentando las ciberamenazas: estrategias nacionales de ciberseguridad en el cono sur, presentan un balance en el que las amenazas cibernéticas han aumentado entre 30% y 40% en América Latina, posicionándose como la región en la que con mayor rapidez se presentaron este tipo de ataques. Esta región ha comenzado a elaborar una serie de estrategias nacionales de ciberseguridad, con el fin de modernizar las herramientas de contrataque para estabilizar el espacio vital que afecta a todos los niveles de la sociedad.

Las estrategias que han tomado los países del cono sur han sido: *i)* la protección que tiene como objetivo elaborar normas destinadas a incrementar los umbrales de seguridad en los recursos y sistemas que se relacionen con el sector público; por otra parte se da la creación de agencias de inteligencia que son vitales para la toma de decisiones; *ii)* la cooperación, que en sus distintas dimensiones, sea internacional, intergubernamental y/o cooperación público-privada, es determinante para que un país cumpla con estándares mínimos de seguridad cibernética, pues la ciberseguridad no será efectiva si solo nutrimos un marco legal entorno a lo nacional, descuidando la parte internacional en esta materia, teniendo en cuenta que este fenómeno rompe fronteras; *iii)* la estrategia es importante al momento de realizar la toma de decisiones; esto hace que se optimicen los recursos y el tiempo para enfocar la política de ciberseguridad de cada nación (Dammert, 2019).

Desarrollo de objetivos

El Plan de Seguridad y Privacidad de la Información del Ejercito nacional de Colombia establece "un conjunto de actividades que buscan crear condiciones de uso confiable en el entorno digital y físico de la información mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información" (Departamento de comunicaciones, 2022), los cuales son los pilares de seguridad de la información. En este apartado se identificarán los tipos de ataques cibernéticos con capacidad de afectar dichos pilares.

En primer lugar se encuentra el Ransomware, el cual como, se mencionó anteriormente, se refiere a los diferentes tipos de software malicioso que, al instalarse en cualquier equipo, otorga privilegios al ciberdelincuente para administrar y dar dominio de la información, pasando a secuestrar esta, o dar empleo de esta, de acuerdo con su propósito e intención. Esta técnica generalmente es empleada mediante correos electrónicos que, una vez vistos por el usuario, víctima u objetivo, irrumpen para dar acceso al ciberataque, el cual emplea técnicas de difícil rastreo con el propósito de estar encubierto y garantizar su permanencia en esta actividad ilegal (Trigo, 2017).

En segundo lugar está el Phising, que es el hurto o robo de contraseñas e información personal, como números de cédula y cuentas, los cuales generalmente se ubican y especializan en el sector bancario para consolidar fraudes en transacciones, compras y retiros de dinero. Este proceso generalmente se da en tres fases muy sencillas para el ciberdelincuente, (1) que la víctima acceda a cualquiera de los ataques, ya sea por correos electrónicos enlaces o formularios; (2) que se permita y suministren datos personales y de acceso; y (3) consolidar el fraude, ya sea mediante transacciones o compras, conservando la clandestinidad del delincuente. En este punto se destaca que el mayor caso de incidentes reportados en el país corresponde al método en mención, alcanzando hasta un 42% del total de las denuncias conocidas (Carrillo, et al., 2019).

Derivado del ciberataque anterior se encuentra el llamado Spear phishing, que utiliza correos electrónicos al igual que el phishing, sin embargo, esta modalidad es aún más sofisticada con el fin de que todo parezca auténtico y de buena procedencia, de esta manera los ciberdelincuentes organizan páginas web o mensajes cortos que no despierten ningún tipo de sospecha, copiando el paso a paso y diseño en una similitud exacta para que la víctima fluya en toda confianza y pueda suministrar todo tipo de información sin restricciones. Adicional a lo anterior, en este concepto los delincuentes pueden instalar virus en los ordenadores para tener el control total del sistema y proyectar de manera sistemática otros ataques que les represente algún tipo de ganancia económica (Ionos, 2020). Esto lo hacen mediante malwares, los cuales son un tipo de software malicioso que tiene como característica afectar cualquier tipo de dispositivo electrónico que esté conectado a una red, destacando equipos de cómputo y celulares. Su operatividad funciona con mucha similitud a cualquiera de las herramientas dispuestas por los ciberdelincuentes, como correos electrónicos, descarga de aplicaciones y redireccionamiento a sitios web infectados, dándose de esta manera la filtración de datos, la cual compromete un sistema a un entorno o red no confiable. Este es un error común en el que caen millones de usuarios curiosos que no conocen ni adoptan las medidas básicas en seguridad de la información, otorgando de manera directa la posibilidad de que ciberdelincuentes puedan adquirir información confidencial, manipulando y administrando bases de datos importantes que significan la obstrucción o daño total de un proceso (MinTIC, 2020).

Otro ciberataque que afecta a los usuarios, empresas o instituciones es el denominado ataque DDOS, que es la denegación de servicios; este inhabilita los servidores que ofrecen herramientas de funcionamiento, haciendo que de manera directa cualquier sistema o proceso colapse. En la actualidad, la mayoría de las organizaciones ofrecen servicios esenciales mediante aplicaciones Web, por ende, este se convierte en un objetivo potencial por parte de los ciberdelincuentes, puesto que al vulnerar la seguridad inhabilita la operación, buscando una reacción inmediata por parte de la víctima y, de manera simultánea, logrando acceder a cualquier exigencia con el único propósito de reestablecer el correcto y normal funcionamiento.

Para el año 2019, en Colombia se reportaron 170 casos de empresas, las cuales fueron atacadas e irrumpieron sus servicios, logrando un grave problema de respuesta y responsabilidad frente a sus clientes. Pese a que las autoridades recomiendan no acceder a las ciberextorsiones, con el fin de no financiar este tipo de actividad ilegal, no se presentan salidas o soluciones que otorguen otro camino para evitar esta situación, lo que finalmente mantiene vigente esta vulnerabilidad, la cual es altamente dominante e invasiva en cualquier organización (Ceballos, 2020).

Seguidamente se encuentra la Ingeniería Social, que es el método más empleado para la propagación de ataques informáticos por los creadores de malware, apuntando siempre a objetivos rentables y que contrastan directamente con la vanidad del ser humano, al tener la necesidad de ser dependiente de una conexión permanente, independiente de que no se trate de un contexto laboral o vital necesario, convirtiéndose en una ventaja que abre millones de oportunidades a los ciberdelincuentes; en este sentido, la modalidad se enfoca en obtener información de personas cercanas a un sistema del cual tengan acceso mediante el engaño, articulando esta obtención de información con sus habilidades sociales para consolidar el delito. La premisa máxima de la ingeniería social radica en que es más fácil manipular personas que máquinas, por ende, la habilidad psicológica o de convencimiento juega un papel determinante. Al momento de lograr acceder sobre un objetivo planteado, generalmente emplean algunas técnicas que buscan atraer la atención de confianza, como el respeto a la autoridad, la calidad del servicio, temor por la pérdida de beneficios, respeto social y la gratuidad en los servicios otorgados. En la última encuesta, desarrollada por ISACA para el 2020 a nivel mundial, ubica en el primer lugar este método con un 15% de los eventos materializados (ISACA, 2020).

El segundo recurso más empleado por la ciberdelincuencia, según ISACA, son los Ataques APT, al tener un 10% de incidencia sobre las demás estrategias existentes en el mundo informático; esto obedece a los avances tecnológicos sistematizados que permiten tener la dirección y administración de un pequeño negocio, reunión, capacitación o coordinación, hasta el gerenciamiento de una multinacional o puesto gubernamental (información, 2019).

Los actores y precursores de las APT se caracterizan por ser personas altamente calificadas y posicionadas en los niveles gubernamentales y económicos de las potencias mundiales, los cuales son herméticos y clandestinos para garantizar los niveles de compartimentación y secreto necesario, teniendo en cuenta la extrema sensibilidad y riesgo que configura esta actividad, al punto de poder desatar una guerra (Cortés, 2018).

Con referencia y soporte en la asociación de auditoría y control de sistemas de información, y el informe de tendencias de cibercrimen en Colombia, se puede proyectar una tendencia y acercamiento claro sobre los principales tipos de ataques cibernéticos que pudieran haber afectado y logrado fuga de información en el Ejército nacional, tanto desde el contexto interno, como supranacional, entendiendo que este tipo de amenazas

no poseen fronteras ni límites en el accionamiento y materialización; de esta manera se ubican con mayor grado de incidencia por casos puestos en denuncia y encuestas, que el Ransomware, Malware, Ingeniería Social y Ataque APT, las modalidades más utilizadas y que mejor otorgan resultados a los ciberdelincuentes (véase **TABLA 1**).

A nivel nacional se presenta un incremento bastante considerable y peligroso, teniendo un comparativo entre el año 2018 y 2019, donde las cifras aumentaron de 99 casos a 705, mostrando que el sector más afectado son las pequeñas y medianas empresas, las cuales no cuentan con la capacidad para brindar cubrimiento de infraestructura informática. Así mismo, y en un contexto supranacional, ISACA adelantó un estudio de tendencias actuales de ataques en seguridad cibernética a nivel mundial y nos expone que el Malware se ubica en la segunda posición después del Phishing con un 31%, bajando siete puntos porcentuales con referencia a los años 2018 y 2019 (ISACA et al, 2019).

Dentro de los análisis efectuados por el estudio de tendencias de cibercrimen en Colombia para los años 2019 y 2020, los códigos maliciosos que más se presentan corresponden a Troyanos, Backdoors, Rootkit, Rat, entre otros, donde como dato curioso se muestra que más del 50% de estos ataques son materializados en los teléfonos celulares; esto tal vez debido al atrapamiento que generan estos dispositivos en los usuarios, haciendo que no se dé importancia al momento de detallar el tipo de información que está llegando a nuestro equipo, permitiendo y otorgando privilegios a los delincuentes para proyectar los códigos maliciosos necesarios y posteriormente tomar dominio del sistema (Bautista, 2019).

TABLA 1. Tendencia de organizaciones comprometidas con ataques cibernéticos en el año 2020

Ataques Cibernéticos	Porcentaje
Social Engineering	15%
Advanced persistent threat (ATP)	10%
Ransomware	9%
Unpatched system	9%
Secutiry misconfiguration	8%
Denial of service (DoS)	7%
Sensitive data exposure	7%
Injection flaws	7%
Insufficient logging & monitoring	7%
Broken authentication	6%
Third party	6%
Physical loss of mobile devices	5%
Broken access control	5%

Insider theft	5%
Mobile malware	4%
Cross-site scripting (XSS)	4%
Man-in-the-middle attacks	3%
Other means of cyberattack	2%
MXL external entities (XXE)	2%
Cryptojacking	2%
Watering hole	1%
Insecure deserialization	1%
Living off the land (lotL)	1%
Prefer not to answer	28%
Not applicable	23%
Don't know	18%

Fuente: Elaboración propia, con datos de State of Cybersecurity 2020, Information Systems Audit and Control Association (ISACA).

Se realizará una evaluación de los riesgos informáticos derivados de los ataques cibernéticos al Ejército nacional de Colombia, partiendo de la premisa de que no existe una organización o empresa en el mundo actual que se encuentra totalmente exenta de sufrir algún tipo de riesgo, el cual pueda afectar de forma directa o indirecta las operaciones y todas aquellas actividades que se realizan para el cumplimiento de los objetivos; es por esta razón que es fundamental contar con un plan adecuado de gestión de riesgos que permita actuar de la mejor manera con el propósito de evitar consecuencias a todo nivel.

Aunado a lo anterior, se considera de vital importancia para el Ejército nacional, y para el propósito del actual documento, la evaluación de los riesgos de seguridad de la información entre enero de 2019 a junio de 2020, con la intención de construir herramientas que contribuyan a la identificación de todos aquellos retos a considerar en Ciberdefensa por el Ejército nacional de Colombia. Conscientes de la importancia que implica la evaluación de los riesgos para el cumplimiento de los objetivos planteados en el presente trabajo, las actividades a desarrollar se establecerán en el marco de la norma ISO 31000 de 2018, de Gestión del Riesgo, tratándose de un estándar internacional que instaura las pautas para que cualquier tipo de organización, sea cual sea su naturaleza, considere el riesgo como elemento generador de valor, porque impulsará la toma de decisiones basadas en aquellos riesgos identificados y evaluados.

El proceso de la gestión del riesgo implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, estableciendo

del contexto, evaluación, tratamiento, seguimiento, revisión, registro e informe de riesgo, tal como se presenta en la **FIGURA 1** (ICONTEC, 2018).

FIGURA 1. Proceso de gestión del riesgo

Fuente: Tomado de (ICONTEC, 2018)

Con el fin de cumplir de manera específica el presente objetivo, se tomarán los elementos del proceso mencionado en la **FIGURA 1** para una adecuada evaluación de riesgos.

La identificación del contexto como primera actividad, seguida de la evaluación del riesgo que incluye: identificación, análisis y valoración del riesgo y, para finalizar con un posible tratamiento, lo cual nos dará las bases primordiales para el desarrollo del tercer objetivo específico.

FIGURA 2. Proceso de gestión del riesgo

Fuente: Tomado de (ICONTEC, 2018)

Habiendo explicado de manera precisa el método a utilizar para la evaluación de riesgo se dará inicio a contextualizar, partiendo desde un entorno global a la situación específica, según los datos recolectados. En este punto es fundamental mencionar que no fue una labor sencilla de realizar, pues además de ser imposible determinar de manera exacta la cantidad de ataques que vive una organización cada segundo, también es imposible conocer diligentemente los resultados o aspectos que hayan podido poner en riesgo los pilares de la seguridad de la información.

Sin embargo, en el trabajo de investigación se logró tener acceso a importantes documentos orientadores con los cuales se consiguió establecer aspectos a considerar en materia de riesgos, entendiendo este como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar (ICONTEC, 2018).

Situación 2019

Para establecer el contexto en este periodo se tomará como base el informe de ISACA para el año 2020, el cual se centra en el panorama de las amenazas y revisa las tendencias y los temas de seguridad, resaltando lo siguiente:

Los diferentes tipos de ataques están aumentando, pero el nivel continúa. Gran parte de los encuestados manifiesta que se observan más afectaciones alcanzando su escala máxima, generando así cambios trascendentales en las ciberamenazas y, por consiguiente, en los ataques cibernéticos que no permitan su identificación.

Con el mismo propósito de lo expuesto en la situación del año 2018, se enfoca el presente en la cuantificación de actores y tipos, toda vez que se requiere evaluar el riesgo. Según indica el informe, los ataques siguen siendo del mismo tipo que se identificaron, con mayor frecuencia en años anteriores. Concluyendo que el 22% de los encuestados indica que los ciberdelincuentes tienen la culpa de las vulnerabilidades, el 19 % manifiesta que son piratas informáticos y el 11 % personas internas maliciosas (ISACA, CyberSecurity GRC Services, 2019).

En este informe se pudo notar que ISACA buscó respuestas más detalladas que en el pasado, dado que los vectores de ataque incrementan dependiendo de la creatividad de la amenaza, por consiguiente, se determina que la ingeniería social es el método más popular; el 15 % de los encuestados comprometidos informa que esta estrategia es el método primordial para el ingreso. Según el informe, la amenaza persistente avanzada (APT) es la segunda fuente más común (10%), y el ransomware continúa con 9 %, según reportan los encuestados. Como es de suponerse, el conjunto de las actividades maliciosas

sigue sin reportarse en una buena porción, y principalmente en situaciones en las que tienen la obligación legal o contractual de hacerlo, convirtiéndose así esta tendencia en un común denominador que dificulta cada vez más el manejo de la seguridad de la información (ISACA, 2020).

Contexto Colombiano Ciberamenaza y Ciberataques

Continuando con la intención de establecer el contexto de la manera más precisa posible, y acorde con los datos encontrados, para este espacio del contexto colombiano se denotará un estudio o informe que publica datos estadísticos sobresalientes de ciberamenazas en Colombia, en los cuales se identificaron diferentes tipos de ciberataques a partir de las 15.948 denuncias y reportes que se realizaron por parte de empresas y ciudadanos al Centro Cibernético Policial (CCP).

Este informe muestra cómo se identificaron los principales métodos o vectores de ataque utilizados por los ciberdelincuentes para lograr su cometido. Lo interesante de este estudio, y que aplica al presente trabajo, fue que se establecieron relaciones de las tendencias identificadas en Colombia con las encontradas en el contexto global utilizando las diferentes bases de datos y publicaciones de Europol, Evaluación de amenazas del Crimen Organizado en Internet y los reportes de empresas líderes en el ámbito de la ciberseguridad en la región, como Microsoft, CISCO, McAfee, Absolut, Claro y Fortinet, todos aliados del programa SAFE (SAFE, 2019).

Continuando con la identificación cuantitativa de carácter porcentual, en este informe se puede observar que Colombia recibió el 30% de los ataques de Ransomware en Latinoamérica en el último año; así mismo, los ataques de denegación de servicio fueron resaltados en el informe, teniendo en cuenta que únicamente 170 empresas reportaron este tipo de ataques durante el año 2019, lo que deja ver la poca cultura de reporte teniendo en cuenta que según la página Netscout en Colombia se registraron más de 25.700 ataques de denegación de servicios (NETSCOUT, 2019).

En el mismo estudio mencionado se conoce que el 57% los ciberdelitos reportados en el país corresponden a hurtos por medios informáticos, lo que indica que la utilización del vector de Malware incrementó, conociéndose también que este tipo de ataques tiene una tasa de éxito del 30%, siendo el complemento a la ingeniería social, que sigue con el vector más importante a nivel mundial y nacional.

Evaluación del riesgo de seguridad de información del Ejército nacional de Colombia

Una vez establecido el contexto global y nacional de las ciberamenazas y ciberataques, conforme la metodología NTC-ISO 31000 lo indica, se debe exteriorizar que respecto al Ejército nacional no fue posible la obtención de información, teniendo en cuenta que esta es clasificada y debe tratarse con suma reserva, conforme a la Ley Estatutaria

1621 de 2013; sin embargo, una de las ventajas de esta metodología de evaluación del riesgo es que de acuerdo con contextos y muestras, se puede inferir los posibles niveles de afectación, los tipos de amenazas, vulnerabilidades, entre otros datos que nos dará conclusiones muy importantes para nuestro trabajo.

Para ello se ha contado con el soporte de una matriz de riesgo que se ha consolidado conforme la norma técnica lo establece; por lo cual, y como fue descrito en el primer objetivo, se determinaron los posibles tipos de ataques cibernéticos que pudieron afectar los pilares de seguridad de información (confidencialidad, integridad y disponibilidad) en el Ejército nacional de Colombia entre enero de 2019 a junio de 2020, así: Phishing, Malware, Ingeniería Social, APT, Ransonware, Denegación de servicios y Filtración y exposición de datos.

Si bien es cierto, todos los datos recolectados son muestras tomadas por diferentes entidades, considerando que es imposible saber la cantidad de ataques con exactitud que se presentan alrededor del mundo, en Colombia y en el Ejército nacional. Aunado a la falta de cultura de reporte a las unidades centralizadoras de respuesta a incidentes, el conocimiento del contexto descrito anteriormente permite estimar probabilidades de ocurrencia a los principales ataques que pudo haber sufrido el Ejército nacional durante el lapso investigado (véase **TABLA 2**).

TABLA 2. Probabilidad de ocurrencia

Escala	Descripción	Ciberataque
1. Muy bajo	Puede ocurrir solamente en circunstancias excepcionales.	Otros
2. Bajo	Puede ocurrir de manera inusual.	Filtración y Exposición de datos Denegación de Servicios
3. Medio	Puede ocurrir algunas veces.	Ransomware Malware
4. Alto	Probablemente ocurra.	APT Ingeniería Social
5. Muy alto	Se espera que ocurra en la mayoría de las circunstancias.	Phishing

Fuente: Elaboración Propia

En contraste con la probabilidad de ocurrencia, se analizarán tres diferentes tipos de impactos o escalas que se consideran transcendentales para la evaluación a realizar, la **TABLA 3** se constituye de los impactos sobre la imagen institucional en la que, de acuerdo con lo establecido, se determina la percepción desde el interior de la institución hasta el nivel internacional. La **TABLA 4** muestra el impacto legal o contractual de manera genérica; y la **TABLA 5** nos expone los posibles impactos que puedan tener los ciberataques en el desarrollo de las Operaciones Terrestres Unificadas.

TABLA 3. Impacto - imagen institucional

Escala	Descripción
1. Muy bajo	El evento afecta la imagen del responsable dentro de su sección o dependencia al interior del Ejército nacional.
2. Bajo	El evento afecta la imagen de la sección o dependencia ante la institución.
3. Medio	El evento afecta la imagen del Ejército nacional frente a las Fuerzas Armadas.
4. Alto	El evento afecta la imagen del Ejército nacional a nivel nacional.
5. Muy alto	El evento afecta la imagen del Ejército nacional a nivel nacional e internacional.

Fuente: Elaboración Propia

Nota. Valor: En la ponderación el valor asignado se computa multiplicando por 0.3

TABLA 4. Impacto - legal o contractual

Escala	Descripción
1. Muy bajo	El evento da lugar a una sanción, de acuerdo con Ley No. 1862 de 2017
2. Bajo	El evento genera la apertura de una investigación, de conformidad con la Ley No. 1862 de 2017
3. Medio	El evento genera investigaciones de carácter contractuales por parte de un ente de control.

4. Alto	El evento genera cancelación de convenios nacionales, internacionales o aliados estratégicos que contribuyan al desarrollo de la acción unificada.
5. Muy alto	El evento genera cancelación de convenios internacionales nacionales o aliados estratégicos miembros de la OTAN, generando sanciones por parte de organismos internacionales.

Fuente: Elaboración Propia

Nota. Valor: En la ponderación el valor asignado se computa multiplicando por 0.3

TABLA 5. Impacto - desarrollo de operaciones terrestres unificadas

Escala	Descripción
1. Muy bajo	El evento genera o influye en el desarrollo de las operaciones terrestres unificadas a nivel táctico.
2. Bajo	El evento genera o influye en el desarrollo de las operaciones terrestres unificadas a nivel operacional.
3. Medio	El evento genera o influye en el desarrollo de las operaciones terrestres unificadas a nivel estratégico.
4. Alto	El evento genera o influye en el desarrollo de las operaciones terrestres unificadas en todos los niveles, con alta probabilidad de pérdida de vidas al interior de la institución.
5. Muy alto	El evento genera o influye en el desarrollo de las operaciones terrestres unificadas en todos los niveles, con alta probabilidad de pérdida de vidas al interior de la institución y población civil.

Fuente: Elaboración Propia

Nota. Valor: En la ponderación el valor asignado se computa multiplicando por 0.4

En el proceso de evaluación y consolidación de la matriz de riesgos aplicada a la información obtenida durante el proceso se logra identificar que, aun cuando no son expresadas de manera puntual, existen vulnerabilidades con muy alta probabilidad de materializar un riesgo, lo cual conlleva estrictamente a afectar un pilar de la seguridad de la información.

De igual manera, como se mostrará en la matriz de riesgo (**TABLA 6**), el riesgo inherente se puede obtener de computar la probabilidad de ocurrencia con el impacto, obteniendo con esto una zona de riesgo inherente la cual será de gran utilidad para la determinación de alternativas de solución u opciones de tratamiento del riesgo.

TABLA 6. Matriz de riesgo

Amenaza	Vulnerabilidad	Descripción del riesgo	Pilar de la SI afectado (CID)	Proba-bilidad	Impacto	Valor riesgo inhe-rente	Zona de riesgo inhe-rente
Phishing	-Falta de cultura en Seguridad de Información. -Concientización del personal acerca de la importancia de la seguridad y responsabilidades compartidas e integrales. -Ignorancia, negligencia o curiosidad por parte de usuarios en general de los sistemas.	Acceso no autorizado a información clasificada o sin clasificar del Ejército nacional debido a falta conciencia en seguridad de la información, explotando las vulnerabilidades mencionadas con el catalizador de los equipos que en su mayoría se encuentran conectados a la red interna.	Confidencialidad	5	3.4	17	**Alta**
Ingeniería Social	-Concientización del personal acerca de la importancia de la seguridad y responsabilidades compartidas e integrales. -Relajamiento de las políticas y procedimientos de seguridad, por falta de seguimiento de los mismos, producidas por un desempeño de seguridad adecuado durante cierto lapso. -Ignorancia, negligencia o curiosidad por parte de usuarios de los sistemas.	Problemas con la confidencialidad, integridad y disponibilidad de la información por ausencia de cultura de seguridad de la información en el Ejército nacional	Confidencialidad Integridad Disponibilidad	4	4	16	**Alta**
APT	-Ignorancia, negligencia o curiosidad por parte de usuarios de los sistemas. -Uso de programas de tipo genérico en aplicaciones críticas. -Equipos, programas y redes "heredados" de generaciones tecnológicas anteriores.	Acceso lógico no autorizado, la información clasificada o sin clasificar del Ejército nacional con base en las vulnerabilidades sobre el sistema, aprovechando la baja cultura de seguridad de la información, utilización de programas genéricos no autorizados y utilización de herramientas heredadas con versiones obsoletas.	Confidencialidad Integridad Disponibilidad	4	5	20	**Extrema**

Malware	-Falta de actualizaciones -Sistemas operativos obsoletos	Pérdida de confidencialidad, integridad y disponibilidad debido a controles insuficientes en el proceso de actualizaciones, utilización de sistemas operativos o programas.	Confidencialidad Integridad Disponibilidad	3	4.1	12.3	**Alta**
Ransomware	-Falta de cultura en Seguridad de Información -Falta de actualizaciones -Sistemas operativos obsoletos -Falta de cultura en Seguridad de Información	-Genéricos de versiones pasadas, así como la implementación de programas de culturización de seguridad de la información. -Pérdida de confidencialidad, integridad y disponibilidad, debido a controles insuficientes en el proceso de actualizaciones, utilización de sistemas operativos o programas genéricos de versiones pasadas, implementación de programas de culturización de seguridad de la información.	Confidencialidad Integridad Disponibilidad	3	3.1	9.3	**Moderada**
Ataque DDOS	-Relajamiento de las políticas y procedimientos de seguridad, por falta de seguimiento de los mismos, producidas por un desempeño de seguridad adecuado durante cierto lapso. -Falla en la adjudicación o seguimiento de responsabilidades. -Planes de contingencia nulos o pobres, tanto para situaciones cotidianas como extremas.	No disponibilidad de los principales servicios brindados por el Ejército nacional por falta de gestión y aplicación de las políticas y procedimientos de seguridad, como resultado de la confianza generada por el desempeño de la seguridad durante un lapso. La asignación de responsabilidades y los planes de contingencia no claros para situaciones de denegación de servicios u otras contingencias.	Disponibilidad	2	3.7	7.4	**Moderada**

Filtración y Exposición de datos	-Confianza excesiva en algún único dispositivo o software. -Uso de computadoras, programas y equipos de red de tipo genérico en aplicaciones críticas. -Cambio frecuente de elementos de la plataforma informática	Pérdida o fuga de datos del Ejercito nacional, debido a la ausencia de controles para la detección, control y uso de dispositivos y canales de comunicación no formales. Pérdida de confidencialidad por ausencia de controles en la disposición final, específicamente en los mecanismos de borrado seguro de información en las estaciones de trabajo.	Confidencialidad	2	4.7	9.4	**Moderada**

Fuente: Elaboración Propia

Nota. Valor: Las zonas de riesgo se representan: Extrema (Mayor o igual a 20), Alta (Mayor o igua al 12 y menor a 20), Moderada (Mayor o igual a 6 y menor a 12) y Baja (Mayor o igual a 1 y menor a 6).

En este apartado se analizarán las causas que dieron lugar a los ciberataques que comprometieron la Seguridad de la Información en el Ejército nacional de Colombia entre enero del año 2019 a junio del año 2020.

En un escenario en el que las ciberamenazas son cada día más avanzadas, mediante diferentes estudios investigativos de tipo científico y académico, existen barreras y desafíos identificados que enfrentan las organizaciones (empresas, instituciones, industrias, entre otras), para lograr una transformación digital exitosa; por lo tanto, requieren de la participación de múltiples actores interesados (Gobierno, individuos, sector educativo, sector defensa, entre otros), para ser más competitivos en el mundo digital. Asimismo, paralelamente se requiere fortalecer niveles y estándares de seguridad para disminuir los riesgos de los cuales son objeto las personas y los estados, toda vez que su alcance ha causado una disrupción al traspasar fronteras y no tener una capacidad y control efectivo por los organismos encargados de la seguridad y defensa de la nación (Asociación Nacional de Empresarios de Colombia, 2017). (Véase **FIGURA 3**).

FIGURA 3. Barreras y desafíos que enfrentan las empresas y organizaciones para lograr una transformación digital exitosa

Fuente: Tomado de Encuesta de Transformación Digital, 2017, (p. 12), por la Asociación Nacional de Empresarios de Colombia (ANDI)

La participación en el entorno digital, la implementación de nuevas tecnologías, trae consigo riesgos e incertidumbres; para ello, se requiere fortalecer las capacidades del potencial humano, para el diseño y desarrollo de estrategias más efectivas en las que de manera conjunta se garantice confianza entre los múltiples actores que interactúan en el mundo digital, buscando potencializar modelos en ciberseguridad y ciberdefensa para el Estado y sus ciudadanos (Departamento Nacional de Planeación, 2019).

Actualmente, el Ejército nacional de Colombia, para garantizar la seguridad y defensa de la información en el entorno cibernético, tiene un batallón de seguridad de la información, un batallón de ciberinteligencia y una unidad de comunicaciones, los cuales cuentan con personal técnico, profesional y, en menor medida, experto para el desarrollo de actividades en el ciberespacio. A pesar de tener personal idóneo en los tres niveles, este no es suficiente para atender la demanda de las ciberamenazas en el entorno digital de la Institución; además, una vez verificada su organización, funciones y capacidades, estos no cuentan con un centro de pensamiento investigativo que permanentemente este estudiando y analizando la mutación y evolución de las ciberamenazas para presentar modelos y estándares de seguridad confiables.

Discusión

Los principales tipos de ataques cibernéticos con capacidad de afectar los pilares de seguridad de la información en el Ejército nacional se consideraron desde un concepto investigativo con fuentes académicas y estadísticas que determinan un acercamiento de la realidad, en cuanto a tendencia y casuística, en referencia a los hechos conocidos y denunciados formalmente. Lo anterior, teniendo en cuenta que este tipo de actividad ilegal no está muy bien configurada en el contexto legal, y mucho menos en el concepto

de prevención y visibilidad. De esta manera, conocer con precisión las características y dinámica de la delincuencia informática se hace imposible cuando en muchos de los eventos las víctimas no se percatan o enteran de un ataque de hurto o pérdida de información. Sin embargo, la persistente actividad ilegal hace que este se consolide como un tema con alto nivel de afectación en la actualidad, tanto para el sector privado, como para los organismos de seguridad del Estado, los cuales se han visto en la necesidad de atender esta problemática y desarrollar capacidades con las cuales puedan dar en cierta medida control y prevención.

"Mientras, los Estados deben distribuir su presupuesto en diversas categorías (también llamadas, obligaciones estatales: salud, educación, vivienda, entre otras)" (Pirateque, 2022). La ciberdefensa aún no es catalogada como una prioridad para el Estado. Sin embargo, las empresas privadas están empezando a invertir en desarrollo, investigación y seguridad cibernética para hacer frente a las nuevas amenazas nacientes derivadas de la globalización. Así las cosas, y en un plano más aterrizado, la presente investigación tomó diferentes artículos académicos, autores y estadísticas de fuentes abiertas, que se aproximan en gran medida sobre los principales ataques cibernéticos que han podido afectar la seguridad informática en el Ejército nacional. Adicionalmente, se tomó asesoría con las capacidades actuales con las que cuenta la Fuerza en materia de seguridad de la información, ciberseguridad y comunicaciones, delimitando un tiempo entre los años 2019 y 2020, con el propósito de tener un contexto actualizado por la cambiante y exponencial evolución de herramientas para la explotación de vulnerabilidades informáticas.

De los diferentes elementos académicos y de consulta, dos de los principales documentos para afirmar y concluir la discusión, son ISACA y el informe de tendencias del cibercrimen para Colombia, que al integrarlos y dar análisis de la información destacan los siguientes:

- Ingeniería Social: Siendo la base inicial y elemental para conocer y emprender cualquier tipo de ataque cibernético, se cataloga como el más utilizado por el fácil acceso y punto de partida de cualquier persona que quiera ensayar en esta temática. A nivel mundial se ubica en primer lugar con un 15%.
- Ransomware: Este método, a nivel nacional, reportó para el último año 31.058 casos, destacándose por encima de los demás y estableciendo un nivel de incidencia del 30% en al ámbito de Latinoamérica.
- Malware: En este ítem se destaca un exagerado crecimiento entre los años 2018 y 2019, donde el incremento paso de 99 a 705 eventos identificados y reportados; así́ mismo, en el plano mundial se cataloga en el segundo puesto con un 31% de incidencia.
- Ataque APT: La cantidad de eventos no es la cualidad por la que destaca este recurso, se trata de su alto nivel de sensibilidad por el concepto de seguridad en cuanto al grado de afectación y conceptos estratégicos de seguridad de Estado, y avances científicos y tecnológicos, los cuales son determinantes en el posicionamiento estratégico mundial.

Acorde con los resultados de la encuesta global anual, sobre el estado de la ciberseguridad llevada a cabo por ISACA, se conoce en uno de sus dos informes las principales tendencias y vectores de ataque, así como las metodologías de respuesta y gestión de programas de seguridad, estableciendo el contexto de la siguiente forma:

El horizonte de las ciberamenazas se ve en términos generales similar con el paso del tiempo; los encuestados indican que los ataques más frecuentes se basan en los mismos vectores observados en años anteriores, pero se prevé que los ataques aumenten en los próximos años. De los aspectos más relevantes en este informe se resaltan los siguientes:

Existe coherencia entre las principales ciberamenazas y los principales ciberataques conocidos, manteniéndose en constancia a través del tiempo; las principales amenazas incluyen ciberdelincuentes, piratas informáticos y personas internas maliciosas, los cuales como vector de ataque sostienen el phishing, el malware y la ingeniería social, consolidándose así tres de los principales ataques cibernéticos que pudieron haber afectado los pilares de seguridad de información (confidencialidad, integridad y disponibilidad) en el Ejército nacional de Colombia entre los años 2018 a 2020.

Según menciona la encuesta, y con motivo de considerar estos datos en la evaluación del riesgo, se conoce que de todos los tipos de ataques que existen el phishing sigue siendo el más frecuente (informado por el 44 % de los encuestados); el malware ocupa un segundo lugar distante (informado por el 31 % de los encuestados); y la ingeniería social es el tercer tipo de ataque más común (informado por el 27 % de los encuestados) (ISACA, 2019).

En la encuesta de transformación digital realizada por la ANDI en el año 2017, podemos comprobar, mediante la Imagen N° 04, que a pesar de que en Colombia se han venido diseñando y desarrollando estrategias de innovación en el entorno digital que impactan positivamente en los diferentes sectores y organizaciones brindando múltiples oportunidades a los individuos, la falta de cultura y el desconocimiento del entorno digital son los factores que más impactan de manera negativa, toda vez que el potencial humano sufre consecuencias adversas al no estar capacitado de cara a los retos que nos exige la cuarta revolución industrial.

Asimismo, nos permite determinar que el principal desafío seguirá siendo un cambio de mentalidad, educación y formación en los ciudadanos (técnico, profesional y experto), la academia, las organizaciones y el Gobierno (mayor presupuesto), ante la realidad digital y las tecnologías emergentes, que terminan impactando la seguridad y defensa del Estado, el crecimiento económico, el empleo, la educación, la salud y, en general, la calidad de vida de las personas (Asociación Nacional de Empresarios de Colombia, 2019). Por consiguiente, se requiere de la interacción del sector público y privado, así como de la cooperación de actores transnacionales, donde mediante el liderazgo y conocimiento de

personal experto se garantizarán entornos digitales más confiables para los Estados y sus individuos (Conpes 3995, 2020).

Las instituciones universitarias, dimensionando la importancia del mundo digital y los riesgos que estos representan para la seguridad, han buscado adelantar estudios investigativos, sirviendo en muchas ocasiones de insumos para el Ministerio de Defensa de Colombia, el cual admite que la protección de la soberanía y los ciudadanos depende en gran medida de la lucha contra la delincuencia cibernética y de la defensa de la Infraestructuras Críticas Cibernéticas Nacionales ICCN, (Comando Conjunto Cibernético, 2017; Ministerio de Defensa, 2016). Por lo anterior, se requiere fortalecer la formación y capacitación en el Ejército de Colombia, incluyendo en los pensum académicos de la Escuela de Inteligencia y de Comunicaciones, de los cursos básicos para oficiales y suboficiales, y en los cursos de ascenso de ley, las materias de ciberinteligencia y seguridad de la información; asimismo, se incentive la creación de los centros de pensamiento e investigación cibernética en alianza y cooperación con otras instituciones, agencias y Estados.

Conclusiones

En un contexto ampliamente globalizado, el uso de las nuevas tecnologías y los avances tecnológicos incrementan la aparición de riesgos y amenazas. Como se analizó en el texto, existen diversos métodos y técnicas de ciberataques que afectan no solo a personas civiles, empresas o instituciones sino también a las Fuerzas Militares del país. Dentro de este trabajo se encontró que la ciberdelincuencia es una potencial amenaza silenciosa y clandestina que, desde diferentes modalidades, especialidades o métodos, puede configurar un ataque exitoso a los sistemas de información del Ejército de Colombia, por lo que se hace necesario identificar las vulnerabilidades de la Institución para fortalecerlas y mitigar dichos ataques, más aún, teniendo presente los alcances sin fronteras que caracterizan los ataques cibernéticos.

Las ciberamenazas y ciberataques se presentan de manera constante; no existe empresa u organización alrededor del mundo que pueda estar exenta de las mismas, lo cual conlleva a que el proceso realizado sea factible y conducente; sin embargo, la falta de información respecto a cantidades y tipos de ataques cibernéticos que se expresó a lo largo del desarrollo del presente trabajo hace que la ciberdefensa se torne compleja frente a los nuevos retos.

Teniendo en cuenta que no fue posible la obtención de información del Ejército nacional, ya que esta es clasificada y debe tratarse con suma reserva conforme la Ley Estatutaria 1621 de 2013, se realizó la identificación de los principales tipos de ataques cibernéticos, lo cual permitió realizar de manera objetiva una evaluación de riesgo con la que se pudo inferir los posibles niveles de afectación, los tipos de amenazas, vulnerabilidades (véase **TABLA 6**), encontrando que la amenaza de ataque ATP representa la mayor zona de riesgo

inherente, clasificándose como extrema, con impacto de 5, siendo este el valor más alto, afectando la confidencialidad, integridad y disponibilidad, las cuales son los pilares de la seguridad de la información del Ejército nacional. Asimismo, se establecieron actores y vectores sobre los cuales se debe estar vigilantes en todo momento, comprendiendo el ambiente cibernético en el cual estamos inmersos cada día.

Además, la evaluación de riesgos contó con diferentes impactos; entre los más relevantes tenemos imagen institucional, legal o contractual y desarrollo de las operaciones terrestres unificadas.

Los ataques Phishing, Ingeniería Social y Malware afectan de igual manera los pilares de la seguridad de la información y se encuentran en una zona de riesgo inherente alta y, por último, los ataques de Ransomware, denegación de servicios y filtración de datos, que se encuentran en una zona de riesgo inherente moderada.

De esta misma manera, se encontró que las causas que dieron lugar a los ciberataques que comprometieron la Seguridad de la Información se deben a los retos y desafíos de lograr una transformación digital exitosa, impidiendo que empresas, instituciones, industrias, entre otras, sean competitivos en el mundo digital; esto debido a la falta de cultura, desconocimiento, presupuesto, falta de capital humano, entre otras, que se pueden visualizar en la **FIGURA 3**.

Para concluir, el Ejército nacional de Colombia, atendiendo a los desafíos para garantizar la seguridad de la información clasificada, tomando como referente organizaciones como el Comando Conjunto Cibernético (CCOC) y Comando Cibernético Policial (CCP), integre mediante un centro integrado de información cibernética, información que genere conocimiento, investigación, desarrollo e innovación, que permita analizar e interpretar con una visión prospectiva los posibles escenarios de las ciberamenazas.

Asimismo, integrando las capacidades del Batallón de Ciberinteligencia, Seguridad de la Información y de las Comunicaciones, se potencialicen actividades, procesos y procedimientos en el entorno cibernético. Además, mediante convenios de cooperación interinstitucionales en el marco OTAN, se fortalezca en capacitación y formación el potencial humano, integración de información y modelos internacionales de seguridad, siguiendo lineamientos, políticas y estrategias y con la participación de personal profesional y experto del sector civil y militar se trabaje de manera coordinada, conjunta e interinstitucional para atender las necesidades del Ejército de Colombia en cuanto a la confidencialidad, integridad y disponibilidad de la información .

Referencias

Asociación Nacional de Empresarios de Colombia. (2017). Encuesta de Transformación Digital. *ANDI*. Obtenido de http://www.andi.com.co/Uploads/Encuesta%20Transformaci%C3%B3n%20Dig ital%20ANDI.pdf

Asociación Nacional de Empresarios de Colombia. (2019). Informe de la Encuesta de Transformación Digital. *ANDI*. Obtenido de http://www.andi.com.co / Uploads/ ANALISIS%20 - % 20ENCUESTA % 20 DE %20TRANSFORMACI%C3%93N%20DIGITAL%20 2019%20-%20ANDI.pdf

Bautista, F. (29 de octubre de 2019). *Tendencias Cibercrimen Colombia 2019-2020.* Obtenido de Tendencias Cibercrimen Colombia 2019-2020: file:///D:/Downloads/informe-tendencias-cibercrimen_compressed-3.pdf

Calle, L. (2016). Metodologías para hacer la revisión de la literatura de una investigación. Obtenido de https://www.researchgate.net/publication/301748735_Metodologias_para_hacer_la_revision_de_literatura_de_una_investigacion.

Cardona Mendoza, S. L. (2016). La interdependencia compleja en los procesos de integración económica: análisis de las estrategias de los BRICS en la región suramericana, caso UNASUR en el periodo de 2009 a 2014. *Negocios y Relaciones internacionales*.

Carrillo, G., Brayham, A., & Bastidas, M. (2019). *Caracterización de la modalidad delictiva "Phishing" en Colombia: avances y retos actuales para la Policía Nacional.* Repositorio Educativo Institucional.

Ceballos, A. (2020). *Tendencias Cibercrimen Colombia 2019-2020.* Obtenido de Tendencias Cibercrimen Colombia 2019-2020: file:///D:/Downloads/informe-tendencias-cibercrimen_compressed-3.pdf

Centro superior de estudios de la defensa nacional. (febrero de 2012). *https://publicaciones.defensa.gob.es.* Obtenido de https:// publicaciones . defensa.gob.es/media/downloadable/files/links/m/o/monog rafia_126.pdf

Conpes 3854. (2016). *Política Nacional de Seguridad Digital.* Departamento Nacional de Planeación. Obtenido de https://bit.ly/3brazVR

Conpes 3975. (2019). *Política Nacional para la Transformación Digital e Inteligencia Artificial.* Departamento Nacional de Planeación. Obtenido de https://www.mintic.gov.co/portal/604/articles-107147_recurso_1.pdf

Conpes 3995. (2020). *Política Nacional de Confianza y Seguridad Digital.* Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

Cortes, A. (2018). *Amenazas Persistentes Avanzadas.* Obtenido de Amenazas Persistentes Avanzadas: http://35.227.45.16/bitstream/handle/20.500.12277/2677/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

Council of Europe Portal. (2019). Obtenido de https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=S5PssuRE

Cujabante, x., Bahamón M, M., Prieto, J., & Quiroga. (2020). *Ciberseguridad y ciberdefensa en Colombia: un posible modelo a seguir en las relaciones cívico-militares.* Bogotá: Revista Científica General José María Córdova.

Dammert L, N. C. (2019). "ENFRENTANDO LAS CIBERAMENAZAS: ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN EL CONO SUR. Seguridad, ciencia y ciencia.

Departamento Nacional de Planeación. (2019). *Política Nacional para la Transformación Digital e Inteligencia Artificial.* Obtenido de https://www.mintic.gov.co/portal/604/articles-107147_recurso_1.pdf

Díaz, J. R. (2016). Ciberamenazas: ¿el terrorismo del futuro? *Instituto español de estudios estratégicos*.

Guguyener, A. (2017). *Understanding the Vulnerabilities of Critical Energy Infrastructure to Cyber Terrorism and Threats: How to Secure Our Energy Systems* (Vol. 48). Strategic Cyber Defense. doi:org/10.3233/978-1-61499-771-9-74

ICONTEC. (18 de julio de 2018). NTC-ISO 31000. Bogotá, Colombia.

ICONTEC. (18 de julio de 2018). NTC-ISO 31000. Bogotá, Colombia. información, A. d. (2019). *Actores de amenazas y tipos de ataques.* RESERVA DE DERECHOS.

Ionos. (30 de abril de 2020). *Digital Guide.* Obtenido de Digital Guide: https://www.ionos.es/digitalguide/correo-electronico/seguridad-correo-electronico/spear-phishing/

ISACA. (Nov. de 2019). *CyberSecurity GRC Services.* Obtenido de CyberSecurity GRC Services: file: ///D: / Downloads/ CONSULTA % 20ARTICULO / state - of-cybersecurity-2019-part-2_res_eng_0619.pdf

ISACA. (2019). *STATE OF CYBERSECURITY 2019: CURRENT TRENDS IN ATTACKS, AWARENESS AND GOVERNANCE.* Schaumburg, IL: ISACA.

ISACA. (2020). *State of Cybersecurity 2020.* All Rights Reserved.

ISACA. (2020). *State of Cybersecurity 2020.* Schaumburg, IL: ISACA.

ITU.IN. (16 de mayo de 2011). *ITU Comprometida para conectar al mundo.* Obtenido de http:// www.itu. int / net / pressoffice / press _ releases/ 2011/ 17 - es .aspx#. YGyX59LPzIU Fernández. (2017). Análisis de las ciberamenazas. *Dialnet*.

Karpesky. (2020). *https://latam.kaspersky.com*. Obtenido de https://latam.kaspersky.com: https://latam.kaspersky.com/resource-center/definitions/spear-phishing

Kaspersky. (2020). *https://latam.kaspersky.com.* Obtenido de https://latam.kaspersky.com/resource-center/definitions/what-is-ransomware

Maroto, J. P. (2009). *El ciberespionaje y la ciberseguridad.* La Rioja: Universidad de la Rioja.

Martínez, R. O. (2009). *Ciberterrorismo.* Alfa Redi, Revista de derecho informático.

MinTIC. (3 de octubre de 2020). *Ministerio de Tecnologías y Comunicaciones*. Obtenido de Ministerio de Tecnologías y Comunicaciones: https://www.mintic.gov.co/portal/inicio/18798:Filtraci-n-de-datos

Moral, L. G. (2014). *Curso de Ciberseguridad y Hacking Ético.* Sevilla: Punto Rojo Libros.

Morgenthau, H. (1948). *Politics among nation.* McGraw-Hill Education. NETSCOUT. (2019). *https://horizon.netscout.com.* Obtenido de https://horizon.netscout.com/?

Pirateque Perdomo, P. (2021). Comunicaciones estratégicas (Stratcom) y Social Media: Su aplicabilidad para el mundo Postwesfaliano. https://esici.edu.co/wp-content/uploads/2022/01/4.-Comunicaciones-estrategicas-enero-2062.pdf

Pirateque Perdomo, P., & Martínez Cruz, D. A. (2022). Espacio exterior: el nuevo tablero de cooperación entre Estados Unidos y Rusia, el papel dominante de las empresas y su desarrollo en Colombia. Perspectivas en Inteligencia, 13(22), 155–173. https://doi.org/10.47961/2145194X.277

Plan Nacional de Desarrollo. (2018). *Pacto por Colombia, Pacto por la Equidad.* Departamento Nacional de Planeación. Obtenido de https://colaboracion.dnp.gov.co/CDT/Prensa/Resumen-PND2018-2022-final.pdf

Política de Defensa y Seguridad. (2019). *Legalidad el Emprendimiento y la Equidad.* Ministerio de Defensa Nacional. Obtenido de https://colaboracion.dnp.gov.co/CDT/Prensa/Resumen-PND2018-2022-final.pdf

Política de Gobierno Digital. (2018). *Manual de Gobierno Digital.* Ministerio de Tecnologías de la Información y las Comunicaciones.

Realpe, M. E. (2012). Amenazas Cibernéticas a la Seguridad y Defensa Nacional.

Reflexiones y perspectivas en Colombia. SAFE. (2019). *TENDENCIAS CIBERCRIMEN COLOMBIA 2019 - 2020.* Bogotá: SAFE.

Santiago, I. V. (18 de enero de 2018). *https://seguridad.cicese.mx.* Obtenido de https://seguridad.cicese.mx/alerta/335/Hacker,-Crackers,-Lamers,-Script- Kiddies-y-Phreakers-Quienes-son

Scopus. (2020). *Scopus Preview*. Obtenido de https://www-scopus- com.ezproxy.umng.edu.co/term/analyzer.uri?sid=e3803c7c100b443e837ed7b4f 66d8e6a&origin=resultslist

Studies, C. F. (2013). *The economic impact of cybercrime and cyberspionage.* McAfee. Trigo, S. (2017). *Ransomware Seguridad, Investigación y Tareas Forenses.* Argentina: Ministerio Publico Buenos Aires.

Universidad Libre. (10 de junio de 2015). *http://www.unilibre.edu.co*. Obtenido de http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152- seguridad-de-la-información

Vera, O. (2009). Cómo escribir artículos de revisión. *Revista Médica de la Paz, 15*. Obtenido de http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S1726-89582009000100010

Waever, O. (1999). Securitization and Desecuritization. *On security*, 46-86.

Zeinab Karake, R. A. (2019). *Enforcing Cybersecurity in Developing and Emerging Economies.* Massachusetts: Edward Elgar Publishing Limited. https://doi.org/10.4337/9781785361333