“Análisis de las nuevas tecnologías en las TIC y el mando y control (oportunidades y amenazas)”

Saltos Narváez, Hugo Fabián

Vicerrectorado de Investigación, Innovación y Transferencia de Tecnología

Centro de Posgrados

Maestría en Defensa y Seguridad

Trabajo de titulación, previo a la obtención del título de Magíster en Defensa y Seguridad mención Estrategia Militar

Tcrn. E.M Narváez Valencia, Santiago Mauricio

30 de octubre del 2021

30/10/21 9:44 Tesis

Informe de originalidad

NOMBRE DEL CURSO
Tesis Revisión 5

NOMBRE DEL ALUMNO
HUGO FABIAN SALTOS NARVAEZ

NOMBRE DEL ARCHIVO
HUGO FABIAN SALTOS NARVAEZ - Tesis

SE HA CREADO EL INFORME
29 oct 2021

Resumen

Fragmentos marcados	24	5 %
Fragmentos citados o entrecomillados	10	1 %

Coincidencias de la Web

infoteknico.com	9	2 %
disenowebakus.net	6	1 %
losrecursoshumanos.com	5	1 %
universidadeuropea.com	3	0,7 %
siagconsulting.es	1	0,3 %
wikipedia.org	2	0,2 %
stringfixer.com	1	0,2 %
gabaformacion.com	1	0,2 %
artsandculture.google.com	1	0,2 %
investigaliacr.com	2	0,2 %
facebook.com	1	0,1 %
esge.edu.pe	1	0,1 %
tesisdeceroa100.com	1	0,1 %

Firma:

Firmado electrónicamente por:
SANTIAGO MAURICIO NARVAEZ VALENCIA

Tcrn. E.M Narváez Valencia Santiago Mauricio

Director

C.C.: . 1708650096.

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA
CENTRO DE POSGRADOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, **"Análisis de las nuevas tecnologías en las TIC y el mando y control (oportunidades y amenazas)"** fue realizado por el señor Saltos Narváez, Hugo Fabián el mismo que ha sido revisado y analizado en su totalidad, por la herramienta de verificación de similitud de contenido; por lo tanto, cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 30 de octubre del 2021

Firma:

Firmado electrónicamente por:
SANTIAGO MAURICIO
NARVAEZ VALENCIA

Tcrn. E.M Narváez Valencia, Santiago Mauricio

Director

C.C.: . 1708650096.

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

RESPONSABILIDAD DE AUTORÍA

Yo, **Saltos Narváez, Hugo Fabián**, con cédula de ciudadanía nº 1713078119, declaro que el contenido, ideas y criterios del trabajo de titulación***: "Análisis de las nuevas tecnologías en las TIC y el mando y control (oportunidades y amenazas)"*** es de mí autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 30 de octubre del 2021

Firma (s)

Firmado electrónicamente por:
HUGO FABIAN
SALTOS
NARVAEZ

Saltos Narváez, Hugo Fabián

C.C.: 1713078119

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CENTRO DE POSGRADOS

AUTORIZACIÓN DE PUBLICACIÓN

Yo, **Saltos Narváez, Hugo Fabián**, con cédula de ciudadanía nº 1713078119, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: ***"Análisis de las nuevas tecnologías en las TIC y el mando y control (oportunidades y amenazas)"*** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 30 de octubre del 2021

Firmado electrónicamente por:
HUGO FABIAN SALTOS NARVAEZ

Saltos Narváez Hugo Fabián

C.C.: 1713078119

Dedicatoria

El presente trabajo lo dedico a mi familia, en especial a mi esposa e hijos, ya que gracias a su comprensión y apoyo han permitido que mis esfuerzos sean encaminados a la consecución de este logro en mi vida y mi carrera profesional.

Hugo Fabián

Agradecimiento

Agradezco a la Academia de Guerra del Ejército, y a todos quienes la conforman, y hacen posible que todos quienes reciben una educación integral en sus aulas puedan desarrollar todo su potencial en la vida militar, para beneficio de la sociedad ecuatoriana.

Saltos Narváez, Hugo Fabián

Índice General

Índice de Tablas

Índice de Figuras

Resumen

La capacidad de mando y control busca disponer de los sistemas de información y sistemas de comunicaciones que integren los niveles estratégico, operacional y táctico, que permitan ejercer, de forma rápida y eficaz, las funciones asignadas en la conducción de operaciones y la gestión de crisis. El presente trabajo de investigación analizará cual es la influencia de la capacidad tecnológica de las Tecnologías de la información y Comunicación (TIC) en la transformación de la capacidad de mando y control de la Fuerza Terrestre durante el año 2020. En las operaciones militares de ámbito interno en el año 2019 se pudo determinar falencias en distintas capacidades, y, entre ellas la capacidad de mando y control. Para el desarrollo de la investigación se utilizará el método cualitativo – cuantitativo, con lo cual, se espera tener datos relevantes con respecto a la aplicación de las nuevas tecnologías en las TIC para caracterizarlas y evaluarlas con el fin de desarrollar una propuesta de optimización de su gestión, en la capacidad de mando y control, y de esta manera contribuir al fortalecimiento institucional y al desarrollo del país, al garantizar la seguridad integral determinada en la constitución.

Palabras clave:

- **TIC**
- **MANDO Y CONTROL**
- **CAPACIDADES MILITARES**
- **OPERACIONES MILITARES**
- **ÁMBITO INTERNO**

Abstract

The command-and-control capacity seeks to have information systems and communications systems that integrate the strategic, operational and tactical levels, which allow the functions assigned in the conduct of operations and crisis management to be carried out quickly and efficiently. This research work will analyze what is the influence of the technological capacity of Information and Communication Technologies (ICT) in the transformation of the command-and-control capacity of the Land Force during the year 2020. In field military operations In the year 2019, it was possible to determine shortcomings in different capacities, and, among them, the command and control capacity. For the development of the research, the qualitative - quantitative method will be used, with which, it is expected to have relevant data regarding the application of new technologies in ICT to characterize and evaluate them in order to develop a proposal to optimize their management, in the capacity of command and control, and in this way contribute to the institutional strengthening and development of the country, by guaranteeing the integral security determined in the constitution.

Keywords:

- **ICT**
- **COMMAND AND CONTROL**
- **MILITARY CAPABILITIES**
- **MILITARY OPERATIONS**
- **INTERNAL SCOPE**

Capítulo Primero: El Problema

Planteamiento del Problema

La capacidad de mando y control busca disponer de los sistemas de información y sistemas de comunicaciones que integren los niveles estratégico, operacional y táctico, y permitan ejercer, de forma rápida y eficaz, las funciones asignadas en la conducción de operaciones y la gestión de crisis (Comando Conjunto de las Fuerzas Armadas 2019).

El objetivo de esta capacidad es “alcanzar la superioridad en la información, decisión y ejecución mediante un eficaz sistema integrado” (Comando Conjunto de las Fuerzas Armadas 2019). Esta capacidad tiene un significativo efecto multiplicador de la fuerza al potenciar, entre otras, sus capacidades de movilidad, supervivencia, enfrentamiento y sostenimiento. Es así que en la actualidad la dependencia de la tecnología de esta capacidad militar es más recurrente, ya que el desarrollo de las amenazas y la necesidad de contar con información fiable y verificable es indispensable para la toma de decisiones, de esta manera el flujo de información debe ser seguro, a tiempo y disponer de los canales adecuados, para obtener respuestas y acciones inmediatas según la demanda de las operaciones u objetivos planteados.

Es así que el desarrollo y optimización de la capacidad de mando y control depende de muchos factores, y uno de los más influyentes corresponde a la gestión de la información y la comunicación, para ello, la aplicación adecuada de las Tecnologías de la información y la comunicación (TIC) es fundamental. Sin embargo, su real aprovechamiento depende de las características tecnológicas de las herramientas que sustentan estos recursos, constituyéndose en un elemento trascendental para la evaluación de esta capacidad militar.

La utilización efectiva de las TIC en la capacidad mando y control puede ser determinante en los resultados esperados y en la efectividad de las operaciones militares

que dependen de la capacidad mencionada (Persson, 2014). Mientras que por el contrario las deficiencias en la utilización de este tipo de tecnologías pueden tener consecuencias en el desarrollo normal de las actividades u operaciones asignadas, en la integridad de quienes efectúan las mismas y, en la seguridad y Defensa del Estado.

Se puede decir que una de las mejores formas de detectar falencias, sucede en la práctica, y específicamente en el campo militar en la aplicación de las capacidades en situaciones reales (García Martín 2017), en donde se pude evaluar la efectividad de las mismas. Es así que, durante los acontecimientos acaecidos en operaciones de ámbito interno durante el año 2019 se ha podido determinar falencias en distintas capacidades y entre ellas la capacidad de mando y control (Ministerio de Gobierno 2019). Esto ha constituido un hecho relevante en la planificación de la fuerza, para aprender y corregir posibles errores para anular vulnerabilidades y enfrentar amenazas posteriores en base a lo aprendido.

Otro aspecto relevante para evaluar la influencia de las TIC en la capacidad de Mando y Control constituye el desarrollo de la pandemia durante el año 2020 lo cual hizo prioritaria a la utilización de las TIC en procesos de capacitación y operativos (El Telégrafo 2020), en todas las áreas de influencia de las capacidades militares y en especial de la capacidad señalada. Es así que el ámbito militar también tuvo que afrontar la emergencia sanitaria en todas sus áreas inicialmente disponiendo de los recursos tecnológicos existentes, con lo cual se pudo percibir problemas identificados como deficiencias tecnológicas, lo cual ha creado inconvenientes específicos en la gestión de la información y la comunicación de la capacidad de mando y control y su relación con otras capacidades militares.

Como se ha podido observar estos hechos y puntuales han permitido percibir de mejor manera la importancia de las TIC en la capacidad de mando y control en un contexto real y práctico. Y constituyen elementos fundamentales para el análisis de la

influencia, determinación de deficiencias y necesidades y posibles soluciones viables a los problemas encontrados. En este contexto a continuación se plantea la formulación del problema en forma de interrogante.

Formulación del Problema

¿Cuál es la influencia de la deficiencia tecnológica de las TIC en la transformación de la capacidad de mando y control de la Fuerza Terrestre durante el año 2020?

Preguntas de Investigación

¿Cuál es la deficiencia tecnológica que existe en la actualidad en las TIC que utiliza la capacidad de mando y control en la Fuerza Terrestre?

¿El proceso de transformación de la capacidad de mando y control implica la actualización tecnológica de las TICS que utiliza para el desarrollo de sus actividades?

¿Cómo se puede determinar las necesidades tecnológicas de las TICS de la capacidad de mando y control?

Objeto de Estudio

Capacidades militares

Campo de Acción

Seguridad y Defensa

Delimitación de la Investigación

Delimitación Temática

Tecnologías de la Información y la Comunicación

Delimitación Espacial

Ejército Ecuatoriano

Delimitación Temporal

Año 2020.

Justificación de la Investigación

A nivel global la tecnología influye en todos los aspectos de la vida y el desarrollo humano. En el ámbito militar la influencia de la tecnología trasciende del desarrollo de armas al desarrollo y transformación de sus capacidades. Es así como los diferentes ejércitos del mundo adoptan y desarrollan aplicaciones para optimizar sus actividades y las operaciones inherentes a su función en la defensa y la seguridad de sus territorios.

A nivel regional los procesos de desarrollo y transformación de las capacidades militares han sido la respuesta al desarrollo de amenazas no convencionales, enmarcadas en lo que se denomina guerras asimétricas o guerras no convencionales (Ecuador, 2018) , así como también a funciones relativas a la seguridad interna o integral que como en el Ecuador ha determinado el desarrollo y especialización de nuevas capacidades militares.

En el Ecuador el desarrollo y transformación de estas capacidades militares requieren de un conocimiento pleno de las necesidades para enfrentar dichas amenazas, pero además de una actualización tecnológica permanente que permita optimizar las actividades y efectivizar las operaciones militares asignadas. Específicamente la capacidad de mando y control requiere de una concepción clara de sus características y de la relación que estas tienen con la gestión de la información para la toma de decisiones (Ecuador, 2018). Este vínculo que esta capacidad posee con la información, determina

en la actualidad una necesidad de contar con tecnología que le permita una gestión de la información eficaz, eficiente e influyente en la toma de decisiones que permitan establecer una comunicación frecuente, monitorear el dispositivo de las tropas y mantener la seguridad de la información durante todos los procesos, mediante la utilización de herramientas tecnológicas como las denominadas TIC.

Es así como la calidad de las TIC puede ser determinante para la consecución de los objetivos de la capacidad de mando y control y por extensión en las capacidades militares relacionadas a esta (Ecuador, 2018). De esta manera conocer las necesidades y deficiencias tecnológicas de las TIC es un elemento fundamental en el proceso de transformación de capacidades militares y específicamente en la capacidad de mando y control vinculada directamente a la gestión de la información y conocimiento y a la toma decisiones.

Es, en este contexto que se plantea la importancia de la presente investigación, en función de su concepción como en una herramienta de apoyo al proceso de transformación de la capacidad de mando y control y por influencia de la misma, al resto de capacidades de la Fuerza Terrestre; y de esta manera contribuir al mejoramiento institucional y la Defensa de la Patria como respuesta al mandato constitucional , la Planificación Estratégica Institucional y la Planificación para el Desarrollo Nacional “Toda una Vida” (Ecuador, 2019) .

Objetivos de la Investigación

Objetivo General

Analizar la influencia de la capacidad tecnológica de las Tecnologías de la información y Comunicación (TIC) en la transformación de la capacidad de mando y control de la Fuerza Terrestre durante el año 2020.

Objetivos Específicos

- Determinar las deficiencias tecnológicas que existen en la actualidad en las TIC que utiliza la capacidad de mando y control en la Fuerza Terrestre.
- Establecer si la transformación de la capacidad de mando y control requiere de actualización tecnológica permanente de las TIC de que dispone.
- Desarrollar un método para determinar las necesidades tecnológicas de las TICS de la capacidad de mando y control de forma permanente.
- Determinar un método adecuado para la optimización y utilización adecuada de las tecnologías de información disponible.

Capítulo Segundo: Marco Teórico

Antecedentes de la Investigación

La ejecución del comando y control militar en la actualidad se ha formado a la luz de los pronósticos previos de futuras innovaciones tecnológicas y las suposiciones de lo que pueden proporcionar a la toma de decisiones (Cubeiro, 2018). En este contexto, el desarrollo, y la utilización adecuada de las TIC ha incrementado el aprovechamiento de la información, que, con la disponibilidad de medios tecnológicos adecuados, el procesamiento y la interacción con los datos efectiviza y optimiza los resultados programados.

En el campo de la investigación relacionada con las teorías de la información actual muchas teorías muchas teorías se han desarrollado en paralelo al desarrollo tecnológico y se entrelazan con equivalentes en la investigación militar (Ríos & Valdivieso, 2016). Estos esfuerzos de investigación se extienden entre, los tecnicismos de los sistemas de información y comunicación y los cambios sociales en los cuales se desenvuelven. A partir de esto, han surgido visiones que describen cómo las nuevas tecnologías empleadas el comando y control militar, podrían o deberían diseñarse para el futuro. Bajo esta perspectiva la tecnología de las TIC puede resultar primordial en el respaldo de la ejecución del comando y control, con la premisa de que estas herramientas tecnológicas simplificarán el trabajo para que los comandantes puedan monitorear cambios, o analizar un conjunto de datos y tomen decisiones sobre cómo actuar apropiadamente sobre la información proporcionada.

El estado actual de los sistemas de apoyo a la decisión está marcado por la multiplicidad y transitoriedad de los vehículos de información que los alimentan (Lucena & Porras, 2016). El ámbito de su aplicación es amplio y decisivo en el campo de batalla

moderno, que se caracteriza por el uso extensivo de equipos tecnológicamente avanzados.

Ese hecho, aunque no excluyente, caracteriza la acción de las Fuerzas Armadas modernas al enfatizar su importancia debido al carácter crítico de la información que fluye en los sistemas de mando y control. La tecnología juega un papel clave en este contexto, no solo como garante de la eficacia de los sistemas de información existentes, sino también como la mejor manera de hacer que esos sistemas garanticen la seguridad de la información.

Los importantes avances tecnológicos presenciados en las áreas de telecomunicaciones y sistemas de información ha influenciado para redefinir y reestructurar nuevos y viejos conceptos vinculados al flujo y uso de la información, incluyendo la concepción y la conceptualización adecuada de términos como la digitalización del campo de batalla, la integración y globalización de las comunicaciones, juegos de guerra virtuales (Ríos & Valdivieso, 2016), Internet militar, vigilancia a través de la ciberdefensa, etc. que se encuentren en el lenguaje común de la planificación y modernización de las Fuerzas Armadas.

Por su creciente importancia, este tema es actualmente objeto de un largo debate tanto en el ámbito militar como en el civil, en un momento en el que se asiste a la progresiva internacionalización de los conflictos y de la economía mundial, donde la globalización es el término operativo en cualquier ámbito.

La nueva era, en la que la ciencia y la industria juegan un papel determinante en el poder de las Fuerzas Armadas. El éxito de las organizaciones que se han adaptado al mundo moderno de las redes informáticas, las comunicaciones y el procesamiento de datos, y el fracaso de las que no lo hicieron, es un argumento convincente para la introducción de nuevos procesos y procedimientos de comando y control en el ejército (Fojón, 2019), el cual bajo ninguna circunstancia puede desestimar a la importancia de la

tecnología en función del desarrollo de las amenazas modernas cuyas variante han aprovechado el desarrollo de la tecnología en todos los ámbitos que han incursionado, mediante actividades ilegales y legales en el contexto de los intereses nacionales y en su afán de mantener impunidad y anonimato.

Es así que existen diversos estudios que relacionan a la tecnología con la capacidad militar de mando y control, por la importancia de la misma en la gestión de la información y la toma de decisiones, sin embargo, no existe una especificidad con respecto a las aplicaciones prácticas reales, pero si se puede encontrar ejemplos de cómo distintas tecnologías utilizadas en las TIC pueden ser de gran ayuda al ámbito de acción del mando y control en los ejércitos del mundo.

Fundamentación teórica

TIC (tecnología o tecnologías de la información y las comunicaciones)

Las TIC, o tecnología (o tecnologías) de la información y las comunicaciones, son la infraestructura y los componentes que permiten la informática moderna sea aplicada e integrada adecuadamente a la transmisión, procesamiento y almacenamiento digitalizado de la información (Díaz & Pérez, 2011). Aunque no existe una definición única y universal de TIC, el término se acepta generalmente para significar todos los dispositivos, componentes de red, aplicaciones y sistemas que combinados permiten a las personas y organizaciones interactuar en el mundo digital.

Componentes de un sistema de TIC

En la actualidad las TIC abarcan el campo del Internet como la tecnología móvil respaldada por redes inalámbricas dedicadas. También incluyen tecnologías de telefonía fija, transmisiones de radio y televisión, y actualmente a la inteligencia artificial y la

robótica (Méndez, 2018), de igual manera en el ámbito militar existen aplicaciones específicas como, redes de datos, sistemas de manejo de las operaciones, sistemas de inteligencia y sistemas logísticos.

Las TIC en ocasiones se utilizan como sinónimo de TI (para tecnología de la información); sin embargo, las TIC generalmente abarcan una lista más amplia y completa de todos los componentes relacionados con las tecnologías informáticas y digitales que las TI (Romero & Rivera, 2019).

La lista de componentes de las TIC aumenta con el desarrollo constante de tecnología (Romero & Rivera, 2019). Sin embargo, las TIC hacen referencia también a las aplicaciones de todos esos diversos componentes, es decir de su software aplicativo o de sustento. Es en este contexto en donde se puede encontrar el potencial real de las TIC.

La integración de las TIC con sistemas informáticos es en la actualidad una constante, fundamentalmente por los beneficios que brinda la interactividad e interdependencia de los procesos que realizan las organizaciones que cuentan con estos elementos, así la globalización y la gestión de información en tiempo real son cada vez más comunes en el mundo de las TIC las cuales , según los datos proporcionados o a los cuales se tiene acceso determinan sus necesidades de actualización lo que a su vez impulsa la innovación. La integración de las TIC a la los sistemas informáticos ha permitido a las organizaciones reducir los costos de transacción, incluidos los relacionados con el transporte, la comunicación, los procesos y el inventario y es por eso que organizaciones de diferentes sectores y tamaños están utilizando actualmente las TIC para transformar sus formas de hacer negocios, integrando procesos, y mejorar la productividad y las relaciones entre socios. Por tanto, la competencia ya no será entre procesos productivos sino en la actualización tecnológica de estos, dado que mundo está

interconectado y las TIC son necesarias para afrontar adecuadamente el dinamismo competitivo.

Impacto social y económico de las TIC

Las TIC se aprovechan para transacciones e interacciones económicas, sociales e interpersonales. Las TIC han cambiado casi disruptivamente la forma en que las personas trabajan, se comunica, y se relacionan. Es un hecho que las TIC revolucionan continuamente la experiencia humana de todo el espectro tecnológico de las aplicaciones que utiliza (Delgado, 2019). La importancia de las TIC para el desarrollo económico y el crecimiento empresarial es casi inconmensurable, al punto de atribuírseles la Cuarta Revolución Industrial.

Las TIC también sustentan grandes cambios en la sociedad, ya que los individuos han migrado de interacciones personales y cara a cara a interacciones en el espacio digital (Díaz & Pérez, 2011). Esta nueva era se denomina con frecuencia la era digital. Sin embargo, a pesar de todos sus aspectos revolucionarios, las capacidades de las TIC no están distribuidas de manera uniforme. Los países y las personas con mejores recursos económicos disfrutan de un mayor acceso y, por lo tanto, tienen una mayor capacidad para aprovechar las ventajas y oportunidades impulsadas por las TIC.

El Banco Mundial, en 2016, afirmó que más del 75% de las personas en todo el mundo tienen acceso a un teléfono celular. Sin embargo, el acceso a Internet a través de banda ancha fija o móvil sigue siendo prohibitivamente caro en muchos países debido a la falta de infraestructura de TIC. Además, el Banco Mundial estimó que, de la población mundial de 7.400 millones de personas, más de 4.000 millones no tienen acceso a Internet (Banco Mundial, 2016). Además, estimó que solo 1.100 millones de personas tienen acceso a Internet de alta velocidad, esta discrepancia en el acceso a las TIC ha creado la llamada brecha digital.

El Banco Mundial, numerosas autoridades gubernamentales y organizaciones no gubernamentales (ONG) abogan por políticas y programas que tienen como objetivo cerrar la brecha digital proporcionando un mayor acceso a las TIC entre las personas y poblaciones que luchan por pagarlas.

Estas diversas instituciones afirman que quienes no tienen capacidades de TIC quedan fuera de las múltiples oportunidades y beneficios que crean las TIC y, por lo tanto, quedarán aún más rezagadas en términos socioeconómicos. Las Naciones Unidas consideran que uno de sus Objetivos de Desarrollo Sostenible "aumenta significativamente el acceso a la tecnología de la información y las comunicaciones y se esfuerza por proporcionar acceso universal y asequible a Internet en los países menos desarrollados para 2020" (ONU, 2019).

Las ventajas económicas se encuentran tanto en el mercado de las TIC como en las áreas más amplias de las organizaciones y la sociedad en su conjunto.

Dentro del mercado de las TIC, el avance de las capacidades de las TIC ha hecho que el desarrollo y la entrega de diversas tecnologías sea más barato para los proveedores de TIC y sus clientes, al tiempo que brinda nuevas oportunidades de mercado.

Componentes de las TIC y su integración

Aunque se pueden determinar diferentes tecnologías en el desarrollo de las TIC, los componentes de los distintos sistemas o aplicaciones generalmente se encuentran basados en (Romero, Figueroa, Vera, & Parrales, 2018):

- Datos: hechos y cifras en bruto.
- Hardware: componentes físicos.
- Software: nombre que se le da a los programas informáticos.

- Información: datos que se convierten para darle un significado.
- Procedimientos: una serie de acciones que se realizan en un orden determinado para asegurarse de que el sistema funcione sin problemas.
- Personas: los datos los ingresan humanos, por ejemplo, un teclado.

Sin embargo, estos componentes por sí solo no constituyen un elemento que pueda ser aplicado como TIC, de ahí que su complejidad implica la necesidad de concebir que su integración depende del desarrollo adecuado de cada aspecto para que la aplicación o utilidad sea efectiva.

La práctica indica que la integración de los diferentes componentes de las TIC tiene una gran efectividad cuando estos funcionan interdependientemente. Es decir, puede que en un momento dado el aspecto tecnológico de una compañía o institución supere a sus pares (Romero & Rivera, 2019), sin embargo, si esta no se encuentra integrada a los procesos no le bastará para ser realmente efectiva, De igual manera el factor humano que controlará la tecnología o tomará decisiones en base a los resultados es un elemento primordial del sistema, es por eso que es necesario de hablar de sistemas y no de partes independientes. En el campo de la competitividad o en el ámbito de la eficiencia institucional, la efectividad de las TIC es determinada por el conjunto de su aplicación , si cada componente actúa eficazmente no será suficiente si no se sabe aprovechar la utilidad de unas con otras partes, por ejemplo si se cuenta con la mejor tecnología, el mejor software y el mejor elemento humano que gestione las TIC, pero no se encuentra definidos los procesos bases o de aplicación el sistema en su conjunto no será del todo efectivo.

Es por eso que para un verdadero aprovechamiento tecnológico que ofrecen las TIC no hace falta solo la innovación, sino, el determinar bases sólidas de sustento para que estas funcionen, preparando el escenario de desempeño y definiendo objetivos que

se esperan alcanzar tras su implementación (Romero & Rivera, 2019), lo cual determina a su vez un proceso de retroalimentación para prever posibles fallas y poder corregirlas sobre la marcha.

La importancia de las TIC en las organizaciones y el estado

Para las organizaciones e instituciones, los avances dentro de las TIC han supuesto una gran cantidad de ahorros de costos, oportunidades y comodidades. Van desde procesos de negocios altamente automatizados que han reducido costos, hasta la revolución del “Big data” donde las organizaciones están convirtiendo el vasto tesoro de datos generados por las TIC en conocimientos que impulsan nuevos productos y servicios, hasta transacciones habilitadas por TIC como compras por Internet y telemedicina y redes sociales (Monleón, 2015), que brindan a los clientes más opciones sobre cómo compran, se comunican e interactúan.

Pero las TIC también han creado problemas y desafíos tanto a las organizaciones como a las personas, así como a la sociedad en su conjunto. La digitalización de datos, el uso cada vez mayor de Internet de alta velocidad y la creciente red global juntos han llevado a nuevos niveles de delincuencia (Díaz & Pérez, 2011), donde los llamados malos actores pueden tramar esquemas habilitados electrónicamente u obtener acceso ilegal a sistemas para robar dinero, propiedad intelectual o información privada o para interrumpir los sistemas que controlan la infraestructura crítica. Las TIC también han traído la automatización y robots que desplazan a trabajadores que no pueden transferir sus habilidades a nuevos puestos. Y las TIC han permitido que más y más personas limiten sus interacciones con otras, creando lo que algunas personas temen es una población que podría perder algo de lo que la hace humana.

. Las TIC en la defensa

El desarrollo de las TIC ha introducido una variedad de transformaciones en la industria de defensa en términos de avances en sus armas, como armas inteligentes y administración para el campo de batalla en redes, superioridad en el aire y el espacio exterior, vigilancia de combate en tiempo real y multiplicadores de fuerza basados en software.

En cuanto a las armas inteligentes, las TIC han cambiado el rumbo de toda la industria de defensa en casi todas sus áreas. La industria ha producido armas que, con la ayuda de las TIC, se han tornado en armas inteligentes, eficientes y de alta precisión (Persson, 2014). Con su ayuda, se han establecido comunicaciones, más frecuentes o en tiempo real y se ha establecido una comunicación directa para informar el estado del armamento y del personal directamente con los comandantes. Se ha establecido sistemas de monitoreo de armas y objetivos para apuntar al enemigo y destruir con precisión el objetivo sin crear ningún daño a los alrededores o a sus combatientes.

Un ejemplo de desarrollo y aplicación del uso de armas inteligentes son los misiles aire-aire que pueden apuntar a los aviones enemigos con velocidad y precisión absoluta. Otra aplicación de las TIC se encuentra en la fuerza naval, la misma que puede identificar al enemigo y destruirlo o neutralizarlo con una localización basada en vibraciones, y una identificación de objetivos militares en base a software especializado.

En el ámbito del mando y control militar las aplicaciones son varias, y se extienden a todas sus actividades, desde la planificación, adquisiciones, capacitación y gestión de activos efectivos existen aplicaciones de TIC perfectamente aplicables. Estas responsabilidades suelen estar integradas en aspectos clave como el diseño operacional, el monitoreo de persona, equipo y armamento, diseño de adquisiciones, gestión de sistemas informáticos y la gestión de información.

El mantener el ritmo de los avances tecnológicos en curso implica además consideraciones estratégicas y de proceso, para lo cual las Fuerzas Armadas deben permanecer a la vanguardia de la tecnología relacionada con la seguridad, para brindar resiliencia y mitigar el daño potencial si un ciberataque tiene éxito, y en este campo la aplicación de las TIC tiene un gran desarrollo (Díaz & Pérez, 2011). Esto es particularmente importante dados los rápidos ciclos de desarrollo de dicha tecnología. En este aspecto la tecnología no necesita desarrollarse desde cero: las principales instituciones financieras, organizaciones de servicios públicos e incluso otras Fuerzas Armadas ya cuentan con herramientas similares; tales como sistemas de detección de intrusos, software cibernético avanzado y sistemas de monitoreo de redes. Una vez que las Fuerzas Armadas tengan capacidades más sólidas, pueden seguir el ejemplo de ejércitos más avanzados y crear su propia función interna de investigación, desarrollo y prueba, que puede generar sistemas patentados y coordinar la integración con la tecnología que poseen.

Tal es el desarrollo de las TIC que, en la actualidad, se está produciendo tecnología de inteligencia artificial para reemplazar a los soldados en el campo de batalla. Todo esto es posible gracias a las TIC y los avances realizados en el sistema de inteligencia artificial para la industria de la defensa.

Al observar la gestión del campo de batalla centrada en la red, pueden identificarse adelantos en el campo operacional para gestionar el campo de batalla con el uso de las ventajas de las TIC, que permiten un visón real de lo que sucede, reducir tiempos de respuesta y minimizar bajas (Persson, 2014). Con el uso de esta tecnología, el comandante militar puede controlar a su ejército y decidir las acciones a tomar con el conocimiento previo de las fortalezas y debilidades del enemigo en tiempo real. Los beneficios de la gestión del campo de batalla centrada en la red van más allá de la observación de la posición de la fuerza militar en el campo de batalla y de la identificación

de su fortaleza, abarca también la gestión y procesamiento de información en el campo logístico y del entorno geográfico y climatológico.

Los dispositivos centrados en la red ayudan a mejorar la comunicación dentro de las tropas y un líder de su escuadrón puede identificar y clasificar las Fuerzas Armadas amigas y las fuerzas enemigas hostiles, generando más posibilidades de alerta temprana., para colaborar efectivamente en el proceso de mando y control.

La superioridad tanto en el aire como en el espacio ultraterrestre[1] es el mayor avance de las TIC para la industria de defensa y esto facilitó a la misma para producir equipos militares de muy alta gama que son utilizados por las fuerzas aéreas en todo el mundo. Existen muchos dispositivos electrónicos en el mercado con avances en componentes de TIC como aviones interceptores, vehículos aéreos no tripulados y satélites para que los militares monitoreen objetivos continuamente.

Los multiplicadores de fuerza basados en el software aplicativo son los que tienen mayores ventajas para la industria de defensa. Los equipos tecnológicos y sus aplicaciones discutidos anteriormente no son nada si no hay un mecanismo de control automatizado e inteligente que los potencie y permita una mejor toma de decisiones a los comandantes. Debido a que estas fuerzas del ejército alcanzaron su capacidad de manera óptima. Para decirlo de otra manera, con la introducción de las tecnologías de la comunicación e información en el área de la defensa, el enfoque de la industria pasó de los multiplicadores de fuerza basados en hardware a los multiplicadores de fuerza basados en software.

La mayoría de las organizaciones de la industria de defensa tienen departamentos separados dedicados al desarrollo de software. Este software incluye muchos equipos de

[1] Espacio de interés internacional, situado más allá del espacio aéreo, cuya explotación, y utilización, está sometida a un régimen jurídico en los principios de la libertad e igualdad de uso (DRAE, 2021)

hardware como el sistema de gestión del campo de batalla, el radar de largo alcance y el sistema de guía activa de misiles y GPS, etc.

De hecho, para que cualquier organización que quiera incursionar en la industria de defensa global, el desarrollo de software es la mejor opción por el alcance que tienen las TIC. La contribución de ellos en el desarrollo de software militar es muy alta. Sin embargo, la automatización no es completa y depende del control humano y de la toma de decisiones adecuada, por lo que el desarrollo de las TIC se encuentra subyugado a su utilización efectiva y por esto el campo de aplicación en la capacidad militar de mando y control es fundamental para concebir adecuadamente la verdadera aplicación de las TIC en el ámbito de la guerra moderna.

Dimensión estratégica

En el campo estratégico la aplicación de las nuevas tecnologías tiene un campo muy amplio, sin embargo, las aplicaciones en el ámbito militar se fundamentan para cubrir dos objetivos fundamentales que son la toma de decisiones estratégicas y el ámbito de la seguridad. Aunque, no se puede desestimar que el campo de la planificación mediante la aplicación de modelos preventivos y previsorios es un campo que se está desarrollando aceleradamente incluso con tecnología de inteligencia artificial lo cual permite obtener acercamiento a escenarios futuros, desarrollo de amenazas y formas de combatirlas.

La mayoría de los estudios existentes sobre este tema se centran en prever vulnerabilidades en esos ámbitos, que puede poner en peligro los recursos nacionales de alto valor que generalmente se encuentran fuera del campo de batalla y fuera del teatro de proyección de poder de un país, de tal manera que su vulnerabilidad para permanecer oculta afecte a su estrategia militar y a la estrategia de seguridad nacional.

Es así que el área de conflicto emergente donde las naciones pueden usar el ciberespacio para afectar operaciones militares estratégicas y dañar la infraestructura de

información nacional se desarrolla en una dimensión estratégica. La cual merece especial atención y reconocimiento como una nueva faceta legítima de la guerra, con profundas implicaciones tanto para las estrategias militares como de seguridad nacional.

En los últimos años, la nueva cultura e infraestructura del ciberespacio ha evolucionado casi exclusivamente fuera del ámbito militar, aunque la contribución de Internet es bien conocida, y ahora ofrecen nuevas oportunidades para el desarrollo de herramientas en la ciberdefensa.

Gestión de información estratégica

Hoy en día, la mayoría de los países industrializados como los EE. UU. Ya tienen una cantidad impresionante de recursos basados en información, incluidos sistemas complejos que controlan la energía eléctrica, la circulación de divisas, el tráfico aéreo, el petróleo, el gas y otros elementos que dependen de la información. Los aliados de Estados Unidos y los posibles socios de la coalición dependen igualmente de varias infraestructuras de información. Conceptualmente, cuando un enemigo potencial intenta dañar estos sistemas mediante técnicas de guerra de información, inevitablemente adquiere connotaciones estratégicas (Molander & Riddle, 2018). El escenario anterior contiene un aspecto fundamental de la guerra de información estratégica: no hay "primera línea". Los objetivos estratégicos ubicados en los EE. UU. Pueden ser tan vulnerables a este tipo de ataque como sus sistemas (comando, control, comunicaciones e inteligencia) ubicados en el teatro de operaciones. Al responder a ataques de guerra de información de esta naturaleza, la estrategia militar no puede permitirse centrarse únicamente en su área de interés al realizar y respaldar operaciones. En la actualidad, se debe examinar en detalle todas las implicaciones de la guerra de la información para las infraestructuras que dependen de la gestión libre de la información.

Efectos físicos

El uso de las tecnologías de la información puede contribuir para el manejo de armas físicas, que podrían incluso destruir componentes físicos de un sistema de seguridad. Una consecuencia directa de esto es la correspondiente denegación de servicios, es decir dejar a un sistema, página web, o servicios básicos, fuera de servicio, con lo cual indirectamente se afecta a otro tipo de tecnologías. Aunque la complejidad asociada a este tipo de armas es baja y su uso es lineal, sin embargo, su peligrosidad es latente. La s amenazas actuales, cuentan con una amplia gama de medios que abarcan sistemas de armas tradicionales como misiles, explosivos, sabotajes, etc., para lo cual la preparación tecnológica de un sistema de defensa es fundamental. También están en desarrollo las denominadas armas de energía dirigida (Molander & Riddle, 2018). Estas armas, también conocidas como armas de radiofrecuencia, son dispositivos que destruyen mediante la emisión de radiación electromagnética en una radio frecuencia con una longitud de onda superior a 1 mm (una frecuencia inferior a 3000 GHz). Este tipo de pulso específico podría causar un daño serio en estaciones informáticas con irreparables pérdidas de información. Estas armas se consideran un avance muy importante porque permiten el uso de fuerza no letal.

Efectos en la concordancia operativa

La concordancia operativa es fundamental para el funcionamiento el sistema y en el campo tecnológico las tecnologías que impidan un acceso ilegal o no autorizado a sistemas para impedir este tipo de accesos, es trascendental y dependen del diseño del sistema informático fundamentalmente.

En este sentido existen armas que producen efectos sintácticos diseñados para atacar la lógica operativa de un sistema de información introduciendo retrasos o

comportamientos impredecibles en su funcionamiento. Corresponde a la creación de virus informáticos, así como sus contramedidas (software antivirus). Actualmente, existen entornos de programación en el mercado que "incuban" virus según los deseos del atacante, los alcances de los daños a los sistemas de defensa solo dependen de la preparación tecnológica de los sistemas y de las vulnerabilidades que presenten. El objetivo de esta clase de arma es controlar o desactivar la lógica de las redes y sistemas de información objetivo (Molander & Riddle, 2018). Al usar el software del sistema operativo u otras herramientas del sistema, un virus puede hacer que el sistema funcione de manera diferente a lo esperado o simplemente experimentar retrasos importantes en su ejecución, pero también pueden enfocarse en el robo o manipulación de información. Aquí radica el axioma central de la guerra de información: controle los sistemas de información del enemigo y controlará su proceso de toma de decisiones y su capacidad para ver y comprender los eventos. En ese caso, no hay necesidad de destruir la información o los sistemas del enemigo en el caso de poder controlarlo. El uso de virus como arma de guerra de información tiene como objetivo designado el componente estructural de la infraestructura de información, es decir, la lógica operativa del sistema. Como tal, el uso de este tipo de arma se vuelve algo complejo e ilegal, para lo cual los sistemas de defensa deben estar actualizados con tecnología predictiva, en el campo de mando y control por las características de la capacidad militar es fundamental el contar permanentemente con actualizaciones tecnológicas que permitan detectar este tipo de amenazas o en el caso de ataques, neutralizar las amenazas y eliminarlas.

Ataque a los sistemas de mando y control

El ataque a los sistemas de mando y control se lleva a cabo mediante acciones que dificultan que el enemigo controle sus fuerzas y se comunique con ellas. Esto encarna uno de los principios más antiguos de la guerra, la capacidad de tomar decisiones más

rápido que el oponente y luego actuar de acuerdo con esas decisiones. El ciclo de decisiones no contiene misterios, es un hecho. Todo lo que se hace, se basa en ciclos de decisión. En el ámbito militar, el ciclo de decisión se puede resumir en el acrónimo OODA (Observar, Orientar nuestra atención hacia lo que acaba de suceder, Decidir cómo proceder y Actuar). La guerra de información puede, por ejemplo, negar la observación.

La falta de información impide orientar adecuadamente la atención para tomar una decisión y, lo más importante restringe la actuación de forma eficaz.

Aporte de las TIC en la toma de decisiones

Dentro de la gestión estratégica, precisamente en el proceso de toma de decisiones, siendo un área importante de la gestión empresarial e institucional, en los países en desarrollo el vínculo entre las TIC y la gestión estratégica, específicamente el papel de las TIC en el proceso de toma de decisiones estratégicas es un tema de investigación actual pero ya desarrollado.

Aunque un modelo participativo tradicional en la toma de decisiones no solo facilita la implementación de decisiones, sino que también ayuda a facilitar la comunicación entre los involucrados en el proceso, no es menos cierto que los procesos carentes de herramientas tecnológicas, son más susceptibles de fallas que aquellos que se respaldan en la tecnología para la toma de decisiones. La utilización de tecnologías virtuales, por ejemplo, pueden acercar a miembros que antes, si no podían estar presentes prácticamente se prescindía de sus valiosos aportes en el contexto de la participación con variables en tiempo real.

Es así que la información que se gestiones no solo debe considerar las fuentes o el volumen de la misma para que pueda influir en la toma de decisiones, sino que, su gestión debe considerar características que debe presentar la misma para que la generación de conocimiento de influencia en la toma de decisiones debe basarse en la veracidad de la

misma, la posibilidad de que esta pueda ser actualizada en cualquier momento y en que de acuerdo a las posibilidades pueda ser en tiempo real. Incluir este tipo de características en la gestión de la información pude ser determinante en la toma de decisiones en el ámbito militar.

De igual manera la detección de errores con herramientas tecnológicas ha permitido un avance en el tiempo de los procesos para optimizarlos y hacerlos más efectivos. Actualmente, se utilizan una serie de herramientas tecnológicas de coordinación y gestión de información para asegurar que la participación en la toma de decisiones (consulta, delegación, reunión y comités) y el proceso de participación en la toma de decisiones tenga un espectro más amplio de información inicialmente y luego de reducción de riesgos y errores propios de la gestión humana.

Esto a su vez a desencadenado software vinculado a la toma de decisiones basado en la predicción y la probabilística, que gestiona datos y alternativas de solución a problemas frecuentes, aunque, también en los últimos años se ha desarrollado software basado en inteligencia artificial que aprende de errores o alternativas de solución frecuentes.

Seguridad operativa

La seguridad operativa está diseñada para garantizar la preservación de la información relevante (secretos) así como el lugar donde éstos, se guardan. Esto se logra salvaguardando información y documentos secretos en lugares seguros, asegurando así que los mensajes electrónicos estén codificados y el enemigo no pueda acceder a ellos fácilmente, y entrenando a las tropas para que guarden información importante solo para ellos mismos.

Conocido como entrono de seguridad operativa en el mundo empresarial civil, este concepto dio lugar a algunos lemas famosos de la Segunda Guerra Mundial, como "labios sueltos hunden barcos" y "el enemigo está escuchando".

La ciberdefensa es un área de preocupación relativamente nueva para los gobiernos y las alianzas militares. La difusión de tecnologías y el bajo costo de los dispositivos aumentaros las amenazas a los sistemas de seguridad estatales. Los ciberataques que tienen como objetivo acceder o eliminar información clasificada generalmente tienen lugar a través de redes de infraestructura de gobiernos, organizaciones e instituciones. Los ciberataques contra redes desplegadas suelen ser menos frecuentes que los que se dirigen a redes de infraestructura. Sin embargo, las consecuencias de este tipo de filtración de información pueden ser drásticamente graves para la seguridad estatal y en el caso del desarrollo de operaciones militares en curso, pueden ser determinantes para la consecución efectiva de las mismas.

El hecho de que los operadores militares subestimen las posibles fugas de información es una de las principales razones del éxito de los ciberataques contra las redes desplegadas. Asumir que no se pueden atacar las redes desplegadas, o que el riesgo es relativamente bajo puede resultar eventualmente un gran error, Para esto los sistemas de ciberdefensa deben basarse en tres niveles de defensa. El primer nivel debe implementar protección estática, como identificación, autorización, protección criptográfica y control de acceso (firewalls o barreras inteligentes). El segundo nivel debe tener mecanismos para recopilar información y monitorear el estado de la red. El tercer nivel debe evaluar constantemente la protección de la red.

La reacción típica cuando se busca una solución a un problema de seguridad es buscar funciones para configurar. Es importante comprender que los problemas operativos no pueden resolverse por completo con funciones, porque la persona que realiza la configuración incorrecta también puede eliminar la función que está destinada

a proteger contra configuraciones incorrectas. Los problemas operativos requieren soluciones operativas y competencia operativa de la organización.

El problema clave con muchas funciones de control operativo es que no siempre pueden evitar que se produzcan errores. Pueden dificultar la ocurrencia de errores, pero una gran parte se enfoca en la detección de errores después de que ocurren. Esto puede, en gran medida, resolver errores de configuración deliberados porque un ingeniero probablemente no violaría la política de seguridad si se sabe que el "ataque" se puede detectar y rastrear hasta el ingeniero. Pero no siempre es posible evitar errores de forma proactiva. Obviamente, esto genera problemas de seguridad.

Muchas organizaciones consideran medidas de seguridad adicionales, de modo que el sistema en general sea más resistente a las configuraciones incorrectas. El uso de varias capas de seguridad se denomina "defensa en profundidad" y es un modelo común en las implementaciones de seguridad. Sin embargo, no se debe agregar capas de seguridad adicionales sin un análisis de riesgos adecuado. Es importante comprender las amenazas, su impacto en la organización y el costo de las medidas de seguridad adicionales.

Soluciones operativas

Los operadores de las tecnologías de información y comunicación son los responsables de su gestión adecuada y responden además a la subordinación jerárquica de acuerdo a la conformación de la organización, en el caso específico de la institución militar, si bien los comandantes no son operadores directos, su responsabilidad sobre el mando y control debe exigir un conocimiento de los procesos operativos, y acerca de la normativa y políticas de la gestión tecnológica y administrativa de los procesos en los que intervengan las TIC.

En este contexto la gestión adecuada determina la toma de decisiones que en caso de ser necesario representen soluciones efectivas, para esto deben existir pautas claras sobre lo que los operadores pueden hacer y lo que no pueden hacer. Es necesario definir rutas de escalada que describan los pasos a seguir si un operador no tiene la autorización requerida para una acción específica. La política de seguridad operativa debe definir claramente las responsabilidades y la autorización, así como las acciones disciplinarias en caso de incumplimientos. La política también actúa como un disuasivo contra configuraciones erróneas deliberadas.

Toda organización que ejecute una red o un sistema de gestión de TIC debe crear procesos precisos que definan y controlen cómo se ejecutan los cambios en la red. Se debe monitorear el estado del hardware, el sistema operativo y las configuraciones, y todos los cambios deben registrarse y ejecutarse de manera controlada. Los registros deben evaluarse y comprobarse para detectar posibles errores de configuración. Los registros también se pueden utilizar para demostrar una infracción deliberada de la política de seguridad operativa. (Para esto, el concepto de control dual es importante y se analiza a continuación).

Control de acceso: es una buena práctica restringir el acceso a los dispositivos de red. Las restricciones de acceso se implementan tradicionalmente en las redes a través de una autenticación normada. Esta medida de seguridad se suele ejecutar, aunque en muchas redes demasiados operadores tienen acceso a los dispositivos de red. Restringir este número a la cantidad mínima de operadores necesaria reduce el riesgo.

Autorización: El acceso que tiene un operador debe restringirse al acceso mínimo necesario para que el operador realice su trabajo. En la mayoría de los casos, no es una buena idea que todos los operadores tengan acceso completo (nivel 15) a los dispositivos. Esta práctica puede ser más difícil de implementar; sin embargo, las simples distinciones,

por ejemplo, quién puede y quién no puede ingresar al modo de configuración, son muy útiles.

Control dual: el control de seguridad y el control de la red no deben ser responsabilidad del mismo grupo. Idealmente, un grupo de seguridad controla quién tiene acceso a qué y un grupo de red ejecuta las acciones de configuración. Normalmente, los registros están controlados por el grupo de seguridad. De esta manera, es mucho más difícil configurar de forma incorrecta los dispositivos de forma deliberada, ya que el equipo de seguridad podría reconocer una configuración incorrecta en los archivos de registro.

Asegurar y verificar: todas las medidas anteriores son intentos activos de detectar un cambio en la red, como un cambio de configuración. También es posible detectar violaciones de políticas analizando el tráfico en la red o el estado de información dinámica como tablas de enrutamiento, tablas ARP, etc. Por ejemplo, los sistemas de detección de intrusos pueden crear alertas cuando se ven flujos en la red que no lo hacen. no corresponde a la póliza. Hay muchas otras formas de monitorear las anomalías del tráfico. Por ejemplo, Cisco IOS NetFlow puede ser fundamental para detectar paquetes mal enrutados en la red y se pueden verificar las tablas de enrutamiento en busca de prefijos de enrutamiento desconocidos o faltantes.

Automatización: generalmente se recomienda automatizar procesos y procedimientos, específicamente los procesos de verificación recurrentes, porque los humanos tienden a pasar por alto detalles en archivos de registro y procesos similares. Los procesos automatizados también tienen menos probabilidades de cometer errores, aunque si ocurre un error, a menudo es sistemático y, por lo tanto, fácilmente detectable.

Puede ser muy difícil implementar un entorno de seguridad operativa integral y algunas medidas (como el control dual) pueden requerir un cierto tamaño de organización para funcionar correctamente. El objetivo debería ser llevar a cabo mejoras incrementales en el proceso de operaciones en general. Por ejemplo, los esquemas precisos de

autorización a nivel de comando pueden ser difíciles de implementar y costosos de operar en redes grandes. Otras partes del proceso de operaciones son mucho más fáciles de hacer cumplir. Por ejemplo, uno de esos mecanismos es un sistema de control dual. Enviar todos los registros de acceso y configuración a un servidor de registros separado, al que los operadores de red no tienen acceso, es un paso hacia desalentar las configuraciones erróneas deliberadas de los dispositivos de red.

Los errores operativos pueden romper las políticas de seguridad y son una preocupación importante tanto para los proveedores de servicios como para las organizaciones en general. La mayoría de los errores operativos no se pueden evitar por completo; sin embargo, es posible reducir el riesgo de error. La capacidad de detectar un error y rastrearlo hasta su origen también podría disuadir a los internos de cometer errores de configuración maliciosos o ayudar a detectar rápidamente los errores del operador.

Las regulaciones de cumplimiento de las organizaciones y en este caso de la institución militar requieren ciertas medidas de seguridad operativa. Los responsables de la gestión de tecnología deben verificar qué regulación se aplica y verificar que se implementen las medidas requeridas.

A menudo es posible proporcionar medidas de seguridad adicionales que no dependen completamente de errores operativos. Sin embargo, antes de implementar medidas de seguridad adicionales, se debe realizar un análisis de riesgo formal para equilibrar el costo de las medidas adicionales con el costo del riesgo incurrido debido a debilidades operativas.

Ciberdefensa en el ámbito ecuatoriano

En el Ecuador el desarrollo de la tecnología ha implicado además la utilización de la tecnología para la gestión empresarial e institucionales en todos los ámbitos de sus actividades. Las instituciones del Estado y entre ellas la institución militar no han

permanecido ajenas a esta inclusión tecnológica. Y ha determinado que diversas instituciones hayan tomado medidas y políticas respecto a la seguridad informática, la defensa contra ataques informáticos y la aplicación y desarrollo de tecnología para la gestión adecuada de la información y la prevención de riesgos informáticos. De igual manera en diversas instituciones se han desarrollado políticas de comportamiento para uso y compartimiento de la información.

Es así que se ha impulsado la creación del plan de gobierno electrónico 2014-2017 (COSEDE, 2014) con el cual se ha impulsado también las políticas de interoperabilidad entre las instituciones del estado y el desarrollo de la política de ciberdefensa, que determinó la creación del Comando de Ciberdefensa a través del cual se han determinado estrategias para contrarrestar ciberataques y la denominada “Ciberguerra” que pudieran darse en contra de entidades críticas para el sector de la defensa (INFODEFENSA, 2021).

Aunque no se tiene aún la percepción real de ataques a la seguridad del estado, los ataques o delitos contra el sistema financiero o contra los organismos electorales que se han dado constituyen también ataques a los sectores estratégicos, es así que las amenazas ya se han presentado, pero no han tenido la atención que implica la potencialidad de sus acciones. Es por eso que se ha desarrollado en la planificación estratégica de los últimos años planes y proyectos para especializar instituciones ante este tipo de ataques y la posibilidad de que estos se magnifiquen. Pero además en el campo institucional de las Fuerzas Armadas se ha producido la transformación de las capacidades de las Fuerzas Armadas en las cuales ya se tiene una perspectiva más clara para el desarrollo de capacidades relacionadas y específicas a la ciberdefensa.

En concordancia con el Plan Nacional de Seguridad Integral (PNSI) 2017-2021, el Centro de Inteligencia Estratégica desarrollo Plan específico de Inteligencia 2019-2030 (Centro de Inteligencia Estratégica, 2021) en el cual ya se identifica como amenaza prioritaria a “acciones contra el estado en el ciberespacio” parta esto el centro de

inteligencia estratégica gestiona la ciberseguridad desde diferentes ámbitos garantizando la interoperabilidad entre ellos, que incluyen a las Fuerzas Armadas, La policía Nacional, el sector Financiero y al servicio de rentas internas, cabe destacar la importancia que da al sistema al incluir además a todas las instituciones del estado en función de su impacto en el sector estratégico.

Fundamentación conceptual

Tecnología de la información y las comunicaciones

La tecnología de la información y las comunicaciones (TIC) es un término que enfatiza el papel de las comunicaciones unificadas y la integración de las telecomunicaciones la computación e informática, así como el software para la gestión organizacional. El término TIC también se utiliza para referirse a la convergencia de redes audiovisuales y telefónicas con redes informáticas a través de un único sistema. Las TIC son un tema amplio y en constante evolución que baraca cualquier producto o dispositivo que almacene, recupere, manipule, transmita o reciba información en forma digital o análoga o electrónica.

Capacidad tecnológica

La capacidad tecnológica, se puede definir como la capacidad de encontrar y utilizar tecnología para mantener y lograr una ventaja competitiva, es el uso de los recursos y funciones técnicos para mejorar y modernizar la productividad y el desempeño de un producto u organización (Rocha Velandia & Echavarría Suarez, 2017). La capacidad tecnológica hace referencia también a las habilidades de gestión y organización que una organización necesita para utilizar de manera eficiente las tecnologías de hardware y software y para complementar los procesos de cambio tecnológico.

Mando y Control

El mando y control corresponde al ejercicio de autoridad y dirección por parte de un comandante designado adecuadamente y debidamente capacitado, sobre las fuerzas asignadas y adscritas en el cumplimiento de un objetivo institucional o una misión (MIDENA, 2014). Los comandantes realizan funciones de mando y control a través de un sistema de mando y control.

A menudo se considera que el mando y el control como una función distinta y especializada, como la logística, la inteligencia, la guerra electrónica o la administración, con sus propios métodos, consideraciones y vocabulario peculiares, y que ocurren independientemente de otras funciones. Pero, de hecho, el mando y el control abarcan todas las funciones y operaciones militares, dándoles significado y armonizándolas en un todo significativo. Ninguna de las funciones anteriores, ni ninguna otra, tendría un propósito sin comando y control. El mando y control no es asunto de especialistas, a menos que consideremos al comandante como un especialista, porque el mando y control es fundamentalmente asunto del comandante.

El mando y control es el medio por el cual un comandante reconoce lo que debe hacerse y se encarga de que se tomen las medidas adecuadas. A veces, este reconocimiento toma la forma de una decisión de mando consciente, como una decisión sobre un concepto de operaciones. A veces toma la forma de una reacción precondicionada, como en los simulacros de acción inmediata, practicados de antemano para que podamos ejecutarlos reflexivamente en un momento de crisis. A veces toma la forma de un procedimiento basado en reglas, como en el guiado de una aeronave en la aproximación final. Algunos tipos de comando y control deben ocurrir de manera tan rápida y precisa que solo pueden realizarse mediante computadoras, como el comando

y control de un misil guiado en vuelo. Otras formas pueden requerir tal grado de juicio e intuición que sólo pueden ser realizadas por un experto.

Operaciones Militares de ámbito Interno

Operaciones militares de ámbito interno son las acciones militares coordinadas de un estado, en respuesta a una situación referente a la seguridad y defensa en desarrollo dentro del territorio nacional (MIDENA, 2014). Estas acciones están diseñadas mediante un plan militar para resolver la situación a favor del Estado. Las operaciones pueden ser de naturaleza combativa o no combativa y pueden denominarse mediante un nombre en clave con fines de seguridad nacional.

En las operaciones militares de defensa interna se reconoce las siguientes operaciones especiales: operaciones con medios aéreos, operaciones ribereñas, operaciones contraterrorismo, operaciones en áreas fronterizas y operaciones de seguridad de la infraestructura nacional.

Ciberseguridad

La ciberseguridad se refiere al conjunto de tecnologías, procesos y prácticas diseñadas para proteger redes, dispositivos, programas y datos de ataques, daños o accesos no autorizados. La seguridad cibernética o ciberseguridad también puede denominarse seguridad de la tecnología de la información.

La seguridad cibernética es importante porque las organizaciones gubernamentales, militares, corporativas, financieras y médicas recopilan, procesan y almacenan cantidades de datos sin precedentes en computadoras y otros dispositivos (Vargas, recalde, & Reyes, 2017). Una parte significativa de esos datos puede ser información confidencial, ya sea propiedad intelectual, datos financieros, información

personal u otros tipos de datos para los que el acceso o la exposición no autorizados podrían tener consecuencias negativas. Las organizaciones transmiten datos confidenciales a través de redes y a otros dispositivos en el curso de sus negocios, y la seguridad cibernética describe la disciplina dedicada a proteger esa información y los sistemas utilizados para procesarla o almacenarla.

A medida que crece el volumen y la sofisticación de los ciberataques, las organizaciones y organizaciones e instituciones en general, especialmente aquellas que tienen la tarea de salvaguardar la información relacionada con la seguridad nacional, la salud o los registros financieros, deben tomar medidas para proteger su información comercial y personal confidencial (Vargas, recalde, & Reyes, 2017). En el contexto actual de la defensa es prioritario para distintos países que los ataques cibernéticos y el espionaje digital se encuentran entre las principales amenazas para la seguridad nacional, eclipsando incluso al terrorismo.

Para una ciberseguridad eficaz, una organización o institución necesita coordinar sus esfuerzos en todo su sistema de información. Los elementos cibernéticos abarcan:

Seguridad de la red: el proceso de proteger la red de usuarios, ataques e intrusiones no deseados.

Seguridad de las aplicaciones: las aplicaciones requieren actualizaciones y pruebas constantes para garantizar que estos programas estén a salvo de ataques.

Seguridad de terminales: el acceso remoto es una parte necesaria del negocio, pero también puede ser un punto débil para los datos. La seguridad de los terminales es el proceso de proteger el acceso remoto a la red de una organización.

Seguridad de los datos: dentro de las redes y aplicaciones están los datos. La protección de la información de la organización y del cliente es una capa de seguridad separada.

Gestión de la identidad: Básicamente, se trata de un proceso de comprensión del acceso que cada individuo tiene en una organización.

Seguridad de la base de datos y la infraestructura: todo en una red involucra bases de datos y equipos físicos. La protección de estos dispositivos es igualmente importante.

Seguridad en la nube: muchos archivos se encuentran en entornos digitales o "la nube". La protección de datos en un entorno 100% en línea presenta una gran cantidad de desafíos.

Seguridad móvil: los teléfonos móviles y las tabletas implican prácticamente todos los tipos de desafíos de seguridad en sí mismos.

Recuperación ante desastres / planificación de la continuidad del sistema: en caso de una infracción, los datos de un desastre natural u otro evento deben protegerse y el sistema debe continuar. Para esto, necesitará una planificación Educación del usuario final, en el cual los usuarios pueden ser empleados que acceden a la red o clientes que inician sesión en una aplicación de la organización o institución. Desarrollar una capacitación o educación respaldada por buenos hábitos en el mundo tecnológico es fundamental (cambios de contraseña, autenticación, etc.) es una parte fundamental de la ciberseguridad (Navarro, 2020). En el ámbito militar se deben tener consideraciones símiles respecto a la organización empresarial, es decir los usuarios finales aunque se encuentren dentro de la institución militar (comandantes y operadores) tiene las mismas consideraciones respecto a las políticas de uso y restricciones a la seguridad.

Entre los desafíos más difícil en la seguridad cibernética se encuentra la naturaleza en constante evolución de los propios riesgos de seguridad. Tradicionalmente, las organizaciones y el gobierno han centrado la mayoría de sus recursos de seguridad cibernética en la seguridad del perímetro para proteger solo los componentes más cruciales del sistema y defenderse de las golosinas conocidas (Romero, Figueroa, Vera,

& Parrales, 2018). Hoy en día, este enfoque es insuficiente, ya que las amenazas avanzan y cambian más rápidamente de lo que las organizaciones pueden seguir. Como resultado, las organizaciones asesoras promueven enfoques más proactivos y adaptativos a la seguridad cibernética.

En el ámbito militar en donde las amenazas son constantes y pueden tener connotaciones graves para la seguridad y la defensa expertos recomiendan un cambio hacia el monitoreo continuo. y evaluaciones en tiempo real, un enfoque de seguridad centrado en los datos en contraposición al modelo tradicional basado en el perímetro (Ríos & Valdivieso, 2016). recomienda un enfoque de arriba hacia abajo para la seguridad cibernética en el que la gestión corporativa lidera la tarea de priorizar la gestión de la seguridad cibernética. en todas las prácticas comerciales.

En el contexto del desarrollo de amenazas actuales respecto a las ciber tecnologías, se advierte que las organizaciones deben estar preparadas para responder al inevitable incidente cibernético, restablecer las operaciones normales y garantizar que los activos y la reputación de la organización estén protegidos. Estos planes se los considera alternativos o en un ámbito más reciente como respuesta a eventos disruptivos. En el contexto de las FF.AA. es necesario contar con la protección perimetral de todas las redes de datos a fin de mantener la seguridad de la información, y del hardware de sustento (servidores). Es así que los principales centros de datos del CC.FF.AA: y FF.TT: deben preocuparse de la actualización constante de sus sistemas informáticos y de mantener los sistemas de seguridad permanentemente controlados y monitoreados.

Las pautas para realizar evaluaciones de riesgo cibernético se centran en tres áreas clave: identificar las prioridades de la organización o institución y la información más valiosa que requiere protección; identificar las amenazas y riesgos que enfrenta esa información; y describiendo el daño que la organización incurriría en caso de que los datos se pierdan o se expongan indebidamente. Las evaluaciones de riesgo cibernético

también deben considerar cualquier regulación que afecte la forma en que esta recopila, almacena y protege los datos en todas las áreas. En el ámbito militar esta planificación es indispensable dado el riesgo para la seguridad nacional y la presencia constante de amenazas.

Después de una evaluación de riesgo cibernético, es necesario desarrollar e implementar un plan para mitigar el riesgo cibernético, protegiendo las prioridades definidas, en la evaluación además de detectar y responder eficazmente a los incidentes de seguridad. Este plan debe abarcar tanto los procesos como las tecnologías necesarias para construir un programa de seguridad cibernética maduro. Un campo en constante evolución, las mejores prácticas de seguridad cibernética deben evolucionar para adaptarse a los ataques cada vez más sofisticados llevados a cabo por los atacantes.

La combinación de sólidas medidas de seguridad cibernética con una base de empleados educada y preocupada por la seguridad proporciona la mejor defensa contra los ciberdelincuentes que intentan obtener acceso a los datos confidenciales de su organización. Si bien puede parecer una tarea abrumadora, comience poco a poco y concéntrese en sus datos más confidenciales, escalando sus esfuerzos a medida que su programa cibernético madura.

Si bien el contexto de la ciberseguridad es muy amplio en la actualidad, la necesidad de una especificidad en el ámbito militar en relación al desarrollo de capacidades es fundamental, sin olvidar el contexto de desarrollo que requiere de una interoperabilidad, en primera instancia de carácter interinstitucional (Diferentes, fuerzas o armas) y posteriormente de forma interinstitucional con el sector de la defensa y de los sectores estratégicos, así la adaptabilidad del desarrollo de la ciberseguridad al contexto militar es fundamental para la concepción de la defensa moderna del estado.

Ciberdefensa

La ciberdefensa es un mecanismo de defensa de la red informática que incluye la respuesta a las acciones y la protección de la infraestructura digital y el aseguramiento de la información para organizaciones, entidades gubernamentales y otras posibles redes (Vargas, recalde, & Reyes, 2017). La ciberdefensa se enfoca en prevenir, detectar y brindar respuestas oportunas a ataques o amenazas para que no se altere ninguna infraestructura digital o información.

Bases teóricas

La base teórica fundamental para el desarrollo de la defensa se encuentra en las teorías de las relaciones internacionales, es así que la concepción del realismo, el neorrealismo, son, fundamentalmente la base que encuadra los distintos enfoques de desarrollo y concepción del poder y la Defensa de los Estados, y permite comprender al poder nacional y su aplicación en el campo de las relaciones internacionales en la consecución del resguardo de los intereses de los países, incluso en la concepción del poder hegemónico o de acciones preventivas con el fin de mantener la estabilidad del poder o promover un poder hegemónico.

Con el desarrollo de las teorías de las relaciones internacionales como el realismo estructural y el liberalismo se ha argumentado también la importancia de otros factores para comprender a la política internacional, la seguridad de los estados y la seguridad global. Es, bajo estas teorías que la importancia del desarrollo económico de los países, y la generación y mantenimiento de recursos dan otro contexto a las relaciones internacionales, en el ámbito de la seguridad y la defensa al incluir actores vinculados a la sociedad, como la influencia de las minorías y el medio ambiente para comprender la

interacción entre los pueblos. Sin embargo, esto permite una amplia discusión de adherentes y detractores entre el realismo y sus tendencias y el liberalismo.

El desarrollo de las tecnologías de la información es fundamental y valiosa para la sociedad. Los sistemas de TI respaldan los procesos comerciales al almacenar, procesar y comunicar datos comerciales críticos y confidenciales. Además, los sistemas de TI se utilizan a menudo para controlar y supervisar procesos industriales físicos. Por ejemplo, el suministro de energía eléctrica, suministro de agua y ferrocarriles están controlados por sistemas de TI. Estos sistemas de "control" tienen muchos nombres.

También es común permitir que los usuarios se conecten de forma remota a las interfaces de operador, por ejemplo, para que los operadores de procesos puedan conectarse de forma remota cuando estén en servicio de reserva y para que los proveedores puedan realizar el mantenimiento de forma remota. La mayor integración con sistemas organizacionales más administrativos también ha contribuido a un entorno de amenazas modificado. Los sistemas administrativos están, con pocas excepciones, conectados (directa o indirectamente) a Internet. Por lo tanto, la posibilidad de que los sistemas administrativos intercambien datos con sistemas tecnológicos inseguros también es una posibilidad para que atacantes o malware entren en contacto con estos sistemas y exploten sus vulnerabilidades, sin proximidad física, y estas vulnerabilidades pueden convertirse en debilidades y potenciadores de amenazas para os sistemas de defensa del ámbito militar.

El umbral reducido para encontrar y utilizar vulnerabilidades relacionadas con las tecnologías de la información y alcanzar integración más estrecha con los sistemas de seguridad y defensa son dos problemas de seguridad cibernética que se suman al volumen de problemas de seguridad relacionados con la arquitectura y la configuración de los sistemas tecnológicos de uso común no solo en el ámbito militar sino como parte

inherente al comportamiento humano, tomando en cuenta la accesibilidad y dependencia tecnológica de la gestión de la información y de las comunicaciones humanas.

En este sentido el contexto sociológico de la relación del desarrollo de la tecnología y la utilización de la misma en sistemas de seguridad determina la proliferación de malas prácticas ya sea por falta de información, de inobservancia de los riesgos y amenazas o por la simple cotidianidad del manejo de este tipo de herramientas.

Con respecto a lo que pueden decir sobre la seguridad en la era digital. Se argumenta que el enfoque liberal en el pluralismo, la interdependencia y la globalización, el énfasis constructivista en el lenguaje, los símbolos y las imágenes (incluida la "virtualidad") y algunos elementos de los estudios estratégicos realistas (sobre la guerra de la información) contribuyen a la comprensión de la tecnología digital. En este sentido y relacionando lo tecnológico la seguridad en el contexto del desarrollo social, se sugiere que el pragmatismo podría ayudar a cerrar la brecha entre la teoría y la práctica, y superar la naturaleza dualista y competitiva de las teorías de las relaciones internacionales que en la actualidad determinan un mejor desarrollo para alcanzar la “competitividad” que necesariamente debe alcanzar el sector de la defensa para contrarrestar o anular las amenazas.

Fundamentación legal

Base Legal

- Constitución de la República del Ecuador 2008.
- Plan Nacional de Desarrollo 2017-2021 “TODA UNA VIDA”
- Agenda Política de la Defensa.
- Ley Orgánica de la Defensa Nacional.
- Ley de Seguridad Pública y del Estado.

- Esquema gubernamental de Seguridad de la Información
- Estrategia nacional de Ciberseguridad

Hipótesis

La capacidad tecnológica de las TIC utilizadas en mando control no contribuye de manera efectiva con en el proceso de transformación de la capacidad de mando y control del Fuerza Terrestre en el año 2020.

Sistema de Variables

Variable Independiente

Capacidad tecnológica de las TIC en mando y control

Variable Dependiente

Transformación de la Capacidad de Mando y Control y /o las buenas prácticas en el uso de la tecnología disponible.

Conceptualización y Operacionalización de las Variables

Conceptualización de las Variables

Tabla 1

Conceptualización de las Variables de Investigación

Tipo Variable	Variable	Conceptualización
Independiente	Capacidad tecnológica de las TIC en mando y control	Conjunto de condiciones y cualidades de los implementos tecnológicos (hardware y software), y modelos de gestión que sustentan las TIC utilizadas por los comandantes y colaboradores del mando y control del ejército ecuatoriano.
Dependiente	Transformación de la Capacidad de Mando y Control	Proceso de optimización basado en las líneas de transformación de capacidades específicos para la capacidad militar del mando y control del ejército ecuatoriano.

Tabla 2

Cuadro de categorización de las variables

Variable	Dimensiones	Indicadores	Instrumento	Escala valorativa
Capacidad tecnológica de las TIC en mando y control	Deficiencia de capacidad tecnológica de TIC	Inventarios Existencias Proyectos de implementación	Encuesta Entrevista	Existencia Sí o no
Transformación de la Capacidad de Mando y Control	Necesidad de actualización tecnológica	Evaluación Requisitos técnicos para Efectividad	Observación Entrevistas encuestas	Cumplimiento Si No

Capítulo Tercero: Marco Metodológico

Enfoque de la Investigación

La relevancia de las hipótesis para el estudio es el principal punto distintivo entre los enfoques deductivo e inductivo que se aplicaran a la presente investigación. El enfoque deductivo prueba la validez de los supuestos (o teorías / hipótesis) en la mano, mientras que el enfoque inductivo contribuye al surgimiento de nuevas teorías y generalizaciones.

La presente investigación tiene un enfoque mixto; cuantitativo y cualitativo. El enfoque mixto es comprendido por (Tashakkori y Teddlie, 2003, citado en Barrantes, 2014, p.100). como “un proceso que recolecta, analiza y vierte datos cuantitativos y cualitativos, en un mismo estudio”. Este enfoque permitirá obtener datos relevantes en el contexto cuantitativo como la situación de la tecnología aplicada por medio de las TIC en la capacidad de mando y control y la percepción de la aplicación y del contexto de la aplicación de las TIC en la transformación de la capacidad recogida en la valoración de las opiniones de los expertos de forma cualitativa.

Tipos de Investigación

Los tipos de investigación que se utilizará, serán el descriptivo y el exploratorio. De esta manera se analizará las nuevas tecnologías existentes en la TIC de la capacidad de mando y control, en el contexto de oportunidades y amenazas que estas ofrecen. De esta manera se pretende abordar la temática de la investigación de una manera objetiva y detallada, interrelacionando y definiendo las variables de investigación

Población

La población, dentro de la investigación científica es un conjunto de elementos o eventos similares que son de interés para un estudio, investigación o experimento (Hernández Sampieri, Fernández Collado, & Baptista Lucio). Una población estadística puede ser un grupo de objetos existentes o hipotéticos finitos, o potencialmente infinitos, también es atribuible a un grupo de objetos concebidos como una generalización de la experiencia objetiva. Un objetivo común del análisis estadístico es producir información sobre alguna población elegida. Para la presente investigación se define a la muestra en base a los objetivos de la misma de la Comandancia General del Ejército.

Para la estadística aplicada (Inferencial), generalmente se elige un subconjunto de la población (una muestra estadística) y de esta manera poder representar a la población en un análisis estadístico determinado (Hernández Sampieri, Fernández Collado, & Baptista Lucio). La relación entre el tamaño de esta muestra estadística y el tamaño de la población se denomina fracción de muestreo o proporción muestral. De esta manera es posible estimar los parámetros de la población utilizando las estadísticas de muestra adecuadas.

La población está constituida por la Comandancia General del Ejército.

Muestra

Para la determinación de la muestra y dadas las características de la investigación, se ha establecido un grupo finito de personas que por la experiencia en lo concerniente a la planificación y aplicación del uso de las TIC en la capacidad de mando y control pueden aportar significativamente en el proceso de la investigación, es así que se ha determinado la muestra cómo se detalla a continuación:

Tabla 3

Conformación de la muestra

origen	**N°**
Personal de Dirección de Transformación del Ejército	6
Personal de la Dirección de Planificación y Gestión Estratégica de la Fuerza Terrestre	6
Personal de la Dirección de Tecnologías de la Información y Comunicaciones del COMACO	12
Total	**24**

Métodos de Investigación

Inicialmente se utilizará un método hipotético deductivo mediante el cual y partiendo de la hipótesis de la investigación: “La deficiencia tecnológica de las TIC tiene una influencia negativa en el proceso de transformación de la capacidad de mando y control del Fuerza Terrestre en el año 2020.”, se tratará de comprobar o desechar su planteamiento con la ayuda de los métodos, cualitativo y cuantitativo.

Técnicas de recolección de datos

Técnica de revisión bibliográfica

Esta técnica de revisión documental y bibliográfica se utiliza preliminarmente en el proceso de elaboración del marco teórico y conceptual de la investigación, con el objetivo de reunir los más importantes estudios, investigaciones, datos e información sobre el problema formulado (Hernández Sampieri, Fernández Collado, & Baptista Lucio), en función de los objetivos planteados por la investigación. Para esta investigación se utilizarán fuentes bibliográficas primarias, relativas al ámbito militar de la capacidad de mando y control y relacionadas a las nuevas tecnologías de la información. Además, por las características de la investigación se incluyen fuentes secundarias, debido a la

especificidad del tema y la oportunidad de acceder a las mismas ya sea en el entorno académico o profesional y laboral, para respaldar el proceso de la investigación planteada.

Técnica de entrevista

La entrevista de investigación cualitativa busca describir significados de temas centrales o la interpretación de los entrevistados del tema de investigación o la problemática subyacente. Una entrevista de investigación busca cubrir tanto un nivel de hechos como de significado, aunque generalmente es más difícil entrevistar a un nivel de significado. (Kvale, 1996)

Las entrevistas son particularmente útiles para obtener datos relevantes detrás de las experiencias de un participante. El entrevistador puede buscar información detallada sobre el tema y el contexto de su desarrollo. Para la presente investigación se ha desarrollado una entrevista semiestructurada con la cual se podrá obtener datos validados por la experiencia de los participantes, guiados y circunscritos al tema y objetivos de la investigación referentes a las TIC, el mando y control y la problemática de su interacción identificando las oportunidades y amenazas.

Técnica de la encuesta

Una encuesta es un método de investigación que se utiliza para recopilar datos de un grupo predefinido de encuestados para obtener información y conocimientos sobre varios temas de interés. Pueden tener múltiples propósitos y los investigadores pueden realizarlo de muchas formas dependiendo de la metodología elegida y el objetivo del estudio. (Hernández Sampieri, Fernández Collado, & Baptista Lucio). La presente investigación utiliza una encuesta semiestructurada direccionada a personas que tiene

cierto grado de experiencia en el tema de las tecnologías de la investigación, y la capacidad de mando y control en diferentes unidades y departamentos de la institución militar y tomando en cuenta las facilidades tecnológicas telemáticas y las restricciones de bioseguridad relativas a la pandemia actual.

Instrumentos de recolección de datos

Los instrumentos aplicados en la presente investigación corresponden a la encuesta y a la entrevista, con el objetivo de recabar información relevante de la utilización, aplicación de las TIC en la capacidad de mando y control.

Técnicas para el análisis e interpretación de datos

La técnica correlacional será aplicada para la interpretación de datos, provechando además los beneficios del programa informático MS Excel para la aplicación de la estadística descriptiva, para la tabulación y elaboración de gráficos estadísticos que permitan comprender y visualizar el comportamiento de las variables de investigación.

Capítulo Cuarto: Desarrollo de Objetivos Específicos

Para desarrollar los objetivos inicialmente se analizarán los resultados obtenidos en la investigación de campo

Análisis de Resultados

Determinar las deficiencias tecnológicas que existe en la actualidad en las TIC que utiliza la capacidad de mando y control en la Fuerza Terrestre.

1. ¿Considera usted que el uso de las TIC en la capacidad de mando y control es de forma explícita o implícita?

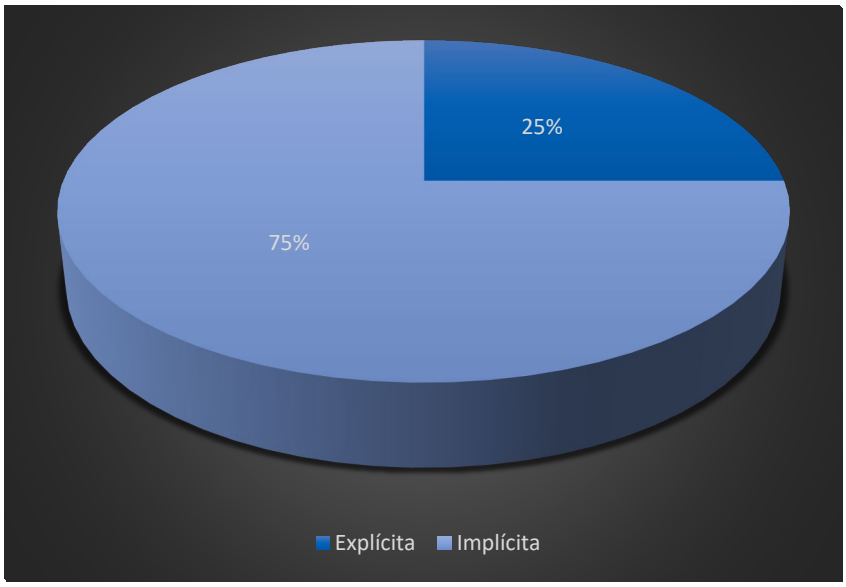
Tabla 4.

Carácter explícito o implícito del uso de las TIC.

Opciones	f	%
Sí	6	25%
No	18	75%
Total	24	100%

Figura 1.

Carácter explícito o implícito del uso de las TIC.



De las respuestas obtenidas de la muestra, se tiene que 6 personas (25%), optaron por explícita, y 18 (75%) optaron por implícita, a la forma de utilizar las TICS.

Como se puede observar una mayoría considerable considera que el uso de las TIC en la capacidad de mando y control se lo hace de forma implícita, para analizar esta respuesta cabe aclarar que mediante la observación y la opinión de los expertos, la utilización de las TIC no tiene un marco normativo o procedimental, en algunos párrafos de la doctrina y procedimientos se hace referencia únicamente como uso de la tecnología, pero además se puedo constatar que la carencia de homologación de tecnologías específicas es una de las cusas para que no se especifique el uso de determinada tecnología aplicativa.

2. De acuerdo a su conocimiento ¿Existen parámetros o normas para la utilización y aplicación de las TIC en la capacidad de mando y control?

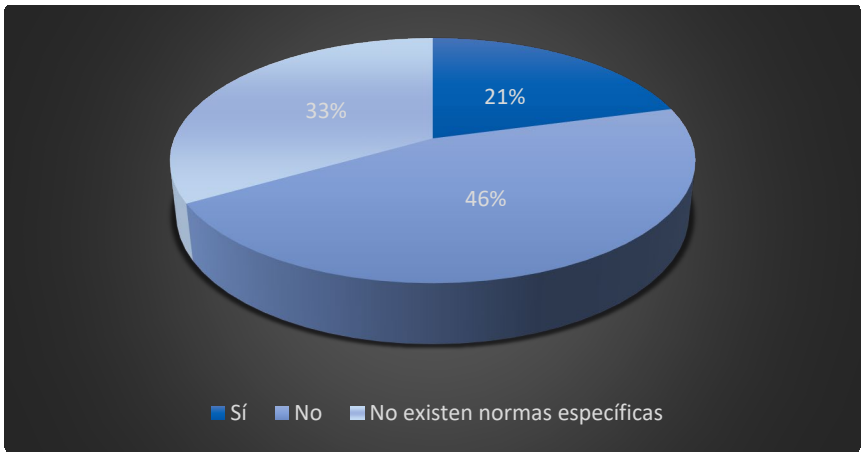
Tabla 5.

Especificidad de normas para la utilización y aplicación de las TIC en la capacidad de mando y control.

Opciones	f	%
Sí	5	21%
No	11	46%
No existen normas específicas	8	33%
Total	**24**	**100%**

Figura 2

Especificidad de normas para la utilización y aplicación de las TIC en la capacidad de mando y control.



Del total de personas que realizaron la encuesta, 5 respondieron que sí (21%), 11 respondieron que no (46%) mientras que 8 respondieron que “no existen normas específicas.”

Ente las opciones de que no y no existen normas específicas forman un grupo mayoritario, lo cual hace suponer que la especificidad de normativa referente al uso del as TIC en la capacidad de mando y control no existe o no está muy clara. Como complemento, en base a la información obtenida en las entrevistas a expertos en el tema,

se pudo contrastar, aunque en forma más amplia se señala que esta falta de especificidad se da porque la utilización de las TIC, es sobreentendida para mejorar los procesos en cada área y además que el uso de la tecnología es casi generalizado para cualquier actividad, sino que no se encuentra especificado o detallado en muchos de los procesos. Cabe mencionar que se señaló que existe diferentes documentos y referencias que promueven el uso adecuado de las TIC, pero también se encuentra implícito en aspectos como: la seguridad de la información, el manejo de las comunicaciones y la generación de respaldos.

3. ¿Qué aspecto considera más relevante en el uso adecuado de las TIC en la capacidad de mando y control? 3 si considera de alta relevancia, 2 con relevancia moderada o media, 1 con baja relevancia y 0 sin relevancia.

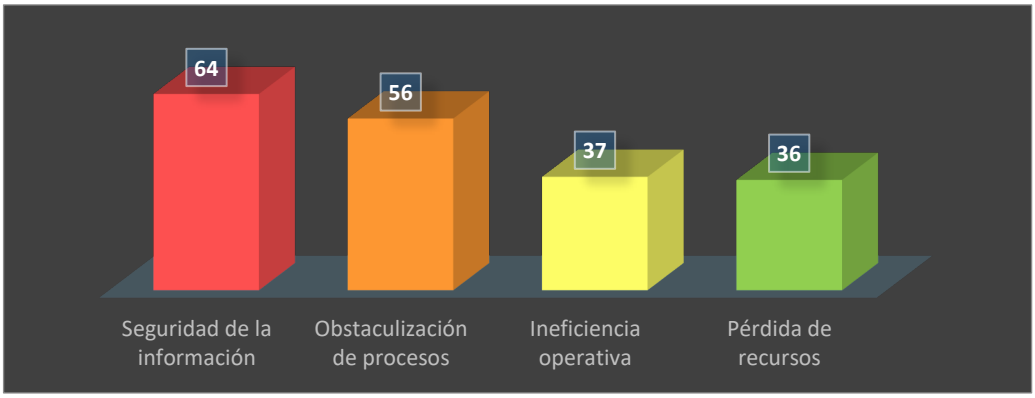
Tabla 6

Relevancia en el uso adecuado de las TIC en la capacidad de mando y control.

Opciones	**3**	**2**	**1**	**0**	**n**	
Actualización tecnológica	16	6	2	0	24	62
Respaldo técnico (asesoramiento y mantenimiento)	6	5	12	1	24	40
Seguridad de la información	14	6	4	0	24	58
Compatibilidad e interoperabilidad	3	11	8	2	24	39

Figura 3

Relevancia en el uso adecuado de las TIC en la capacidad de mando y control.



Para cuantificar la relevancia de las respuestas se utilizó una valoración simple que los encuestados pusieron en cada una de las opciones siendo 3 si consideraba de alta relevancia, 2 con relevancia moderada o media, 1 con baja relevancia y 0 sin relevancia.

De los resultados obtenidos se puede observar que para los encuestados la opción que consideraron más relevante en el uso de las TIC en la capacidad de mando y control es la actualización tecnológica, seguida de la seguridad de la información, el respaldo técnico y por último la compatibilidad e Inter operatividad.

Para analizar esta valoración también se ha recurrió a las referencias en las encuestas que han hecho los expertos en el tema, y se ha podido evidenciar que existe la percepción casi generalizada de la necesidad de actualización tecnológica de las TIC utilizadas, pero de igual manera se hace referencia permanente a la seguridad que debe brindar la misma, en los hechos acontecidos en el año 2019, según algunas opiniones este hecho se evidencio de forma clara el incidir en la comunicación y manejo de información. Bajo la suposición de contar con tecnología que permita un mejor apoyo a la capacidad de mando y control, la toma de decisiones podría ser más eficaz, sin embargo, también se pudo recopilar información, que la interoperabilidad que, aunque no es muy

valorada en la encuesta, para los expertos es fundamental en el contexto de la incidencia de la capacidad de mando y control en el resto de capacidades militares.

4. ¿Conoce Ud. si existen procesos o normativa de evaluación específica para el uso y utilidad de las TIC en la capacidad de mando y control?

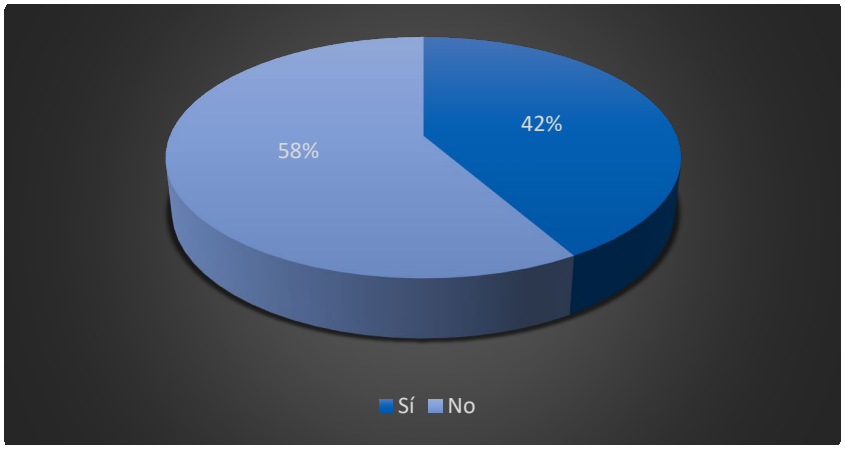
Tabla 7

Normativa de evaluación específica para el uso y utilidad de las TIC en la capacidad de mando y control.

Opciones	f	%
Sí	10	42%
No	14	58%
Total	24	100%

Figura 4

Normativa de evaluación específica para el uso y utilidad de las TIC en la capacidad de mando y control.



Del total de personas encuestadas, 10 respondieron afirmativamente (42%), mientras que 14 respondieron de forma negativa (58%).

Aunque existe una leve mayoría (58%) que responde que no existe una normativa específica respecto a la existencia de normativa para la evaluación del uso de las TIC en

la capacidad de mando y control, las personas que afirman son una cantidad importante, para complementar la información y en base a las entrevistas realizadas, existen argumentos respecto a la normativa que especifican que esta normativa aunque no es específica está inmersa en los procesos de evaluación permanente del ejército a cargo de los comandantes de las diferentes unidades, y de equipos especializados como los de transformación de capacidades, sin embargo no explícita sobre las TIC. En este sentido, la evaluación se considera una herramienta fundamental para el desarrollo de iniciativas, la planificación y el respaldo tecnológico, y una evaluación específica podría ayudar en esta capacidad y ser extensiva para otras.

5. ¿Cuáles considera a su criterio las principales amenazas de la utilización inadecuada de las TIC en la capacidad de mando y control? Valore cada respuesta de la siguiente manera: 3 si considera con alta probabilidad, 2 con probabilidad moderada, 1 con baja probabilidad y 0 sin probabilidad.

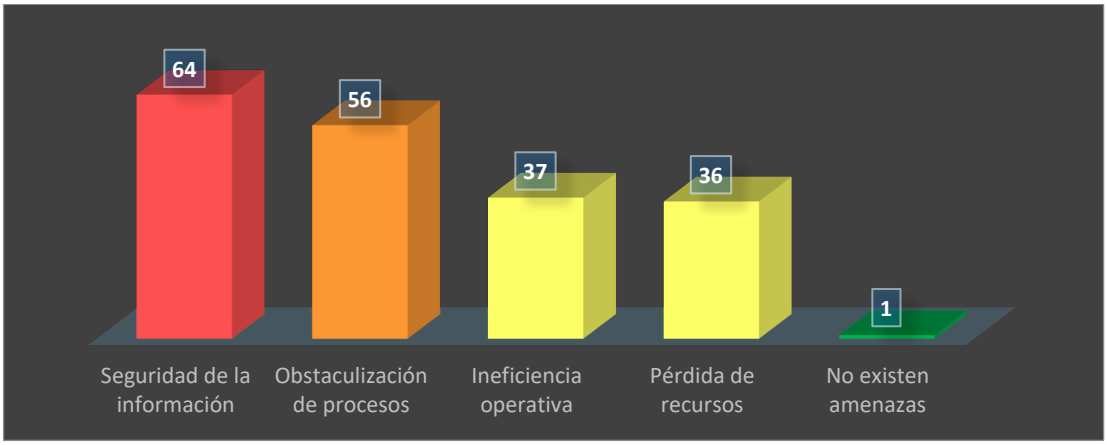
Tabla 8

Principales amenazas de la utilización inadecuada de las TIC en la capacidad de mando y control

Opciones	**3**	**2**	**1**	**0**	**n**	
Seguridad de la información	18	4	2	0	24	64
Obstaculización de procesos	14	4	6	0	24	56
Ineficiencia operativa	4	6	13	1	24	37
Pérdida de recursos	3	8	11	2	24	36
No existen amenazas	0	0	1	23	24	1

Figura 5

Principales amenazas de la utilización inadecuada de las TIC en la capacidad de mando y control.



Para cuantificar la relevancia de las respuestas se utilizó una valoración simple que los encuestados pusieron en cada una de las opciones siendo 3 si consideraba de alta probabilidad, 2 con probabilidad moderada o media, 1 con baja probabilidad y 0 sin probabilidad.

Como se puede apreciar en los datos obtenidos la seguridad de la información es la amenaza que se considera de mayor probabilidad o recurrencia ante el uso inadecuado de las TIC en la capacidad de mando y control, seguido por la obstaculización de procesos, la ineficiencia operativa y la pérdida de recursos. Existe un dato referente a la inexistencia de amenazas que es desechado en base a la dispersión que representa.

Como respaldo en la ampliación de las respuestas y en las entrevistas realizados a expertos en el tema se puede advertir la preocupación por la seguridad de la información, de acuerdo a las características de la misma en la toma de decisiones, y en referencia a los sucesos acontecidos en el marco de las operaciones de ámbito interno de los últimos años en los cuales, sucesos puntuales de fuga o descoordinación de la información conllevaron a problemas en los procesos y eventualmente afectaron el desenvolvimiento normal de las operaciones. Otro aspecto relevante es la obstaculización de procesos

entendida como los problemas que pueden suscitarse ante fallas tecnológicas de las TIC, en el cuso de los operativos o misiones, así la fiabilidad de las TIC es necesaria.

6. ¿Cuáles cree Ud. son las deficiencias tecnológicas de las TIC utilizadas en la capacidad de mando y control en la actualidad?

Tabla 9

Deficiencias tecnológicas de las TIC utilizadas en la capacidad de mando y control en la actualidad

Opciones	f
Inexistencia de herramientas adecuadas	15
Obsolescencia de las herramientas existentes	16
Interoperabilidad deficiente	11
Uso inadecuado	10
Inseguridad	24
Falta de capacitación para su utilización	19
Falta de respaldo técnico ya asesoramiento	23

Figura 6

Deficiencias tecnológicas de las TIC utilizadas en la capacidad de mando y control en la actualidad

Para la cuantificación de esta pregunta se escogió un criterio simple de recurrencia de la respuesta del total de encuestas, es decir cada opción es valorada del total de encuestados, así cada respuesta puede tener un número máximo de frecuencia de 24.

De los resultados obtenidos se puede observar que las respuestas de mayor frecuencia son las de Inseguridad, falta de asesoramiento técnico y asesoramiento y falta de capacitación para su utilización, posteriormente y con menos recurrencia se puede advertir a la obsolescencia, Inexistencia de herramienta adecuadas, la interoperabilidad deficiente y uso inadecuado de las mismas.

Para el análisis de esta pregunta se considera también el resultado de las entrevistas, en las mismas, también se aborda la temática relativa a las deficiencias tecnológicas percibidas en las TIC utilizadas en la capacidad de mando y control, identificando características que pueden ser representadas en la obsolescencia tecnológica, la falta de respaldo técnico, el uso inadecuado de tecnología, la deficiencia en la interoperabilidad, la seguridad en la gestión de la información y la ausencia de métodos que permitan una gestión y evaluación de la tecnología existente, estos valores serán analizados más adelante.

7. ¿Considera necesario establecer estrategias específicas para la actualización, renovación y mantenimiento de las TIC utilizadas en la capacidad de mando y control?

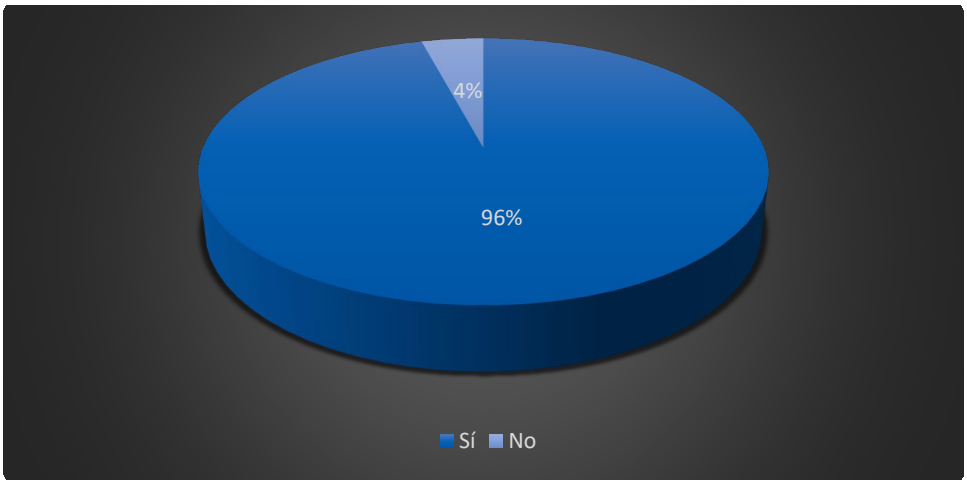
Tabla 10

Necesidad de establecimiento de estrategias de mejora

Opciones	**f**	**%**
Sí	23	96%
No	1	4%
Total	24	100%

Figura 7

Necesidad de establecimiento de estrategias de mejora



De las personas encuestadas 23 es decir el 96% respondieron afirmativamente, mientras que 1 es decir el 4%, respondió de forma negativa.

Se puede advertir que casi la totalidad están de acuerdo con estrategias específicas para la actualización, renovación y mantenimiento de las TIC utilizadas en la capacidad de mando y control, en este sentido y corroborado por la opinión de los expertos se ha de hacer en temas que abarquen a las deficiencias detectadas, fundamentalmente en la evaluación de la tecnología existente, para que esta evaluación puede sostenerse en el tiempo y mediante procesos o modelos que puedan coincidir con los objetivos de actualización tecnológica de las capacidades , desarrollados en la transformación de capacidades, así, esta investigación diseñará un propuesta que planteo modelos para cubrir estas demandas.

8. ¿Qué aspectos principales considera deben ser cubiertos por las estrategias para la actualización, renovación y mantenimiento de las TIC utilizadas en la capacidad de mando y control? Valorar cada respuesta de la siguiente manera 3 si

considera de alta relevancia, 2 con relevancia moderada o media, 1 con baja relevancia y 0 sin relevancia.

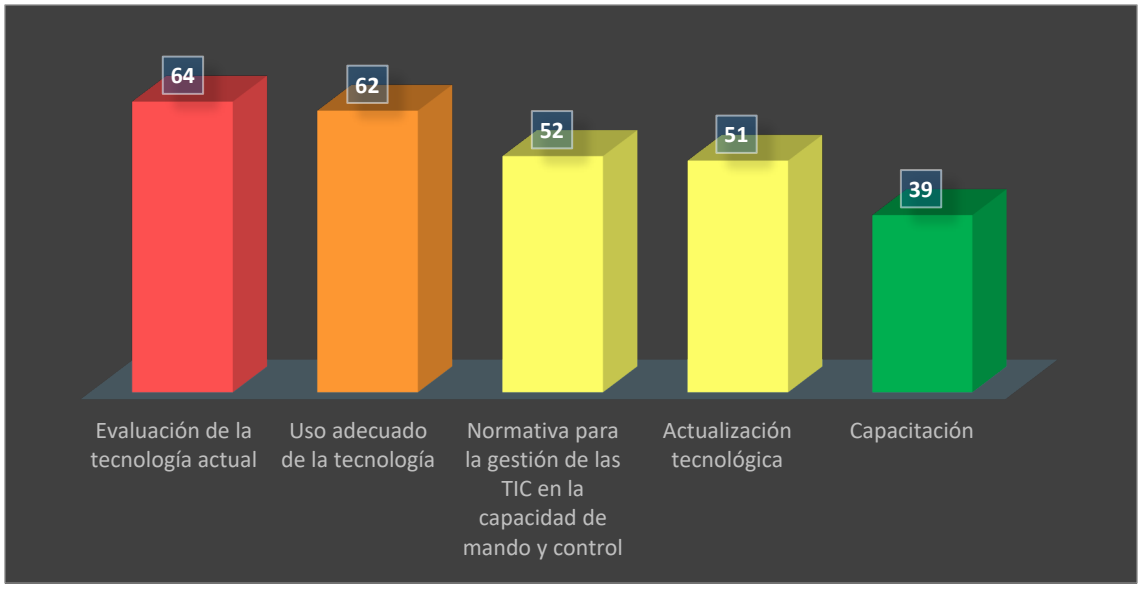
Tabla 11

Aspectos a ser cubiertos por las estrategias para la actualización, renovación y mantenimiento de las TIC utilizadas en la capacidad de mando y control.

Opciones	3	2	1	0	n	
Evaluación de la tecnología actual	18	4	2	0	24	64
Uso adecuado de la tecnología	16	6	2	0	24	62
Normativa para la gestión de las TIC en la capacidad de mando y control	8	12	4	0	24	52
Actualización tecnológica	6	15	3	0	24	51
Capacitación	2	12	9	1	24	39

Figura 8

Aspectos a ser cubiertos por las estrategias para la actualización, renovación y mantenimiento de las TIC utilizadas en la capacidad de mando y control.



Para valorar cada respuesta se asignó 3 unidades si considera de alta relevancia, 2 con relevancia moderada o media, 1 con baja relevancia y 0 sin relevancia.

De los resultados obtenidos y en base a la estimación adicional que se pudo extraer de la información proporcionada de las entrevistas, se determinó que la evaluación es fundamental para la actualización tecnológica, además la gestión de la tecnología, implica no solo un adecuado manejo sino la propia actualización permanente, es así que en estos aspectos se ha centrado la investigación para desarrollar una propuesta de mejora de las nuevas tecnologías en las TIC y el mando y control.

Desarrollo del Primer Objetivo Específico

Determinar las deficiencias tecnológicas que existe en la actualidad en las TIC que utiliza la capacidad de mando y control en la Fuerza Terrestre.

Luego de los datos obtenidos en el proceso de la presente investigación se pudieron percibir amenazas, las cuales son evidentes no solo desde la observación externa sino desde la apreciación de expertos en el tema los cuales al ser entrevistados y encuestados han permitido determinar algunos aspectos puntuales que determinan las falencias detectadas en la utilización de las TIC en la capacidad de mando y control así se determina el siguiente cuadro con las falencias más relevantes detectadas.

Deficiencias tecnológicas detectadas en las TIC utilizadas en mando y control.

Obsolescencia tecnológica

En el contexto del desarrollo tecnológico actual, las herramientas a las que tiene acceso la capacidad de mando y control y las que utiliza, aunque se encuentran operativas, carecen de ciertas características que las van tornando en obsoletas, fundamentalmente por causas como, deficiencias en la actualización , carencia de licencias (en el caso de software) incompatibilidad, lo que no permite interoperabilidad

efectiva, y carencia de tecnología de punta como , ubicación en tiempo real y conectividad remota.

En el contexto del desarrollo de la Defensa del Estado y la importancia de estas políticas en el campo de las Fuerzas Armadas y específicamente del Ejército, se han tratado de desarrollar políticas que integren a las instituciones involucradas para alcanzar estándares de coordinación mediante la interoperabilidad del sistema. Y es así que en distintas ocasiones en el contexto inicial del desarrollo de capacidades y posterior transformación de capacidades se ha tomado en cuenta a la necesidad de invertir en sistemas que mejoren la interoperabilidad, sin embrago las características técnicas de los sistemas actuales y los modelos de gestión de las tecnologías utilizadas no se encuentran desarrolladas para asumir ese reto.

El carácter de la obsolescencia en las TIC es un tema que inicialmente podría concebirse como estrictamente tecnológico, sin embargo, el contexto de la realidad de la gestión en la institución militar demanda, concebir un contexto general de una mejora necesaria de la gestión de la tecnología y la información a todo nivel, lo que a su vez implica innovación efectiva en el desarrollo e implementación de metodologías y procesos para que la actualización tecnológica sea efectiva.

Otro aspecto fundamental de la obsolescencia tecnológica a nivel institucional es el desarrollo de tecnología que permita una actualización específica a las necesidades de la capacidad de mando y control lo cual en sistemas complejos y que necesitan atención específica como lo es el caso de la defensa y específicamente de las capacidades militares es el desarrollo de tecnología propia y aplicada de forma específica para las necesidades de la capacidad a desarrollar, esto es posible mediante dos vías; la primera, una gran inversión de recursos, lo cual no parece ser una vía muy aplicable de acuerdo a la realidad actual, y la segunda, que constituye una real y práctica vinculación con la Academia, tomando en cuenta que la institución militar cuenta con los recursos

académicos de las diferentes escuelas de formación e institutos de educación superior que pueden asumir la responsabilidad de proveer a la institución de tecnología de apunta aplicada a necesidades específicas, con beneficios mutuos como la constante capacitación, en tecnología de la defensa, generación de recursos a mediano y largo plazo y evitar problemas como la obsolescencia programada comercial o la dependencia de terceros en el contexto de respaldo y mantenimiento técnico.

Cabe considerar que el cambio tecnológico es un factor muy grave para cualquier institución y más aún para Fuerzas Armadas dadas las implicaciones en el campo de la inversión y cambio de infraestructura y en si de las herramientas y medios tecnológicos, a esto es de añadir el carácter de interoperabilidad que deben poseer los sistemas inmersos, es por esta razón que el incentivo a la innovación no solo tecnológica sino además metodológica puede viabilizar este tipo de actualizaciones en bien de la institución militar y de la seguridad y defensa del estado.

Falta de respaldo técnico

Aunque muchas herramientas se encuentran operativas y funcionales, el aprovechamiento de toda su potencialidad no es el adecuado ya que requieren de una asistencia permanente que en muchas ocasiones supera al personal militar propio, por diferentes razones entre ellas la especificidad del desarrollo de software y hardware por lo que se hace necesario, la implementación de respaldos técnicos, ya sea con la organizaciones fabricantes o con la academia militar para generar innovación y actualización de componentes tecnológicos.

Pensar en el respaldo técnico para la tecnología utilizada en el contexto militar implica además de los conceptos del mundo empresarial como la fiabilidad, pertinencia y eficiencia la inclusión de elementos relacionados a la seguridad y la confidencialidad, lo cual determina además respaldos normativos y legales, por la trascendencia del entorno

en el cual se aplican y utilizan los elementos tecnológicos, lo cual no siempre es considerado, y genera problemas en la fuga de información que generalmente determina vulnerabilidades. Es, en este sentido que el desempeño del respaldo técnico para el sector de la defensa trata de ser cubierto por elementos propios de las Fuerzas Armadas en los diferentes países, para lo cual se necesita una mayor inversión interinstitucional y la vinculación permanente con las academias de formación militares que permitan una menor dependencia de recursos externos en el campo del respaldo técnico pero además del desarrollo de procedimientos y normativas que reduzcan los riesgos en la seguridad de los sistemas tecnológicos utilizados en este caso en el campo de la capacidad de mando y control.

Uso inadecuado de tecnología

Este es una deficiencia que tiene que ver con las anteriores, y que depende inicialmente de un asesoramiento técnico permanente pero además de la creación de normativa específica para el uso de las TIC ya sea en el contexto de aprovechamiento de las ventajas y aplicaciones tecnológicas o de la metodología para efectivizar su uso e impedir problemas subyacentes como la seguridad y la interoperabilidad e integración de las capacidades.

Este es un aspecto que tiene fundamentalmente dos fuentes, la una que se refiere a las habilidades para la utilización de herramientas tecnológicas y que pueden ser mejoradas mediante capacitación y entrenamiento y la otra que se refieren generalmente a la gestión de la información. Aunque las fuentes citadas no pudieran ser las únicas (socialización, complementariedad, etc.) son las más relevantes en las implicaciones con la seguridad.

Es en este sentido que la relevancia de un uso adecuado de las tic parta los propósitos específicos para las que fueron creadas es fundamental, sin embargo se han

podido percibir una serie de elementos que implican que el uso inadecuado de la tecnología pueda convertirse en un riesgo en el campo de la capacidad de mando y control, es así que los procedimientos son muy generales y en muchos casos no existen por lo cual no se respeta por ejemplo el uso dedicado y exclusivo para los fines institucionales o de mando y control pertinentes, o por ejemplo la subutilización de los beneficios de herramientas tecnológicas lo que genera elementos que pueden retrasar la productividad y la eficiencia, o la desatención de procedimientos y elementos necesarios para la seguridad de la información.

En este sentido cabe mencionar que se encontraron, además, opiniones respecto a la utilización de herramientas tecnológicas ajenas a la institución, pero que en muchos casos por comodidad o necesidad deben ser utilizadas, los cuales son otra fuente de fuga de información, o acceso a sistemas institucionales lo cual constituye un riego para la seguridad y ya ha presentado problemas en la planificación de operaciones o en la inteligencia militar, para citar algunos casos.

Como casos relevantes y que aunque no pueden ser considerados trascendentales la utilización de memorias de almacenamiento extraíbles y su inadecuada gestión por los miembros de Fuerzas Armadas y sus colaboradores ha sido por su mala gestión, una causa recurrente de fuga de información y mala utilización de la misma, ya que ya sea por pérdida o por su tracción en lugares destinados a la reparación de dispositivos móviles la información que estos contienen se ha diseminado fuera de la institución en múltiples ocasiones.

Es así que la seguridad de la información es fundamental en el contexto institucional, la responsabilidad en el manejo de información es fundamental no solo en quienes manejan información clasificada o importante sino de cada miembro de la institución militar. En este sentido es necesaria un cambio de la cultura organizacional, en lo referente al uso de la información y a la necesidad de fomentar una introspección

respecto a la responsabilidad de pertenecer a una institución militar, que genere una concepción real de pertinencia institucional real con la responsabilidad que implica respecto a la seguridad personal, institucional y nacional.

Deficiencia en la interoperabilidad, e integración con sistemas similares

En el contexto de la conjuntes de las Fuerzas Armadas y de conceptos como gobierno electrónico y sistemas de seguridad integral, se necesita una actualización referente a esta característica, que debe tener la tecnología que utiliza la capacidad de mando y control para una interacción de la seguridad y la defensa y de la toma de decisiones en el ámbito militar.

La plena realización de la visión conjunta de las capacidades militares y su desarrollo transformación, se puede concebir en un concepto de superioridad de la información habilitado y respaldado por una red de sistemas, cuyos elementos constituyentes interoperan y cooperan para respaldar a toda la jerarquía de combate, en el contexto de la Defensa. La interoperabilidad de los sistemas es un habilitador clave del objetivo operativo general de la integración de Fuerzas: la fusión de los recursos en una fuerza militar unificada que logra una alta efectividad militar, explotando y coordinando las capacidades de las fuerzas individuales.

El logro de un alto nivel de interoperabilidad requiere un nivel acorde de esfuerzo y priorización de recursos en todo el sistema de defensa.

El rango de complejidad de los requisitos para el flujo de datos en una misión de este tipo subraya la importancia de la interoperabilidad en todos los niveles. La interoperabilidad a nivel técnico es fundamental para lograr la interoperabilidad operativa. Un problema que surge entre sistemas y no entre organizaciones, la interoperabilidad técnica debe considerarse en una variedad de contextos y alcances, incluso para una sola misión. Mientras que la interoperabilidad operativa hace referencia a la capacidad de

los sistemas, unidades o fuerzas para proporcionar servicios a y. aceptar servicios de otros sistemas, unidades o fuerzas y utilizar los servicios intercambiados para permitirles operar juntos de manera efectiva.

En cualquiera de los casos la interoperabilidad necesita recursos tecnológicos y estos deben estar coordinados y sobre todo ser compatibles, en este sentido existen esfuerzos a nivel de Fuerzas Armadas y del gobierno por desarrollar la interoperabilidad pero, por sobre estos esfuerzos cabe plantear la concepción de esta interoperabilidad en todo el sistema de defensa ya que la planificación y la definición de objetivos se encuentran basados en esta concepción, es así que el énfasis necesario de que los procesos desarrollados en cada una de las capacidades militares y específicamente en la capacidad de mando y control deben asegurarse que guarden los principios de interoperabilidad ya definidos y planteados intrainstitucional e interinstitucionalmente.

En ejemplos puntuales como las operaciones de ámbito interno o de catástrofes la necesidad de interoperabilidad interinstitucional e intrainstitucional es fundamental, ya que en casos en los cuales se necesita de información o de operaciones de instituciones relacionadas con el sistema de defensa nacional como la Policía Nacional o el cuerpo de bomberos (solo para citar algunos) el tiempo es fundamental para la efectividad de las mismas, es, entonces donde incompatibilidades o barreras en las comunicaciones puede ser la cusa de demoras y retrasos que derivan en la inefectividad de las operaciones o en la alerta de las posibles amenazas. Así, el sentido de interoperabilidad de las aplicaciones como las TIC es fundamental para la seguridad del Estado.

Seguridad en la gestión de la información

Un aspecto fundamental en el contexto de las TIC aplicada o utilizadas en la capacidad de mando y control es la seguridad, que integra a la seguridad informática con el concepto de seguridad de la información, en la actualidad no existen normativas

específicas en este aspecto y es necesario desarrollar ya sea mediante cambios en la doctrina o mediante la socialización de su importancia o inclusión de procedimientos y normativa específica.

En las organizaciones en general y en el ejército en particular, la información es uno de los más importantes activos de apoyo a todos los procesos para el desarrollo de sus operaciones. Su manipulación depende de tres elementos principales:

(i) Sistema tecnológico, que permite el almacenamiento, procesamiento y transmisión;

(ii) Partes interesadas, que pueden acceder a él a través de Internet o redes institucionales y;

(iii) El proceso institucional que lo utiliza.

Por ello, es fundamental buscar, continuamente, asegurar las propiedades fundamentales de la seguridad, como la confidencialidad, la integridad y la disponibilidad. Los efectos de algunos de los métodos de ataque apoyados principalmente en Tecnología de la Información, pueden ser representado en el conocimiento de información que tuvieron los grupos violentos en las operaciones de ámbito interno del año 2019 en el Ecuador, en donde se pudo evidenciar la vulnerabilidad de los sistemas de información utilizados sean estos propios o ajenos a la institución militar y que conllevaron a la previsión de estos grupos respecto a las operaciones planificadas.

La creciente importancia de la seguridad de la información en las organizaciones militares también se debe al surgimiento de conceptos, desarrollados en función de los avances tecnológicos en el campo de la seguridad, las comunicaciones y el acceso a la información, como Superioridad de la Información (Alberts, Garstka, Hayes y Signori, 2001) y Guerra de Información (Arquilla & Ronfeldt, 1999; M. Libicki, 1995; Waltz, 1998), basados principalmente, en la idea de que la información se ve en los sistemas de defensa como un arma y un objetivo simultáneamente.

Es así que, debido a los conceptos de la doctrina militar, el uso de las tecnologías de la información como arma ofensiva, el surgimiento del ciberespacio como una nueva dimensión del campo de batalla, y la importancia de la información pertinente y confiable, para lograr superioridad de la información en un entorno de guerra de información, es importante desarrollar nuevos enfoques de la seguridad de la información y, por tanto, nuevos procesos de planificación en las organizaciones militares.

Esta actividad en busca de nuevos enfoques puede asumirse en la actualidad como una “Batalla Defensiva”. El contexto descrito justifica la relevancia de diseñar una nueva planificación de seguridad de la información, para las organizaciones militares, asumiendo como esencial el foco en los posibles modos de acción de un oponente (es decir, sus métodos de ataque). De esta manera el garantizar la confidencialidad, integridad y disponibilidad de la información dentro de una organización militar en el contexto de un entorno de guerra de información, con el fin depara minimizar el riesgo de seguridad de la información debería ya considerarse una prioridad, para la cual el análisis del contexto normativo y técnico de la tecnología utilizada sea propia o ajena es fundamental para lograrlo.

Métodos específicos para gestión de las TIC.

No existen métodos específicos aplicados a la capacidad de mando y control, por eso una adecuada aplicación de métodos específicos puede mejorar la evaluación adecuada de las necesidades tecnológicas y la adaptación de herramientas específicas para que resulten más beneficiosas, permitiendo de esta manera eliminar las deficiencias detectadas.

Aunque las deficiencias detectadas en el contexto de la tecnología utilizada en la capacidad mando y control son varias, la utilización de métodos de diagnóstico y evaluación pueden constituirse en el inicio de una programación permanente de recursos

tecnológicos, que logren sentar las beses para alcanzar eficiencia en el uso de la tecnología ya que la aplicación de un método fiable puede ahorrar y optimizar recursos, para de ahí en adelante poder gestionar los elementos con los cuales se trabaja y desarrollar o innovar los mimos posteriormente.

La utilización de metodologías claras, permite a los procesos institucionales el ahorro de recursos y la definición de los mismos, claro está que estos métodos deben ser reutilizables permanentemente y además modificables en función de los cambios que requiera en este caso específico el desarrollo o transformación de la capacidad de mando y control. así las condiciones de actualización, realimentación y constante evaluación son fundamentales para el desarrollo de metodologías para la evaluación, adquisición mantenimiento y utilización adecuada de las TIC en la capacidad de mando y control.

Desarrollo del Segundo Objetivo Específico

Establecer si la transformación de la capacidad de mando y control requiere de actualización tecnológica permanente de las TICS de que dispone.

En base a la información recolectada y a los hallazgos encontrados en la investigación de campo se puede concluir que es necesaria una actualización tecnológica permanente, tomando en cuenta las deficiencias que en la actualidad poseen las tic utilizadas en la capacidad de mando y control en relación, a la seguridad, gestión de la información, desactualización y falta de especificidad de procesos y normativa, que eventualmente ha incidido negativamente en el mando y control de las operaciones militares de los últimos años fundamentalmente aquellas de ámbito interno, ya que las amenazas presentadas en las mismas pudieron evidenciar dichas falencias. Es así que esta investigación, desarrollará una propuesta de solución y la presenta como una oportunidad para enfrentar las amenazas actuales, y de esta manera contribuir al proceso de transformación de capacidades que se desarrolla en la Fuerzas Armadas.

Desarrollo del Tercer Objetivo Específico

Desarrollar un método para determinar las necesidades tecnológicas de las TICS de la capacidad de mando y control de forma permanente.

Una vez desarrollada la investigación de campo y los objetivos específicos previos se ha logrado obtener la información suficiente para la elaboración de la propuesta de mejora para el tema de la investigación la cual se desarrollará en el capítulo quinto, y se validará en el capítulo sexto más adelante.

Desarrollo del Cuarto objetivo específico

Determinar un método adecuado para la optimización y utilización adecuada de las tecnologías de información disponible

El desarrollo de un método adecuado para la optimización y la utilización adecuada de las tecnologías de la información disponible estará basado en los hallazgos encontrados por la investigación de campo y respaldados por el estudio bibliográfico documental del tema. Para esto se prevé diseñar Metodología de gestión de las TIC en la capacidad de mando y control que será desarrollada en el siguiente capítulo.

Capitulo Quinto: Propuesta

Título de la Propuesta

Metodología de gestión de las TIC en la capacidad de mando y control.

Objetivo de la Propuesta

Desarrollar una metodología adecuada para la gestión del as tic en la capacidad de mando y control.

Alcance de la Propuesta

El alcance de la propuesta abarca el ámbito de la Fuerza Terrestre como parte de las Fuerzas Armadas del Ecuador.

Desarrollo de la Propuesta

La implementación de las tecnologías de la información y la comunicación. (TIC) impacta la distribución de responsabilidad en el mando y cadena de control. En algunos casos, la introducción de nuevas tecnologías puede favorecer la centralización; en otros, representan la fuente de nuevas formas de delegación y descentralización. Los diversos niveles de la jerarquía pueden tomar mejores decisiones porque obtienen acceso a datos detallados sobre la situación táctica.

Un método para determinar las necesidades de la capacidad de mando y control relacionado con las TIC pude tener diversos impactos en el desarrollo de la capacidad militar considerando que las nuevas tecnologías no pueden por sí mismas explicar la realidad de su desarrollo, sino que son en la actualidad un componente importante que ayudará entre otros a uno de los objetivos primordiales que es la toma de decisiones. Los

sistemas de mando y control se han vuelto cada vez más complejos en los últimos años. La distinción entre niveles estratégico, operativo y táctico ha sido ampliamente considerada como una forma precisa de análisis porque fundamenta las relaciones en la separación entre políticas responsabilidades y aspectos netamente militares.

Otro aspecto importante para el mando y control resulta la velocidad del flujo de información y la cobertura de los medios de comunicación, ambos aumentan los efectos estratégicos de cada decisión tomada en los niveles operativos y tácticos. En este contexto, no existe algo como un modelo único de control sino, más bien, un marco general remodelado por las especificidades de cada operación militar.

Para comprender el impacto de las TIC sobre la subsidiariedad en la organización militar es necesario lograr un equilibrio entre unidad de responsabilidades políticas y militares, por un lado; y, la optimización de la eficiencia operativa militar por el otro. La distinción entre los niveles estratégico, operativo y táctico sigue siendo esencial; pero no es suficiente para comprender los principios de delegación y el impacto de la introducción de nuevas TIC.

Esta propuesta inicialmente aborda el problema en la elaboración de la diferencia entre información y conocimiento. La información está relacionada con los mensajes y el flujo de datos. El conocimiento está incrustado en los procesos humanos relacionados con las aptitudes, la práctica y la acumulación de experiencias. Los flujos de información pueden modificar aspectos colectivos e individuales del conocimiento. La producción de conocimiento depende del aprendizaje de procesos, sobre capacidades individuales y colectivas. La naturaleza de la información. Es decir, la producción y difusión del conocimiento, y, la producción resulta muy diferentes.

Así el modelo plantea inicialmente la concepción de información y su diferenciación con el conocimiento, para para posteriormente determinar las acciones que deberá comprenderse para que el modelo parta de un contexto estratégico y llegue al nivel

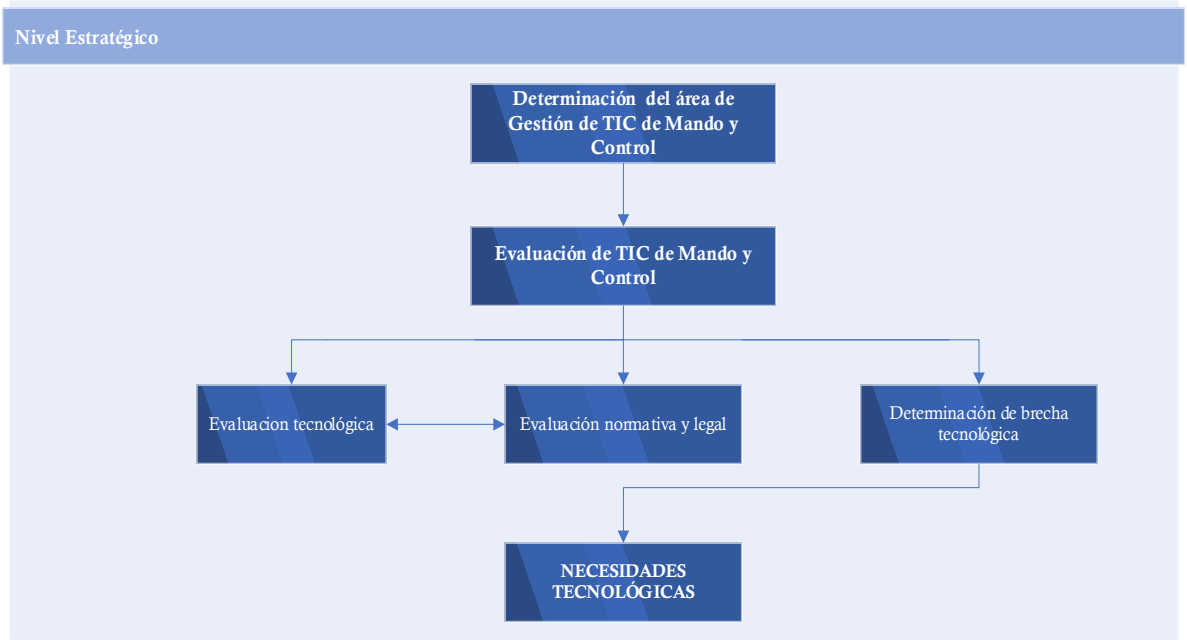
operativo, resguardando características esenciales como la retroalimentación y la sustentabilidad de los modelos para su permanencia en el tiempo y su evolución.

Método para determinar las necesidades tecnológicas de las TIC de la capacidad de mando y control de forma permanente

El método planteado corresponde al nivel estratégico de la gestión de la capacidad de mando y control debido a que estas decisiones trascienden en la planificación de la capacidad para ello, es necesaria la concepción de la gestión de las tecnologías TIC como parte fundamental para el proceso, basados en la influencia de la tecnología para la capacidad.

Figura 9

Estructura del Método



Definir a la gestión tecnológica de mando y control

Dentro de las funciones de las atribuciones y responsabilidades del proceso adjetivo de apoyo, denominado “Gestión de Tecnologías de la Información y Comunicaciones” en el marco del Estatuto Orgánico de la Gestión Organizacional por Procesos (Dirección de Planificación de la Gestión Institucional del Ejército., 2013) se señala:

Gestionar el desarrollo, implantación y producción de los proyectos de las tecnologías de información y comunicaciones de la Fuerza Terrestre;

Asesorar al Mando y Unidades de la Fuerza Terrestre, en lo relacionado a las tecnologías de información y comunicaciones.

Es entonces que existe la viabilidad para generar la atención necesaria para la gestión del área tecnológica de la capacidad de mando y control, que por las características de la capacidad puede ser vinculante en el contexto de la transformación de capacidades militares.

En el contexto del desarrollo de capacidades militares la especificación de la tecnología necesaria para que las mismas puedan desarrollarse ya no constituye una alternativa, ya que la inserción de la tecnología en cada ámbito de la estructura organizacional o en este caso, de las capacidades militares requiere de especificidad para que su gestión sea lo más eficiente posible. Sin embargo, debe existir un sentido de interoperabilidad eficiente entre Fuerzas para evitar la redundancia y la incompatibilidad de datos e información.

Evaluación de las TIC de mando y control

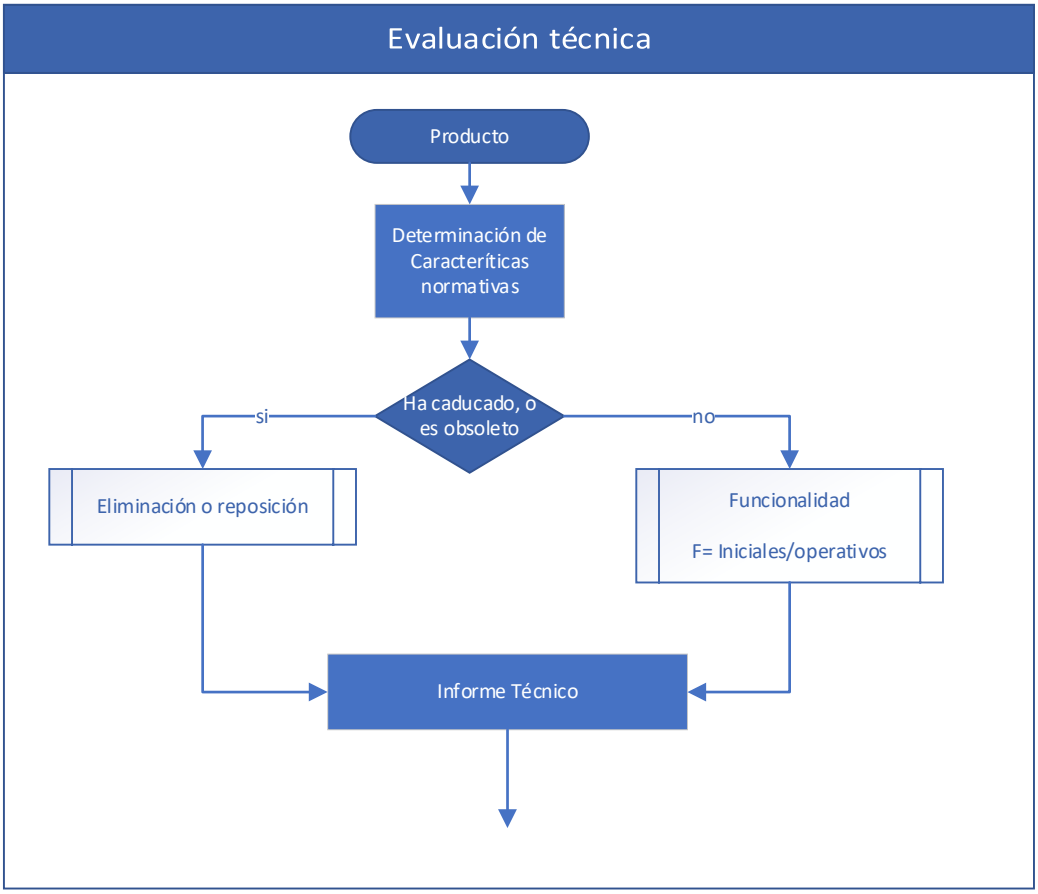
Evaluación tecnológica

La evaluación tecnológica de las TIC es un componente esencial del método ya que en este, se estimará las condiciones reales de las TIC utilizadas en mando y control y requiere de un asesoramiento de expertos de la institución vinculados a la gestión de tecnologías de la información y de comunicaciones, pero además la dirección y planificación de comando y control, cuyo conocimiento es fundamental para el aporte de las necesidades y característica específicas y problemática en torno de la tecnología aplicada.

Para la evaluación tecnológica se deberá considerar las características del producto, su funcionalidad y el respaldo técnico necesario, esta evaluación se traducirá en un informe que emita estos criterios para la consideración de las mismas en la determinación de alternativas de las TIC. El proceso se lo puede observar en el siguiente diagrama

Figura 10

Diagrama de flujo evaluación técnica



Para determinar la funcionalidad de los elementos a ser evaluados se considerará el número de elementos o el elemento que inicialmente conformaron el sistema y el número de elementos que se encuentran funcionales

Evaluación Normativa y legal

Aunque existen procesos de apoyo en la planificación general es necesario indicar que el contexto normativo y legal debe ser tratado con la especificidad del caso, en el contexto de la independencia de esta capacidad militar, la cual puede generar innovación y desarrollo de tecnologías propias o modificadas en base a las necesidades específicas de la capacidad. Así el uso de patentes o desarrollo de las mismas con el apoyo de

desarrollo de las Escuelas de formación, institutos y universidades pertenecientes a la fuerza es una perspectiva que no se ha abordado lo que generalmente produce conflictos o falta de seguimiento técnico y obsolescencia, lo cual podría ser controlado de mejor manera con el estudio y análisis de la normativa y el contexto legal de las aplicaciones utilizadas.

Figura 11

Diagrama de flujo evaluación técnica normativa (software)

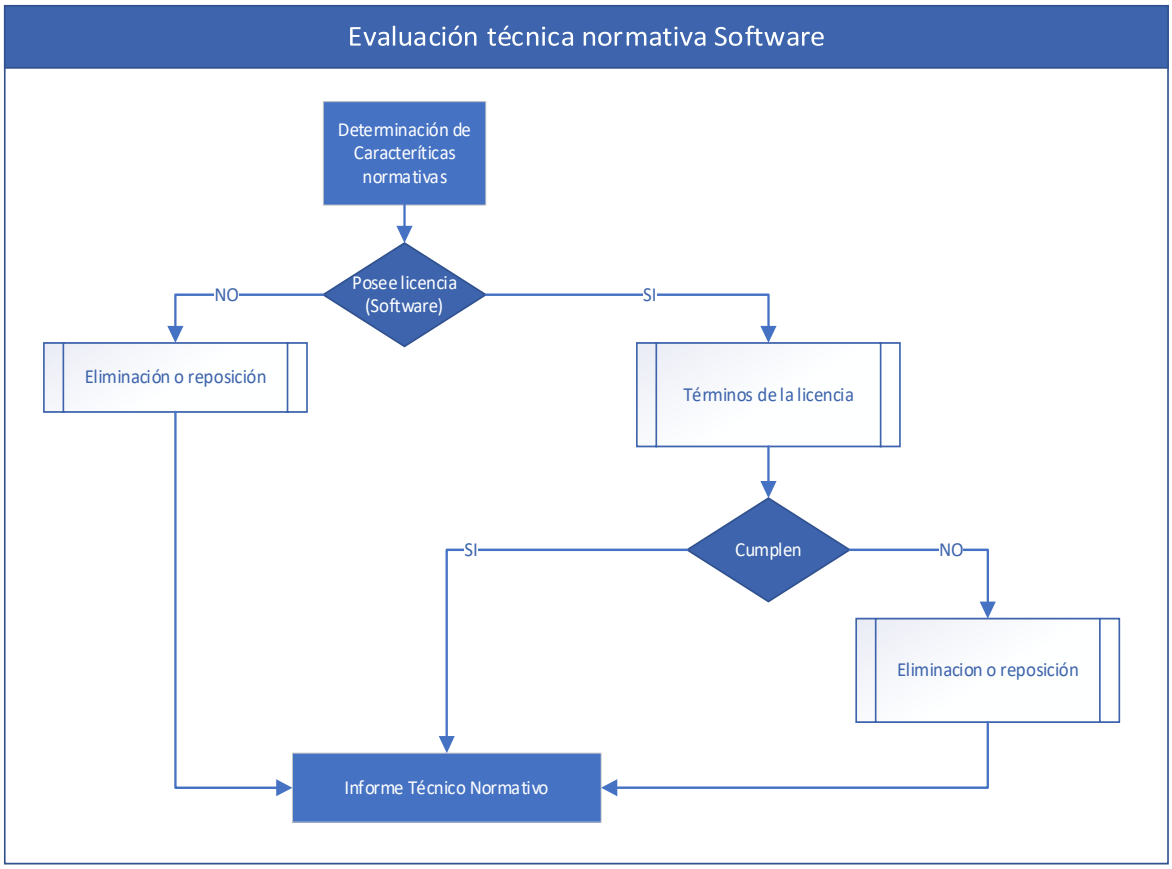
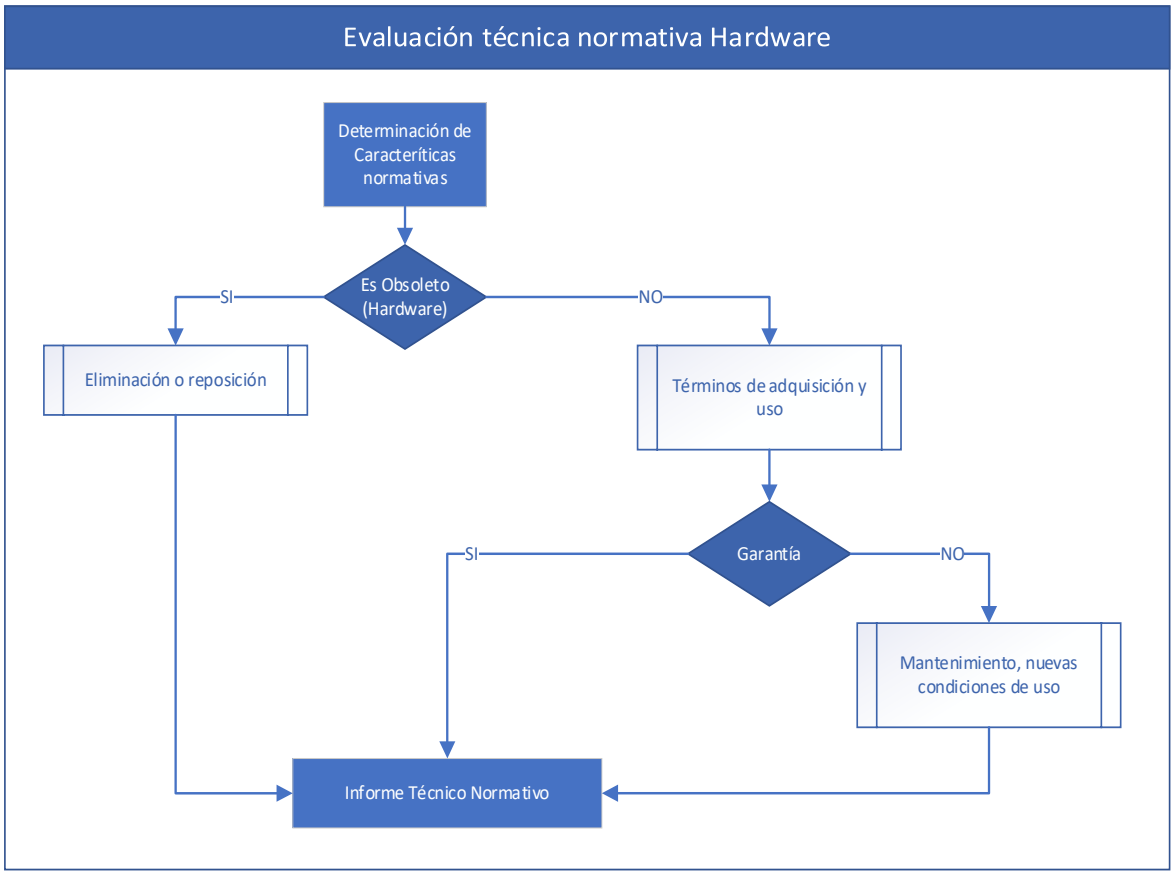


Figura 12

Diagrama de flujo evaluación técnica normativa (hardware)



Determinación de brecha tecnológica

Aunque en el desarrollo y seguimiento de las líneas de transformación planteadas por el equipo de transformación de capacidades de las Fuerzas Armadas se determina la brecha de capacidad de comando y control, sería necesario contar con la especificidad suficiente para las tecnologías Utilizadas por esta capacidad militar, de esta manera se puede definir en función de los requerimientos y proyecciones de ésta una estimación real de la brecha de las tecnologías, es, en ésta instancia en donde con un sustento cuantificable se puede proseguir en la determinación de estrategias para que dicha brecha se cierre.

Determinación de necesidades tecnológicas para las TIC de mando y control

Con los elementos desarrollados en la fase de evaluación de las TIC y en la determinación de la brecha tecnológica se tiene los elementos suficientes para determinar las necesidades reales de las TIC que requiere mando y control, no solo en base a los requerimientos generales definidos en una planificación, sino tomando en cuenta proyecciones de desarrollo de la capacidad considerados en el análisis de la brecha de capacidad pero además con un conocimiento de la realidad de la utilización y aplicación de la tecnología existente, cabe señalar que esta etapa además debe incluir elementos relacionados al contexto presupuestario y orientados a cubrir requisitos procedimentales y tecnológicos actuales como la interoperabilidad e interdependencia con sistemas afines del contexto tecnológico del resto de capacidades militares. Características que deberán ser consideradas:

- Evaluación técnica
- Evaluación normativa y legal
- Determinación de brecha tecnológica
- Interoperabilidad e interdependencia de Alternativas

Recomendaciones de la Propuesta

En base al desarrollo de la investigación bibliográfica documental y considerando los hallazgos de la investigación de campo se recomienda:

- La creación de un equipo técnico de evaluación de las TIC utilizadas en la capacidad de mando y control con el fin de coordinar las mismas necesidades tecnológicas.
- Coordinar con los responsables de la Gestión de Tecnologías de la Información y Comunicaciones de la Fuerza Terrestre, para definir a la

gestión tecnológica de mando y control, y delimitar los métodos, herramientas y procesos específicos y relacionados para con la capacidad de mando y control.

- Coordinar la información relevante a cada uno de los niveles de la Fuerza que puede ser manejada a través de TIC.
- Es necesario estandarizar la tecnología a ser utilizada.
- Se necesita una capitación técnica del personal que gestiona y utiliza las TIC.

Fundamentación Doctrinaria, Técnica y Documental

Las nuevas tecnologías pueden cambiar la doctrina militar y la forma en que se lleva a cabo la guerra. Las nuevas tecnologías pueden hacer obsoletos a los sistemas de defensa existentes o proporcionar una capacidad militar nueva y más eficaz, esto depende de la concepción de la planificación de la especificidad que se logre con las aplicaciones tecnológicas. Port ejemplo se puede destruir los sistemas informáticos o de telecomunicaciones dejando inhabilitada la unidad en vez de enviar a un equipo de Fuerzas Especiales para destruirlo físicamente. En general, la atención ha tendido a centrarse en tecnologías nuevas en el mundo, pero las combinaciones novedosas de tecnologías generales y específicas también pueden tener profundas implicaciones militares. La consideración del vínculo entre las tecnologías emergentes y las capacidades militares y la importancia de los factores institucionales y el sistema de adquisición para determinar la velocidad de adopción de las tecnologías emergentes son procesos que cada se van tomando en los procesos de planificación militar. Se argumenta que el cambio tecnológico y económico significa que este es un tema cada vez más importante en función de la efectividad y el mejoramiento y optimización de la defensa.

La defensa está desempeñando un papel cada vez menor como patrocinador de tecnologías avanzadas y se convertirá en un seguidor en lugar de un líder en muchas (la mayoría) de las áreas de la tecnología. En consecuencia, la mayoría de las tecnologías

emergentes surgirán de actividades científicas, tecnológicas e innovadoras que tengan lugar en sectores civiles, pequeñas organizaciones y universidades de todo el mundo. En el futuro, el proceso de innovación de la defensa deberá poner más énfasis en la identificación oportuna y la explotación efectiva del conocimiento tecnológico emergente dondequiera que resida. Es probable que el futuro de la política de tecnología de defensa esté en la creación de capacidad de absorción y agilidad mediante (i) el desarrollo de mecanismos de búsqueda efectivos para identificar tecnologías emergentes potencialmente importantes y sus fuentes, (ii) la creación de asociaciones efectivas con proveedores (potencialmente) no tradicionales de dichas capacidades tecnológicas y (iii) encontrar medios para la explotación ágil de esas tecnologías emergentes en beneficio militar.

Fundamentación Histórica, Filosófica, Social, Cultural

En los últimos años, se han producido cambios considerables en el equipamiento de las organizaciones y unidades militares con tecnologías de la información y comunicaciones con diferentes connotaciones y grados de integración. La industria militar ha respondido rápidamente a las demandas del desarrollo de las amenazas y al contexto de la globalización y necesidad de información de la Defensa, diseñando, desarrollando, construyendo y produciendo herramientas tecnológicas para sustentar sistemas de defensa.

La operación y el mantenimiento de estas herramientas requieren la capacitación adecuada y constante que no siempre es considerada dentro de la institución lo que supone un interés adicional en términos de seguridad y dependencia tecnológica externa.

Esto se relaciona principalmente con la aplicación de tecnología informática y de telecomunicaciones en donde el manejo de sus herramientas tiene una dependencia de factores externos que puede determinar problemas como fallas en la seguridad,

desaprovechamiento y subutilización de todo tipo de elementos, lo cual conlleva a problemas con los procesos de respaldo en la toma de decisiones generalmente vinculados al mando y control.

El amplio uso de las TIC en todos los campos empresariales y también en el ámbito militar, incluida la gestión de la producción, el desarrollo del diseño, la simulación, la construcción, la producción y la operación de tecnología militar, plantea mayores exigencias al desarrollo de las capacidades militares, que en la actualidad tiene una mayor dependencia de las TIC.

Los requisitos específicos para la introducción de nuevas tecnologías en el desarrollo de capacidades militares se manifiestan en la diferenciación de la mismas en función de sus objetivos básicos, de ahí la importancia de su concepción para una posible especificidad de la aplicación de tecnologías que podrían ser comunes en el ámbito empresarial. Sin embargo, cabe señalar que muchos problemas teóricos y prácticos, en particular la introducción de tecnologías modernas de información e informática radican en la definición de necesidades específicas y la habilidad para aplicar las tecnologías en función de la satisfacción de esas necesidades, así por ejemplo el desarrollo de las TIC aplicadas al contexto militar. Es así que tecnologías acordes al desarrollo de amenazas son fundamentales, la inclusión de drones y de programas adecuados para su operación efectiva, sistemas d comunicaciones en tiempo real con sistemas avanzados de seguridad y codificación que mejoren la comunicación especializada con imagen de alta resolución remota, aplicaciones logísticas de localización en tiempo real y seguimiento de la cadena logística, programas de gestión de la información del personal, y gestión de información de amenazas, reconocimiento facial, etc. Es decir las tecnologías que se utilizan en los sistemas actuales de defensa integrados al mando y control de forma directa o indirecta, deberán contar con elementos que permitan priorizar la seguridad, la

efectividad ante eventuales ataques, la reposición inmediata y la sistematización para la evaluación y reorientación operativa.

Es en este sentido que el desarrollo tecnológico necesario de la actividad militar requiere de innovación y especificidad, lo que requiere de un conocimiento adicional de la cultura institucional, y de la vinculación con elementos que coadyuben a la efectividad y la seguridad, ya que des estos procesos no depende únicamente la seguridad o la efectividad personal o institucional sino depende además la seguridad nacional y el resguardo de los intereses comunes en la Patria.

Validación de la Propuesta

La validación se la efectuará mediante el método denominado CAME (corregir, afrontar, mantener y explotar), con el objetivo de definir estrategias de validación para la eventual aplicación de las estrategias de la propuesta, y así definir estrategias ofensivas, defensivas, de reorientación y de supervivencia.

Conceptualización de la Propuesta

La propuesta definida como “Estrategias para la optimización y utilización adecuada de las TIC para la capacidad de mando y control de la Fuerza Terrestre”, plantea estrategias para la optimización de la gestión de las TIC de esta capacidad de la Fuerza terrestre, e influir en la responsabilidad en la utilización de herramientas tecnológicas, en función de la seguridad y el mejoramiento en la toma de decisiones.

Método y Criterios de Validación

Para la validación de la propuesta se plantea un análisis FODA de la situación actual de la gestión de las TIC de la capacidad de Mando y Control con la prospectiva de la

implementación de las estrategias planteadas, tomando en cuenta los resultados de la investigación y el respaldo teórico de la misma. Para el proceso de validación se considerará la especificidad de la problemática en la capacidad de Mando y control, para percibir las fortalezas y debilidades de las estrategias planteadas (aplicación de métodos desarrollados) y su entorno de desarrollo (interno), mientras que para oportunidades y amenazas se considera el contexto externo.

Tabla 12

Análisis FODA de validación de la propuesta

ANÁLISIS INTERNO		**ANÁLISIS INTERNO**
Fortalezas		**Oportunidades**
• F1. Propuesta basada en hallazgos de estudio de campo actual • F2. Propuesta viable • F3. Mejora de la calidad de las TIC • F4. Simplificación de análisis • F5. Mejora de la gestión tecnológica a nivel estratégico y táctico • F6. Complementariedad con la transformación de la capacidad de mando y control		• O1. Ley de Modernización del Estado • O2. Proceso general de gestión de las TIC establecido • O3. Ssistema organizacional institucional sólido • O4. Proceso de transformación de capacidades militares en marcha
Debilidades		**Amenazas**
• D1. Mecanismo de implementación i de proyectos de TIC indefinido • D2. Procesos de Gestión de TIC aun no detallado • Falta de especificidad de manejo de las TIC a nivel de capacidades individuales		• A1. Presupuestos insuficientes o limitados • A2. Cultura organizacional débil en favor de la innovación • A3. Ciber amenazas • A4. Falta de seguridad en gestión de TIC y de la información

Tabla 13

Estrategias derivadas del método FODA y CAME

ESTRATEGIA OFENSIVA		**ESTRATEGIA DEFENSIVA**
(<u>Explotar</u> Fortalezas para aprovechar Oportunidades)		**(<u>Mantener</u> Fortalezas para reducir Amenazas)**
Determinar la importancia de la implementación de la propuesta para la optimización y aprovechamiento de las TIC de mando y control para la Fuerza Terrestre como correspondiente a Ley de Modernización del Estado y a Ley Orgánica de Transparencia y acceso a la información pública.		Resaltar que la aplicación de las estrategias propuestas para la mejora del proceso de gestión de las tecnologías de la información y comunicaciones, como herramienta de la ciberdefensa.
ESTRATEGIA DE REORIENTACIÓN		**ESTRATEGIA DE SUPERVIVENCIA**
(<u>Corregir</u> Debilidades aprovechando Oportunidades)		**(<u>Afrontar</u> Amenazas minimizar Debilidades)**
Aprovechar el proceso de transformación de capacidades para definir la brecha tecnológica de las diferentes capacidades del ejército.		Promover la aplicación de la propuesta) como modelo de mejora en la toma de decisiones en las diferentes capacidades de la Fuerza Terrestre, por la especificidad de su aplicación

Capitulo Sexto: Conclusiones y recomendaciones

Conclusiones

Luego del desarrollo de la presente investigación se pudo determinar falencias en la capacidad tecnológica de la capacidad de mando y control mediante una investigación documental y de campo respaldada por técnicas de obtención de datos como la encuesta y la entrevista a expertos en el tema y al personal vinculado al mando y control del ejército ecuatoriano fundamentalmente en la Comandancia General del Ejército. Estas falencias fueron principalmente la obsolescencia tecnológica determinada por la falta de actualización tecnológica de las herramientas utilizadas, además se pudo evidenciar que muchas TIC se encuentran operativas pero que no se encuentran desarrolladas de acuerdo a las demandas actuales en el ámbito de las telecomunicaciones, plataformas de respaldo y compatibilidad; otro falencia constituye el respaldo técnico que no brinda la oportunidad real de aprovechamiento óptimo de la capacidad de muchas herramientas, por diferente motivos entre ellos falta de capacitación del personal responsable, dependencia de terceros (técnicos externos), e incompatibilidad de metodologías y herramientas; además se encuentra como falencia latente el uso inadecuado de la tecnología existente de forma interna y externa lo que supone un riesgo a la seguridad; la interoperabilidad es un punto en el cual la incompatibilidad de sistemas se hace más latente lo que bloquea o retarda procesos inter e intrainstitucionales de coordinación administrativa y operativa. Estos factores se encuentran interrelacionados fundamentalmente con la seguridad de la información ya sea por manejo inadecuado o por limitaciones tecnológicas. Finalmente se pudo evidenciar la deficiencia de la metodología para la gestión tecnológica, lo que dificulta estandarización de procesos

desde la determinación de necesidades hasta la adquisición de tecnología adecuada a las necesidades de mando y control.

Una vez analizada la información necesaria para el desarrollo de la presente investigación y considerando los hallazgos encontrados en la investigación de campo se ha concluido que es necesaria una actualización tecnológica permanente de las TIC de la capacidad de mando y control, dada la importancia que tiene esta capacidad militar en la toma de decisiones, la planificación y la coordinación con el resto de capacidades militares y que influye en la interoperabilidad del sistema de defensa del Estado.

La propuesta planteada se basa en el desarrollo de una metodología como estrategia para la optimización de la gestión de las TIC de mando y control que contempla las distintas fases sobre las cuales pueden ejecutarse procedimientos que puedan determinar las necesidades tecnológicas de la capacidad de mando y control y para la utilización adecuada de las TIC, considerando la importancia de la información que maneja esta capacidad militar y seguridad que debe poseer su gestión adecuada que impida el desarrollo de riesgos y la presencia de amenazas a la seguridad y defensa del Estado.

Recomendaciones

En el contexto de desarrollo y transformación de capacidades es necesario influir en que la innovación generada por los diferentes estudios de las academias militares e institutos de formación militar deben ser estudiados y aprovechados por este proceso que buscan un beneficio institucional y se encuentran respaldados por investigaciones viables y en el contexto de las necesidades actuales de la institución frente a las amenazas ala seguridad que se han presentado en los últimos tiempos.

Es necesario además fomentar y respaldar una cultura organizacional basada en valores institucionales para generar conciencia respecto a la importancia de la gestión

adecuada de la información d y de la tecnología utilizada en la capacidad de mando y control, ya que se ha podido evidenciar que las amenazas actuales utilizan a esta mala gestión como una vulnerabilidad que pude tener consecuencias nefastas para la defensa del Estado y para la eficiencia institucional.

Bibliografía

Andrade, W., Martinez, J., & Pineda, J. (2011). *Las Operaciones de Información en las Guerras de Información.* Bogotá: Universidad Piloto de Colombia.

Banco Mundial. (13 de 1 de 2016). *Tecnologías digitales: Su enorme potencial de desarrollo aun escapa a los 4000 millones de personas que no tienen acceso a Internet.* Obtenido de Banco Mundial: https://www.bancomundial.org/es/news/press-release/2016/01/13/digital-technologies-huge-development-potential-remains-out-of-sight-for-the-four-billion-who-lack-internet-access

Centro de Inteligencia Estratégica. (3 de 2 de 2021). *Plan Específico de Inteligencia 2019-2030.* Obtenido de Plan Nacional de Seguridad Integral: https://www.defensa.gob.ec/wp-content/uploads/downloads/2019/07/plan-nacional-inteligencia-web.pdf

Comando Conjunto de las Fuerzas Armadas. (2019). *Plan de CApacidades COT.* Quito: Ministerio de Defensa Nacional.

COSEDE. (2014). *"Plan de Gobierno Electrónico".* Obtenido de Corporación del Seguro de Depósitos, Fondo de Liquidez y Fondo de Seguros Privados: http://www.cosede.gob.ec/?p=3677.

Cubeiro, E. (2018). Los Sistemas de Mando y Control una visión histórico perspectiva. *Armada de la República de Argentina*, 31-57.

Delgado, H. (12 de 5 de 2019). *¿Qué son las TICs? Tecnologías de la Información y Comunicación.* Obtenido de AKUS: https://disenowebakus.net/tics.php

Díaz, J., & Pérez, A. (2011). Impacto de las Tecnologías de la Información y comunicación para disminuir la brecha digital. *CULTROP*, 81-90.

Dirección de Planificación de la Gestión Institucional del Ejército. (2013). *Estatuto Orgánico de la Gestión Organizacional .* Quito: MIDENA.

DRAE. (8 de 1 de 2021). *EspacioUltraterrestre*. Obtenido de Diccionario Panhispánico: https://dpej.rae.es/lema/espacio-ultraterrestre

Ecuador. (2018). *Política de la Defensa Nacional del Ecuador . Libro Blanco de la Defensa.* Quito: Ministerio de Defensa Nacional.

Ecuador. (2019). *Plan Nacional de Desarrollo "Toda una vida" 2017-2021.* Obtenido de Secretaría Nacional de Planificación y Desarrollo: https://www.planificacion.gob.ec/wp-content/uploads/downloads/2017/10/PNBV-26-OCT-FINAL_0K.compressed1.pdf

El Telégrafo. (2 de 7 de 2020). *Ejército habilita plataforma educativa para cursos de capacitación de soldados*. Recuperado el 6 de 10 de 2020, de https://www.eltelegrafo.com.ec/noticias/sociedad/6/ejercito-plataforma-educativa-capacitacion-soldados

Fojón, E. (2019). Desarrollos tecnológicos militares frente a nuevos conceptos operativos. *Estudios Internacionales y Estratégicos*, on line.

García Martín, R. (2017). *Introduucción a la optimización de operaciones militares.* Madrid: Ministerio de Defensa de España.

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (s.f.). *Metodología de la Investigación.* México, México. Obtenido de Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2006). Metodología de la Investigación. México.

INFODEFENSA. (5 de marzo de 2021). *Ecuador crea el Comando de Ciberdefensa para blindar al país ante ataques cibernéticos.* Obtenido de América, Seguridad: https://www.infodefensa.com/latam/2021/03/05/noticia-39ecuadores-ecuador-inaugura-comando-ciberdefensa.html

Lucena, C., & Porras, H. (2016). *Sistemas de Apoyo a las decisiones.* Santander: Universidad Industrial de Santander.

Méndez, N. (2018). Componentes de las TIC. *Revista Digital*, 36-48.

MIDENA. (2014). *Manual de Conducción Militra.* Sangolquí: CEDE.

Ministerio de Gobierno. (15 de 10 de 2019). *1330 detenidos y 1507 heridos fue el resultado de las paralizaciones en el Ecuador*. Recuperado el 6 de 10 de 2020, de https://www.ministeriodegobierno.gob.ec/1330-detenidos-y-1507-heridos-fue-el-resultado-de-las-paralizaciones-en-el-ecuador/

Molander, R., & Riddle, A. (2018). *Guerra de información estratégica: una nueva cara de la guerra.* New York: RAND.

Monje, C. (2011). *Metdología de la Investigación Cuantitativa y Cualitativa.* Bogotá: EUS.

Monleón, A. (2015). El impacto del Big-data en la Sociedad de la Información. Significado y utilidad. *Historia y Comunicación Social*, 427-445.

Navarro, M. (2020). La ciberseguridad se sitúa en el primer plano. *Byte*, 26-45.

ONU. (2019). *Influencia de las Tecnologías Digitales.* Recuperado el 5 de 12 de 2020, de organización de las Naciones Unidad: https://www.un.org/es/un75/impact-digital-technologies

Peláez, A., & Rodríguez, J. (marzo de 2015). *La Entrevista.* Obtenido de Universidad Autónoma de Madrid Investigación Educativa: https://www.uam.es/personal_pdi/stmaria/jmurillo/InvestigacionEE/Presentaciones/Curso_10/Entrevista.pdf

Persson, M. (2014). *Soporte tecnológico futuro de mando y control. Evaluación del impacto de las tecnologías futuras asumidas en el mando y control cooperativo.* Uppsala : Universidad de Uppsala .

Ríos, D., & Valdivieso, J. (2016). Avances de las tecnologías de la Información y las comunicaciones para la Seguridad y la Defensa. Nuevos modelos de operaciones de seguridad y defensa. *CESEDEN*, 13-33.

Rocha Velandia, T., & Echavarría Suarez, S. (2017). Importancia de las TIC en el ambiente empresarial. *UNISALLE*, 43-65.

Romero, L., & Rivera, D. (2019). *La comunicación en el escenario digital.* México: Pearson.

Romero, M., Figueroa, G., Vera, D., & Parrales, G. (2018). *Introducción a la segurida informática y el análisis de vulnerabilidades.* Portoviejo: Editorial Área de Innovación y Desarrollo,S.L.

Sierra Caballero, F. (2013). La guerra en la era de la información: Propaganda, violencia simbólica y desarrollo panóptico del sistema global de comunicación. *Sphera Pública*, 252-278.

Vargas, R., recalde, L., & Reyes, R. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: Modelo ecuatoriano de gobernanza en ciberdefensa. *Revista Latinoamericana de Estudios de Seguridad*, 31-45.

Anexos