MAESTRÍA EN DEFENSA Y SEGURIDAD
MENCIÓN LOGÍSTICA MILITAR

“ANÁLISIS DE LAS OPERACIONES DE FUERZAS ARMADAS ECUATORIANAS EN EL CIBERESPACIO Y LOS MEDIOS NECESARIOS PARA CONTRARRESTAR EL CIBERESPIONAJE Y EL CIBERSABOTAJE DESDE LA CREACIÓN DEL COMANDO DE CIBERDEFENSA HASTA EL 2022”

TCRN EM PATRICIO ESPINOSA Y TCRN EM CHRISTIAN ESPINOZA

DIRECTOR: CRN EM ÁNGELO SEMANATE

Tabla de contenidos

CAPÍTULO I

Formulación del problema

Formulación del problema

Ciberespionaje y cibersabotaje

“Amenazas relacionadas con el robo de información. Propósitos múltiples: aspectos económicos, causar daños y desprestigio a una institución.”

Ecuador no cuenta con estrategias de seguridad cibernética.

Índice de Ciberseguridad Global 26.3

Formulación del problema

¿Cuál es la situación de las operaciones de Fueras Armadas en el ciberespacio para enfrentar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022?

Antecedentes

Dependencia del ciberespacio en funciones básicas como apoyo logístico, el mando y control de las fueras, información de inteligencia en tiempo real.

Interés por mantener la seguridad nacional del Estado para un desarrollo constante.

Justificación e importancia

Las acciones en el ciberespacio, que tienen cada vez más influencia en las operaciones militares en sus dominios tradicionales (tierra, mar y aire), han irrumpido con fuerza en el marco de la guerra híbrida.

La intervención de las amenazas sustentadas por redes delincuenciales, con carácter dimensional, no tienen limitaciones internas o externas.

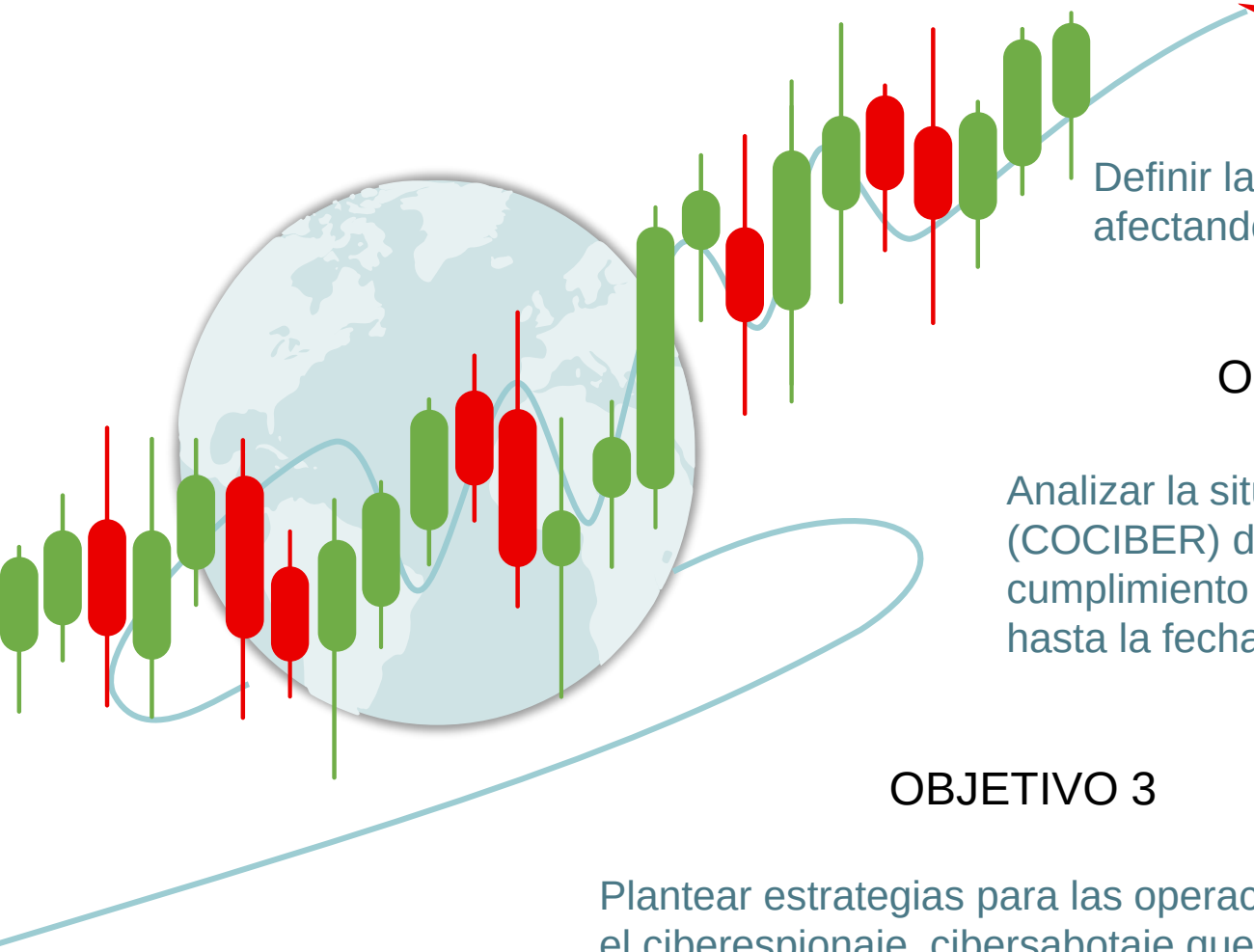
Comprobación de la presencia de las amenazas cibernéticas en el ciberespacio ecuatoriano, sus actores y la afectación a la Seguridad Nacional.

Contar con un marco jurídico que intervenga en las amenazas del ciberespacio.

OBJETIVO GENERAL

- Ejecutar un análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio y los medios para contrarrestar el ciberespionaje, el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022.

Obejtivos específicos



OBJETIVO 1

Definir las amenazas cibernéticas que atentan el ciberespacio afectando a la Seguridad Nacional.

OBJETIVO 2

Analizar la situación actual del Comando de Ciberdefensa (COCIBER) dentro de Fuerzas Armadas y las limitaciones para el cumplimiento de sus objetivos y metas desde su creación en 2014 hasta la fecha.

OBJETIVO 3

Plantear estrategias para las operaciones del ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

CAPÍTULO II

Marco teórico

Antecedentes investigativos

La ciberseguridad emerge ante el creciente uso del ciberespacio como nueva dimensión para la interacción social, resultado de la revolución de la tecnología de la información y comunicación.

Las amenazas recurrentes se acoplan, mantienen la particularidad de “ciber”, que etimológicamente indica “redes informáticas”.
De aquí parte el ciberespionaje y el cibersabotaje .

Fundamentación legal

1. Constitución de la República del Ecuador
2. Política de Defensa Nacional Libro Blanco 2018
3. Política de Ciberseguridad
4. Código Orgánico Integral Penal
5. Ley Orgánica de Telecomunicaciones

Sistema de variables

Variable independiente

Comando de Ciberdefensa
desde 2014 hasta 2022
Operaciones Militares

Dimensiones

- Político
- Institucional
- Militar

Variable dependiente

- Amenazas cibernéticas
- Ciberespionaje, cibersabotaje

Dimensiones

- Institucional
- Tecnológico

Hipótesis

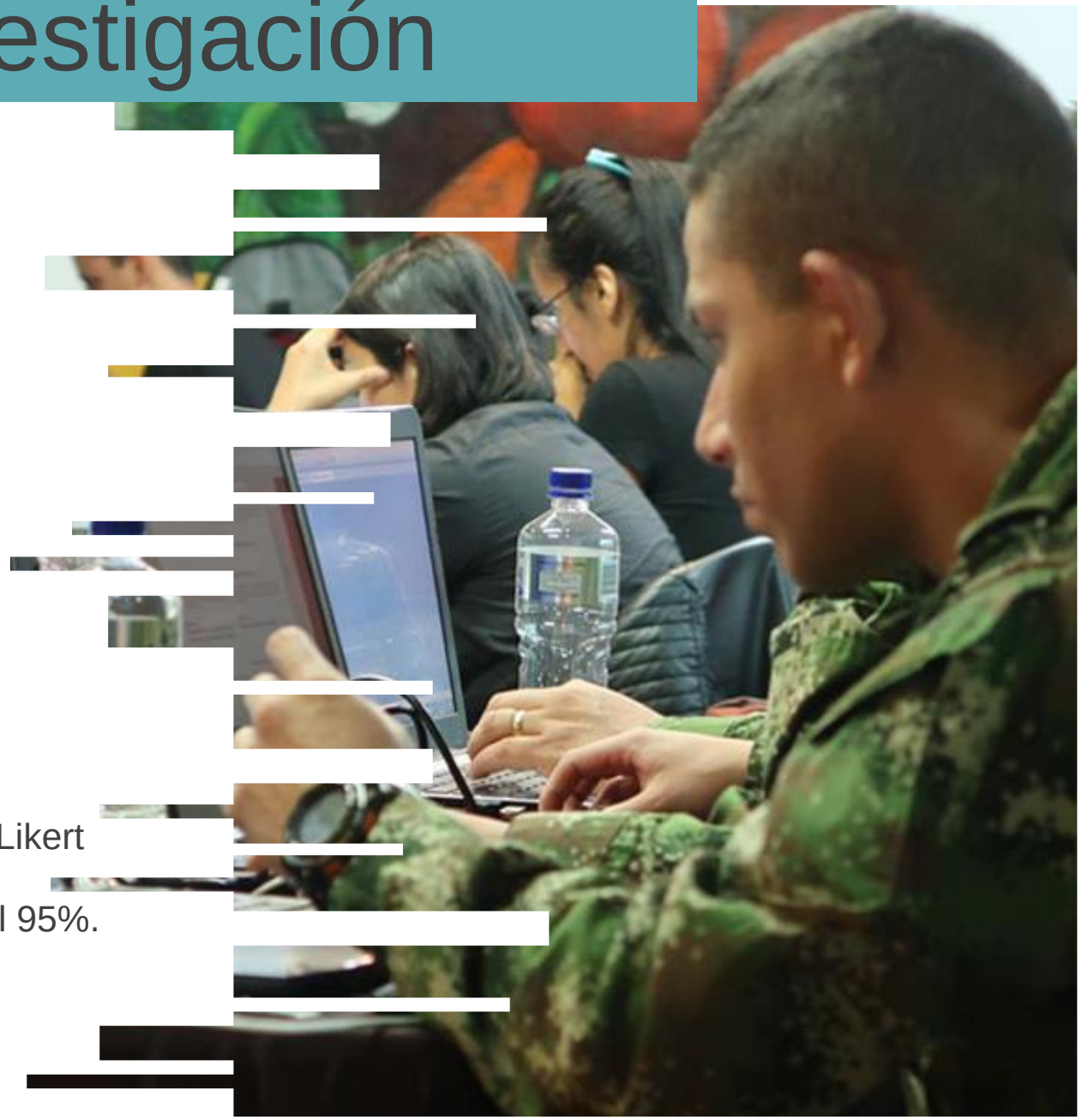
- H0 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio no permitirá enfrentar el ciberespionaje y el cibersabotaje.

- H1 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje.

CAPÍTULO III

Metodología

Modalidad de la investigación



Tipos de investigación

- Exploratorio
- Descriptivo
- Correlacional

Diseño de la investigación

No experimental transversal descriptivo

Enfoque cuantitativo

Población y muestra

- 152 Oficiales
- Muestra 125
- Herramientas: Encuesta – cuestionario Escala de Likert
- Muestreo que cumpla con un nivel de confianza del 95%.

Comprobación de hipótesis

- Un valor p (0,05) más pequeño proporciona una evidencia más fuerte en contra de la hipótesis nula.

CAPÍTULO IV

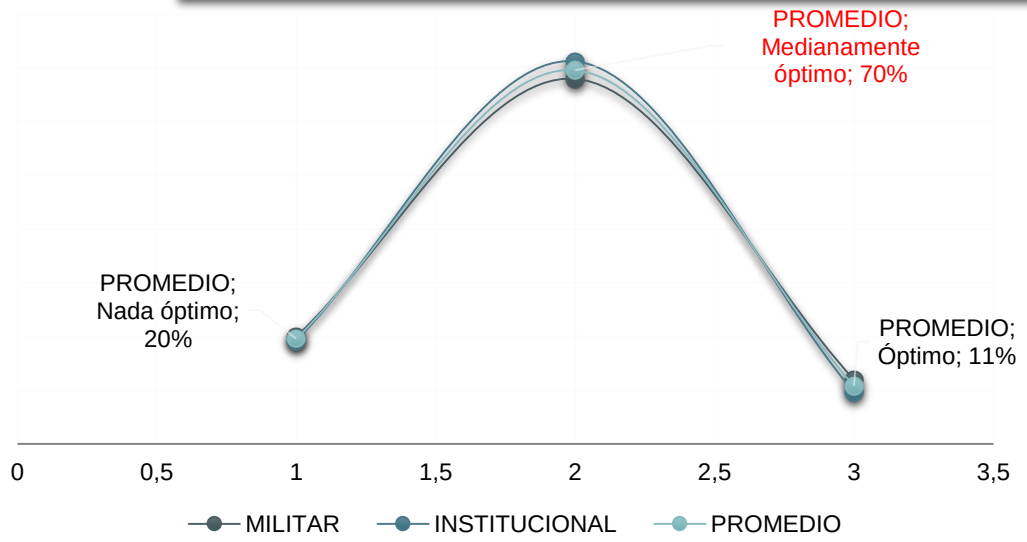
Resultados de la investigación

Variable independiente

Situación actual del Comando de Ciberdefensa desde 2014 hasta 2022

Dimensiones Militar e Institucional

OPCIÓN	MILITAR	INSTITUCIONAL	PROMEDIO
Nada óptimo	20%	19%	20%
Medianamente óptimo	68%	71%	**70%**
Óptimo	12%	10%	11%
TOTAL	100%	100%	100%

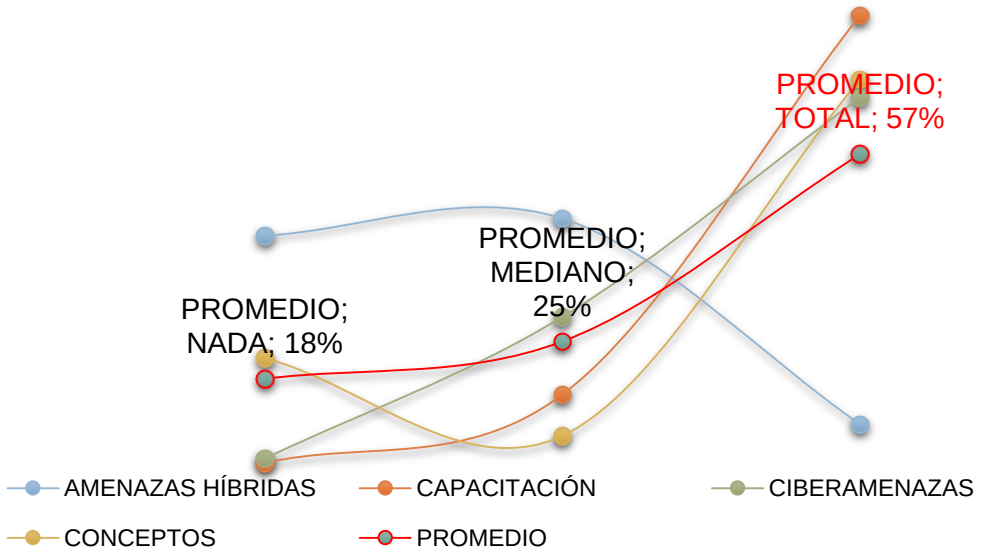


El porcentaje no se podría considerar apto 70% MEDIANAMENTE APTO ya que se trata de dos aspectos fundamentales para una institución

Variable dependiente

Amenazas cibernéticas – Dimensión institucional

	AMENAZAS HÍBRIDAS	CAPACITACIÓN	CIBERAMENAZAS	CONCEPTOS	PROMEDIO
Nada	43%	3%	4%	22%	18%
Mediano	46%	15%	29%	8%	25%
Totalmente	10%	82%	67%	70%	57%
TOTAL	100%	100%	100%	100%	100%



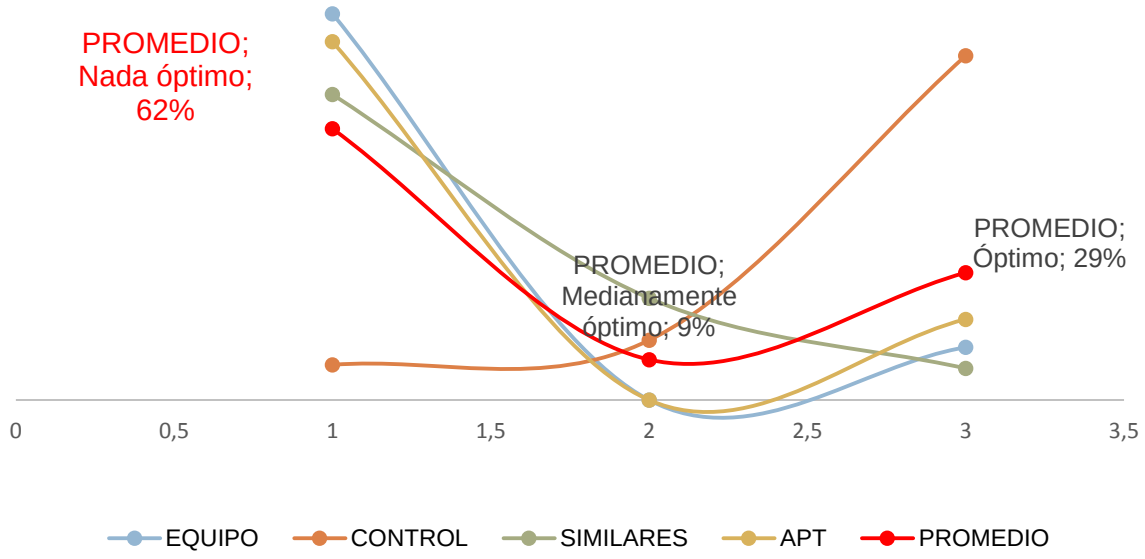
Variable dependiente en 57% en el nivel TOTALMENTE

Para ser un valor realmente óptimo debe pasar el 65% para un cumplimento eficiente y eficaz.

Variable dependiente

Ciberespionaje y cibersabotaje – Dimensión tecnología

	EQUIPO	CONTROL	SIMILARES	APT	PROMEDIO
Nada óptimo	88%	8%	70%	82%	**62%**
Medianamente óptimo	0%	14%	23%	0%	9%
Óptimo	12%	78%	7%	18%	29%
TOTAL	100%	100%	100%	100%	100%

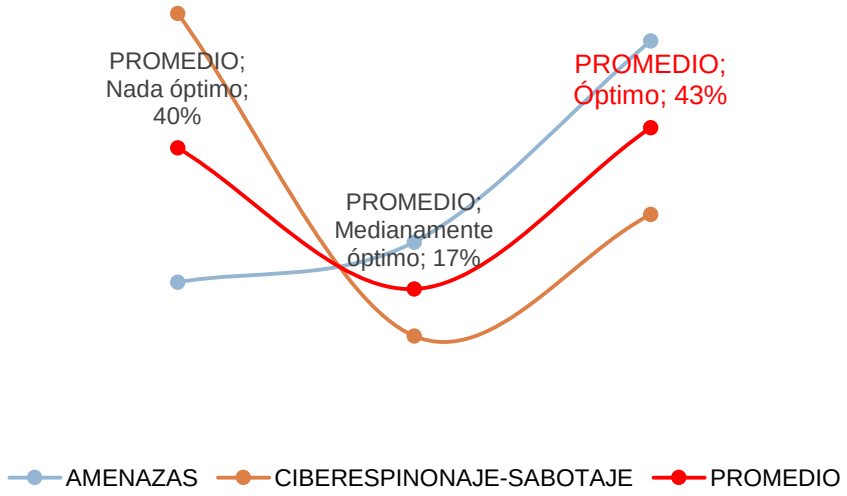


Los encuestados calificaron la dimensión tecnológica como NADA ÖPTIM con el 62%.

Variable dependiente

Ccorrelación dimensiones variable dependiente

	AMENAZAS	CIBERESPINONAJE-SABOTAJE	PROMEDIO
Nada óptimo	18%	62%	40%
Medianamente óptimo	25%	9%	17%
Óptimo	57%	29%	**43%**
TOTAL	100%	**100%**	100%

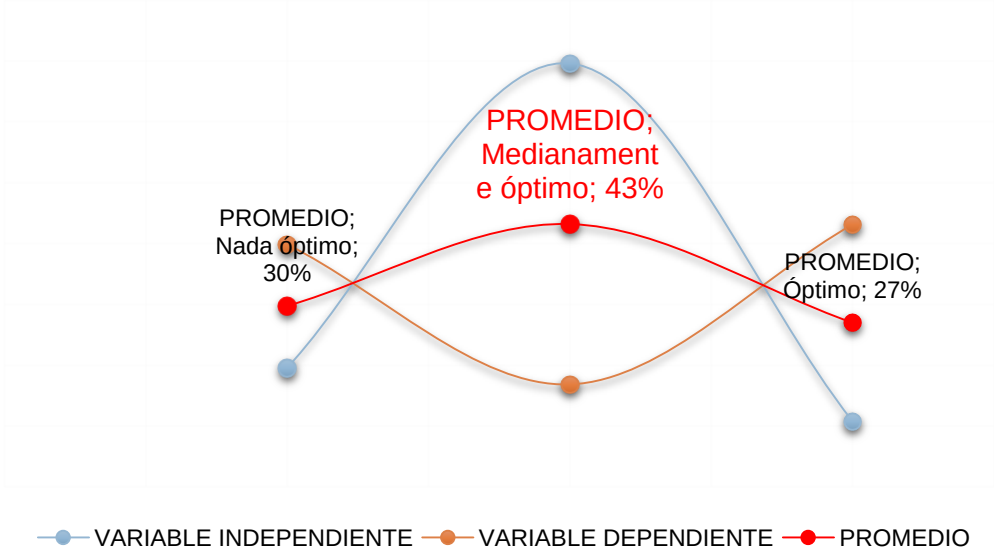


Variable dependiente en 43% en el nivel ÓPTIMO.

Para ser un valor realmente óptimo debe pasar el 65% para un cumplimento eficiente y eficaz.

Correlación entre variables

OPCIÓN	VARIABLE INDEPENDIENTE	VARIABLE DEPENDIENTE	PROMEDIO
Nada óptimo	20%	40%	30%
Medianamente óptimo	70%	17%	**43%**
Óptimo	11%	43%	27%
TOTAL	100%	100%	100%



MEDIANAMENTE del 43%.

Planteamiento de estrategias para las operaciones ciberespacio que contrarresten el ciberespionaje y cibersabotaje que atentan a la Seguridad Nacional, justificando plenamente el presente trabajo.

Discusión

- **Trabajo del Comando de Ciberdefensa de FF.AA está limitado en su trabajo por falta de un marco legal actualizado.**
- **Falta de equipo para control del ciberespacio y capacitación.**
- **Índice de ciberseguridad de Ecuador 26,3/100 le vuelve vulnerable ante las amenazas cibernéticas.**

67%

Responsabilidad de FF.AA

Amenazas híbridas.
Afectación a infraestructuras críticas.
Amenazas híbridas del ciberespacio.

82%

Amenazas persistentes avanzadas

Amenazas del ciberespacio desconocidas.

70%

Nuevos lineamientos

Amenazas con nuevos conceptos que se desconoce su alcance.

Comprobación de la hipótesis

Correlación entre variables

OPCIÓN	VARIABLE INDEPENDIENTE	VARIABLE DEPENDIENTE	PROMEDIO
Nada óptimo	20%	40%	30%
Medianamente óptimo	70%	17%	43%
Óptimo	11%	43%	27%
TOTAL	100%	100%	100%

Prueba estadística descriptiva

Prueba t para medias de dos muestras emparejadas		
	VARIABLE INDEPENDIENTE	VARIABLE DEPENDIENTE
Media	0.3333	0.3329
Varianza	0.1006	0.0205
Observaciones	3.0000	3.0000
Grados de libertad	2.0000	
Estadístico t	0.0016	
P(T<=t) una cola	0.4994	
Valor crítico de t (una cola)	2.9200	
P(T<=t) dos colas	0.9989	
Valor crítico de t (dos colas)	4.3027	

Valor de p de 0.999 superior a la significancia utilizada de 0.05, por lo tanto la hipótesis aceptada es la alterna que dice:

H_1 A partir de la creación del Comando de Ciberdefensa hasta el 2022, el análisis de la capacidad de FF.AA. para utilizar las operaciones militares del ciberespacio permitirá enfrentar el ciberespionaje y el cibersabotaje.

CAPÍTULO V

La propuesta

Datos informativos

Análisis de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio y los medios necesarios para contrarrestar el ciberespionaje y el cibersabotaje desde la creación del Comando de Ciberdefensa hasta el 2022.

Beneficiarios

Directos. -

Fuerzas Armadas del Ecuador, permitiendo el planteamiento de estrategias para las operaciones del ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

Indirectos. –

Todas las instituciones e infraestructuras críticas que están bajo el resguardo de Fuerzas Armadas, cuyo fin es mantener la seguridad y defensa en todos las dimensiones de su entorno.

Ubicación

Distrito Metropolitano de Quito

Antecedentes

- OTAN dice: fracasar cuando hay un nivel inadecuado de concienciación y educación sobre seguridad cibernética.
- Para las FF.AA. el enfoque integral radica en la posibilidad de respaldar y reforzar las capacidades operativas en todos los dominios.
- Las capacidades cibernéticas defensivas disponibles deben ser capaces de proteger la infraestructura de TI de la organización de Defensa.
- Si no es posible reconocer el origen, autor y objetivos del ataque, las posibilidades de respuesta son limitadas.

Justificación

- El ciberespacio es la nueva arena de interacción, cooperación y conflicto de la política global, así como de la intrusión del delito y del crimen, manejados por grupos ilegales.
- Los avances tecnológicos han dado impulso para las acciones beligerantes se realicen con mayor fuerza en el ciberespacio.
- Ecuador en el Índice de Ciberseguridad Global (ICG), 26%., mientras que Colombia presenta el 64% y Chile el 69%, dentro de los mejor punteados de Latinoamérica.

Objetivo general de la propuesta

Plantear estrategias para las operaciones militares en el ciberespacio que contrarresten el ciberespionaje, cibersabotaje que atentan a la seguridad nacional.

Objetivos específicos

- Identificar las amenazas y oportunidades, así como las fortalezas y debilidades de las operaciones de Fuerzas Armadas ecuatorianas en el ciberespacio.
- Estructurar la matriz FODA que permita establecer las estrategias adecuadas a ser planteadas.
- Plantear las estrategias esenciales para las operaciones en el ciberespacio.

Análisis FODA

- **Amenazas**
- La Política de Estado en el campo de la ciberdefensa no es completa, falta lineamientos precisos.
- El nuevo Plan de Desarrollo es muy escueto en los objetivos y políticas para incrementar el índice de ciberseguridad de 26.3 a 55,67.
- Recursos escasos para la implementación de equipos y la debida capacitación.
- Los actores ilegales cuentan con tecnología para operar en el ciberespacio.
- FF. AA no cuenta con equipo actualizado para actuar de manera precisa en el ciberespacio y enfrentar el ciberespionaje y el cibersabotaje.
- Aumento de ciberataques provenientes de grupos delictivos.
- Faltan leyes para la regulación del uso de internet y redes sociales.
- Marco legal inadecuado para garantizar la intervención de FF. AA en el ciberespacio.

Debilidades

- Operaciones en el ciberespacio centralizadas en el Comando de Ciberdefensa de FF.AA.
- Escaso personal capacitado para operaciones de inteligencia para el control de cibersabotaje y ciberespionaje.
- Inadecuada capacitación para hacer frente a las amenazas del ciberespacio.
- Desconocimiento de la magnitud y alcance de las nuevas amenazas híbridas del ciberespacio y Amenazas Persistentes Avanzadas.
- Equipo tecnológico caduco para interceptar las amenazas del ciberespacio.
- Escaso presupuesto para una actualización técnica y

SWOT

Oportunidades

- Decisión del Estado por mejorar las condiciones de la seguridad en el ciberespacio con intervención de FF.AA.
- Crecimiento Tecnológico apropiado para operaciones en el ciberespacio
- Alto nivel de confianza por la institución
- Colaboración con entidades educativas para la innovación de tecnología a través de programas I+D+i

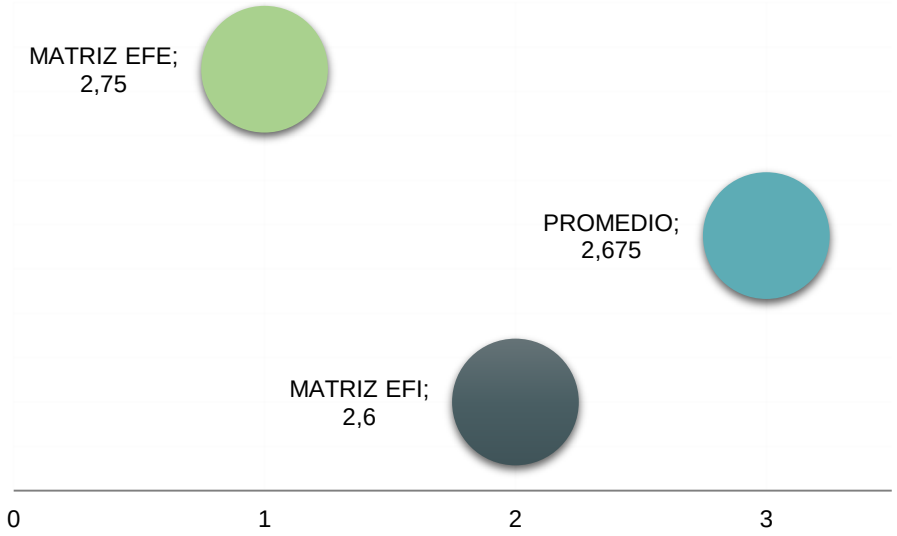
Fortalezas

- Estructura jerárquica propia de las FF. AA fortalecen todas las operaciones militares
- Personal de inteligencia disponible para las operaciones en el ciberespacio.
- Conocimiento del ciberespacio con información de primera mano al nivel político estratégico
- Compromiso de FF. AA por mantener la seguridad en todas las dimensiones.

Diagnóstico FODA

FACTORES EXTERNOS		FACTORES INTERNOS	
Oportunidades	2.00	Fortalezas	2.00
Amenazas	0.75	Debilidades	0.60
MATRIZ EFE	2.75	MATRIZ EFI	2.60

MATRIZ EFE	MATRIZ EFI	PROMEDIO
2,75	2,60	2,675



El promedio de las dos matrices recae en las ESTRATEGIAS DEFENSIVAS destinadas a MANTENER las fortalezas y afrontar las amenazas.

Propuesta

ESTRATEGIAS PARA LAS OPERACIONES MILITARES EN EL CIBERESPACIO QUE CONTRARRESTEN EL CIBERESPIONAJE, CIBERSABOTAJE QUE ATENTAN A LA SEGURIDAD NACIONAL

OBJETIVO GENERAL: Lograr que las operaciones militares en el ciberespacio hagan uso de sistemas de información y telecomunicación seguro para prevenir, detectar y proporcionar una respuesta inmediata a las amenazas del ciberespacio.

OBJETIVO 1: Potenciar la implantación de un marco legal nacional, coherente e integrado a las políticas del Estado, así como a todas las instituciones civiles y militares, públicas y privadas para garantizar la protección de la información, los sistemas y servicios interconectados y las redes que los soportan.

Acción 1.1. Contar con recursos técnicos y humanos para integral un sistema seguro.

Acción 1.2. Mejorar la ciberseguridad en todos los campos, difundiendo cultura de protección de información.

Acción 1.3. Colaborar con la experiencia y liderazgo de la institución para promulgar el uso seguro y responsable de la tecnología de la información y comunicación.

Acción 1.4. Promover la capacitación adecuada y constante al personal específico y destinado al manejo de información y transmisión de datos.

OBJETIVO 2: Garantizar que las redes, los datos y los sistemas que operan en las FF.AA. estén protegidos contra ataques cibernéticos.

Acción 2.1. Diseñar e implementar un marco legal interinstitucional que limite el uso de redes no autorizadas

Acción 2.2. Implementar medidas de seguridad para fortalecer una red o sistema para hacerlo más robusto contra ataques.

Acción 2.3. Utilizar la experiencia institucional, capacidades e influencia únicas para lograr un cambio radical en la seguridad cibernética nacional para responder a las amenazas cibernéticas..

Acción 2.4. impulsar la capacidad de generación y desarrollo de I+D+i en el ciberespacio obteniendo productos propios, seguros y certificados.

OBJETIVO 3: Proteger el tráfico de Internet y telecomunicaciones contra el secuestro por parte de actores malintencionados para evitar el ciberespionaje y el cibersabotaje.

Acción 3.1. Promover la soberanía tecnológica aprovechando de las oportunidades que ofrece la transformación digital, desarrollando industria propia de sistemas de información y comunicación.

Acción 3.2. Mantener la cooperación regional y de países desarrollados para la estabilidad del ciberespacio, sobre todo en lo relacionado al ciberespionaje y cibersabotaje.

Acción 3.3. Fomentar acuerdos bilaterales y multilaterales que aporten con la capacitación de profesionales con conocimientos y habilidades explicitas para el control de las operaciones de inteligencia en el ciberespacio.

Acción 3.4. Proteger las infraestructuras críticas para garantizar el normal funcionamiento y perjuicios al país.

OBJETIVO 4: Incrementar las capacidades de prevención, detección, reacción, recuperación, recuperación, investigación y coordinación para hacer frente a las actividades de actores ilegales que incurren en el ciberespacio.

Acción 4.1. Mejorar las capacidades de detección y análisis de las ciberamenazas para reaccionar con tiempo ante un ataque cibernético que podría afectar a una infraestructura crítica.

Acción 4.2. Fortalecer la cooperación judicial y policial nacional e internacional a través del intercambio de información y de los canales propios de la inteligencia ciberespacial.

Acción 4.3. Desarrollar procesos de prevención y detección incluyendo procedimientos de respuesta ante situaciones de crisis, así como planes contingencia que estén apoyados en el Plan de Seguridad Integral.

Acción 4.4. Fomentar la colaboración ciudadana con información de interés militar para prevenir ataques en el campo cibernético.

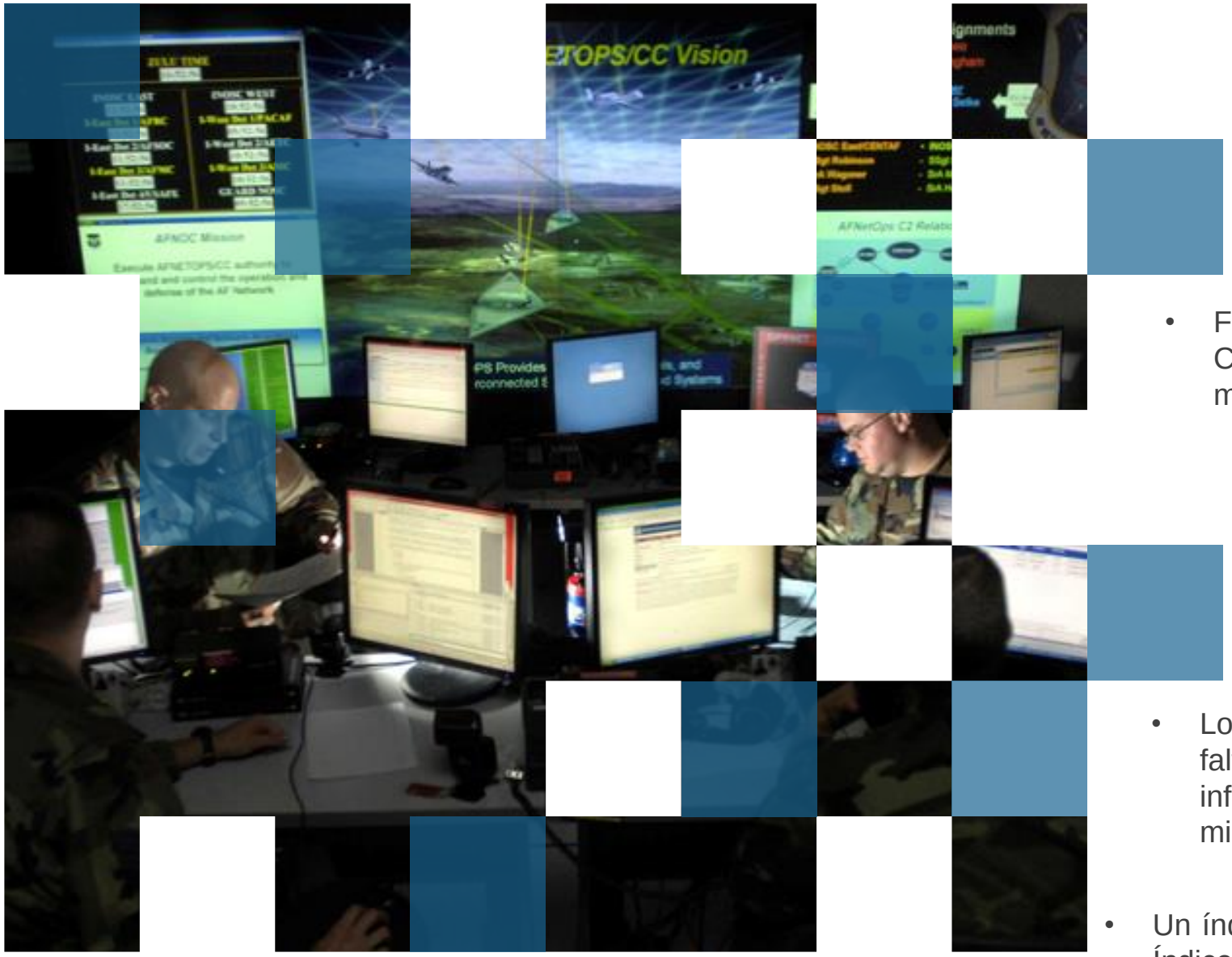
Acción 4.5. Potenciar las capacidades de cibersabotaje y ciberespionaje, mejorando las operaciones de ciberinteligencia.

OBJETIVO 5: Implementar sistemas de información y telecomunicación seguros en las infraestructuras críticas para evitar el cibersabotaje y el ciberespionaje.

Acción 5.1. Impulsar la creación de una normativa para protección de información y transmisión de datos de las infraestructuras críticas.

Acción 5.2. Fomentar la cultura de protección de datos en todas las instituciones públicas y privadas, inclusive en sistemas personales particulares que podrían ser víctimas de un cibersabotaje.

Acción 5.3. Establecer indicadores de avances en el control y manejo de la información y realizar evaluaciones periódicas para identificar posibles entradas de espionaje o amenazas cibernéticas.



Conclusiones

- En el espacio cibernético las amenazas fluyen sin limitación, muchas acogidas a objetivos tradicionales pero con un amplio uso de la tecnología

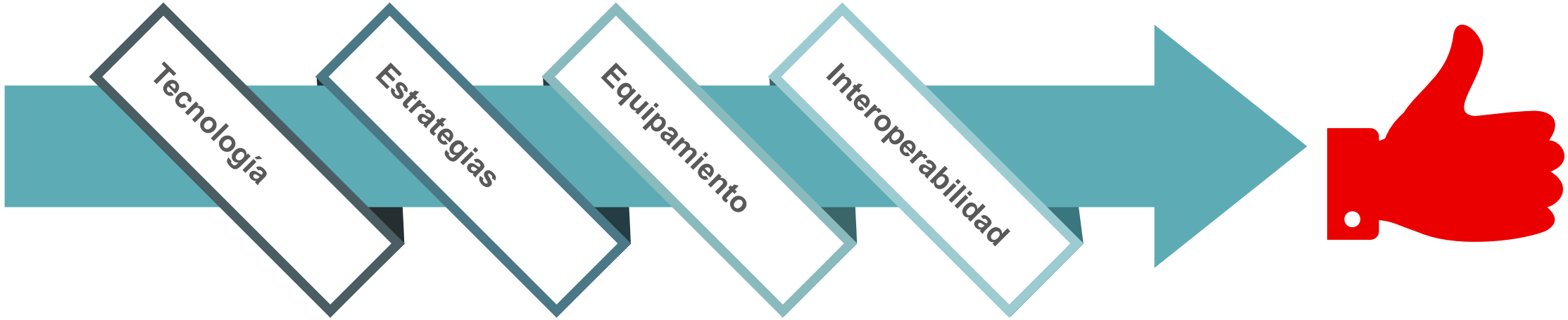
- Falencias para el cumplimiento de los objetivos del Comando de Ciberdefensa, ubicándole en un manejo medianamente óptimo del 68%.

- La correlación de las variables dependiente e independiente y los indicadores trabajados, ubican en un nivel medianamente óptimo del 43% las operaciones militares en el ciberespacio.

- Los factores que aportan para este porcentaje son: la falta de equipo tecnológico, capacitación del personal, influyendo de manera constante en las operaciones militares en el ciberespacio.

- Un índice que ha sido analizado en este trabajo es el Índice de Ciberseguridad Global de Ecuador que se sitúa en el 26% y en el puesto 89 de 150 países analizados.

Recomendaciones



01 Las FF.AA. se enfrentan a situaciones difíciles ante las amenazas híbridas cibernéticas. La tecnología, aprovechando la transferencia digital, aumentan los riesgos en los sistemas de información y transmisión de datos.

02 FF.AA está obligada a establecer estrategias actualizadas, integrales, direccionadas a la capacitación del personal idóneo, equipamiento, concientización en el manejo seguro de la información y de los sistemas que controlan las redes.

03 Se recomienda implementar estas estrategias, así como actividades para el desarrollo y evaluación de las acciones a seguir.

04 Establecer programas y proyectos de I+D+i propios de FF.AA. para implementar sistemas de información y comunicación seguros.


TCRN EM Christian Martínez
TCR EM Jaime Espinoza
Agradecen su atención