ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Departamento de Seguridad y Defensa

MAESTRÍA EN DEFENSA Y SEGURIDAD MENCIÓN EN CONDUCCIÓN MILITAR
COHORTE I

"LA CIBERDEFENSA EN LA FUERZA TERRESTRE ECUATORIANA DESDE UNA VISIÓN PROSPECTIVA AL 2033"

Tcrn. EM Acosta S. Bolívar V. – Tcrn. EM Vizcaíno V. Christian M.

MSC. Muñoz Morales Bethy Andrea

17 de noviembre de 2023

CONTENIDO

- Planteamiento del Problema
- Marco Teórico
- Marco Metodológico
- Análisis de Resultados
- Propuesta del Proyecto

OBJETIVO

Determinar los actores del sistema, factores de cambio, hechos portadores y los posibles escenarios futuros de la ciberdefensa al año 2033 que permitan el desarrollo de la capacidad ciberespacial en la Fuerza Terrestre ecuatoriana.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

PLANTEAMIENTO DEL PROBLEMA

El problema


Servicios esenciales que requieren ser asegurados
Dependencia del ciberespacio por la globalización de la era digital
Uso exponencial de plataformas de almacenamiento en IE
PROBLEMA
Ciberespacio no es dominio emergente
PDN 2018, reconoce como agresión la vulneración de SI
Aparecimiento de ciberamenazas debido al CUT

Formulación del problema

Cuáles son los actores del sistema, factores de cambio, hechos portadores

Posibles escenarios futuros de la ciberdefensa al año 2033

Desarrollo de la capacidad ciberespacial en la Fuerza Terrestre

Preguntas de investigación

¿Qué aspectos se deben tomar en cuenta en el estudio prospectivo de la ciberdefensa en la Fuerza Terrestre al 2033?

¿Cuáles son las capacidades específicas de la ciberdefensa que debe desarrollar la Fuerza Terrestre al 2033?

¿Para construir el mejor escenario futuro de la ciberdefensa en la Fuerza Terrestre, cuáles son las mejores estrategias se deben diseñar en el presente?

Objetivos específicos

- Realizar un diagnóstico sobre la situación actual de la capacidad de ciberdefensa en la Fuerza Terrestre.
- Determinar los actores y variables que influyen en la capacidad de ciberdefensa de la Fuerza Terrestre ecuatoriana, con respecto a los posibles escenarios planteados.
- Establecer los hechos portadores de futuro que influyen en las capacidades de ciberdefensa.
- Construir los escenarios apuesta, tendencial y cisne negro de la ciberdefensa en la Fuerza Terrestre ecuatoriana al año 2033.
- Proponer estrategias de ciberdefensa que permitan alcanzar el escenario apuesta al año 2033.

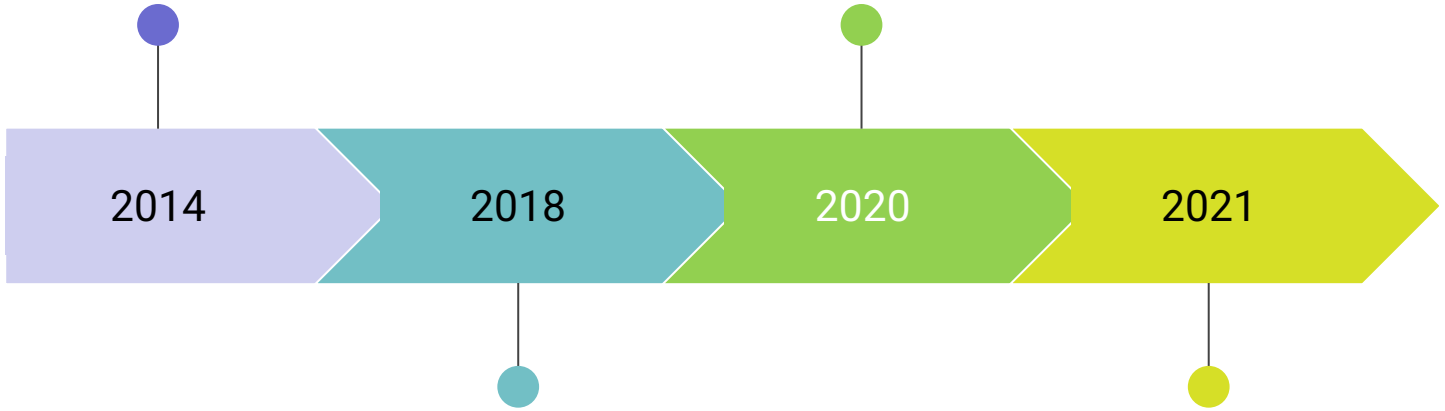
ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

MARCO TEÓRICO

Estado del arte

Estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas del Ecuador.
Peralvo Edwin

Análisis de la situación actual de la Ciberdefensa en la Fuerza Terrestre 2020.
Abad Antonio

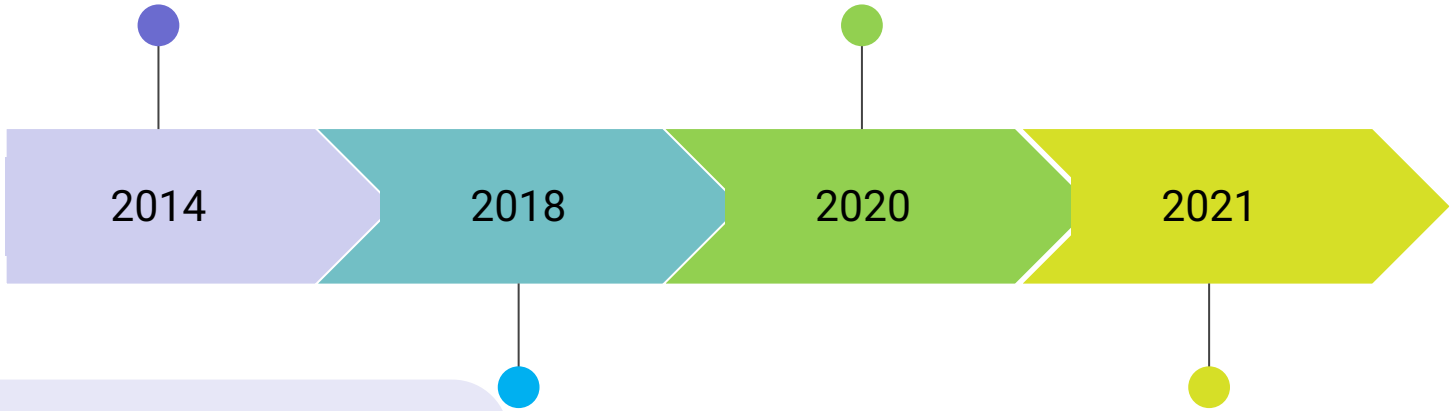


Ciberdefensa en el estado ecuatoriano periodo 2013-2016.
Abad Nora

Proyección de la ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021.
Jácome Luis

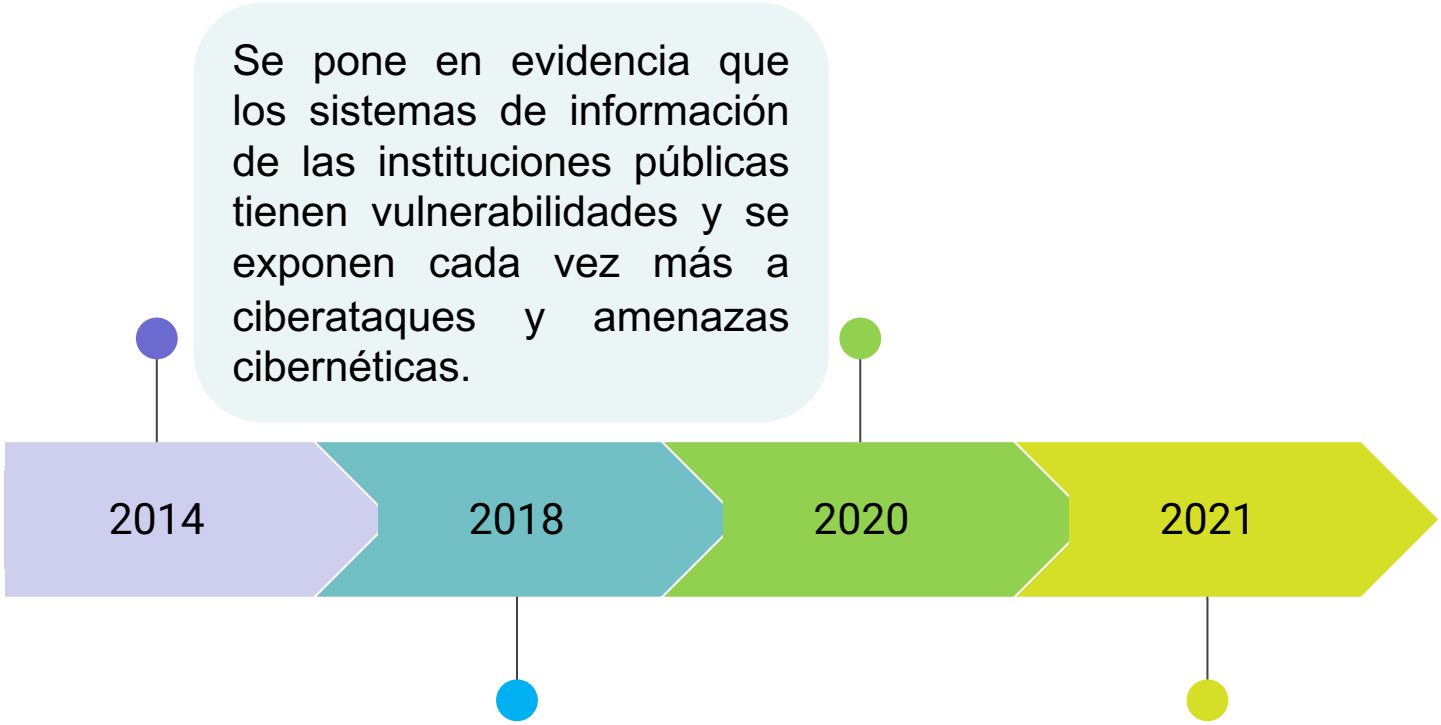
Estado del arte

Estudio prospectivo de la Ciberdefensa en las Fuerzas Armadas del Ecuador. **Peralvo Edwin**



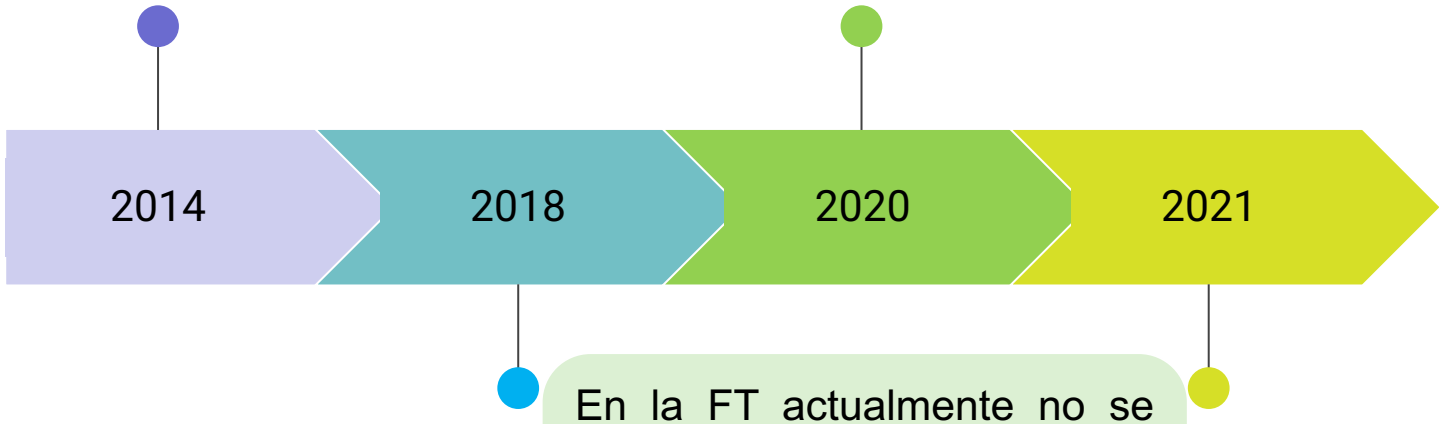
(COCIBER) ha recibido el presupuesto adecuado para el desarrollo de capacidades con las que se pueda enfrentar, neutralizar o adaptarse a los efectos de ciberamenazas.

Estado del arte



Estado del arte

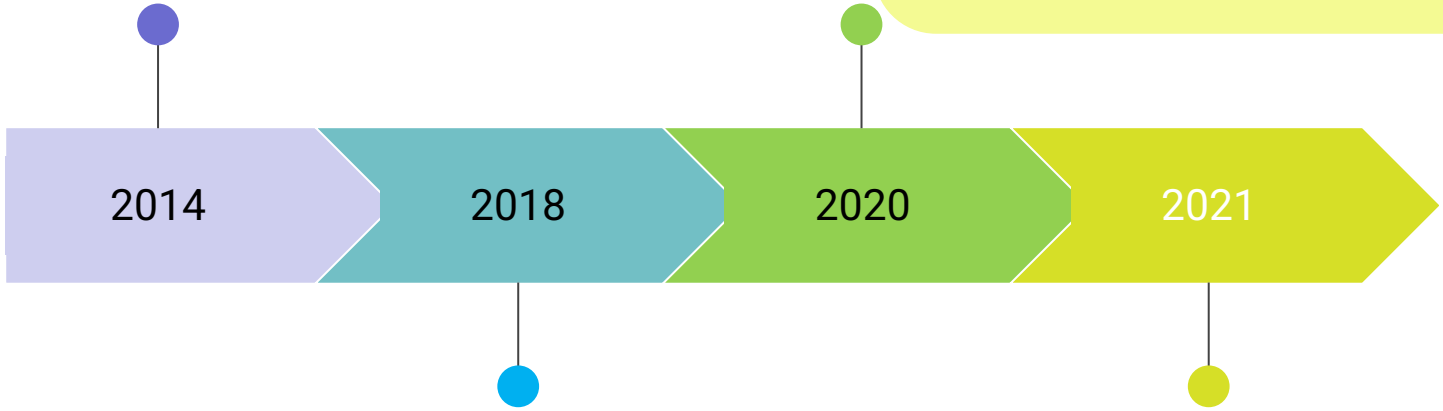
Análisis de la situación actual de la Ciberdefensa en la Fuerza Terrestre 2020.
Abad Antonio



En la FT actualmente no se ha implementado unidades o dependencias con estas capacidades, peor aún programas de capacitación, recursos y desarrollo de procesos

Estado del arte

Describe que Fuerzas Armadas deberá estandarizar los procedimientos de seguridad de manera que permitan prevenir y mitigar los posibles ataques en el ciberespacio.



Proyección de la ciberdefensa en las Fuerzas Armadas del Ecuador para el 2021.
Jácome Luis

Fundamentación legal

Art. 3, 16, 66 (Núm., 19 y 21), 158, 313, y 393

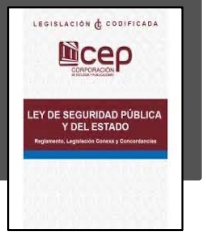
Constitución de la República del Ecuador

Art 178, 188, 190, 202, 229 al 234, 262.

Código Orgánico Integral Penal

Art. 2,3,10,11,38, 41y 43.

Ley de Seguridad Pública y del Estado



Documentos directrices

27001, 27002, 27005, 27031.

Normas técnicas

Carta de Naciones Unidas
Convenios y protocolos

Instrumentos Internacionales

- Estrategia de ciberseguridad
- Política de ciberseguridad
- Estrategia de ciberdefensa
- Guía Política -Estratégica

Instrumentos Nacionales

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

MARCO METODOLÓGICO

Metodología

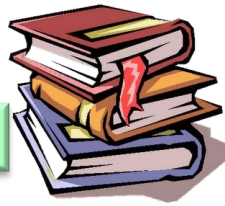
Enfoque cualitativo y cuantitativo.

Enfoque de la investigación

Por sus fuentes

Primarias

Secundarias



Modalidad de la investigación

Exploratoria y correlacional

Por el alcance

Diseño de la investigación

No experimental

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

ANÁLISIS DE RESULTADOS

Prospectiva francesa

1 PROBLEMÁTICA

2 ANÁLISIS PESTM

3 ÁRBOL DE GIGET

4 ÁBACO DE RÉGNIER

5 MATRIZ MORFOLÓGICA

6 DESCRIPCIÓN ESCENARIOS

7 MATRIZ IGO

8 JUEGO DE ACTORES

1 Problemática

a. **Falta de presupuesto** para mantenimiento, renovación, modernización o compra de equipo tecnológico.

b. **Falta de capacitación** del personal técnico de ciberdefensa.

c. **Obsolescencia del equipo tecnológico**.

d. **Falta de un horizonte a mediano plazo** que permita **proyectar** la **ciberdefensa** en la Fuerza Terrestre

e. **Falta de equipamiento y material** técnico para el mantenimiento de la infraestructura tecnológica.

f. **Falta de capacidad técnica** para la modernización permanente de los aplicativos y sistemas de ciberdefensa.

Problemática

g. **Falta de personal, material y equipo** tecnológico para la defensa de la infraestructura digital de la Fuerza Terrestre.

h. **Falta de personal, material y equipo tecnológico** para la exploración del ciberespacio (identificar ciberamenazas a la infraestructura crítica de la F.T)

i. **Falta de personal, material y equipo tecnológico** para la respuesta contra ciberamenazas a la ejecución de las operaciones en el ámbito externo e interno.

j. **Falta de marco normativo** en temas de ciberdefensa.

k. **Falta de cultura de ciberseguridad** en el personal de la F.T.

l. **Falta de cooperación internacional** en temas de ciberdefensa

Problema

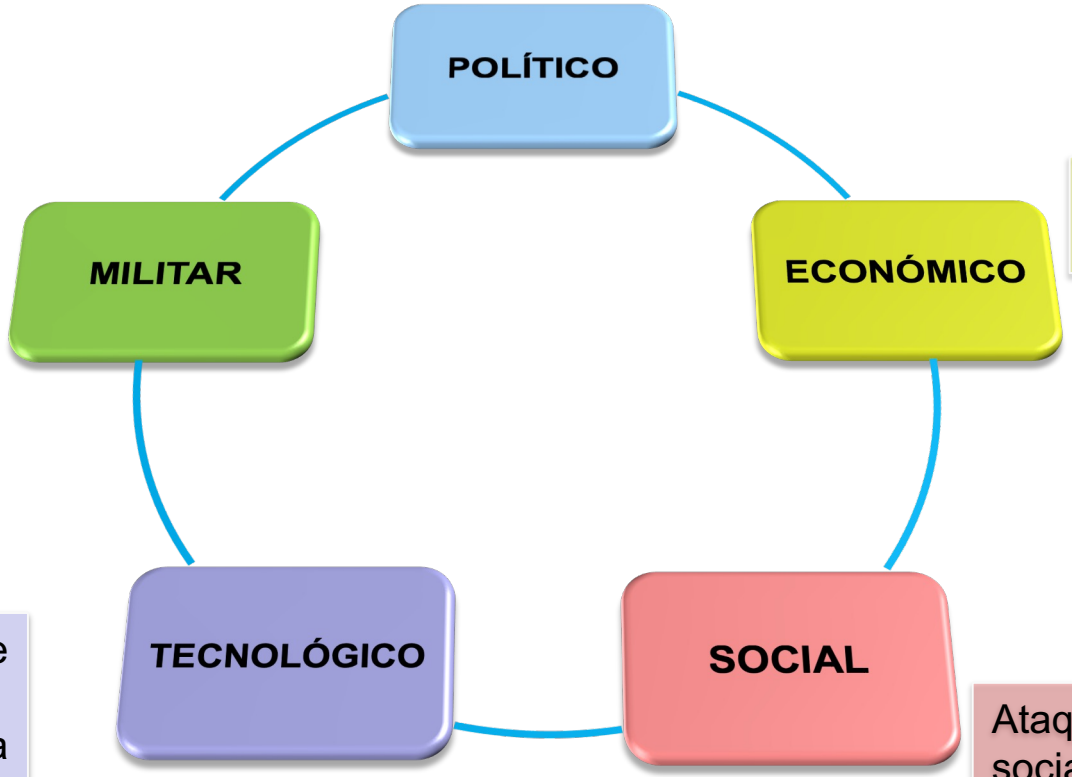
La planificación estratégica permitirá, tener una consciencia situacional de lo que ocurre en el quinto dominio de la guerra, ya que esta incluye; el desarrollo de capacidades para detectar y analizar la naturaleza de las ciberamenazas, desarrollar la doctrina de ciberdefensa, formación de cibersoldados y por último los procedimientos organizativos y tecnológicos que deberán ser considerados por la Fuerza Terrestre para la implementación del Grupo de Ciberdefensa (GRUCIBER).

Interrogante fundamental: ¿Qué estrategias se deben plantear en el presente para construir el mejor escenario futuro de la ciberdefensa en la Fuerza Terrestre?

Tema. *"La Ciberdefensa en la Fuerza Terrestre ecuatoriana desde una visión prospectiva al 2033".*

2 Análisis del macroambiente PESTM

Hipótesis de conflicto interno por poder y amenazas híbridas



Incremento de ciberespionaje y ciberataques a la infraestructura digital de la FT.

Presupuesto e inversión insuficiente

Falta de Infraestructura tecnológica para gestión de ciberdefensa en la F.T.

Ataques de la protesta social al Ejército mediante el uso del ciberespacio.

3 Árbol de GIGET o competencias

Componentes	Pasado	Presente	Futuro	Factor de cambio
	1998	2023	2033	
Productos y servicios	Apoyo a la seguridad de la información digital de la FT.	Ejecución de operaciones de ciberseguridad para la protección de la infraestructura de la FT.	Operaciones de ciberdefensa en apoyo a las operaciones de defensa del territorio nacional y ámbito interno desarrolladas por la FT.	Cambio de teatros de operaciones para el empleo (externo e interno)
Capacidades	Equipos y sistemas con tecnología analógica	Equipos y herramientas de ciberseguridad con capacidades básicas para su empleo.	Equipos y herramientas de ciberdefensa con capacidades tecnológicas modernas para el empleo.	Herramientas de ciberdefensa de última generación
	Unidades de comunicaciones en todos los niveles de la FT.	Grupo de Ciberdefensa de la FT.	Grupo de Ciberdefensa de la FT. y unidades menores de ciberdefensa en las divisiones y brigadas de la FT.	Unidades de ciberdefensa en los niveles de la FT para cumplir misiones en el ciberespacio.
	Personal de comunicaciones capacitado para proteger la información digital de la FT.	Personal especialista capacitado para operaciones de defensa.	Personal especialista capacitado para operaciones de defensa, exploración y respuesta.	Personal de comunicaciones capacitado en operaciones de ciberdefensa.
	Capacidades propias para el mantenimiento de los equipos informáticos de la FT.	Capacidades propias de mantenimiento preventivo de los equipos y herramientas de ciberdefensa.	Capacidades propias de mantenimiento correctivo de los equipos y herramientas de ciberdefensa.	Mantenimiento con transferencia tecnológica, certificados por organismos internacionales.
Conocimientos / recursos	Conocimientos para configurar equipos informáticos.	Conocimientos para ejecutar operaciones de defensa y exploración en el ciberespacio.	Conocimientos para ejecutar operaciones de defensa exploración y respuesta en el ciberespacio.	Capacitación en el uso de nuevas tecnologías de ciberdefensa.
	Conocimientos en: Operaciones de seguridad informática. Actividades de certificación informática.	Conocimientos en: Operaciones del Centro de Operaciones de ciberseguridad (SOC). Actividades de empleo de sistemas de ciberdefensa con certificación nacional.	Conocimientos en: Operaciones en el Centro de Fusión Cibernético. Actividades de empleo de sistemas de ciberdefensa con certificación internacional.	- Cumplimiento de operaciones de ciberdefensa. - Certificaciones de empleo de equipos de ciberdefensa.
	Conocimiento de: Mantenimiento nivel I (Básico)	Conocimiento de: Desarrollo e implementación de políticas de ciberseguridad (EGSI) en la FT.	Conocimiento de: Desarrollo e implementación de políticas de ciberdefensa con estándares internacionales en la FT.	Certificaciones tecnológicas de ciberseguridad y ciberdefensa.

Variables estratégicas

Coeficiente de experta

Expertos	Coeficiente de conocimiento	Coeficiente de argumentación	Conocimiento de competencia experta
Henry Delgado Salvador	0,6	0,8	0,7
Diego Chiza López	0,9	0,9	0,9
Bolívar Acosta Sánchez	0,9	0,85	0,875
Christian Vizcaíno Villavicencio	0,9	0,85	0,875
José Ramos Vargas	1	0,9	0,95
Gustavo Santiago	0,9	0,95	0,925
Paúl Machado Soto	0,6	0,9	0,75
Marcelo López Báez	0,6	0,9	0,75
Pablo Paredes Valencia	0,6	0,9	0,75

4 Ábaco de Régnier

Nro.	Lista de variables	Experto 1 DCL	Experto 2 BAS	Experto 3 CVV	Experto 4 JRV	Experto 5 GS
1	Marco regulatorio en el ciberespacio.	5	4	4	5	5
2	Cumplimiento de operaciones de ciberdefensa.	5	5	5	5	5
3	Gestión política en ciberdefensa.	4	3	3	4	3
4	Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	5	4	4	5	5
5	Conocimiento del nivel político de la defensa del ciberespacio.	5	4	3	4	4
6	Presupuesto para un grupo con capacidades de ciberdefensa.	5	5	5	5	5
7	Políticas de optimización de recursos.	4	5	4	3	2
8	Presupuesto para capacitación en ciberdefensa.	4	4	5	5	3
9	Presupuesto para mantenimiento de equipo.	4	3	3	4	2
10	Presupuesto para licencias, programas y herramientas tecnológicas.	4	4	3	4	3
11	Capacidad de ciberseguridad para atender demanda de la sociedad civil.	4	4	4	4	3
12	Cambio de teatros de operaciones para el empleo de ciberdefensa	5	3	5	4	3
13	Políticas estatales para transparentar procesos de compras.	3	3	3	4	4
14	Capacidades de ciberseguridad y ciberdefensa para apoyar a instituciones del Estado.	3	3	3	2	2
15	Apoyar al desarrollo de una cultura de ciberseguridad en la sociedad.	5	5	5	5	5
16	Equipos y herramientas de ciberdefensa de última generación.	5	5	5	5	5
17	Actualización de ciberdefensa on-line, virtuales o mediante red de datos.	5	5	4	4	4
18	Mejoramiento tecnológico de capacitación en ciberdefensa.	4	3	4	4	4
19	Mejoramiento de infraestructura tecnológica para ciberdefensa.	4	2	4	3	1
20	Recurso humano capacitado en operaciones de ciberdefensa.	5	5	5	5	5
21	Cumplimiento de protocolos de protección de información digital.	5	4	4	5	4
22	Capacidad de ciberdefensa a nivel de seguridad del Estado.	4	4	4	3	2
23	Entrenamiento en operaciones de ciberdefensa.	4	4	3	4	4

LEYENDA	
Muy Probable	5
Probable	4
Duda	3
Improbable	2
Muy Improbable	1

Ábaco de Régnier

Ordenado y priorizado

Nro.	Lista de variables	Experto 1 DCL	Experto 2 BAS	Experto 3 CVV	Experto 4 JRV	Experto 5 GSA
2	Ejecución de operaciones de ciberdefensa.	5	5	5	5	5
7	Presupuesto para un grupo con capacidades de ciberdefensa	5	5	5	5	5
15	Apoyar al desarrollo de una cultura de ciberseguridad	5	5	5	5	5
28	Equipos y herramientas de ciberdefensa de última generación	5	5	5	5	5
29	Recurso humano capacitado en operaciones de ciberdefensa.	5	5	5	5	5
30	Marco regulatorio en el ciberespacio.	5	5	5	4	4
4	Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	5	5	5	4	4
12	Doctrina de operaciones en el ciberespacio.	5	5	5	4	4

LEYENDA	
Muy Probable	5
Probable	4
Duda	3
Improbable	2
Muy Improbable	1

5 Construcción de escenarios

Matriz morfológica

Variables estratégicas	Estados o hipótesis del futuro				
	Hipótesis Optimista "AMERICANO"	Hipótesis Pesimista "BRASILEÑO"	Hipótesis Tendencial "ECUATORIANO"	Hipótesis Cisne Negro "VENEZOLANO"	Hipótesis Apuesta "ESPAÑOL"
Ejecución de operaciones de ciberdefensa.	Permanente	Mínima	Parcial	Inexistente	Continua
Presupuesto para un grupo de con capacidades de ciberdefensa.	Elevado	Insuficiente	Reducido	Nulo	Suficiente
Apoyar al desarrollo de una cultura de ciberseguridad.	Estable	Mínimo	Parcial	Irreal	Continuo
Equipos de ciberdefensa de la FT de última generación	Elevado	Reducido	Bajo	Insubsistente	Alto
Recurso humano capacitado en operaciones de ciberdefensa.	Permanente	Mínimo	Parcial	Inexistente	Equilibrado
Marco regulatorio en el ciberespacio.	Excelente	Pésimo	Improcedente	Nulo	Moderado
Reducir las vulnerabilidades cibernéticas en la infraestructura tecnológica digital.	Permanente	Imperceptible	Limitada	Inefectiva	Continua
Doctrina de operaciones en el ciberespacio.	Elevada	Incompleta	Baja	Nula	Suficiente

Líneas de acción

Desarrollar capacidades de ciberdefensa

Consolidar la ejecución de operaciones en el ciberespacio

Desarrollar un marco regulatorio, una cultura de ciberseguridad y una doctrina de ciberdefensa

Proteger la infraestructura tecnológica digital de la Fuerza Terrestre

6 Descripcción de escenarios

Escenario o hipótesis de fururo

Escenario Apuesta al 2033

Se caracteriza por: tener una **CONTINUA** ejecución de las operaciones de ciberdefensa, un **SUFICIENTE** presupuesto para disponer de un grupo de ciberdefensa con capacidades de defensa, exploración y respuesta, un **CONTINUO** apoyo de la FT. al desarrollo de la cultura de ciberseguridad, un **ALTO** número de equipos y herramientas de ciberdefensa de la FT. de última generación, con un **EQUILIBRADO** recurso humano capacitado en operaciones de ciberdefensa, con un **MODERADO** marco regulatorio en el ciberespacio, con una **CONTINUA** reducción de las vulnerabilidades cibernéticas en la infraestructura tecnológica digital, y una **SUFICIENTE** doctrina de operaciones en el ciberespacio.

7 Matriz IGO

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario APUESTA	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
Ejecución de operaciones de ciberdefensa.	Continua	Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	Estableciendo un equipo de respuesta a incidentes seguridad informática que le permita ejecutar operaciones de defensa en el ciberespacio.	20	5	Urgente
			Planificando ciberoperaciones de defensa y respuesta en función de resultados de ciberinteligencia.	25	5	Urgente
Presupuesto para un grupo con capacidades de ciberdefensa.	Suficiente	Optimizar el presupuesto suficiente para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	Presentando proyectos integrales para que se tramiten a través de acuerdos internacionales para el desarrollo de capacidades de ciberdefensa.	25	3	Necesaria
			Fortaleciendo acuerdos con empresas privadas dedicadas al ámbito de ciberseguridad para el apoyo técnico económico.	20	1	Necesaria
Desarrollo de una cultura de ciberseguridad.	Continuo	Generar productos para el continuo apoyo al desarrollo de una cultura de ciberseguridad.	Planificando y ejecutando cursos permanentes de ciberseguridad para todo el personal de la Fuerza Terrestre a través del Comando de	20	1	Necesaria

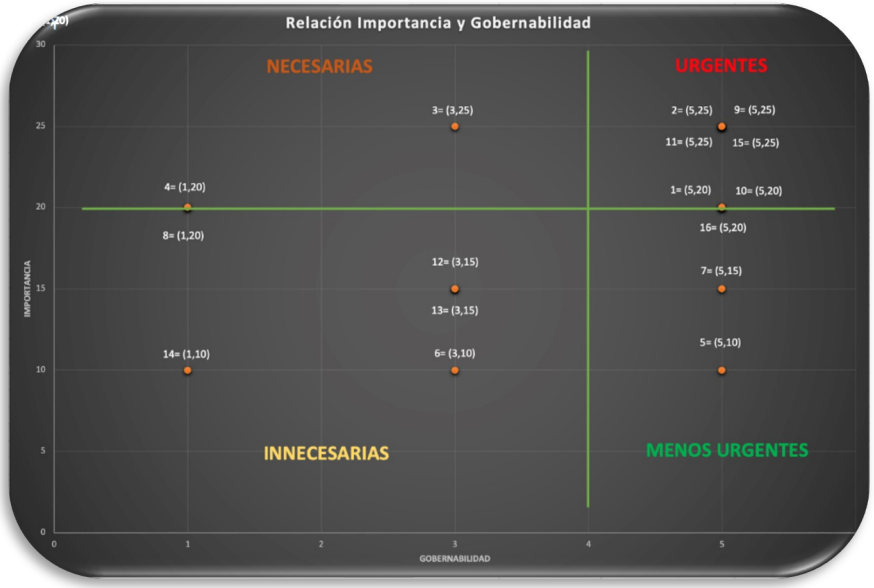
Matriz IGO

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario APUESTA	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
			Concientizando al personal en ciberseguridad a través de una política, impulsada del Comando General.	10	3	Innecesaria
Herramientas y equipos de ciberdefensa de última generación.	Alto	Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	Negociando con empresas pares para la implementación de herramientas de ciberdefensa a bajos costos.	15	5	Menos urgente
			Impulsando el desarrollo de conocimiento a través de los Centros de Investigación, para eliminar la dependencia extranjera.	20	1	Necesaria
Recurso humano capacitado en operaciones de ciberdefensa	Equilibrado	Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa	Creando una subespecialidad de ciberdefensa en la Fuerza Terrestre.	25	5	Urgente
			Adiestrando y entrenando en la planificación y ejecución de ciberoperaciones al personal de ciberdefensa.	20	5	Urgente

Matriz IGO

Variables estratégicas	Hipótesis apuesta "Español"	Objetivo escenario APUESTA	Acciones estratégicas	Importancia	Gobernabilidad	Tipo de acciones
Marco regulatorio en el ciberespacio.	Moderado	Alcanzar un moderado con marco regulatorio en el ciberespacio.	Promoviendo reformas legales, que legalicen el empleo de la Fuerza Terrestre en el ciberespacio.	25	5	Urgente
			Proponiendo reglas de enfrentamiento y normas de comportamiento en el ciberespacio.	20	1	Necesaria
Reducir las vulnerabilidades cibernéticas en la ITD.	Continua	Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD	Incrementando la capacidad de monitoreo, detección y eliminación de ciberamenazas en la ITD.	20	1	Necesaria
			Ejecutando ciberoperaciones conjuntas con el COCIBER y el CIES, para la reducción de vulnerabilidades cibernéticas en la ITD	10	1	Innecesaria
Doctrina de operaciones en el ciberespacio.	Suficiente	Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	Generando la doctrina básica de ciberoperaciones	25	5	Urgente
			Participando en ejercicios de ciberdefensa nacionales e internacionales en todos los niveles de mando.	20	1	Necesaria
TOTAL				**300**		
Valor establecido como base				**300**		

Relación de importancia y gobernabilidad



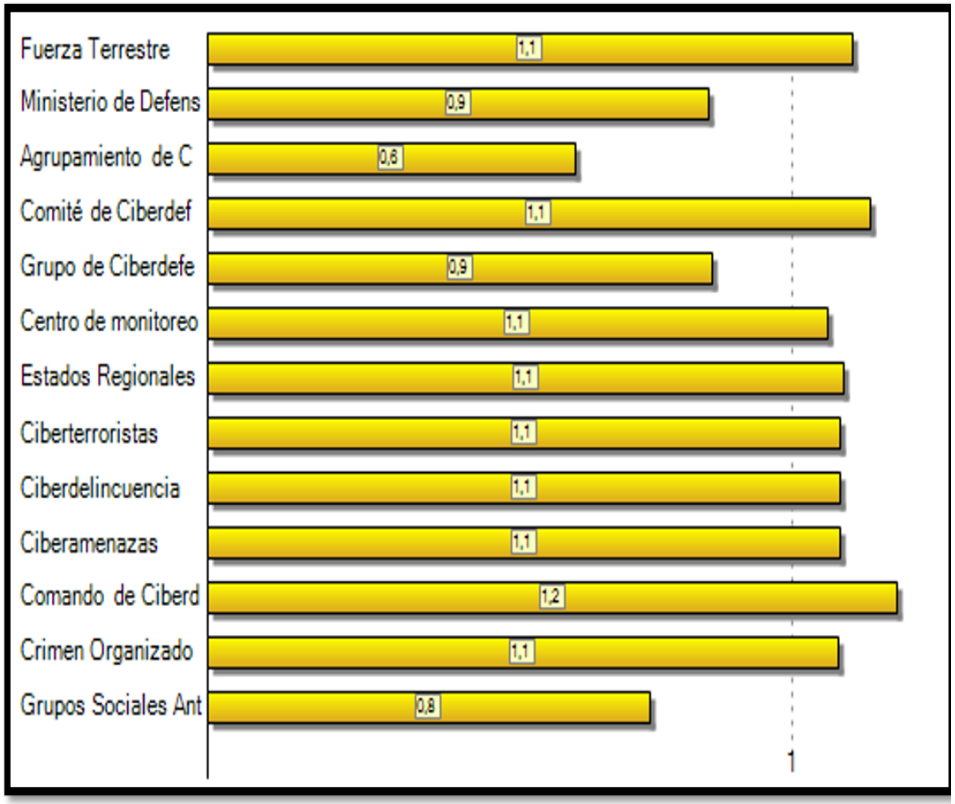
Acciones estratégicas urgentes		
Acciones	**Gobernabilidad**	**Importancia**
Estableciendo un equipo de respuesta a incidentes seguridad informática que le permita ejecutar operaciones de defensa en el ciberespacio.	20	5
Planificando ciberoperaciones de defensa y respuesta en función de resultados de ciberinteligencia.	25	5
Creando una subespecialidad de ciberdefensa en la Fuerza Terrestre.	25	5
Adiestrando y entrenando en la planificación y ejecución de ciberoperaciones al personal de ciberdefensa.	20	5
Promoviendo reformas legales, que legalicen el empleo de la Fuerza Terrestre en el ciberespacio.	25	5
Generando la doctrina básica de ciberoperaciones	25	5
Acciones estratégicas necesarias		
Presentando proyectos integrales para que se tramiten a través de acuerdos internacionales para el desarrollo de capacidades de ciberdefensa.	25	3
Fortaleciendo acuerdos con empresas privadas dedicadas al ámbito de ciberseguridad para el apoyo técnico económico.	20	1
Planificando y ejecutando cursos permanentes de ciberseguridad para todo el personal de la Fuerza Terrestre a través del Comando de Educación y Doctrina Militar Terrestre.	20	1

8 Relación de actores y objetivos

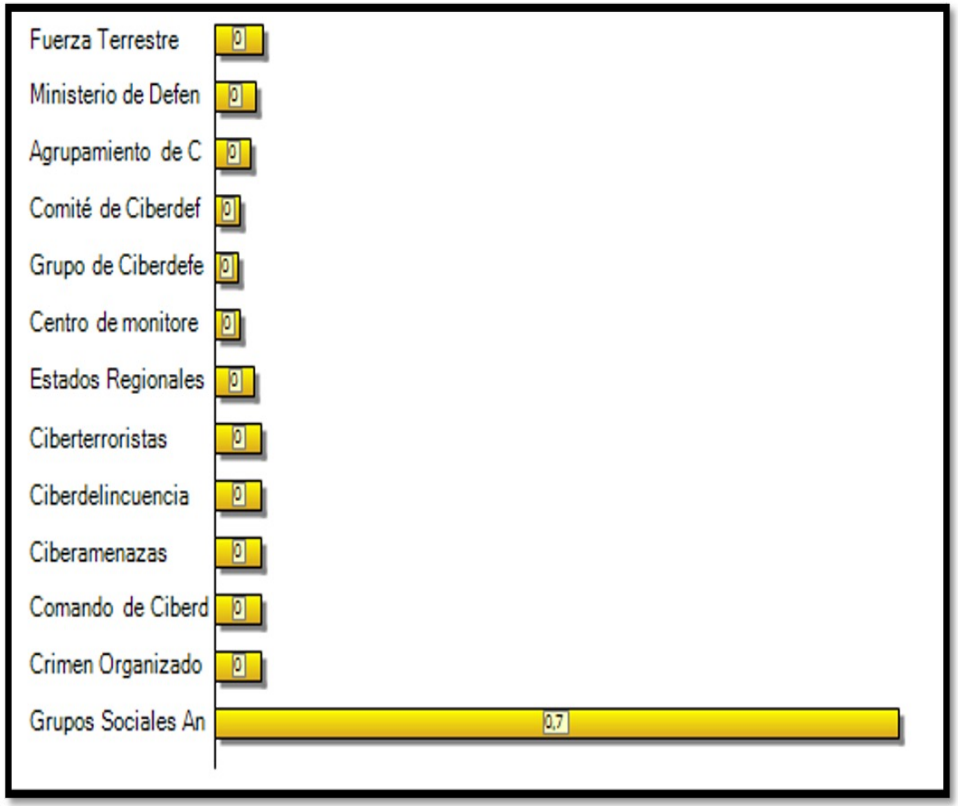
Variables estratégicas	HIPÓTESIS APUESTA "Español"	Objetivo escenario APUESTA	Actores	
			Favor	En contra
Ejecución de operaciones de ciberdefensa.	Continua	Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	Fuerza Terrestre	Estados regionales e internacionales
Presupuesto para un grupo con capacidades de ciberdefensa.	Suficiente	Optimizar el presupuesto para el suficiente desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	AGRUCOMGE	Ministerio de Economía y Finanzas
Apoyar al desarrollo de una cultura de ciberseguridad.	Continuo	Generar un continuo apoyo al desarrollo de una cultura de ciberseguridad.	Comité de Ciberdefensa	Ciberdelincuencia
Equipos y herramientas de ciberdefensa de la FT de última generación.	Alto	Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	GRUCIBER	Ciberamenazas
Marco regulatorio en el ciberespacio.	Moderado	Alcanzar un moderado con marco regulatorio en el ciberespacio.	Fuerza Terrestre	Ciberamenazas y ciberoponentes
Reducir las vulnerabilidades cibernéticas en la ITD.	Continua	Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD	Fuerza Terrestre	Ciberamenazas
Doctrina de operaciones en el ciberespacio.	Suficiente	Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	Fuerza Terrestre	Ciberamenazas

MACTOR

Poder de Actores

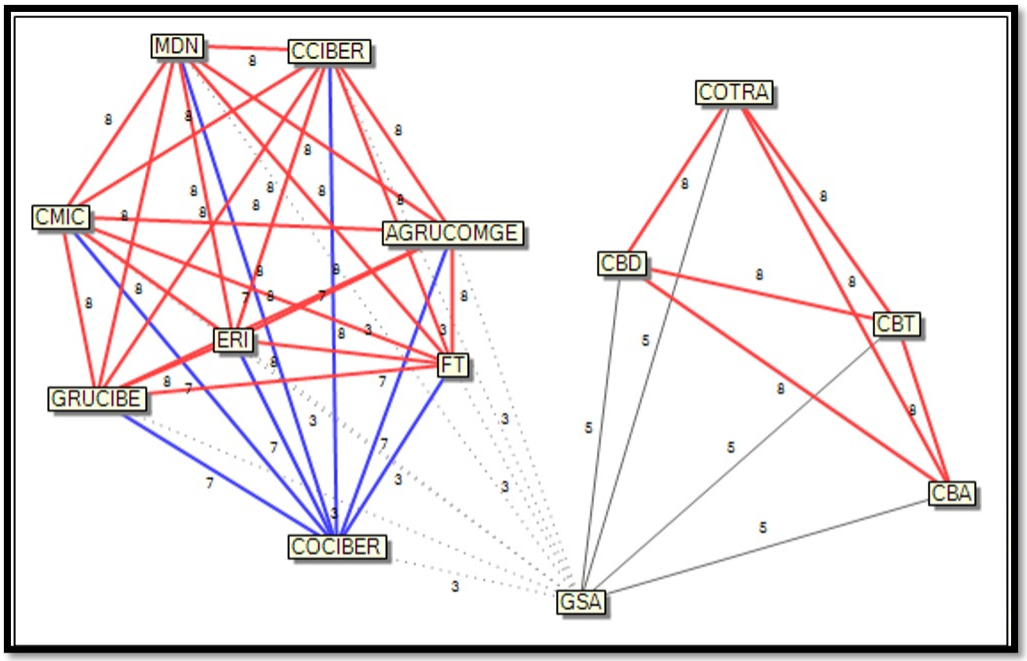


Ambivalencia de Actores

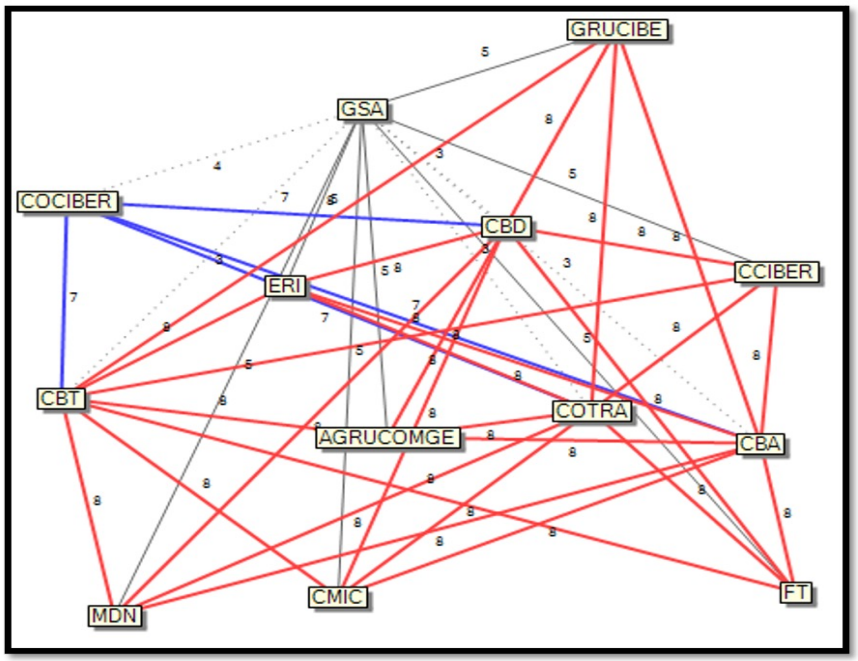


MACTOR

Convergencia de Actores



Divergencia de Actores



Análisis estratégico de actores

ANÁLISIS ESTRATÉGICO DE ACTORES

INFLUENCIA

Comando de Ciberdefensa
Fuerza Terrestre
Ministerio de Defensa Nacional
Comité de ciberseguridad
CMIC, Estados regionales e internacionales
AGRUCOMGE, Grupos antagónicos

ALIANZA

Ministerio de Defensa Nacional
con
Comité de Ciberseguridad, CMIC y COCIBER.

Fuerza Terrestre
con
AGRUCOMGE,
Grupo de Ciberdefensa de la FT y los Estados Regionales e internacionales.

CONFLICTO

MDN **Contra**
Unidad de Ciberdefensa de la FT

COCIBER
Contra
Ciberamenazas, ciberterroristas, crimen organizado y protesta social.

Grupo de ciberdefensa de la FT
Contra
Ciberamenazas, ciberterroristas, crimen organizado y protesta social.

RIESGOS

Ciberamenazas,
ciberterroristas,
crimen organizado
y grupos antagónicos

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

PROPUESTA DE PROYECTO

Misión

La Fuerza Terrestre a través del Grupo de Ciberdefensa efectuará operaciones de defensa y exploración en el ciberespacio de forma permanente en apoyo a las operaciones militares en todo el teatro de operaciones, para proteger la infraestructura tecnológica digital de la institución; operaciones de respuesta, con orden, para degradar o neutralizar la infraestructura crítica tecnológica del adversario y así contribuir con el cumplimiento de las misiones del Comando de Operaciones Terrestres.

Visión

Al 2033, la Fuerza Terrestre tendrá una elevada capacidad tecnológica, innovadora e interoperable en el ciberespacio, que le permita ejecutar acciones de defensa exploración y respuesta en el quinto dominio en apoyo a las operaciones militares, para conocer, prevenir, disuadir y responder a las ciberamenazas, en escenarios de alta incertidumbre, en el ámbito de la seguridad y defensa, proporcionando el apoyo con efectividad, cohesión institucional y trabajo en equipo, empleando personal profesional calificado, experimentado y certificado, con capacidad disuasiva, permanente y sostenible.

Principios

Cooperación. - Depende de colaboración y aporte de varios actores, es uno de los principios fundamentales de la ciberdefensa. El intercambio de información e inteligencia de ciberamenazas, permite reducir los riesgos, mejorar los controles y responder oportuna y adecuadamente a las ciberamenazas.

Disimulación. - Se adoptan medidas activas para no ser detectados por las ciberoperaciones de exploración y respuesta del oponente, realizando el enmascaramiento de las ciberoperaciones ofensivas propias

Resiliencia. - Toma de decisiones orientadas a que la ciberdefensa de la FT tenga la capacidad de resistir, adaptarse y/o recuperarse de una ciberamenaza de manera oportuna y eficiente, a través de la prevención y restauración de su estructura y funciones básicas.

Principios

Adaptabilidad. - Mediante proactividad, la defensa en el ciberespacio se adapta o se mantiene flexible a la capacidad de mutación del oponente.

Restricción. - Limita el uso innecesario de la fuerza, para evitar los daños colaterales mediante el equilibrio de la necesidad de seguridad, la conducción de las ciberoperaciones y el estado final deseado

Objetivos Estratégicos

1. Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.

2. Generar productos para el continuo apoyo al desarrollo de una cultura de ciberseguridad.

3. Alcanzar una suficiente doctrina de operaciones en el ciberespacio.

4. Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.

5. Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa.

6. Alcanzar un moderado marco regulatorio en el ciberespacio.

7. Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD.

8. Optimizar el presupuesto suficiente para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.

Variables Estratégicas

PERSPECTIVAS	Fuerza Terrestre		Ciberdefensa de la Fuerza Terrestre	
	OBJETIVOS	Ideas de innovación estratégica	Objetivo estratégico	Estrategias
Cliente / Sociedad	OBJ. 1 "Incrementar la efectividad en el control del territorio nacional".	Optimizando las operaciones militares en la defensa de la soberanía y seguridad integral.	OBJ. 1 Ejecutar operaciones de ciberdefensa de forma continua en apoyo a las operaciones militares para la defensa de la soberanía e integridad territorial.	Estableciendo un equipo de respuesta a incidentes de seguridad informática que le permita ejecutar operaciones de defensa en el ciberespacio.
		Estructurando unidades militares flexibles, móviles y multipropósito que puedan operar en diversos tipos de misiones y escenarios geográficos		Planificando ciberoperaciones de defensa y respuesta en función de resultados de ciberinteligencia.
		Proponiendo los cambios pertinentes al Marco Legal	OBJ. 2 Alcanzar un moderado marco regulatorio en el ciberespacio.	Promoviendo reformas legales, que legalicen el empleo de la Fuerza Terrestre en el ciberespacio. Proponiendo reglas de enfrentamiento y normas de comportamiento en el ciberespacio.
	OBJ. 2 "Mantener la imagen institucional".	Fortaleciendo la imagen institucional y cohesión interna con el manejo adecuado de los temas legales.	OBJ. 3 Generar productos para el continuo apoyo al desarrollo de una cultura de ciberseguridad.	Planificando y ejecutando cursos permanentes de ciberseguridad para todo el personal de la Fuerza Terrestre a través del Comando de Educación y Doctrina Militar Terrestre.

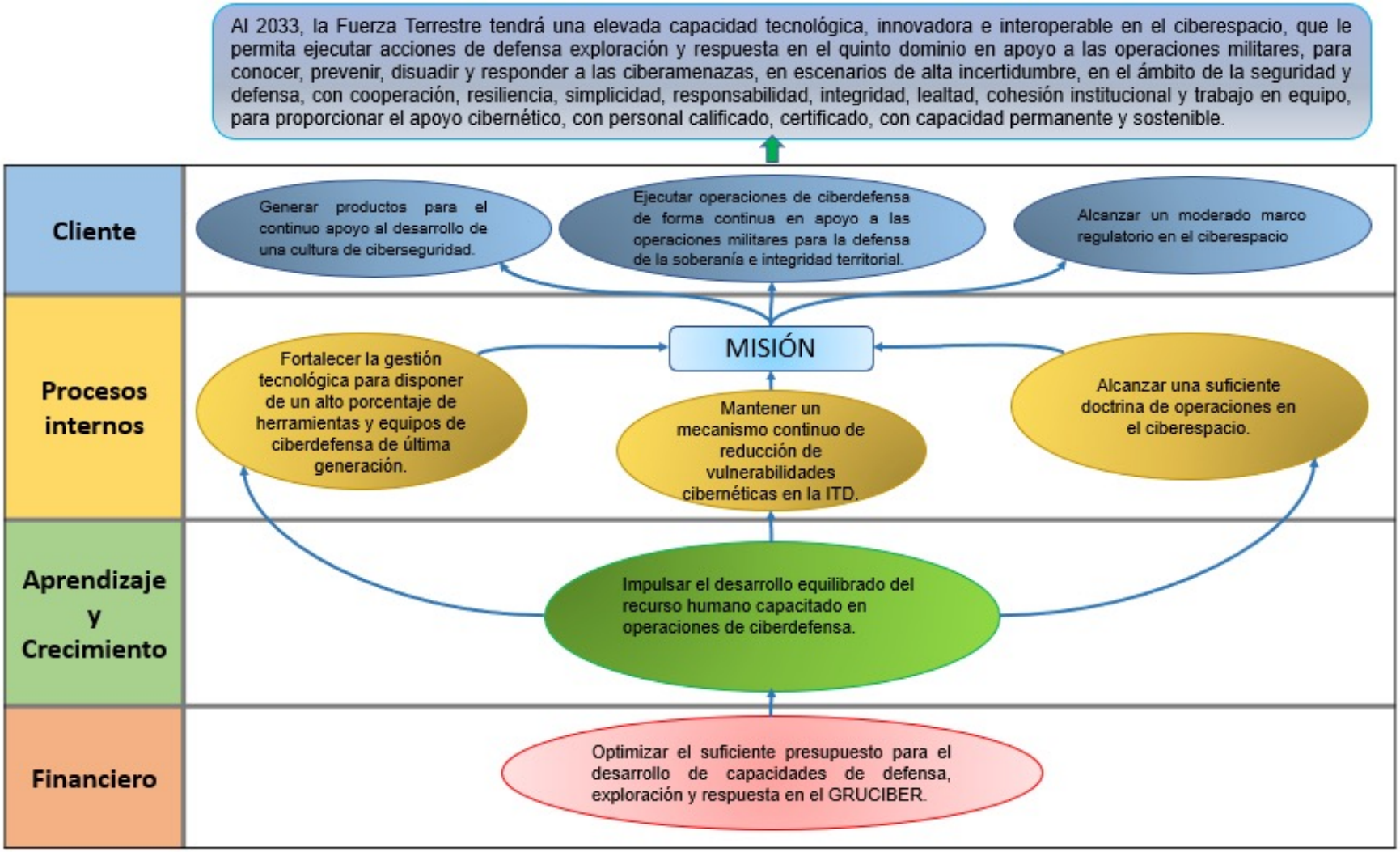
Variables Estratégicas

PERSPECTIVAS	Fuerza Terrestre		Ciberdefensa de la Fuerza Terrestre	
	OBJETIVOS	Ideas de innovación estratégica	Objetivo estratégico	Estrategias
Cliente / sociedad	OBJ. 3 "Incrementar la efectividad operacional de las unidades militares".	Optimizando la infraestructura de las unidades militares acorde a los requerimientos operacionales Desarrollando protocolos y procedimientos que definan las condiciones de empleo, tareas específicas y coordinaciones que se deben realizar para el cumplimiento de misiones y tareas de apoyo a la seguridad integral.	OBJ. 4 Mantener un mecanismo continuo de reducción de vulnerabilidades cibernéticas en la ITD.	Incrementar la capacidad de monitoreo, detección y eliminación de ciberamenazas en la ITD. Ejecutar ciberoperaciones conjuntas con el COCIBER y el CIES, para la reducción de vulnerabilidades cibernéticas en la ITD
Procesos	OBJ. 4 "Incrementar las capacidades militares".	Fortaleciendo la capacidad de "ciberdefensa"	OBJ. 5 Fortalecer la gestión tecnológica para disponer de un alto porcentaje de herramientas y equipos de ciberdefensa de última generación.	Negociando con empresas pares para la implementación de herramientas de ciberdefensa a bajos costos. Impulsando el desarrollo de conocimiento a través de los Centros de Investigación, para eliminar la dependencia extranjera.
	OBJ. 5 "Incrementar el alistamiento operacional".	Mejorar los niveles de entrenamiento, educación militar y generación de doctrina	OBJ. 6 Alcanzar una suficiente doctrina de operaciones en el ciberespacio.	Generando la doctrina básica de ciberoperaciones. Participando en ejercicios de ciberdefensa nacionales e

Variables Estratégicas

PERSPECTIVAS	Fuerza Terrestre		Ciberdefensa de la Fuerza Terrestre	
	OBJETIVOS	Ideas de innovación estratégica	Objetivo estratégico	Estrategias
Aprendizaje y Crecimiento	OBJ. 8 "Incrementar el desarrollo del talento humano".	Mejorando las competencias del personal militar y de servidores públicos en función del perfil profesional.	OBJ. 7 Impulsar el desarrollo equilibrado del recurso humano capacitado en operaciones de ciberdefensa.	Creando una subespecialidad de ciberdefensa en la Fuerza Terrestre. Adiestrando y entrenando en la planificación y ejecución de ciberoperaciones al personal de ciberdefensa.
Financiero	OBJ. 9 "Incrementar el uso eficiente del presupuesto".	Mejorar los procesos y procedimientos que permitan optimizar la planificación y ejecución presupuestaria, y el manejo administrativo de las unidades. Realizar el manejo del presupuesto y recursos institucionales bajo una política de priorización en virtud de los requerimientos operacionales y administrativos más importantes	OBJ. 8 Optimizar el suficiente presupuesto para el desarrollo de capacidades de defensa, exploración y respuesta en el GRUCIBER.	Presentando proyectos integrales para que se tramiten a través de acuerdos internacionales para el desarrollo de capacidades de ciberdefensa. Fortaleciendo acuerdos con empresas privadas dedicadas al ámbito de ciberseguridad para el apoyo técnico económico.

Mapa Estratégico



Conclusiones

- El escenario prospectivo al 2033 de la ciberdefensa de la F.T ecuatoriana forma parte de un estudio a futuro, el mismo dependerá de las acciones que generen cada uno de sus actores.

- El estudio prospectivo fue desarrollado mediante la utilización de la herramienta prospectiva francesa de Godet siguiendo cada uno de sus pasos, y complementada con el empleo del programa MACTOR, permitiendo establecer un análisis prospectivo integral de la ciberdefensa en la Fuerza Terrestre.

- En función del análisis prospectivo, se estableció como propuesta un Plan Estratégico Institucional de la ciberdefensa para la Fuerza Terrestre.

Recomendaciones

- Considerando que las ciberamenazas pueden causar alteración, destrucción o la inhabilitación de la infraestructura digital de la Fuerza Terrestre, es necesario potencializar las capacidades de defensa, explotación y respuesta de la institución a través de las acciones planteadas en el presente estudio, para lograr alcanzar el escenario apuesta al 2033.

- Mediante el módulo de seguimiento y evaluación de la Dirección de Planificación Estratégica de la Fuerza Terrestre, se verifique la implementación de las acciones recomendadas en el presente análisis prospectivo de ciberdefensa evaluando si han sido o no alcanzados los objetivos.

¡Gracias!