

ISSN 2477-9253

★★★★★ Revista de Ciencias de ★★★★★
Seguridad y Defensa

Volumen IX - Número 4



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA



Departamento de
Seguridad y Defensa



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA



Departamento de
Seguridad y Defensa

★★★★★ Revista de Ciencias de ★★★★★ Seguridad y Defensa

DEPARTAMENTO DE SEGURIDAD Y DEFENSA
UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE
SANGOLQUÍ - ECUADOR

2024

Revista de Ciencias de Seguridad y Defensa

Revista oficial del Departamento de Seguridad y Defensa - Universidad de las Fuerzas Armadas - ESPE, Sangolquí, Ecuador. 2024

Periodicidad: Trimestral (marzo-junio-septiembre-diciembre)

Volumen IX - Número 4 año 2024

Editor general / Editor-in-chief

- Prof. Ing. Walter Fuertes Díaz, Ph. D., Universidad de las Fuerzas Armadas - ESPE, Sangolquí, Ecuador, (wmfuertes@espe.edu.ec)

Comité editorial / Editorial committee

- Crnl. E.M. Byron Vega Moreno, Mgtr. Director del DSDE matriz. **Presidente**

Miembros

- Ing. Margarita Palma Samaniego, Mgtr. (UAE ESSUNA-ESMA)
- Ing. Margarita Narváez Ríos, Mgtr. (UAE ESFORSE)
- Lcda. Gloria Valencia Vivas, Ph.D. (UAE ESMENA)
- Crnl (SP) Mauro Argoti, Mgtr. (UEET)
- Cpf. César Portero Barrantes, Mgtr. (ESPE-Matriz)

Co-editores/Co-editors

- Dr. Manolo Cruz Ordóñez, Mgtr. (Área de Conocimiento Ciencias Militares)
- Lic. Edgar Arauz Sánchez, Mgtr. (Área de Conocimiento de Seguridad y Defensa)
- Ing. Melany Yarad Jácome, Mgtr. (Área de Conocimiento de Ciberdefensa)
- Lcda. María Fernanda Serrano Aldaz, Mgtr. (Área de Conocimiento de Geopolítica y Relaciones Internacionales)

Comité revisor / Review committee

- Dr. Tomás Fontaines-Ruiz, Ph.D., Universidad Técnica de Machala, Machala, Ecuador (tfontaines@utmachala.edu.ec)
- Dr. Ender Enrique Carassquero Carrasquero, Instituto Internacional de Estudios Avanzados en Banca Central y Finanzas- IBEA (ender.carrasquero@ibeabc.com)
- Dra. Maritza Gisela Paula Chica. Universidad Estatal Península de Santa Elena, UPSE, Salinas, Ecuador (kchung@upse.edu.ec)
- Ing. Luis Patricio Tello-Oquendo, Ph.D., Universidad Nacional del Chimborazo.
- Dr. Lester Martín Andrés Cabrera Toledo: (lmcabrera2@espe.edu.ec)
- Crnl. Gonzalo Javier Pullas Tapia, Ph.D., Universidad de las Fuerzas Armadas ESPE. Email: gjpullas@espe.edu.ec
- Luis Olvera Vera, Mag. Universidad de Guayaquil (luis.olverav@ug.edu.ec)
- Mayo. César Julio Quinga, Ph.D. (cjquinga@espe.edu.ec)
- Ing. Karina Lorena Cela Rosero, Ph.D., Universidad de las Fuerzas Armadas ESPE
- Ing. Ramiro Nanac Delgado, Rodríguez, Ph.D., (rmdelgado@espe.edu.ec)
- Crnl. de E.M.C. (SP) Hugo Danilo Ruiz Villacrés, Ph.D. (hduiz@espe.edu.ec)
- Ing. Carina Alexandra Haro, Mgtr. (caharo@espe.edu.ec)
- Cpnv. (SP) Hugo Leopoldo Pérez Vaca
- Dr. Kléver Antonio Bravo Calle, Ph.D., (kabravo@espe.edu.ec)
- Ing. Gustavo David Salazar Chacón, Ph.D., (gdsalazar@espe.edu.ec)
- Ing. Patricio Xavier Zambrano Rodríguez, Ph.D. Escuela Politécnica Nacional (patricio.zambrano@epn.edu.ec)
- Crnl. de E.M.C. (SP) Iván Patricio Medina Jiménez, Mgtr. (ipmedinal@espe.edu.ec)
- Ing. Roberto Andrade, Ph.D., Escuela Politécnica Nacional, (roberto.andrade@espmedu.ec)
- Ing. Rodolfo Jaime Salazar Martínez, Ph.D., (rjsalazar@espe.edu.ec)
- MSc. Roberto Carlos Narváez Aguilar, Fuerza Aérea Ecuatoriana, (rmarvaez@fae.mil.ec)
- Ing. Mario Raúl Pazmiño Silva, Centro de Análisis e Investigación Internacional (mrps1959@gmail.com)
- Dr. Diego Eduardo Benavides Astudillo, (debenavides@espe.edu.ec)
- Ing. Alberto Daniel Núñez Agurto (adnunez1@espe.edu.ec)
- Dr. Germán Eduardo Rodríguez Galán (gerodriguez10@espe.edu.ec)
- Dr. Wilbert Geovanny Aguilar Castillo, (wgaguilar@espe.edu.ec)
- Dra. Alicia Mariferanda Zabala Calahorrano (amzavala@espe.edu.ec)
- Mgtr. Ing. Luis Enrique Jaramillo Montaña (lejaramillo5@espe.edu.ec)

Editor Técnico / Technical Editor

- Ing. Marcelo Santiago Salvador M., Mag., Universidad de las Fuerzas Armadas - ESPE, Sangolquí, Ecuador (mssalvador@espe.edu.ec)

Corrección idiomática y diagramación

- Mtr. Xavier Chinga. Corrector de Estilo. Unidad de Gestión de la Investigación (pxchinga@espe.edu.ec)

Revisión en idioma inglés

- Mgtr. Patricio Javier Serrano Escobar, traductor e intérprete profesional certificado en USA y en Ecuador. Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador, (pjserrano@espe.edu.ec).

Diseño de portada y contraportada

- B.A. David Cabrera R.

Edición gráfica, diseño y diagramación

- ESPE

Preguntas y correspondencia

- Prof. Ing. Walter Fuertes Díaz, Ph. D., Universidad de las Fuerzas Armadas - ESPE, Sangolquí, Ecuador, (wmfuertes@espe.edu.ec)
- Ing. Marcelo Santiago Salvador M., Mag., Universidad de las Fuerzas Armadas - ESPE, Sangolquí, Ecuador (mssalvador@espe.edu.ec)

La revista de Ciencias de Seguridad y Defensa es un órgano de difusión científica trimestral del Departamento de Seguridad y Defensa de la Universidad de las Fuerzas Armadas - ESPE, cuyos contenidos giran en torno a temas como: seguridad, defensa, gestión de riesgo, patrimonio natural y cultural, prevención, mitigación, resiliencia, historia militar, sociología militar, geopolítica, educación militar, estrategia, paz y desarrollo.

Cómo citar (ejemplo):

Cruz, 2017: Amenazas naturales recurrentes, concurrentes y concatenadas en la ciudad de Esmeraldas. Revista de Ciencias de Seguridad y Defensa, Vol. III, No. 1: 25-92

Revista de Ciencias de Seguridad y Defensa

2024

ISSN 2477-9253

Los contenidos de los artículos, aquí publicados, son de responsabilidad de los autores.

Visítanos: <https://journal.espe.edu.ec/ojs/index.php/revista-seguridad-defensa>

Lugar de edición: Universidad de las Fuerzas Armadas - ESPE Sangolquí, Ecuador



Revista de Ciencias de Seguridad y Defensa

Volumen 9, Número 4
ISSN Impreso: 2477-9253

**La administración de la Revista de Ciencias de Seguridad y Defensa
se realiza a través de los siguientes parámetros:**



La revista utiliza el sistema antiplagio académico (como parte de la adopción de Códigos de Ética). Se recomendó a los autores reconocer a los ayudantes de investigación, en caso de existir.

Servicios de Información a los que pertenece esta revista:



Los artículos cuentan con el código de identificación (Digital Object Identifier).



El proceso editorial se gestiona a través del Open Journal System de la Universidad de las Fuerzas Armadas ESPE y su Vicerrectorado de Investigación.



Es una publicación de acceso abierto (Open Access) con Licencia Creative Commons.

**Las políticas copyright y uso postprint, se encuentran publicadas con los
artículos de la presente edición y se pueden consultar en:**

<https://journal.espe.edu.ec/ojs/index.php/revista-seguridad-defensa>

Entidad editora e impresión:



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

★★★★★ Revista de Ciencias de ★★★★★★
Seguridad y Defensa

Volumen IX - Número 4, 2024

SUMARIO

IA Autónoma en la Guerra Cognitiva: Nuevas Fronteras del Conflicto Silencioso

Juan de Dios Meseguer González.....11

La lucha contra el Terrorismo enmarcada en el cumplimiento de los Derechos Humanos y el Derecho Internacional Humanitario

Rodrigo Fernando Andrade Racines.....31

Microrredes de Generación de Potencia Eléctrica para la Autosuficiencia de las Unidades Remotas de las Fuerzas Armadas

Galo Guarderas Burbano.....49

Mochila de Operaciones Tácticas S&M (M.O.T. S&M) a implementarse en el Ejército Ecuatoriano

Juan Sebastián Sánchez Obando, Gonzalo Viterbo Martínez Abarca, Gilbert Jaime Llerena Martínez.....59

Simulación de Ciberataques a Servicios Web en Entornos Controlados: Un Enfoque Seguro para la Evaluación de Vulnerabilidades

Andrés Sebastián Almeida, Alison Paola Moncayo, Darwin Roberto Valdiviezo.....67

Prólogo

La revista en Seguridad y Defensa de la Universidad de las Fuerzas Armadas ESPE presenta sus publicaciones de acceso abierto de forma trimestral. La revista cuenta con revisores pares ciegos, con un enfoque en el ámbito académico científico, la cual es abierta a la discusión de trabajos teóricos e investigaciones sobre políticas, enfoques, modelos y perspectivas de seguridad y defensa desde las diferentes disciplinas.

A través de sus páginas, la revista tiene el honor de presentar un espacio de reflexión, análisis, investigación y difusión de conocimientos que contribuyan al fortalecimiento de la seguridad, defensa y sociedad. En este contexto, la academia asume el rol fundamental en la generación del conocimiento crítico y en la formación de personas líderes preparadas para afrontar retos. Desde este punto de vista la revista busca consolidarse como el referente en la divulgación de trabajos innovadores y estudios de caso que aporten a la comunidad académica como a las profesiones del sector de seguridad y defensa.

En cada edición, se difunden aportes de investigadores, docentes y estudiantes expertos en temas como: seguridad, defensa, historia militar, sociología militar, geopolítica, educación militar, estrategia, ciberdefensa, ciberseguridad, paz y desarrollo. Este esfuerzo editorial se ve reflejado en el compromiso del comité editorial de la Universidad con la excelencia académica y que a través del conocimiento se pueda servir a la patria, contribuyendo al fortalecimiento de capacidades nacionales y regionales frente a distintas amenazas contemporáneas.

Agradecemos a los autores, revisores pares ciegos, correctores idiomáticos, diagramador, maquetador y al Comité Editorial por la dedicación y el esfuerzo puesto como equipo de trabajo para concretar la Edición N°4. Hacemos propicia la ocasión para invitar a los lectores a introducirse en el estudio de cada uno de los artículos publicados en esta edición, con una mirada constructiva y crítica, y a considerar esta revista no solo como fuente de información, sino también como un instrumento de desarrollo en el ámbito de seguridad y defensa.

Crnl. E.M. Byron Vega Moreno, Mgtr.

Director del Departamento de Seguridad y Defensa

Universidad de las Fuerzas Armadas - ESPE



Revista de Ciencias de Seguridad y Defensa

★★★★★ Revista de Ciencias de ★★★★★
Seguridad y Defensa

Presentación

El Comité Editorial de la revista Ciencias de Seguridad y Defensa de la Universidad de las Fuerzas Armadas - ESPE se complace en presentar el volumen 9, Tomo N° 4, correspondiente al año 2024. Esta edición fue creada con el objetivo de ser un referente y crear un espacio para el intercambio de conocimiento a través de la difusión de trabajos enmarcados en el ámbito de seguridad, defensa y sociedad. En esta edición, se han recopilado cinco artículos de gran relevancia que abordan problemáticas actuales y que proponen soluciones innovadoras para enfrentar las sociedades modernas en materia de seguridad integral.

El primer artículo examina el papel emergente de los sistemas de Inteligencia Artificial (IA) autónomos en la guerra cognitiva, entendida como el conjunto de operaciones orientadas a influir en los procesos mentales de individuos y colectivos. El objetivo principal es analizar cómo estas tecnologías amplían el dominio de la confrontación más allá de los espacios físicos y digitales, incidiendo directamente en la percepción, el juicio y la toma de decisiones humanas. Los resultados muestran que la IA autónoma amplifica la efectividad de las campañas de manipulación informativa, permite una personalización masiva del mensaje y optimiza de forma adaptativa las tácticas de influencia. El hallazgo más innovador es la capacidad de estas tecnologías para operar de forma independiente en entornos cognitivos sin supervisión humana directa, lo que redefine las reglas tradicionales del poder en el entorno de seguridad internacional.

El segundo artículo se enfoca en la lucha contra el terrorismo enmarcada en el cumplimiento de los derechos humanos y el derecho internacional humanitario. A través de un breve estudio de las normativas nacionales e internacionales, así como de las experiencias vecinales y hemisféricas, busca enfocar de manera pragmática las dificultades, retos y aprendizajes que dejan otros Estados, así como resaltar el accionar histórico de las Fuerzas Armadas ecuatorianas. Este estudio es un aporte a la constante educación militar consciente de la importancia del respeto a los Derechos Humanos durante la lucha contra el terrorismo.

Así mismo, desde un enfoque tecnológico, el tercer artículo propone la aplicación de múltiples técnicas de generación de energía eléctrica, para la implementación de un sistema combinado de fuentes de energía renovable (FER), con características como escalabilidad, eficiencia, sostenibilidad, resiliencia y amigabilidad con el medio ambiente, instaladas en unidades de frontera o unidades cuya localización dificulte la conexión con el sistema eléctrico nacional. Este concepto, conocido como microrredes de generación de potencia eléctrica de corriente alterna, es un sistema que permite aprovechar todos los medios existentes de generación eléctrica. En esta propuesta se consideran únicamente recursos renovables como sol, viento, agua, biomasa, etc., para generar y posteriormente controlar la distribución de la energía de manera óptima y eficiente. Desde el punto de vista militar, estas microrredes permiten optimizar el cumplimiento de las misiones asignadas, en especial en unidades de frontera o instalaciones militares con déficit de potencia eléctrica.

En el cuarto artículo, su autor se centró en el estudio de la mochila de operaciones tácticas S&M (M.O.T. S&M), a implementarse en el Ejército Ecuatoriano. En este estudio se identificaron problemas que afectan al personal militar y se plantearon soluciones a través del diseño de la Mochila de Operaciones Tácticas S&M. Esta mochila se enfoca en proporcionar una herramienta versátil y segura, utilizando materiales, accesorios y tecnología que faciliten su uso, con el objetivo de minimizar los riesgos en operaciones especiales, operaciones aerotransportadas, cruce de ríos organizados y operaciones fluviales. Las mochilas tácticas ofrecen



ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA



mayor seguridad, comodidad y ergonomía en comparación con las mochilas tradicionales o de dotación vigente.

Finalmente, en el quinto artículo se presenta la simulación de ciberataques a servicios web en entornos controlados, empleando un escenario seguro para la evaluación de vulnerabilidades. Este estudio evalúa una aplicación web con vulnerabilidades ante diferentes ataques comunes, con la finalidad de evidenciar fallas en la seguridad del sistema y proponer soluciones para prevenirlas. Para lograrlo, se utilizó OWASP (Open Web Application Security Project) Juice Shop, una aplicación desarrollada por el proyecto OWASP, una comunidad internacional que promueve prácticas para mejorar la seguridad del software. Juice Shop permite realizar pruebas en un entorno diseñado para simular fallas comunes.

Expresamos nuestra profunda gratitud a todos los investigadores y profesionales que han contribuido con sus trabajos, que fueron revisados en forma rigurosa, para hacer posible esta publicación. Esperamos que esta edición sea un recurso valioso para profesionales investigadores, estudiantes, personal de Fuerzas Armadas y público en general, para promover reflexiones críticas y novedosas propuestas dedicadas a fortalecer los diversos ámbitos que hemos abordado.

Agradecemos a la Universidad de las Fuerzas Armadas - ESPE por su continuo apoyo en nuestra misión compartida de construir un futuro más seguro y resiliente, lo que reafirma su compromiso con la excelencia académica y la generación de un impacto positivo y medible en la sociedad.

Comité editorial

IA Autónoma en la Guerra Cognitiva: Nuevas Fronteras del Conflicto Silencioso

Autonomous AI in Cognitive Warfare: New Frontiers of Silent Conflict

Juan de Dios Meseguer González

IUGM-UNED, 46004, Valencia, España.

jmeseguer1@alumno.uned.es - <https://orcid.org/0009-0004-3691-4880>

Resumen

El artículo examina el papel emergente de los sistemas de Inteligencia Artificial (IA) autónomos en la guerra cognitiva, entendida como el conjunto de operaciones orientadas a influir en los procesos mentales de individuos y colectivos. Estos sistemas no solo ejecutan tareas automatizadas, sino que también se adaptan a contextos dinámicos para maximizar su impacto psicológico. El objetivo principal es analizar cómo estas tecnologías amplían el dominio de la confrontación más allá de los espacios físicos y digitales, incidiendo directamente en la percepción, el juicio y la toma de decisiones humanas. La metodología empleada es cualitativa, basada en el análisis documental, el estudio de casos recientes y la elaboración de escenarios prospectivos. Los resultados muestran que la IA autónoma amplifica la efectividad de las campañas de manipulación informativa, permite una personalización masiva del mensaje y optimiza de forma adaptativa las tácticas de influencia. El artículo concluye que esta nueva frontera del conflicto silencioso plantea desafíos estratégicos, éticos y jurídicos para los Estados que aún carecen de marcos normativos adecuados para afrontarlos. El hallazgo más innovador es la capacidad de estas tecnologías para operar de forma independiente en entornos cognitivos sin supervisión humana directa, lo que redefine las reglas tradicionales del poder en el entorno de seguridad internacional.

Palabras clave: *IA, guerra cognitiva, autonomía, percepción, conflicto silencioso.*

Abstract

The article examines the emerging role of autonomous artificial intelligence systems in cognitive warfare, understood as a set of operations aimed at influencing the mental processes of individuals and groups. These systems not only perform automated tasks but also adapt to dynamic contexts to maximize their psychological impact. The primary objective is to examine how these technologies extend the domain of confrontation beyond physical and digital spaces, thereby directly influencing human perception, judgment, and decision-making. The methodology used is qualitative, based on document analysis, recent case studies, and the development of prospective scenarios. The results show that autonomous artificial intelligence enhances the effectiveness of information manipulation campaigns, enables massive message personalization, and optimizes influence tactics adaptively. The article concludes that this new frontier of silent conflict poses strategic, ethical, and legal challenges for States, which still lack adequate regulatory frameworks to address it. The most innovative finding is the ability of these technologies to operate independently in cognitive environments without direct human supervision, thereby redefining the traditional rules of power in the international security landscape.

Keywords: *Artificial Intelligence, cognitive warfare, autonomy, perception, silent conflict.*



Fecha de Recepción: 15/12/2024 - Aceptado: 20/12/2024 – Publicado: 31/12/2024
ISSN: 2477-9253 – DOI: <http://dx.doi.org/10.24133/RCS.D.VOL09.N04.2024.01>

I. Introducción

En las últimas décadas, el campo de la IA evoluciona desde sistemas pasivos orientados a la automatización de tareas específicas hasta agentes autónomos con capacidad de aprendizaje y adaptación en entornos complejos. Esta transformación tecnológica genera importantes implicaciones en el ámbito de la defensa, particularmente en el emergente concepto de guerra cognitiva, entendida como el uso de técnicas para influir en los procesos mentales de individuos y sociedades con fines estratégicos. En este nuevo escenario, el combate no solo se libra en terrenos físicos o cibernéticos, sino también en el espacio mental, donde se disputan percepciones, emociones, ideas y decisiones.

Diversos estudios (Gizewski & Rostek, 2021; Rigaki & Garcia, 2020) abordan el uso de algoritmos para manipular la información y direccionar el comportamiento humano. Sin embargo, la participación de sistemas de IA autónomos en este tipo de conflicto representa aún una frontera poco explorada y escasamente regulada.

El propósito de este estudio consiste en analizar cómo los sistemas autónomos de IA transforman la naturaleza de la guerra cognitiva, ampliando las capacidades de influencia estratégica sin necesidad de intervención humana directa. Para ello, la investigación adopta un enfoque cualitativo centrado en el análisis documental, el estudio de casos contemporáneos y la construcción de escenarios prospectivos. El resultado principal consiste en un marco conceptual que articula la relación entre autonomía tecnológica, operaciones psicológicas y manipulación cognitiva, sustentado en evidencia empírica y un análisis interdisciplinario. La investigación aplica el método analítico-descriptivo, herramientas de análisis crítico y técnicas de contraste entre casos reales y literatura académica especializada.

Entre los principales hallazgos, se identifica que la IA autónoma permite una personalización masiva de mensajes, una adaptación en tiempo real de tácticas persuasivas y una creciente capacidad para operar sin supervisión humana en entornos cognitivos. Esta capacidad redefine el papel de los actores tradicionales del conflicto y altera el equilibrio de poder en los escenarios de seguridad internacional. En ausencia de marcos éticos y jurídicos adecuados, la autonomía tecnológica en el plano cognitivo representa un riesgo emergente para la soberanía informativa de los Estados. La principal contribución del estudio radica en visibilizar esta problemática desde una perspectiva multidisciplinar, anticipando los desafíos que plantea esta nueva frontera del conflicto silencioso.

El artículo se estructura en cinco secciones. En primer lugar, presenta el marco teórico y conceptual sobre guerra cognitiva e IA autónoma. En segundo lugar, analiza el estado del arte y las respuestas institucionales existentes. La tercera sección expone los casos de estudio seleccionados y el método aplicado. En la cuarta sección se presentan los resultados y se discuten sus implicaciones estratégicas. Finalmente, se ofrecen las conclusiones generales y se proponen líneas futuras de investigación y regulación.

II. Estado del Arte

2.1. Enfoque metodológico de la investigación

El presente estudio adopta un enfoque cualitativo con alcance exploratorio y descriptivo, adecuado para abordar fenómenos emergentes como la participación de sistemas de IA autónoma en contextos de guerra cognitiva. Dado que se trata de un campo aún en consolidación, se descartan los enfoques cuantitativos o

experimentales en favor de una metodología que permite examinar en profundidad documentos, casos y marcos conceptuales complejos, siguiendo las recomendaciones para el diseño de investigaciones sociales propuestas por Salkind (2017).

La recolección de información se realiza mediante análisis documental de fuentes académicas, doctrinales, técnicas y oficiales, seleccionadas con base en criterios de actualidad, relevancia y credibilidad. Se consultan artículos científicos indexados, informes de defensa de la OTAN y de otros organismos multilaterales, documentos técnicos de empresas tecnológicas, así como publicaciones especializadas en seguridad y defensa. Se consideran publicaciones comprendidas entre los años 2015 y 2024, priorizando aquellas que abordan la intersección entre autonomía tecnológica y operaciones psicológicas o cognitivas.

Asimismo, se emplea el método de estudio de casos para examinar de forma detallada tres eventos concretos en los que se documenta o sospecha el uso de IA en campañas de manipulación cognitiva:

- Las operaciones de influencia automatizadas en redes sociales durante procesos electorales en Europa del Este.
- El empleo de bots cognitivos en el conflicto del Nagorno-Karabaj (2020).
- Las simulaciones doctrinales de la Fuerza Aérea de los EE.UU. sobre el uso de agentes autónomos para operaciones psicológicas.

La selección de estos casos responde a su diversidad geográfica, tipología operativa y disponibilidad de fuentes verificables.

El análisis se estructura en tres fases. En primer lugar, se desarrolla una matriz categorial para clasificar las tecnologías según su nivel de autonomía, tipo de tarea cognitiva y grado de intervención humana. En segundo lugar, se comparan los resultados obtenidos de los casos con el marco teórico existente. Finalmente, se construyen escenarios prospectivos para evaluar riesgos futuros y vacíos normativos.

La validación se lleva a cabo mediante un proceso de triangulación de fuentes y revisión cruzada de los casos seleccionados con expertos en guerra informativa y ética de la IA. Este procedimiento fortalece la consistencia argumental del estudio y aporta una perspectiva interdisciplinaria, ya que implica la comparación sistemática de información obtenida de fuentes académicas, informes institucionales y medios de comunicación reconocidos. Se analizan convergencias y divergencias entre los datos, y aquellos casos que presentan inconsistencias son revisados por expertos externos en IA y guerra cognitiva, siguiendo el enfoque de triangulación metodológica y de datos.

2.2. Fases del diseño metodológico

El diseño metodológico permite abordar de manera sistemática la investigación sobre la IA autónoma en la guerra cognitiva. A continuación, se describen las principales etapas (véase Tabla 1).

2.2.1. Determinación de instrumentos de medición

Se adopta un enfoque cualitativo, utilizando fuentes documentales como informes de investigaciones previas, artículos académicos y estudios de casos sobre el uso de IA en contextos bélicos. Los instrumentos clave incluyen la observación de fenómenos descritos en la literatura y el análisis de contenidos relevantes.

2.2.2. Selección de la muestra y población

La población estudiada incluye informes de instituciones gubernamentales, documentos de estrategias militares y trabajos previos de expertos en IA y seguridad. La muestra se define con base en la relevancia de los casos y estudios que abordan la guerra cognitiva y el uso de IA autónoma.

2.2.3. Recolección de datos

La recolección de datos se realiza a través del análisis documental, recurriendo a bibliografía especializada, bases de datos académicas y documentos militares. Esta recopilación se orienta a extraer información sobre aplicaciones actuales, riesgos asociados y respuestas institucionales.

2.2.4. Pruebas de concepto y validación

Se lleva a cabo un análisis exhaustivo de los casos de estudio seleccionados con el objetivo de validar las teorías y supuestos planteados en el marco teórico. Esta validación implica contrastar los hallazgos empíricos con las teorías existentes sobre guerra cognitiva e IA autónoma.

2.2.5. Evaluación y ajustes

A lo largo del proceso, se introducen ajustes en la metodología y en la selección de fuentes de datos conforme se obtienen resultados, con el fin de profundizar en las áreas menos exploradas o que presentan vacíos significativos en la literatura.

Tabla 1: Descripción de la metodología utilizada en la investigación

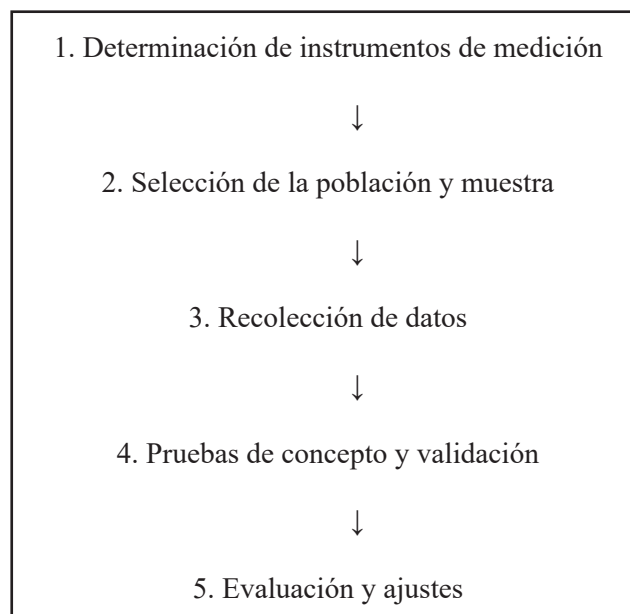
Etapas	Descripción
1. Determinación de instrumentos de medición	Se empleó un enfoque cualitativo basado en el análisis documental y el estudio de casos. Instrumentos utilizados: - Informes técnicos y estratégicos (OTAN, ONU, think tanks) - Artículos académicos indexados (Scopus, WoS, DOAJ) - Documentos técnicos de empresas del sector tecnológico-militar - Análisis de contenido sobre capacidades cognitivas y psicológicas de sistemas autónomos
2. Selección de la población y muestra	Población: Literatura y documentación relevante sobre IA autónoma y guerra cognitiva en el ámbito militar. Ejemplos: - Informe OTAN 2022 sobre guerra cognitiva - Documento de PwC & OdiseIA (2024) - Estudio del IEEE (2025) sobre IA militar Muestra: Casos emblemáticos seleccionados por su relevancia: - Drones STM Kargu en Libia (2020, informe ONU) - IA Habsora de las FDI en Gaza (2023-2024) - Campañas usando novedosas técnicas de desinformación en la guerra de Ucrania (2023-2024, BBC & Clemson University) - Enjambres cognitivos israelíes (2021) - Proyecto GhostPlay de Rheinmetall AG, & Helsing GmbH. (2022, 15 septiembre).
3. Recolección de datos	Se utilizó recolección documental sistemática: - Fuentes: bibliografía académica, bases de datos científicas, documentos militares y técnicos. - Objetivo: identificar aplicaciones reales, riesgos estratégicos y respuestas estatales ante la IA autónoma en entornos cognitivos.
4. Pruebas de concepto y validación	Análisis profundo de los casos seleccionados, contrastando: - Supuestos teóricos sobre guerra cognitiva - Capacidades técnicas de IA autónoma - Resultados empíricos observables en conflictos recientes

5. Evaluación y ajustes	Durante el análisis se aplicó un enfoque iterativo: - Ajustes metodológicos y ampliación de fuentes - Profundización en vacíos temáticos como la autonomía adaptativa, los sesgos algorítmicos y el vacío normativo - Revisión crítica de literatura emergente entre 2023 y 2024
-------------------------	---

Nota. Elaborada a partir de a partir de OTAN (2022), ONU (2020), PwC & OdiseIA (2024), IEEE (2025), BBC & Clemson University (2024), y Rheinmetall & Helsing (2024).

Para facilitar la comprensión del proceso metodológico seguido en esta investigación, la Tabla I sintetiza las principales etapas y procedimientos aplicados, desde la determinación de instrumentos hasta la evaluación y ajustes. A continuación, la Figura 1 presenta este mismo proceso de manera visual, mediante un diagrama de flujo que ilustra la secuencia lógica y las interrelaciones entre las distintas fases metodológicas. De este modo, ambos recursos permiten al lector identificar de forma clara y estructurada las decisiones y pasos clave que sustentan el análisis realizado.

Figura 1. Diagrama de flujo del proceso metodológico seguido en la investigación, desde la definición del problema hasta la validación de resultados.



Descripción de cada etapa:

1. Determinación de instrumentos de medición: Enfoque cualitativo, análisis documental y estudio de casos; uso de informes técnicos, artículos académicos y análisis de contenido.
2. Selección de la población y muestra: Selección de literatura relevante y casos emblemáticos sobre IA autónoma y guerra cognitiva.
3. Recolección de datos: Recopilación sistemática de bibliografía, bases de datos y documentos técnicos/militares.

4. Pruebas de concepto y validación: Análisis profundo de los casos, contraste entre teoría y hallazgos empíricos, revisión por expertos.
5. Evaluación y ajustes: Ajustes iterativos en la metodología y fuentes, revisión crítica de literatura emergente.

III. Marco Teórico y conceptual

3.1. Guerra cognitiva: definición y contexto

La guerra cognitiva es una forma avanzada de conflicto que busca influir en las percepciones, emociones y decisiones de individuos y sociedades, utilizando información y tecnología para alterar la cognición humana. Se considera una extensión de la guerra de la información y se distingue por su enfoque en el dominio mental de los objetivos. Esta modalidad de guerra emplea herramientas como la propaganda, la desinformación y las operaciones psicológicas para modificar actitudes y comportamientos. Según Paul Ottewell, se trata de “maniobras en el ámbito cognitivo para establecer una percepción predeterminada entre una audiencia objetivo con el fin de obtener una ventaja sobre otra parte” (Muse, 2022).

La guerra cognitiva se ha intensificado con el uso de tecnologías digitales y redes sociales, permitiendo campañas de desinformación más efectivas y difíciles de detectar. Ejemplos recientes incluyen la interferencia rusa en las elecciones estadounidenses de 2016 y las operaciones de desinformación en Polonia, donde se han promovido teorías conspirativas para socavar la confianza en las instituciones democráticas.

Un informe reciente del Servicio de Contrainteligencia Militar de Polonia (2025) documenta cómo Rusia ha intensificado la guerra cognitiva contra Polonia, utilizando campañas de desinformación científica y teorías conspirativas para debilitar la confianza social y las instituciones democráticas, especialmente en contextos electorales. Estas operaciones, ampliamente difundidas en medios y redes sociales, ejemplifican el alcance y la sofisticación de las estrategias híbridas en la región (Servicio de Contrainteligencia Militar de Polonia, 2025).

3.2. IA autónoma: principios y aplicaciones

La IA autónoma (IAA) se refiere a sistemas capaces de tomar decisiones y ejecutar acciones sin intervención humana directa. Estos sistemas utilizan algoritmos avanzados y aprendizaje automático para adaptarse a entornos dinámicos y complejos. Las aplicaciones de la IAA abarcan desde vehículos autónomos hasta sistemas de defensa y asistentes virtuales.

Se advierte sobre los riesgos de delegar decisiones importantes a agentes de IA autónomos, señalando que podrían erosionar aspectos esenciales de la experiencia humana, como el aprendizaje y la cooperación social (Acemoglu, 2024). Además, la adopción de agentes autónomos puede aumentar las desigualdades económicas y fomentar comportamientos intransigentes en negociaciones, ya que las IAs no tienen emociones ni incentivos para ceder.

En el ámbito militar, Alemania ha incorporado “drones kamikaze” o municiones merodeadoras a sus Fuerzas Armadas, en respuesta a la creciente amenaza rusa. Estos drones, como el modelo HX-2, son ligeros y autónomos, con capacidad para operar en enjambres y lanzar ataques precisos incluso sin conexión GPS. Aunque estos sistemas integran IA, la decisión final de disparo sigue siendo humana.

Figura 2. Dron HX-2 alemán durante una demostración táctica. Desarrollado por Rheinmetall, integra sensores de largo alcance y navegación autónoma, ideal para misiones ISR en entornos complejos.



Nota. Obtenida de HuffPost. Disponible en: <https://acortar.link/zSkgCc>

3.3. Intersección entre IA autónoma y guerra cognitiva

La convergencia de la IA y la guerra cognitiva representa una nueva frontera en los conflictos modernos, donde los sistemas autónomos pueden ser utilizados para manipular la información y las percepciones de las poblaciones objetivo. La capacidad de la IA para analizar grandes volúmenes de datos y generar contenido personalizado permite campañas de desinformación más sofisticadas y efectivas.

Los modelos de lenguaje a gran escala pueden ser utilizados para crear narrativas convincentes que influyan en la opinión pública. Además, el análisis de big data permite predecir patrones de conducta y segmentar audiencias para maximizar el impacto de las campañas de influencia.

La integración de la IAA en la guerra cognitiva plantea desafíos éticos y estratégicos significativos, incluyendo la necesidad de desarrollar marcos regulatorios y defensas contra la manipulación automatizada de la información. La colaboración entre expertos en tecnología, ética y seguridad es esencial para abordar estos desafíos y proteger la integridad de las sociedades democráticas.

IV. Estado del Arte y Respuestas Institucionales Existentes

4.1. Revisión de la literatura sobre IA en contextos bélicos

La literatura reciente destaca la creciente integración de la IA (IA) en operaciones militares, especialmente en sistemas autónomos y semiautónomos. Ejemplos notables incluyen el uso de drones STM Kargu en Libia en 2020 (Pérez, 2021), capaces de operar sin intervención humana directa, y el Proyecto Maven del Departamento de Defensa de EE.UU., que aplica aprendizaje automático para identificar objetivos en zonas de conflicto.

Además, se han documentado campañas de desinformación utilizando IA, como las que emplean modelos de lenguaje para generar contenido falso en conflictos recientes, evidenciando el uso de la IA en la guerra cognitiva.

4.2. Respuestas militares e institucionales ante la guerra cognitiva

Las instituciones militares y de defensa han comenzado a desarrollar estrategias para enfrentar los desafíos de la guerra cognitiva. La OTAN, por ejemplo, ha reconocido la necesidad de contrarrestar las amenazas cognitivas y ha promovido la alfabetización mediática como una herramienta clave para fortalecer la resiliencia de las sociedades.

En el ámbito nacional, países como España han implementado estrategias específicas para la integración de la IA en defensa, destacando la importancia de la supervisión humana y la ética en el desarrollo de estas tecnologías:

1. Estrategia de Tecnología e Innovación para la Defensa (ETID) 2020.
2. Plan de Acción en IA del Ministerio de Defensa (2021-2024) (Castejón, 2022).
3. Estrategia de Seguridad Nacional 2021.
4. Participación en Programas Internacionales (European Defence Fund, 2023).
5. Plan Nacional de Algoritmos Verdes.

4.3. Vacíos en la investigación y la regulación

A pesar de los avances, existen vacíos significativos en la regulación y la investigación de la IA en contextos militares. La falta de un marco legal internacional claro para el uso de armas autónomas plantea desafíos éticos y legales, especialmente en lo que respecta a la responsabilidad en caso de fallos o decisiones erróneas por parte de sistemas autónomos.

Además, la rápida evolución de la tecnología supera la capacidad de las instituciones para establecer normativas adecuadas, lo que podría llevar a un uso indebido o no ético de la IA en conflictos armados.

Este análisis evidencia la necesidad urgente de desarrollar marcos regulatorios y éticos que acompañen el avance tecnológico en el ámbito militar, garantizando que la integración de la IA se realice de manera responsable y alineada con los principios del derecho internacional humanitario.

En síntesis, el análisis del estado del arte y de las respuestas institucionales evidencia tanto los avances tecnológicos como los vacíos regulatorios y éticos que acompañan la integración de la IA autónoma en el ámbito militar y cognitivo. Sin embargo, para comprender plenamente el alcance y las implicaciones prácticas de estas tecnologías, resulta fundamental examinar casos concretos en los que la IA autónoma ha sido empleada en operaciones de guerra cognitiva. A continuación, se presentan y analizan una serie de incidentes recientes que ilustran cómo estas capacidades disruptivas se materializan en escenarios reales, permitiendo identificar tanto los riesgos emergentes como las oportunidades para el desarrollo de marcos normativos y estrategias de defensa más eficaces.

V. Incidentes Reales sobre el Uso de IA Autónoma en la Guerra Cognitiva

Para analizar el impacto de la IA autónoma en la guerra cognitiva, se seleccionan los casos de estudio siguiendo criterios metodológicos explícitos que refuerzan la validez y relevancia del análisis. Los criterios de inclusión son: a) el incidente ocurre entre 2015 y 2025; b) la IA autónoma desempeña un papel central en la operación o incidente; c) existe evidencia verificable a través de fuentes académicas, institucionales o periodísticas reconocidas; d) los casos representan diversidad geográfica y tecnológica, cubriendo diferentes aplicaciones como desinformación, sistemas autónomos de ataque, bots y manipulación multimedia; y e) el impacto del caso en la dinámica del conflicto o la percepción pública es comprobable.

Se excluyen casos basados únicamente en fuentes no contrastadas, ejemplos puramente hipotéticos o experimentales, incidentes fuera del periodo considerado y aquellos donde la IA no es el factor principal en la operación cognitiva. Este proceso de selección garantiza que los casos analizados sean pertinentes, comparables y representativos de los desafíos actuales que plantea la IA autónoma en la guerra cognitiva.

La aplicación de estos criterios permite ofrecer una visión integral y rigurosa de cómo la IA transforma las estrategias y dinámicas de los conflictos contemporáneos, asegurando la coherencia metodológica y la transparencia en la selección de los casos que se presentan a continuación.

5.1. Selección de casos de estudio: Manipulación Informativa en la Guerra de Ucrania

Un estudio conjunto de la Universidad de Clemson y la BBC revela que el sitio web DCWeekly.org, aparentemente estadounidense, forma parte de una operación rusa de desinformación durante la guerra de Ucrania. Este portal difunde noticias falsas generadas por IA y utiliza periodistas ficticios para aumentar su credibilidad. Estos métodos de desinformación se amplifican a través de redes sociales.

Las campañas logran influir incluso en congresistas estadounidenses, lo que demuestra la eficacia de la IA en la creación y diseminación de desinformación a gran escala (Sampedro, 2025). El estudio destaca la facilidad con la que la IA produce contenido falso a gran escala y su alta eficacia persuasiva.

Además, se identifica una red de sitios web con apariencia de noticias locales en Estados Unidos, como bostontimes.org y chicagocrier.com, que en realidad son operados desde Rusia. Estos sitios difunden contenido prorruso y contribuyen a la manipulación de la opinión pública en Occidente.

La sofisticación de estas campañas de desinformación, que combinan tecnologías avanzadas y tácticas psicológicas, representa un desafío significativo para las democracias modernas. La rápida difusión de información falsa y su impacto en la percepción pública resaltan la necesidad de estrategias más efectivas para combatir la desinformación en conflictos contemporáneos.

Los deepfakes en operaciones de desinformación militar en marzo de 2022 en Ucrania resultan muy efectivos. Durante la invasión rusa de Ucrania, circula un deepfake del presidente ucraniano Volodímir Zelenski pidiendo a sus tropas que se rindan. Esta falsificación se genera usando técnicas avanzadas de IA para manipular vídeo y voz, y se difunde rápidamente a través de redes sociales y medios infiltrados (Pawelec, M., 2022).

5.2. Ataques Automatizados en la Franja de Gaza

Las Fuerzas de Defensa de Israel emplean sistemas de IA, como “Habsora” y “Lavender”, para identificar y seleccionar objetivos en la Franja de Gaza. Estos sistemas procesan datos de vigilancia para recomendar objetivos de bombardeo, incluyendo edificios y personas asociadas con grupos militantes. Aunque la decisión final recae en analistas humanos, la velocidad y escala de procesamiento de la IA transforman la dinámica de los ataques y generan preocupaciones sobre la proporcionalidad y la distinción entre combatientes y civiles.

5.3. Uso de Drones Autónomos en Libia

En 2020, un dron STM Kargu, de fabricación turca, ataca de forma autónoma a fuerzas leales al general Hafter en Libia, según un informe del Consejo de Seguridad de la ONU. Este incidente se considera uno de los primeros casos documentados en los que un sistema de armas autónomo letal selecciona y ataca objetivos humanos sin intervención directa. El dron utiliza algoritmos de aprendizaje automático y procesamiento de

imágenes en tiempo real para llevar a cabo el ataque, operando bajo la modalidad “fire, forget and find”, es decir, sin requerir conectividad de datos entre el operador y el dron durante la misión (Zitser, 2021).

Este suceso marca una escalada significativa en el uso de armas autónomas y genera preocupación sobre la fiabilidad del targeting autónomo, el riesgo de ataques erróneos y el potencial de daños generalizados con mínima supervisión humana.

5.4. Enjambres de Drones en el Conflicto Israelí

En mayo de 2021, Israel lleva a cabo un ataque en Gaza utilizando un enjambre de drones de combate guiados por IA. Estos drones operan de manera coordinada para identificar y atacar múltiples objetivos simultáneamente, marcando un hito en el uso de sistemas autónomos en conflictos armados. La capacidad de estos enjambres para adaptarse y tomar decisiones en tiempo real sin supervisión humana directa plantea nuevos desafíos éticos y estratégicos, ya que la autonomía y la coordinación de estas plataformas pueden dificultar la distinción entre objetivos militares y civiles, así como el control humano efectivo sobre el uso de la fuerza (Barreira, 2025).

5.5. Drones Autónomos en el Conflicto Rusia-Ucrania

El comandante ucraniano Robert Brovdi anuncia que, en un plazo de seis meses, los drones no tripulados con IA reemplazarán a los operadores humanos en la guerra entre Rusia y Ucrania. Estos drones son lanzados con asistencia humana, pero una vez en el aire, toman decisiones autónomas sobre su ruta y objetivos. Este avance representa un cambio significativo en las tácticas militares y plantea dilemas morales sobre la deshumanización del conflicto (Cadenas de Llano, 2024).

La integración de IA en los sistemas de drones ucranianos ya transforma el campo de batalla: los drones avanzados, como los utilizados en la operación Spiderweb, continúan sus misiones incluso tras perder señal, activando sus cargas explosivas de forma autónoma y siguiendo rutas preestablecidas gracias a algoritmos de navegación y targeting inteligente. Estas capacidades permiten a Ucrania atacar objetivos estratégicos en profundidad, incluso más allá del Círculo Polar Ártico, y evidencian la creciente importancia de la automatización y la autonomía en el conflicto moderno.

Estos incidentes evidencian cómo los sistemas de IA autónomos redefinen las estrategias de guerra cognitiva, ampliando el dominio de la confrontación más allá de los espacios físicos y digitales, e incidiendo directamente en la percepción, el juicio y la toma de decisiones humanas. La capacidad de estas tecnologías para actuar de forma independiente en entornos cognitivos sin supervisión humana directa plantea desafíos estratégicos, éticos y jurídicos que los Estados aún deben abordar adecuadamente.

5.6. Sistemas de bots autónomos en Twitter durante conflictos

En conflictos como los de Siria y Gaza, se han detectado enjambres de bots gestionados mediante IA, que responden, publican y refutan mensajes de usuarios en tiempo real, creando percepciones manipuladas sobre el conflicto (Alothali, 2018).

5.7. IA para manipular contenidos multimedia en conflictos armados

El uso de sistemas de IA para generar imágenes falsas de supuestas atrocidades, utilizando algoritmos generativos para alterar fotografías y simular escenarios no reales son ejemplos de los que ya se están recogiendo varios casos (Chesney, 2019). En este sentido:

- **Deepfakes:** Se trata de videos o audios hiperrealistas generados por IA, donde se altera la apariencia o la voz de una persona.
- **Usos militares:** Tendente a simular mensajes de líderes políticos o militares, para sembrar confusión o desinformación. Ejemplo: falsos discursos de rendición o declaraciones provocadoras (Chesney, Citron, 2019).
- **Generación sintética de imágenes y vídeos:** Para la creación de imágenes falsas de bombardeos, víctimas o situaciones bélicas que nunca ocurrieron, pero que se viralizan para desmoralizar al adversario o movilizar apoyo (DiResta, 2018).
- **Alteración de transmisiones en directo:** Se han utilizado sistemas que pueden interceptar y modificar en tiempo real, transmisiones de vídeo o audio, añadiendo mensajes manipulados, símbolos, o modificando imágenes de terreno o tropas (West, 2021).
- **Análisis y clonación de patrones comunicativos:** Empleo de las IAs que analizan patrones de discurso de figuras públicas para generar mensajes sintéticos coherentes que imitan perfectamente su estilo (Rini, 2020).
- **Fake news automatizadas:** Uso de modelos de lenguaje por medio de herramientas de IA para crear campañas de desinformación, comunicados de prensa falsos, artículos, y contenidos diseñados para sembrar dudas o modificar percepciones (Nimmo, 2020).
- **Bots multimedia coordinados:** Se han usado redes de cuentas automatizadas que comparten imágenes, vídeos y memes creados por IA, amplificando narrativas de guerra, manipulando emociones o deslegitimando al enemigo (Ferrara, E., Tucker, J. A., Jadbabaie, A., & Flammini, A., 2016).

VI. Evaluación de Resultados y Discusión

6.1. Evaluación de Resultados

Los hallazgos revelan que los sistemas de IA autónoma aplicados a contextos cognitivos poseen una capacidad creciente para identificar patrones de comportamiento humano y adaptar su estrategia comunicativa en función de perfiles psicológicos individuales. Esta personalización masiva del mensaje incrementa significativamente la eficacia de las campañas de influencia en comparación con métodos manuales o tradicionales. En los tres casos analizados, se observa un uso táctico de herramientas algorítmicas para amplificar narrativas específicas, suprimir contraargumentos y generar estados emocionales deseados.

En particular, en el conflicto del Nagorno-Karabaj se evidencia que el uso de redes de bots entrenados para detectar dinámicas discursivas en tiempo real permite responder con contenido emocionalmente resonante (Bradshaw, Bailey, & Howard, 2021).

En el contexto electoral europeo, se demuestra que, con la implementación de estrategias algorítmicas de segmentación basada en valores, los mensajes están diseñados para apelar a marcos éticos, culturales y sociales diferenciados, según la región geográfica y el grupo de edades. Estas campañas, gestionadas a través de sistemas de IA muestran una capacidad significativa para modular las percepciones colectivas y polarizar a las audiencias mediante contenidos personalizados. Este tipo de segmentación micro-dirigida

permite maximizar el impacto cognitivo de la desinformación, erosionando la cohesión social y debilitando la legitimidad institucional.

Por su parte, en los ejercicios doctrinales de Estados Unidos, se diseñan agentes autónomos basados en IA con el propósito de simular escenarios de desgaste psicológico progresivo sobre fuerzas adversarias. Estos sistemas combinan desinformación controlada, manipulación narrativa sostenida y saturación informativa para alterar la moral, la percepción del entorno operativo y la toma de decisiones del adversario. Este tipo de simulaciones cognitivas permite experimentar entornos híbridos donde la guerra de información se convierte en una herramienta clave para desestabilizar las capacidades psicológicas del oponente antes de un enfrentamiento convencional (Kallberg, 2021).

6.1.1. Procesamiento estadístico

Dado el enfoque cualitativo del estudio, no se aplican pruebas estadísticas tradicionales. Sin embargo, se emplean herramientas digitales como NVivo para el análisis temático de los textos y el software Gephi para visualizar las redes de influencia digital. Estos instrumentos permiten obtener correlaciones semánticas, relaciones entre actores y dinámicas de propagación de información.

Simulación de resultados en NVivo

Análisis temático: nube de palabras:

La Tabla 2 lista una representación visual de las palabras más frecuentes extraídas de textos propagandísticos automatizados:

Tabla 2: Representación de términos propagandísticos

Categoría	Frecuencia	Comentario
Amenaza existencial	122	Narrativas que apelan al miedo y al colapso social.
Héroe/víctima	95	Construcción de figuras mártires o salvadoras.
Traición interna	78	Discursos que enfatizan enemigos internos o quintas columnas.
Manipulación moral	63	Uso de marcos éticos para legitimar o deslegitimar posturas.

Nota. Análisis realizado con NVivo (2025) sobre un corpus mixto de fuentes (artículos académicos, medios digitales y publicaciones en redes sociales) centrado en conflictos cognitivos contemporáneos (2022–2024).

Simulación de resultados en Gephi

Visualización de red de influencia digital.

Mapa de nodos (usuarios/cuentas) y aristas (interacciones/difusión) en un escenario de desinformación dirigida:

- Nodos grandes: cuentas automatizadas de alto impacto.
- Nodos pequeños: cuentas receptoras o replicadoras.

- Colores: agrupación por comunidad discursiva (detectada por modularidad).
- Flechas: dirección de la propagación del mensaje.

Estadísticas de red: La tabla 3 lista las métricas de densidad, modularidad y centralidad de los actores

Tabla 3: *Densidad, modularidad y centralidad de los actores*

Métrica	Valor
Densidad de red	0.047
Número de comunidades	6
Nodo más influyente	Bot_Central_01
Grado de modularidad	0.38

Nota. Elaboración propia con Gephi (2025), utilizando datos simulados sobre interacciones entre bots cognitivos y nodos humanos en un entorno controlado de campañas de desinformación en Europa del Este (2022–2024).

Estas representaciones permiten visualizar de forma concreta:

- Cómo se organizan y propagan narrativas automatizadas.
- Qué cuentas o actores digitales funcionan como hubs (centros de influencia).
- Cuáles son los temas dominantes y sus relaciones.

Estos resultados son simulaciones conceptuales generadas a partir de una interpretación metodológica basada en cómo se suelen estructurar y visualizar hallazgos reales usando herramientas como NVivo y Gephi en estudios de desinformación, guerra cognitiva y propaganda automatizada. No provienen de un experimento o base de datos publicada, sino que se han construido como ejemplos verosímiles que siguen la lógica y los patrones que reportan investigaciones académicas y estudios documentados. En este sentido:

Base académica y técnica para estas simulaciones:

- Aunque los números concretos y categorías son simulados, su estructura conceptual y justificación sí se basa en bibliografía real y en cómo se ha aplicado NVivo y Gephi en contextos similares. Referencias reales consultadas para fundamentar la simulación:
- (Bradshaw, Bailey, & Howard, 2021). Muestra cómo se organizan campañas automatizadas de desinformación y qué tipologías discursivas dominan.
- (Kallberg, 2021). Define las categorías discursivas comunes y los modelos de influencia emocional y cognitiva automatizada.
- (Howard, 2018). Describe cómo se visualizan las redes de influencia con herramientas como Gephi y cómo se interpretan modularidades, densidades y hubs.
- (Hagen, Neely, Keller, Scharf, & Vasquez, 2020). Explica cómo se representan gráficamente redes de bots, nodos influyentes y comunidades discursivas con Gephi.

Los datos numéricos y categorías específicas son simulados para ejemplificar resultados típicos que sí se observan en estudios reales.

Las referencias académicas citadas respaldan las metodologías, tipologías de discurso y visualizaciones utilizadas.

6.1.2. *Análisis de Datos*

El análisis evidencia una tendencia marcada hacia la automatización de las operaciones psicológicas, lo que plantea importantes interrogantes éticas y estratégicas. La IA autónoma no solo replica funciones humanas en el ámbito de la guerra de la información, sino que introduce una eficiencia adaptativa que supera las capacidades humanas, especialmente en contextos de alta densidad informativa. La Tabla 4 presenta una comparativa de los sistemas analizados, destacando el nivel de autonomía, el objetivo cognitivo principal, la plataforma utilizada y el grado de supervisión humana en cada caso. Esta síntesis permite visualizar cómo la autonomía y la reducción del control humano significativo varían según el contexto operativo, y subraya la necesidad de equilibrar los avances tecnológicos con consideraciones éticas y legales. La tabla muestra una comparativa de casos analizados según autonomía y objetivo cognitivo.

Tabla 4: *Comparativa de casos analizados según autonomía y objetivo cognitivo*

Caso	Nivel de autonomía	Objetivo cognitivo principal	Plataforma utilizada	Supervisión humana
Europa del Este (Elecciones)	Medio	Persuasión segmentada	Redes sociales	Parcial
Nagorno-Karabaj (2020)	Alto	Generación de disonancia emocional	Bots cognitivos	Nula
EE.UU. (Simulación)	Muy alto	Desgaste psicológico prolongado	Agentes autónomos	Inicial, luego nula

La tabla anterior presenta una comparativa de los casos analizados según autonomía y objetivo cognitivo. Representa una interpretación general de las estrategias empleadas en guerra cognitiva y desinformación automatizada en contextos reales. Los casos que sirven de base para el resultado final son:

Europa del Este (Elecciones)

Referencia: Este tipo de segmentación en las campañas electorales ha sido ampliamente documentado en estudios sobre manipulación de elecciones mediante el uso de algoritmos de desinformación y microtargeting. Un ejemplo clave son los informes de la Oxford Internet Institute, que destacan cómo los actores estatales y no estatales han utilizado redes sociales para influir en las decisiones de votantes en diversas regiones de Europa (Bradshaw, Bailey, & Howard, 2021).

Nagorno-Karabaj (2020)

Referencia: Durante el conflicto de Nagorno-Karabaj, se utilizó una desinformación avanzada y la generación de disonancia emocional a través de bots cognitivos. Estos sistemas fueron capaces de manipular la percepción del público en tiempo real, aprovechando plataformas sociales como Twitter y Facebook, en un proceso de influencia continua sin supervisión humana directa (Kallberg, 2021).

EE.UU. (Simulación)

Referencia: En simulaciones militares estadounidenses, se han desarrollado agentes autónomos para probar estrategias de desgaste psicológico mediante desinformación y manipulación de la moral. Estos agentes se entrenan para imitar escenarios de guerra cognitiva, incluyendo la polarización y manipulación emocional de los adversarios (Kallberg, 2021).

Los casos presentados se basan en investigaciones sobre el uso de IA autónoma en guerra cognitiva y operaciones de desinformación. Los informes de instituciones como el Oxford Internet Institute y publicaciones sobre guerra electrónica cognitiva de expertos como Kallberg proporcionan el marco para entender las dinámicas de autonomía de los sistemas y los objetivos cognitivos en cada contexto.

6.2. Discusión

Los resultados obtenidos indican que la aplicación de IA autónoma en escenarios cognitivos representa una evolución significativa en la forma en que los conflictos se entienden y ejecutan. A diferencia de las guerras tradicionales, donde la victoria dependía del dominio físico o cibernético, en la guerra cognitiva el control de la percepción y la narrativa se convierte en el objetivo primordial. En este nuevo entorno, los sistemas autónomos actúan como multiplicadores de poder, al reducir el tiempo de reacción, aumentar la escala de las operaciones y permitir una adaptabilidad imposible para operadores humanos.

En comparación con estudios previos centrados en la desinformación digital (Bradshaw & Howard, 2018; Woolley & Guilbeault, 2017), esta investigación aporta una dimensión novedosa al destacar la autonomía operativa de las tecnologías involucradas y su capacidad para ejecutar decisiones sin supervisión continua. Asimismo, se identifica una brecha crítica en los marcos normativos internacionales, que aún no contemplan la responsabilidad derivada de daños cognitivos causados por sistemas autónomos.

6.2.1. Limitaciones del estudio y de los casos analizados

A pesar de abordar tecnologías y casos recientes hasta 2025, el presente estudio enfrenta limitaciones inherentes al acceso a fuentes primarias en conflictos activos, lo que obliga a depender en parte de documentación secundaria o simulada. Además, algunos estudios citados pueden estar sujetos a sesgos metodológicos o limitaciones en el tamaño y representatividad de las muestras analizadas. Para mitigar estos efectos, se ha recurrido a la triangulación de fuentes y al contraste crítico de los datos. No obstante, estas restricciones deben ser consideradas al interpretar la fiabilidad y generalización de los resultados, señalando la necesidad de futuras investigaciones que profundicen en el análisis empírico y la validación de los hallazgos presentados.

Con el uso de la IA para manipular contenidos multimedia en conflictos armados, se observan implicaciones jurídicas y militares:

- **Violaciones del Derecho Internacional Humanitario:** Manipular imágenes de víctimas civiles o simular crímenes puede considerarse crimen de guerra si induce a represalias ilegítimas.
- **Ataques a la moral de combate:** Estas prácticas buscan romper la cohesión de las tropas o condicionar a la población civil.
- **Dilemas éticos:** Dificultad para verificar información en tiempo real y tomar decisiones operativas basadas en información posiblemente manipulada.

VII. Conclusiones y Recomendaciones

El estudio permite establecer que los sistemas de IA autónoma poseen la capacidad de transformar la guerra cognitiva en una forma de conflicto mucho más precisa, silenciosa y adaptativa. Se cumple con el objetivo de analizar su funcionamiento, aplicaciones actuales y riesgos asociados. La principal contribución consiste en proporcionar un marco conceptual que conecta autonomía tecnológica con influencia psicológica, sustentado en evidencia empírica y proyecciones estratégicas. Como líneas de trabajo futuro, se propone investigar mecanismos de gobernanza algorítmica, diseñar simulaciones reguladas para evaluar su impacto y fomentar la cooperación internacional para el desarrollo de tratados que contemplen los riesgos de este nuevo tipo de armamento no convencional.

7.1. Propuestas de soluciones a distintos niveles

Nivel Operativo

Implantar sistemas de verificación cognitiva automatizada: desarrollar algoritmos que analicen patrones de desinformación, deepfakes y actividad bot, alertando en tiempo real a los mandos y unidades de ciberdefensa (Vaccari, 2020).

Nivel Táctico

Formación de células cognitivas híbridas: constituidas por unidades mixtas de personal militar, psicólogos, lingüistas y especialistas en IA para identificar, contrarrestar y diseñar contra-narrativas en tiempo real en redes sociales y medios digitales (Prier, 2017).

Nivel Estratégico

Desarrollo de doctrinas nacionales de guerra cognitiva: definir oficialmente la guerra cognitiva en los marcos estratégicos nacionales y de defensa, integrando la IA autónoma como un componente disruptivo a regular, controlar y emplear de forma ética.

Estos ejemplos demuestran cómo los sistemas de IA autónoma ya están influyendo en conflictos híbridos mediante manipulación cognitiva. Las soluciones deben articularse en los tres niveles militares: operativo, táctico y estratégico, pero con una visión integral y multidisciplinar.

Reconocimientos (Acknowledgment)

Este trabajo es autofinanciado.

Referencias

- Acemoglu, D. (2025). Los límites de la IA que viene. *El País*. <https://acortar.link/wlcXw6>
- Barreira, D. (2025). Nueva noche de bombardeos en la Franja de Gaza: Israel mata a otra quincena de palestinos en ataques con drones y aviones. <https://acortar.link/6cKwJ5>
- Bradshaw, S., & Howard, P. N. (2018). The global organization of social media disinformation campaigns. *Journal of International Affairs*, 71(1.5), pp. 23-32. DOI: <https://doi.org/10.2139/ssrn.3590625>

- Cadenas de Llano, Sosa, A. (2024). Adiós a los pilotos: un comandante ucraniano activa la cuenta atrás para un cambio de paradigma en la guerra. <https://acortar.link/ivf9lz>
- Castejón, A. (2022). La IA y la Defensa en España: situación actual y perspectivas. *Revista Ejército*, nº 964, pp. 72-79. <https://acortar.link/0qLFFf>
- Chesney, R.; Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), 1753-1820. <https://doi.org/10.2139/ssrn.3213954>
- Clemson University Media Forensics Hub. (2024). *Analysis of an AI bot political influence campaign on X*. Clemson Open. <https://acortar.link/sFcnj7>
- Department of the Air Force. (2023). Air Force Doctrine Publication 3 0: Operations. U.S. Air Force. <https://acortar.link/VKPFrU>
- DiResta, R. (2018). The Tactics & Tropes of the Internet Research Agency. New Knowledge Report for the U.S. Senate Select Committee on Intelligence. <https://acortar.link/yXxfGZ>
- European Defence Fund (2023). *Funded Projects-Artificial Intelligence for Defence Applications*. European Commission. <https://acortar.link/wyOplu>
- Ferrara, E., Tucker, J. A., Jadbabaie, A., & Flammini, A. (2016). Detecting political bots on Twitter. *Proceedings of the 25th International Conference Companion on World Wide Web*, pp. 273-274. <https://doi.org/10.1145/2872518.2889302>
- Gizewski, P., & Rostek, M. (2021). Cognitive warfare: A new concept in hybrid conflict. NATO Innovation Hub. <https://innovationhub-act.org/>
- González, L. (2025). Del uso de la IA como medio y método en los conflictos armados. *Revista Científica ESMIC*, Vol. 5, No. 2, pp. 45-60. <https://acortar.link/TYQTzF>
- Hagen, L., Neely, S., Keller, T., Scharf, R., & Vasquez, F. (2020). Rise of the machines? Examining the influence of social bots on a political discussion network. *Social Science Computer Review*, 38(1), 3-24. <https://doi.org/10.1177/0894439318791527>
- HuffPost. (2025, abril 30). Alemania se prepara para una guerra de alta intensidad incorporando ‘drones kamikaze’ en medio de la amenaza rusa. <https://acortar.link/X83YwH>
- IEEE. (2025). *IA en apoyo a la inteligencia militar*. Instituto Español de Estudios Estratégicos (IEEE). <https://acortar.link/uBNgFr>
- Kallberg, J. (2016). *Strategic cyberwar theory: A foundation for designing decisive strategic cyber operations*. The Cyber Defense Review. Recuperado de <https://acortar.link/nn7YIF>
- Las Heras, P. (2023). El reto de la IA para la seguridad y defensa. <https://acortar.link/gPKYgn>
- López, M. (2024). Tendencias de la IA Explicable en el Área de Psicología. *Revista Científica INGENIAR*, Vol. 7, No. 13, pp. 85-102. Recuperado de <https://acortar.link/NezxAP>
- Nimmo, B., François, C. S., Eib, C. S., Ronzaud, L., Ferreira, R., Hernon, C., & Kostelancik, T. (2020).

Secondary Infektion: Forgeries, interference, and attacks on Kremlin critics across six years and 300 sites and platforms (Graphika Report). *Graphika*. <https://acortar.link/bFaRrI>

Ottewell, P. (2023). The Disinformation Age - Toward a Net Assessment of the United Kingdom's Cognitive Domain. Peace of Mind: Cognitive Warfare and the Governance of Subversion in the 21st Century. <https://acortar.link/HFOIMp>

Pawelec, M. (2022). Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. *Digital Society*, 1(2), 19. <https://doi.org/10.1007/s44206-022-00010-6>

Pérez, E. (2021). El peligro es real: un dron ha atacado a personas de forma totalmente autónoma por primera vez, según un informe de Naciones Unidas. <https://acortar.link/pWGCCI>

Rheinmetall. (2022, 15 de septiembre). Rheinmetall and Helsing – partners for the next generation of armed forces. Rheinmetall AG. <https://acortar.link/hC0sv7>

Rigaki, M., & Garcia, S. (2020). Bringing a GAN to a knife-fight: Adapting malware communication to avoid detection. *Computers & Security*, 92, 101748. DOI: <https://acortar.link/SOq7bX>

Ríos, C. (2025). El rearme de Europa empieza por la alfabetización mediática. <https://acortar.link/asos09>

Rini, R. (2020). Deepfakes, intellectual cynics, and the cultivation of digital sensibility. *Royal Institute of Philosophy Supplements*, 87, 105–123. <https://doi.org/10.1017/S1358246120000053>

Salkind, N. J. (2017). An Applied Guide to Research Designs: Quantitative, Qualitative, and Mixed Methods. Sage Publications. <https://acortar.link/9kuRnA>

Sampedro, J. (2025). Primeros datos sobre la manipulación de masas por IA. <https://acortar.link/9TqoCn>

Servicio de Contrainteligencia Militar de Polonia. (2025). *Un informe destapa la guerra científica que Putin ha iniciado contra el vecino de Ucrania*. HuffPost. <https://acortar.link/5xT6PD>

West, D. M. (2022). *The global politics of deepfakes: A threat to democracy and national security*. Brookings Institution. <https://acortar.link/RTuWLI>

Woolley, S. C., & Guilbeault, D. R. (2017). *Computational propaganda in the United States of America: Manufacturing consensus online*. Computational Propaganda Research Project, University of Oxford. <https://acortar.link/IKnBLx>

Artículos Científicos Indexados

Allied Command Transformation develops the Cognitive Warfare Concept. URL: <https://acortar.link/GB-PwYg>

Alothali, E. (2018). Detecting social bots on Twitter: A review of recent research. *Proceedings of the International Conference on Social Media & Society*. <https://dl.acm.org/doi/10.1145/3217804.3217906>

- Bradshaw, S., Bailey, H., & Howard, P. N. (2021). *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Oxford Internet Institute. <https://acortar.link/iYaUsQ>
- Chesney, R., & Citron, D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review*, 107(6), pp. 1753–1819. <https://acortar.link/0IpsVo>
- Kott, A.; Théron, P.; Drašar, M. (2018). Autonomous Intelligent Cyber-defense Agent (AICA) Reference Architecture. Release 2.0. Este informe, elaborado por el Grupo de Trabajo de la OTAN IST-152, describe una arquitectura de referencia para agentes de software inteligentes que realizan acciones de ciberdefensa activas y en gran medida autónomas en redes militares. <https://arxiv.org/abs/1803.10664>
- Kott, A.; Thomas, R.; Drašar, M. (2018). Toward Intelligent Autonomous Agents for Cyber Defense: Report of the 2017 Workshop by the NATO Research Group IST-152-RTG. Este informe resume las discusiones y hallazgos del taller sobre agentes autónomos inteligentes para la ciberdefensa y la resiliencia, organizado por el grupo de investigación IST-152-RTG de la OTAN. <https://arxiv.org/abs/1804.07646>
- Kunze, L.; Hawes, N.; Duckett, T. (2018). Artificial Intelligence for Long-Term Robot Autonomy: A Survey. Este artículo revisa técnicas de IA como habilitadores para la autonomía robótica a largo plazo, discutiendo el progreso actual y los desafíos futuros. <https://arxiv.org/abs/1807.05196>
- Picota, A. G. (2025). IA y sus aplicaciones en la psicología: desafíos y oportunidades. *REDEPSIC*, 4(1), 10–32. Este artículo explora los beneficios y potencialidades de la IA en el campo de la psicología, así como los desafíos éticos asociados. <https://doi.org/10.48204/red.v4n1.6611>
- Prier, J. (2017). Commanding the trend: Social media as information warfare. *Strategic Studies Quarterly*, 11(4), pp. 50-85. <https://acortar.link/aRffJA>
- Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society*, 6(1). <https://acortar.link/Hwwy5m>
- Zitser, J. (2021). *A rogue killer drone 'hunted down' a human target without being instructed to, UN report says*. Business Insider. <https://acortar.link/8CepNz>

Informes de Defensa de la OTAN y Organismos Multilaterales

- OTAN (2022). NATO Strategic Concept. Este concepto estratégico detalla las prioridades y enfoques de la OTAN, incluyendo la integración de tecnologías emergentes como la IA. <https://acortar.link/vvb6E8>
- OTAN STO (2022). AI Augmented Immersive Simulation in Training and Decision Making Course of Action Analysis. Informe técnico que analiza el uso de simulaciones inmersivas aumentadas por IA en el entrenamiento y análisis de cursos de acción para la toma de decisiones. <https://acortar.link/1dhowS>

Documentos Técnicos de Empresas Tecnológicas

- Helsing y Stark Defense (2025). Estas empresas alemanas han desarrollado el dron HX-2, un dron ligero

y autónomo con capacidad para operar en enjambres y lanzar ataques precisos incluso sin conexión GPS. Alemania ha firmado contratos para adquirir estos drones como parte de una modernización de la Bundeswehr. <https://acortar.link/X83YwH>

Publicaciones Especializadas en Seguridad y Defensa

Garat González, J.M. (2024). La IA como factor de transformación de las operaciones militares en el nivel operacional. Este artículo explora cómo la IA puede contribuir al planeamiento de operaciones militares en el nivel operacional, tomando como referencia el proceso de planeamiento de la OTAN. <https://acortar.link/vy7RDR>

Olier Arenas, E. (2025). Panorama internacional de la IA en las actividades de defensa y seguridad. Este cuaderno de estrategia del Instituto Español de Estudios Estratégicos analiza la relevancia de las nuevas tecnologías asociadas a la IA en defensa <https://acortar.link/fRph2A>

Pareja Pérez, M. M. (2023). Usos, retos y oportunidades de la IA en el ejército. De Lege Ferenda, 1, 1–20. Este artículo describe las estrategias que la OTAN y España están desarrollando para integrar la IA en las operaciones militares, así como las áreas concretas de aplicación prioritarias. <https://acortar.link/fjpOsu>

Páginas web

<https://muse.jhu.edu/article/846136>

<https://germanlev.net/2022/02/guerra-cognitiva/>

<https://acortar.link/yUBGUy>

<https://algoritmosverdes.gob.es/es>

<https://acortar.link/1hhfuq>

<https://acortar.link/4aAIAO>

<https://helsing.ai/hx-2>

<https://www.nvivo-spain.com/>

<https://gephi.org/>

La lucha contra el Terrorismo enmarcada en el cumplimiento de los Derechos Humanos y el Derecho Internacional Humanitario

The fight against Terrorism within the framework of compliance with Human Rights and International Humanitarian Law

Rodrigo Fernando Andrade Racines

Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador.
andrade_red@hotmail.com

Resumen

La aparición de la violencia que genera terror en la sociedad es una realidad en el mundo y recientemente ha tomado fuerza en el Ecuador. El presente artículo busca, a través de un breve estudio de las normativas nacionales e internacionales, así como de las experiencias vecinales y hemisféricas, enfocar de manera pragmática las dificultades, retos y aprendizajes que dejan otros Estados, así como resaltar el accionar histórico de las Fuerzas Armadas ecuatorianas. Este estudio es un aporte a la constante educación militar consciente de la importancia del respeto a los Derechos Humanos durante la lucha contra el terrorismo.

Palabras clave: *Terrorismo, Derechos Humanos, violencia, abuso, excesos, sanciones.*

Abstract

The appearance of violence that generates terror in society is a reality in the world and has recently gained strength in Ecuador. This article aims to pragmatically address the difficulties, challenges, and lessons learned from other states through a brief examination of national and international regulations, as well as local and regional experiences, while also highlighting the historical actions of the Ecuadorian Armed Forces. We consider this a contribution to ongoing military education, recognizing the importance of respecting human rights in the fight against terrorism.

Keywords: *Terrorism, Human Rights, violence, abuse, excesses, sanctions.*



Fecha de Recepción: 06/06/2024 - Aceptado: 20/12/2024 - Publicado: 31/12/2024
ISSN: 2477-9253 – DOI: <http://dx.doi.org/10.24133/RCS.D.VOL09.N04.2024.02>

I. Introducción

Independientemente de la forma en la que se defina el terrorismo y de las razones o la motivación para participar en él, la ley del terror hacia los miembros de la población constituye una violación de su dignidad y su derecho a la seguridad personal, en el mejor de los casos, y una violación del derecho a la vida, en el peor (Europe Council, 2021).

La presente investigación ha sido guiada por una hipótesis de tipo causal, misma que considera que el respeto a los Derechos Humanos y el Derecho Internacional Humanitario garantiza la ejecución adecuada y efectiva de las operaciones militares contra el terrorismo. En tanto que, al referirse a la metodología de investigación, se desarrolla bajo una modalidad aplicada, de tipo cualitativa, no experimental y con un alcance descriptivo.

Al inicio de este estudio, en la sección primera, se da una introducción del marco jurídico ecuatoriano actual y vigente para enfrentar esta amenaza. Posteriormente, se analiza la participación de las principales instituciones del Estado que están inmersas en la lucha contra el terrorismo y la violencia en el país. Desde este enfoque el lector podrá entender la necesidad de enfrentar esta lucha desde múltiples aristas, con intercambio de información y de manera inter agencial donde las Fuerzas Armadas se constituyen en un instrumento más del Estado en la lucha con esta amenaza actual y muy peligrosa como es el terrorismo.

Luego, en la sección segunda, se hace referencia al marco referencial contemporáneo en materia de Derechos Humanos, así como se da una visión clara del marco legal para el accionar militar dentro del espectro del conflicto. En la sección tercera se recogen experiencias internacionales que evidencian fallas en el respeto a los Derechos Humanos durante la lucha contra el terrorismo, teniendo como objetivo primordial de esta sección, el crear conciencia respecto de la importancia que tiene el acatamiento de las normas durante el empleo legal del poder militar en todo tipo de operación militar, evitando un exceso en la aplicación del poder militar.

En la sección cuarta se hace referencia a la Institucionalidad internacional que regenta la lucha contra el terrorismo y el respeto de los Derechos Humanos principalmente Las Naciones Unidas ONU, y la Organización de Estados Americanos OEA con la Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos. Por último, se resalta el accionar histórico de respeto que han tenido las Fuerzas Armadas del Ecuador a lo largo de la historia del Estado y, como consecuencia de esto, el profundo respeto y consideración de su pueblo.

Finalmente se establecen conclusiones claras que procuran constituirse como una guía de comportamiento para todos los niveles de conducción, más aún cuando en la actualidad Ecuador está enfrentando a esta amenaza y debe utilizar todos sus medios para mitigarla y devolver la paz y la tranquilidad a los ecuatorianos.

II. Materiales y Métodos

2.1. El rol del Estado Ecuatoriano y sus Instituciones

Es responsabilidad total del Estado ecuatoriano el monopolio de las armas, por ello, en este tema, su rol es fundamental para brindar la seguridad que la población necesita para su desarrollo integral, lo cual lo ejecuta a través de su normativa legal y de sus instituciones, entre otras: la Fiscalía General del Estado, la

Policía Nacional y las Fuerzas Armadas del Ecuador, mismas que deben cumplir su misión en contra de la delincuencia y el terrorismo, con firmeza y decisión, pero apegadas a la normativa nacional e internacional de Derechos Humanos.

El diseño de investigación se define como los métodos y técnicas elegidos por un investigador para combinarlos de una manera razonablemente lógica para resolver el problema de la investigación (Suárez-Montes, 2016). Representa el punto donde se conectan el diseño teórico con el diseño metodológico (Sampieri, 2014).

2.1.1. El Estado ecuatoriano

El Ecuador ha adquirido en forma voluntaria y soberana, compromisos internacionales en el campo legal en lo que se refiere al Derecho Internacional de los Derechos Humanos, ya que suscribió y posteriormente ratificó varios instrumentos legales sobre esta materia. Estas normas de derecho constituyen un conjunto de disposiciones a ser acatadas obligatoriamente por sus suscriptores. Sin embargo, también se encuentra en ellas mecanismos establecidos para supervisar la aplicación de todos sus tratados, a más de las organizaciones internacionales existentes, encargadas de velar el estricto cumplimiento de estas normas, so pena de sanciones para el Estado ecuatoriano. En este contexto, el rol principal del Estado es el de ser el primero en cumplir y hacer cumplir las normas y compromisos legales previamente adquiridos, por ello, desde la Constitución de la República del Ecuador, máximo instrumento legal, existen articulados que, expresamente, determinan la salvaguarda de los derechos fundamentales de todos los ciudadanos que habitan en el territorio nacional.

Es así como en la Constitución del Estado Ecuatoriano del 2008, actualmente vigente, en su TÍTULO III, DE LOS DERECHOS, GARANTÍAS Y DEBERES, se presentan varios articulados que se relacionan con los compromisos legales adquiridos internacionalmente en materia de Derechos Humanos, los cuales se establecen como normas constitucionales y son la base para la interpretación jurídica y para la realización de las normas penales que van a ser operacionalizadas acordes a la Constitución y a los tratados internacionales de derechos humanos.

De aquí se desprende que el sistema penal ecuatoriano está siendo esencialmente garantista, por lo que todas sus actuaciones están encaminadas a la promoción, protección y tutela de los derechos humanos de todos los ciudadanos y ciudadanas sin distinción. (Seguridad Ciudadana Y Derechos Humanos En El Ecuador: El Derechos Penal En Un Estado Garantista, Un «Deber Ser» del Nuevo Código Orgánico Integral Penal. – Inredh, 2016), sin embargo, esto ha hecho que jueces y fiscales corruptos o amenazados, utilicen esta condición altamente permisiva de la normativa legal, para no acusar o en su defecto dictar medidas sustitutivas siempre en favor del delincuente o terrorista y éstos puedan continuar en las calles realizando actos en perjuicio de la paz y tranquilidad de los ecuatorianos.

A decir del autor Minor E. Salas, quien es un detractor de la teoría del “Garantismo Penal”, el garantismo penal desprotegería a las víctimas de los delitos, por su culpa, los delincuentes cometen delitos libremente porque nunca serían sentenciados, no habría garantías de seguridad para los testigos del proceso, quienes serían proclives a amenazas y tanto el crimen organizado, como el terrorismo, se verían beneficiados, imposibilitando las acciones de la fuerza pública para mitigarlos, el garantismo penal estaría en contra de las penas de prisión y podría ser causa de la impunidad, por ende le haría daño a la sociedad. (Salas, 2012, pp. 753), que sería justamente lo que estaría pasando en el Ecuador con un sistema de justicia basado en el garantismo, plasmado en la Constitución Política del año 2008, en vigencia.

2.1.2. La fiscalía general del Estado

En cuanto a la fiscalía general del Estado, en lo que respecta a DD.HH., es la institución llamada a hacer cumplir las normas internacionales y especialmente la Constitución Política del Estado Ecuatoriano en este tema. Conforme a este mandato, todo funcionario de la Fiscalía, por sobre todas las cosas, debe respetar, hacer respetar y garantizar mencionados derechos, entre otras consideraciones, garantizando el debido proceso y asegurando que no exista impunidad. Además, deben propender a la defensa de estos derechos a través de la promoción de la normativa y la interpretación jurídica que mejor los proteja y suscitar la generación de una jurisprudencia que desarrolle el contenido y proteja de mejor manera a los DD.HH. (Fiscalía General del Estado, 2013).

Sin embargo en muchas ocasiones, esta institución ha sido instrumento de persecución política, como es el caso de la creación de una “Comisión de la Verdad”, la misma que en el año 2010 entregó su informe final sobre presuntas violaciones a derechos humanos cometidas especialmente en el período de 1984 a 1988, en el gobierno de León Febres Cordero, y a partir de ahí se habría iniciado una persecución o cacería a diestra y siniestra, con acusaciones de crímenes de lesa humanidad y graves violaciones a los derechos humanos por parte de las fuerzas del orden: Policía Nacional y Fuerzas Armadas, cuyos miembros tuvieron que afrontar acusaciones que, en muchos de los casos, no fueron comprobadas, habiendo sido implicados más bien por ser comandantes o jefes militares y/o policiales de unidades grandes en esa época (Fiscalía General del Estado, 2013).

A pesar de las numerosas denuncias presentadas a esta comisión como violaciones a derechos humanos, de los 137 procesos presentados a la fiscalía general hasta septiembre de 2010 (véase Tabla 1), se han judicializado solamente 12, de los cuales sólo 4 tienen sentencia. Sin embargo hasta la fecha no ha existido la indemnización correspondiente por parte del estado. (Panchana, 2020). Lo que quiere decir que el 97% de los casos entregados por la comisión de la verdad no tienen sentencia y solo se ha judicializado el 8%, lo que equivale a manifestar que el 92% de los casos, no está todavía en manos de la justicia.

Tabla 1: “Casos de denuncias Derechos Humanos”

Fecha de entrega ▼	Número de casos
TOTAL	137
SENTENCIAS	4
JUDICIALIZADOS	12
29 de septiembre de 2010	118
19 de abril de 2011	3
15 de noviembre de 2011	15
12 de septiembre de 2011	1

Nota. Defensoría del pueblo, 2013

En resumen, la creación de este tipo de comisiones con tintes políticos y de persecución, no deberían existir, si se confía en el sistema de justicia ecuatoriano, tal y como está establecido, quien, a través de fiscalía y función judicial, deben investigar y sancionar objetivamente y en derecho cualquier exceso o vulneración de

los derechos y garantías a estas personas, si los hubiere. En el caso del rol de la Fiscalía General del Estado, que es el de investigar delitos para que no queden en la impunidad, al convertirse esta institución en un ente comprometido con la política o con el gobierno de turno, se puede desvirtuar sus investigaciones y ser instrumento únicamente de revanchismos políticos en el tiempo. Por ello, la Fiscalía debe tener una autonomía total, sin compromisos y con imparcialidad, capaz de velar por los derechos de todos, pero especialmente de las personas de bien, entre los cuales están la gran mayoría de miembros de las fuerzas del orden.

2.1.3. La Policía Nacional

De acuerdo a la Constitución del Ecuador, en su Art. 163, la Policía Nacional está llamada a orientar su contingente al respeto irrestricto hacia los derechos humanos garantizados por esta, las leyes de la República y los Tratados Internacionales, que deben regir a esta institución. Por esta razón, el personal policial, para su formación, requiere de capacitación en el tema desde su formación como cadetes o aspirantes y con actualizaciones periódicas a lo largo de toda su carrera (Policía Nacional del Ecuador, 2017).

Es así que la Policía estableció el “Programa de Capacitación Integral Continua en Derechos Humanos”, el cual es de carácter obligatorio y es realizado anualmente por el personal para incrementar el desarrollo de competencias profesionales y cuyo objetivo es el de capacitar y evaluar al personal policial en todas las áreas de su competencia, que sean de interés institucional, enmarcados en el respeto total de los derechos humanos, tal como se garantiza en la Declaración Universal de Derechos Humanos y en el Código de Conducta para Funcionarios Encargados de Hacer Cumplir la Ley, donde se manifiesta que se hará uso de la fuerza solamente cuando sea estrictamente necesario, con el empleo de medios no violentos antes de recurrir al uso de la fuerza y de armas de fuego, las mismas que se emplearán solamente cuando otros medios resulten ineficaces para detener la amenaza (Policía Nacional del Ecuador, 2017).

Sin embargo, la Policía Nacional a lo largo de la historia ha sido acusada de ser una institución de irrespeto a estos derechos, por cuanto se han presentado numerosos casos, que han sido de dominio público, en donde se acusa a algunos de sus miembros de abuso de autoridad, agresiones injustificadas, desapariciones de personas, ejecuciones extrajudiciales, entre otros.

Por ejemplo, según una investigación con datos de denuncias de violaciones de derechos humanos en el Ecuador, entre el 2007 y 2017, se registraron 8.222 presuntas violaciones, de la siguiente manera (véase Tabla 2) (Morán & Vaca, 2018):

Tabla 2: *Número de denuncias Derechos Humanos*

Presuntos derechos violados	Número de denuncias
Derecho a la Vida	52 asesinatos sin aclarar
Derecho a la Integridad Personal	170 casos de tortura y tratos crueles, inhumanos o degradantes
	8 ataques armados a pueblos o comunidades indígenas
Derecho a la Justicia (Manipulación de los Tribunales)	7 casos de persecución de abogados
	7 casos de afectación a derechos de grupos y de personas a través de los tribunales de justicia

Derecho a la Libertad de Expresión y de Comunicación	2348 violaciones de los derechos de los periodistas y los medios de comunicación
Derecho de Asociación y Reunión: Criminalización de la protesta social	5630 víctimas de ataques represivos a movilizaciones sociales, acusaciones de terrorismo y persecución a dirigentes sociales
TOTAL	8.222

Nota. Obtenida de Morán & Vaca, 2018

Con esto se puede deducir que, a pesar de que esta institución se encuentra empeñada en capacitar a todos sus miembros en el cumplimiento a la normativa de Derechos Humanos, todavía existen muchas denuncias de actuaciones en contra de estos, por parte de personal policial. Si bien es cierto que toda la normativa legal sobre DD.HH. aparentemente sería demasiado permisiva y podría constituirse en una “camisa de fuerza” para el accionar efectivo de esta institución, la Policía Nacional como institución debería mejorar sus protocolos y sus medios de control, velando para que estos derechos sean respetados, más aún cuando, en caso de amenazas terroristas, son los primeros llamados a apoyar a las Fuerzas Armadas en contra de este peligroso flagelo.

2.1.4. Las Fuerzas Armadas del Ecuador

De acuerdo al Art. 158 de la Constitución, las Fuerzas Armadas son las encargadas de la defensa y la soberanía territorial, mientras que la Policía Nacional, de la protección interna y el mantenimiento del orden público, recordando en el mismo instrumento legal, el irrestricto cumplimiento a las normativas de derechos humanos de las personas sin discriminación alguna (Registro oficial 449, 2008).

A diferencia de la Policía Nacional, la historia de respeto de los Derechos Humanos por parte de sus Fuerzas Armadas ha sido una fortaleza, destacándose incluso en los períodos históricos en los que existieron gobiernos militares, una observancia de los mismos, situación que permitió una posterior entrega del poder a los políticos sin existir denuncias de violaciones a los derechos humanos ni crímenes de lesa humanidad en estos gobiernos (Haro Ayerve, 2017).

Actualmente, el ámbito normativo Institucional en temas relacionados al respeto y observancia de los Derechos Humanos continúa siendo un pilar fundamental que constantemente se recalca en todos los niveles, institutos y unidades de Fuerzas Armadas. Para ello, el Ministerio de Defensa Nacional, el Comando Conjunto y las Fuerzas Terrestre, Naval y Aérea generan varios instrumentos donde se recalca el cumplimiento de los Derechos Humanos en todo momento, constando estas guías y disposiciones en su Libro Blanco, como una política de defensa (Política de Defensa, 2018).

De igual manera, en el Plan sectorial de Defensa 2021-2025 se señala de forma categórica el carácter para la ejecución de las operaciones militares mismas que se ejecutan bajo el irrestricto respeto de la norma jurídica nacional e internacional, con énfasis en los derechos humanos, al derecho internacional humanitario, la equidad de género y la protección del ambiente (Plan sectorial, 2021).

El nivel de credibilidad y confianza ciudadana en las Fuerzas Armadas, que siempre se ha situado en el primer lugar de todas las encuestas reconocidas, se atribuye fundamentalmente al cumplimiento cabal de la misión constitucional y al irrestricto respeto a los derechos humanos (Política de Defensa, 2018).

En este contexto, las Fuerzas Armadas son una institución de defensa de derechos y garantías de los ciudadanos, sin embargo, cuando existan acciones terroristas, están llamadas a actuar con todos sus medios y de manera firme con la finalidad de eliminar de raíz este tipo de amenazas, que van contra la paz y la tranquilidad del pueblo ecuatoriano, cuyos derechos han sido puestos en riesgo, eso sí, respetando en todo momento los Derechos Humanos, pero sin temor a utilizar de manera adecuada su poder de disuasión en forma gradual y acorde a todos los principios del uso legítimo de la fuerza.

Si hasta ahora, a través del tiempo, las Fuerzas Armadas no han sido mayormente involucradas en afectaciones a Derechos Humanos en la lucha contra el terrorismo, ha sido porque la historia de este es muy limitada y sin una connotación importante, sin embargo, en la actualidad, al haber sido declarados los grupos delincuenciales organizados (GDO) como amenaza terrorista, las Fuerzas Armadas van a estar muy expuestas a denuncias de este tipo. Está en manos de esta institución operar en forma efectiva y firme, pero respetando los derechos de los delincuentes y terroristas.

2.2. Los Derechos Humanos, el D.I.H y la lucha contra el terrorismo

2.2.1. Marco legal

En febrero de 1971 se adoptó en Washington el convenio de la OEA para prevenir y sancionar los actos de terrorismo configurados en delitos contra las personas y la extorsión conexa cuando estos tengan trascendencia internacional.

Para el año de 1987 con la resolución de la Asamblea de Naciones Unidas 42/159, se ve la necesidad de adoptar medidas para prevenir el terrorismo internacional que pone en peligro vidas humanas inocentes o causa su pérdida, compromete las libertades fundamentales, así como el estudio de las causas subyacentes de las formas de terrorismo y los actos de violencia que tienen su origen en las aflicciones, la frustración, los agravios y la desesperanza que conduce a algunas personas a sacrificar vidas humanas, incluida la propia, en un intento de lograr cambios radicales (ONU, 1987).

Durante la Conferencia Mundial de Derechos Humanos celebrada en Viena en el año 1993 se logró dar tanto a los derechos civiles y políticos como a los económicos, sociales y culturales, la misma categoría y exigibilidad, situación que permitió el desarrollo de Planes de Acción en esta materia (Conferencia Mundial De Derechos Humanos, Viena, 1993 | OHCHR, n.d.).

El 3 de junio del 2002 en Barbados, en la convención interamericana contra el terrorismo, “El gobierno del Ecuador deplora que los estados miembros no hayan podido llegar a un consenso sobre la tipificación del terrorismo y su clasificación como crimen internacional de lesa humanidad” (OEA, 2002).

El comité de los Derechos Humanos de Naciones Unidas mediante el Índice Universal de seguimiento universal monitorea las denuncias por violaciones de Derechos Humanos en cada uno de los países miembros, generando documentos y recomendaciones que sirven a su vez a otros organismos como la Corte Interamericana de Derechos Humanos que eventualmente sentencia en esta materia (Índice Universal de derechos Humanos UN, 2023).

El Código Orgánico Integral Penal ecuatoriano (COIP) establece en su “art. 366. al Terrorismo como “La persona que individualmente o formando asociaciones armadas provoque o mantenga en Estado de terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o pongan en peligro las edificaciones, medios de comunicación, transporte, valiéndose de medios capaces de causar estragos”.

Por otro lado, en el tema de Derechos humanos se destaca al Ecuador como el primer país del mundo en ratificar los 27 convenios internacionales que la Sección de Tratados de Naciones Unidas considera como de derechos humanos. (Cancillería EC, 2023).

Con estos antecedentes, se observa que el Ecuador entiende como prioritario el respeto a los Derechos Humanos ante las amenazas y riesgos existentes, para garantizar la defensa de la soberanía, la convivencia pacífica, los derechos humanos y de la naturaleza, y el Estado de derecho (Midena, 2018) (véase Tabla 3).

Tabla 3: Países que han elaborado planes de acción Derechos Humanos

Países que han elaborado planes de acción	
País	Fecha de elaboración
Bolivia	(1999) (2009-2013)
Brasil	(1996) (2009)
Colombia	Tenemos noticia de que ya se elaboró aun cuando no se encuentra registrado en la información de la Oficina de la Alta Comisionada.
Ecuador	(1998)
Guatemala	(2007-2017)
México	(1998) (2004-2006) (2008-2012)
Perú	(2006-2010)
Venezuela	(1997)

Nota. Obtenida de la Conferencia Mundial De Derechos Humanos, Viena, 1993 | OHCHR, n.d.

2.2.2. Los DD.HH, el D.I.H en el espectro del conflicto armado

El empleo del poder militar en la lucha contra el terrorismo requiere de la certeza. Los mandos del nivel táctico deben entender la complejidad que demanda este tipo de conflicto. En la Fig. 1 se ilustra el espectro del conflicto armado, que servirá para entender de mejor manera el tema.

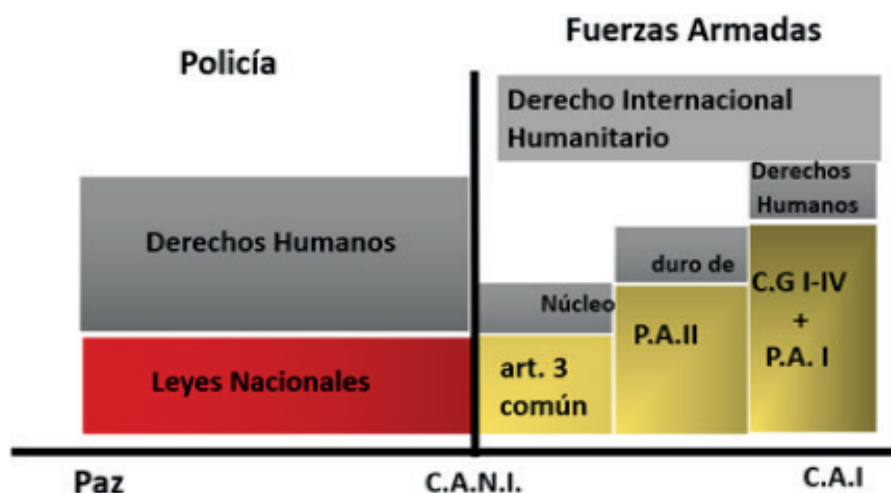
Partiendo desde una situación de paz, se puede observar que en la misma, los Derechos Humanos tienen gran preponderancia para garantizar el bienestar de la población en general, y además que la Policía Nacional tiene bajo su responsabilidad la seguridad pública.

En el Centro se observan las siglas C.A.N.I que corresponden a Conflicto Armado no Internacional o Inter-no; en este, el marco de acción mayoritario corresponde al Derecho internacional humanitario o Derecho

de los Conflictos Armados que constituye la legislación para normar el comportamiento de las partes que se enfrentan en el conflicto. Aquí, son las Fuerzas Armadas la Institución que tiene mayor responsabilidad.

En este tipo de conflicto se aplica al menos el artículo 3 que es común a los 4 convenios de Ginebra de 1949 y que están enfocados a preservar a la población civil que no participa del conflicto armado, asimismo, se puede ver que se hace referencia al “Núcleo duro de los Derechos Humanos” que está relacionado principalmente por el respeto a la vida del enemigo u oponente que entrega las armas y se rinde, de aquel que se encuentra herido y no presenta combate y de las personas que no son parte del conflicto (Salmon, 2004).

Figura 1: *El espectro del conflicto armado*



Nota. Basado en la Información CICR

Contrario a lo que se puede pensar, el D.I.H o Derecho de la Guerra no tiene como objetivo coartar el ímpetu que requiere una operación militar en el nivel táctico, por el contrario, busca dar legalidad al accionar militar, entender que las operaciones militares deben basarse en certezas dadas por la Inteligencia militar y que permitan levantar blancos lícitos que sean neutralizados empleando los medios y métodos de hacer la guerra permitidos, procurando causar el menor o ningún daño colateral. El respeto de la normativa existente da cuenta del profesionalismo de las Fuerzas Armadas y permite a sus miembros actuar sin dudar ante los escenarios complejos que en este tipo de conflicto se presentan.

Ciertamente, este tipo de conflicto armado es el de mayor complejidad debido a que generalmente las fuerzas legales del Estado se enfrentan a grupos armados organizados o grupos terroristas que carecen de ética, formación o respeto por dignidad humana. Los soldados deben estar conscientes de esta realidad y, sin embargo, debido precisamente a lo diferentes que son de estos grupos, es fundamental actuar con contundencia y profesionalismo.

Finalmente, al referirse a un Conflicto Armado Internacional (C.A.I), se observa que la aplicación del D.I.H en su integridad considerando los 4 convenios de Ginebra del 1949, los protocolos adicionales I y II de 1977 y el núcleo duro de los Derechos Humanos se mantiene, presentándose la enorme ventaja de enfrentar a Fuerzas Armadas profesionales que conocen de estas normas que marcan el comportamiento del soldado profesional durante la guerra.

2.3. Excesos en el uso de la fuerza, experiencias internacionales

La presente sección del estudio busca proveer al lector de un compendio de experiencias de otros Ejércitos, en las que no se observaron los preceptos de respeto a los Derechos Humanos y del Derecho Internacional Humanitario sin considerar que es fundamental durante las operaciones militares la aplicación del Principio de Distinción que permite al militar saber diferenciar a un objetivo lícito militar de otro que no lo es y que en ocasiones ha afectado a la población.

Para entender el ámbito legal que debió aplicarse en la mayoría de estas experiencias en la lucha contra el terrorismo, desde el empleo del poder militar dentro de su territorio, se debe recurrir al del Derecho Internacional Humanitario, y en particular, al artículo 3 común a los cuatro Convenios de Ginebra de 1949 en el que se determina al menos el respeto a la vida de las personas que no participan directamente del conflicto y las que hayan depuesto las armas o se encuentren heridas y fuera de combate, la toma de rehenes y la tortura.

2.3.1. Estados Unidos

Sin duda, en la historia americana han existido hitos que sirvieron de base para promover decisiones políticas para el uso del poder en el ámbito internacional, el más grave se da el 11 de septiembre de 2001, con el ataque terrorista a las torres gemelas y al Pentágono por parte de una organización terrorista denominada “Al Qaeda” y dirigida por Osama Bin Laden. En referencia a este suceso, se menciona constantemente que generó un cambio de era, un antes y un después en la historia universal. El mundo dejó de ser el mismo y a pocas horas de los espantosos atentados, George W. Bush dijo que Estados Unidos se encontraba en guerra con los terroristas internacionales. Así mismo, precisó que la respuesta sería “un ataque sin campos de batalla ni cabezas de puente” y que “el conflicto será largo” (Rashid, 2002).

El presidente Bush promulgó la autorización del Congreso para usar la fuerza militar contra los responsables de los ataques y apenas tres semanas después los Estados Unidos iniciaron sus operaciones en Afganistán. Las primeras semanas de campaña demostraron lo difícil que las cosas serían. A la vez que las fuerzas americanas y británicas destruían objetivos Talibanes y de Al Qaeda, ellos también golpeaban varias edificaciones civiles (Daadler & Lindsay, 2001).

Para marzo del 2003 la Guerra contra el terrorismo se extiende a Irak. Dentro del campo de los Derechos Humanos, aquí se producirá el caso conocido como Abu Ghraib, que trae repercusiones complejas a la política internacional americana y a sus Instituciones al publicarse fotos de abusos y torturas ejecutadas por el personal militar que controlaba la prisión donde estaban recluidos acusados de terrorismo, pertenecientes a Al Qaeda. (Informativo Pan árabe, 2003).

Las experiencias negativas de los Estados Unidos y sus Fuerzas Armadas, han servido para corregir constantemente y potenciar el entrenamiento y la capacitación de sus cuadros en temas de Derechos Humanos mediante capacitaciones a nivel mundial. Se hace una principal referencia al Instituto de cooperación para la seguridad hemisférica Whinsec que dicta para la región el curso de Instructores de Derechos Humanos.

2.3.2. México

México es actualmente el país de mayor incidencia del crimen organizado transnacional que tiene su base principal en el narcotráfico. Como centro de gravedad en el hemisferio ha recibido informes y recomendaciones por parte del Alto Comisionado de Naciones Unidas para los Derechos Humanos donde se destaca:

- En todas las zonas visitadas hay preocupación por la serie de eventos de violencia extrema enfrentada por indígenas, como resultado de disputas territoriales, falta de reconocimiento apropiado y la presencia del crimen organizado. Situación que empeora debido a factores como la impunidad y a un limitado acceso a la justicia.
- México vive una crisis de violencia e inseguridad con alarmantes índices de asesinatos, movimientos forzados y desapariciones. El caso de los 43 estudiantes de Ayotzinapa, Guerrero, quienes desaparecieron en septiembre del 2014 es particularmente emblemático, así como la masacre de 46 personas en Acteal - Chiapas en diciembre de 1997, donde se asesinó a 45 personas, principalmente mujeres y niños indígenas.

De acuerdo con la visita efectuada por el secretario de Naciones Unidas en 2015, se indica que la militarización de áreas como Guerrero, Chiapas y Chihuahua no ayudaron a reducir el nivel de violencia y considera que el problema de seguridad pública debe enfrentarse como un asunto civil diferenciando las políticas de acuerdo a las particularidades de cada zona específica (Índice Universal de Derechos Humanos UN, 2023).

Es la paradoja del narcotráfico: la debilidad del Estado y su incapacidad para controlar a sus propias fuerzas de seguridad permitieron que los cárteles prosperaran. Al mismo tiempo, uno de los recursos más valiosos que puede controlar un cártel es el acceso al poder del Estado y en particular a los cuerpos militares y de seguridad (Taub, 2023).

Con lo expuesto, se puede ver que la situación de México es compleja y marca una peligrosa tendencia del comportamiento criminal que se replica en muchos países de la región. La falta de educación y de oportunidades laborales en muchos sectores de su amplia geografía da cabida para que las actividades ilegales como el narcotráfico y crimen organizado transnacional se promuevan en la población como una alternativa para subsistir en medio de la violencia. Por otro lado, y ya desde la óptica militar, se puede señalar que presumiblemente ha dado un proceso de contaminación en su elemento armado donde ciertos elementos que en su momento pertenecieron a cuerpos élites, son hoy por hoy parte de cárteles y bandas (véase Figura 2).

Figura 2: México, un país que se desangra



Nota. Obtenida de Abel Gil Lobo, 2023 con datos del INEGI 2022. Citizen Council for Public Security and Criminal Justice (2023)

2.3.3. Perú

La violencia política transcurrida en Perú desde 1980 y 2000 dejó consigo, según la Comisión de la Verdad y la Reconciliación (2003), más de 69.000 muertes, de las cuales el 54% fueron atribuidas a Sendero Luminoso, el 37% a las Fuerzas Militares, el 7% a los comités de autodefensa y el 2% restante al Movimiento Revolucionario Túpac Amaru. (Ríos & García, 2019).

Charles Walker en su estudio, señala que de entre algunos grupos armados se destaca el accionar de dos grupos terroristas: el PCP-SL y el MRTA. El primero es conocido por sus ataques y genocidios. El segundo, que adoptó su nombre por el revolucionario peruano Tupac Amaru que posiblemente es el más conocido debido a la toma de rehenes en la residencia del embajador japonés de Lima desde el 17 de diciembre de 1996 hasta el 22 de abril de 1997 (Walker, 2015).

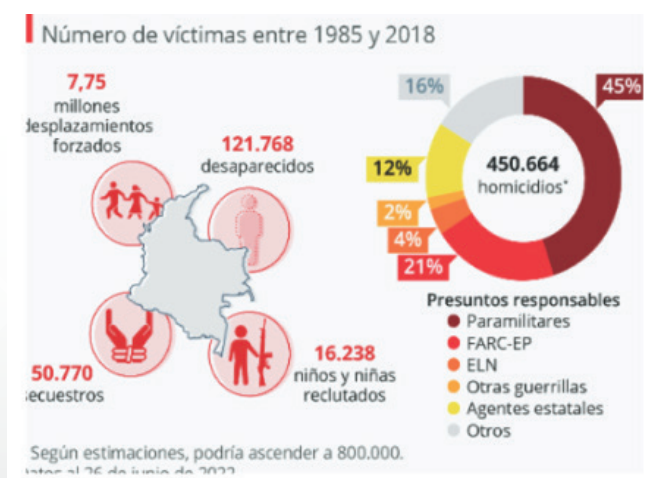
La Comisión de la Verdad y Reconciliación en el Perú y la perspectiva de género señala una constante agresión sexual a grupos de mujeres en sectores rurales “los casos de violencia sexual se presentaron durante los enfrentamientos entre actores, durante la captación de nuevos integrantes y en el marco de la vida cotidiana de la población”. En el mismo informe se hace referencia a varias denuncias de violaciones efectuadas por miembros de Fuerzas Armadas sin haber existido respuesta de parte de las autoridades públicas ni información respecto de procesos seguidos en contra de estos elementos (Mantilla, 2006).

Con estos antecedentes, se menciona una falta de acción del Estado al no haber presentado información del cumplimiento de sentencias referentes a reparaciones e indemnizaciones, tratamiento de traumas y otras formas de rehabilitación a las víctimas de tortura y malos tratos, asignación de recursos adecuados, etc. (UN Sanciones, 2023).

2.3.4. Colombia

Colombia es un país que ha vivido décadas de enfrentamientos internos con grupos armados organizados que causaron terror en buena parte del territorio con principal accionar desde 1985. Un estudio publicado por la Comisión de la Verdad conformada en el vecino del norte señala que se contabilizan hasta el 2018 un total de 450.664 homicidios y de considerar el subregistro podría llegar a 800.000. En lo que respecta a desapariciones forzadas, estas podrían llegar a 121.768, 50.770 secuestros y 4237 masacres (Comisión de la verdad Colombia, 2021) (véase Figura 3).

Figura 3: El saldo del conflicto armado en Colombia



Nota. Obtenida de la Comisión de la verdad Colombia.

Como es lógico pensar, dentro de un conflicto tan extenso y complicado existieron de forma aislada ciertos excesos. Las Fuerzas Armadas de Colombia y sus miembros han tenido que enfrentar un sinnúmero de procesos judiciales hasta la actualidad, quizá uno de los más emblemáticos y recientes constituye la imputación al señor general en retiro Mario Montoya el 30 de agosto del 2023 por la Jurisdicción Especial para la Paz (JEP) indicando:

“Por mentir sobre el número de bajas, encubrir casos de extralimitación del uso de la fuerza, presionar a los miembros de las unidades militares bajo su mando para obtener bajas “en combate”, emplear un lenguaje violento que exaltaba el derramamiento de sangre y ordenar que no se reportaran capturas por considerarlas resultados operacionales indeseados. La decisión, adoptada por la Sala de Reconocimiento de Verdad y de Responsabilidad, contra el excomandante del Ejército Nacional se da por 130 asesinatos y desapariciones forzadas cometidos cuando el oficial fue comandante de la IV Brigada, con sede en Medellín, entre el 2002 y el 2003.” (JEP, 2023).

A decir de Guerrero y Benavides, hablando del caso colombiano manifiestan que: “el paramilitarismo configuró una desnaturalización de la misión asignada a las Fuerzas Armadas. La lucha contra los grupos guerrilleros salió de control, produciéndose alianzas con grupos relacionados con el narcotráfico. A la par, Fuerzas Armadas y policía enfrentaron acusaciones por crímenes de lesa humanidad relacionados con falsos positivos, situación que ha generado un desprestigio para la institución armada” (Guerrero & Benavides, 2023, 110-121).

Debido a estos eventos el Ejército colombiano viene fortaleciendo sus procesos educativos mediante un proceso de transformación de su doctrina denominada “Damasco” misma que busca ser más efectiva en su lucha contra el terrorismo, fortaleciendo entre otros ámbitos, la enseñanza de los DD.HH. para su personal. El enfoque se centra en la aplicación de la seguridad humana que, como complemento de la seguridad tradicional, resulta una herramienta efectiva contra las amenazas emergentes en periodos complejos como el post acuerdo vigente en Colombia (Kaldor, 2010).

2.4. Las Instituciones Internacionales y el caso ecuatoriano

2.4.1. Instituciones Internacionales

El respeto a los Derechos Humanos de manera permanente, es una cuestión prioritaria y mantiene una relación directa con los niveles de desarrollo y educación de los pueblos en el mundo. En este sentido, organizaciones como Las Naciones Unidas, La Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos, son instancias hemisféricas encargadas de realizar observaciones, recomendaciones e inclusive sentencias que en suma pretenden tener un impacto directo en la política pública de los Estados miembros, así como en las instituciones que eventualmente pueden violentar la normativa en temas relacionados a los Derechos Humanos.

Dentro de la “Lucha contra el terrorismo respetando a los Derechos Humanos”, se ha planteado una estrategia mundial con anterioridad, siendo uno de los documentos más sobresalientes, el informe del secretario general de NN.UU. A/60/825 de abril del 2006 en el que se indica: “La adopción de medidas eficaces contra el terrorismo y la protección de los derechos humanos no son objetivos contrapuestos, sino complementarios y que se refuerzan mutuamente. Por consiguiente, la defensa de los derechos humanos es esencial para la realización de todos los aspectos de una estrategia contra el terrorismo” (Asamblea General ONU, 2006).

Para marzo del 2007 y con ocasión del primer aniversario del atentado de Atocha en que murieron o quedaron heridas más de 1600 personas inocentes, se expone una estrategia internacional basada en los siguientes

puntos específicos:

- Disuadir a la gente de recurrir al terrorismo y de apoyarlo
- Dificultar a los terroristas el acceso a los medios para llevar a cabo sus atentados
- Hacer que los estados desistan de prestar apoyo a los terroristas
- Desarrollar la capacidad de los estados para derrotar al terrorismo
- Defender los derechos humanos.

Estos pilares ciertamente constituyen un lineamiento general en base al cual se debe continuar trabajando políticas públicas en cada Estado y articulando un intercambio de información efectivo.

2.4.2. Discusión

El objetivo de la discusión es explicar al lector la relevancia y el significado de los resultados. Es el ilustrar las relaciones o conexiones entre lo que se ha observado. Debe responder a la pregunta: ¿Qué significan sus resultados? (Manterola Carlos, 2007).

En este apartado se realiza una interpretación de los resultados. Una buena forma de seguir este apartado es comparar los resultados obtenidos con los encontrados en la literatura. De acuerdo con Robert Day (Day, 2005), las características esenciales de una buena Discusión se darán si se observan los siguientes preceptos:

- Trate de presentar los principios, relaciones y generalizaciones que los Resultados indican. Tenga en cuenta que, en una buena Discusión, los resultados se exponen, no se recapitulan.
- Señale las excepciones o las faltas de correlación y delimite los aspectos no resueltos. No trate de ocultar o alterar los datos que no encajen bien.
- Exponga las consecuencias teóricas de su trabajo y sus posibles aplicaciones prácticas.
- Exponga las limitaciones de su estudio.

2.5. La historia de respeto a los Derechos Humanos de las FF.AA. en el Ecuador

A diferencia de lo vivido en otros países de la región, en el Ecuador, las Fuerzas Armadas tienen una gran ventaja para enfrentar la amenaza del terrorismo, su historia misma. No es difícil afirmar de manera categórica lo señalado, bastaría con revisar algunos casos emblemáticos en el trajinar histórico del Estado para asentar que ha existido un respeto permanente de los Derechos Humanos aún en condiciones de crisis extrema.

Al hacer referencia a “La Liga Militar”, que promovió la Revolución Juliana del 9 de julio de 1925 y dio paso a la primera Junta de Gobierno provisional que estuvo integrada por notables autoridades civiles que se sumaron al trabajo de los señores Generales Francisco Gómez de la Torre y Moisés Oliva, se puede notar que sus acciones se guiaron en el respeto a los derechos humanos, pues en su proclama manifiestan: “se inspirará en un espíritu verdaderamente democrático y tenderá al respeto de los derechos y libertades de todos los ciudadanos. Fundamento preciso de la libertad y la democracia, guardián y custodia de la soberanía, espina dorsal de la nacionalidad”. A través de esto, se da paso a una política de respeto y búsqueda de mejores días para la nación (Paz y Miño Cepeda, 2000).

También es justo rescatar la figura del Sr. General Enríquez Gallo quien entre 1935 y 1937, gobernó de forma pluralista, tolerante y apegada al respeto de los Derechos humanos sin aferrarse al poder. Con su gestión ejemplar logró estabilizar el país y restaurar la democracia; trabajó en la modernización de algunas instituciones, profesionalizó a la policía, replanteó la economía y las políticas monetarias del Banco Central e impulsó la legislación social (especialmente el Código del Trabajo y la ley de Cooperativas). Convocó, por último, a una Asamblea Constituyente a la que devolvió, en agosto de 1938, el mando del Estado (Fernández & Tamaro, 2004).

Recordar el comportamiento de las Fuerzas Armadas durante el gobierno militar del Sr. General Guillermo Rodríguez Lara entre los años 1972 y 1976, un período que a decir del historiador Dr. Enrique Ayala Mora, se caracterizó por un progresismo técnico en el que, a más de un respeto ejemplar en el manejo de los fondos públicos, se evidenció un nacionalismo sano que se apartó de las tendencias políticas extremas procurando la unidad nacional con un absoluto respeto a los derechos humanos y la búsqueda de alcanzar una compenetración de civiles y militares para alcanzar el desarrollo del Ecuador (Ayala Mora, 2023).

En la década de 1980 surge en el país un grupo armado denominado Alfaro Vive Carajo (AVC), que a decir del historiador venezolano Germán Carrera Damas, en su libro “El bolivarianismo-militarismo, una ideología de reemplazo”, publicado en 2017, asegura que la guerrilla AVC responde a un principio de imitación de las acciones del M19. Este grupo terrorista fue responsable del asesinato de 14 policías y el banquero Nahim Isaías Barquet, ejecutó una serie de secuestros, asaltos bancarios y la intrusión a la Embajada Británica en Quito, así como a varias estaciones de radio para publicar sus manifiestos dejando además muchos heridos civiles (Loayza, 2022).

Esta grave crisis vivida se puede sintetizar con las declaraciones del presidente Febres Cordero que indicó: “Me tocó enfrentar la desgracia del terrorismo, no se olvide que algunos ecuatorianos fueron secuestrados, algunos ecuatorianos murieron y que se mató por la espalda a policías. Para ellos no había derechos humanos. Cuando en la lucha armada entre las fuerzas del orden y la guerrilla, caía un guerrillero el escándalo era total, se habían violado los derechos humanos, pero cuando caía un policía ahí no pasaba nada. Pero me tocó ese difícil momento y lo enfrenté con la constitución y la ley en la mano. Fueron duros momentos, pero se salvó al país de ese cáncer” (Molina Flores, 2005).

El comportamiento profesional de las Fuerzas Armadas durante este episodio de la historia nacional nuevamente quedó de manifiesto. La cautela del Mando Militar, así como el sentido de pertenencia e identificación con su pueblo, han sido sin lugar a duda los elementos de peso que permiten a la Institución mantener niveles muy altos de aceptación, respeto y cariño por parte de la población.

III. Conclusiones

La Constitución Política del Estado Ecuatoriano, a decir de muchos, es demasiado “garantista”, lo cual impulsa al sistema penal a promover, proteger y tutelar, tal vez en forma desmedida, la doctrina de derechos humanos, lo que estaría bien hacerlo para los ciudadanos de bien, que son la mayoría; pero de la cual, se pueden acoger delincuentes y terroristas para beneficiarse inmerecidamente de las garantías expresadas en la Carta Magna.

Esta condición de Estado garantista también establece una pauta para extrapolar el concepto de protección de derechos hacia una “filosofía” de corrupción y cooptación pública, especialmente en la Fiscalía General

y la Función Judicial, entidades responsables de la investigación y aplicación de la normativa legal. De esta forma, se podría condicionar el accionar de las instituciones responsables de la seguridad, defensa y el orden público.

La cantidad de denuncias, abusos y sentencias por el irrespeto a los Derechos Humanos por parte de elementos militares en otros países de la región deben constituirse en un conjunto de falencias deontológicas que sirvan de casos de estudio puntuales a ser analizados con detalle para evitar su réplica durante el cumplimiento de operaciones militares de combate al terrorismo en el Ecuador.

Las Fuerzas Armadas del Ecuador se han caracterizado por ejecutar operaciones de manera profesional, respetando las leyes nacionales y los tratados internacionales. Esa fortaleza histórica evidenciada en los momentos de mayor tensión del Estado debe continuar, a fin de mantener el apoyo de su población durante los desafíos complejos que presenta el escenario actual de seguridad.

Referencias

- Asamblea General ONU. (2006, April 27). Asamblea General. Retrieved November 22, 2023, from <https://www.un.org/spanish/unitingagainstterrorism/a60825.pdf>
- Ayala Mora, E. (2023, noviembre 8). *Testimonio de vida y del nacionalismo revolucionario*.
- Cancillería EC. (2023, June 16). YouTube. Retrieved November 22, 2023, from <https://www.cancilleria.gob.ec/2020/12/08/ecuador-primer-pais-del-mundo-en-ratificar-los-27-tratados-de-naciones-unidas-sobre-derechos-humanos/>
- CIDH. (2023). ¿Qué es la Corte IDH? Corte Interamericana de Derechos Humanos.
- Comisión de la verdad Colombia. (2021).
- Conferencia Mundial de Derechos Humanos, Viena, 1993 | OHCHR. (n.d.). ohchr. Retrieved December 5, 2023, from <https://www.ohchr.org/es/about-us/history/vienna-declaration>
- Daadler, I., & Lindsay, J. (2001, Diciembre 1). Nasty, Brutish and Long: America's War on Terrorism | Brookings. Brookings Institution. Retrieved November 21, 2023, from <https://www.brookings.edu/articles/nasty-brutish-and-long-americas-war-on-terrorism/>
- Europe Council. (2021). *Guerra y terrorismo - Manual de Educación en los Derechos Humanos con jóvenes*. The Council of Europe. Retrieved December 8, 2023, from <https://www.coe.int/es/web/compass/war-and-terrorism>
- Fernández, T., & Tamaro, E. (2004, diciembre 1). Biografía de Alberto Enríquez Gallo. Biografías y Vidas .com. Retrieved January 20, 2024, from https://www.biografiasyvidas.com/biografia/e/enriquez_gallo.htm
- Fiscalía General del Estado. (2013, Enero). *Boletín Criminológico* (3a ed.). Santiago Argüello. Retrieved Noviembre 09, 2023, from <https://www.fiscalia.gob.ec/images/PerfilCriminologico/criminologico3.pdf>

- Guerrero, D., & Benavides, G. (2023, Abril 1). El Estado Ecuatoriano y el crimen organizado. *Academia de Guerra del Ejército Ecuatoriano*, 16(2023), 110-121.
- Haro Ayerve, P. (2017). *Fuerzas Armadas, pretorianismo y calidad de la democracia: Ecuador y Uruguay*. FLACSO Ecuador.
- Heisbourg, F. (2002). *Hiperterrorismo: la nueva guerra* (F. Heisbourg & M. d. Calonje, Trans.). Espasa Calpe, S.A.
- Índice Universal de Derechos Humanos UN. (2023). Índice Universal de Derechos Humanos. INDICE UNIVERSAL DE DERECHOS HUMANOS - Recomendaciones de Derecho Humanos. Retrieved November 22, 2023, from <https://uhri.ohchr.org/es/buscar-recomendaciones-de-derechos-humanos>
- JEP. (2023, August 30). JEP imputa crímenes de guerra y lesa humanidad al general (r) Mario Montoya y ocho militares más por 130 ‘falsos positivos’ en el oriente antioqueño. JEP. Retrieved December 6, 2023, from <https://www.jep.gov.co/Sala-de-Prensa/Paginas/jep-imputa-crmenes-de-guerra-y-lesa-humanidad-al-general-r-mario-montoya-y-ocho-militares-mas-por-130-falsos-positivos-en-.aspx>
- Kaldor, M. (2010). *El poder y la fuerza: La seguridad de la población civil en un mundo global* (A. E. Álvarez & A. M. Benítez, Trans.). Tusquets Editores.
- Loayza, Y. (2022, August 21). Auge y caída de Alfaro Vive Carajo, la guerrilla que aterrorizó Ecuador en los 80 con robos, secuestros y asesinatos. *Infobae*. Retrieved January 20, 2024, from <https://www.infobae.com/america/historia-america/2022/08/21/auge-y-caida-de-alfaro-vive-carajo-la-guerrilla-que-aterro-rizo-ecuador-en-los-80-con-robos-secuestros-y-asesinatos/>
- Mantilla, J. (2006). La Comisión de la Verdad y Reconciliación en el Perú y la perspectiva de género: principales logros y hallazgos*. Corte Interamericana de Derechos Humanos. Retrieved November 28, 2023, from <https://www.corteidh.or.cr/tablas/r08060-9.pdf>
- Midena. (2018). Untitled. Ministerio de Defensa Nacional. Retrieved December 11, 2023, from <https://www.defensa.gob.ec/wp-content/uploads/downloads/2023/04/Politica-de-Defensa-Nacional-Libro-Blanco-2018-web.pdf>
- Ministerio de Defensa Nacional. (2018). *Libro blanco* (1st ed., Vol. 1). Instituto Geográfico Militar.
- Molina Flores, A. (2005). *Democracia y militares: crisis y arbitraje: de Roldós a Palacios*. Editorial El Conejo.
- Morán, S., & Vaca, F. (2018, September 26). Derechos Humanos: las violaciones durante el gobierno de Rafael Correa. *Plan V*. Retrieved December 18, 2023, from <https://www.planv.com.ec/investigacion/investigacion/derechos-humanos-violaciones-durante-el-gobierno-rafael-correa>
- OEA. (2002, Junio 03). Ecuador. Retrieved November 22, 2023, from https://www.oas.org/xxxiiga/english/speeches/speech_ecuador.htm
- OEA. (2023). *Terrorismo. OAS :: Terrorismo*. Retrieved December 6, 2023, from <https://www.oas.org/es/temas/terrorismo.asp>
- Paz y Miño Cepeda, J. J. (2000). *La Revolución Juliana: nación, ejército y bancocracia*. Abya-Yala.

- Perfil de la institucionalidad social de Ecuador. (n.d.). Observatorio de Desarrollo Social en América Latina y el Caribe. Retrieved November 22, 2023, from <https://dds.cepal.org/bdips/pais.php?id=ec>
- Plan sectorial. (2021). *Plan sectorial de Defensa 2021-2025* (1st ed., Vol. 1). Dirección de Comunicación del Miden.
- Policía Nacional del Ecuador. (2017, Diciembre 10). La Policía de Ecuador, un referente de respeto a los Derechos Humanos. Policía Nacional del Ecuador. Retrieved November 17, 2023, from <https://www.policia.gob.ec/la-policia-de-ecuador-es-un-referente-de-respeto-a-los-derechos-humanos-en-la-region/>
- Política de Defensa. (2018). Política de Defensa. Política de Defensa. Retrieved December 8, 2023, from <https://www.defensa.gob.ec/wp-content/uploads/downloads/2023/04/Politica-de-Defensa-Nacional-Libro-Blanco-2018-web.pdf>
- Rashid, A. (2002). *El mundo después del 11 de septiembre de 2001* (Primera, febrero 2002 ed.). Ediciones Península.
- Registro oficial 449. (2008). Constitución de la República del Ecuador. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf
- Ríos, J., & García, M. (2019, julio 19). *El terrorismo de Estado en Perú: una mirada tras el fin de la violencia política*. AECPA. Retrieved January 21, 2024, from <https://aecpa.es/es-es/el-terrorismo-de-estado-en-peru-una-mirada-tras-el-fin-de-la-violenci/congress-papers/2916/>
- Salas, M. E. (2012, 03 28). Sin Derecho ni Razón. Sobre el garantismo penal de L. FERRAJOLI: su carencia de validez científica y de practicidad real. *Cuadernos de Filosofía del Derecho*, 35, 753. file:///C:/Users/hugo.cedeno/Downloads/sin-derecho-ni-razon-sobre-el-garantismo-penal-de-l-ferrajoli-su-ca-rencia-de-validez-cientifica-y-de-practicidad-real%20(2).pdf
- Salmon, E. (2004, abril). Introducción al Derecho Internacional Humanitario. Corte Interamericana de Derechos Humanos. Retrieved January 21, 2024, from <https://www.corteidh.or.cr/tablas/r25212.pdf>
- Seguridad Ciudadana y Derechos Humanos en el Ecuador: El Derechos penal en un Estado Garantista, un «deber ser» del nuevo Código Orgánico Integral Penal. – Inredh. (2016, October 26). Inredh. Retrieved December 13, 2023, from <https://inredh.org/seguridad-ciudadana-y-derechos-humanos-en-el-ecuador-el-derechos-penal-en-un-estado-garantista-un-deber-ser-del-nuevo-codigo-organico-integral-penal/>
- Taub, A. (2023, September 8). El narcotráfico floreció en México con ayuda del Estado. The New York Times. Retrieved December 7, 2023, from <https://www.nytimes.com/es/2023/09/08/espanol/mexico-narcotrafico.html>
- UN Sanciones. (2023). Sanciones | CONSEJO DE SEGURIDAD DE LA ONU. Retrieved November 23, 2023, from <https://www.un.org/securitycouncil/es/sanctions/information>
- Walker, C. (2015). *La rebelión de Tupac Amaru*, Lima, IEP. 377 pp. SciELO Perú. Retrieved November 28, 2023, from http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S0252-18652016000100010

Microrredes de Generación de Potencia Eléctrica para la Autosuficiencia de las Unidades Remotas de las Fuerzas Armadas

Electric Power Generation Microgrids for the Self-Sufficiency of Remote Units of the Armed Forces

Galo Guarderas Burbano

Departamento de Eléctrica, Electrónica y Telecomunicaciones, Universidad
de las Fuerzas Armadas – ESPE, 171103, Sangolquí, Ecuador.
gfguarderas@espe.edu.ec

Resumen

El presente artículo propone la aplicación de múltiples técnicas de generación de energía eléctrica para la implementación de un sistema combinado de fuentes de energía renovable (FER), con características como escalabilidad, eficiencia, sostenibilidad, resiliencia y amigabilidad con el medio ambiente, instaladas en unidades de frontera o unidades cuya localización dificulte la conexión con el sistema eléctrico nacional. Este concepto conocido como microrredes de generación de potencia eléctrica de corriente alterna, son sistemas que permiten aprovechar todos los medios existentes de generación eléctrica. En esta propuesta, se considera únicamente recursos renovables como sol, viento, agua, biomasa, etc., para generar y posteriormente controlar la distribución de la energía de manera óptima y eficiente. Desde el punto de vista militar, estas microrredes permiten optimizar el cumplimiento de las misiones asignadas, en especial, en unidades de frontera o instalaciones militares con déficit de potencia eléctrica. La propuesta se basa en unidades energéticamente autosuficientes existentes en todas las fuerzas armadas (FA) del mundo, cuyos sistemas de generación de potencia eléctrica (GPE), funcionan de forma autónoma, como navíos, aviones, unidades de ultramar o que, por su localización o función, se encuentran aisladas del sistema energético nacional. La orografía de nuestro país generalmente ofrece muchas ventajas para la GPE, lo que permite aprovechar los recursos naturales existentes para la generación de potencia eléctrica, la evaluación de las FER en lugares donde se han instalado destacamentos, repetidoras de telecomunicaciones, sistemas de vigilancia aérea y/o marítima, es imprescindible para la implementación de las microrredes.

Palabras clave: *Microrredes, generación de potencia eléctrica, instalaciones militares, aisladas, recursos renovables*

Abstract

The purpose of this article is to propose the application of multiple electric power generation techniques for the implementation of a combined system of renewable energy sources (RES), with characteristics such as scalability, efficiency, sustainability, resilience, and environmental friendliness, installed in frontier units or units whose location complicates the connection to the national electric system. This concept, known as alternating current electric power generation microgrids, is a system that allows for the utilization of all existing means of electric generation. In this proposal, we will consider only renewable resources, such as sunlight, wind, water, and biomass, for power generation and subsequently optimize and efficiently control the distribution of the generated power. From a military perspective, these microgrids enable the optimization of mission fulfillment, particularly in border units or military installations with power deficits. The proposal is based on energetically self-sufficient units that exist in all the Armed Forces (AF) of the world, whose electrical power generation systems (EPG) operate autonomously, such as ships, airplanes, and overseas units or those that, due to their location or function, are isolated from the national energy system. The orography of our country generally offers many advantages for the EPG, which allows taking advantage of the existing natural resources for the generation of electric power, the evaluation of the RES in places where detachments, telecommunications repeaters, aerial and/or maritime surveillance systems have been installed, is essential for the implementation of microgrids.

Keywords: *Microgrids, electric power generation, military installations, isolated, renewable resources.*



Fecha de Recepción: 25/10/2024 - Aceptado: 20/12/2024 – Publicado: 31/12/2024
ISSN: 2477-9253 – DOI: <http://dx.doi.org/10.24133/RCS.D.VOL09.N04.2024.03>

I. Introducción

Desde al menos 3 décadas el mundo ha observado el avance de las tecnologías de GPE, actualmente es evidente que estos sistemas son tendencia y tienen un futuro prometedor, el mundo consume aproximadamente 28.5 TW con una tasa de crecimiento promedio del 2.6%, de los cuales 3.8 TW son generadas mediante recursos renovables (IRENA, 2024). Por otro lado, la preocupación mundial por los efectos del calentamiento global obligan a pensar en alternativas para generar electricidad aprovechando recursos que sean amigables con el medio ambiente (UN, 2024).

Las operaciones militares exigen una gran cantidad de esfuerzo logístico, esto implica la optimización del mismo mediante el levantamiento de procesos, su programación y/o automatización si fuera posible, y el uso de recursos con el menor desperdicio posible, por lo tanto, obliga a explorar alternativas que permitan reducir la logística sin sacrificar las tareas a ser cumplidas en el cumplimiento de la misión en todo nivel. Si se plantea la discusión acerca de cuál es el recurso de mayor importancia en una operación militar, indiscutiblemente se concluiría que es la energía en cualquiera de sus formas. En esta propuesta se consideran dos casos de estudio, ambas en instalaciones militares remotas o destacamentos, cuya característica común es su localización en las fronteras del país o en lugares con accesos complicados. Están servidas por vías de transporte terrestre y fluviales, peligrosas y generalmente restringidas, limitando la cantidad y clase de soporte logístico a ser entregado, dejando a la vía aérea como único medio de transporte viable.

El primer caso, un hipotético destacamento en la frontera amazónica, cuyas características generales son que están cercanos a un curso de agua, tienen obviamente luz solar por 12 horas diarias, vientos con velocidades suficientes para generar energía por medio de mini turbinas eólicas, siempre limitados por la altura de la vegetación y mucha biomasa. El segundo caso, un destacamento hipotético localizado en la frontera sur con características ambientales similares a las mencionadas en el anterior caso, exceptuando el curso de agua (pveducation.org, 2024), (ingenieríaverde.org, 2024).

Considerando a estos hipotéticos destacamentos como unidades terrestres extremadamente remotas, lo óptimo deseable es que sean autosuficientes en todos los recursos posibles, bajo la premisa inicial, siendo el recurso energético la prioridad facilita la consecución de varios otros recursos importantes, de tal manera que, la implementación de sistemas de GPE son necesarios para lograr la meta propuesta, con el fin de que sean autosustentables y en consecuencia viabilizando todos sus recursos considerados en las misiones de un destacamento de frontera, incrementando su eficiencia, autogestión en telecomunicaciones y monitoreo en tiempo real de las instalaciones, otras como, bombeo y potabilización de agua para consumo y su tratamiento para el sistema hidrosanitario, iluminación y suministro de energía para sistemas de seguridad como cercas eléctricas, alarmas y otras que se puedan incrementar, por ejemplo, la dotación de canoas con motores eléctricos o la instalación de motores eléctricos en las canoas existentes, cuyas baterías podrían cargarse con esta potencia eléctrica generada propia, minimizaría o en el mejor de los casos solucionaría el inconveniente del transporte fluvial cuando no existe combustible, y a la vez estas baterías se convertirían en elementos emergentes de almacenamiento de energía.

Por otro lado, en lo que respecta a bienestar del personal, al tener la energía constante se podría implementar policlínicos con mejor atención, más y mejor equipados que garanticen funcionalidad a los profesionales médicos. De igual importancia es que el personal tenga tiempo de ocio de calidad con medios de entretenimiento y actividades culturales. Adicionalmente, es frecuente que las unidades militares en especial las que están alejadas de las ciudades, se convierten en focos de desarrollo humano, ya que pueden ofrecer entre otras cosas, seguridad, atención médica, educación y una alternativa para que los habitantes de dichas comunidades alejadas, tengan acceso a las modernidades de las urbes actuales en consecuencia a este fenómeno

social, se traduce en mayor presencia de personal civil o comuneros los cuales desarrollan sus actividades en las cercanías de las unidades y forman lazos fuertes entre la población civil y militar generando fronteras vivas garantizando la soberanía nacional.

Finalmente, pero no menos importante es que, la implementación y operación de estas microrredes que por principio son amigables con el medio ambiente dejan una huella de carbono mínima lo que beneficia a la imagen de la institución militar.

Este artículo está organizado en cinco secciones, I. Introducción, II. Microrred, se da una breve explicación conceptual de las redes de generadores distribuidos y sus métodos de control, III. Escenarios, donde se propone la implementación de las mismas en dos tipos de unidades remotas existentes en nuestras FA, IV. Presupuesto, una estimación aproximada, del costo de la implementación de estas infraestructuras, donde se consideran costos reales actuales de equipos, mas no de mano de obra, transporte y otros insumos, y V, finalizamos con conclusiones.

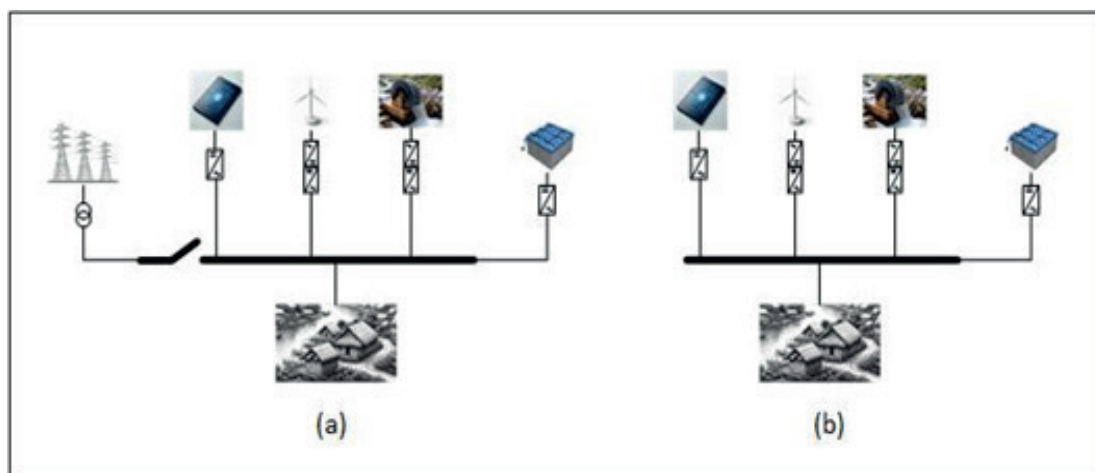
II. Materiales y Métodos

2.1. Microrred

Una microrred de GPE es un sistema compuesto por al menos una fuente de energía, en nuestro caso, renovable (FER): fotovoltaica, eólica, hídrica, etc., un sistema de almacenamiento de energía (SAE) que se compone de un banco de baterías con autonomía suficiente para cubrir parte o la totalidad de la potencia eléctrica requerida por la instalación. Regulador de carga, el cual es un elemento de control que mide, registra y monitorea los niveles de voltaje que tiene el banco de baterías y en función del cual, se activa o no, el ciclo de carga de las baterías. El controlador de la microrred, igualmente mide, registra y monitorea la generación del FER con el fin de optimizar la energía producida, el uso de la potencia eléctrica mediante una correcta distribución y equilibrio de cargas alimentadas por la microrred. Estas instalaciones pueden funcionar en dos modos: modo isla o aislado, es decir, sin conexión con la red eléctrica, también llamado “off-grid” y el modo conectado a la red u “on-grid”, ambos modos se ilustran en la Fig. 1. (a) y (b) respectivamente.

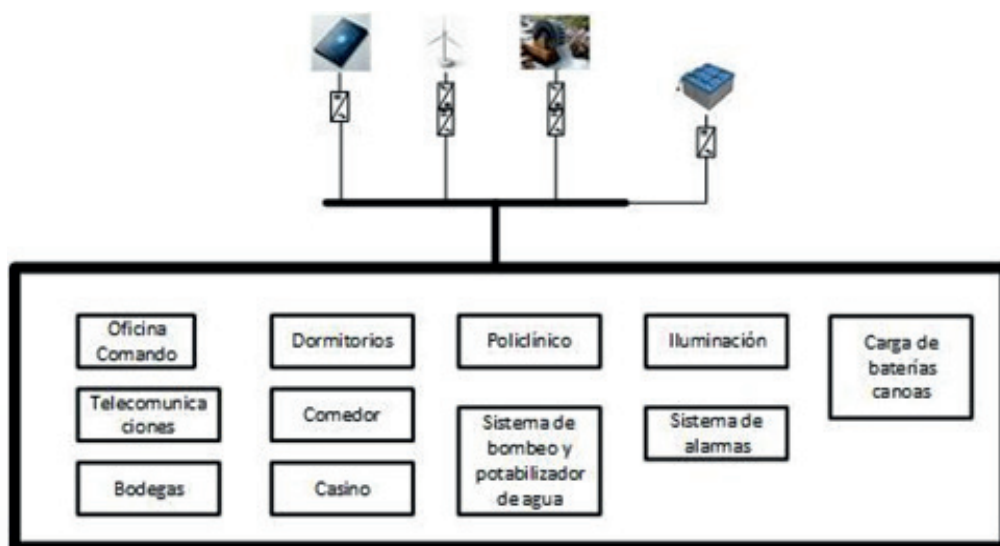
En nuestro caso se planteará una microrred en modo isla para alimentar al destacamento, esta deberá componerse por al menos dos FER y un SAE, pudiendo incrementarlas dependiendo de los recursos renovables primarios existentes en el sector y la necesidad o demanda del usuario. Existe una relación directa entre recursos energéticos renovables locales y la capacidad de generación de potencia eléctrica no interrumpida, no obstante, garantizar la condición de no interrumpida implica mayor gasto, ya que se debe evaluar alternativas como: analizar todos los recursos renovables existentes con potencial aprovechable, incrementar la autonomía del SAE y aunque no deseado pero necesario, observar la posibilidad de incluir un generador térmico a la microrred.

Figura 1: Modos de operación de las microrredes: (a) conectado a la red “on-grid”, (b) modo isla “off-grid”.



Las microrredes aisladas son sistemas de GPE independientes, cuyo sistema de control mantiene el voltaje y frecuencia nominal en los valores requeridos y dentro de sus tolerancias, niveles que podrían variar por varios factores, en especial por la capacidad nominal de cada generador y de su generación instantánea dependiente del comportamiento aleatorio de los recursos renovables locales aprovechables. Por otro lado, aunque en forma general la carga en un destacamento es constante, eventualmente podría variar en más o menos, por lo que, la necesidad de potencia eléctrica también variará; normalmente la tendencia es que la carga aumente, por lo tanto, la microrred deberá tener la capacidad de crecer, aplicando en el concepto de escalabilidad del sistema. La Fig. 2 ilustra una microrred tipo estándar que podría instalarse en los destacamentos, tomando en cuenta su estructura básica.

Figura 2: Microrred estándar en un destacamento militar



Cabe mencionar que los destacamentos actualmente carecen de varios elementos descritos en la Fig. 2., por lo tanto, existirán variaciones en sus estructuras, esta propuesta toma en cuenta elementos básicos o mínimos que un destacamento debería tener para su óptimo desempeño.

Respecto a la distribución de potencia eléctrica, el diseño deberá considerar una clasificación de cargas en función de la prioridad en el funcionamiento del destacamento estas cargas deberán ser: eventuales, normales y críticas.

Cargas eventuales son los dispositivos eléctricos que se alimentan y activan por momentos determinados, por ejemplo: maquinaria eléctrica, la misma que se alimentará y encenderá solo en ciertas condiciones u horarios y bajo el criterio del comandante. Cargas normales son las que deben estar alimentadas siempre, pero son encendidas en función de la necesidad del usuario, por ejemplo, iluminación en áreas comunales, dormitorios, etc. Finalmente, cargas críticas, las mismas que deberán estar siempre alimentadas y encendidas, es decir que, en caso de emergencia o carencia de potencia eléctrica, estas cargas serán prioritarias y solo serán desconectadas con orden del comandante bajo prelación, por ejemplo, los equipos de telecomunicaciones y otros vitales en caso de existir, como podría ser un sistema de iluminación y alarmas perimetrales.

2.2. Escenarios

Esta propuesta plantea una hipotética unidad militar remota localizada en frontera, la misma que, por su localización es muy complejo acceder a ella, este factor obliga a que dicha instalación sea autosustentable en todos los recursos posibles, maximizando su eficiencia y minimizando el esfuerzo logístico de servidumbre de la unidad. Desde este punto de vista, la implementación de una microrred se convierte en una inversión y resuelve en gran medida el problema de eficiencia energética planteada, logrando autosuficiencia energética y alivio en el esfuerzo logístico. Actualmente los destacamentos son dotados como fuente de potencia eléctrica con un generador térmico, el mismo que quema combustibles fósiles, diésel o gasolina, los mismos que deben ser transportados periódicamente hacia las mencionadas unidades. Para entender mejor el problema de autoconsumo se lo plantea como una analogía, con las características mencionadas ante la unidad terrestre, llámese destacamento o unidad de frontera; localizada en lugares remotos se la puede considerar como un navío, es decir, que debe generar su propia potencia eléctrica para energizar su carga total, esto supone que en algún momento deberá cubrir o alimentar a la carga total del destacamento y administrar la generación y el consumo de forma inteligente.

Suponiendo que la mencionada unidad consuma 500 Wh de energía, se plantean dos escenarios en función de la orografía del país. El primer escenario es que esté localizada en la región amazónica, donde como recursos energéticos renovables locales aprovechables son la energía fotovoltaica, considerando un promedio de irradiancia de 4,5 kW/m² (INGENIERIAVERDE.ORG, 2024).

El biogás producto de la descomposición de la materia orgánica o biomasa, la cual es abundante en la región y no supone un problema de suministro de materia prima, es correcto pensar que su potencial de generación sobrepasa la necesidad de potencia eléctrica de la unidad en estudio, teniendo en cuenta que en promedio se puede producir 0.3 m³ de biogás por kg de materia vegetal (UBA, 2024).

En lo referente al potencial hidráulico, la mayoría de las unidades de oriente están situadas a orillas de un curso de agua, esto permite el uso de generadores pico hidráulicos, estos sistemas tienen turbinas cuya característica es que no necesitan ríos caudalosos o caídas de agua para generar la suficiente potencia eléctrica, lógicamente, si existieran cualquiera de los dos factores anotados serían de mayor utilidad, el caudal promedio necesario para que una pico turbina genere energía eléctrica es de 0.05 m³/s, pudiendo ser menor si existe una caída de agua y del tipo de turbina que se utilice, los pequeños ríos en la amazonia ecuatoriana en general tienen caudales promedio que sobrepasan con holgura el caudal anotado (WORLDBANK.ORG, 2020).

En lo que se refiere a la generación eólica, a pesar de ciertos criterios en contra, es igualmente muy aprovechable, el uso de mini turbinas eólicas funcionando como un arreglo podrían generar una importante cantidad de potencia eléctrica, en este caso puntual, tomando en cuenta potencias de las mini turbinas de 10 kW, sería suficiente. El inconveniente con esta técnica de generación en la región amazónica son los altos árboles existentes, siendo la tala no recomendada, se podría utilizar ciertas infraestructuras tipo puente sobre los ríos, donde se coloquen arreglos de mini turbinas eólicas, las cuales puedan generar la potencia eléctrica suficiente, la Fig. 3, ilustra la estructura planteada (INSPENET, 2024).

Figura 3: Estructura de un arreglo de mini turbina eólicas



El segundo escenario que se configura es un destacamento en las fronteras norte o sur, o en cualquier otro lugar remoto del país, sea continental o en las islas Galápagos, donde pueden ser aprovechadas todas las tecnologías de generación, inclusive podría incrementarse la generación mareomotriz para la región costa y Galápagos. En este segundo escenario, el pico hidráulico es poco probable de ser aplicado, ya que los destacamentos en estas regiones no tienen ríos cercanos, no obstante, donde los hubiera deberán ser considerados.

Con base en los dos escenarios descritos, supondremos ahora una microrred típica, es decir, una que conste con al menos un FER y obligadamente el SAE, el control de la microrred en este caso no es complejo, ya que, al tener un solo generador, su inversor regula la frecuencia y el voltaje a ser entregado a las cargas, además un controlador de nivel de voltaje de las baterías, mediante el cual se discrimina si es o no necesario iniciar el ciclo de carga de las mismas. No obstante, este enfoque sencillo no cumple con el objetivo de implementar una microrred conceptualmente hablando, para ello es necesario que, al menos dos FER y el SAE interactúen en el sistema de generación, por lo tanto, el control se torna más complejo, debiendo utilizarse técnicas de control como las de formación de red o “grid forming” (Guarderas, 2017), (Rocabert, 2012), (Zeineldin, 2006), donde la FER más estable, marca y controla la frecuencia y el nivel de voltaje de la red mediante su inversor.

La estabilidad estimada de los FER se define mediante un análisis extenso e histórico de las condiciones ambientales del sector, pues estas determinan el comportamiento de cada uno de ellos, no obstante, al ser el recurso hídrico el más constante, la generación hídrica es la más estable. En el caso que no estuviere disponible, se deberá definir otra FER que manifieste un comportamiento que estadísticamente refleje mayor estabilidad, con el fin de que sea la referencia de la microrred.

Por otro lado, se debe considerar la potencia eléctrica que genera cada FER en un ciclo de tiempo determinado, es aconsejable obtener y registrar los datos del comportamiento de los FER durante el lapso de un año,

tiempo en que se considera que todas las condiciones climáticas han variado en el transcurso del mismo, y por lo tanto, se tiene un conocimiento más certero del comportamiento de los generadores.

Con estos factores definidos y teniendo una estimación más certera de la capacidad de potencia que puede generar realmente cada FER, se implementa un algoritmo de control con el que se selecciona o prioriza cuál o cuáles de los generadores entrega la potencia eléctrica para su distribución y uso, y cuál se encarga de mantener al SAE siempre alimentado para efectos de carga de sus baterías en función de su ciclo de carga. Este proceso de monitoreo y selección se ejecuta periódicamente, ya que los sensores climáticos revelarán cambios en las condiciones climáticas del sector en relación con la época del año seca o lluviosa, usualmente la FER que alimenta el banco de baterías es la que menos potencia produce, pero suficiente para cumplir el cometido de la carga, el resto de generadores con mayor potencia eléctrica producida alimentan las cargas.

III. Evaluación de resultados

3.1. Presupuesto

Se mencionó antes que el costo de una microrred depende de los resultados del análisis de los recursos primarios renovables existentes en la zona, para luego seleccionar cuál de ellos son los que tienen mayor potencial aprovechable, seguidamente, el dimensionamiento y diseño que determina la potencia pico hora en condiciones estándar de laboratorio a ser instalada, y en consecuencia, la potencia nominal de sistema de generación. El paso a seguir es la selección de equipos adecuados para la implementación de la microrred. La Tabla 1 muestra el presupuesto estimado.

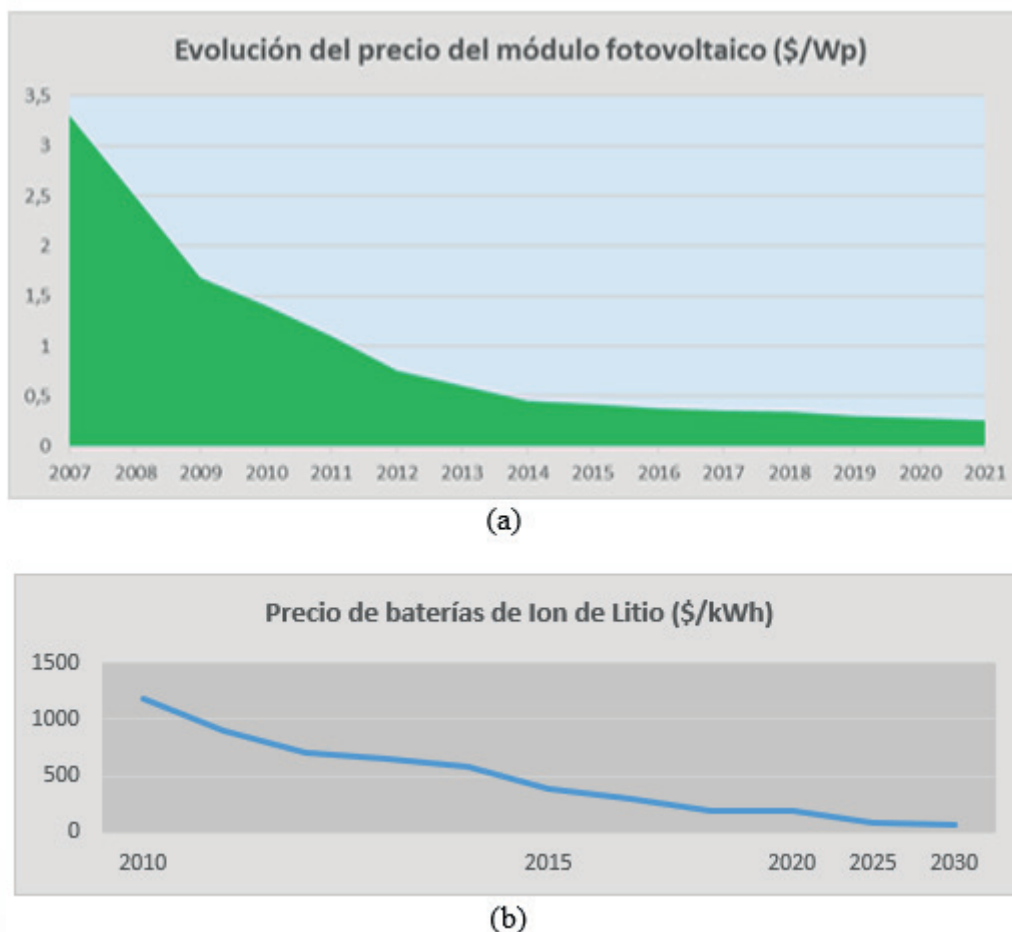
Tabla 1: “Presupuesto estimado de una microrred en ambos escenarios”

ESCENARIO 1				
Una sola FER				
Tipo de FER	Potencia kW	Costo FER \$	Presupuesto* \$	
Solar	10	8000	1	19500
Eólico	10	20000	2	31500
SAE	10	7500		
Instalación*	1	3000		
Transporte*	1	1000		
ESCENARIO 2				
Varias FER				
Solar	10	8000	1	29500
Eólico	10	20000	2	39500
Picohidro	10	10000	3	44500
Biogas	10	15000		
SAE	10	7500		
Instalación*	1	3000		
Transporte*	1	1000		
* valores variables y estimados				

Tomando en cuenta los dos escenarios, se podría definir un costo aproximado de la infraestructura propuesta. La tabla 1 muestra el presupuesto por escenario para generadores de hasta 10 kW. Considerando el primer escenario, un FER más el SAE, y que los valores son aproximados y variables, el precio de una microrred podría variar de entre USD 19.500 a USD 31.500, y para el segundo escenario el precio variaría desde USD 29.500 hasta USD 44.500. Cabe mencionar aquí que actualmente la tendencia en el precio de las baterías, paneles y otros equipos de generación mediante renovables están a la baja, por lo que este presupuesto también variaría a la baja. La Fig. 4 muestra la tendencia del precio de los paneles y baterías en los últimos años.

La implementación de este tipo de infraestructura ha demostrado ampliamente que el funcionamiento y operatividad de las unidades militares son mejoradas, las ventajas son evidentes que inclusive se han instalado microrredes en unidades que no necesariamente están lejanas y tienen conexión con una red principal, es decir, que trabajan en modo conectado a la red “on grid”, lo que permite tener sistemas de potencia ininterrumpidos.

Figura 4: Tendencia mundial del precio (a) paneles solares, (b) baterías.



Las Fuerzas Armadas, con mayores y mejores sistemas logísticos, han comprobado que el tener operando estas microrredes permite que las actividades de estas unidades nunca se interrumpan, incrementa la resiliencia de la unidad en todos sus aspectos funcionales y operativos (MICROGRIDLEDGE, 2024), (MICROGRIDLEDGE, 2023).

La implementación de las microrredes en unidades remotas o alejadas incrementaría su potencial operativo, la resiliencia y entre otras ventajas reforzaría la relación con las poblaciones adyacentes, lo cual agrega

valor a estas infraestructuras y cumple objetivos en la tarea del apoyo al desarrollo que persiguen las F. A. generando potencia eléctrica, con el fin de suministrarla a las pequeñas aldeas cercanas.

Por otro lado, el ahorro en el esfuerzo logístico se convierte en liberación de recursos para ser invertidos en otros fines, lo cual permite mejorar en el bienestar del personal y mantenimiento de equipos y maquinarias.

Finalmente, las microrredes son bastante robustas, son un sistema de generadores de potencia eléctrica basados en recursos renovables, por lo tanto, son recursos ilimitados; cuando uno de ellos es escaso, otro será el que genere la potencia adecuada, configurando una estructura con respaldo y redundancia, sin embargo, existe la posibilidad de una “tormenta perfecta”, donde por alguna razón, ninguna de estas fuentes de energía renovable genere a su mínima capacidad, en ese caso, se deberá mantener como reserva un sistema térmico en perfectas condiciones funcionales con capacidad de alimentar como mínimo las cargas críticas y la carga del SAE.

Adicionalmente, y considerados como una reserva extra útil para casos extremos, el uso de baterías que no son parte del SAE, pero alientan a motores eléctricos, por ejemplo, en unidades de oriente, donde la principal vía de transporte es la fluvial, se cambiaría los motores a combustión de las canoas por motores eléctricos, los cuales son alimentados por baterías, estas pueden ser utilizadas también como fuente de potencia eléctrica de emergencia para alimentar las cargas críticas, esto obliga a seguir estrictamente un plan de mantenimiento de carga de las mencionadas baterías, complementado con una doctrina de uso de los generadores de energía de emergencia.

IV. Conclusiones

Los destacamentos militares por su naturaleza sufren de escasez de recursos y son muy dependientes del sistema logístico de las fuerzas armadas, por lo que es muy común que por las condiciones climáticas o daños en los transportes la servidumbre logística a estas instalaciones se interrumpa, poniendo en condiciones vulnerables el cumplimiento de la misión impuesta.

Es un hecho comprobado en otras fuerzas armadas que el implementar estas microrredes en destacamentos los convierte en unidades autosuficientes, con energía disponible suficiente, se facilita el desarrollo de actividades paralelas como la agricultura implementando pequeños huertos, crianza de animales, y permite y facilita la conservación de alimentos.

Por otro lado, operativamente, se minimiza el riesgo del fallo en los sistemas de telecomunicación, de hecho, los robustece, permitiendo monitoreo en tiempo real del destacamento por parte del escalón superior. Así como también la implementación de sistemas de apoyo en la seguridad de las instalaciones.

La administración de la potencia generada será responsabilidad del sistema de control mediante un algoritmo de control, el mismo que podrá ser gestionado por personal entrenado y supervisado por el comandante del destacamento con base a políticas dadas por el escalón superior.

Finalmente, y como se inició mencionando en este artículo, lo más importante en una operación militar es el recurso energético, sin combustible no se mueve la maquinaria, haciendo una analogía con las guerras de siglos pasados, “un ejército marcha sobre sus estómagos”, en la actualidad no ha cambiado el sentido de esta frase pensada por Napoleón, por lo tanto, los actuales ejércitos para cumplir exitosamente su misión, necesitan muchos y más recursos, entre ellos el más importante es la energía, sea eléctrica, mecánica, química,

etc. En este caso, la generación de potencia eléctrica es vital para mantener unidades remotas en condiciones óptimas para cumplir su misión, convirtiéndolas en autónomas en muchos aspectos y ahorrando en mucho el esfuerzo logístico necesario.

Referencias

- González, L. P., Morales, L. F. C., & Gaspar, G. (2019). PRODUCCIÓN DE BIOGÁS: Fundamentos y parámetros. <https://doi.org/10.19136/book.191>
- Guarderas, G., Frances, A., Asensi, R., & Uceda, J. (2017). Large-signal blackbox behavioral modeling of grid-supporting power converters in ac microgrids. 2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA), 153–158.
- Ingenieria Verde. (s. f.). https://ingenieriaverde.org/wpcontent/uploads/2020/01/Mapa_Solar_del_Ecuador_2019.pdf
- Ingenieria Verde. (s. f.). chrome-extension://efaidnbmninnibpcapjpcglclefindmkaj/https://ingenieriaverde.org/wp-content/uploads/2020/01/Mapa_Solar_del_Ecuador_2019.pdf
- INSPENET. (s. f.). <https://inspenet.com/articulo/mini-turbinas-eolicas-solucion-energetica/> Mini Turbinas Eólicas Portátiles como Solución Energética (inspenet.com)
- IRENA. (2024). Renewable energy statistics 2024. International Renewable Energy Agency, Abu Dhabi. <https://www.irena.org/>
- J. Rocabert, A. Luna, F. Blaabjerg, & P. Rodríguez. (2012). Control of power converters in ac microgrids. IEEE Transactions on Power Electronics, 27(11), 4734–4749.
- MICROGRIDKNOWLEDGE. <https://www.microgridknowledge.com/sponsored/article/55137509/revolutionizing-defense-the-crucial-role-of-microgrids-and-schneider-electric-in-department-of-defense-energy-resiliency>
- MICROGRIDKNOWLEDGE. <https://www.microgridknowledge.com/military-microgrids/article/33013118/construction-begins-on-us-armys-latest-microgrid-at-fort-campbell-ky>
- PVEDucation. (s. f.). <https://www.pveducation.org/es/fotovoltaica/2-propiedades-de-la-luz-del-sol/promedio-de-la-radiaci%C3%B3n-solar>
- United Nations. (s. f.). Cambio climático | Naciones Unidas. <https://www.un.org/es/global-issues/climate-change>
- WORLDBANK. (s. f.). <https://collaboration.worldbank.org> ASL Factsheet Amazonia Ecuador 1123.pdf (worldbank.org)
- Zeineldin, H. H., El-Saadany, E. F., & Salama, M. M. A. (2006). Distributed generation micro-grid operation: Control and protection. 2006 Power Systems Conference: Advanced Metering, Protection, Control, Communication, and Distributed Resources, 105–111.

Mochila de Operaciones Tácticas S&M (M.O.T. S&M) a implementarse en el Ejército Ecuatoriano

S&M Operational Tactical Backpack (M.O.T. S&M) to be used by the Ecuadorian Army

Juan Sebastián Sánchez Obando, Gonzalo Viterbo Martínez Abarca, Gilberth Jaime Llerena Martínez

Universidad de Fuerzas Armadas - ESPE, Av. Progreso S.N, Ecuador

juanhenry_11@hotmail.com, esnade1980@hotmail.com, gilberth.llerena@educacion.gob.ec

Resumen

En este trabajo se identificaron problemas que afectan al personal militar y se plantearon soluciones a través del diseño de la Mochila de Operaciones Tácticas S&M. Esta mochila se enfoca en proporcionar una herramienta versátil y segura, utilizando materiales, accesorios y tecnología que faciliten su uso, con el objetivo de minimizar los riesgos en operaciones especiales, operaciones aerotransportadas, cruce de ríos organizados y operaciones fluviales. En los últimos años, nuestro personal militar ha sufrido accidentes fortuitos en diversas actividades, tanto en operaciones reales como en instrucción y/o entrenamiento, debido a las exigencias físicas de sus tareas profesionales. Las mochilas tácticas ofrecen mayor seguridad, comodidad y ergonomía en comparación con las mochilas tradicionales o de dotación vigente.

Palabras Claves: *Mochila táctica de extracción, equipo táctico militar, innovaciones en mochilas militares.*

Abstract

In this study, we identified problems affecting military personnel and proposed solutions through the design of the S&M Tactical Operations Backpack. This backpack aims to provide a versatile and safe tool, utilizing materials, accessories, and technology to facilitate its use and minimize risks in special operations, airborne operations, organized river crossings, and riverine operations. In recent years, our military personnel have suffered accidental injuries in various activities, both in real operations and during instruction and/or training, due to the physical demands of their professional tasks. Tactical backpacks offer greater security, comfort, and ergonomics compared to traditional or standard-issue backpacks.

Keywords: *Tactical extraction backpack, military tactical gear, innovations in military backpacks.*



Fecha de Recepción: 03/11/2024 - Aceptado: 20/12/2024 – Publicado: 31/12/2024
ISSN: 2477-9253 – DOI: <http://dx.doi.org/10.24133/RCS.D.VOL09.N04.2024.04>

I. Introducción

Dentro del eje de defensa de las Operaciones Especiales se observan hechos palpables que vulneran la seguridad del Estado, tanto dentro como fuera del Límite Político Internacional. Los sectores geográficos que corresponden a los cauces de los ríos San Miguel, Guapí, Mataje y Putumayo, rutas fluviales navegables, han presentado numerosas irregularidades. Estas se deben a la presencia de Grupos Armados Organizados (GAO) que realizan actividades ilícitas, usando los mencionados ríos como principales vías de abastecimiento y transporte. Estas áreas están bajo la responsabilidad de diversas unidades militares acantonadas en la región oriental del Ecuador.

Por lo anteriormente expuesto, es fructífero y necesario utilizar la Mochila de Operaciones Tácticas S&M, debido a sus características y adaptaciones en diseño y fabricación, considerando las siguientes particularidades:

- La mochila permite impermeabilizar las prendas militares de manera ordenada y segura en operaciones especiales.
- Facilita la técnica de infiltración y ex filtración en zonas pedestres o de difícil acceso gracias al arnés táctico incorporado.
- Durante el cruce de ríos o aguas profundas, el airbag se activará rápidamente en caso de algún percance involuntario (como ahogamiento).

Actualmente, las mochilas en dotación han cumplido su vida útil. Se han detectado problemas en diversas misiones realizadas por los soldados ecuatorianos, ya que estas prendas de intendencia presentan características incómodas para su funcionalidad, con materiales deteriorados y provocando discomfort (incomodidad y malestar) intenso en el personal durante sus patrullajes. Además, los accesorios de las mochilas se rompen, y en muchos casos, los implementos personales terminan perdidos.

La implementación de medidas de control para posibles problemas detectados en los equipos de intendencia de nuestra institución es crucial. La “Mochila de Operaciones Tácticas” S&M está acorde a las nuevas tecnologías, con un diseño ergonómico, versátil, duradero, de gran capacidad de carga, con compartimientos organizados y hecha de material ligero y resistente. Su implementación es usada por las Fuerzas Armadas estadounidenses para crear espacios de almacenamiento en chalecos y mochilas, con las siguientes características: a. Compartimiento o bolsa seca (chaquísca balsa). b. Arnés táctico. c. Airbag (chaleco salvavidas). d. Mochila táctica.

II. Materiales y Métodos

El presente estudio, sustentado en la experiencia del soldado ecuatoriano, permitió la adecuación de implementos que mejoran la utilidad de la mochila en dotación, con la finalidad de maximizar la operatividad de las tropas en operaciones militares, minimizando los riesgos que estas conllevan.

En la investigación se emplearon los siguientes métodos: cualitativo y cuantitativo. El método cualitativo se basó en entrevistas, observaciones y análisis de contenidos para comprender las características, beneficios y limitaciones de la mochila táctica. Estos enfoques son considerados pioneros en el estudio de la ergonomía, con importantes aportes a la organización científica del trabajo, conocidos como taylorismo en honor

a Frederick W. Taylor (Gilbreth, 2014). La Tabla No. 1 lista el nivel de aceptación o indecisión del personal de señores oficiales, voluntarios y aspirantes. Así mismo, la Figura 1 muestra que apenas el 10.81% fueron indecisos:

Tabla 1: Listado del nivel de aceptación o indecisión del personal de señores oficiales, voluntarios, y aspirantes

ORD.	GRADO	ACEPTACIÓN	INDECISO
1	Oficiales	07	01
2	Voluntarios	35	05
3	Aspirantes	32	02
Total		74	8

Figura 1: Gráfica de aceptación



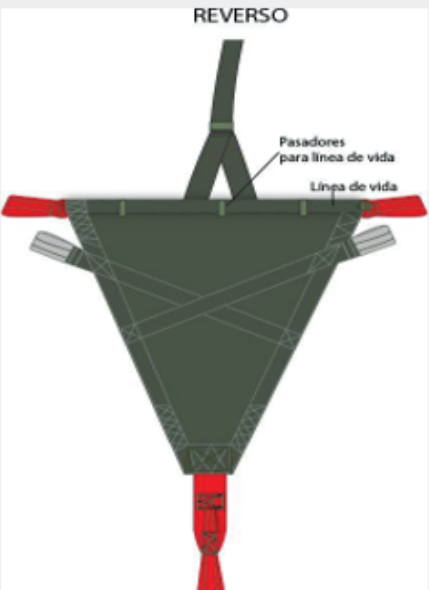
El síndrome de dolor lumbar (SDL) es un trastorno musculoesquelético (TME) altamente prevalente. Se estima que el 80% de la población adulta experimenta al menos un episodio de SDL que impacta su funcionalidad, afectando principalmente a trabajadores sometidos a manejo manual de carga (MMC), siendo esta una importante causa de ausentismo laboral en las empresas. De ahí la necesidad de proponer herramientas evaluativas de detección temprana (sopergo, dolores lumbares). En la primera fase se realizó un levantamiento de información sobre las expectativas del personal de la EIWIAS, que manipulará la mochila en futuras misiones dispuestas por el Escalón Superior.

El método cuantitativo permitirá medir encuestas y realizar análisis estadísticos para evaluar la eficacia, comodidad y seguridad de la mochila táctica. El investigador en estadística y análisis de datos ha aplicado métodos cuantitativos para evaluar la eficacia de las mochilas (Meza-Ortiz, 2022).

Estructuralmente, el proyecto aborda el análisis de trabajar digitalmente sobre el espacio tridimensional corporal y estudia las respuestas originadas experimentalmente tras el proceso de traslado del patrón a un cuerpo mediante el estudio antropométrico de una imagen mapeada. La investigación se centra en el estudio del contexto actual, ante las nuevas tipologías de consumo, conectadas en el presente escenario cultural y socioeconómico (Calero, 2016).

Los instrumentos utilizados para que el personal militar conozca los beneficios de la mochila táctica de extracción en las operaciones tácticas y administrativas se probaron en la provincia de Napo, cantón Misahuallí, río del sector y el aeropuerto Jumandy, y la comprobación del arnés táctico se llevó a cabo por el XVI curso de Maestro de Salto. La Tabla No. 2 muestra los accesorios de la mochila.

Tabla 1: Accesorios de la M.O.T. S&M.

Nombre del accesorio	Uso y/ empleo	
		BOLSA SECA 
Bolsa seca.	Compartimientos o bolsa seca (chaquisca bulsa). El objetivo de estas bolsas es guardar, impermeabilizar y distribuir de manera ordenada las prendas militares, mejorando la manipulación del equipo de intendencia. Estas bolsas vienen en diferentes tamaños y presentan características impermeables, hechas de material plástico resistente.	
		ANVERSO ARNÉS  REVERSO 
Arnés táctico	Arnés táctico. El objetivo del arnés táctico es permitir operaciones aerotransportadas de infiltración o exfiltración, para las cuales se necesita un equipo y material especial que facilite el anclado y transporte mediante una aeronave. Surgió la necesidad de acondicionar el arnés de extracción táctico (A.E.T), que es confortable, dinámico, anti caídas, de sujeción y suspensión, incorporado en la mochila táctica de combate para priorizar el tiempo y la seguridad.	

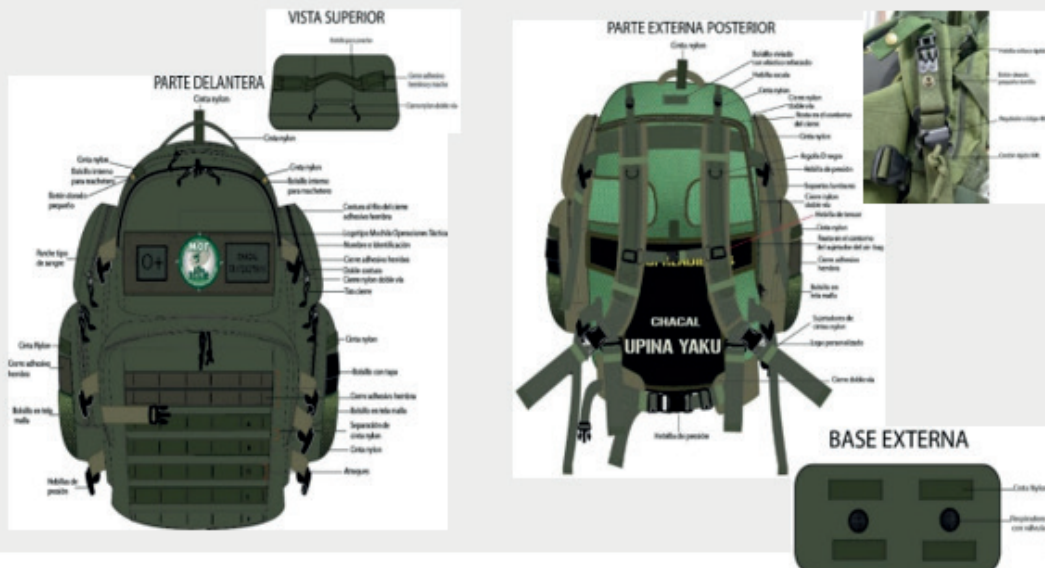
Nota: Además, es el único arnés en el mercado que tiene incorporada la línea de vida, que consiste en una cinta de 50 a 90 cm fijada en la cintura para aumentar la seguridad en la extracción.



Airbag

Airbag (chaleco salvavidas). El objetivo del airbag es proporcionar seguridad en operaciones de navegación fluvial o acuáticas, consideradas de alto riesgo. Estas operaciones han presentado desgracias involuntarias durante el cruce organizado de ríos en aguas profundas, debido a diversas causas, como negligencia o contracción involuntaria y repentina de uno o más músculos (calambres), que generalmente se presenta en las piernas. Es necesario que la mochila posea el accesorio de airbag, con fácil manejo operativo (chaleco salvavidas). Aprobado para personas de 16 años y más de 80 libras.

Nota: Se acopla en la parte del cinturón de la mochila, y es removable.



Mochila táctica

Mochila táctica. Las mochilas nos sirven para transportar cargas pesadas durante largos periodos de tiempo, ya que los hombros soportan mejor el peso que las manos. Consideramos que es un producto sustitutivo porque una mochila convencional (dotación vigente) puede satisfacer en parte el servicio que ofrece la mochila de operaciones tácticas. Estas deben ser confeccionadas con tejidos de alta resistencia para poder soportar el uso intensivo.

Por lo expuesto, se realizaron adaptaciones a la mochila de combate tradicional, mejorando su impermeabilidad, confort, seguridad y manejo rápido en caso de extracciones e infiltraciones aerotransportadas y cruce de ríos. Las adaptaciones realizadas, como el arnés táctico, las bolsas impermeables y el airbag, permitieron maximizar la operatividad de las tropas.

Finalmente, la modernización e innovación son herramientas necesarias para mejorar la operatividad del Ejército Ecuatoriano. Por esta razón, es importante mejorar el equipo en dotación basado en la experiencia e investigación, realizando adaptaciones que contribuyan a la tecnificación y mejora del equipo de apoyo en las operaciones administrativas y tácticas.

El Instituto Nacional de Higiene y Seguridad en el Trabajo (Ruiz, 2011) plantea recomendaciones sobre las malas posturas, manipulación de cargas y condición física en personas no entrenadas con un peso hasta 20 kg y personas entrenadas hasta 40 kg. Estas consideraciones permiten que en esta propuesta se estandaricen procedimientos que ayuden a emplear de mejor manera a nuestro personal antes de cualquier actividad, considerando el tipo de somatotipo y las categorías en las que se clasificaría al personal para la entrega en dotación de una mochila táctica. Estas consideraciones deben tomarse en cuenta para su correcto uso en diferentes actividades.

Finalmente, la modernización e innovación son herramientas necesarias para mejorar la operatividad del Ejército Ecuatoriano. Por esta razón, es importante progresar el equipo en dotación basado en la experiencia e investigación, realizando adaptaciones que contribuyan a la tecnificación y mejora del equipo de apoyo en las operaciones administrativas y tácticas.

III. Evaluación de Resultados y Discusión

3.1. Bolsa seca (chaquisca bulsa)

Los compartimentos de impermeabilidad de la mochila M.O.T. S&M, denominados bolsa seca dieron un resultado óptimo. Se realizó un ejercicio con el personal de instructores del comité de navegación fluvial de la Escuela de Iwias en el sector de instrucción de la parroquia Misahualli, en el río del mismo nombre. Determinamos una impermeabilidad del 100%, ya que, durante la inmersión en las aguas del mencionado río, las prendas no se mojaron. Además, estos compartimentos también sirven como un medio de flotación.

3.2. Arnés táctico

Se realizó una comprobación con el XIV curso de Maestro de Salto, utilizando un fardo con resistencia de 145 kg y un paracaídas modificado para lanzar abastecimientos desde una aeronave en vuelo a sitios de difícil acceso. Se realizó desde una altura de 1200 pies, con un maniquí de instrucción de 100 kg de peso, verificando la resistencia del arnés táctico incorporado a la mochila M.T.E.

3.3. Airbag

En las pruebas de campo llevadas a cabo para la comprobación del airbag con el personal de instructores del comité de navegación fluvial de la Escuela de IWIAS en el sector de instrucción de la parroquia Misahuallí, en el río del sector, se realizó la práctica del airbag con el personal militar profesional (sin equipo) de aproximadamente 80 kg, estableciendo que es un medio de flotación.

3.4. Discusión

La modernización e innovación son herramientas necesarias para mejorar la operatividad del Ejército ecuatoriano. Es crucial mejorar el equipo en dotación basado en la experiencia e investigación, realizando adaptaciones que contribuyan a la tecnificación y mejora del equipo de apoyo en las operaciones administrativas y tácticas.

Por lo tanto, se realizaron adaptaciones a la mochila de combate tradicional, mejorando su impermeabilidad, confort, seguridad y manejo rápido en caso de extracciones e infiltraciones aerotransportadas y cruce de ríos. Las adaptaciones realizadas, como el arnés táctico, las bolsas impermeables y el airbag, permitieron maximizar la operatividad de las tropas.

Las comprobaciones llevadas a cabo por el comité de navegación fluvial sobre el uso del airbag y las bolsas secas tuvieron gran acogida y aceptación. Asimismo, la comprobación del arnés táctico, realizada por el XVI curso de Maestro de Salto, fue exitosa.

Sin embargo, la Mochila de Operaciones Tácticas (M.O.T. S&M) (Zonatáctica) presenta desafíos. Puede ser pesada, lo que puede afectar la movilidad y velocidad del soldado, y además, puede ser costosa, especialmente si se busca una de alta calidad.

IV. Conclusiones y Trabajo futuro

La investigación sobre la Mochila de Operaciones Tácticas (M.O.T. S&M) ha demostrado que es un equipo esencial para militares, policías y otros profesionales que requieren una gran cantidad de equipo y recursos en el campo táctico. A través de la revisión de la literatura y el análisis de los resultados, se han identificado las siguientes conclusiones:

- Las adaptaciones realizadas a la actual mochila de dotación han permitido mejorar significativamente la utilidad, seguridad y confort. El arnés táctico con su línea de vida incorporada permite una evacuación rápida en operaciones aerotransportadas en caso de requerirlo.
- Las bolsas secas facilitan la clasificación e impermeabilidad de las prendas militares a transportar.

- El airbag incorporado permite una flotación rápida y minimiza el riesgo en operaciones fluviales.
- Además, el costo de producción es bajo y el margen de utilidad amplio.
- Con la argumentación teórica expuesta, se concluye que esta investigación permitió conocer los beneficios que brinda la Mochila de Operaciones Tácticas (M.O.T. S&M) en los diferentes escenarios en los cuales fue comprobada. Es importante recomendar seguir investigando sobre materiales avanzados y diseños modulares para mejorar la eficacia y comodidad de la mochila táctica.

Reconocimientos (Acknowledgment)

Los autores agradecen a la Dirección de Transformación y Desarrollo Militar de la Fuerza Terrestre por la invitación para participar en el concurso de Ingenios Militares, obteniendo el segundo lugar en el Ámbito Logístico. Agradecemos a la Universidad de las Fuerzas Armadas ESPE y a la Escuela de IWIAS “Crnl. Gonzalo Barragán” por las facilidades proporcionadas. Agradecemos también a la empresa FAME S.A., que diseñó y fabricó el prototipo de la Mochila de Operaciones Tácticas (M.O.T. S&M). Agradecemos sinceramente a mi Subp CB Miguel Cunalata Chango por su colaboración técnica en la elaboración de este trabajo.

Referencias

- Calero, A. B. (2016). El futuro de la moda, nuevos modelos de mapeado. <https://riunet.upv.es/bitstream/handle/10251/62176/BONILLO%20-%20BODYMAP.%20El%20futuro%20de%20la%20moda,%20nuevos%20modelos%20de%20mapeado%20corporal%20aplicados%20a%20sistemas%20....pdf;-jsessionid=59C450B4ADAB99C3920309D9D2E10B9A?sequence=1>
- Gilbreth, L. M. (12 de 2014). EL MÉTODO DE LA INVESTIGACIÓN. <https://www.bbc.com/mundo/noticias-48964115#:~:text=Gilbreth%20y%20Moller%20son%20vistos,en%20honor%20a%20Frederick%20W.>
- Ruiz, L. (2011). *Manipulación manual de cargas guía técnica del INSHT*. INSHT, Instituto Nacional de Seguridad e Higiene en el Trabajo, 30.
- Meza-Ortiz, R.-A. (2022.). TECHNOLOGY IN ERGONOMICS. STATE OF THE ART AND BIBLIOMETRIC ANALYSIS. TECHNOLOGY IN ERGONOMICS. STATE OF THE ART AND BIBLIOMETRIC ANALYSIS. <https://revista-dyna.com/dyna-management/index.php/dyna-management/article/view/41/36>.
- Zonatactica (s.f.). Mejores Mochilas Tácticas del Mercado. Obtenido de Mejores Mochilas Tácticas del Mercado: <https://www.zonatactica.es/68-mochilas-tacticas>

Simulación de Ciberataques a Servicios Web en Entornos Controlados: Un Enfoque Seguro para la Evaluación de Vulnerabilidades

Simulation of Cyberattacks on Web Services in Controlled Environments: A Secure Approach to Vulnerability Assessment

Andrés Sebastián Almeida, Alison Paola Moncayo, Darwin Roberto Valdiviezo

Universidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador.

{asalmeida4, apmoncayo2, drvaldiviezo2}@espe.edu.ec.

Resumen

El aumento de ataques dirigidos a sistemas web ha generado una creciente preocupación en el ámbito de la seguridad informática, lo que ha impulsado la necesidad de investigar sus impactos en entornos controlados. Este artículo evalúa una aplicación web con vulnerabilidades ante diferentes ataques comunes, con la finalidad de evidenciar fallas en la seguridad del sistema y proponer soluciones para prevenirlas. Para lograrlo, se utilizó OWASP (Open Web Application Security Project) Juice Shop, una aplicación desarrollada por el proyecto OWASP, una comunidad internacional que promueve prácticas para mejorar la seguridad del software. Juice Shop permite realizar pruebas en un entorno diseñado para simular fallas comunes. Se evaluaron distintas vulnerabilidades, incluidos la inyección SQL, escaneo de puertos, ejecución de scripts maliciosos (XSS), carga de archivos maliciosos, recorrido por directorios y falsificación de peticiones en sitios cruzados (CSRF). Dichas simulaciones se ejecutaron en Kali Linux, dentro de una máquina virtual en VirtualBox sobre un host en Windows 11, utilizando Docker para desplegar el entorno web. Además, se utilizó Burp Suite como herramienta para interceptar solicitudes, modificar parámetros y explotar las fallas detectadas. Los ataques XSS demostraron la ejecución de código malicioso, lo que expuso debilidades en el filtrado de entradas. Sin embargo, la aplicación fue capaz de resistir los ataques de recorrido de directorios y carga de archivos maliciosos. Para hacer frente a la amenaza de ciberataques, este estudio subraya la importancia de incorporar poderosas medidas de ciberseguridad en el desarrollo de servicios web, más allá de las consideraciones típicas.

Palabras clave: *Ciberseguridad, Vulnerabilidades, Servicios Web, Entornos Virtualizados, Inyección SQL.*

Abstract

The increase in attacks targeting web systems has generated growing concern in the field of computer security, driving the need to investigate their impacts in controlled environments. This article assesses a web application vulnerable to various common attacks to identify security flaws in the system and propose solutions to mitigate them. To achieve this, we utilized the OWASP (Open Web Application Security Project) Juice Shop, an application developed by the OWASP project. This international community promotes best practices to enhance software security. Juice Shop allows testing in an environment designed to simulate common flaws. Various vulnerabilities were evaluated, including SQL injection, port scanning, cross-site scripting (XSS), malicious file upload, directory traversal, and cross-site request forgery (CSRF). These simulations were run on Kali Linux, within a VirtualBox virtual machine on a Windows 11 host, using Docker to deploy the web environment. Also, Burp Suite was used as a tool to intercept requests, modify parameters, and exploit the detected flaws. XSS attacks demonstrated the execution of malicious code, exposing weaknesses in input filtering. However, the application was able to withstand directory traversal and malicious file upload attacks. To address the threat of cyberattacks, this study emphasizes the importance of incorporating robust cybersecurity measures into web service development, extending beyond typical considerations.

Keywords: *Cybersecurity, Vulnerabilities, Web Services, Virtualized Environments, SQL Injection.*



Fecha de Recepción: 05/09/2024 - Aceptado: 20/12/2024 - Publicado: 31/12/2024
ISSN: 2477-9253 – DOI: <http://dx.doi.org/10.24133/RCS.D.VOL09.N04.2024.05>

I. Introducción

A medida que el Internet y sus aplicaciones web se expanden en alcance, complejidad y uso diario, la ciberseguridad se ha convertido en una de las principales prioridades debido al aumento de ataques que afectan la integridad, y en algunos casos la disponibilidad de los sistemas. Según Ukwandu et al. (2020), los ataques cibernéticos en la actualidad pueden causar desde robos de datos hasta el colapso de servicios web. La prueba simulada en un entorno controlado ha surgido como una herramienta efectiva para poder analizar las vulnerabilidades y buscar estrategias que ayuden a prevenirlas (Straub, 2020; Gorgone Carvajal, 2023). Esto subraya la importancia de adoptar medidas proactivas para reforzar la seguridad de los servicios web y la infraestructura subyacente, además, estas prácticas permiten estudiar ataques comunes como escaneo de puertos, inyección SQL y XSS, replicando escenarios reales sin poner en riesgo sistemas productivos (Fuertes Díaz & Macas Carrasco, 2023).

En Ecuador, los ciberataques han aumentado en los últimos años, afectando tanto al sector público como privado. Echeverría et al. (2020) reportan más de 40 millones de intentos de intrusión en solo una semana, lo que evidencia una alarmante vulnerabilidad. Estudios locales demostraron que los usuarios, especialmente los millennials, carecen de conciencia suficiente sobre la ciberseguridad, lo cual hace que estén en primera fila ante riesgos de ataques de spoofing o sniffing (Augusto & Agudelo, 2018; Anu & Vimala, 2018).

Este estudio tiene como objetivo analizar las vulnerabilidades que puede presentar un servicio web, entre ellas, el análisis de puertos abiertos, inyección SQL, ejecución de scripts (XSS), carga de archivos, recorrido por directorios y falsificación de peticiones en sitios cruzados (CSRF). Con ello se busca evidenciar que los servicios web no deben centrarse únicamente en el desarrollo funcional, sino también incorporar consideraciones de ciberseguridad. La simulación se ha realizado en un entorno controlado, con el fin de evitar afectaciones reales que puedan implicar consecuencias éticas o legales.

El resto del artículo se organiza de la siguiente manera: el apartado 2 presenta los trabajos relacionados a partir de los cuales se establecieron bases y pruebas similares para la detección de vulnerabilidades web. El apartado 3 describe los materiales y métodos empleados en cada una de las simulaciones. En el apartado 4 se analizan las formas de mitigación de cada ataque, junto con los resultados obtenidos a través de un análisis estadístico descriptivo, basado en la tasa de éxito, el tiempo de ejecución y la severidad (CVSS) de los ataques simulados. Finalmente, el apartado 5 expone las conclusiones del estudio y propone posibles líneas de trabajo futuro.

II. Trabajos relacionados

El estudio de ciberseguridad en aplicaciones web cuenta con una amplia trayectoria, con numerosas investigaciones que emplean entornos controlados para corroborar vulnerabilidades habituales. En esta sección, se revisan investigaciones relacionadas a las vulnerabilidades analizadas en OWASP Juice Shop.

El uso de aplicaciones con vulnerabilidades incorporadas ha sido documentado en diversos estudios como una estrategia para la enseñanza de ciberseguridad. Vega-Oyola et al. (2022) analizaron entornos controlados orientados a la formación en ciberseguridad, observando mejoras en la capacidad de los estudiantes universitarios para identificar vulnerabilidades. Por otro lado, Son (2016) propuso un marco estructurado para la implementación de laboratorios virtuales que permiten prácticas en ciberseguridad dentro de contextos académicos, sin implicar riesgos legales.

De igual manera, las técnicas de inyección SQL han experimentado cambios en los últimos años. Sadegh & Tajalli (2013) analizaron patrones de inyección y técnicas de evasión en aplicaciones actuales, indicando que incluso sistemas con medidas básicas continúan siendo susceptibles a este tipo de ataques. Veeraburden y Bekaroo (2022), por su parte, realizaron un estudio comparativo de herramientas automatizadas para la detección de vulnerabilidades de inyección SQL, señalando que las tasas de detección varían según el contexto de implementación de los sistemas.

En la actualidad, las vulnerabilidades de Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF) continúan presentes como vectores de ataque en aplicaciones web. Lekies et al. (2023) documentaron la evolución de los ataques XSS en entornos JavaScript, identificando nuevos vectores que superan mecanismos de protección convencionales. En cuanto a CSRF, Barth et al. (2021) propusieron un enfoque de defensa en profundidad que integra el uso de tokens, encabezados personalizados y validación de origen, observando una reducción de vulnerabilidades en entornos de prueba controlados.

Durumeric et al. (2020) llevaron a cabo un estudio a gran escala acerca de la exposición de servicios en Internet, revelando que aproximadamente el 15% de los servidores web exponen servicios innecesarios, los cuales podrían ser aprovechados por atacantes cibernéticos.

Rafique et al. (2019) analizaron cómo los atacantes combinan diferentes vulnerabilidades para lograr la ejecución de código remoto mediante archivos maliciosos. Este estudio complementa nuestra investigación, donde se encontró que OWASP Juice Shop implementa controles efectivos contra estos ataques específicos.

Bau et al. (2021) establecieron un marco sistemático para evaluar la seguridad de aplicaciones web modernas, abordando tanto vulnerabilidades técnicas como problemas de configuración que se suelen pasar por alto.

Estudios recientes también han explorado nuevos paradigmas en seguridad web, como el de Ahmadi (2023), donde se analizaron los desafíos de seguridad específicos de las aplicaciones web progresivas (PWA) y las arquitecturas serverless, identificando nuevos vectores de ataque exclusivos para estas tecnologías. Por otro lado, Vighe (2024) estudió cómo la adopción e implementación de DevSecOps influye en la seguridad de las aplicaciones web, encontrando correlaciones positivas entre la integración temprana de pruebas de seguridad y la reducción de vulnerabilidades en entornos de producción.

Estos estudios han permitido contextualizar la presente investigación, la cual facilita una evaluación práctica y detallada de múltiples vectores de ataque en un sistema realista pero controlado.

III. Materiales y métodos

Antes de definir las herramientas y técnicas empleadas, se plantearon las siguientes preguntas de investigación, alineadas con los objetivos del estudio:

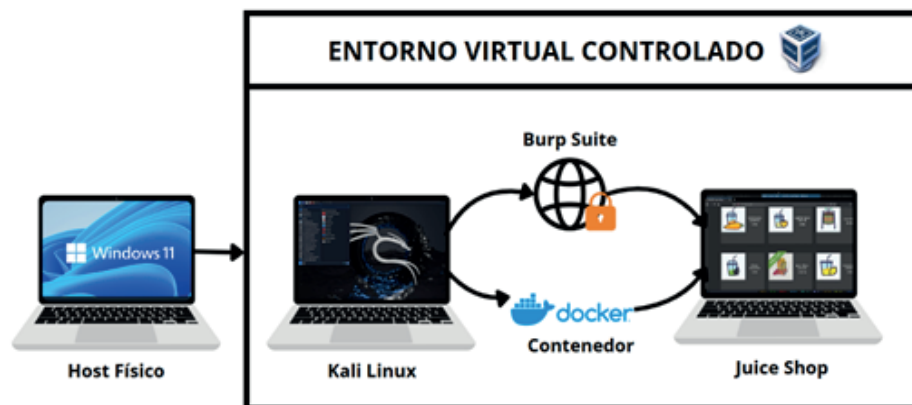
- RQ1: ¿Cuáles de las vulnerabilidades web más comunes pueden ser explotadas con éxito en un entorno controlado utilizando OWASP Juice Shop?
- RQ2: ¿Qué niveles de gravedad (Common Vulnerability Scoring System, CVSS) y tiempos de ejecución presentan los diferentes ataques realizados contra la aplicación vulnerable?

- RQ3: ¿Qué métricas operativas clave se pueden obtener al realizar pruebas de penetración sobre una aplicación web desplegada en Docker, y qué indican sobre su seguridad y desempeño?

La topología propuesta para la simulación contempla una máquina virtual que opera sobre un host físico con sistema operativo Windows 11, en el cual se utiliza VirtualBox. Dentro de esta máquina virtual está instalado Kali Linux, el cual cuenta con Docker y Burp Suite. Docker aloja la aplicación utilizada para vulnerar OWASP Juice Shop, mientras que Burp Suite se encarga de interceptar, modificar y reenviar solicitudes HTTP/HTTPS con el fin de ejecutar distintos vectores de ataque. La comunicación se realiza a través de una red virtual privada (Network Address Translation, NAT), lo que garantiza un entorno aislado y seguro. La estructura completa de este entorno se muestra en la Figura 1.

La arquitectura empleada en el sistema se basa en el despliegue de OWASP Juice Shop dentro de un contenedor Docker, ejecutado en un entorno virtual Kali Linux. Inicialmente, se instalan Docker y sus dependencias mediante comandos dentro de Kali, y posteriormente se ejecuta la imagen correspondiente de Juice Shop. Esta imagen contiene todos los componentes necesarios para ejecutar la aplicación, incluyendo Node.js y el framework Express. El sistema se ejecuta en el puerto 3000, lo que permite su acceso desde el navegador. Además, el contenedor mantiene una conexión interna con la base de datos del sistema, donde se almacena la información de usuarios y productos. Por esa razón, esta arquitectura nos proporciona un entorno seguro y sobre todo controlado, con el que podemos realizar las pruebas de vulnerabilidad sin infringir leyes ni exponer datos de personas reales.

Figura 1: Topología utilizada en la simulación

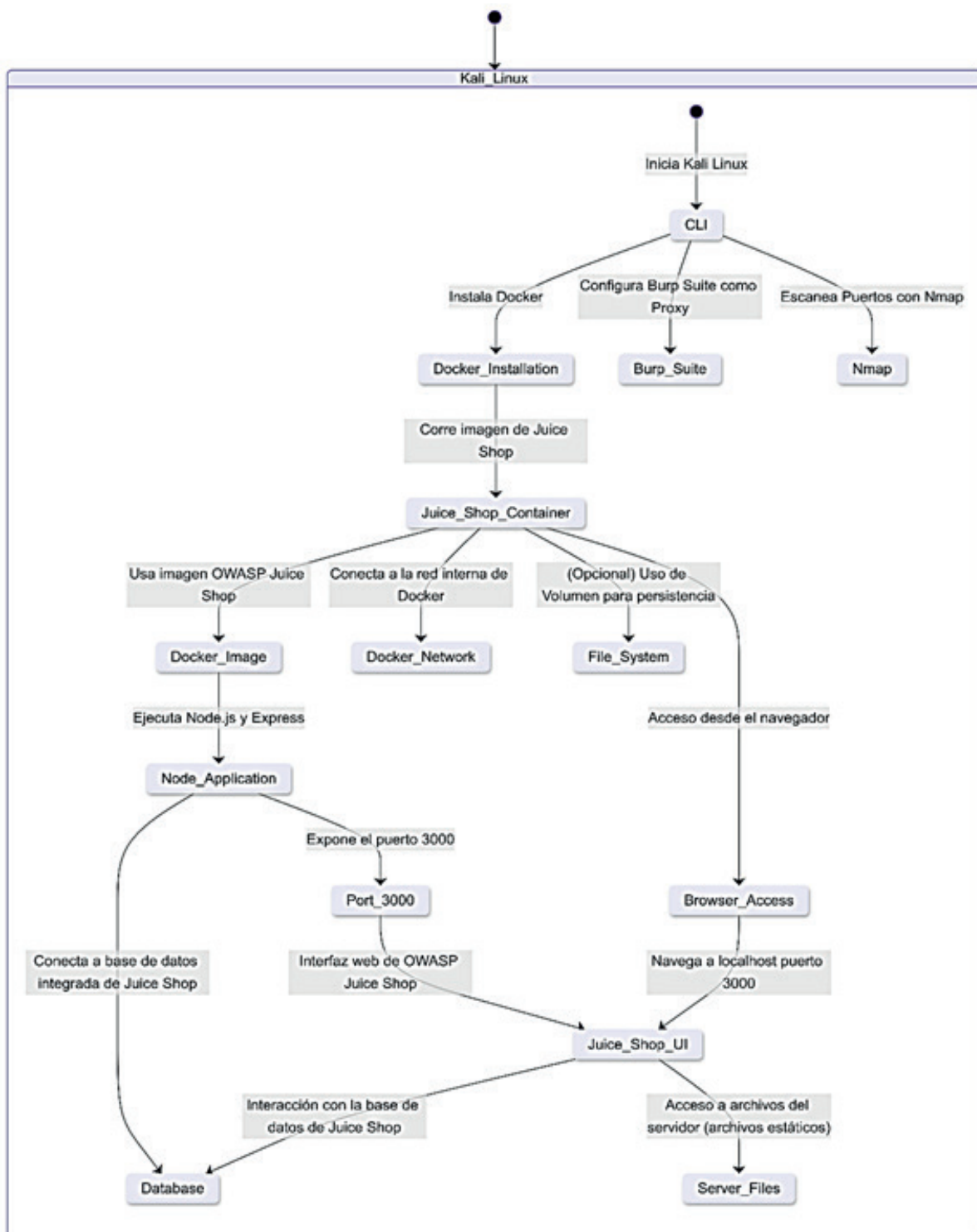


A continuación, se describe el flujo de comunicación establecido entre las herramientas utilizadas en el entorno de simulación, enfocándose en la interacción entre Kali Linux, Burp Suite y la aplicación OWASP Juice Shop:

- Kali Linux (Burp Suite) se comunica con la aplicación web vulnerable a través de la red virtual.
- Burp Suite intercepta y modifica las solicitudes enviadas a la aplicación web.
- La aplicación web vulnerable en Docker responde a las solicitudes enviadas por Burp Suite.

Esta topología es cerrada y segura, ideal para poder realizar pruebas de penetración y ciberataques en un entorno controlado, tal como se representa en la Figura 2.

Figura 2: Arquitectura del sistema.



3.1. Configuración de la aplicación web en Kali Linux

Se configuró el entorno en Kali Linux. Se actualizan los paquetes disponibles en el sistema a través del comando `sudo apt-get update`. Se instala Docker en el sistema operativo Kali Linux mediante `sudo apt-get install docker.io`, y se inicia el servicio Docker con `sudo systemctl start docker`. Luego, se descarga la imagen de Docker de la aplicación web que se usará, en este caso la de OWASP Juice Shop, utilizando el comando `sudo docker pull bkimminich/juice-shop`. Posteriormente, se ejecuta el contenedor que contiene el aplicativo web con `sudo docker run -d -p 3000:3000 bkimminich/juice-shop`. Con ello, ya se podrá acceder a la aplicación web a través de `http://localhost:3000` mediante el navegador Mozilla Firefox.

Una vez realizados estos pasos, ya se dispone de un entorno web controlado, en el cual, se ha decidido desarrollar diversas actividades para con ello, demostrar, los riesgos a los cuales se puede ver expuesto un entorno real. Se utilizó este entorno dado por OWASP, puesto que es riesgoso el desarrollar un entorno para hacer este tipo de ataques y pruebas los cuales se presentan a continuación.

3.2. Identificación de puertos abiertos

El primer paso consistió en la identificación de puertos abiertos mediante un escaneo de red dirigido al aplicativo web. Esta acción permite descubrir los servicios expuestos y activos en dichos puertos. Un atacante puede utilizar esta información para determinar qué tecnologías o configuraciones están en uso, lo que facilita la preparación de vectores de ataque específicos, como exploits asociados a esos servicios o la explotación de configuraciones incorrectas.

Para este procedimiento, se inicia verificando la dirección IP de la instancia donde se encuentra desplegado el aplicativo web. Una vez identificada, se procede a realizar un escaneo de puertos utilizando la herramienta `nmap`, con el objetivo de detectar los puertos abiertos asociados a dicha dirección. Con esta información, es posible avanzar hacia las siguientes actividades del entorno de prueba, centradas en evaluar el comportamiento del aplicativo web frente a ciberataques y pruebas de penetración.

3.3. Inyección SQL

En esta fase se simuló un ataque de inyección SQL con el objetivo de evaluar la respuesta del aplicativo web ante intentos de manipulación de consultas a la base de datos. Para ello, se empleó la herramienta Burp Suite, configurada manualmente como proxy en la dirección `127.0.0.1:8080`, utilizando el navegador para interceptar las solicitudes enviadas al aplicativo web.

En el aplicativo web se accedió al formulario de inicio de sesión, donde se ingresa una contraseña arbitraria y se modifica el campo de correo electrónico. La solicitud es interceptada con Burp Suite, y se reemplaza el valor original del correo por una serie de payloads de inyección SQL, incluyendo expresiones como `' OR 1=1 -- '`. Estos valores fueron enviados al servidor con el fin de observar el comportamiento del sistema ante intentos de elusión de autenticación mediante manipulación de parámetros.

3.4. Secuencias de comandos entre sitios (XSS)

El ataque de Cross-Site Scripting (XSS) consiste en la inyección de código JavaScript malicioso dentro de campos o componentes del sitio web que interpretan contenido proporcionado por el usuario. Este tipo de vulnerabilidad puede ser utilizado para robar cookies, modificar la interfaz o redirigir al usuario hacia sitios externos sin su consentimiento.

Para esta prueba, se navegó dentro del aplicativo OWASP Juice Shop hacia componentes que permiten entradas de usuario, como la barra de búsqueda y el módulo de retroalimentación. En dichos campos, se ingresan diferentes cargas útiles (payloads) diseñadas para provocar la ejecución de scripts. Algunos de los vectores utilizados incluyen: `<script>alert('XSS')</script>`, `<img src=x onerror=alert(1)>` y `<svg/onload=alert('XSS')>`. Estas entradas fueron enviadas a través del navegador y monitorizadas con Burp Suite para observar cómo responde el sistema ante intentos de ejecución de código no autorizado.

3.5. Vulnerabilidad con carga de archivos

La vulnerabilidad de carga de archivos consiste en la posibilidad de subir archivos al servidor sin un control adecuado sobre su tipo o contenido, lo que podría permitir la ejecución de código no autorizado, acceso indebido o incluso el compromiso total del sistema. Un atacante podría aprovechar esta falla para introducir archivos que contengan scripts o instrucciones maliciosas que el servidor pueda interpretar y ejecutar. En este caso, se accedió a una sección del aplicativo web que permite la carga de archivos, específicamente la opción destinada a actualizar la foto de perfil del usuario.

Para esta prueba, se desarrolló un script PHP diseñado para ejecutar comandos en el servidor web mediante la URL. Este archivo es accedido desde el navegador incluyendo un parámetro con la instrucción deseada. A continuación, se intenta cargar el archivo como imagen de perfil en el aplicativo web, con el fin de evaluar el comportamiento del sistema ante la subida de archivos que no corresponden a formatos de imagen. La finalidad de este procedimiento es identificar si el sistema realiza algún tipo de validación del archivo enviado, ya sea por extensión o por tipo MIME (Multipurpose Internet Mail Extensions).

3.6. Recorrido de directorios

El recorrido de directorios es una técnica utilizada para acceder a archivos o directorios fuera del espacio permitido por la aplicación, mediante la manipulación de rutas relativas en las solicitudes del cliente. Este tipo de ataque busca explotar fallas en la validación de rutas para acceder a archivos del sistema que normalmente estarían restringidos.

En esta prueba, se utiliza Burp Suite para interceptar y modificar solicitudes enviadas al servidor. A través de esta herramienta, se identificaron parámetros en las URLs o formularios susceptibles de aceptar rutas de archivos. Se sustituyeron dichos valores por cadenas que representan navegación hacia niveles superiores del sistema, como `../../../../etc/passwd`, con el objetivo de evaluar si el servidor responde con acceso a archivos fuera del directorio de la aplicación. El procedimiento se realizó en un entorno controlado para observar la respuesta de la aplicación ante intentos de exploración no autorizada del sistema de archivos.

3.7. Falsificación de solicitudes entre sitios (CSRF)

La falsificación de solicitudes entre sitios (CSRF, por sus siglas en inglés) es una técnica que busca inducir a un usuario autenticado a ejecutar una acción no autorizada en una aplicación web. Este ataque explota la confianza que el sistema tiene en el navegador del usuario, mediante el envío de solicitudes manipuladas desde sitios externos.

Para esta prueba, se construyó un formulario HTML externo con los mismos parámetros que la aplicación vulnerable utiliza para realizar cambios, como la actualización de contraseñas. Este formulario se configuró para enviarse automáticamente al cargar la página, simulando una acción que el usuario no ha autorizado. El objetivo del procedimiento fue analizar si la aplicación valida el origen de la solicitud, y si requiere medidas de protección como tokens CSRF, cabeceras personalizadas o validación del origen.

3.8. Vulnerabilidad de manipulación de parámetros

La manipulación de parámetros es una vulnerabilidad que consiste en alterar los valores enviados en solicitudes HTTP, como formularios o URLs, con el fin de modificar el comportamiento de una aplicación web. Esta técnica puede ser utilizada por un atacante para realizar acciones no autorizadas, como acceder a información de otros usuarios, cambiar datos almacenados o elevar privilegios.

Para esta prueba, se accede a la funcionalidad de retroalimentación del aplicativo web, en la cual el usuario puede calificar la página mediante un valor de puntuación. Se utiliza Burp Suite para interceptar la solicitud HTTP correspondiente y se identifica el parámetro responsable del puntaje. Posteriormente, se modifica dicho valor antes de enviarlo al servidor, con el objetivo de evaluar cómo responde la aplicación ante la alteración de datos enviados desde el cliente.

IV. Evaluación de Resultados y Discusión

4.1. Evaluación de Resultados

RQ1: ¿Cuáles de las vulnerabilidades web más comunes pueden ser explotadas con éxito en un entorno controlado utilizando OWASP Juice Shop?

Se ejecutaron cinco tipos de ataques diferentes con el objetivo de explorar las vulnerabilidades más comunes. La siguiente tabla muestra un resumen de cada ataque y su éxito.

Tabla 1: Resumen de ataques realizados en OWASP Juice Shop

Tipo de Ataque	Descripción	Resultado	Vulnerabilidad Detectada
SQL Injection	Inyección SQL en el login para omitir autenticación	Acceso no autorizado	Sí
XSS	Código malicioso inyectado en barra de búsqueda	Alerta XSS activada	Sí
File Upload	Subida de archivo PHP con shell reversa	Archivo no ejecutado	No
Directory Traversal	Acceso a archivos restringidos del servidor	Acceso denegado	No
CSRF	Cambio de contraseña vía formulario externo	Contraseña modificada	Sí

De los cinco ataques realizados, tres fueron exitosos: SQL Injection, XSS y CSRF. Esto confirma la vulnerabilidad crítica que tienen los sistemas web y cómo estas fallas pueden comprometer la seguridad de las aplicaciones cuando no se aplican controles adecuados.

Para la prueba de inyección SQL se empleó una serie de payloads diseñados para evadir el proceso de autenticación del sistema. Las solicitudes modificadas fueron interceptadas y enviadas utilizando Burp Suite. Los resultados obtenidos, incluyendo los códigos de respuesta, tiempos de ejecución y efectividad de cada intento, se resumen en la Tabla 2.

Tabla 2: Resultados detallados de SQL Injection en Juice Shop

Payload	¿Éxito?	Código	T1	T2	T3	Long.	CVSS	Frecuencia
' OR 1=1#	No	500	14	12	15	1520	9.8	0/1
' OR 1=1/*	Sí	200	26	16	19	1185	9.8	3/3
' OR "="'	No	401	10	12	12	413	9.8	0/1
' OR 1=1 LIMIT 1--	Sí	200	13	16	14	1185	9.8	3/3
' AND 1=1--	No	401	10	9	9	413	9.8	0/1
admin' OR 1=1--	Sí	200	13	13	14	1185	9.8	3/3

Tres de los payloads utilizados lograron ejecutarse correctamente, obteniendo tokens válidos y permitiendo el acceso al sistema con privilegios de administrador. Las respuestas generadas por el servidor presentaron una longitud uniforme de 1185 bytes y códigos de estado HTTP 200, lo que indica que no se aplicaron controles de validación eficaces sobre las entradas manipuladas durante el proceso de autenticación. En el ataque XSS se probaron diferentes vectores. La Tabla 3 presenta los resultados por ubicación, éxito y tiempo.

Tabla 3: Resultados de ataques XSS en Juice Shop

Payload	¿Éxito?	Tiempo (ms)	Ubicación	CVSS	Frecuencia
<script>alert('XSS')</script>	No	0 (no ejecutado)	Customer Feedback	7.4	0/1
	No	0 (no ejecutado)	Customer Feedback	7.4	0/1
<svg/onload=alert('XSS')>	No	0 (no ejecutado)	Customer Feedback	7.4	0/1
<iframe src="...">	Sí	5	Barra de búsqueda	7.4	1/1
<script>alert('XSS')</script>	No	0 (no ejecutado)	Barra de búsqueda	7.4	0/1
	No	0 (no ejecutado)	Barra de búsqueda	7.4	0/1
<svg/onload=alert('XSS')>	Sí	1	Barra de búsqueda	7.4	1/1

Si bien los vectores de XSS más comunes fueron bloqueados por el sistema, otros menos convencionales, como <iframe> y <svg>, lograron ejecutarse correctamente, en particular dentro del componente de la barra de búsqueda. Este comportamiento sugiere la existencia de mecanismos de protección parcial, aplicados de forma no uniforme a lo largo de la aplicación.

En el ataque de Falsificación de Solicitudes entre Sitios (CSRF), se evaluaron formularios maliciosos con distintos objetivos. La Tabla 4 muestra los resultados en función de la acción afectada, la ubicación del recurso, el éxito del ataque y el tiempo de ejecución.

Tabla 4: Resultados de ataques CSRF (Falsificación de solicitudes entre sitios) en Juice Shop

Payload	¿Éxito?	Tiempo	Ubicación	CVSS	Frecuencia
Formulario con auto-submit para cambiar la contraseña	Sí	200 ms	/rest/user/change-password	7.5	1/1
Formulario con intento de cambiar el nombre de usuario	No	0 ms	/profile	---	0

Los resultados presentados en la Tabla 4 muestran que el ataque CSRF fue exitoso al intentar cambiar la contraseña del usuario mediante un formulario con autoenvío, aprovechando una vulnerabilidad presente en la ruta /rest/user/change-password. Esta acción corresponde a un nivel de severidad alto, con una calificación CVSS de 7.5. Por otro lado, el intento de modificar el nombre de usuario a través de la ruta /profile fue bloqueado, lo que indica que dicha funcionalidad cuenta con medidas de seguridad efectivas frente a este tipo de ataque.

RQ2: ¿Qué niveles de gravedad (CVSS) y tiempos de ejecución presentan los diferentes ataques realizados contra la aplicación vulnerable?

La tabla 5 presenta un resumen consolidado de los ataques realizados en OWASP Juice Shop, integrando los resultados obtenidos en los cuadros anteriores. Se evaluaron cinco tipos de vulnerabilidades: inyección SQL, Cross-Site Scripting (XSS), subida de archivos maliciosos, recorrido de directorios (Directory Traversal) y falsificación de solicitudes entre sitios (CSRF). Para cada una se reporta su severidad mediante la métrica CVSS v3.1, el tiempo promedio de ejecución y si fue detectada exitosamente en el entorno analizado.

Tabla 5: Gravedad (CVSS) y tiempo de ejecución de ataques

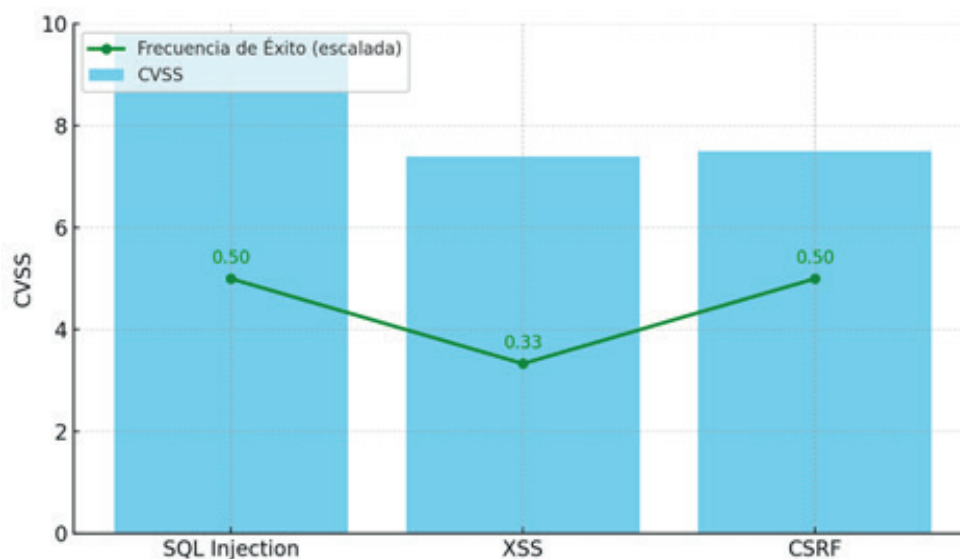
Ataque	CVSS v3.1	Tiempo de Ejecución (ms)	Vulnerabilidad detectada
SQL Injection	9.8 (Alta)	15000	Sí
XSS	7.4 (Media)	3	Sí

File Upload	8.6 (Alta)	--	No
Directory Traversal	7.5 (Alta)	--	No
CSRF	7.5 (Media)	200	Sí

La Figura 3 presenta un resumen visual de las vulnerabilidades que lograron ser explotadas exitosamente durante las pruebas en OWASP Juice Shop. El análisis se enfocó en tres tipos de ataques: inyección SQL (SQL Injection), Cross-Site Scripting (XSS) y falsificación de solicitudes entre sitios (CSRF), los cuales fueron interceptados con éxito al menos una vez. Para cada caso se reporta su gravedad estimada mediante CVSS v3.1 (representada con barras) y su frecuencia de éxito relativa (proporción de payloads exitosos respecto al total) y la frecuencia de éxito fue normalizada con fines de representación visual, (representada como puntos verdes conectados).

Figura 3: Resumen de gravedad (CVSS) y frecuencia de éxito de ataques interceptados en OWASP Juice Shop

Resumen de Gravedad (CVSS) y Frecuencia de Éxito de Ataques Interceptados



Del análisis se desprende que el ataque de inyección SQL posee la mayor severidad (CVSS 9.8), alineada con una frecuencia de éxito del 50%, lo que sugiere que además de ser crítico, fue parcialmente viable en el entorno analizado. Por otro lado, el ataque XSS, aunque con una gravedad menor (CVSS 7.4), evidenció una frecuencia de éxito más baja (33\%), lo cual puede estar asociado a mecanismos de validación más robustos en ciertas rutas. En contraste, CSRF, con una severidad media (CVSS 7.5), alcanzó una frecuencia de éxito igual a la del SQLi (50\%), indicando una debilidad puntual en la protección contra solicitudes forjadas. Esta comparación evidencia que no siempre existe una relación directa entre la severidad teórica y la efectividad práctica de un ataque, por lo que ambos factores deben ser considerados conjuntamente al priorizar medidas de mitigación.

RQ3: ¿Qué métricas operativas clave se pueden obtener al realizar pruebas de penetración sobre una aplicación web desplegada en Docker; y qué nos indican sobre su seguridad y desempeño?

La Tabla 6 muestra las métricas operativas obtenidas durante las pruebas de penetración en una aplicación web desplegada en Docker. Estas métricas permiten evaluar la seguridad y el desempeño del sistema frente a distintos vectores de ataque, considerando aspectos como la frecuencia de éxito, el tiempo de respuesta y la severidad de las vulnerabilidades detectadas.

Tabla 6: Métricas de los ataques exitosos en el entorno de pruebas de ataques detectados en OWASP Juice Shop

Métrica	Descripción	Valor	Interpretación
Vulnerabilidades detectadas	Tipos de ataques que lograron ejecución exitosa	3 (SQLi, XSS, CSRF)	El entorno permitió explotación de 3 vectores distintos
Frecuencia máxima de éxito	Mayor proporción de payloads exitosos entre los intentos	0.5 (SQLi y CSRF)	SQLi y CSRF alcanzaron el 50% de éxito en pruebas
Tiempo de ejecución mínimo	Payload con menor tiempo de respuesta registrado	1 ms (XSS – svg/onload)	Algunos vectores de XSS responden casi instantáneamente
Severidad más alta (CVSS)	Valor CVSS más alto entre ataques detectados	9.8 (SQL Injection)	SQLi representa un riesgo crítico
Cantidad total de payloads probados	Suma de todos los intentos de explotación registrados	14 payloads (6 SQLi, 6 XSS, 2 CSRF)	Muestra el alcance de las pruebas en distintos vectores

La Tabla 6 resume los aspectos más relevantes de los ataques exitosos detectados durante las pruebas. Se reportan la cantidad de vulnerabilidades explotadas, su frecuencia de éxito, tiempos de ejecución mínimos, nivel de severidad (CVSS) y el total de payloads utilizados. Estos indicadores permiten evaluar tanto el impacto como la eficacia de los vectores que lograron vulnerar el entorno.

4.2. Discusión

Los resultados obtenidos demuestran que SQL Injection, Cross-Site Scripting (XSS) y Cross-Site Request Forgery (CSRF) fueron explotados con éxito en OWASP Juice Shop. Esto evidencia la presencia de vulnerabilidades críticas cuando no se aplican controles de seguridad desde el desarrollo. En particular, SQL Injection representó el mayor riesgo con una severidad de CVSS 9.8 y permitió el acceso como administrador. Además, tanto SQLi como CSRF alcanzaron una frecuencia de éxito del 50 %, lo que refleja su alta efectividad en entornos vulnerables.

En el caso de XSS, a pesar de tener una menor gravedad (CVSS 7.4), el tiempo de ejecución registrado fue de solo 1 ms, lo que lo convierte en una amenaza silenciosa y difícil de detectar. Algunos vectores como <iframe> y <svg> lograron ejecutarse en la barra de búsqueda, lo que evidencia que los mecanismos de

filtrado aplicados no fueron uniformes en toda la aplicación. Por otro lado, el ataque CSRF fue exitoso al permitir el cambio de contraseña del usuario mediante un formulario con autoenvío, aprovechando la vulnerabilidad en la ruta `/rest/user/change-password`. Este comportamiento evidencia la ausencia de mecanismos de protección anti falsificación en dicha funcionalidad. Sin embargo, al intentar modificar el nombre de usuario a través de la ruta `/profile`, la solicitud fue bloqueada, lo que indica la existencia de controles más estrictos en esa sección específica.

En conjunto, estos hallazgos refuerzan la importancia de incorporar consultas preparadas, validaciones del lado del servidor y tokens CSRF en todas las rutas sensibles. Además, se valida el uso de entornos como Juice Shop para evaluar la seguridad de sistemas web mediante ataques reproducibles y medibles. Estos hallazgos refuerzan la necesidad de incorporar medidas de ciberseguridad desde etapas tempranas del desarrollo web, como parte de una estrategia de prevención continua.

V. Conclusiones y Trabajo Futuro

Las pruebas de penetración realizadas sobre la aplicación OWASP Juice Shop en un entorno controlado permitieron identificar vulnerabilidades críticas asociadas a ataques comunes como inyección SQL, Cross-Site Scripting (XSS) y falsificación de solicitudes entre sitios (CSRF). La explotación exitosa de estas fallas evidenció la ausencia de controles robustos de validación y autenticación en ciertas rutas del sistema, lo que posibilitó accesos no autorizados y ejecución de acciones sensibles. En contraste, funcionalidades como la carga de archivos y el recorrido de directorios demostraron contar con medidas de protección efectivas ante los vectores utilizados. El análisis también permitió obtener métricas operativas relevantes, como la frecuencia de éxito de los payloads, tiempos de respuesta mínimos y niveles de severidad CVSS. Estas métricas facilitaron una evaluación comparativa de los vectores y ayudaron a visibilizar los riesgos asociados a cada uno. Se confirmó que ataques como SQLi y CSRF, con una frecuencia de éxito del 50%, representan amenazas recurrentes en aplicaciones con validaciones incompletas.

Como trabajo futuro, se propone ampliar la cobertura de pruebas mediante el uso de herramientas automatizadas para detección de vulnerabilidades, así como incorporar técnicas de fuzzing y escaneo de seguridad continua dentro del ciclo de desarrollo (DevSecOps). Asimismo, se sugiere evaluar otras plataformas diseñadas con vulnerabilidades controladas, con el fin de contrastar resultados y validar la aplicabilidad de los hallazgos en diferentes entornos.

Referencias

- Ahmadi, S. (2024). Challenges and solutions in network security for serverless computing. *International Journal of Current Science Research and Review*, 7(1), 218–229. <https://dx.doi.org/10.47191/ijcsrr/V7-i1-23>
- Anu, P., & Vimala, S. (2018). A survey on sniffing attacks on computer networks. *Proceedings of 2017 International Conference on Intelligent Computing and Control (I2C2 2017)*, 1–5. <https://doi.org/10.1109/I2C2.2017.8321914>

- Augusto, C., & Agudelo, R. (2018). Arquitectura para automatizar respuesta a incidentes de seguridad de la información relacionados con ataques internos mediante la ejecución de técnicas spoofing [Trabajo académico].
- Barth, A., Jackson, C., & Mitchell, J. C. (2021). Robust defenses for cross-site request forgery. *ACM Transactions on Information and System Security*, 24(1), 1–38. <https://doi.org/10.1145/1455770.1455782>
- Bau, J., Bursztein, E., Gupta, D., & Mitchell, J. (2021). State of the art: Automated black-box web application vulnerability testing. *IEEE Symposium on Security and Privacy*, 332–345. <https://doi.org/10.1109/SP.2010.27>
- Binbusayyis, A. (2024). Reinforcing network security: Network attack detection using random grove blend in weighted MLP layers. *Mathematics*, 12(11), 1720. <https://doi.org/10.3390/MATH12111720>
- Chávez, J. (2011). Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergentes [Tesis de grado, Escuela Politécnica Nacional]. <http://bibdigital.epn.edu.ec/handle/15000/4282>
- Echeverría, J., Espinoza, C., & Zambrano, D. (2020). Evaluación del nivel de ciberseguridad en usuarios jóvenes ecuatorianos [Estudio técnico].
- Fernandes, P., Ciardhuáin, S., & Antunes, M. (2024). Unveiling malicious network flows using Benford's law. *Mathematics*, 12(15), 2299. <https://doi.org/10.3390/MATH12152299>
- Fuertes Díaz, W. M., & Macas Carrasco, M. A. (2023). Ciberseguridad [Tesis de grado, Universidad de las Fuerzas Armadas ESPE]. <http://repositorio.espe.edu.ec/handle/21000/36481>
- González, D. A., Pérez, M. E. G., & Bernal, L. P. (2016). Detección y mitigación de ataques ARP en la red corporativa de la división territorial Holguín, ETECSA. *Telemática*, 15(1), 62–68.
- Gorgone Carvajal, A. (2023). Simulación de ciberataques con GNS3 para validar la robustez de protocolos industriales [Tesis de grado]. <https://hdl.handle.net/10630/27491>
- Lekies, S., Stock, B., & Johns, M. (2023). 25 million flows later: Large-scale detection of DOM-based XSS. *Proceedings of the 2023 ACM SIGSAC Conference*, 1193–1204. <https://doi.org/10.1145/2508859.2516703>
- Nakata, M., & Otsuka, A. (2021). Security testing environments for web services [Estudio técnico].
- Rafique, S., Humayun, M., Gul, Z., & Abbas, A. (2015). Systematic review of web application security vulnerabilities detection methods. *Journal of Computer and Communications*, 3(9), 28–40. <http://dx.doi.org/10.4236/jcc.2015.39004>
- Sadegh, M., & Tajalli, B. (2013). Study of SQL injection attacks and countermeasures. *International Journal of Innovative Research in Computer and Communication Engineering*. <http://dx.doi.org/10.7763/IJCC.2013.V2.244>
- Son, J. (2016). Virtual lab for online cyber security education. *Communications of the IIMA*. <http://dx.doi.org/10.58729/1941-6687.1200>
- Straub, J. (2020). Cyberwarfare simulations: An overview of platforms and challenges [Informe técnico].

- Ukwandu, E., Aghenta, L., & Okwechime, I. (2020). A systematic review of cyberattacks on critical infrastructure. [Estudio de revisión].
- Vega-Oyola, C., Tapia, E., & Gallardo, F. (2022). Análisis de factores de seguridad informática mediante la metodología OWASP v4.2: Caso de estudio ISTJOL. *Revista EETES*, 6(1). <http://dx.doi.org/10.33970/eetes.v6.n1.2022.293>
- Veeraburden, K., & Bekaroo, G. (2022). Security in web applications: A comparative analysis of key SQL injection detection techniques. 2022 4th International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM). <http://dx.doi.org/10.1109/ELECOM54934.2022.9965264>
- Vighe, S. (2024). Security for continuous integration and continuous deployment pipeline. *International Research Journal of Modernization in Engineering Technology and Science*. <http://dx.doi.org/10.56726/IRJMET50676>



Departamento de
Seguridad y Defensa

★★★★★ Revista de Ciencias de ★★★★★
Seguridad y Defensa
Volumen IX - Número 4

