ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.940

The importance of teaching free software for ethical hacking and cybersecurity training from an ethical and pragmatic perspective – FBCEM Model

José Fernando Espinoza León
Docente del Servicio Nacional de Adiestramiento en Trabajo Industrial (SENATI)
Escuela de Tecnologías de la Información (ETI)
Programa de Ingeniería de Ciberseguridad / Redes y Seguridad Informática
jespinozal@senati.pe , *jose.espinoza.l@uni.pe*

Abstract– *This study examines the role of Free and Open Source Software (FOSS) in cybersecurity education from both ethical and pragmatic perspectives. While traditional approaches to ethical hacking training have focused primarily on proprietary tools and certification-oriented methodologies, this paper proposes a structured pedagogical framework known as the FOSS-Based Cybersecurity Educational Model (FBCEM). The model integrates four progressive stages: technological foundations, system architecture, IT infrastructure, and cybersecurity operations, culminating in the implementation of Security Operations Centers (SOC) using FOSS tools. A qualitative descriptive methodology based on multi-cohort teaching experience is employed. Results indicate improvements in critical thinking, ethical awareness, technological autonomy, and system-level understanding among students. Furthermore, the implementation of SOC environments enabled effective detection and mitigation of cybersecurity threats. The findings support the integration of FOSS not only as a technical resource but as a foundational element for sustainable, ethical, and autonomous cybersecurity education.*

Keywords- *Cybersecurity, Free and Open Source Software (FOSS), Ethical Hacking, Ethical Hacker, Security Operations Center (SOC), SIEM, Engineering Education.*

Importancia de la enseñanza de Software Libre para la formación de Ethical Hacking y la Ciberseguridad desde un enfoque ético y pragmático – Modelo FBCEM

José Fernando Espinoza León
Docente del Servicio Nacional de Adiestramiento en Trabajo Industrial (SENATI)
Escuela de Tecnologías de la Información (ETI)
Programa de Ingeniería de Ciberseguridad / Redes y Seguridad Informática
jespinozal@senati.pe , jose.espinoza.l@uni.pe

Resumen– *Este estudio analiza el papel del Software Libre y de Código Abierto (FOSS) en la enseñanza de la ciberseguridad desde una perspectiva ética y pragmática. Mientras que los enfoques tradicionales de formación en ethical hacking se han centrado principalmente en herramientas propietarias y certificaciones, este trabajo propone un marco pedagógico estructurado denominado FBCEM (FOSS-Based Cybersecurity Educational Model). El modelo se organiza en cuatro etapas progresivas: fundamentos tecnológicos, arquitectura de sistemas, infraestructura TI y operaciones de ciberseguridad, culminando en la implementación de Centros de Operaciones de Seguridad (SOC) mediante herramientas FOSS. Se emplea una metodología cualitativa descriptiva basada en la experiencia docente en múltiples cohortes. Los resultados evidencian mejoras en el pensamiento crítico, la conciencia ética, la autonomía tecnológica y la comprensión profunda de los sistemas. Asimismo, la implementación de entornos SOC permitió la detección y mitigación efectiva de amenazas. Los hallazgos respaldan la integración del Software Libre no solo como recurso técnico, sino como base para una formación sostenible, ética y autónoma en ciberseguridad.*

.

Palabras clave - *Ciberseguridad, Software Libre y de Código Abierto, Ethical Hacking, Hacker Ético, Centro de Operaciones de Seguridad (SOC), SIEM, Educación en Ingeniería.*

I. INTRODUCCIÓN

En la última década, la ciberseguridad se ha consolidado como un pilar fundamental para la protección de infraestructuras digitales, sistemas de información y servicios críticos en un contexto de creciente digitalización. La formación de profesionales en este campo ha adquirido una relevancia estratégica, especialmente ante el incremento de amenazas cibernéticas y la necesidad de contar con especialistas capaces de prevenir, detectar y mitigar incidentes de seguridad [15], [14].

Sin embargo, los enfoques tradicionales de enseñanza en ciberseguridad, particularmente en el ámbito del ethical hacking, han estado predominantemente orientados hacia el uso instrumental de herramientas específicas y la obtención de certificaciones profesionales como CEH y OSCP [4], [5]. Este modelo, si bien resulta efectivo para el desarrollo de habilidades operativas, presenta limitaciones al centrarse en el dominio técnico de plataformas, muchas de ellas de carácter privativo, lo que puede generar dependencia tecnológica y restringir la comprensión profunda de los sistemas. Asimismo, la ausencia de un enfoque ético estructurado puede debilitar la formación integral del profesional en ciberseguridad [13].

En contraste, el Software Libre y de Código Abierto (FOSS) emerge como una alternativa que trasciende su carácter técnico, incorporando dimensiones éticas, filosóficas y sociales. Basado en las libertades fundamentales de uso, estudio, modificación y distribución del software [1], este enfoque promueve la transparencia, la colaboración y el acceso al conocimiento como elementos clave para el desarrollo de la autonomía tecnológica [2]. En el contexto de la ciberseguridad, estas características resultan especialmente relevantes, ya que permiten analizar el funcionamiento interno de los sistemas, facilitando la identificación de vulnerabilidades y el fortalecimiento de mecanismos de defensa alineados con estándares internacionales de seguridad [15].

Adicionalmente, resulta necesario recuperar el sentido original de la cultura hacker como una práctica ética orientada a la mejora de sistemas, el aprendizaje continuo y la responsabilidad profesional. La frecuente confusión entre los conceptos de hacker y cracker ha contribuido a una visión distorsionada en el ámbito educativo, limitando su potencial como base formativa en ciberseguridad. En este sentido, la incorporación de principios éticos formales, como los propuestos por la ACM, resulta clave para fortalecer la formación profesional [13].

A partir de estas consideraciones, este trabajo propone el modelo FBCEM (FOSS-Based Cybersecurity Educational Model), un marco pedagógico estructurado que integra progresivamente cuatro dimensiones clave: fundamentos tecnológicos, arquitectura de sistemas, infraestructura de tecnologías de la información y operaciones de ciberseguridad.

El modelo culmina con la implementación de Centros de Operaciones de Seguridad (SOC), los cuales constituyen entornos fundamentales para la detección, análisis y respuesta a incidentes de seguridad, alineados con prácticas reconocidas en la industria [18], [16].

.

II. MARCO TEÓRICO

A. Origen y evolución del Software Libre y de Código Abierto

El Software Libre surge como un movimiento tecnológico, social y filosófico a partir de la década de 1980, impulsado por la necesidad de garantizar las libertades de los usuarios frente a modelos restrictivos de software privativo. Uno de los principales referentes de este movimiento es Richard Stallman, quien establece las bases del proyecto GNU y la Free Software Foundation, definiendo las cuatro libertades fundamentales: la libertad de usar, estudiar, modificar y redistribuir el software [1].

Posteriormente, el término Open Source se introduce como una estrategia para promover el modelo desde una perspectiva más pragmática y orientada a la industria, destacando ventajas como la calidad del software, la colaboración distribuida y la innovación abierta [2]. Aunque ambos enfoques presentan matices ideológicos distintos, convergen en la importancia del acceso al código fuente y la transparencia como elementos clave del desarrollo tecnológico.

En el contexto actual, el Software Libre y de Código Abierto (FOSS) constituye la base de gran parte de la infraestructura digital global, incluyendo sistemas operativos, servidores web, plataformas cloud y herramientas de ciberseguridad [3].

B. Fundamentos éticos y cultura hacker

La cultura hacker, en su concepción original, se fundamenta en principios de curiosidad intelectual, aprendizaje continuo, colaboración y mejora de sistemas. Este enfoque ético promueve el uso responsable del conocimiento técnico para fortalecer la seguridad y la resiliencia de los sistemas informáticos.

Sin embargo, en el ámbito educativo y mediático, el término *hacker* ha sido frecuentemente asociado con actividades ilícitas, generando confusión con el concepto de *cracker*. Esta distorsión ha limitado la incorporación de la ética hacker como eje formativo en programas académicos de ciberseguridad.

Integrar estos principios dentro del proceso educativo permite formar profesionales con una visión crítica, ética y responsable, capaces de comprender no solo el funcionamiento de las herramientas, sino también las implicaciones sociales y tecnológicas de su uso [4].

La filosofía del Software Libre se alinea de manera natural con la ética hacker, al promover la transparencia, la colaboración comunitaria y el respeto por los usuarios y la sociedad.

TABLA I
PERSPECTIVA DE ASPECTOS DEL SOFTWARE LIBRE EN CIBERSEGURIDAD

Aspecto	**Ventajas del Software Libre (FOSS)**	**Impacto en la Formación Académica**
Accesibilidad	Licencias sin costo (Ej: Kali Linux, Metasploit).	Democratiza la enseñanza de *ethical hacking* sin barreras presupuestarias.
Transparencia	Código auditable (Ej: Wireshark, OWASP ZAP).	Permite el análisis profundo de protocolos, reforzando el aprendizaje empírico.
Personalización	Adaptabilidad mediante módulos (Ej: scripts en Python).	Facilita el despliegue de laboratorios y entornos de práctica específicos.
Colaboración	Ecosistemas activos (Ej: GitHub, Offensive Security).	Interacción con comunidades globales y estudio de casos reales.
Ética y Legalidad	Cumplimiento de marcos normativos (GPL, MIT, Apache).	Promueve el uso de software legal y la integridad profesional.
Actualización	Desarrollo colaborativo constante (Ej: Nmap, John the Ripper).	Garantiza el uso de herramientas alineadas con los estándares de la industria.
Portabilidad	Compatibilidad multiplataforma (VirtualBox, Docker).	Flexibilidad para ejecutar laboratorios en diversos entornos de HW/SW.
Habilidades	Superación del modelo de "caja negra" privativa.	Fomenta el pensamiento crítico y la resolución compleja de problemas.

C. Licencias de software y modelos de distribución

La cultura hacker, en su concepción original, se fundamenta en principios de curiosidad intelectual, aprendizaje continuo, colaboración y mejora de sistemas. Este enfoque ético promueve el uso responsable del conocimiento técnico para fortalecer la seguridad y la resiliencia de los sistemas informáticos.

Sin embargo, en el ámbito educativo y mediático, el término *hacker* ha sido frecuentemente asociado con actividades ilícitas, generando confusión con el concepto de *cracker*. Esta distorsión ha limitado la incorporación de la ética hacker como eje formativo en programas académicos de ciberseguridad.

Integrar estos principios dentro del proceso educativo permite formar profesionales con una visión crítica, ética y responsable, capaces de comprender no solo el funcionamiento de las herramientas, sino también las implicaciones sociales y tecnológicas de su uso [4].

Las principales licencias del ecosistema FOSS se resumen en la Tabla II.

TABLA II
Principales licencias de software libre usadas en ciberseguridad

Licencia	Características clave	Ejemplos en ciberseguridad
GPL (GNU General Public License)	Copyleft fuerte. Las obras derivadas deben usar la misma licencia.	Metasploit Framework (GPLv3), John the Ripper (en parte)
MIT License	Muy permisiva. Permite uso, modificación, distribución incluso en software propietario.	Nmap, Recon-ng
Apache License 2.0	Permisiva con protección de patentes. No exige que el derivado sea libre.	OWASP ZAP, Volatility
BSD License (2 o 3 cláusulas)	Muy permisiva, parecida a MIT. Permite código cerrado derivado.	Wireshark (BSD-style), tcpdump
Creative Commons (CC)	Más usada en documentación, no recomendada para software.	Usada en informes, blogs técnicos o guías de hacking ético.

D. Software Libre vs. Software Privativo en ciberseguridad

En el ámbito de la ciberseguridad, el uso de herramientas basadas en Software Libre presenta ventajas significativas en comparación con soluciones propietarias. Entre ellas destacan:

- Acceso al código fuente para auditoría y análisis de vulnerabilidades
- Mayor transparencia en el funcionamiento de los sistemas
- Flexibilidad para personalización e integración
- Reducción de costos en entornos educativos

No obstante, el software propietario continúa siendo ampliamente utilizado en entornos empresariales, debido a su soporte comercial y a la estandarización en ciertas plataformas.

Diversos estudios han señalado que la combinación de ambos enfoques puede ser útil en contextos profesionales; sin embargo, en el ámbito educativo, el uso de Software Libre favorece una comprensión más profunda de los sistemas y promueve la autonomía tecnológica [3], [5].

El software libre no solo democratiza el acceso al conocimiento en ethical hacking, sino que también:

✓ Promueve la ética al evitar licencias restrictivas o ilegales.

✓ Estimula la investigación al permitir modificar y estudiar el código fuente.

✓ Prepara para la industria, donde muchas herramientas estándar son de Código abierto (Ej: Kubernetes en seguridad cloud).

Como se muestra en la Tabla III, existen diferencias estructurales entre ambos enfoques

TABLA III
PERSPECTIVA COMPARATIVA: SOFTWARE LIBRE VS SOFTWARE PRIVATIVO

Característica	Software Libre	Software Privativo
Acceso al código fuente	Abierto y disponible para todos	Cerrado. No accesible.
Licencia	Licencias libres (GPL, MIT, Apache, etc.)	Licencias restrictivas del fabricante
Costo	Generalmente gratuito	Usualmente de pago
Modificación	El usuario puede modificar el software	Solo el propietario puede modificar
Distribución	Libremente distribuible	La distribución está restringida

Característica	Software Libre	Software Privativo
Ejemplos	GNU/Linux, LibreOffice, GIMP, Firefox	Windows, Microsoft Office, Adobe Photoshop
Soporte	Comunidad, foros, documentación abierta	Soporte oficial del proveedor
eguridad	Transparente; en la detección de errores	Más difícil de auditar
Actualizaciones	Hechas por la comunidad FOSS	Controladas por empresas.
Dependencia del proveedor	Baja	Alta

E. Formación en ciberseguridad: enfoque tradicional vs. enfoque formativo

La enseñanza de la ciberseguridad ha estado tradicionalmente vinculada a certificaciones profesionales como CEH (Certified Ethical Hacker) y OSCP (Offensive Security Certified Professional), las cuales se centran en el desarrollo de habilidades técnicas específicas orientadas a la práctica del *ethical hacking*.

Si bien estas certificaciones aportan valor en términos de empleabilidad, su enfoque suele ser instrumental, priorizando el uso de herramientas sobre la comprensión profunda de los sistemas. Esto puede limitar el desarrollo de competencias como el pensamiento crítico, la autonomía tecnológica y la capacidad de innovación.

En contraste, los enfoques formativos basados en Software Libre permiten una construcción más integral del conocimiento, al integrar aspectos técnicos, éticos y filosóficos dentro del proceso educativo [4].

F. Fundamentos del modelo FBCEM

A partir de los elementos teóricos descritos, se plantea el modelo FBCEM (FOSS-Based Cybersecurity Educational Model), el cual propone una estructura formativa basada en cuatro etapas progresivas:

1. Fundamentos tecnológicos y filosóficos
2. Arquitectura de sistemas
3. Infraestructura de tecnologías de la información
4. Operaciones de ciberseguridad (SOC)

Este modelo busca superar la fragmentación de la enseñanza tradicional, promoviendo una integración coherente entre teoría y práctica, así como entre tecnología y ética. A diferencia de enfoques centrados exclusivamente en herramientas o certificaciones, el modelo FBCEM plantea una progresión estructurada que permite al estudiante desarrollar competencias desde la comprensión conceptual hasta la aplicación en entornos reales.

Asimismo, el modelo incorpora el uso de laboratorios virtuales y entornos prácticos, facilitando el aprendizaje activo y la experimentación controlada en escenarios de ciberseguridad.

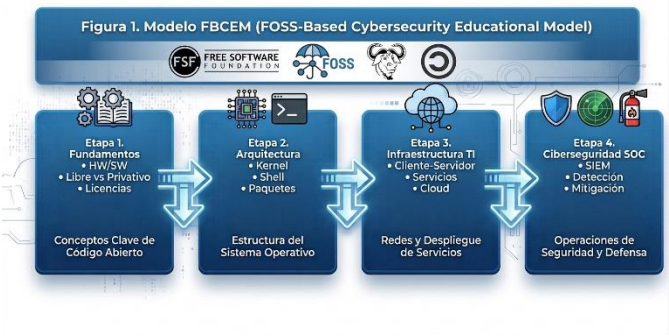


Fig. 1. Modelo FBCEM (FOSS-Based Cybersecurity Educational Model) basado en cuatro etapas formativas. Fuente: Elaboración propia.

Como se muestra en la Fig. 1, el modelo FBCEM se estructura en cuatro etapas progresivas que integran fundamentos conceptuales, arquitectura de sistemas, infraestructura tecnológica y operaciones de ciberseguridad. Esta organización permite una transición gradual desde la comprensión teórica hasta la aplicación práctica en entornos SOC.

De esta manera, el modelo no solo facilita la adquisición de habilidades técnicas, sino que también fortalece la comprensión sistémica, la autonomía tecnológica y la responsabilidad ética, elementos fundamentales en la formación de profesionales en ciberseguridad.

III. METODOLOGÍA

A. Enfoque y diseño de la investigación

El presente estudio adopta un enfoque cualitativo de tipo aplicado, orientado al análisis y validación de un modelo educativo en el ámbito de la ciberseguridad. Se emplea un diseño de investigación basado en estudio de caso, sustentado en la implementación del modelo FBCEM (FOSS-Based Cybersecurity Educational Model) en contextos reales de enseñanza en programas de formación en Ingeniería de Ciberseguridad, Seguridad Informática y Tecnologías de la Información.

Este enfoque permite analizar de manera contextualizada la efectividad del modelo en entornos educativos específicos, considerando variables como el desarrollo de competencias técnicas, la autonomía tecnológica y la comprensión ética por parte de los estudiantes.

B. Contexto de aplicación y participantes

El modelo FBCEM fue implementado en múltiples cohortes de estudiantes (entendidas como grupos académicos que cursan simultáneamente un programa formativo en un periodo

determinado) pertenecientes a programas técnicos y profesionales vinculados a la ciberseguridad y tecnologías de la información.

Los participantes incluyeron estudiantes con distintos niveles de conocimiento previo, desde niveles introductorios hasta intermedios, lo que permitió evaluar la adaptabilidad del modelo en diferentes etapas de formación.

C. Estructura metodológica del modelo FBCEM

La implementación del modelo FBCEM se organizó en cuatro etapas progresivas, alineadas con los fundamentos teóricos previamente descritos:

1. **Fundamentos tecnológicos y filosóficos:** Introducción a los conceptos de hardware y software, diferenciación entre software libre y privativo, análisis de licencias y comprensión de la filosofía del Software Libre.
2. **Arquitectura de sistemas:** Estudio del funcionamiento interno de los sistemas operativos, incluyendo kernel, gestión de procesos, sistemas de archivos, intérpretes de comandos y gestión de paquetes en entornos GNU/Linux.
3. **Infraestructura de tecnologías de la información:** Implementación de entornos cliente-servidor, configuración de servicios, virtualización y fundamentos de cloud computing orientados a la preparación de entornos seguros.
4. **Operaciones de ciberseguridad (SOC):** Diseño e implementación de un entorno de Centro de Operaciones de Seguridad (SOC) utilizando herramientas de Software Libre como SIEM e

IDS/IPS, permitiendo la detección, análisis y mitigación de amenazas.

D. Procedimiento de implementación del entorno SOC

Para la validación práctica del modelo, se diseñó un entorno de laboratorio basado en un enfoque SOC, estructurado en las siguientes fases:

- **Fase 1: Preparación del entorno**
  Configuración de máquinas virtuales, redes internas y sistemas operativos basados en GNU/Linux.
- **Fase 2: Implementación de herramientas**
  Instalación y configuración de herramientas de monitoreo y detección, incluyendo soluciones SIEM (por ejemplo, Wazuh) y sistemas IDS/IPS (como Suricata).
- **Fase 3: Generación de eventos de seguridad**
  Simulación de escenarios de ataque controlados para generar eventos de seguridad en el sistema.
- **Fase 4: Monitoreo y análisis**
  Observación de logs, correlación de eventos y análisis de alertas generadas por el SIEM. El proceso de monitoreo incluyó la recolección de logs, correlación de eventos y generación de alertas, siguiendo principios establecidos en marcos de respuesta a incidentes y gestión de eventos de seguridad [16], [15].
- **Fase 5: Respuesta y mitigación**
  Aplicación de medidas correctivas y evaluación de la efectividad de las acciones de respuesta.

Este procedimiento permitió replicar un entorno realista de operación en ciberseguridad, facilitando el aprendizaje práctico y la integración de conocimientos adquiridos en las etapas previas del modelo.

El diseño de escenarios de ataque y generación de eventos de seguridad se realizó considerando patrones de comportamiento adversarial basados en marcos de referencia ampliamente utilizados en ciberseguridad, como MITRE ATT&CK, lo que permitió estructurar ejercicios realistas y alineados con técnicas de ataque observadas en entornos reales [17].

E. Técnicas de recolección de datos

Para la evaluación del modelo FBCEM, se emplearon las siguientes técnicas:

- Observación directa del desempeño de los estudiantes en entornos prácticos
- Análisis de resultados de actividades y laboratorios
- Evaluación de la capacidad de resolución de problemas en escenarios simulados
- Registro de indicadores de desempeño en tareas de detección y respuesta a incidentes

F. Criterios de evaluación

Los resultados fueron analizados considerando los siguientes criterios:

- Nivel de comprensión conceptual de los sistemas
- Capacidad de implementación técnica
- Habilidad para detectar y analizar amenazas
- Capacidad de respuesta ante incidentes
- Desarrollo de pensamiento crítico y autonomía tecnológica

G. Consideraciones éticas

El desarrollo del estudio se realizó respetando principios éticos relacionados con el uso responsable de herramientas de ciberseguridad, asegurando que todos los escenarios de prueba se desarrollaran en entornos controlados y sin afectar sistemas reales o terceros.

Asimismo, se promovió el uso ético del conocimiento adquirido, reforzando la distinción entre prácticas legítimas de ciberseguridad y actividades maliciosas.

El desarrollo del estudio se realizó respetando principios éticos relacionados con el uso responsable de herramientas de

ciberseguridad, alineados con códigos profesionales reconocidos internacionalmente [13].

IV. RESULTADOS Y DISCUSIÓN

A. Implementación del entorno SOC basado en FBCEM

La aplicación del modelo FBCEM permitió la implementación de un entorno funcional de Centro de Operaciones de Seguridad (SOC) en laboratorio, integrando herramientas de Software Libre y de Código Abierto. Este entorno fue diseñado para simular condiciones reales de monitoreo, detección y respuesta ante incidentes de ciberseguridad.

El SOC implementado incluyó componentes clave como:

- Plataforma SIEM para correlación de eventos (Wazuh)
- Sistema de detección de intrusos IDS/IPS (Suricata)
- Infraestructura virtualizada basada en GNU/Linux
- Generación de tráfico y eventos simulados

Como resultado, los estudiantes lograron interactuar con un entorno operativo realista, comprendiendo el flujo completo de la gestión de incidentes de seguridad [18], [15].

B. Procedimiento de detección y análisis de amenazas

Durante la implementación, se desarrolló un flujo estructurado de detección de amenazas, que incluyó:

1. Generación de eventos (escaneo, tráfico anómalo, intentos de acceso)
2. Captura de paquetes y registros de sistema
3. Análisis mediante reglas de detección
4. Correlación de eventos en el SIEM
5. Generación de alertas.

Este proceso se desarrolló considerando modelos estructurados de gestión de incidentes y técnicas de ataque basadas en marcos como MITRE ATT&CK **[16], [17]**.

Este proceso permitió a los estudiantes comprender la relación entre eventos individuales y su interpretación dentro de un contexto de seguridad.

Figura 2: ADVANCED WAZUH SIEM DASHBOARD FOR THREAT INTELLIGENCE AND COMPLIANCE (INTEGRATED VIEW)

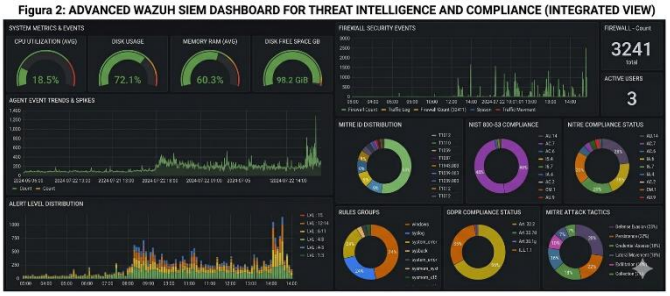


Fig. 2. Visualización de eventos de seguridad en plataforma SIEM basada en Wazuh. Fuente: Elaboración propia.

Como se observa en la Fig. 2, el sistema SIEM permite centralizar y correlacionar eventos en tiempo real, facilitando la identificación de patrones de comportamiento anómalo [15]

C. Resultados de detección y mitigación de amenazas

Los resultados obtenidos evidencian la capacidad del modelo [15] para desarrollar competencias prácticas en ciberseguridad. En particular, se observaron mejoras en:

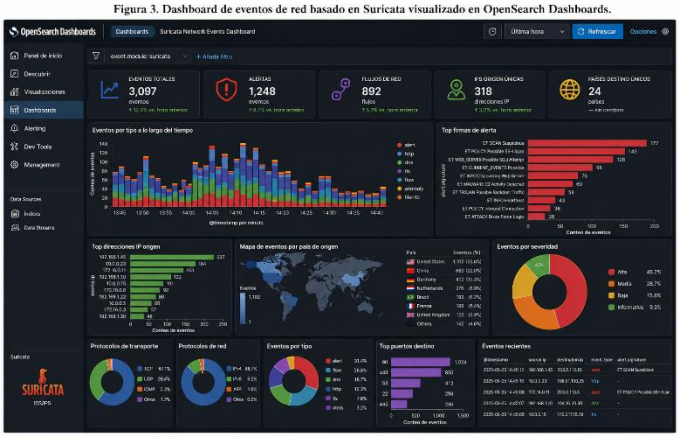
- Identificación de eventos sospechosos
- Análisis de logs y tráfico de red
- Interpretación de alertas
- Aplicación de medidas de mitigación

TABLE IV
TIPOS DE AMENAZAS DETECTADAS EN EL ENTORNO SOC

Tipo de evento	Descripción	Herramienta
Escaneo de puertos	Detección de reconocimiento de red	Suricata
Intentos de acceso	Fallos de autenticación	Wazuh
Tráfico anómalo	Comportamiento irregular	Suricata
Eventos correlacionados	Incidentes complejos	Wazuh

Asimismo, los estudiantes fueron capaces de ejecutar acciones de mitigación, tales como bloqueo de direcciones IP, análisis de vulnerabilidades y configuración de reglas de detección.

Figura 3. Dashboard de eventos de red basado en Suricata visualizado en OpenSearch Dashboards.



Fuente: Elaboración propia con Suricata + Filebeat + OpenSearch.

Fig. 3. Detección de tráfico sospechoso mediante IDS basado en Suricata. Fuente: Elaboración propia.

Como se observa en la fig. 3, el dashboard presenta una visión integral de los eventos de red generados por Suricata, visualizados mediante OpenSearch Dashboards, permitiendo el monitoreo en tiempo real de alertas, flujos de tráfico, direcciones IP y distribución geográfica. La interfaz facilita la identificación de patrones anómalos, análisis de protocolos y detección temprana de posibles amenazas en la red dentro de una arquitectura completamente FOSS.

D. Evaluación del impacto del modelo FBCEM

Los resultados evidencian que el modelo FBCEM contribuye significativamente al desarrollo de competencias en ciberseguridad, especialmente en:

- Comprensión profunda de sistemas
- Autonomía tecnológica
- Pensamiento crítico
- Capacidad de análisis de incidentes [14], [19]

A diferencia de enfoques tradicionales, los estudiantes no solo utilizan herramientas, sino que comprenden su funcionamiento interno y su integración dentro de un ecosistema de seguridad.

E. Comparación con modelos tradicionales de formación

Para contextualizar los resultados, se realizó una comparación entre el modelo FBCEM y enfoques tradicionales basados en certificaciones como CEH y OSCP.

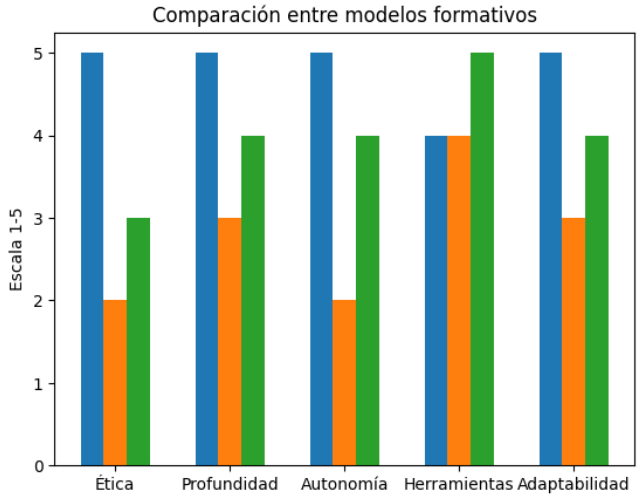


Fig. 4. Comparación conceptual entre modelos tradicionales y modelo FBCEM

A nivel conceptual, es posible diferenciar los enfoques tradicionales centrados en herramientas frente a modelos formativos integrales. Como podemos apreciar la Fig. 4 ilustra esta diferencia, destacando la evolución desde un enfoque instrumental hacia un enfoque basado en formación integral.

TABLE V
COMPARACIÓN ENTRE FBCEM, CEH Y OSCP

Criterio	FBCEM	CEH	OSCP
Enfoque	Formativo integral	Herramientas	Práctico ofensivo
Filosofía	Alta	Baja	Media
Profundidad técnica	Alta	Media	Alta
Autonomía	Alta	Baja	Media
Costo	Bajo	Alto	Alto
Enfoque educativo	Académico	Certificación	Profesional

Como se observa en la Tabla IV, el modelo FBCEM presenta ventajas significativas en términos de formación integral, al incorporar dimensiones éticas, filosóficas y técnicas.

F. Discusión: formación vs. certificación

Los resultados obtenidos permiten plantear una reflexión sobre el enfoque predominante en la enseñanza de la ciberseguridad. Mientras que las certificaciones profesionales priorizan la empleabilidad y el dominio de herramientas específicas, el

modelo FBCEM propone una formación más profunda, orientada al desarrollo de capacidades analíticas y comprensión sistémica.

Este enfoque se alinea con metodologías de aprendizaje basado en problemas que promueven el pensamiento crítico [20].

Este enfoque no busca reemplazar las certificaciones, sino complementarlas, proporcionando una base sólida sobre la cual los estudiantes puedan posteriormente especializarse. Asimismo, el uso de Software Libre reduce barreras económicas y facilita la replicabilidad del modelo en diferentes contextos educativos, lo que amplía su impacto social.

En este sentido, el modelo FBCEM se posiciona como una alternativa viable para transformar la enseñanza de la ciberseguridad, integrando tecnología, ética y formación crítica en un mismo marco educativo.

G. Implicancias éticas en la formación en ciberseguridad

La formación en ciberseguridad no puede limitarse al desarrollo de habilidades técnicas, ya que su ejercicio profesional tiene implicancias directas en la protección de personas, organizaciones e infraestructuras críticas. En los últimos años, la falta de una formación ética sólida en tecnología ha contribuido a incidentes de alto impacto, tales como la exposición masiva de datos personales, ataques a sistemas de salud y vulneraciones de infraestructuras críticas.

En sectores sensibles como el ámbito sanitario, una brecha de seguridad puede comprometer no solo la confidencialidad de la información, sino también la integridad de los servicios, afectando directamente la vida de las personas. Estos escenarios evidencian que la ciberseguridad debe ser comprendida como una práctica profesional con responsabilidad social, donde el conocimiento técnico debe estar acompañado de principios éticos claros [15].

En este contexto, el modelo FBCEM incorpora la ética como un eje transversal del proceso formativo, promoviendo el uso responsable de herramientas, la comprensión del impacto social de la tecnología y la diferenciación entre prácticas legítimas (*ethical hacking*) y actividades maliciosas.

H. Implementación y Validación del Modelo FBCEM en un Entorno SOC basado en FOSS

Como parte del proceso de validación del modelo FBCEM (Figura 1), se implementó un entorno de ciberseguridad basado en un Centro de Operaciones de Seguridad (SOC) en laboratorio, utilizando herramientas de Software Libre (FOSS). Este entorno permitió operacionalizar la Etapa 4 del modelo (Ciberseguridad SOC), enfocada en la detección, monitoreo y mitigación de amenazas en escenarios controlados.

Diseño e implementación del entorno SOC

El entorno fue desplegado mediante virtualización, integrando sistemas GNU/Linux y herramientas especializadas para la recolección, análisis y correlación de eventos de seguridad. Durante su implementación, los estudiantes realizaron actividades orientadas a la configuración de infraestructura, generación de eventos mediante ataques controlados y análisis de logs.

Las herramientas utilizadas en el entorno SOC se presentan en la Tabla VI.

TABLE VI
HERRAMIENTAS UTILIZADAS EN EL ENTORNO SOC BASADO EN FBCEM

Herramienta	Tipo	Función en el modelo	Justificación pedagógica
Wazuh	SIEM	Correlación de eventos	Permite análisis centralizado de logs
Suricata	IDS/IPS	Detección de amenazas	Facilita comprensión de tráfico de red
Kali Linux	Entorno de pruebas	Simulación de ataques	Uso controlado en ethical hacking
Ubuntu Server	Sistema base	Infraestructura	Entorno estable y configurable
VirtualBox	Virtualización	Laboratorio	Permite entornos seguros y replicables

Arquitectura del entorno

La arquitectura implementada responde a un modelo distribuido que integra generación de eventos, detección de intrusos, correlación y gestión centralizada, permitiendo simular el flujo completo de información dentro de un SOC.

Esta arquitectura se describe en la Tabla VII.

TABLE VII
ARQUITECTURA DEL ENTORNO SOC BASADO EN FBCEM

Componente	Tecnología	Función
Endpoint	Ubuntu/Linux	Generación de eventos
IDS/IPS	Suricata	Detección de tráfico

Componente	Tecnología	Función
SIEM	Wazuh	Correlación de eventos
Servidor	Linux Server	Gestión centralizada
Red virtual	VirtualBox	Simulación del entorno

El uso del SIEM basado en Wazuh permitió desarrollar capacidades clave como recolección de logs, correlación de eventos, generación de alertas y visualización de información, tal como se resume en la Tabla VIII.

TABLE VIII
CAPACIDADES DEL SIEM EN EL ENTORNO FBCEM

Funcionalidad	Descripción	Aplicación educativa
Recolección de logs	Centralización de eventos	Análisis de sistemas
Correlación	Relación entre eventos	Detección de incidentes
Alertas	Notificación automática	Interpretación de amenazas
Visualización	Dashboards	Comprensión operativa

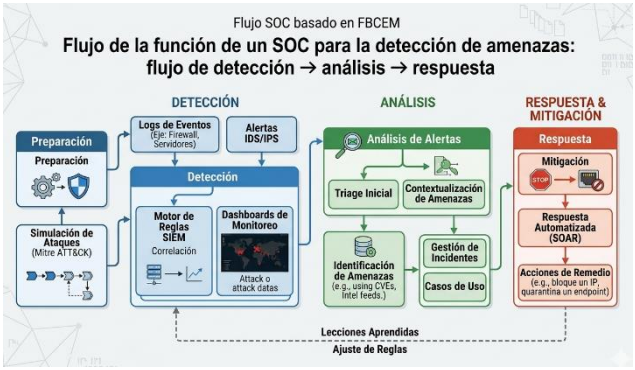
Validación mediante casos prácticos
La validación del modelo FBCEM se realizó mediante la implementación de dos casos prácticos dentro del entorno SOC, diseñados para evidenciar la aplicación progresiva de competencias en ciberseguridad.

Caso práctico 1: Implementación de entorno SOC básico. En este caso, los estudiantes configuraron la infraestructura virtual, instalaron sistemas GNU/Linux e implementaron el SIEM. Asimismo, generaron eventos de seguridad y realizaron el monitoreo de logs y alertas. Este escenario permitió comprender el funcionamiento general de un SOC y la importancia de la centralización de eventos.

Caso práctico 2: Detección y mitigación de amenazas. En este caso, se incorporaron capacidades avanzadas mediante la implementación de un sistema IDS/IPS como Suricata, permitiendo el análisis de tráfico de red, la identificación de patrones anómalos y la correlación de eventos. Esta fase incluyó la aplicación de medidas de mitigación, abordando el ciclo completo de la ciberseguridad.

La ejecución de ambos casos se apoya en herramientas de monitoreo y visualización, como se muestra en la Figura 2, donde se presenta un dashboard del SIEM que integra métricas de eventos, cumplimiento normativo y análisis de amenazas.

Fig. 5. GRÁFICO SOC / DETECCIÓN flujo de detección → análisis → respuesta



La Fig. 5 representa el flujo de detección y respuesta implementado en el entorno SOC, evidenciando el proceso de análisis de eventos, identificación de amenazas y mitigación.

Análisis de resultados
La implementación evidenció una progresión significativa en el desarrollo de competencias. Mientras el primer caso permitió una comprensión operativa del entorno SOC, el segundo fortaleció habilidades relacionadas con el análisis de incidentes y la toma de decisiones.

Los resultados observados se resumen en la Tabla IX.

TABLE IX
RESULTADOS OBSERVADOS EN LA IMPLEMENTACIÓN DEL MODELO FBCEM

Indicador	Resultado observado
Comprensión de logs	Alta
Detección de amenazas	Alta
Análisis de incidentes	Media-Alta
Uso autónomo de herramientas	Alta
Conciencia ética	Alta

Con el objetivo de comparar el impacto formativo del modelo propuesto frente a enfoques tradicionales, se presenta un análisis comparativo multidimensional basado en criterios como autonomía tecnológica, comprensión de sistemas, capacidades técnicas y formación ética.

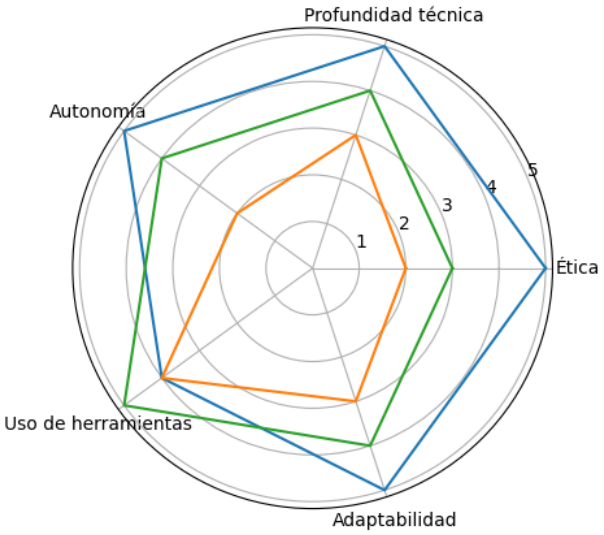


Fig. 6. Comparación multidimensional entre FBCEM, CEH y OSCP

La Fig. 6 muestra un gráfico radar donde se evidencia que el modelo FBCEM presenta un desempeño superior en dimensiones relacionadas con la formación integral.

Síntesis de validación del modelo

En conjunto, la implementación del entorno SOC y la ejecución de los casos prácticos confirman la efectividad del modelo FBCEM como una estrategia formativa integral. La articulación entre las etapas del modelo (Figura 1) y su aplicación práctica mediante herramientas FOSS permite desarrollar competencias técnicas, analíticas y éticas alineadas con los requerimientos actuales de la ciberseguridad [15], [16], [17], [18].

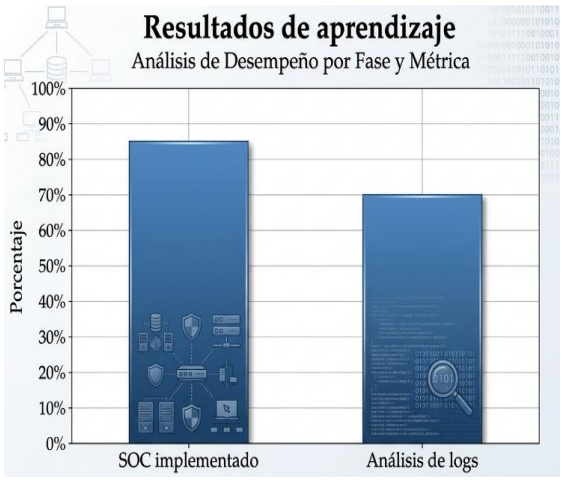


Fig. 7. Evaluación de los resultados de aprendizaje y desempeño en las fases de implementación y análisis del SOC.

La Fig. 7 presenta los porcentajes de éxito obtenidos tras la ejecución del modelo propuesto. Se observa que la fase de "SOC implementado" alcanzó un 85%, mientras que la capacidad de "Análisis de logs" se situó en un 70%. Estos resultados cuantitativos sugieren que la arquitectura es funcional y posee una alta viabilidad operativa para la gestión de eventos de seguridad.

V. LIMITACIONES DEL ESTUDIO

El estudio presenta limitaciones asociadas a su enfoque cualitativo y al uso de entornos controlados. La ausencia de métricas cuantitativas limita comparaciones estadísticas, y la falta de seguimiento longitudinal impide evaluar impacto a largo plazo.

Asimismo, la implementación del modelo depende del contexto institucional y del nivel de formación docente.

VI. CONCLUSIONES.

El modelo FBCEM constituye una propuesta formativa integral que articula tecnología, ética y práctica en ciberseguridad.

Los resultados evidencian mejoras en competencias técnicas, análisis de amenazas y autonomía tecnológica, así como una mayor conciencia ética.

La implementación de entornos SOC permite trasladar la teoría a la práctica, fortaleciendo la preparación profesional.

El modelo es replicable y adaptable, representando una alternativa viable para la enseñanza de la ciberseguridad.

Se recomienda incorporar métricas cuantitativas y estudios longitudinales en futuras investigaciones.

AGRADECIMIENTO/RECONOCIMIENTO

Agradezco a las diferentes comunidades de software libre y a los espacios académicos donde realice la labor docente y se desarrolló la experiencia docente que dio origen a este trabajo.

REFERENCIAS

[1] Richard Stallman, “Free Software, Free Society: Selected Essays,” GNU Press, 2002.

[2] Free Software Foundation, “The Free Software Definition,” 2023. [Online]. Available: https://www.gnu.org/philosophy/free-sw.html

[3] E. S. Raymond, “The Cathedral and the Bazaar,” O’Reilly Media, 2001.

[4] EC-Council, “Certified Ethical Hacker (CEH),” 2024. [Online]. Available: https://www.eccouncil.org/

[5] Offensive Security, “Offensive Security Certified Professional (OSCP),” 2024. [Online]. Available: https://www.offsec.com/

[6] National Institute of Standards and Technology, “Computer Security Incident Handling Guide,” NIST SP 800-61 Rev. 2, 2012.

[7] MITRE Corporation, “MITRE ATT&CK Knowledge Base,” 2024. [Online]. Available: https://attack.mitre.org/

[8] Wazuh, “Wazuh Documentation,” 2024. [Online]. Available: https://documentation.wazuh.com/

[9] Open Information Security Foundation, “Suricata IDS Documentation,” 2024. [Online]. Available: https://suricata.io/

[10] Linux Foundation, “The Linux Kernel Documentation,” 2023. [Online]. Available: https://www.kernel.org/doc/

[11] Open Source Initiative, “The Open Source Definition,” 2023. [Online]. Available: https://opensource.org/osd

[12] IEEE, “IEEE Editorial Style Manual,” 2022.

[13] ACM, “Code of Ethics and Professional Conduct,” 2018. [Online]. Available: https://www.acm.org/code-of-ethics

[14] European Union Agency for Cybersecurity (ENISA), “European Cybersecurity Skills Framework,” 2022. [Online]. Available: https://www.enisa.europa.eu/

[15] National Institute of Standards and Technology, “Cybersecurity Framework (CSF) 2.0,” NIST, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[16] National Institute of Standards and Technology, “Computer Security Incident Handling Guide,” NIST SP 800-61 Rev. 2, 2012.

[17] MITRE Corporation, “MITRE ATT&CK Framework,” 2024. [Online]. Available: https://attack.mitre.org/

[18] SANS Institute, “Building and Running a Security Operations Center (SOC),” 2023. [Online]. Available: https://www.sans.org/

[19] D. A. Kolb, “Experiential Learning: Experience as the Source of Learning and Development,” 2nd ed., Pearson, 2015.

[20] C. E. Hmelo-Silver, “Problem-Based Learning: What and How Do Students Learn?” Educational Psychology Review, vol. 16, no. 3, pp. 235–266, 2004.