CONESCAPANHONDURAS2025paper65.pdf

Institute of Electrical and Electronics Engineers (IEEE)

Document Details

Submission ID
trn:oid:::14348:477758459

Submission Date
Jul 31, 2025, 11:25 PM CST

Download Date
Aug 12, 2025, 2:43 PM CST

File Name
CONESCAPANHONDURAS2025paper65.pdf

File Size
95.2 KB

6 Pages

4,466 Words

27,104 Characters

13% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Top Sources

12% Internet sources
7% Publications
0% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Top Sources

12% Internet sources
7% Publications
0% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
es.scribd.com		1%
2	Internet	
risti.xyz		<1%
3	Internet	
www.coursehero.com		<1%
4	Internet	
espanol.libretexts.org		<1%
5	Internet	
koreascience.kr		<1%
6	Publication	
Khaled Salah, Mohammad Hammoud, Sherali Zeadally. "Teaching Cybersecurity ...		<1%
7	Publication	
Ines Aubel, Sebastian Zug, Andre Dietrich, Johannes Nau et al. "Adaptable Digital ...		<1%
8	Internet	
www.slideshare.net		<1%
9	Publication	
Saif Al-Dean Qawasmeh, Ali Abdullah S. AlQahtani, Muhammad Khurram Khan. "...		<1%
10	Internet	
pages.mtu.edu		<1%
11	Publication	
Buckley, Sarah. "An Analysis and Ontology of Teaching Methods in Cybersecurity ...		<1%

12 Internet

ts.riss.kr <1%

13 Internet

www.google.com <1%

14 Publication

Ali Vafaei-Zadeh, Davoud Nikbin, Kit Yik Teoh, Haniruzila Hanifah. "Cybersecurity ... <1%

15 Internet

www.byronvargas.com <1%

16 Internet

de.slideshare.net <1%

17 Internet

iucn.org <1%

18 Internet

podyssey.fm <1%

19 Publication

Sandra N. Koch, Sheila M. F. Torres, Sandra Diaz, Sophie Gilbert, Aaron Rendahl. "... <1%

20 Internet

www.es.amnesty.org <1%

21 Internet

www3.gobiernodecanarias.org <1%

22 Internet

banguat.gob.gt <1%

23 Internet

catalog.gfcmsu.edu <1%

24 Internet

e-pri4all.erasmus.site <1%

25 Internet

idus.us.es <1%

26 Internet
papers.academic-conferences.org <1%

27 Internet
worldwidescience.org <1%

28 Internet
www.desertfishes.org <1%

29 Publication
S. Carber. "Commonalities in IB practice and the Schoolwide Enrichment Model", J... <1%

30 Internet
bibdigital.epn.edu.ec <1%

31 Internet
gly.uzz.mybluehost.me <1%

32 Internet
libros.cecar.edu.co <1%

33 Internet
pesquisa.teste.bvsalud.org <1%

34 Internet
repositorio.udec.cl <1%

35 Internet
repositorio.uotavalo.edu.ec <1%

36 Internet
www.nordakademie.de <1%

Aprendizaje basado en casos y virtualización: Potenciando el análisis forense digital.

***Resumen*—Durante este trabajo de graduación se aborda la necesidad crítica y necesaria de fortalecer las habilidades prácticas en ciberseguridad y análisis de la forense digital en los estudiantes de pregrado. Para ello, se propone una metodología de aprendizaje útil e innovadora conocida como "basada en casos"(CBL), con la cual, se integran entornos virtuales controlados y herramientas forenses de código abierto o freeware. El estudio realizado fue implementado mediante la utilización de un enfoque mixto con diseño cuasi-experimental, cuyos resultados evidenció un incremento significativo en las diversas competencias de los participantes para identificar, preservar y analizar la evidencia digital. Se concluye que los entornos realizados con un efoque de aprendiza basado en casos son una herramienta pedagógica altamente efectiva para el desarrollo de habilidades prácticas (especialmente, en esta área de la forense digital); además, este trabajo de graduación sienta las bases para futuras investigaciones que busquen amplíar la complejidad de los casos y mejorar la infraestructura virtual tecnológica utilizada.**

***Index Terms*—Ciberseguridad, Forense digital, Aprendizaje Basado en Casos (CBL), Entornos virtuales, Educación, Seguridad informática, Herramientas forenses.**

ÍNDICE

I. Introducción

I-A. Planteamiento del problema

La ciberseguridad se estableció como uno de los pilares fundamentales en la protección de los activos de información y continuidad de operaciones en diversas organizaciones; a pesar de ello, en el ámbito de la ciberseguridad como en el análisis forense digital existen desafíos significativos en la formación educativa de los estudiantes de pregrado. Muchos programas académicos se centran principalmente en una base teórica que, si bien es fundamental, puede resultar insuficiente para desarrollar las competencias prácticas que se consideran necesarias para la identificación, análisis y manejo de evidencias digitales e incidentes.

Los ataques de ciberseguridad como ransomware, phishing y fuga de datos, con el paso del tiempo y la evolución de la tecnología se han vuelto cada vez más sofisticados y exigen conocimiento práctico que muy pocas veces se consigue mediante los métodos tradicionales; por ello, la falta de metodologías pedagógicas que integran de manera efectiva la simulación de escenarios reales (o los más parecidos a estos) donde los estudiantes pueden practicar como realizar un triage y el correcto análisis de artefactos forenses digitales, evidencia la brecha entre la formación académica tradicional y las exigencias reales dentro del campo profesional.

Frente a este panorama, surge la necesidad y se hace indispensable el desarrollo de un entorno de aprendizaje práctico y accesible mediante la combinación de escenarios realistas, la integración de herramientas forenses especializadas y el uso de metodologías innovadoras como el aprendizaje basado en casos (CBL). Con este enfoque, se permite a los estudiantes de pregrado enfrentarse a incidentes de ciberseguridad a través del uso de máquinas virtuales creadas con artefactos preconfigurados fundamentados en situaciones que reflejan la complejidad del mundo real y que facilitan no solo la obtención de habilidades técnicas, sino también facilitan el desarrollo del análisis crítico y la toma de decisiones.

I-B. Antecedentes

En las últimas décadas, la educación en ciberseguridad ha experimentado una evolución muy notable con muchos cambios significativos, todos estos cambios fueron impulsados por la necesidad creciente de formar profesionales en el área que sean capaces de enfrentar situaciones e incidentes que cada vez se vuelven más complejos y sofisticados. Estudios recientes como "Case-based learning for cybersecurity leaders: A systematic review and research agenda" [1] de la Universidad de Melbourn, destaca la efectividad del uso de

CBL para potenciar habilidades críticas como el liderazgo y la resolución de problemas; dicho enfoque permite a los estudiantes y profesionales enfrentarse a escenarios realistas que promueven el pensamiento crítico mediante la aplicación práctica de los conocimientos teóricos adquiridos. De igual manera, la investigación "Using case studies to teach cybersecurity courses" [2] de la Universidad Tecnológica de Michigan, demuestra que utilizar el CBL en la enseñanza de la ciberseguridad ayuda a facilitar la comprensión de incidentes reales, mientras integra aspectos técnicos y legales.

En el campo del análisis forense digital, se reconoce la importancia de contar con laboratorios virtuales controlados y seguros que permitan reproducir incidentes y realizar análisis de evidencias de estos mismos; investigaciones como "Virtual laboratory environments: methodologies for educating cybersecurity researchers" [3] y "Cyber security teaching and learning laboratories: A survey" [4] evidencian el potencial y la relevancia que las máquinas virtuales tienen al momento de establecer agendas educativas que integren estas prácticas para simular escenarios de ciberseguridad sin exponer a los estudiantes a los riesgos y peligros que un entorno real podría llegar a presentar.

Por otro lado, las investigaciones "Digital forensics with open source tools" [5] y "Open source tools for digital forensic investigation: capability, reliability, transparency and legal requirements" [6] de la Universidad Kebangsaan Malaysia, exploran y reconocen el uso e integración de herramientas de código abierto para el análisis forense por su flexibilidad, transparencia y bajo costo, lo cual, permite el desarrollo de entornos didácticos replicables. De igual manera, para que estas herramientas puedan ser aprovechadas de manera efectiva en el ámbito educativo, es necesario adecuarlas pedagógicamente con metodologías como la gamificación y el aprendizaje adaptativo presentadas en investigaciones como "Educación en ciberseguridad mediante estrategias de Gamificación" [7] y "Increasing cybersecurity interest and self-efficacy through experiential labs" [8] de la Universidad del oeste de Georgia, muestran un impacto positivo en el interés y la autoeficacia de los estudiantes cuando se les presentan ejercicios prácticos.

En conjunto, estos antecedentes respaldan la necesidad de desarrollar un entorno de aprendizaje virtualizado que combine la simulación de escenarios realistas, la integración de herramientas de código abierto para el análisis forense y metodologías basadas en CBL.

I-C. Objetivo general

Desarrollar un entorno de aprendizaje basado en casos para el análisis forense digital en pregrado, creando e implementando casos de estudio práctico, integrando herramientas forenses especializadas, y evaluando su efectividad en la formación práctica de los estudiantes.

I-C1. Objetivos específicos:

a) Diseñar casos de estudio práctico basado en el enfoque Case-Based Learning en forense digital, apoyados en escenarios realistas sustentados en máquinas virtuales con artefactos preconfigurados y recursos especializados que simulen incidentes de seguridad.
b) Integrar un conjunto de herramientas de código abierto didácticas y forenses, para facilitar el análisis técnico de los casos, garantizando su compatibilidad, accesibilidad y aplicación en contextos educativos de pregrado.
c) Evaluar el impacto formativo y la efectividad práctica del entorno de aprendizaje, mediante pruebas piloto con estudiantes universitarios, midiendo la adquisición de competencias técnicas, la capacidad de análisis crítico y la transferencia de conocimientos a situaciones forenses reales.

II. Marco teórico

II-A. Aprendizaje basado en casos

El aprendizaje basado en caso o CBL (Case-Based Learning) por siglas en inglés puede ser referenciado por muchos nombres dependiendo de la literatura consultada, por ejemplo: "enfoque de estudio de caso", "estudio de caso", "aprendizaje experiencial y autoeficacia" o "aprendizaje basado en problemas". Por fines prácticos, nos referiremos a este como CBL.

En base a Shivapurkar, Bhatia y Ahmed [9], la implementación un CBL se puede encontrar predominantemente dentro del campo de la medicina. Por ejemplo, en 1969 la facultad de medicina de la Universidad McMaster introdujo este enfoque en un curso de medicina que se enfocaba en proporcionar a los estudiantes casos reales, con los cuales, se esperaba que los estudiantes investigaran y presentaran los hallazgos encontrados durante su próxima clase. Revelando que al utilizar este método en su programa posdoctoral los estudiantes podían identificar con mayor facilidad sus fortalezas y debilidades en áreas específicas de cada contenido.

El CBL es un enfoque de estudio y aprendizaje centrado en los estudiantes, basándose en escenarios de naturaleza hipotética o real que ayudan a los estudiantes a practicar la aplicación de conceptos teóricos en situaciones profesionales; dichos escenarios y su forma de realización, van desde los estudiantes practicando con casos que se les muestran como ejemplos hasta los estudiantes construyendo casos por ellos mismos [1]. Además, según establece Towhidi y Pridmore [8] este enfoque de aprendizaje experimental práctico permite a los estudiantes desarrollar la autoeficacia. Lo cual, es muy importante porque se ha descubierto que la autoeficacia percibida es un factor muy influyente en la toma de decisiones.

II-B. Metodologías y enfoques pedagógicos complementarios

La gamificación (también conocida como ludificación) consiste en transformar tareas técnicas que los estudiantes pueden encontrar tediosas y aburridas en desafíos lúdicos que sirven para motivar, comprometer y mejorar las experiencias educativas de los estudiantes. Esencialmente, es el proceso de enseñanza y aprendizaje que traslada el funcionamiento de los juegos a un ámbito educativo, aumentando el interés de los estudiantes promoviendo la comprensión teórica.

Pacheco, Staino y Sliafertas [7] centrándose en el uso de métodos de gamificación en el contexto de la educación en ciberseguridad, debido que, los juegos presentan un contexto seguro y controlado donde los estudiantes pueden aplicar sus

conocimientos de manera práctica y experimentar con la toma de decisiones; nos presentan dos dinámicas distintas utilizadas actualmente:

- ***Dinámicas basadas en ejercicios prácticos*** (también llamada simulación), por lo general estas dinámicas involucran situaciones reales específicas en contextos preestablecidos, donde se propone una consigna, se entregan los elementos básicos y el estudiante es evaluado por sus resultados, pudiendo recibir una retroalimentado a lo largo del proceso. Un ejercicio práctico puede considerarse como un juego si se establecen elementos clave como un sistema de puntos o tiempo límite.
- ***Dinámicas basadas en juegos***, por lo general incorpora un conjunto de limitaciones en forma de reglas y puntajes junto con una narrativa que permite desarrollar un escenario competitivo en el que existe la posibilidad de perder o ganar al no cumplir los objetivos definidos.

Seguidamente, Cai [2] nos expone como existe un creciente esfuerzo en materia de educación en ciberseguridad, que incluyen las pedagogías de enseñanza, materiales curriculares, plataformas de laboratorio y capacitación del personal docente con el fin de mejorar los resultados de aprendizaje de los estudiantes. Por ejemplo, se presentan planes de estudios para hackers y seguridad ofensiva, las competencias de hacking de ciberseguridad y hackathons son introducidas en iCTF; así como otros enfoques que incluyen el aprendizaje basado en juegos, el aprendizaje basado en proyectos, el aprendizaje basado en problemas y el aprendizaje basado en la investigación.

Finalmente, los autores Towhidi y Pridmore [8] nos presentan como desarrollaron un laboratorio de ciberseguridad de aprendizaje experiencial y práctico, en base a el modelo de Aprendizaje Experiencial de Kolb; el cual, se basa en el aprendizaje y como este es un proceso de creación de conocimiento a través de experiencias transformadoras. El aprendizaje efectivo ocurre cuando una persona progresa a través de un ciclo de cuatro etapas:

- ***Experiencia concreta***, consiste en vivir o experimentar una nueva experiencia.
- ***Observación reflexiva de la nueva experiencia***, consiste en revisar o reflexionar sobre la experiencia.
- ***Conceptualización abstracta***, consiste en aprender o extraer conclusiones de la experiencia y generar nuevas ideas.
- ***Experimentación activa***, consiste en probar o aplicar lo aprendido en una nueva situación.

II-C. Entornos virtuales para la educación

La virtualización se refiere a la implementación virtual de un dispositivo, sistema operativo o red; permitiendo el uso simultáneo de diferentes sistemas operativos en una sola máquina física, reduciendo los costes de hardware y software de una institución gracias a un uso más eficiente. Por ello, representa un gran beneficio para las instituciones de educación superior, ya que permite impartir clases de ciberseguridad en los mismos laboratorios físicos de uso general utilizados por otras clases [4].

Los entornos físicos están completamente limitados por el espacio y la disponibilidad de recursos, en contraste, los entornos virtuales son más accesibles y flexibles. Además, la personalización y adaptabilidad también varía en los entornos físicos, la personalización es más complicada debido a las limitaciones de logística y la necesidad de adaptar las actividades manualmente; en cambio, los entornos virtuales dentro de sus plataformas permiten ofrecer una experiencia más individualizada, personalizada y con un seguimiento detallado [7].

Por ello, Nance, Hay, Dodge et al. [3] nos presentan que las capacidades de los laboratorios virtuales que apoyan actividades educativas también son adecuadas para apoyar actividades de investigación, proporcionando a los investigadores lo siguiente:

- Un entorno de acceso remoto para realizar experimentos, análisis y generar informes.
- Un entorno que puede aislarse tanto para proteger a terceros como para restringir el acceso público a la propiedad intelectual y la metodología durante su fase de desarrollo.
- La capacidad de implementar y redistribuir rápidamente recursos informáticos sin necesidad de comprar, instalar, reconfigurar hardware, software o redes.
- Soporte para realizar capturas instantáneas de entornos completos para reproducir experimentos y repetirlos desde un punto de partida definido utilizando diferentes parámetros.

Según Topham, Kifayat, Younis et al. [4] cualquier laboratorio de ciberseguridad debe satisfacer las siguientes necesidades del proceso de enseñanza:

- Los laboratorios deben brindar la flexibilidad necesaria para implementar ejercicios creativos.
- Los ejercicios se deben poder implementar de forma rápida y sencilla para varios estudiantes.
- Todas las máquinas y software del laboratorio deben estar aislados de las redes externas.
- Debe ser posible otorgar permisos de administrador a los estudiantes para cualquier VM que se les asigne; esto es importante para ciertos experimentos.
- Se debe proporcionar almacenamiento y copias de seguridad para que los estudiantes puedan realizar un progreso continuo en su trabajo, así como restaurar los sistemas en caso de errores.

II-D. Ciberseguridad y forense digital

II-D1. Ciberseguridad: Debemos tener en cuenta que una amenaza en ciberseguridad es cualquier evento, acción o circunstancia con el potencial de causar daño a sistemas, redes o datos; debemos tener en cuenta que estas pueden ser de origen natural, accidental o intencional. Luego tenemos a los actores de amenaza, donde un individuo, grupo u organización se aprovecha de las amenazas para comprometer los activos digitales.

Las amenazas no siempre implican malicia, pero su existencia resalta la necesidad de identificar vulnerabilidades y aplicar controles regulatorios para mitigar su impacto; donde

su gravedad dependerá de factores como la exposición del sistema y la probabilidad de que se materialicen. Seguidamente, identificar a los actores de amenaza ayuda a anticipar, planear y diseñar tácticas de defensa específicas.

II-D2. Forense digital: En algún momento, el término *forense digital* se consideraba sinónimo de *informática forense*, pero ahora abarca todos los dispositivos capaces de almacenar datos digitales Oettinger [10].

La investigación forense digital se describe alternativamente y simultáneamente como un arte y una ciencia; donde, el uso de métodos científicamente derivados y probados para la preservación, recopilación, validación, identificación, análisis, interpretación, documentación y presentación de la evidencia digital derivada de fuentes digitales con el propósito de facilitar o promover la reconstrucción de eventos considerados delictivos, o ayudar a anticipar acciones no autorizadas que se demuestre que perturban las operaciones planificadas (Altheide y Carvey, 2011).

Por ello, el objetivo de cualquier examinación forense es encontrar hechos, con los cuales, el investigador revela la verdad de un suceso al descubrir y exponer los restos que han quedado en el sistema; donde estos restos son conocidos como *artefactos*. A estos restos a veces se les llama *evidencia* pero dado que los investigadores forense tratan frecuentemente con abogados por escrito, es preferible evitar el uso excesivo del término debido a sus connotaciones legales cargadas y su relación durante un procedimiento legal; debido que, usar este término a la ligera puede causar problemas al investigador, porque los artefactos son rastros que dejan tras de sí actividades y eventos, que pueden ser inofensivos o no [5].

La ética y responsabilidad legal en forense digital garantiza que los profesionales manejen la evidencia y datos con total integridad, confidencialidad y transparencia. Los investigadores deben adherirse a ciertos principios como la imparcialidad evitando conflictos de interés y a la no alteración de pruebas, asegurando que los hallazgos encontrados sean válidos en procesos administrativos/judiciales. Además, deben cumplir normativas como el Reglamento General de Protección de Datos (GDPR) de Europa o la Ley HIPAA en salud de Estados Unidos, que exigen la protección de la privacidad de la información durante investigaciones. Un error ético, como sería filtrar datos sensibles, no sólo invalida completamente una investigación, sino que también para el investigador puede derivar en sanciones legales o pérdida de credibilidad profesional.

III. Herramientas para forense digital

La fiabilidad y la integridad de los resultados obtenidos son aspectos cruciales e indispensables en la investigación forense digital, ya que la precisión y la credibilidad de la misma puede influir significativamente en el resultado final de los procedimientos legales o de investigaciones corporativas; por ello, para garantizar una correcta admisibilidad de la evidencia digital, las herramienta de código abierto/freeware utilizadas para recopilar, preservar y analizar la evidencia digital deben ser completamente precisas sin comprometer la integridad. Además, las herramientas de código abierto cuentan con su código fuente disponible públicamente, lo que permite a cualquier persona ver, usar, modificar o distribuir el código; donde este nivel de transparencia permite a los profesionales, investigadores y otras partes interesadas en la investigación comprender exactamente cómo funciona la herramienta, ayudando a garantizar que los métodos y técnicas utilizados en una investigación forense digital sean transparentes y estén abiertos al escrutinio, evitando posibles sesgos o inexactitudes en los resultados, aumentando la fiabilidad y credibilidad de la evidencia digital obtenida [6].

III-A. Herramientas forenses digitales propietarias vrs. de código abierto

Cuando se adquieren herramientas forenses digitales propietarias no solo es necesario adquirirlas, sino que los proveedores suelen cobrar una tarifa de renovación de licencia anual por uso y/o usuarios; este costo representa una carga para las agencias al tener que continuar sus operaciones y mantener el laboratorio de investigación cuando en comparación, las herramientas de código abierto pueden definirse como software libre que no limita el uso y/o usuarios resultando en costos mínimos o ningún costo. Las herramientas presentan capacidades y limitaciones únicas y variables, destacando que las herramientas de código abierto producen la misma precisión que las herramientas propietarias en términos de precisión y capacidad; sin embargo, las herramientas de código abierto pueden presentar una menor eficiencia al abordar la escalabilidad de los datos y podrían prolongar el proceso de investigación debido a las restricciones legales de cada país. Además, se destacan varios riesgos asociados al uso de código abierto, como la falta de soporte, documentación, actualizaciones o funciones de seguridad [6].

IV. Evaluación de competencias y métricas de aprendizaje en ciberseguridad

Los autores Karjalainen, Puuska y Kokkonen [11] explican que para gestionar los conocimientos prácticos en el ámbito de la ciberseguridad, el NIST creó la iniciativa nacional para la educación en ciberseguridad (NICE) (https://niccs.cisa.gov/workforce-development/nice-framework) como un marco de la fuerza laboral de ciberseguridad. Este marco NICE puede utilizarse para describir las competencias requeridas para diversos puestos de trabajo en ciberseguridad; su objetivo es unificar los conceptos y las taxonomías de empresas, industrias y proveedores de educación para las necesidades específicas de contenido cibernético en diferentes áreas de especialización. El marco también puede aplicarse para definir los contenidos necesarios de la competencia básica de habilidades cibernéticas y, por lo tanto, para desarrollar planes de estudio y contenido de 00cursos.

En consecuencia, durante este trabajo de graduación se ha utilizado el marco NICE, explicitamente en la categoría de trabajo de Investigación (IN) que contiene dos roles, cada uno conteniendo sus propia declaración de tareas, conocimientos y habilidades asociadas:

- ***Investigación de delitos cibernéticos (Cybercrime Investigation - IN-WRL-001)***, es la persona responsable de investigar incidentes y delitos de intrusión en

el ciberespacio; aplicando tácticas, técnicas y procedimientos para una amplia gama de herramientas y procesos de investigación, equilibrando adecuadamente las ventajas del enjuiciamiento frente a la recopilación de inteligencia, para mayor información consultar en: https://niccs.cisa.gov/workforce-development/nice-framework/work-role/cybercrime-investigation.

- ***Análisis de evidencia digital (Digital Evidence Analysis - IN-WRL-002)***, es la persona responsable de identificar, recopilar, examinar y preservar evidencia digital utilizando técnicas analíticas y de investigación controladas y documentadas, para mayor información consultar en: https://niccs.cisa.gov/workforce-development/nice-framework/work-role/digital-evidence-analysis.

Finalmente, para evaluar el aumento de conocimientos, Karjalainen, Puuska y Kokkonen [11] seleccionan un total de cinco preguntas que abordaban el nivel de conocimientos antes (pre-test) y después (post-test) de experimentar el ejercicio

V. Metodología

La investigación adoptó un enfoque mixto, combinando elementos cualitativos y cuantitativos para una comprensión integral del impacto del entorno de aprendizaje. El diseño fue cuasi-experimental, utilizando un grupo de estudiantes de pregrado con conocimientos básicos en informática como participantes. La metodología incluyó las siguientes fases:

1. **Diseño del caso de estudio:** Creación del escenario realista de incidentes de ciberseguridad (ej., ingeniería social, phishing, ransomware) con artefactos digitales preconfigurados.
2. **Configuración de entornos virtuales:** Implementación de máquinas virtuales (Windows 10, Debian server, Fedora workstation) en Oracle VirtualBox para simular los sistemas afectados.
3. **Integración de herramientas forenses:** Selección y configuración de herramientas de código abierto esenciales para el análisis (ej., FTK Imager, Autopsy, Eric Zimmerman's tools, KAPE).
4. **Evaluación:** Utilización de pre-tests y post-tests para medir el conocimiento inicial y la mejora de competencias, complementados con rúbricas para evaluar habilidades prácticas y cuestionarios para obtener percepciones cualitativas de los estudiantes.

El procedimiento consistió en la introducción del caso, la fase de análisis por parte de los estudiantes en el entorno virtual y la posterior evaluación de sus resultados y comprensiones.

VI. Resultados

Durante este trabajo de graduación se demostró el correcto acierto y beneficio de utilizar el enfoque de aprendizaje práctico del Aprendizaje Basado en Casos (CBL) para desarrollar las habilidades de los estudiantes universitarios de pregrado en la informática forense. Las comparaciones previas y posteriores a la prueba (obtenidas de los pre-test y post-test) mostraron una mejora notable y significativas en las habilidades, confianza y seguridad de los estudiantes durante la identificación, preservación y análisis de la evidencia forense en eventos de ciberseguridad. A pesar de los obstáculos iniciales experimentados, los estudiantes demostraron que adquirieron valiosas habilidades prácticas; esto confirma los beneficios e importancia tanto del método de aprendizaje practico del CBL como del uso de entornos virtuales controlados para la formación en ciberseguridad y forense digital.

VII. Discusión

Los resultados de la investigación coinciden con la literatura existente presentada durante el marco teórico que defiende las estrategias educativas prácticas; con la cual, se resalta la idea de que los métodos como el Aprendizaje Basado en Casos es vital para la enseñanza y aprendizaje en campos altamente técnicos como puede ser la forense digital. Por ello, la capacidad de replicar y simular incidentes de seguridad y utilizar software real en un entorno gestionado y seguro para los estudiantes ha demostrado ser fundamental para desarrollar las habilidades buscadas y requeridas en el mercado laboral.

Sin embargo, se observaron algunas limitaciones durante la creación y configuración del entorno; entre ellas, la demanda de poder de computo de sistemas informáticos con computadoras de alto procesamiento para realizar eficazmente el procesamiento forense de imágenes y la pronunciada curva de aprendizaje inicial asociada con la utilización de algunos programas. A pesar de estas dificultades, el resultado y la principal contribución de la investigación es la aplicación de un marco de aprendizaje activo a la investigación forense digital y la validación de una combinación eficaz de herramientas de acceso fácil y cómodo para los estudiantes.

VIII. Conclusiones y recomendaciones

VIII-A. Conclusiones

La conclusión final de este trabajo de graduación consiste en que establecer y utilizar un entorno educativo práctico con máquinas virtuales y software de código abierto/freeware son una estrategia eficaz para mejorar las habilidades de análisis forense digital entre estudiantes universitarios; por esto mismo, los resultados obtenidos del trabajo de graduación demuestran que se cumplió con los objetivos planteados al inicio, lo que se traduce en un crecimiento claro y cuantificable de las habilidades de los participantes.

VIII-B. Recomendaciones

A partir de los resultados y las lecciones aprendidas de la investigación, se sugieren las siguientes acciones y consideraciones a futuro:

1. **Crear materiales de incorporación completos:** Producir guías y tutoriales detallados, paso a paso, sobre cómo configurar el entorno de aprendizaje y utilizar las herramientas esenciales, lo que ayudará a simplificar la curva de aprendizaje inicial para los nuevos usuarios.
2. **Ampliar la variedad de casos prácticos:** Desarrollar una colección más amplia de casos prácticos que incluya diversos niveles de dificultad y diferentes tipos de amenazas de ciberseguridad, como malware, fraude financiero y/o análisis de tráfico de red.

3. **Explorar la integración de herramientas comerciales:** Introducir gradualmente software forense estándar en el currículo para familiarizar a los estudiantes con las herramientas comerciales a medida que avanzan en sus estudios.
4. **Realizar estudios de mayor alcance:** Iniciar estudios/pruebas a largo plazo que incluyan grupos de control para confirmar estos hallazgos a mayor escala y evaluar los efectos a largo plazo de la metodología.
5. **Optimizar la infraestructura tecnológica:** Evaluar y actualizar la configuración del sistema para acelerar el análisis de evidencia y garantizar que pueda ampliarse para brindar soporte a más estudiantes.

Referencias

[1] A. Anderson, A. Ahmad y S. Chang, "Case-Based Learning for Cybersecurity Leaders: A Systematic Review and Research Agenda," *Information & Management*, pág. 104 015, 2024.

[2] Y. Cai, "Using case studies to teach cybersecurity courses," *Journal of Cybersecurity Education, Research and Practice*, vol. 2018, n.º 2, pág. 3, 2018.

[3] K. Nance, B. Hay, R. Dodge, A. Seazzu y S. Burd, "Virtual laboratory environments: Methodologies for educating cybersecurity researchers," *Methodological Innovations Online*, vol. 4, n.º 3, págs. 3-14, 2009.

[4] L. Topham, K. Kifayat, Y. A. Younis, Q. Shi y B. Askwith, "Cyber security teaching and learning laboratories: A survey," *Information & Security*, vol. 35, n.º 1, pág. 51, 2016.

[5] H. Carvey y C. Altheide, *Digital forensics with open source tools*. Elsevier, 2011.

[6] I. Ismail y K. A. Z. Ariffin, "Open Source Tools for Digital Forensic Investigation: Capability, Reliability, Transparency and Legal Requirements," *KSII Transactions on Internet and Information Systems (TIIS)*, vol. 18, n.º 9, págs. 2692-2716, 2024.

[7] F. Pacheco, D. Staino y M. Sliafertas, "Educación en ciberseguridad mediante estrategias de Gamificación,"

[8] G. Towhidi y J. Pridmore, "Increasing cybersecurity interest and self-efficacy through experiential labs.," *Issues in Information Systems*, vol. 23, n.º 2, 2022.

[9] M. Shivapurkar, S. Bhatia e I. Ahmed, "Problem-based learning for cybersecurity education," en *Journal of The Colloquium for Information Systems Security Education*, vol. 7, 2020, págs. 6-6.

[10] W. Oettinger, *Learn Computer Forensics: Your one-stop guide to searching, analyzing, acquiring, and securing digital evidence*, 2.ª ed. Packt Publishing, 2022.

[11] M. Karjalainen, S. Puuska y T. Kokkonen, "Measuring learning in a cyber security exercise," en *Proceedings of the 12th International Conference on Education Technology and Computers*, 2020, págs. 205-209.