



Universidad Autónoma del Estado de México

Centro Universitario UAEM Valle de Chalco

PLATAFORMA DE SIMULACIÓN EN CIBERSEGURIDAD PARA LA CAPACITACIÓN DE ESTUDIANTES UNIVERSITARIOS

T E S I S

QUE PARA OBTENER EL GRADO DE

MAESTRO EN CIENCIAS DE LA COMPUTACIÓN

P R E S E N T A

ING. KEVIN GYOVANI RAMIREZ VITE

DIRECTORA

DRA. ANABELEM SOBERANES MARTIN

CO-DIRECTOR

DR. SAMUEL OLMOS PEÑA

TUTORA

DRA. MAGALLY MARTÍNEZ REYES

VALLE DE CHALCO SOLIDARIDAD, MÉXICO SEPTIEMBRE 2025.



CUVCH

**PLATAFORMA DE SIMULACIÓN EN
CIBERSEGURIDAD PARA LA CAPACITACIÓN
DE ESTUDIANTES UNIVERSITARIOS**

RESUMEN

El presente estudio documenta el desarrollo, e implementación de una plataforma de simulación denominada CyberSimU, diseñada para fortalecer competencias técnicas en estudiantes universitarios, CyberSimU incorpora nueve simulaciones interactivas que reproducen escenarios prácticos en entornos controlados, que van desde el manejo de consolas en Linux y Windows hasta la detección y mitigación de ataques como denegación de servicio distribuido, sistemas comprometidos, *sniffing* de red, técnicas post-explotación, *phishing* y *ransomware*.

El desarrollo de la plataforma se realizó bajo el Proceso Unificado Simplificado (SUP), seleccionado por su idoneidad en proyectos con recursos humanos limitados, requerimientos de agilidad y mínima carga documental. El diseño instruccional se estructuró mediante el modelo ADDIE, asegurando una secuencia pedagógica que favorece el aprendizaje progresivo y la transferencia práctica de conocimientos.

La evaluación se llevó a cabo mediante un diseño cuasi-experimental con aplicación de *Pre-Test* y *Post-Test* de conocimientos generales en ciberseguridad a estudiantes de diversas instituciones. El análisis estadístico, basado en métricas descriptivas e inferenciales, evidenció un incremento significativo en los puntajes obtenidos tras la interacción con la plataforma. Adicionalmente, se aplicó una evaluación de funcionalidad siguiendo la norma ISO/IEC 25010, midiendo dimensiones de usabilidad, eficiencia y satisfacción, con resultados favorables en la mayoría de los indicadores.

El proyecto también contempló acciones de difusión y transferencia social del conocimiento, incluyendo ponencias y talleres en instituciones de educación básica, media y superior, así como la presentación de artículos en foros académicos especializados.

Los hallazgos confirman que CyberSimU es una herramienta viable para la enseñanza y evaluación de habilidades en ciberseguridad. Se propone como trabajo futuro la incorporación de escenarios de mayor complejidad, el uso de analítica avanzada para personalizar el entrenamiento y la ampliación de la plataforma a contextos no académicos, como la capacitación empresarial.

Palabras clave

ciberseguridad, simuladores educativos, aprendizaje basado en simulación, entrenamiento práctico, educación superior, ISO/IEC 25010, Proceso Unificado Simplificado, modelo ADDIE, evaluación de competencias, formación en seguridad informática

ABSTRACT

This research presents the design, development, and evaluation of CyberSimU, an educational cybersecurity simulation platform aimed at enhancing the training of higher education students. The platform incorporates nine interactive simulations that replicate realistic cyberattack and defense scenarios, enabling participants to acquire and strengthen practical skills in a controlled and pedagogical environment. The development followed the Simplified Unified Process (SUP) as the software development methodology, ensuring agility and minimal documentation requirements due to the single-developer nature of the project. Additionally, the ADDIE model was applied to guide the educational design, aligning learning objectives, simulation content, and evaluation strategies.

Functionality testing was conducted under the ISO/IEC 25010 standard, covering usability, functionality, efficiency, and user satisfaction, with participation from students, administrators, and experts. The platform's effectiveness was measured through pre- and Post-Tests in general cybersecurity knowledge applied to 48 students from three institutions, including a control group with prior knowledge in the subject. Statistical analyses both descriptive and inferential showed a significant improvement in performance, highlighting the pedagogical value of CyberSimU as a complementary tool in formal cybersecurity education.

The project not only contributes to the academic field through empirical evidence and methodological rigor but also to social outreach, having been disseminated in scientific forums, academic workshops, and training sessions in primary, secondary, and higher education institutions. This dual contribution underscores CyberSimU's potential for scalability, adaptation to different educational contexts, and integration into future research and doctoral studies.

Keywords

cybersecurity, educational simulators, simulation-based learning, practical training, higher education, ISO/IEC 25010, Simplified Unified Process, ADDIE model, skills assessment, information security training

ÍNDICE

1. INTRODUCCIÓN	15
1.1 ANTECEDENTES.....	16
Historia y evolución de la simulación en seguridad cibernética	17
Plataformas actuales y tendencias emergentes en simulación.....	20
Simuladores en la enfermería.....	21
Educación en ciberseguridad.....	22
Estrategia nacional de ciberseguridad en México.....	23
Frameworks para desarrollar entornos de realidad virtual	24
1.2 PLANTEAMIENTO DEL PROBLEMA	26
1.3 OBJETIVOS	27
General	27
Específicos.....	28
1.4 DELIMITACIÓN O ALCANCE DE LA INVESTIGACIÓN.....	28
Delimitación y alcances	28
Delimitación de la investigación	29
1.4 HIPÓTESIS	29
1.5 JUSTIFICACIÓN	29
2. MARCO TEÓRICO	32
Metodología aplicada para realizar la revisión sistemática	33
SALSA Framework	34
Búsqueda.....	35
Evaluación	37
Análisis	38
Síntesis	40
MARCO TEÓRICO	40

La ciberseguridad significa diferentes cosas a las personas	41
Concepto de ciberseguridad	42
Objetivos de la ciberseguridad.....	43
Clasificación de la ciberseguridad.....	45
Ataques gestados por los ciber delincuentes.....	46
DoS.....	47
Phishing.....	50
Malware	53
3. METODOLOGÍA	55
Investigación.....	56
Características de la investigación.....	56
Objetivos de la investigación.....	57
Desarrollo.....	57
Justificación de la elección del SUP	58
Aplicación del SUP en CyberSimU	58
Aplicación del modelo ADDIE en el diseño instruccional de las simulaciones	59
Justificación de uso del modelo ADDIE en CyberSimU	60
Aplicación de las fases de ADDIE.....	60
4. RESULTADOS.....	64
Elección del nombre CyberSimU	65
Opinión estudiantil sobre la importancia de la ciberseguridad en instituciones educativas.....	66
Grupo de control: Estudiantes con conocimientos previos en seguridad informática	67
Desarrollo del simulador	68
Descripción de simulaciones.....	69
Simulación 1: Introducción a consolas y comandos básicos.....	69

Simulación 2: Entrenamiento de Consolas en Windows	70
Simulación 3: Escaneo de Puertos con Nmap	71
Simulación 4: Ataques de Denegación de Servicio Distribuidos (DDoS)	72
Simulación 5: Sistema Comprometido	74
Simulación 6: Sniffing de Red	75
Simulación 7: Técnicas de evasión en post-explotación	76
Simulación 8: Simulador de Phishing	78
Simulación 9: Simulador de Ransomware	79
Participantes y contexto de evaluación	80
Resultados del Pre-Test y Post-Test	81
Análisis descriptivo de los puntajes obtenidos	83
Media Aritmética (μ)	83
Mediana (Me)	84
Desviación Estándar (σ)	84
Análisis Descriptivos de los resultados obtenidos	85
Análisis estadístico inferencial	86
Hipótesis del análisis	86
Resultados	86
Interpretación educativa	87
Evaluación de la plataforma mediante pruebas de funcionalidad	87
Instrumento aplicado	88
Análisis de satisfacción por dimensiones según ISO/IEC 25010	88
Análisis Cualitativo de Comentarios Abiertos	90
Interpretación de la gráfica	92
Difusión de los resultados y retribución social	92
Movilidad académica en la Universidad de Hildesheim	93

Cierre de la sección de Resultados	94
5 CONCLUSIONES Y TRABAJOS FUTUROS	96
6. REFERENCIAS DE CONSULTA.....	99
ANEXOS	108
ANEXO 1	109
Resultados de la encuesta.....	109
ANEXO 2	120
ANEXO 3	144
ANEXO 4	148
ANEXO 5	152
ANEXO 6	153
ANEXO 7	154
ANEXO 8	156

ÍNDICE DE FIGURAS

Figura 1. Primer Gusano informático 1988 (Malenkovich, 2023)	19
Figura 2. Datos expuestos en plataformas en los últimos años (McCandless, 2022).	23
Figura 3. Entorno de desarrollo de A-Frame (Campos, 2017).	25
Figura 4. Fases del SALSA Framework.	35
Figura 5. Pregunta al ChatGPT acerca de las palabras clave en la investigación. ...	37
Figura 6. Mejora de la ecuación solicitando la optimización de una ecuación de búsqueda.	37
Figura 7. Pregunta hecha al ChatGPT de acuerdo con el Abstract de un artículo candidato.....	38
Figura 8. Respuesta del ChatGPT respecto al abstract presentado.	39
Figura 9. Mendeley Reference Manager, ejemplo de organización de artículos.	39
Figura 10. Triada de la Seguridad (Ethical, 2014).	45
Figura 11. Ejemplo de ataque DDOS (Steinberg, 2019).	48
Figura 12. Ejemplo de ataques de Botnet, (Scott, 2020).	49
Figura 13. Ejemplo de Ransomware en equipo infectado, (Vanderbilt, 2020).	50
Figura 14. Ejemplo de Phising, (University, 2021).	52
Figura 15. Ejemplo de ataque del hombre en Medio (Steinberg, 2019).	53
Figura 16. Metodología ADDIE dentro de CyberSimU.	61
Figura 17. Cuestionario Pre-test aplicado a estudiantes universitarios.	62
Figura 18 Cuestionario Post-Test aplicado a estudiantes universitarios	62
Figura 19. Cuestionario de Funcionalidad de acuerdo con ISO/IEC 25010.	63
Figura 20 Logotipo CyberSimU	65
Figura 21. Resultados de encuesta de participación de estudiantes sobre temas relacionados a ciberseguridad.	66
Figura 22. Sitio principal de CyberSimU para ejecución de simulaciones.....	68

Figura 23. ejemplo de simulación de la línea de comandos en Linux.	70
Figura 24. Simulación de Entrenamiento de Consolas Windows.	71
Figura 25. Simulador de Escáner de Puertos Nmap.	72
Figura 26. Simulador de ataque DDos en funcionamiento.	74
Figura 27. Simulación de Sistema Comprometido.	75
Figura 28. Sniffing de Red en funcionamiento.	76
Figura 29. Simulación de Post Explotación en funcionamiento.	78
Figura 30. Reconociendo y mitigando Phising, simulador en funcionamiento.....	79
Figura 31. Comparación de puntajes de Pre-Test y Post-Test.....	82
Figura 32. Comparación general de promedios entre las pruebas Pre-Test y Post-Test.	82
Figura 33. Mejora individual entre resultados Pre-Test y Post-Test.....	83
Figura 34. Formula de media aritmética.....	84
Figura 35. formula mediana cuando n es impar.	84
Figura 36. Formula mediana cuando n es par.....	84
Figura 37. Formula de la desviación estándar.	85
Figura 38. Evidencia del formulario de pruebas de funcionalidad de CyberSimU....	88
Figura 39. Gráfico de evaluación por dimensiones ISO/IEC 25010.	90
Figura 40. Gráfico de clasificación de comentarios abiertos.	91

1. INTRODUCCIÓN

En este capítulo, se contextualiza la importancia de los simuladores en diferentes contextos, ya que se abordan tópicos referentes al área de ciberseguridad, así como es que estos tienen diferentes aplicaciones en otras áreas importantes de la investigación y desarrollo, se presenta una narrativa acerca de la evolución de los temas de esta investigación y su impacto dentro de la educación.

1.1 ANTECEDENTES

La rápida evolución de las amenazas cibernéticas y la necesidad de formar a profesionales altamente capacitados en seguridad informática han impulsado la investigación y el desarrollo de herramientas educativas avanzadas, dentro de este contexto, el desarrollo de una " plataforma de simulación en ciberseguridad para la capacitación de estudiantes universitarios" surge como una respuesta innovadora para abordar los desafíos en la formación de expertos en ciberseguridad.

La realidad virtual ofrece la posibilidad de crear escenas simuladas interactivas que permiten sumergirse en entornos virtuales realistas generando situaciones de seguridad ofensiva como métodos y tácticas que podrían ser usados por un adversario real esta simulaciones proporcionan un lugar seguro que permite a los estudiantes practicar y explorar diversos contextos enfrentándose a situaciones prácticas y desafiantes que podrían suscitarse en su futura trayectoria profesional (Villena-Taranilla et al., 2025) .

La creación de una plataforma que promueva la participación de estudiantes usando un modelo pedagógico que permita aumentar la motivación y mejorar la comprensión de conceptos de seguridad ofensiva interactividad e inmersión de realidad virtual generando una experiencia de aprendizaje envolvente y memorable que permita a los estudiantes practicar y desarrollar habilidades para adquirir un conocimiento más profundo del tema (Rohan et al., 2023).

La presente investigación se ubica en el ámbito de la educación específicamente en el campo del cómputo aplicado a la educación y sistemas de

información abarcando la tecnología educativa y el uso de realidad virtual como alternativa para la capacitación en instituciones de educación superior la realidad virtual se usa para crear escenas simuladas interactivas dentro de entornos web que permiten a estudiantes experimentar y practicar situaciones de seguridad ofensiva con el objetivo de mejorar la comprensión de conceptos desarrollar habilidades prácticas y preparar a los estudiantes para su futura carrera profesional en el campo de la ciberseguridad.

Además, se enfoca en el análisis del impacto que tendrá el desarrollo de una plataforma de realidad virtual en la capacitación profesional de los alumnos en instituciones universitarias del oriente del Estado de México, este análisis se centra en aspectos como la toma de decisiones al momento de resolver los problemas presentados dentro de un simulador, a través de la investigación, se busca evaluar cómo la realidad virtual a través de plataformas de simulación distribuida puede mejorar el aprendizaje y preparar de manera efectiva a los estudiantes para su futuro desempeño profesional en el campo de la seguridad ofensiva (Prümmer et al., 2024).

Historia y evolución de la simulación en seguridad cibernética

El uso de simuladores en el ámbito de la seguridad cibernética tiene sus raíces en la necesidad de proporcionar a los estudiantes experiencias prácticas que imiten de cerca los desafíos del mundo real, a lo largo de las décadas se han desarrollado diversas herramientas para simular escenarios de ataques cibernéticos, pero es necesario con el surgimiento de nuevos vectores de ataques que existan medios de capacitación que se adecuen de manera rápida y efectiva a las razones que mueven a los ciberdelincuentes a atacar a los sistemas, es por ello que actualmente se crean entornos de laboratorio virtual hasta simuladores más avanzados que incorporan inteligencia artificial.

Históricamente, la formación en seguridad cibernética se ha basado en enfoques teóricos y prácticos, pero la simulación distribuida ha ganado relevancia debido a su capacidad para recrear entornos complejos y desafiantes, la simulación distribuida permite a los estudiantes interactuar con escenarios realistas desde

ubicaciones dispersas sin la necesidad de tener un *hardware* robusto para poder ejecutar las diversas secuencias simuladas, de esta manera brindando una experiencia de aprendizaje más inmersiva y adaptada a las demandas del mundo moderno, a continuación se presenta un recuento a lo largo del siglo XX de cómo han evolucionado los simuladores (Ashtiani & Abdollahi Azgomi, 2014).

Durante la década de los 70s se presentaron los primeros pasos en la simulación cibernética durante estos años la seguridad cibernética no era una preocupación principal y las simulaciones se centraban en el desarrollo de sistemas informáticos las primeras herramientas se usaron para modelar el comportamiento de sistemas de información y evaluar su rendimiento

En los 80s surgieron las amenazas cibernéticas y las simulaciones comenzaron a incorporar escenarios de ataques de virus informáticos, así como gusanos se presentó el famoso gusano Morris de 1988 ver Figura 1, despertando la conciencia sobre la importancia de simular amenazas en entornos controlados para comprender y combatir estos eventos

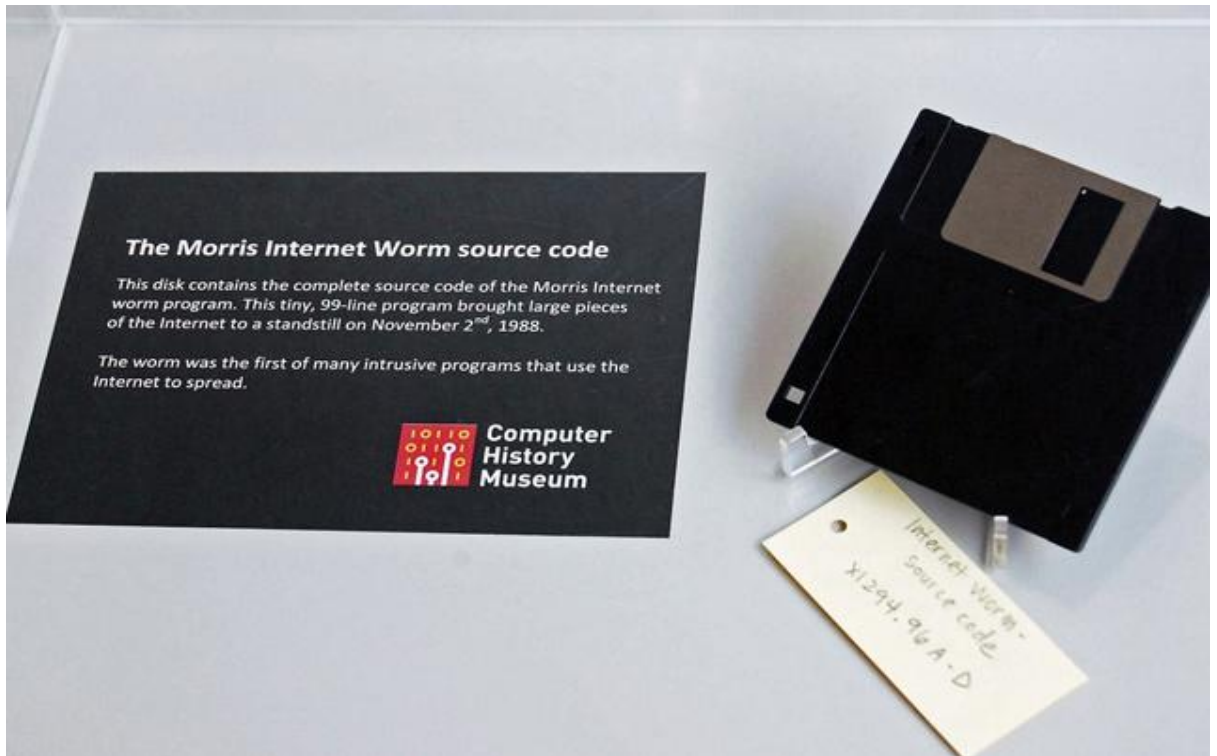


Figura 1. Primer Gusano informático 1988 (Malenkovich, 2023)

Década de 90's: Desarrollo de herramientas de simulación más especializadas, el campo de la seguridad cibernética experimentó un rápido crecimiento, surgieron herramientas más especializadas que permitían la simulación de ataques específicos, como escáneres de vulnerabilidades y simuladores de intrusos. Sin embargo, estas herramientas aún no estaban completamente integradas en entornos de formación y educación.

Para los años 2000 se aumentaron los ataques sofisticados, así como la dependencia tecnológica por lo que el enfoque se centró en la simulación en tiempo real y así en el campo de la seguridad comenzaron a surgir plataformas de simulación avanzadas que permitían a los profesionales practicar en entornos virtuales que simulaban situaciones del mundo real

Para la década de los 2000's la simulación distribuida y aplicación de inteligencia artificial se ha vuelto más prominente, permitiendo la colaboración de estudiantes y profesionales en entornos virtuales complejos, además, la aplicación de inteligencia artificial en la simulación cibernética ha mejorado la autenticidad de los escenarios al permitir la emulación de comportamientos de adversarios virtuales más realistas y dinámicos.

Finalmente, en la década de los 2020 se desarrollaron tecnologías emergentes y desafíos incesantes para áreas como la simulación de la seguridad cibernética que ha evolucionado con la integración de tecnologías como el aprendizaje automático la inteligencia artificial y la realidad virtual permitiendo contar con simulaciones avanzadas en las cuales aún persisten desafíos de creación de entornos que reflejen con precisión las amenazas cibernéticas actuales.

A lo largo de la historia, la simulación en diversas áreas de especialización y de la seguridad informática ha pasado de ser una herramienta sencilla de modelado a convertirse en una parte compleja para la formación y el desarrollo de habilidades en el ámbito de la ciberseguridad, el continuo avance tecnológico seguirá dando forma a la evolución futura de la simulación cibernética.

Plataformas actuales y tendencias emergentes en simulación

Actualmente hay varias plataformas para la simulación de seguridad cibernética, pero la mayoría está centrada en entornos cerrados o simulaciones aisladas, sin embargo la tendencia apunta hacia la simulación distribuida que permite la colaboración de los participantes en diversas ubicaciones geográficas, generando la cooperación para la resolución de problemas, además de la integración de inteligencia artificial en plataformas de simulación es cada vez más común permitiendo mejorar la autenticidad de escenarios y producir adversarios virtuales adaptables.

Derivado de estos desarrollos se identifica la importancia de simular amenazas cibernéticas más sofisticadas y dinámicas, lo cual genera desafíos para la implementación de plataformas de simulación distribuidas enfocadas a la capacitación de ataques cibernéticos en instituciones de educación superior. La presente investigación busca abordar estos desafíos y contribuir con el desarrollo de

esa área, generando soluciones educativas efectivas y enfocadas a las demandas actuales de la ciberseguridad.

Simuladores en la enfermería

La simulación como método de aprendizaje se ha ido extendiendo a diversas áreas como en la enfermería, los laboratorios de habilidades se han ido instaurando como una modalidad de aprendizaje para el desarrollo de habilidades y conocimiento sin depender de prácticas clínicas. Existen simulaciones simples de baja fidelidad hasta otras muy complejas y versátiles que pueden adaptarse para la formación de enfermeras principiantes o experimentadas, planteando una amplia gama de situaciones clínicas. (Padilha et al., 2019).

Bajo esta forma de aprendizaje se usan recursos como juegos de roll, maniqués y pacientes simulados que permiten desarrollar las habilidades clínicas y la toma de decisiones de las enfermeras, esto dentro de un espacio seguro, considerando situaciones complejas, riesgosas y hasta preocupaciones éticas. La tecnología de realidad virtual (VR) es una alternativa factible comparada con laboratorios de habilidades, siendo accesible, ahorrando recursos y sin depender de restricciones de ubicación o tiempo. También permite un aprendizaje de bajo riesgo y ansiedad además que puede ser a distancia de un maestro que proporcione orientación y retroalimentación virtual objetiva e inmediata. Aun así, resulta crucial tener claro el uso de la simulación y no confundirla con la realidad virtual para evitar confusiones y falsas expectativas. La realidad virtual, según los estándares de la Asociación Internacional Enfermería para la Simulación y el Aprendizaje Clínicos (INACSL), requiere una experiencia generada por computadora que estimule múltiples sentidos a través de dispositivos especializados. La presencia se deriva de los niveles de inmersión, un nivel más alto genera una mayor sensación de presencia (Padilha et al., 2019).

Educación en ciberseguridad

La escasez de profesionales en ciberseguridad es un problema que afecta a la seguridad a diversos sectores de la población, los expertos enfatizan la importancia de abordar este problema desde edades tempranas y hacer que las ofertas de trabajo en ciberseguridad sean más claras y atractivas, se reconoce la necesidad de despertar vocaciones en el campo de la ciberseguridad desde niveles básicos de educación y crear conciencia sobre las oportunidades que ofrece. No es necesario tener un perfil técnico, ya que la ciberseguridad abarca una amplia gama de habilidades (Kaur et al., 2023).

Aunque tanto gobiernos como empresas han aumentado su atención en este tema, los efectos de estas iniciativas tomarán tiempo en materializarse, ya que se requiere tiempo para formar nuevas generaciones de profesionales y para capacitar al personal existente, en la actualidad, Latinoamérica tiene un déficit de más de 700,000 especialistas en ciberseguridad, lo cual demuestra la importancia de incentivar la educación en este asunto, según datos de Microsoft, para el 2025 habrá 3.5 millones de empleos de ciberseguridad abiertos en todo el mundo. No obstante, tan sólo en América Latina faltan 701,000 profesionales en esa materia, de acuerdo con el *Cyber Workforce Report* de 2021, mientras que en México se calcula un déficit de más de 260,000 profesionales en ese ámbito (Shin et al., 2022).

La iniciativa de ciberseguridad de la OEA es crucial para América Latina, ya que la región es afectada por un creciente número de ataques cibernéticos tanto en organizaciones privadas como gubernamentales, en México, un estudio reciente muestra que el 74% de las empresas han sido víctimas de *ransomware*, y en la mitad de los casos, los ciberdelincuentes lograron cifrar información, el director de ciberseguridad de Microsoft Latinoamérica informa que durante la pandemia se ha observado un aumento del 600% en cibercrimen, lo que demuestra la amenaza latente que representan los ataques cibernéticos, ya que a menudo se realizan en silencio y sin atraer la atención pública, el gobierno de Estados Unidos está trabajando en abordar las amenazas cibernéticas y los métodos de pago ilícitos que hacen que el *ransomware* sea financieramente viable, especialmente a través de criptomonedas (Shojaifar & Järvinen, 2021).

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) señala un aumento drástico en el fraude cibernético, pasando del 7% de las reclamaciones en 2011 al 42 por ciento en 2017. Los fraudes cibernéticos en comercio electrónico han aumentado, con un promedio mensual de 193 mil casos en 2017, en comparación con 131 mil casos en el año anterior. En cuanto a la ciberseguridad en sistemas bancarios es frecuente encontrar fraudes de banca móvil, lo cual indica que se requieren esfuerzos conjuntos para garantizar el uso seguro y responsable de las Tecnologías de la Información, fomentando un desarrollo de oportunidades, crecimiento económico, político y social en la población.

Actualmente en México se aplica la estrategia nacional de ciberseguridad que tiene como objetivo principal dar acción en los ámbitos social económico y político permitiendo un uso responsable de las TIC y promoviendo un desarrollo sostenible en México, para realizarlo se aplican planes y programas gubernamentales que destacan la importancia de las TIC para el desarrollo social. Sin embargo, la digitalización y el aumento de servicios en línea incrementan las vulnerabilidades y riesgos de forma alarmante, presentando ciber ataques a nivel global, por lo que la ciberseguridad es un elemento esencial para la protección de información y el desarrollo social y económico dentro de un país.

***Frameworks* para desarrollar entornos de realidad virtual**

Las herramientas para crear entornos de realidad virtual llamadas *frameworks* son esenciales para los desarrolladores pues simplifican el proceso de diseño y desarrollo de experiencias inmersivas, existen los muy famosos *Unity 3D* y *Unreal Engine* así como opciones de código abierto como *A-Frame* y *Godot Engine* que proporcionan una variedad adaptable a las necesidades y preferencias de desarrolladores, su uso puede ser desde crear videojuegos de VR, aplicaciones educativas, experiencias de entretenimiento o simulaciones industriales, son un punto de partida importante en la generación de proyectos de realidad virtual (Picard et al., 2024), A continuación, se describen algunos de los *frameworks* usados para crear entornos de realidad virtual:

- *Unity 3D*: Es uno de los frameworks más populares para el desarrollo de aplicaciones de realidad virtual. Ofreciendo un motor sólido y soporte para múltiples plataformas de VR

- *Unreal Engine*: Es un motor de juego desarrollado por Epic Games que ofrece una serie de herramientas y características avanzadas para crear entornos inmersivos de VR.
- *Godot Engine*: Es un motor de código abierto, popular en los últimos años que ofrece soporte a través de complementos permitiendo crear experiencias VR de alta calidad.
- *SteamVR/OpenVR*: Es un framework creado por Valve compatible con gran variedad de dispositivos utilizado para desarrollar contenido en la plataforma de la misma compañía. *OpenVR* es la interfaz de programación de aplicaciones (API) de código abierto que se usa con múltiples dispositivos
- *A-Frame*: Es un *framework* de desarrollo web basado en HTML para crear experiencias de realidad virtual en el navegador, utilizando tecnologías web como *WebGL* y *WebVR/WebXR*, ver Figura 3.

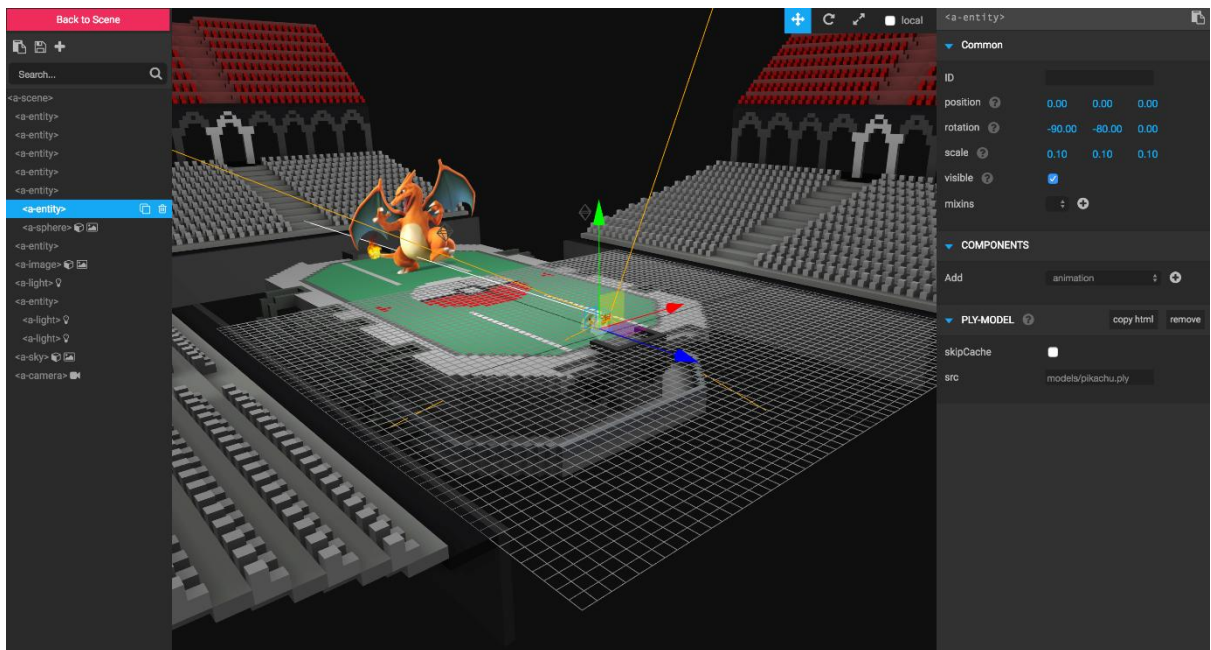


Figura 3. Entorno de desarrollo de A-Frame (Campos, 2017).

- *Vuforia*: Es un *framework* de realidad aumentada que se puede utilizar para crear aplicaciones de realidad virtual y aumentada, es especialmente útil para experiencias de AR/VR en dispositivos móviles.

- *CryEngine*: es un motor de juego para alta calidad visual y capacidades avanzadas de renderizado.

1.2 PLANTEAMIENTO DEL PROBLEMA

En la última década, la seguridad informática es un tema de gran importancia debido ya que el creciente número de amenazas cibernéticas que enfrentan individuos, organizaciones y entidades de gobierno en todo el mundo, ha aorillado a tomar medidas drásticas para hacer frente a esta problemática, cada una de estas entidades a determinado que es fundamental contar con profesionales capacitados en temas fundamentales como la seguridad defensiva y ofensiva, que sean capaces de identificar y detectar vulnerabilidades, clasificar los riesgos y aplicar estrategias eficaces para detener o bloquear las posibles amenazas y reducir los efectos que estas puedan causar en los sistemas y los datos almacenados en los diversos medios de las organizaciones públicas y privadas (Aiyanyo et al., 2020).

En este contexto, la enseñanza y el aprendizaje de la seguridad ofensiva adquieren una relevancia crucial en las instituciones de educación superior, donde se forman los futuros expertos en el campo y la generación que serán los evangelistas de esta cultura a la que nombrare como “promotores de la conciencia cibernética”; Sin embargo, a pesar de los esfuerzos realizados para mejorar los programas de formación en seguridad informática, existen desafíos significativos que dificultan la adquisición de conocimientos y habilidades prácticas por parte de los estudiantes, uno de los principales desafíos radica en la falta de experiencias realistas y contextualizadas, en las que los estudiantes puedan poner en práctica los conceptos teóricos aprendidos dentro del salón de clases, ya que usando las metodologías tradicionales de enseñanza, basadas en la exposición teórica y ejercicios prácticos limitados, no logran proporcionar a los estudiantes un entorno de aprendizaje que refleje fielmente los escenarios y desafíos reales a los que se enfrentarán en el campo laboral.

Por esta razón, la utilización de los simuladores computacionales surge como una alternativa viable para fortalecer la enseñanza y el aprendizaje sobre la seguridad ofensiva y defensiva en la educación superior, es conocido que el uso de los simuladores en diversos contextos ofrece la posibilidad de crear entornos inmersivos y realistas (Admass et al., 2024), donde los estudiantes pueden interactuar con

elementos y escenarios de seguridad reales, a través de estos se pueden experimentar las consecuencias de sus decisiones, que pueden estar determinadas por el tiempo de respuesta a incidentes que son muy similares a los ambientes reales, las malas decisiones se ven reflejadas en costos a las diferentes áreas como lo pueden ser entidades públicas o privadas en donde se lleven a cabo los diversos vectores de ataque, sin embargo, a pesar de su potencial, la utilización de la realidad virtual en la formación en seguridad ofensiva aún no ha sido ampliamente explorada ni evaluada en el contexto de las instituciones de educación superior de la región oriente del Estado de México.

Por lo tanto, al existir una brecha en la investigación que impide comprender a fondo el impacto del uso de los simuladores en la educación superior en la región oriente del Estado de México utilizando tecnologías más accesibles como la web, en el desarrollo profesional de estudiantes y la mejora que tendrá en sus habilidades y conocimientos relacionados a la seguridad ofensiva.

De esta forma la pregunta de investigación que se plantea es:

- ¿Cómo contribuye el desarrollo de una plataforma de simulación en ciberseguridad, que utiliza lógica difusa para ofrecer recomendaciones de estudio, al fortalecimiento de la formación académica de estudiantes universitarios en seguridad informática en la región oriente del Estado de México?

1.3 OBJETIVOS

General

- Desarrollar una plataforma de simulación en ciberseguridad que integre escenarios prácticos y evaluaciones interactivas para fortalecer la capacitación de estudiantes universitarios en la región oriente del Estado de México, abordando desafíos específicos y amenazas emergentes del entorno cibernético.

Específicos

1. Diseñar la arquitectura y la interfaz de usuario de la plataforma de simulación en ciberseguridad, considerando requisitos pedagógicos y tecnológicos, de acuerdo con una revisión sistemática de la literatura.
2. Integrar escenarios realistas y desafiantes que abarquen los vectores de ataque más frecuentes durante el 2023.
3. Evaluar la efectividad de la plataforma mediante métricas de rendimiento de los estudiantes, como tiempo en el simulador, evaluación, tiempo de respuesta de la prueba y realizar recomendaciones usando lógica difusa.
4. Desarrollar una plataforma de simulación en ciberseguridad que incorpore recomendaciones educativas basadas en lógica difusa, dirigida a fortalecer la formación académica en seguridad informática de los estudiantes universitarios en la región oriente del Estado de México.

1.4 DELIMITACIÓN O ALCANCE DE LA INVESTIGACIÓN

Delimitación y alcances

Universo de estudio: La investigación se centró en instituciones de educación superior ubicadas en el oriente del Estado de México, se seleccionaron específicamente universidades que ofrecen programas relacionados con la seguridad informática y que cuentan con acceso a internet de banda ancha para ejecutar aplicaciones web robustas.

Características de los componentes a utilizar; La investigación se centra en la utilización de tecnología de realidad virtual para la creación de escenas simuladas en entornos *web*, se utilizaron dispositivos como computadoras, que ayuden a los alumnos interactuar con las escenas simuladas sin tener la necesidad de contar con equipos muy sofisticados para la utilización del entorno de simulación.

Delimitación de la investigación

- La investigación se centró exclusivamente en instituciones de educación superior, como universidades, tecnológicos de estudios y centros universitarios, excluyendo otros niveles educativos.
- La simulación se enfocó en un conjunto específico de tipos de ataques cibernéticos gestados en 2023, con soporte en el trabajo de (Kaur et al., 2023), identificando como los principales ataques: *Phishing*, *ransomware*, *spyware*, DDOS y gusanos informáticos, en lugar de abordar todos los posibles escenarios.
- La investigación se enfocó en un grupo específico de usuarios, como estudiantes de seguridad informática y carreras relacionadas a la informática dentro de las universidades seleccionadas son el Centro Universitario UAEM Valle de Chalco, Tecnológico de Estudios Superiores de Chalco estas dos instituciones tienen las carreras de Ingeniería en Computación, Licenciatura en Informática Administrativa e Ingeniería Informática.

1.4 HIPÓTESIS

- La creación de una plataforma de simulación en ciberseguridad que integra la lógica difusa mejora la comprensión teórica de conceptos de seguridad informática entre los estudiantes universitarios en la región oriente del Estado de México.
 - Variable Independiente (VI): Creación de la plataforma de simulación en ciberseguridad.
 - Variable Dependiente (VD): Mejora en la comprensión teórica de conceptos de seguridad informática.

1.5 JUSTIFICACIÓN

En la presente investigación se propuso analizar el impacto de la utilización simuladores aplicados a la ciberseguridad en la enseñanza y el aprendizaje de la

seguridad ofensiva mediante escenas simuladas en entornos *web* en universidades, tecnológicos de estudios y centros universitarios del oriente del Estado de México, a continuación, se exponen las razones por las cuales fue importante llevar a cabo esta investigación, considerando su importancia teórica, metodológica, práctica y social no sin antes mencionar una definición clara de lo que es un mundo virtual (Nesenbergs et al., 2020).

Un mundo virtual es el contenido de un medio dado puede existir únicamente en la mente de su creador o transmitirse de tal manera que pueda compartirse con otros, puede existir sin mostrarse en un sistema de realidad virtual (es decir, una colección integrada de *hardware*, *software* y contenido ensamblado para producir experiencias de realidad virtual), al igual que los guiones de obras de teatro o películas existen independientemente de las instancias específicas de su desempeño, tales guiones, de hecho, describen mundos virtuales (Czarnocka & Mazurek, 2025).

- **Beneficios y utilidad:** La implementación de escenas simuladas en realidad virtual en la enseñanza de la seguridad ofensiva puede tener varios beneficios, en primer lugar, permite a los estudiantes vivir experiencias realistas y prácticas en un entorno seguro y controlado, lo que facilita el aprendizaje y la comprensión de conceptos y técnicas (Beuran et al., 2018) esto fomenta el desarrollo de habilidades prácticas y la toma de decisiones basadas en situaciones reales, lo que prepara a los estudiantes de manera más efectiva para enfrentar los desafíos del mundo laboral en el campo de la seguridad ofensiva.
- **Fortalecimiento de la investigación:** Esta investigación ha enriquecido el conocimiento y la comprensión sobre el uso de la realidad virtual en la enseñanza y el aprendizaje de la seguridad ofensiva en la educación superior en la región oriente del Estado de México, proporciona evidencia empírica sobre la efectividad de las simulaciones y su impacto en el desarrollo de habilidades y competencias de los estudiantes, además, contribuirá al avance del campo de la educación virtual y servirá como un recurso valioso para futuras investigaciones.

- **Consecuencias de no llevar a cabo la investigación:** La falta de investigación en este tema podría implicar la pérdida de oportunidades para mejorar la calidad de la enseñanza en seguridad ofensiva en la educación superior en región oriente del estado de México, sin el conocimiento y la comprensión adecuada de las posibilidades que ofrece la realidad virtual, se corre el riesgo de continuar utilizando métodos tradicionales que pueden resultar menos efectivos en el desarrollo de habilidades prácticas y en la preparación de los estudiantes para enfrentar los desafíos reales en el campo de la seguridad ofensiva.

2. MARCO TEÓRICO

En este capítulo se describe cómo se llevó a cabo la revisión de literatura, esto implicó detectar, consultar y obtener bibliografía y otros materiales para enmarcar el problema de investigación, este marco metodológico incluyó la búsqueda, evaluación crítica, extracción y compilación de información relevante, como señalan (Page et al., 2021), una revisión de literatura rigurosa permite identificar tendencias, sintetizar hallazgos previos y sustentar teóricamente el estudio. Además, esenciales en el proceso son herramientas como la búsqueda en bases de datos, la selección de fuentes pertinentes y la estructuración lógica del contenido a emplear. También, la importancia de una revisión de literatura bien elaborada se enfatiza en trabajos como el que propone (Snyder, 2019), donde se destaca su función para establecer el campo problemático, guiar la metodología y garantizar que el estudio aporte de manera clara y concisa a la disciplina (Xiao & Watson, 2019).

Metodología aplicada para realizar la revisión sistemática

Una práctica recomendable para cualquier nuevo proyecto de investigación es iniciar con una revisión exhaustiva de la literatura desde las etapas iniciales de su desarrollo, principalmente según (Xiao & Watson, 2019), se listan elementos importantes a considerar en este proceso de búsqueda de materiales relevantes para la investigación tales como:

- La ciencia es un proceso acumulativo
- Las nuevas investigaciones deben de construirse sobre conocimientos anteriores
- Es la demostración de que los autores conocen los antecedentes de su investigación
- Aportan ideas para la investigación
- Aporta credibilidad al trabajo

Existen revisiones sistemáticas de la literatura basadas en (Snyder, 2019):

- Resultados de investigaciones previas, comunicados principalmente en artículos de revistas científicas
- Bases de datos académicas para la búsqueda sistemática de los artículos

- Opcionalmente, puede utilizarse otra clase de evidencias: comunicaciones, informes, libros y literatura gris
- Manejan criterios específicos para la evaluación, esto es para la inclusión o exclusión de los documentos
- Se componen de fases que pueden agruparse en: Búsqueda, evaluación, análisis y síntesis

La metodología seleccionada, después de un análisis de diversas fuentes de consulta, fue *SALSA Framework*, ya que se ajustó a los parámetros en los cuales se desarrolló la investigación. Esta metodología combina las fases presentes en otros enfoques y, además, como propuesta de apoyo, permite auxiliarse de herramientas de Inteligencia Artificial (IA) para mejorar las tareas de cada fase.

SALSA Framework

En el *framework* SALSA se considera que las revisiones sistemáticas constan al menos de cuatro fases fundamentales: Búsqueda (*Search*), Evaluación (*Appraisal*), Síntesis (*Synthesis*) y Análisis (*Analysis*). Aunque en algunas propuestas estas fases pueden subdividirse en subfases, el núcleo del método permanece constante. Este modelo fue inicialmente descrito por (Grant & Booth, 2009) como una herramienta para categorizar y comparar hasta catorce tipos diferentes de revisión, analizando cómo cada uno incorpora estos cuatro procesos esenciales, el *framework* SALSA se puede interpretar como una guía que exige la respuesta a cuatro preguntas fundamentales, ver Figura 4.

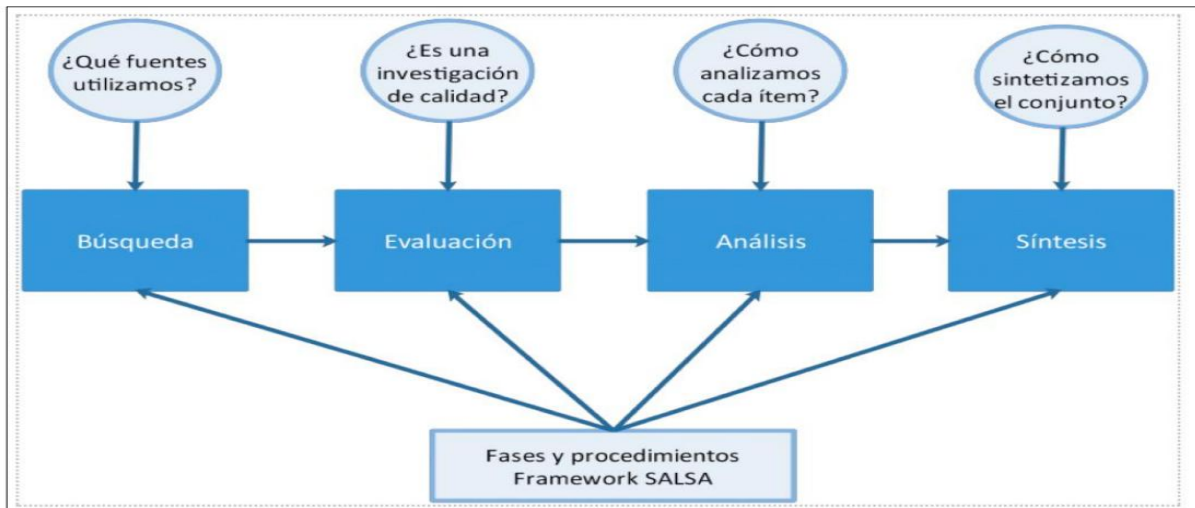


Figura 4. Fases del SALSA Framework.

Búsqueda

La etapa inicial de búsqueda debe abordarse mediante la identificación y selección cuidadosa de las fuentes que servirán como base de evidencia, esto implica diseñar ecuaciones de búsqueda para bases de datos académicas o establecer procedimientos adecuados para otras fuentes, asegurando siempre una claridad completa en las fuentes y métodos de obtención de documentos, es importante mencionar que las bases de datos utilizadas dentro de esta etapa fueron, Scopus, Google Académico, *Science Direct*, estas fueron propuestas por parte del director de tesis ya que son plataformas que concentran documentos de carácter científico relacionado con el tema de investigación, en la Tabla 1 se describen de manera clara y detallada las palabras clave utilizadas en inglés para obtener mejores resultados de búsqueda, y además se integra la respectiva ecuación de búsqueda.

Palabras Clave	Ecuación de búsqueda
<ul style="list-style-type: none"> • <i>Cybersecurity simulation platforms</i> • <i>Cybersecurity training environments</i> • <i>Cyber defense simulation tools</i> • <i>Security training platforms</i> • <i>Cyber range platforms</i> 	<p><i>(Cybersecurity simulation platforms OR Cyber range platforms OR Security training environments OR Cyber defense simulation tools) AND (Comprehensive analysis OR In-depth examination OR Thorough review OR</i></p>

<ul style="list-style-type: none"> • <i>Security simulation software</i> 	<i>Comprehensive evaluation) AND (Cybersecurity OR Network security OR Information security OR Data protection)</i>
<ul style="list-style-type: none"> • <i>Cybersecurity simulation platforms</i> • <i>Cybersecurity training environments</i> • <i>Cyber defense simulation tools</i> • <i>Security training platforms</i> • <i>Cyber range platforms</i> • <i>Security simulation software</i> 	<i>(Cybersecurity simulation OR Cyber range) AND (Comprehensive analysis OR In-depth review) AND (Cybersecurity OR Network security)</i>
<ul style="list-style-type: none"> • <i>Cybersecurity</i> • <i>Network security</i> • <i>Information security</i> • <i>Data protection</i> • <i>Threat analysis</i> • <i>Vulnerability assessment</i> 	<i>(Cybersecurity simulation platforms OR Cyber range platforms) AND (Detailed analysis OR Comprehensive evaluation) AND (Cybersecurity OR Network security vulnerabilities)</i>
<ul style="list-style-type: none"> • <i>Systematic review</i> • <i>Literature review</i> • <i>Meta-analysis</i> • <i>Research synthesis</i> • <i>Evidence synthesis</i> • <i>Review article</i> 	<i>(Cybersecurity simulation platforms OR Cyber range platforms) AND (Holistic analysis OR Comprehensive assessment) AND (Cybersecurity OR Network security)</i>

Tabla 1. Palabras clave y ecuaciones de búsqueda aplicadas a la fase de revisión.

Es importante mencionar que la metodología *SALSA Framework*, propone como herramienta de apoyo el uso de una inteligencia Artificial, esto para facilitar las tareas del investigador, en ocasiones se puede interpretar mal el uso del concepto de emplear una Inteligencia Artificial ya que puede infringir en ciertas reglas que se estipulan en la revisión final del documento, se aclara que se usa solo para poder gestionar de manera más óptima la literatura en la Figura 5, se muestra la forma en que se utilizó la herramienta, más adelante se muestran las capturas de pantalla y la forma de utilizar el *ChatGPT*, se optó por el uso de este LLM (*Large Language Model*) para llevar a cabo la gestión de tareas propuestas por el *framework*.

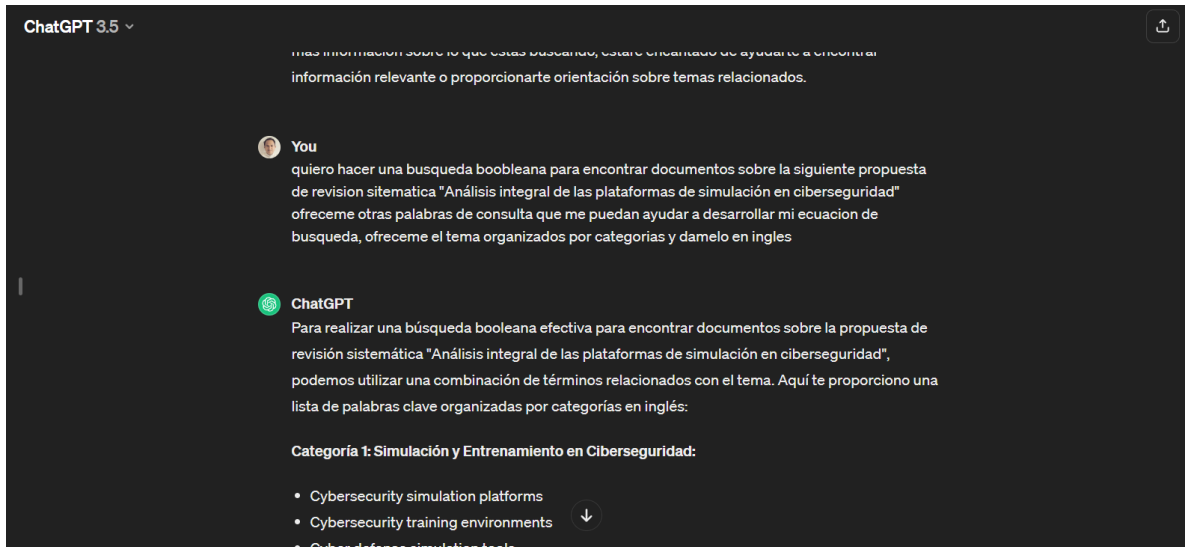


Figura 5. Pregunta al ChatGPT acerca de las palabras clave en la investigación.

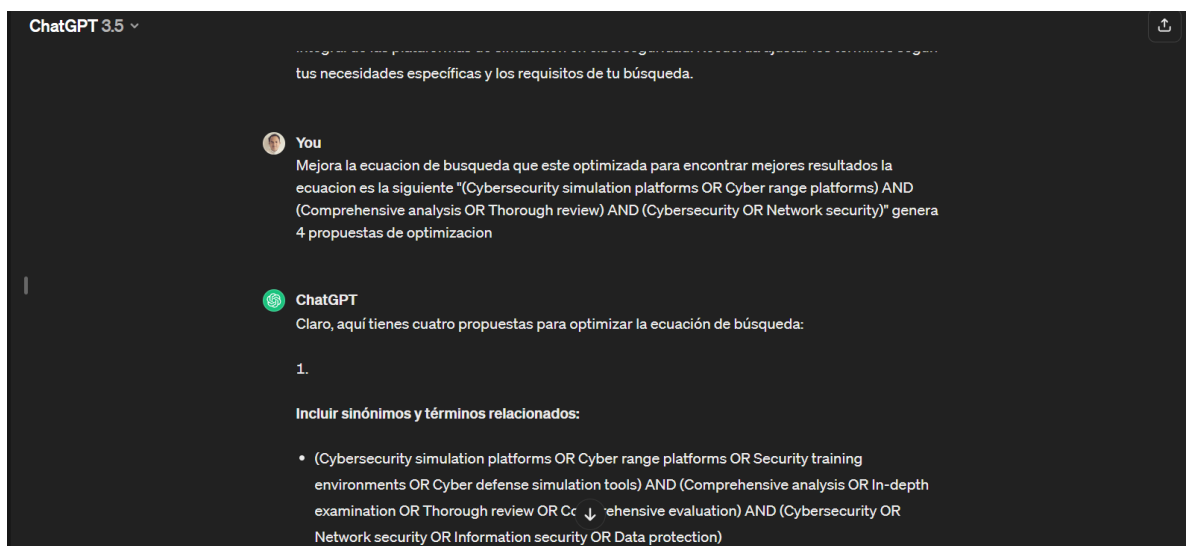


Figura 6. Mejora de la ecuación solicitando la optimización de una ecuación de búsqueda.

Evaluación

La etapa de evaluación, conocida como "*Appraisal*", es fundamental para garantizar que la base de evidencia seleccionada cumpla con los requisitos del estudio, esto implica aplicar criterios de inclusión y exclusión que abarcan temas específicos, rangos de fechas de publicación, metodología y asegurarse de la calidad de cada documento identificado en la etapa anterior.

Análisis

La fase de análisis significa hacer diagramas que saquen datos para mirar mejor todas las fuentes que forman la base de prueba. Se pueden usar tablas o grupos especiales para sustraer datos importantes, como los propósitos, métodos y resultados principales de cada estudio, o pensar en áreas temáticas relacionadas con cada proyecto.

En esta etapa se consultó al modelo ChatGPT para que revisara la adecuación de un documento candidato para formar parte de la base de evidencia documental científica, se realizó el siguiente cuestionamiento ¿puedes confirmarme con un sí o un no y justificar tu respuesta si este resumen tiene que ver con "Análisis integral de las plataformas de simulación en ciberseguridad: ¿Evaluación, tendencias y metodologías educativas?", el texto que se ingreso fue el *abstract* que se presenta en cada uno de los artículos de investigación en las Figuras 7 y 8, se muestra el procedimiento empleado para generar las preguntas correspondientes con cada uno de los posibles documentos candidatos.

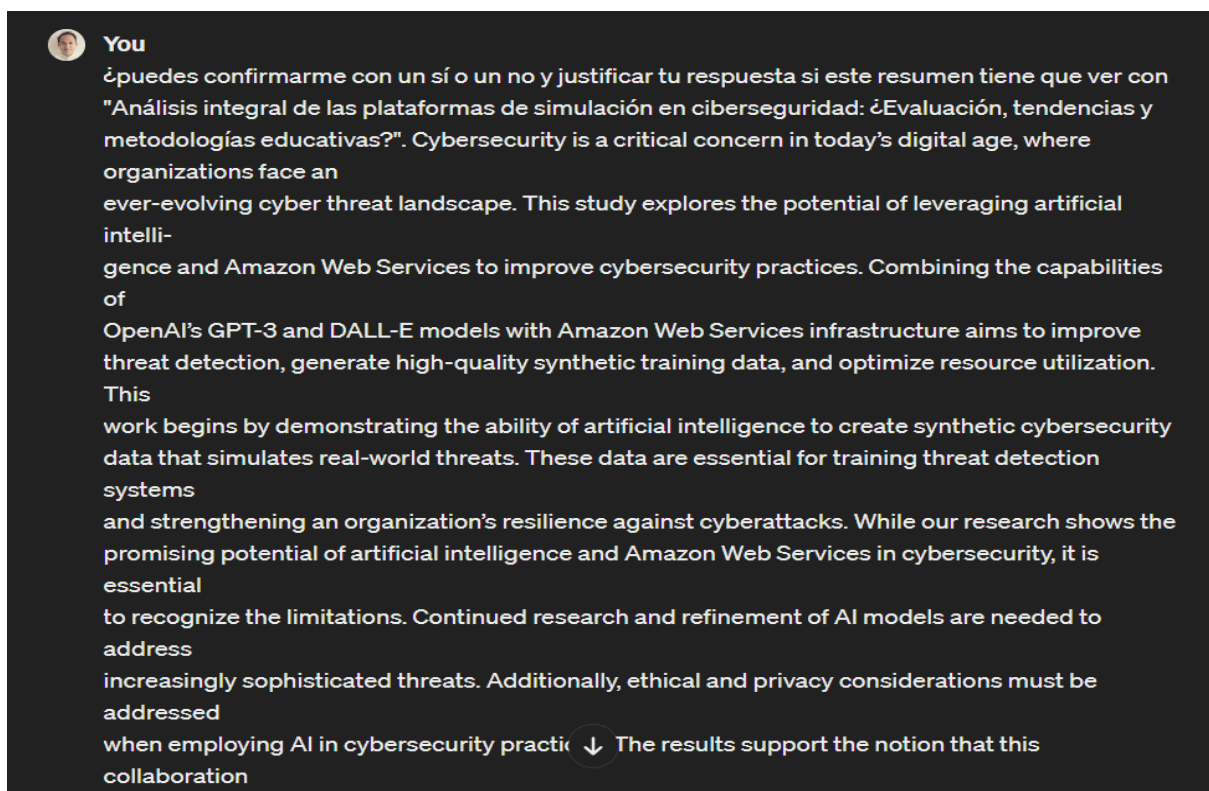


Figura 7. Pregunta hecha al ChatGPT de acuerdo con el Abstract de un artículo candidato.

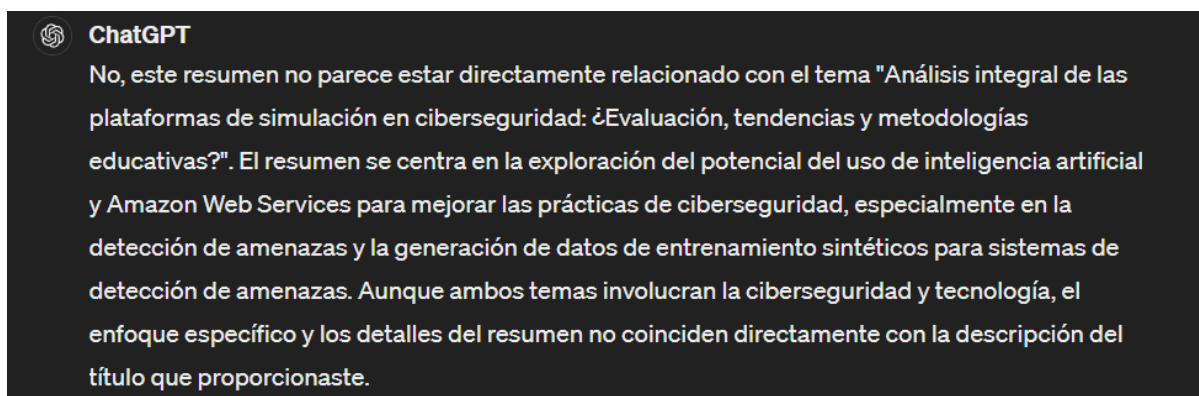


Figura 8. Respuesta del ChatGPT respecto al abstract presentado.

Una vez que un artículo presento características de acuerdo con lo solicitado se utilizó la herramienta de *Mendeley Reference Manager* para ir realizando el registro de los artículos candidatos y de esta manera tener todos los documentos listos para la fase de síntesis, en la Figura 9, se muestra la captura de pantalla de cómo se estuvieron organizando cada uno de los artículos.

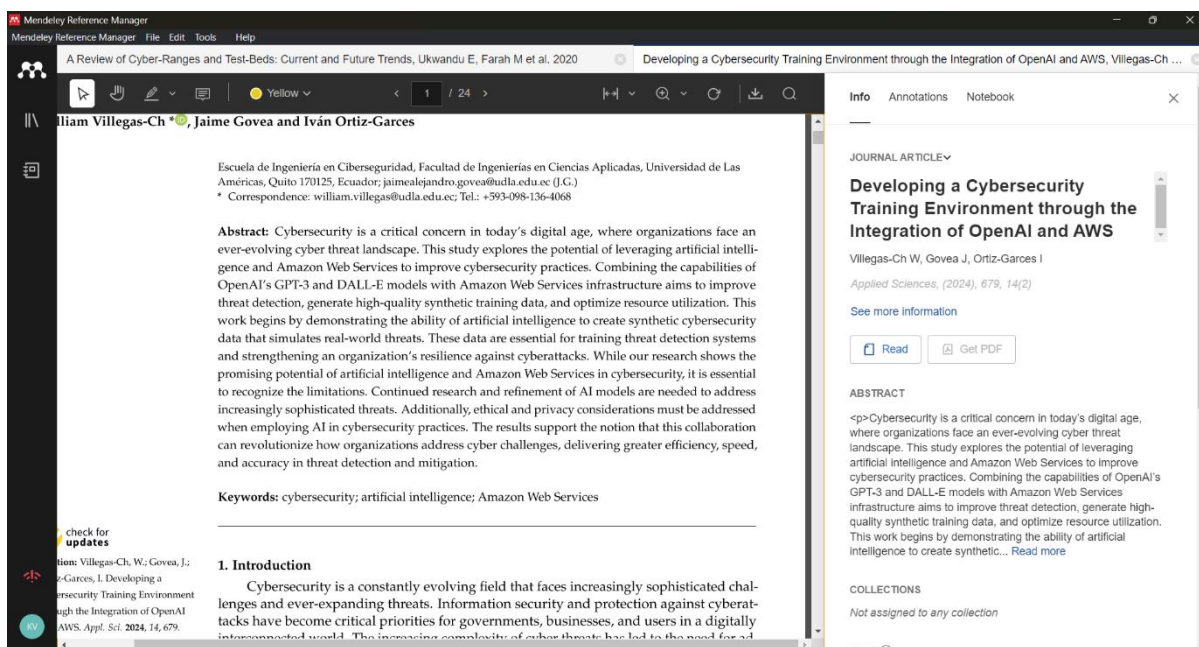


Figura 9. Mendeley Reference Manager, ejemplo de organización de artículos.

Síntesis

La fase de síntesis implica presentar los resultados principales utilizando tablas, matrices y resúmenes narrativos, con la posibilidad de incluir diagramas o mapas conceptuales, el objetivo es crear un compendio de artículos candidatos que ayude a fortalecer elementos teóricos, integrando configuración e interpretación de resultados. Se espera identificar patrones, temas emergentes, que se puedan usar para fortalecer el compendio en la sección del marco teórico así como identificar áreas de investigación potenciales a través de la identificación de vacíos y oportunidades (Rohan et al., 2023).

Durante esta etapa, se exponen los resultados principales utilizando tablas o matrices, así como resúmenes narrativos, ocasionalmente, se pueden integrar diagramas o mapas conceptuales, el propósito es generar una síntesis que trascienda la simple suma de partes, para lo cual se requiere una presentación que no se limite a la agregación de datos, sino que incluya la configuración e interpretación de los resultados, específicamente, se busca identificar patrones, temas emergentes y áreas de investigación aún por explorar, con el fin de aprovechar las oportunidades de estudio que se presenten.

MARCO TEÓRICO

En este apartado se incluyen los datos o ideas que se han expuesto anteriormente sobre el tema a investigar, la manera en que han sido formulados y lo que ha contribuido al esclarecimiento del problema, es importante mencionar cuales son las áreas descriptivas en las que está fundamentada la investigación como lo son:

- Enseñanza práctica y sin riesgos: La realidad virtual crea oportunidades para que los estudiantes aprenden de manera práctica, intentando y arreglando retos reales sin peligros. Pueden usar ideas en situaciones virtuales que cambian y recibir comentarios rápidos sobre lo que hacen, esto anima a aprender haciendo y ayuda a desarrollar destrezas prácticas en seguridad ofensiva. Importancia de la formación efectiva en seguridad ofensiva: resalta que la formación efectiva en seguridad ofensiva es esencial para combatir las

amenazas cibernéticas. Los profesionales de seguridad ofensiva son responsables de proteger los sistemas y datos al identificar y corregir vulnerabilidades.

- Personalización y adaptabilidad: La realidad virtual ayuda a adaptar la experiencia de aprendizaje a las necesidades de los estudiantes, los escenarios pueden ajustarse al nivel de habilidad y conocimiento de cada estudiante, lo que ayuda a que un aprendizaje sea personalizado y eficiente en la adquisición de habilidades en el área de ciberseguridad.
- Simulaciones inmersivas: La realidad virtual proporciona una experiencia que permite a los estudiantes interactuar con entornos virtuales que simulan situaciones relacionadas con la seguridad ofensiva, estas pueden abarcar desde escenarios de ciberataques hasta prácticas de respuesta a incidentes.

La ciberseguridad significa diferentes cosas a las personas

Aunque la ciberseguridad pueda parecer un concepto fácil de definir, en la práctica adquiere significados diversos según la perspectiva y la situación de cada individuo, esto se traduce en una amplia variedad de políticas, procedimientos y prácticas relevantes. Por ejemplo, alguien interesado en salvaguardar sus cuentas de redes sociales de ataques cibernéticos probablemente no adoptará las mismas estrategias y tecnologías que los profesionales del Pentágono, quienes resguardan redes clasificadas (Pramanik, 2022).

- Para las personas, la ciberseguridad significa que nadie más que ellos mismos y otras personas a las que hayan autorizado pueden acceder a sus datos personales, y que sus dispositivos informáticos funcionen correctamente y estén libres de *malware*.
- Para los propietarios de pequeñas empresas, la ciberseguridad puede incluir garantizar que los datos de las tarjetas de crédito estén adecuadamente protegidos y que los estándares de seguridad de los datos se implementen adecuadamente en los registros de los puntos de venta.

- Para las empresas que realizan negocios en línea, la ciberseguridad puede incluir la protección de servidores con los que interactúan regularmente personas externas que no son de confianza.
- Para los proveedores de servicios compartidos, la ciberseguridad puede implicar proteger numerosos centros de datos que albergan numerosos servidores que, a su vez, albergan muchos servidores virtuales pertenecientes a muchas organizaciones diferentes.
- Para el gobierno, la ciberseguridad puede incluir el establecimiento de diferentes clasificaciones de datos, cada una con su propio conjunto de leyes, políticas, procedimientos y tecnologías relacionados. (Steinberg, 2019)

De manera general, aunque la definición de la ciberseguridad pueda ser sencilla, las expectativas prácticas asociadas con esta palabra difieren considerablemente entre las personas, desde una perspectiva técnica, la ciberseguridad constituye un subconjunto de la seguridad de la información que se ocupa de salvaguardar la información y los sistemas de información que almacenan y procesan datos en formato electrónico. En contraste, la seguridad de la información engloba la protección de todas las formas de datos, incluyendo, por ejemplo, la seguridad de archivos en papel y archivadores.

Concepto de ciberseguridad

Se puede definir a la ciberseguridad como un campo que involucra proteger sistemas, redes, programas y datos contra ataques, daños o accesos no autorizados, convirtiéndolo en un campo multidisciplinario, autores y expertos han proporcionado definiciones donde engloban aspectos de este concepto, algunas de estas sirven como guía para la presente investigación, las cuales se muestran a continuación:

1. Bruce Schneier: La ciberseguridad se encarga de proteger la información, los sistemas informáticos y las infraestructuras de comunicaciones contra el acceso no autorizado, el daño, el robo o el ataque. Incluye la práctica de asegurar la confidencialidad, la integridad y la disponibilidad de la información (Schneier, 2000)

2. CIS (Center for Internet Security): Ciberseguridad es el conjunto de prácticas, medidas y tecnologías diseñadas para proteger sistemas, redes y datos de amenazas, ataques y accesos no autorizados (Veale & Brown, 2020).
3. Eric Cole: Ciberseguridad no se trata solo de tecnología, sino también a las personas y los procesos que respaldan la seguridad informática. Incluye la gestión de riesgos, la conciencia del usuario y la capacidad de responder de manera efectiva a incidentes de seguridad (Zimmermann et al., 2024).
4. National Institute of Standards and Technology (NIST): La ciberseguridad es la práctica de proteger sistemas, redes y programas de ataques digitales, daños o acceso no autorizado.
5. Acuerdo por el que se establece el esquema de interoperabilidad y de datos abiertos de la administración pública federal: Artículo 2. Para los efectos del presente Acuerdo, se entenderá por ciberseguridad, a la aplicación de un proceso de análisis y gestión de riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información, así como con los sistemas y procesos usados para ello, que permite llegar a una situación de riesgo conocida y controlada.

Estas definiciones reflejan la naturaleza integral de la ciberseguridad, que abarca tanto aspectos tecnológicos como humanos y organizativos. La protección de la información y la infraestructura digital es esencial en un entorno cada vez más interconectado y dependiente de la tecnología.

Objetivos de la ciberseguridad

Los expertos en ciberseguridad generalmente argumentan que el propósito fundamental de este campo es asegurar la Confidencialidad, Integridad y Disponibilidad (CIA) de la información ver Figura 10. A esta triple premisa a veces se

le conoce como la tríada de la seguridad, en un ingenioso juego de palabras que se podría expresar así:

- La confidencialidad implica asegurar que la información permanezca resguardada y no sea divulgada ni puesta al alcance de entidades no autorizadas, lo que incluye tanto individuos como organizaciones o procesos informáticos, se debe evitar mezclar confidencialidad con privacidad, la confidencialidad representa una parte más específica de la esfera de la privacidad, su función principal es resguardar la información contra accesos no autorizados, mientras que la privacidad, en un sentido más amplio, abarca diversas dimensiones, la acción de piratas informáticos que sustraen datos compromete directamente la confidencialidad (Yang et al., 2021).
- La integridad implica asegurar la precisión y plenitud de los datos, la precisión se define como la certeza de que los datos no sufrirán alteraciones de ninguna índole, ya sea por intervención no autorizada o por problemas técnicos, respecto a la plenitud, se garantiza que ninguna entidad no autorizada o fallo técnico haya eliminado alguna parte de los datos, así mismo, la integridad abarca la preservación del no repudio, lo que implica que los datos se crean y gestionen de manera que sea extremadamente difícil de cuestionar con respecto a su autenticidad o integridad, ciberataques que interceptan datos y los alteran antes de que sean transmitidos al destino, (también llamados ataques de intermediario) donde se amenaza la integridad del sistema
- La disponibilidad se refiere a garantizar que la información, los sistemas utilizados para almacenarla y procesarla, los mecanismos de comunicación utilizados para acceder a ella y transmitirla, y todos los controles de seguridad asociados funcionen correctamente para cumplir con algún punto de referencia específico (por ejemplo, 99,99 por ciento de tiempo de actividad). Las personas ajenas al campo de la ciberseguridad a veces piensan que la disponibilidad es un aspecto secundario de la seguridad de la información después de la confidencialidad y la integridad. De hecho, garantizar la disponibilidad es una parte integral de la ciberseguridad. Sin embargo, lograrlo a veces resulta más difícil que garantizar la confidencialidad o la integridad. Una de las razones por las que esto es cierto es que mantener la disponibilidad a menudo requiere involucrar a muchos más profesionales no relacionados con la ciberseguridad, lo que genera un desafío del

tipo “demasiados cocineros en la cocina”, especialmente en organizaciones más grandes. Los ataques distribuidos de denegación de servicio intentan socavar la disponibilidad. Además, hay que tener en cuenta que los ataques suelen utilizar grandes cantidades de potencia informática y ancho de banda robados para lanzar ataques DDoS, pero los respondedores que buscan garantizar la disponibilidad sólo pueden aprovechar la cantidad relativamente pequeña de recursos que pueden permitirse (Yang et al., 2021).

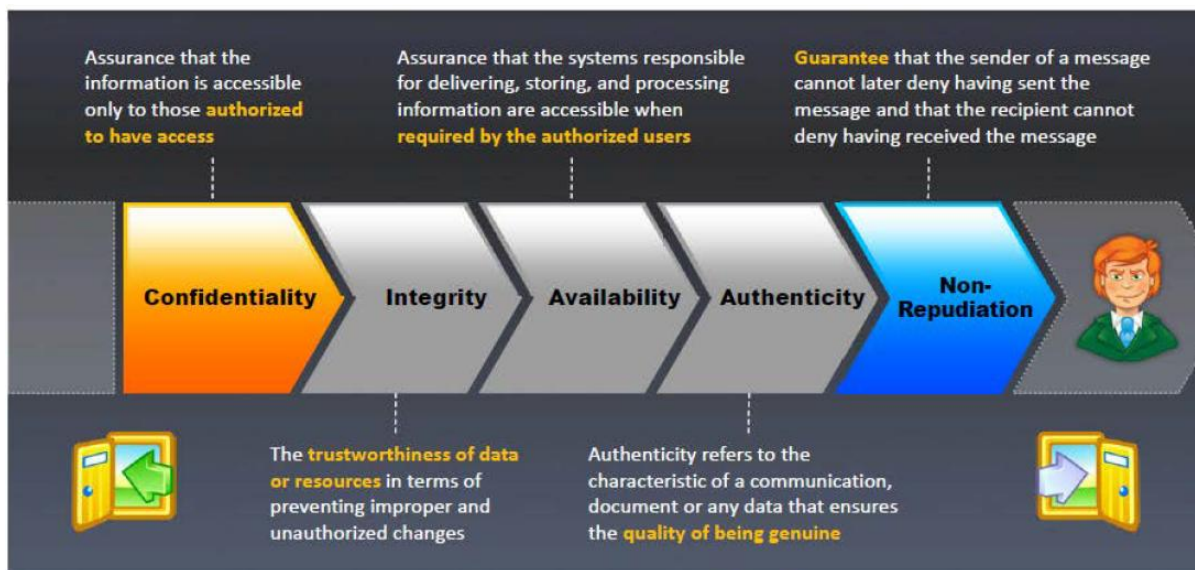


Figura 10. Triada de la Seguridad (Ethical, 2014).

Clasificación de la ciberseguridad

La ciberseguridad se clasifica en diversas categorías o dimensiones, cada una enfocada en aspectos específicos de la protección contra amenazas digitales. A continuación, se presentan algunas de las clasificaciones comunes dentro del campo de la ciberseguridad:

- Seguridad de la Información: Se enfoca en proteger la confidencialidad, integridad y disponibilidad de la información. gestiona el acceso, la transmisión y el almacenamiento de datos.
- Seguridad de la Red: Su objetivo es asegurar la integridad y disponibilidad de las comunicaciones y los recursos de red, su enfoque es la detección de intrusiones, VPNs y medidas para prevenir ataques como el *phishing*.

- Seguridad de Sistemas: Su finalidad es proteger sistemas operativos y *software* contra vulnerabilidades y ataques se enfoca en *software*, configuración segura, antivirus y otras medidas específicas del sistema.
- Seguridad de Aplicaciones: Se especializa en garantizar que las aplicaciones sean seguras contra amenazas y vulnerabilidades, se realizan pruebas de seguridad de aplicaciones, desarrollo seguro, y protección contra ataques como inyecciones SQL.
- Seguridad Física: Su meta es proteger el acceso físico a sistemas y equipos, realiza controles de acceso físico, monitoreo de instalaciones y protección contra robos o daños físicos.
- Seguridad en la Nube: Su propósito es asegurar los datos y servicios almacenados y procesados en entornos de nube genera políticas de acceso, cifrado, autenticación y medidas específicas para entornos en la nube.
- Seguridad en el Internet de las Cosas (IoT): Su interés se centra en proteger dispositivos conectados y datos en el entorno del IoT genera cifrados, autenticación, y monitoreo de dispositivos IoT para prevenir vulnerabilidades.

Los anteriores conceptos se entrelazan para estructurar una estrategia de ciberseguridad efectiva que generalmente aborda múltiples dimensiones para ofrecer una protección integral contra las amenazas digitales en evolución.

Ataques gestados por los ciber delincuentes

Los atacantes pueden lanzar ciertos ciberataques no con la intención directa de robar dinero o datos, sino con el propósito de infligir un daño específico a la víctima. Este daño puede traducirse, de forma directa o indirecta, en beneficios financieros, militares, políticos u otro tipo de ventajas para el atacante, mientras que para la víctima puede implicar perjuicios significativos.

Entre los tipos de ataques que buscan infligir daño destacan:

- Ataques de denegación de servicio (DoS)
- Ataques distribuidos de denegación de servicio (DDoS)
- *Botnets y zombis*

- Ataques de destrucción de datos

Este enfoque, que va más allá del robo de información, es consistente con la taxonomía propuesta por Agrafiotis, Nurse, Goldsmith, Creese y Upton (2018), quienes identifican diversas formas de daño derivadas de ciberataques, incluyendo impactos físicos o digitales, económicos, psicológicos, reputacionales y sociales (Agrafiotis et al., 2018).

DoS

Un ataque DoS tiene como objetivo inutilizar una computadora o una red al saturarla con una gran cantidad de solicitudes o datos, sobrecargando el objetivo y evitando que responda adecuadamente a solicitudes legítimas. En muchos casos, las solicitudes enviadas por el atacante son legítimas por sí mismas (por ejemplo, peticiones comunes para cargar una página *web*). En otros casos, estas solicitudes aprovechan vulnerabilidades o protocolos para optimizar o potenciar el impacto del ataque.

Este tipo de ataque busca dañar la disponibilidad del sistema, sin necesidad de robar dinero o información directamente, sino simplemente interrumpir el servicio. Esta perspectiva está respaldada en revisiones académicas que describen cómo los atacantes consumen recursos del sistema para bloquear el acceso legítimo (Mahjabin et al., 2017).

Sea cual sea el método, los ataques de denegación de servicio operan al abrumar las unidades centrales de procesamiento (CPU) y/o la memoria de los sistemas informáticos. Esto se logra utilizando todo el ancho de banda de comunicación de red disponible y/o agotando los recursos de la infraestructura de red, como los enrutadores.

Ataques Distribuidos de Denegación de Servicio (DDoS); Un ataque DDoS se caracteriza por la colaboración de múltiples computadoras u otros dispositivos distribuidos geográficamente, que inundan el objetivo con una avalancha de solicitudes simultáneas como se representa en la Figura 11. Esta modalidad ha sido predominante entre los principales ataques recientes. Además, en algunos casos se han utilizado dispositivos no convencionales como cámaras conectadas a Internet o vehículos en lugar de depender solo de computadoras tradicionales. Esta técnica compromete la disponibilidad del sistema al sobrecargar sus recursos. Estas características están bien documentadas en estudios recientes sobre DDoS en entornos IoT, que analizan cómo grandes redes de dispositivos comprometidos ejecutan estas ofensivas masivas (Alahmadi et al., 2023).

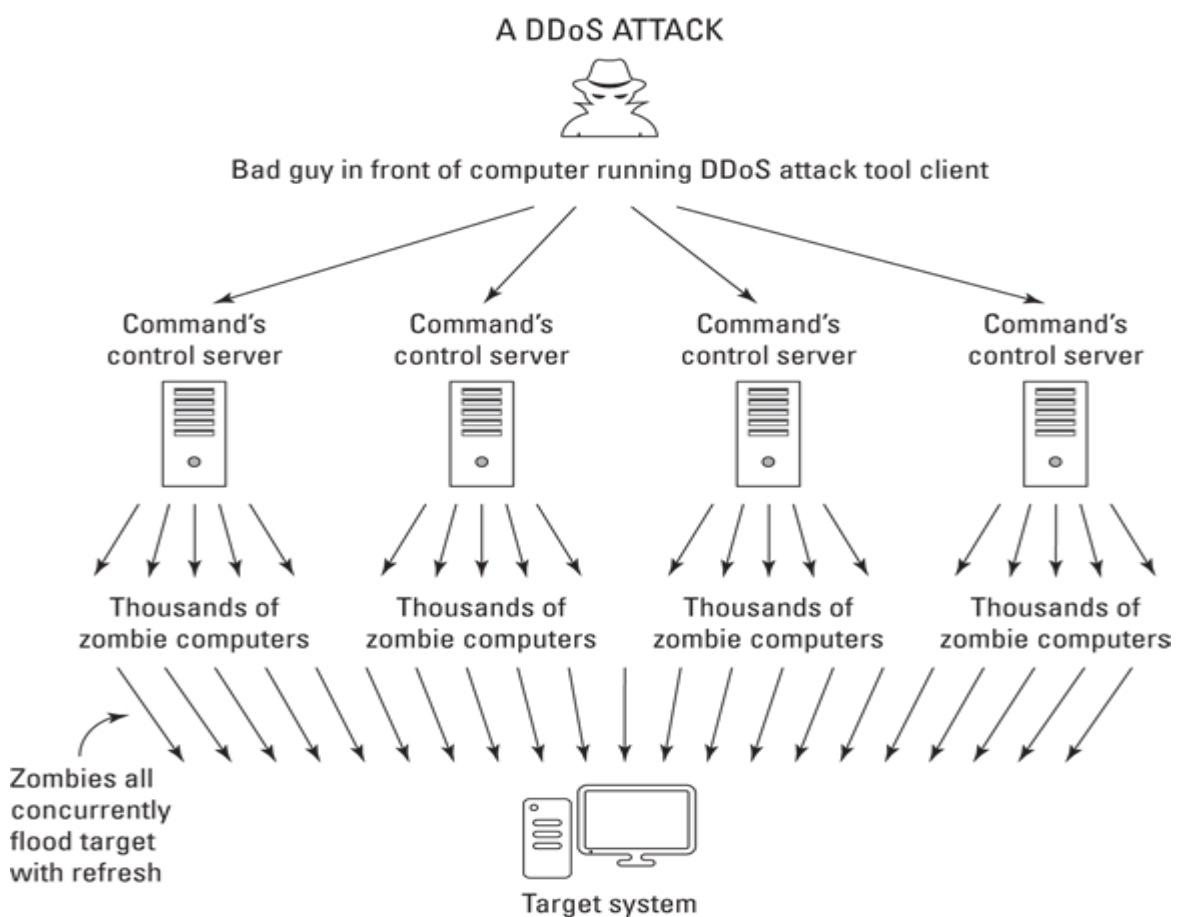


Figura 11. Ejemplo de ataque DDOS (Steinberg, 2019).

Botnets y zombies: Los *botnets* están formadas por redes de computadoras comprometidas ("*zombis*") que son controladas remotamente por un atacante sin que los dueños de los dispositivos lo sepan, estos dispositivos infectados pueden

coordinarse para realizar ataques masivos, del tipo DDoS, distribución de *malware* o campañas de *spam*. Por ejemplo, si un atacante infecta y controla un millón de computadoras, puede utilizarlas para enviar solicitudes masivas desde múltiples ubicaciones controladas lo que amplifica considerablemente el impacto del ataque.

Esta amenaza se analiza en la literatura relacionada a *botnets*, que describe cómo estos ataques distribuidos son posibles gracias a redes de *zombis* sincronizadas y controladas remotamente y que son mencionados por (Thanh Vu et al., 2021).

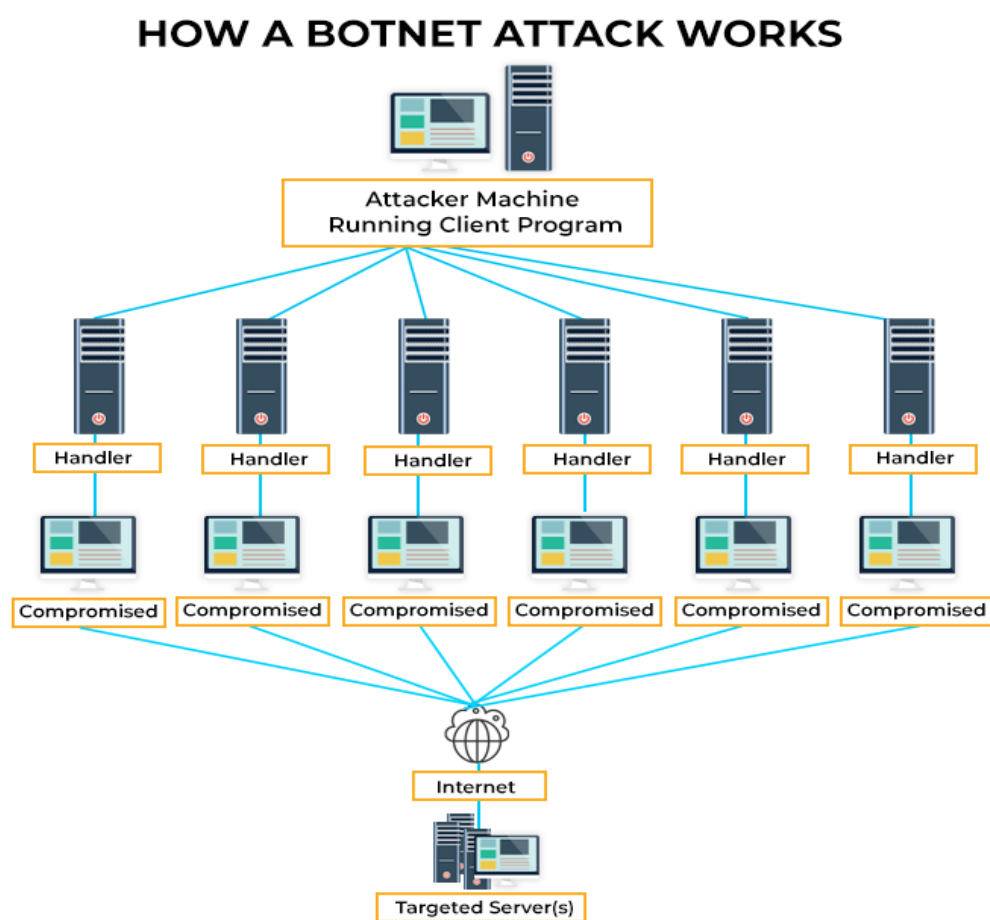


Figura 12. Ejemplo de ataques de Botnet, (Scott, 2020).

Los ataques de destrucción de datos buscan causar un daño más profundo que la interrupción temporal del servicio, su objetivo es destruir o corromper información y sistemas críticos del objetivo.

Por ejemplo, si la víctima rechaza pagar un rescate en un caso de *ransomware*, el atacante podría optar por emplear *malware* especializado en limpieza de datos ver Figura 13, que borra por completo la información del disco duro o SSD, dejándola irrecuperable. En ausencia de copias de seguridad, la víctima podría perder completamente el acceso a su *software* e información.

Los mismos motivos detrás de ataques DDoS pueden motivar estos ataques destructivos: más allá de la saturación, buscan la eliminación permanente de datos. Este fenómeno está documentado dentro del marco más amplio de "ataques a los datos", definidos como acciones que manipulan, destruyen o cifran información dentro de una red víctima (Thanh Vu et al., 2021).



Figura 13. Ejemplo de Ransomware en equipo infectado, (Vanderbilt, 2020).

Phishing

El *phishing* hace referencia a un intento de persuadir a una persona para que realice ciertas acciones, simulando ser una entidad confiable que, de manera razonable,

podría solicitar legítimamente al usuario llevar a cabo dichas acciones, por ejemplo, un perpetrador podría enviar un correo electrónico que aparenta provenir de un banco reconocido, solicitando al destinatario que haga clic en un enlace para restablecer su contraseña debido a una posible violación de datos. Al hacer clic en el enlace, el usuario es redirigido a un sitio web que aparenta ser parte del banco, pero que, en realidad, es una copia controlada por el delincuente. De esta manera, el atacante utiliza el sitio *web* fraudulento para recopilar información confidencial, como nombres de usuario y contraseñas del sitio bancario (Ping Wang & Peyton Lutchkus, 2023).

Phishing Dirigido (*spear phishing*): se refiere a ataques de *phishing* meticulosamente diseñados y dirigidos a una persona, empresa u organización específica. Si un delincuente busca obtener credenciales, por ejemplo, en el sistema de correo electrónico de una empresa en particular, enviará correos electrónicos específicamente diseñados para individuos específicos dentro de la organización ver ejemplo en Figura 14. Con frecuencia, los perpetradores que llevan a cabo *spear phishing* realizan investigaciones en línea sobre sus objetivos y utilizan la información compartida en exceso en las redes sociales para crear correos electrónicos que parezcan extraordinariamente auténticos (Halevi et al., 2015).

Por ejemplo, el siguiente tipo de correo electrónico suele ser mucho más convincente que "Inicie sesión en el servidor de correo y restablezca su contraseña":

“Hola, voy a tomar mi vuelo en diez minutos. ¿Puede iniciar sesión en el servidor Exchange y comprobar cuándo es mi reunión? Por alguna razón, no puedo entrar. Puedes intentar llamarme por teléfono primero por razones de seguridad, pero, si no me encuentras, continúa, verifica la información y envíamela por correo electrónico, ya que sabes que estoy recibiendo en un vuelo que está a punto de despegar”.

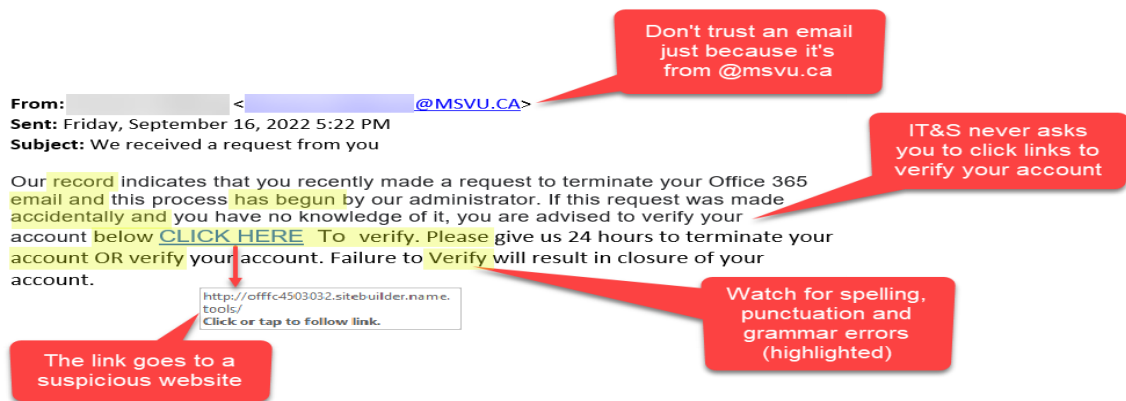


Figura 14. Ejemplo de Phising, (University, 2021).

El *vishing*, o *phishing* basado en voz, es *phishing* a través de POTS, que significa "servicio telefónico simple y antiguo". Sí, los delincuentes utilizan métodos antiguos y probados para estafar a las personas. Hoy en día, la mayoría de estas llamadas se transmiten mediante sistemas de voz sobre IP, pero, al final, los estafadores llaman a las personas a teléfonos normales de la misma manera que lo han estado haciendo durante décadas.

Man in the Middle: La interceptación se produce cuando los atacantes capturan información en tránsito entre computadoras. Si los datos no están cifrados de manera adecuada, la parte que realiza la interceptación puede aprovecharse de ellos de manera indebida ver ejemplo en Figura 15. Un tipo especial de interceptación se conoce como ataque de intermediario. En este caso, el intermediario transfiere los datos entre el remitente y el destinatario con el objetivo de ocultar la interceptación de datos. En este escenario, el "*proxy*" actúa como el intermediario que intercepta las solicitudes, las transmite (ya sea modificadas o sin modificar) a los destinos originales previstos, recibe las respuestas de esos destinos y las transmite de vuelta al remitente (también modificadas o sin modificar). La utilización de un *proxy* dificulta que el remitente detecte la interceptación, ya que recibe respuestas esperadas al comunicarse con un servidor (Conti et al., 2016).

Por ejemplo, un delincuente podría crear un sitio bancario falso y transmitir la información ingresada en el sitio falso al sitio real del banco, de esta manera, el delincuente puede responder con la misma información que el banco legítimo habría enviado. Este tipo de *proxy* no solo ayuda al delincuente a pasar desapercibido (un usuario que proporciona su contraseña al delincuente y luego realiza sus actividades

bancarias en línea puede no darse cuenta de ninguna anomalía durante la sesión), sino que también asegura al delincuente capturar la contraseña correcta. Si un usuario ingresa una contraseña incorrecta, el delincuente sabrá que debe solicitar la contraseña correcta.

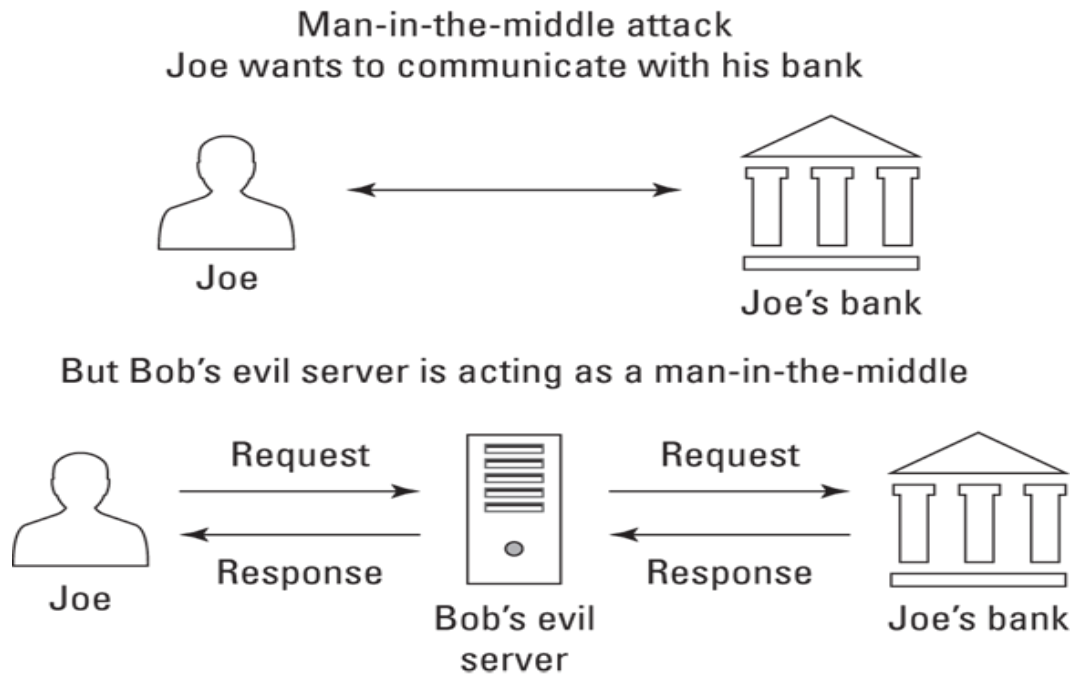


Figura 15. Ejemplo de ataque del hombre en Medio (Steinberg, 2019).

Malware

El *malware*, o *software* malicioso, es un término que engloba cualquier tipo de software diseñado con la intención de causar daño a sus usuarios, quienes generalmente no tienen conocimiento de que están ejecutando dicho *software*. Este concepto abarca una variedad de amenazas, como virus informáticos, gusanos, troyanos, *ransomware*, *scareware*, *spyware*, mineros de criptomonedas, *adware* y otros programas destinados a explotar recursos informáticos con propósitos malintencionados (Aboaoja et al., 2022).

Los virus informáticos representan ejemplos de *malware* que, al ejecutarse, se reproducen al insertar su propio código en los sistemas informáticos. Esta inserción suele ocurrir en archivos de datos, como macros no autorizadas dentro de documentos de *Word*, en áreas específicas de discos duros o unidades de estado sólido que contienen el código y los datos necesarios para iniciar un dispositivo

(también conocidos como sectores de inicio), o en otros programas informáticos (Salomon, 2010).

Similar a los virus biológicos, los virus informáticos requieren hosts para propagarse. Algunos de estos virus afectan de manera significativa el rendimiento de los sistemas que infectan, mientras que otros, al menos en ocasiones, pasan desapercibidos, aunque los virus informáticos aún causan daños extensos en todo el mundo, la mayoría de las amenazas significativas de *malware* en la actualidad se presentan en forma de gusanos y troyanos.

Los gusanos informáticos son piezas independientes de *malware* que se replican sin depender de hosts para su propagación. Suelen difundirse a través de conexiones al aprovechar vulnerabilidades de seguridad en las computadoras y redes objetivo, debido a su consumo de ancho de banda, los gusanos pueden causar daños sin necesidad de modificar sistemas o robar datos pueden ralentizar las conexiones de red, algo que a pocas personas les agrada experimentar en sus conexiones internas y de *Internet*.

Troyanos Los troyanos, apropiadamente llamados así por la famosa historia del caballo de Troya, son *malware* que se camufla como *software* no malicioso o se oculta dentro de una aplicación o dato digital legítimo y no malicioso por lo general, los troyanos se propagan mediante ingeniería social, engañando a las personas para que hagan clic en enlaces, instalen aplicaciones o ejecuten archivos adjuntos de correo electrónico, a diferencia de virus y gusanos, los troyanos no se autopropagan mediante tecnología; en cambio, dependen del esfuerzo (o más precisamente, de los errores) humanos (Salomon, 2010).

3. METODOLOGÍA

Investigación

El proceso de investigación se enfoca en crear y evaluar nuevos procesos, productos o métodos, en este caso implica el desarrollo de una plataforma de simulación en ambiente cliente servidor y la ejecución de simulaciones controladas para evaluar su efectividad en la capacitación en seguridad cibernética.

La elección de una metodología experimental se justifica por sus características clave: permite validar la validez interna mediante grupos controlados, asegurar replicabilidad del experimento, y medir resultados de manera objetiva y comparativa. Esta lógica de validación experimental ya fue aplicada en contextos de desarrollo de *software*: por ejemplo, (Khayretdinova & Kubach, 2019) presentan una metodología para la evaluación experimental de un asistente de *software*, utilizando estudios de caso controlados para comparar equipos apoyados por un asistente frente a equipos sin apoyo.

Características de la investigación

- **Manipulación de Variables:** La investigación implica la manipulación controlada de variables para observar cómo afectan a los resultados. En este caso, las variables podrían incluir características específicas de la plataforma de simulación, como la dificultad de cada una de las simulaciones, la inclusión de inteligencia artificial, o la distribución geográfica de los participantes.
- **Entorno Controlado:** Se estableció un entorno controlado para llevar a cabo las diferentes pruebas, esto permitió que las condiciones fueran adecuadas y que cualquier variación en los resultados pueda atribuirse a las modificaciones realizadas en la plataforma de simulación.
- **Medición Objetiva:** La investigación se basa en mediciones cuantificables, Se utilizaron métricas como el rendimiento de los participantes en escenarios simulados, tasas de detección de amenazas cibernéticas y tiempo de respuesta a incidentes para evaluar la eficacia de la plataforma.
- **Grupo de Control:** Se establecerá un grupo de control que experimente las manipulaciones realizadas en la plataforma

Objetivos de la investigación

- **Desarrollo de la Plataforma:** Diseñar y desarrollar la plataforma de simulación, incorporando características identificadas en la revisión de la literatura y los objetivos específicos de la investigación.
- **Evaluación de la Efectividad:** Evaluar la efectividad de la plataforma en términos de mejora en las habilidades y conocimientos en seguridad cibernética, Se utilizarán pruebas, simulaciones y evaluaciones prácticas para medir la plataforma en comparación con métodos tradicionales.
- **Comparación con Métodos Convencionales:** Comparar el rendimiento de los participantes que utilizan la plataforma de simulación distribuida con aquellos que siguen métodos convencionales de enseñanza en seguridad cibernética.
- **Análisis de Resultados Cuantitativos:** Realizar un análisis cuantitativo de los resultados obtenidos, utilizando estadísticas para determinar las diferencias observadas entre los grupos de control y experimentales.
- **Iteración y Mejora Continua:** Implementar mejoras en la plataforma en función de los resultados y retroalimentación obtenidos durante las fases experimentales, este enfoque de mejora continua ayuda a el perfeccionamiento de la plataforma a lo largo de la investigación.

Desarrollo

Para el desarrollo de la plataforma CyberSimU, se optó por emplear el Proceso Unificado Simplificado (SUP, por sus siglas en inglés: *Simplified Unified Process*) como enfoque metodológico. Esta elección se sustentó en la necesidad de contar con una metodología ágil, estructurada y adaptable al contexto particular del proyecto, el

cual fue desarrollado por un solo programador, bajo supervisión académica, con requerimientos claros, plazos limitados y necesidad de documentación mínima (Khayretdinova & Kubach, 2019).

El SUP es una variante ligera del Proceso Unificado (RUP) que conserva sus pilares fundamentales desarrollo iterativo, gestión de requisitos, arquitectura centrada y verificación continua, pero reduce significativamente la carga documental y la complejidad operativa, esto lo convierte en una alternativa viable para proyectos académicos o de pequeña escala con recursos limitados y alta necesidad de flexibilidad

Justificación de la elección del SUP

La elección del SUP responde a las siguientes condiciones del proyecto:

- Desarrollo individual: El proyecto fue ejecutado por un único desarrollador, lo que limitó la posibilidad de aplicar marcos colaborativos más complejos como SCRUM o XP. SUP permite mantener control y trazabilidad sin necesidad de un equipo extenso.
- Asesoría académica periódica: El modelo favorece la incorporación iterativa de mejoras a partir de revisiones continuas con el asesor, lo cual es coherente con la estructura de fases de SUP (inicio, elaboración, construcción y transición).
- Necesidad de agilidad y simplicidad: Al no requerirse una producción documental exhaustiva, el SUP permitió avanzar de forma práctica, enfocándose en la entrega funcional de simulaciones educativas sin sacrificar aspectos clave como control de versiones, pruebas y validación con usuarios reales.

Aplicación del SUP en CyberSimU

Durante la ejecución del proyecto, se adaptaron las cuatro fases del SUP de la siguiente manera:

1. Fase de inicio: Definición del problema, establecimiento de objetivos, análisis del contexto educativo, y levantamiento de requisitos.
2. Fase de elaboración: Diseño preliminar de las simulaciones, selección de tecnologías base (PHP, MySQL, *JavaScript*, *A-Frame*) y prototipado de interfaz.
3. Fase de construcción: Desarrollo de las nueve simulaciones, integración del módulo de lógica difusa, y vinculación con sistema de evaluación donde cada simulación fue probada por usuarios en ciclos cortos.
4. Fase de transición: Publicación en entorno web (<https://kevinvite.com/simulador/>), pruebas de funcionalidad con estudiantes, ajustes finales y documentación académica del proceso.

Esta metodología permitió alcanzar un equilibrio en la estructura formal, facilitando la construcción de un producto funcional alineado con estándares académicos, pedagógicos y técnicos.

Aplicación del modelo ADDIE en el diseño instruccional de las simulaciones

El diseño de las simulaciones desarrolladas en la plataforma CyberSimU se apoyó en el modelo instruccional ADDIE, un enfoque ampliamente adoptado en la planeación y desarrollo de recursos educativos (Moses Adeleke Adeoye et al., 2024), esta metodología, que hace referencia al acrónimo corresponde a las fases de Análisis, Diseño, Desarrollo, Implementación y Evaluación, permitió estructurar el contenido educativo de manera coherente para que el aprendizaje sea significativo y adaptable a los estudiantes de nivel superior.

El uso de ADDIE en este proyecto responde a la necesidad de construir experiencias formativas que no solo fueran funcionales, sino también en la práctica educativa efectiva, sobre todo desde en un contexto donde se requiere desarrollar habilidades prácticas en ciberseguridad mediante el aprendizaje activo y la interacción con entornos simulados.

Justificación de uso del modelo ADDIE en CyberSimU

El modelo ADDIE fue especialmente adecuado por las siguientes razones:

- a) Enfoque centrado en el estudiante: permite adaptar los objetivos y contenidos al nivel de conocimientos previo de los participantes, los cuales fueron evaluados con un *Pre-Test*.
- b) Flexibilidad estructural: Su carácter iterativo se acopló a las mejoras continuas realizadas tras pruebas piloto y retroalimentación docente-estudiantil.
- c) Orientación práctica: Ayuda en la alineación de competencias, actividades simuladas y mecanismos de evaluación.

Aplicación de las fases de ADDIE

Durante el desarrollo de las simulaciones en **CyberSimU**, se siguieron las fases propuestas por el modelo instruccional **ADDIE**, aplicando acciones concretas en cada fase clave Figura 16 :

- I. **Análisis:** Se identificaron las necesidades formativas tanto en niveles básicos como avanzados de ciberseguridad a través de una revisión sistemática de literatura, complementada con sesiones de discusión con la dirección académica de la tesis.
- II. **Diseño:** Se establecieron los objetivos de aprendizaje, en donde se estructuraron las interacciones de cada simulador y un flujo lógico de tareas, retos y pruebas para cada uno.
- III. **Desarrollo:** Se construyeron los entornos utilizando tecnologías web, agregando componentes del tipo visuales, funcionales y de retroalimentación inmediata dentro de una arquitectura cliente-servidor.
- IV. **Implementación:** Las simulaciones fueron cargadas en la página web (<https://kevinvite.com/simulador/>) y se realizaron sesiones guiadas con estudiantes para asegurar su correcta aplicación y adopción.
- V. **Evaluación:** Se aplicaron instrumentos cuantitativos (*Pre-Test* y *Post-Test*) Figuras 17 y 18 y cuestionarios de funcionalidad basados en la norma

ISO/IEC 25010 Figura 19, lo que permitió validar la experiencia del usuario y su opinión respecto a elementos educativos

La incorporación del modelo ADDIE en entornos tecnológicos está ampliamente documentada. Por ejemplo, un artículo de una revisión sistemática reciente demuestra la flexibilidad del modelo ADDIE al integrarse exitosamente con herramientas digitales para fortalecer el diseño instruccional y adaptarlo a diversos contextos educativos, optimizando enseñanza-aprendizaje (Abuhassna et al., 2024)

De igual forma, indagaciones llevadas a cabo en contextos de aprendizaje virtual han arrojados hallazgos prácticos palpables a través de enfoques casi experimentales; en ellos, el uso del modelo ADDIE en plataformas tipo *Blackboard* propició notables avances tanto en las aptitudes académicas como en la eficiencia didáctica (Almelhi,2021).

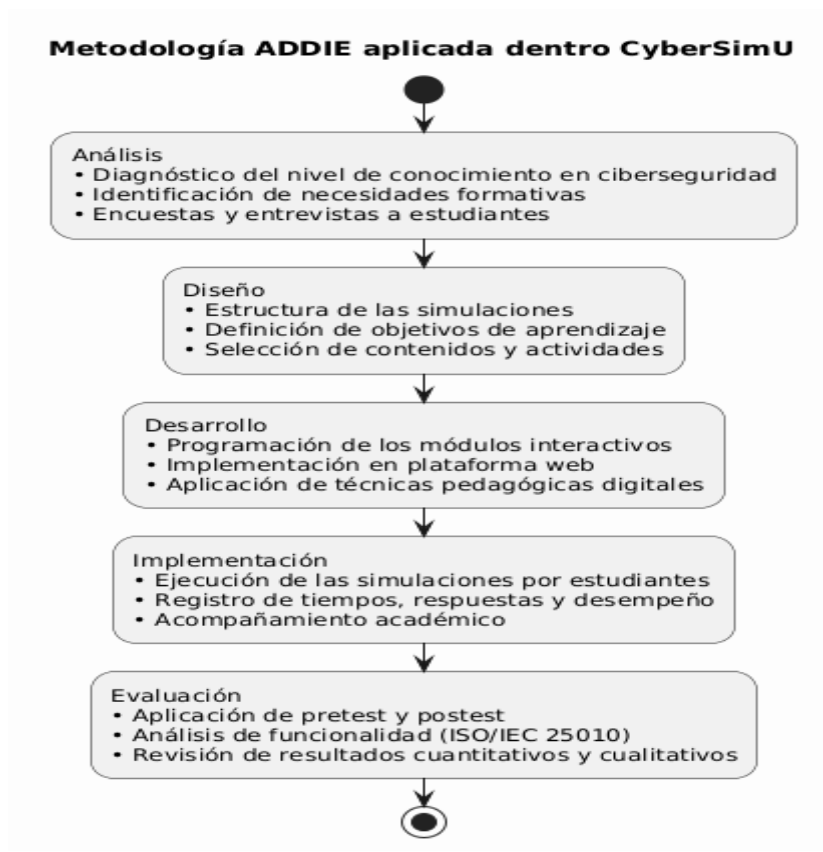


Figura 16. Metodología ADDIE dentro de CyberSimU.

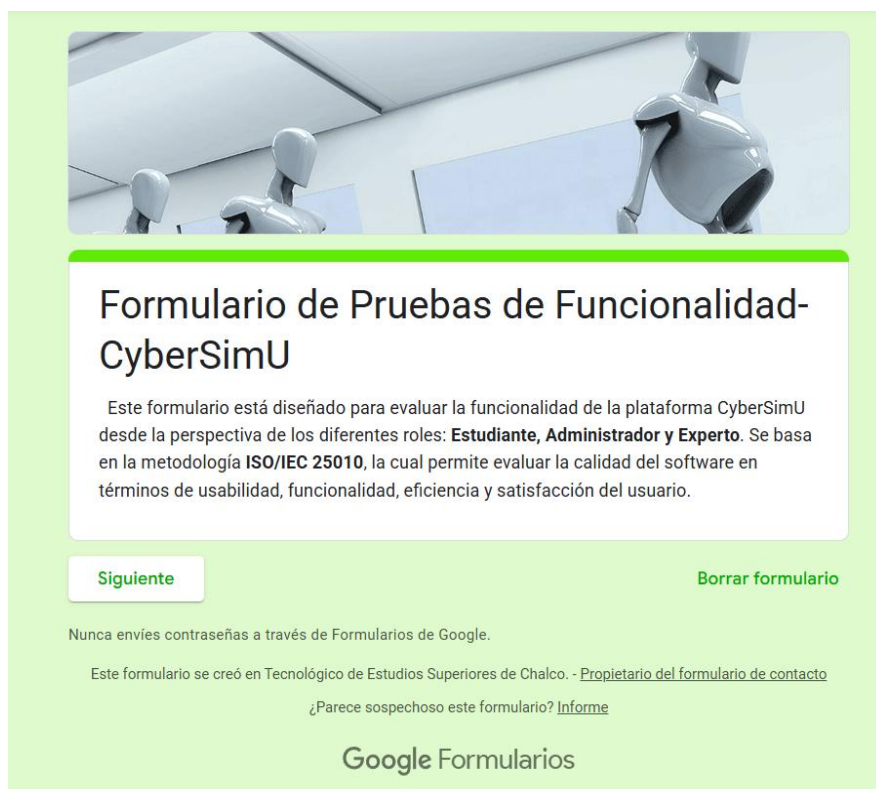
Esta metodología garantiza que el diseño instruccional de proyectos como CyberSimU sea sólido, replicable y alineado con buenas prácticas en el ámbito de la educación basada en tecnología y como en este caso en el desarrollo aplicado a los simuladores, promoviendo la apropiación activa del conocimiento por parte del estudiante.



Figura 17. Cuestionario Pre-test aplicado a estudiantes universitarios.



Figura 18 Cuestionario Post-Test aplicado a estudiantes universitarios



Formulario de Pruebas de Funcionalidad-CyberSimU

Este formulario está diseñado para evaluar la funcionalidad de la plataforma CyberSimU desde la perspectiva de los diferentes roles: **Estudiante, Administrador y Experto**. Se basa en la metodología **ISO/IEC 25010**, la cual permite evaluar la calidad del software en términos de usabilidad, funcionalidad, eficiencia y satisfacción del usuario.

[Siguiente](#) [Borrar formulario](#)

Nunca envíes contraseñas a través de Formularios de Google.

Este formulario se creó en Tecnológico de Estudios Superiores de Chalco. - [Propietario del formulario de contacto](#)

¿Parece sospechoso este formulario? [Informe](#)

Google Formularios

Figura 19. Cuestionario de Funcionalidad de acuerdo con ISO/IEC 25010.

Al concluir esta sección, se subraya que la combinación del Proceso Unificado Simplificado (SUP) y el modelo instruccional ADDIE y como este aportó un marco metodológico alineando el desarrollo técnico ágil con un diseño educativo estructurado y centrado en el estudiante. La adopción del SUP permitió aplicar eficientemente el ciclo de vida del *software* dentro de un contexto de recursos limitados, manteniendo coherencia entre las fases de análisis, elaboración, construcción y transición. Por otro lado, el modelo ADDIE, ampliamente reconocido en entornos de educación a distancia como guía efectiva para el diseño instruccional, asegura que el diseño, desarrollo, implementación y evaluación del contenido estén sistemáticamente alineados con los objetivos pedagógicos. Asimismo, la evaluación bajo la norma ISO/IEC 25010 entregó una base estándar internacional para valorar cualidades como la usabilidad, eficiencia, seguridad y satisfacción del *software*, contribuyendo al aseguramiento de calidad del producto final (Estdale & Georgiadou, 2018). En conjunto, estas metodologías fortalecen la validez técnica como educativa de CyberSimU, proporcionando un marco replicable y con respaldo académico para futuras investigaciones y desarrollos en formación en ciberseguridad.

4. RESULTADOS

En esta sección se presentan resultados obtenidos a lo largo del desarrollo de la investigación, detallando los aspectos clave del proyecto, se describirá desde la elección del nombre de la plataforma que se desarrolló, su desarrollo, las tecnologías utilizadas, y las evidencias correspondientes a cada fase que se estuvo llevando a cabo dentro de la investigación, además, se abordarán los productos generados para la divulgación científica, resultado de este trabajo, finalmente se explicarán la interpretación de los resultados obtenidos a través de las diferentes técnicas de recolección de datos, en las universidades en donde se tuvo el permiso para llevar a cabo las pruebas.

Elección del nombre CyberSimU

El nombre CyberSimU véase Figura 20, surge como una propuesta que hace alusión a la ciberseguridad (*Cyber*) y la simulación universitaria (*SimU*), esta denominación responde tanto a criterios funcionales como pedagógicos, buscando reflejar la naturaleza y los objetivos del sistema desarrollado.

Desglosando la palabra, el prefijo *Cyber*, alude de forma directa al ámbito temático central del proyecto el cual es la seguridad informática, y su inclusión en el nombre permite una asociación inmediata con los contenidos abordados en las simulaciones, por su parte, el elemento *SimU* es una contracción de “Simulación Universitaria”, la cual enfatiza el enfoque educativo y práctico, las simulaciones desarrolladas están orientadas a estudiantes de nivel superior, con el propósito de facilitar la comprensión y aplicación de conceptos clave en ciberseguridad mediante entornos interactivos, intuitivos y controlados.



Figura 20 Logotipo CyberSimU

Opinión estudiantil sobre la importancia de la ciberseguridad en instituciones educativas

Como parte del presente trabajo, se aplicó una encuesta en la asignatura Administración de PYMES, con el objetivo de conocer la percepción de estudiantes de diversas instituciones educativas respecto a la enseñanza de la ciberseguridad, la encuesta fue respondida por un total de 174 participantes, los resultados obtenidos reflejan un alto nivel de interés en el tema, tal como se muestra en la gráfica correspondiente véase Figura 21, el 74.1% de los encuestados considera que la ciberseguridad es “muy importante” en su institución, mientras que un 23% la califica como “importante”, esto ayuda a identificar una clara conciencia sobre la relevancia del tema dentro del entorno académico.

La inclusión de estos datos refuerza la pertinencia del desarrollo de plataformas como *CyberSimU*, al responder a una necesidad identificada directamente entre los estudiantes: contar con herramientas prácticas y formativas que fortalezcan sus competencias en seguridad informática, los resultados completos de la encuesta realizada se pueden consultar en el Anexo 1.

¿Qué tan importante considera la ciberseguridad en su institución educativa?

174 respuestas

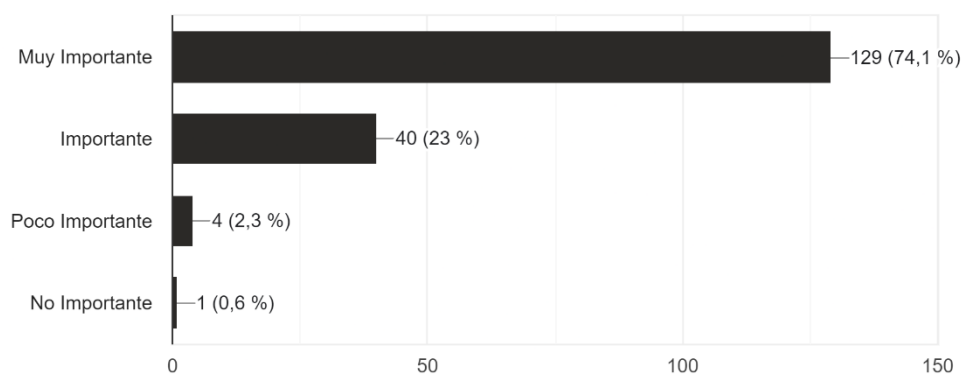


Figura 21. Resultados de encuesta de participación de estudiantes sobre temas relacionados a ciberseguridad.

Grupo de control: Estudiantes con conocimientos previos en seguridad informática

Durante la implementación de la fase experimental del proyecto *CyberSimU*, se identificó un subconjunto de participantes que, por su perfil académico y grado de formación, fueron considerados como grupo de control con conocimientos previos en ciberseguridad. Este grupo estuvo conformado por 29 estudiantes de la carrera de Ingeniería Informática del octavo semestre del Tecnológico de Estudios Superiores de Chalco, quienes habían cursado previamente asignaturas especializadas en seguridad informática y contaban con una base teórica y práctica más sólida que el resto de los participantes, se anexan las evidencias correspondientes de las pruebas a los estudiantes en el Anexo 3.

A diferencia de un grupo de control tradicional que no recibe tratamiento, en este caso particular, los estudiantes sí participaron activamente en las simulaciones desarrolladas en la plataforma *CyberSimU* (Bobrownicki et al., 2022). No obstante, su experiencia previa permitió establecer una línea comparativa diferenciada para observar cómo se comporta la plataforma frente a usuarios con distintos niveles de competencia en la temática.

Este enfoque permitió realizar análisis respecto a:

- El nivel de desafío percibido por los participantes con experiencia.
- Las diferencias en la progresión de puntajes entre estudiantes expertos y novatos.
- La validación de la dificultad y pertinencia de las simulaciones diseñadas.

La participación de este grupo contribuyó significativamente a validar la utilidad del simulador como herramienta educativa transversal, al demostrar que incluso para usuarios con antecedentes formativos en ciberseguridad, *CyberSimU* representó un recurso útil para reforzar, aplicar y evaluar sus conocimientos en un entorno simulado y controlado.

Además, los resultados obtenidos por este grupo aportaron una referencia cuantitativa para contrastar los avances observados en estudiantes de menor

trayectoria académica, ayudando así a establecer indicadores diferenciales de aprendizaje y efectividad del entorno virtual desarrollado.

Desarrollo del simulador

La plataforma fue diseñada para funcionar directamente desde el navegador, sin necesidad de instalaciones adicionales. Esto se logró mediante tecnologías *web* como HTML5, CSS, *JavaScript*, *PHP*, y *A-Frame*, integradas a una base de datos MySQL. El desarrollo siguió principios de programación ágil, permitiendo ajustar cada módulo con base en retroalimentación directa de usuarios durante la etapa de pruebas.

El simulador quedó hospedado en la siguiente dirección de internet <https://kevinvite.com/simulador/>, véase Figura 22, desde donde los estudiantes pueden acceder a sus simulaciones, visualizar resultados, recibir recomendaciones de estudio generadas por lógica difusa y consultar reportes. Se establecieron dos perfiles de usuario: administrador y estudiante, cada uno con funcionalidades diferenciadas.



Figura 22. Sitio principal de CyberSimU para ejecución de simulaciones.

A partir de una revisión sistemática fundamentada con el marco de trabajo *SALSA Framework*, que abarcó artículos publicados entre 2019 a 2023, se establecieron los temas prioritarios a abordar dentro del simulador, en consecuencia, las simulaciones

actualmente implementadas corresponden a los siguientes ámbitos de la ciberseguridad:

- *Phishing*: Se diseñó un entorno que permite a los estudiantes identificar y responder a intentos de suplantación de identidad a través de correos electrónicos y sitios web fraudulentos.
- Denegación de Servicio (DoS y DDoS): Se ha desarrollado una simulación interactiva donde los participantes pueden visualizar y comprender el impacto de ataques de denegación de servicio en sistemas informáticos.
- Troyanos y *Malware*: Se han agregado a la plataforma escenarios donde los estudiantes pueden resolver diversos ejercicios y aprender diferentes tipos de amenazas y aplicar estrategias de detección y mitigación.

Las simulaciones han sido diseñadas de manera que permiten que los estudiantes avancen desde conceptos básicos hasta situaciones más complejas, con el objetivo de fortalecer su capacidad de análisis y respuesta ante incidentes de ciberseguridad.

Descripción de simulaciones

La plataforma de simulación incluye nueve escenarios, cada uno diseñado para abordar un tipo específico de amenaza relacionada con la ciberseguridad, las simulaciones fueron ordenadas de manera consecutiva, con el fin de ayudar a gestionar el aprendizaje de conceptos nuevos, cada escenario plantea una situación que requiere, toma de decisiones y ejecución de acciones por parte del usuario.

Simulación 1: Introducción a consolas y comandos básicos

Este primer escenario tuvo como objetivo inducir al estudiante en el uso básico de la terminal de comandos en sistemas operativos basados en Linux ver Figura 23, la simulación contiene diversos retos interactivos donde los participantes debían ejecutar instrucciones para resolver tareas, tales como la navegación por directorios, creación y eliminación de archivos, así como el uso de comandos de ayuda.

Durante el desarrollo de la actividad, cada tarea incluyó una breve explicación sobre el comando utilizado y un problema práctico a resolver, el sistema asignó puntos por cada respuesta correcta, penalizando con una reducción en la puntuación en caso de errores, además, se integró una prueba teórica al finalizar la práctica para reforzar la comprensión de los conceptos abordados, además como apoyo adicional, se habilitó el uso del comando *help*, que permitió a los estudiantes consultar su progreso y las tareas pendientes.

Este escenario fue diseñado como una base introductoria para los siguientes módulos, y sirvió también para diagnosticar el nivel inicial de familiaridad de los participantes con la línea de comandos.

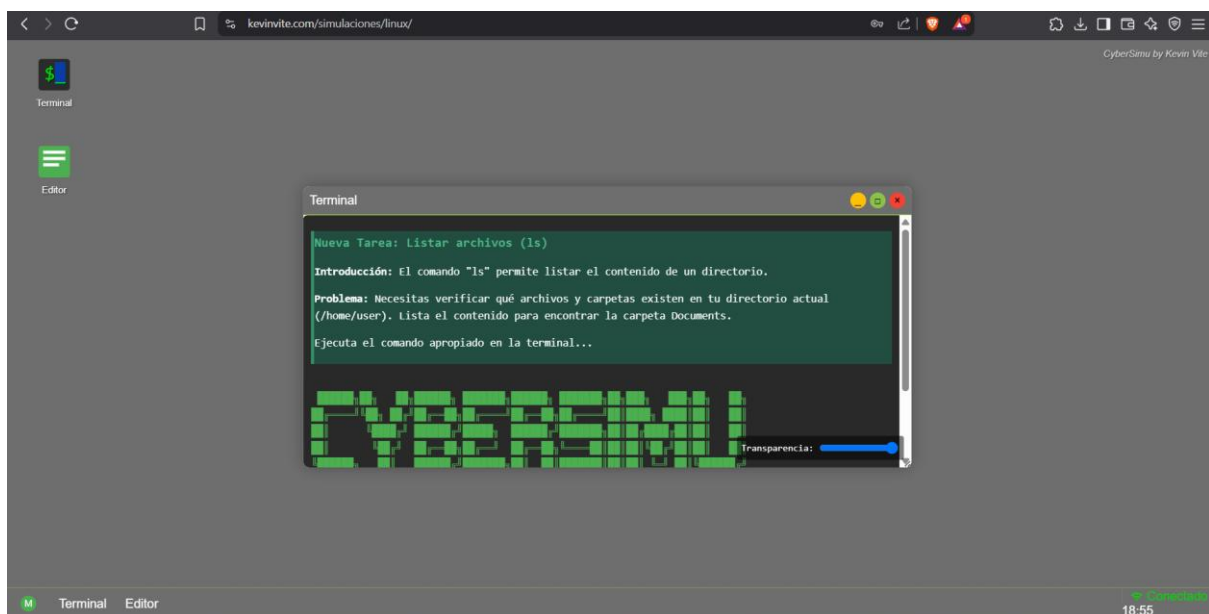


Figura 23. ejemplo de simulación de la línea de comandos en Linux.

Simulación 2: Entrenamiento de Consolas en Windows

La segunda simulación se enfocó fortalecer las capacidades de los estudiantes en sistemas operativos Windows y resolver los diferentes retos presentados en la pantalla ver Figura 24, todo esto haciendo uso de la consola CMD (*Command Prompt*), dentro de este escenario tuvo como objetivo que los participantes desarrollaran habilidades para operar desde la línea de comandos, tópicos necesarios para poder iniciar una buena especialización en el área de ciberseguridad.

Durante la práctica, los usuarios debían resolver distintos retos introduciendo comandos que les permitieran realizar las actividades como navegar entre directorios, listar archivos, gestionar procesos, y consultar configuraciones básicas del sistema, el entorno otorgaba puntos por cada respuesta correcta y aplicaba penalizaciones en caso de errores, el simulador también ofrecía la posibilidad de utilizar el comando *help* en cualquier momento, con el propósito de brindar apoyo contextual sin abandonar el entorno práctico, al finalizar la sesión, se mostraba una puntuación total, lo que permitía al estudiante valorar su desempeño de forma inmediata.

Esta simulación resulta particularmente relevante debido a que muchas herramientas de ciberseguridad en sistemas *Windows* requieren competencias mínimas en el uso del CMD para ejecutar scripts, validar configuraciones o realizar diagnósticos en equipos comprometidos.

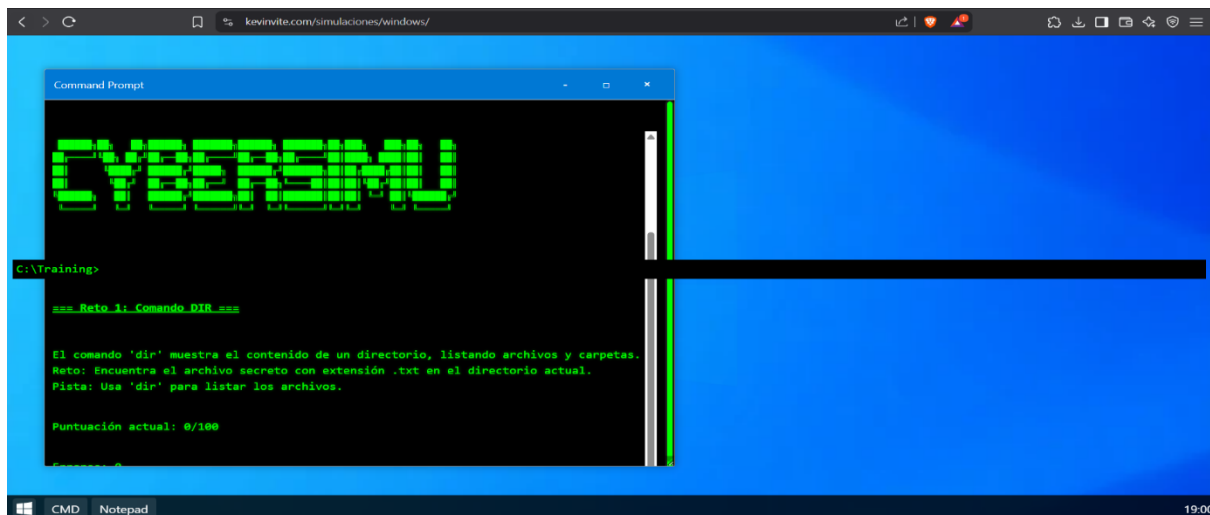


Figura 24. Simulación de Entrenamiento de Consolas Windows.

Simulación 3: Escaneo de Puertos con Nmap

Esta simulación introdujo a los estudiantes en el uso básico de **Nmap**, una herramienta ampliamente utilizada en ciberseguridad para el reconocimiento de redes y escaneo de puertos, el objetivo principal fue familiarizar a los participantes con los distintos tipos de reconocimiento, en especial aquellos que forman parte del proceso de recolección de información previa al análisis de vulnerabilidades ver Figura 25.

El escenario abarcó tanto el reconocimiento pasivo como el activo, en el primer caso, se incluyeron prácticas con comandos *WHOIS*, consultas DNS y búsqueda de

información en motores abiertos, de forma consecutiva, se avanzó al reconocimiento activo mediante la ejecución de escaneos con Nmap, permitiendo observar la respuesta de un *host* específico frente a diferentes configuraciones de exploración.

Entre los comandos disponibles en el simulador se incluyeron:

- `nmap 192.168.1.100` – escaneo básico de puertos,
- `nmap -p- 192.168.1.100` – escaneo completo de todos los puertos,
- `nmap -sV 192.168.1.100` – detección de versiones de servicios,
- `nmap -O 192.168.1.100` – detección del sistema operativo.

Esta simulación fue diseñada para resaltar la importancia del reconocimiento en entornos reales de análisis de seguridad, siendo una etapa clave dentro del ciclo de pruebas de penetración, además, permitió que los estudiantes comprendieran las diferencias entre escaneo discreto y técnicas más invasivas, fortaleciendo su criterio técnico al momento de planificar una auditoría de red.



Figura 25. Simulador de Escáner de Puertos Nmap.

Simulación 4: Ataques de Denegación de Servicio Distribuidos (DDoS)

En este escenario se recreó un ataque de denegación de servicio distribuido con el fin de ilustrar las fases esenciales del fenómeno y las señales que indican un estado de sobrecarga en el servidor, el estudiante configuraba inicialmente tres parámetros; el primero la dirección IP objetivo, el segundo es el número de peticiones por segundo y por último la duración del ataque ver Figura 26.

Una vez iniciado el ejercicio, la interfaz mostraba en tiempo real el tráfico legítimo generado por dispositivos domésticos, tales como, una Smart TV, un altavoz inteligente, una cámara de seguridad y tráfico malicioso, este último estaba representado con un código de color distinto con el objetivo de identificar los diversos elementos, el gráfico incluyó contadores dinámicos de solicitudes, latencia y tasa de errores, de modo que el participante pudiera percibir de forma inmediata la degradación del servicio.

La práctica se basó en encontrar la combinación de intensidad (peticiones > 15 por segundo) y persistencia (duración > 10s) capaz de saturar el servidor, aún en la ejecución del proceso, era posible detener o reiniciar el ataque sin perder el registro de eventos. Al finalizar, el sistema arrojaba un reporte detallado que incluía una vista temporal donde mostraba si el servidor había entrado en estado crítico, así como el volumen total de peticiones que fueron procesadas y las distintas recomendaciones a seguir para la mitigación de DDoS (filtrado de tráfico, balanceo de carga y límite de *rate*).

Esta simulación permitió que el alumnado comprendiera, en un entorno controlado, la diferencia entre tráfico benigno y malicioso, y visualizara los principales indicadores de alerta que preceden la interrupción del servicio, sentando las bases para módulos posteriores de defensa activa.

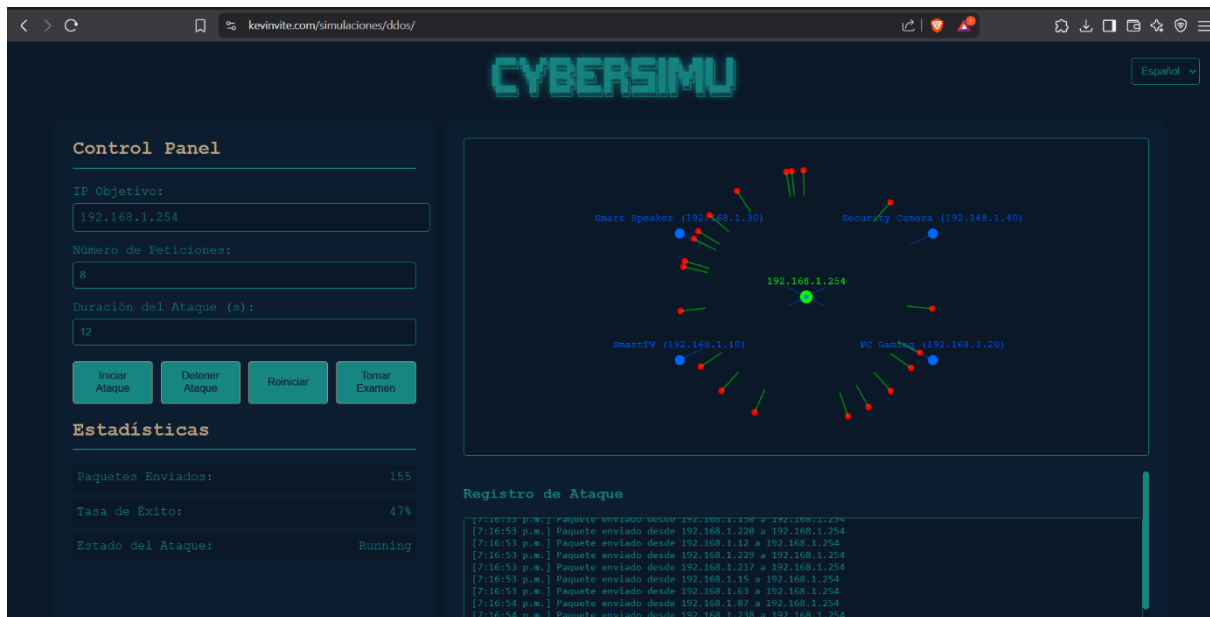


Figura 26. Simulador de ataque DDos en funcionamiento.

Simulación 5: Sistema Comprometido

En este escenario, se representó un entorno en el que un equipo informático es comprometido y transformado en un “zombie”, es decir, un sistema controlado de forma remota por un atacante con fines maliciosos, la simulación en cuestión permitió a los estudiantes explorar de forma didáctica los indicadores de compromiso, así como la ejecución de medidas defensivas para tratar de neutralizar las distintas amenazas activas ver Figura 27.

El sistema, en principio presentaba señales de infección como son: presencia de malware, un *backdoor* habilitado para acceso remoto, un *rootkit* que ocultaba la actividad maliciosa y un troyano era utilizado para enviar ataques hacia otros dispositivos conectados.

Así mismo, se podían inspeccionar los nodos de la red simulada, identificando comportamiento sospechoso y tomando decisiones basadas en evidencia.

La simulación disponía de cuatro herramientas principales:

1. Escanear Sistema: localiza *software* malicioso activo
2. Eliminar *Backdoor*: interrumpe el acceso no autorizado

3. Analizar Tráfico: identifica conexiones salientes sospechosas
4. Restaurar *Backup*: restablece el sistema a un estado funcional seguro

El objetivo era que el estudiante lograra detectar y eliminar las amenazas antes de que el sistema comprometido causara daños mayores a la infraestructura simulada, este módulo reforzó la capacidad de análisis ante escenarios de respuesta a incidentes y brindó un acercamiento más práctico a la noción de persistencia y movimiento lateral dentro de una red.



Figura 27. Simulación de Sistema Comprometido.

Simulación 6: *Sniffing* de Red

Este módulo permitió a los estudiantes comprender, de forma visual y práctica, el funcionamiento básico de un ataque de *sniffing* en una red local, esta técnica, comúnmente utilizada por *hackers* malintencionados, consiste en la interceptación del tráfico de red con el fin de capturar datos sensibles que viajan sin cifrado o mediante protocolos vulnerables como lo pueden ser el protocolo TCP/IP ver Figura 28.

Durante la simulación, se ilustraron las acciones realizadas por un atacante que utiliza un “*sniffer*”, es decir, una herramienta capaz de capturar paquetes que transitan entre dispositivos conectados a la misma red, entre los objetivos que se

mostraron como vulnerables se incluyeron contraseñas transmitidas en texto plano, mensajes intercambiados entre usuarios, y datos de autenticación.

Además de la captura de información, la actividad permitió observar cómo este tipo de ataque puede escalar hacia un ataque de tipo *man-in-the-middle*, donde el atacante no solo escucha, sino que puede modificar el contenido de los mensajes antes de que lleguen a su destinatario.

La simulación se enfocó en resaltar la importancia de:

- Usar cifrado en las comunicaciones (por ejemplo, HTTPS),
- Evitar redes abiertas sin protección,
- Identificar patrones anómalos en el tráfico de red.

Este escenario ayudó a reforzar la noción de que muchas vulnerabilidades no dependen exclusivamente de fallas técnicas, sino también de configuraciones débiles o malas prácticas comunes entre los usuarios.

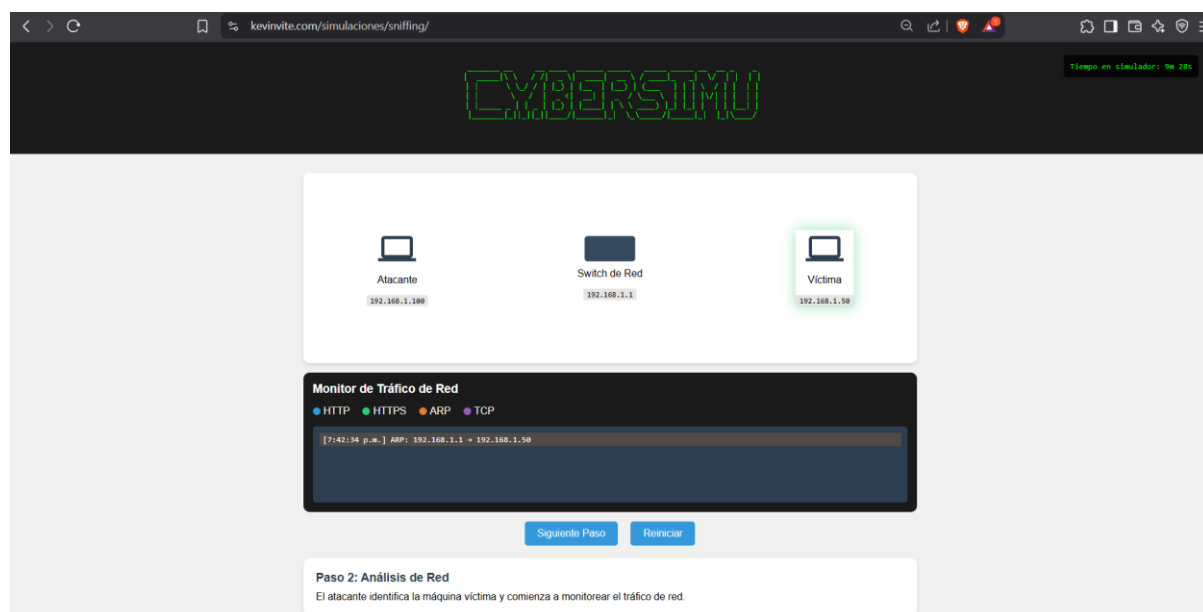


Figura 28. Sniffing de Red en funcionamiento.

Simulación 7: Técnicas de evasión en post-explotación

En la séptima práctica el énfasis se trasladó a la fase post-explotación, momento en que un atacante tras comprometer un objetivo busca afianzar su presencia y mantenerse fuera del radar de los sistemas de detección, la actividad dentro del

simulador se dividió en tres apartados interactivos, cada uno dedicado a una técnica de evasión distinta:

1. **Esteganografía**

El estudiante observó cómo información sensible puede ocultarse dentro de archivos aparentemente inofensivos (imágenes, audio o documentos). Se mostraron métodos de inserción *bit-a-bit* sin alteración perceptible y rutinas para extraer los datos encubiertos, destacando por qué este recurso dificulta el análisis forense cuando no se dispone de huellas previas.

2. **Tunneling**

Se demostró la encapsulación de tráfico malicioso a través de protocolos legítimos (por ejemplo, SSH o HTTP) con el fin de sortear cortafuegos y sistemas de inspección profunda de paquetes, el participante ajustó parámetros de un túnel y comprobó cómo el tráfico quedaba camuflado dentro de un flujo cifrado, retrasando su identificación por parte de un IDS.

3. **Log Wiping**

En la última sección se abordó la manipulación de registros del sistema, la consigna consistió en localizar eventos críticos inicio de sesión, escalamiento de privilegios, creación de servicios y ensayar rutinas de borrado selectivo, manteniendo la coherencia temporal para evitar anomalías obvias. Se hizo hincapié en que la ausencia total de registros suele levantar sospechas, por lo que la modificación sutil resulta más efectiva que el vaciado completo.

Como última parte de la simulación, un cuestionario de opción múltiple permitió verificar la comprensión de los riesgos y las contramedidas asociadas, el ejercicio dejó claro que las técnicas de persistencia y ocultamiento representan un reto constante para los equipos de defensa, subrayando la importancia de la monitorización continua y la correlación de eventos para detectar indicadores de compromiso aparentemente aislados ver Figura 29.

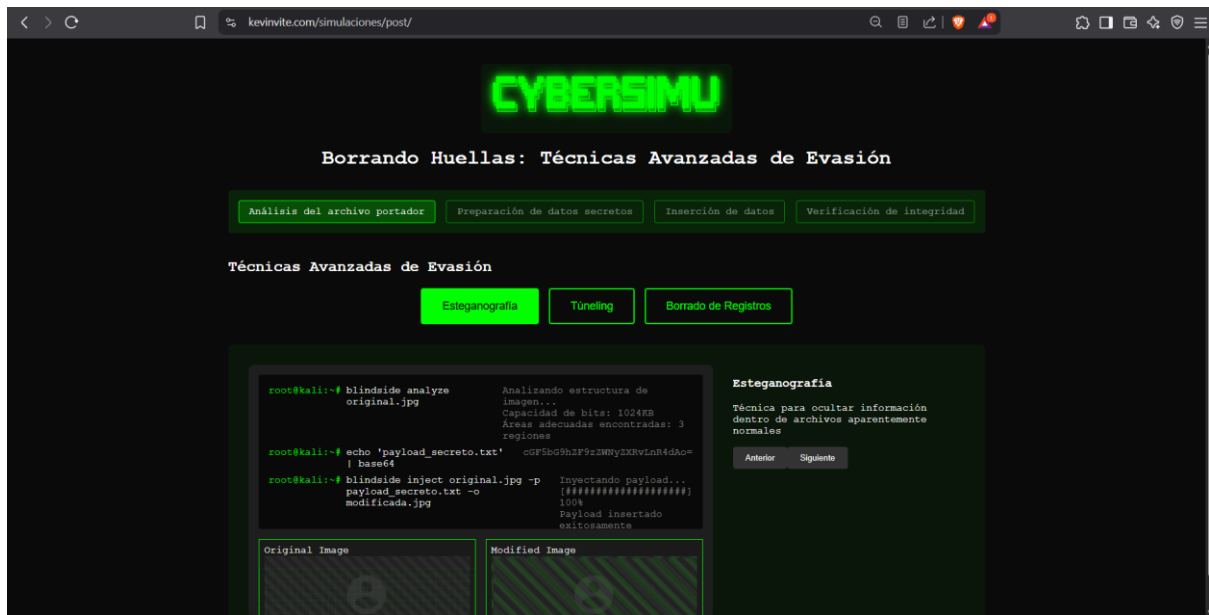


Figura 29. Simulación de Post Explotación en funcionamiento.

Simulación 8: Simulador de *Phishing*

Este escenario tuvo como objetivo entrenar a los estudiantes en la identificación de correos electrónicos maliciosos, mediante la simulación de situaciones realistas de ingeniería social, específicamente ataques de tipo *phishing*, la actividad consistió en el análisis de distintos mensajes de correo electrónico con el fin de distinguir entre comunicaciones legítimas y mensajes fraudulentos, durante la simulación, el participante debía inspeccionar el contenido de cada correo y tomar una decisión fundamentada antes de marcarlo como seguro o sospechoso, para ello, se integraron herramientas de análisis como el comando *dig* dominio.com, utilizado para consultar registros DNS del dominio remitente, y *whois* dominio.com, que permitía obtener información sobre la fecha de registro y datos administrativos del sitio ver Figura 30.

Además de los análisis técnicos, se generó la instrucción para detectar patrones clásicos asociados al *phishing*, tales como:

- Errores ortográficos o gramaticales evidentes,
- Tono de urgencia o presión para actuar rápidamente,
- Solicitudes inusuales de credenciales o información sensible.

Al emplear y llevar a cabo el ejercicio, este brinda múltiples beneficios como son, el evaluar la capacidad técnica del estudiante y el evaluar el criterio para conocer señales contextuales del ataque. Al concluir el reto, se da retroalimentación inmediata de cada selección tomada, fortaleciendo la comprensión sobre las distintas estrategias utilizadas por los atacantes y las prácticas recomendadas para la prevención de incidentes.

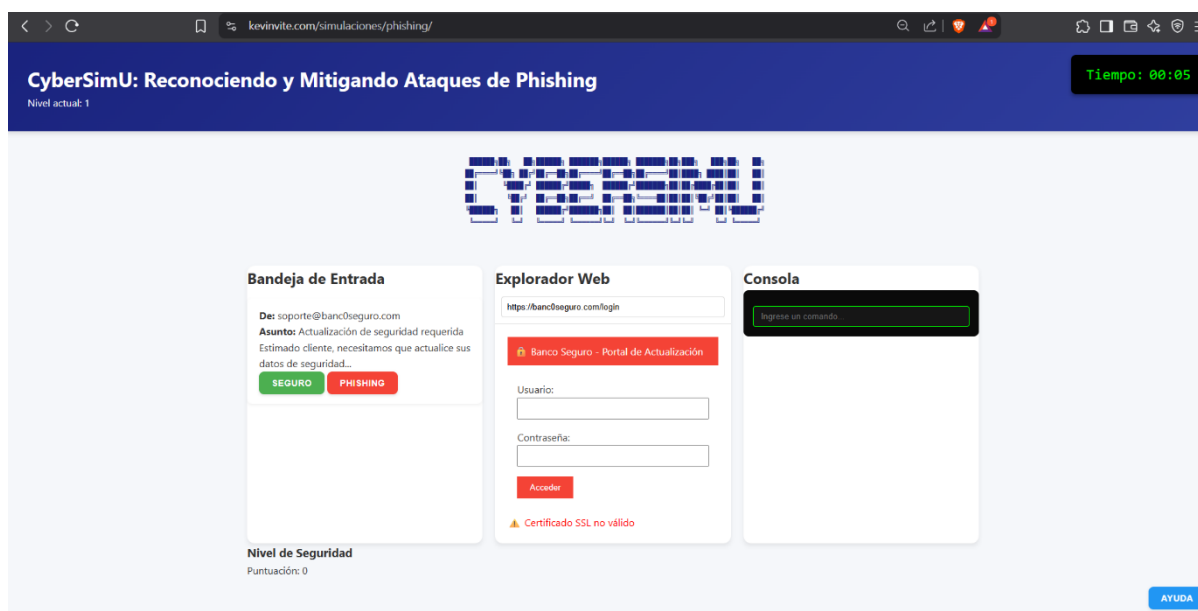


Figura 30. Reconociendo y mitigando Phishing, simulador en funcionamiento.

Simulación 9: Simulador de *Ransomware*

La última simulación se enfocó en la mitigación de infecciones por *ransomware*, abordando uno de los puntos de origen más comunes como es el correo electrónico, el escenario donde se trabajó incluía una dinámica interactiva donde los estudiantes debían analizar los mensajes recibidos y de ello tomar decisiones sobre su legitimidad, así mismo evaluando los riesgos de que algunos de los correos activaran una carga maliciosa.

En el transcurso de la solución del ejercicio, se presentaron correos uno por uno, donde se replicaron situaciones reales de entrega de *ransomware* a través de campañas de phishing. Los estudiantes debían evaluar cuidadosamente cada mensaje, considerando indicadores de alerta como:

- Dominios de correo remitente poco fiables o mal redactados,
- Errores gramaticales u ortográficos,
- Tono de urgencia o amenazas veladas,
- Ofertas engañosas o fuera de contexto.

El simulador advertía que una decisión incorrecta podría simular una infección del sistema, reflejando las consecuencias de abrir archivos adjuntos comprometidos o hacer clic en enlaces maliciosos, esta mecánica buscó reforzar la toma de decisiones basada en evidencia, así como fomentar el hábito de análisis crítico antes de interactuar con correos de origen dudoso.

Al concluir, el sistema proporcionaba una retroalimentación detallada sobre los aciertos y errores cometidos, junto con algunas recomendaciones específicas sobre cómo detectar y evitar este tipo de amenazas. La simulación no solo ofreció una visión clara de cómo actúan las campañas de *ransomware*, sino que también se promovió una cultura preventiva enfocada hacia el usuario final como un sistema de defensa.

Participantes y contexto de evaluación

El estudio contó con la participación de estudiantes de nivel superior de las carreras de Ingeniería Informática del Tecnológico de Estudios Superiores de Chalco (TESCH), los participantes incluidos en el análisis fueron 48 estudiantes, quienes fueron divididos en dos grupos: uno de intervención, que trabajó con la plataforma CyberSimU , las evidencias están disponibles en el Anexo 3, y el segundo grupo fue de control, aunque este segundo utilizó dicha herramienta, cabe señalar que, a diferencia de los modelos experimentales tradicionales, el grupo de control fue incluido tanto en el *Pre-Test* como en el *Post-Test* con el objetivo de establecer una base más sólida y permitir comparaciones cuantitativas que evidencien el impacto de la plataforma.

La evaluación se llevó a cabo mediante un cuestionario estructurado compuesto por preguntas cerradas que abordaron conocimientos generales en ciberseguridad. Dicho cuestionario se aplicó en dos momentos: antes de utilizar la

plataforma *Pre-Test* y después de haber completado las simulaciones asignadas *Post-Test*.

Resultados del *Pre-Test* y *Post-Test*

Con el propósito de evaluar el impacto del uso del simulador CyberSimU en el proceso de aprendizaje de los estudiantes en temas de ciberseguridad, se aplicó un instrumento diagnóstico al inicio y al final de la experiencia educativa, este instrumento consistió en un cuestionario de 25 preguntas de opción múltiple, elaborado con base en los contenidos cubiertos por las simulaciones interactivas. El mismo instrumento se empleó para el *Pre-Test*, aplicado antes de que los estudiantes utilizaran la plataforma, y para el *Post-Test*, aplicado una vez concluidas las nueve simulaciones propuestas.

En total, participaron 48 estudiantes de nivel superior pertenecientes a tres instituciones educativas: el Tecnológico de Estudios Superiores de Chalco, la Universidad Mexiquense del Bicentenario, Plantel Ixtapaluca y la Universidad Mexiquense del Bicentenario, Plantel La Paz. Todos los participantes completaron ambas evaluaciones.

Los resultados obtenidos fueron sistematizados y analizados para identificar posibles diferencias en el nivel de conocimientos antes y después del uso del simulador. En la Figura 31 se presenta un gráfico comparativo, en el que se visualizan las distribuciones de puntajes correspondientes al *Pre-Test* y al *Post-Test*.

Como puede observarse en el gráfico, los puntajes obtenidos en el *Post-Test* muestran una tendencia ascendente con respecto al *Pre-Test* ver Figura 32, en términos generales, se observó una mejora significativa en los resultados, lo cual sugiere que el uso de la plataforma contribuyó positivamente al aprendizaje de los contenidos evaluados ver Figura 33.

Dichas diferencias son relevantes si se consideran que las simulaciones cumplen con un amplio espectro de conceptos técnicos, como comandos en entornos *Linux* y *Windows*, hasta el análisis de amenazas de ataques de denegación de servicios (DDoS), *phishing*, *ransomware*, y técnicas avanzadas de post-explotación.

La interacción continua con estos entornos simulados parece haber fortalecido la comprensión teórica y práctica de los estudiantes.

En párrafos posteriores se muestra el análisis con pruebas estadísticas inferenciales para determinar las diferencias.

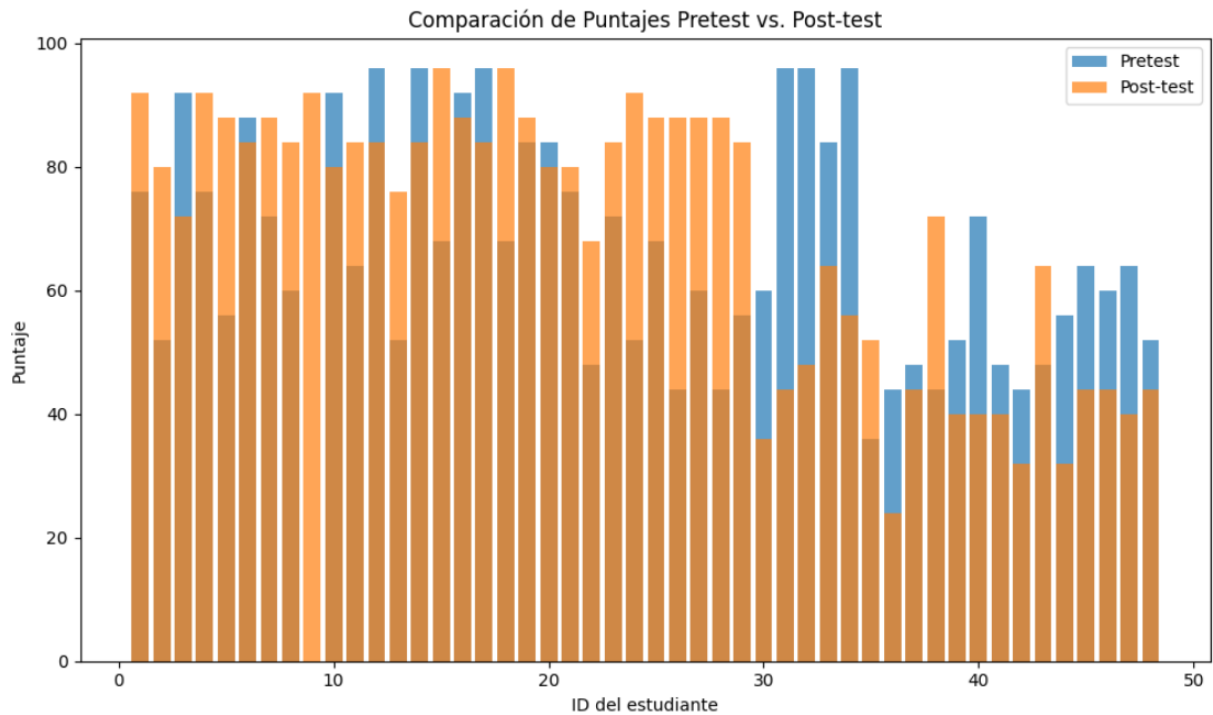


Figura 31. Comparación de puntajes de Pre-Test y Post-Test.

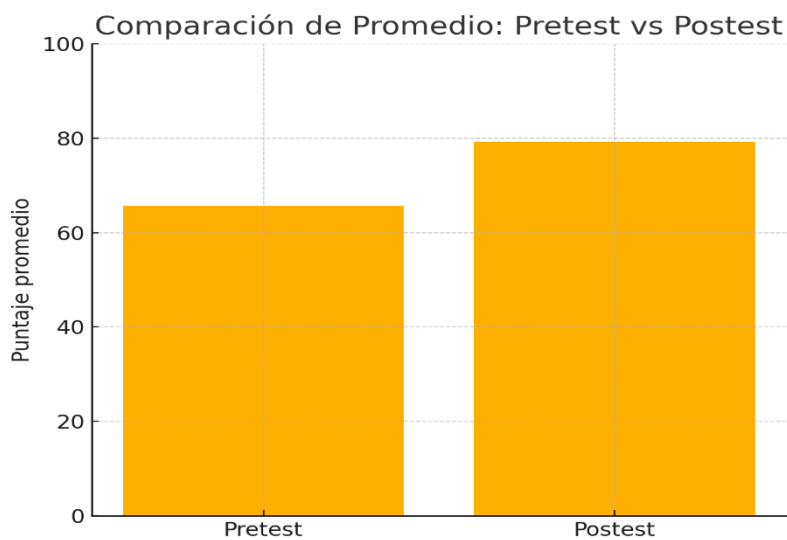


Figura 32. Comparación general de promedios entre las pruebas Pre-Test y Post-Test.

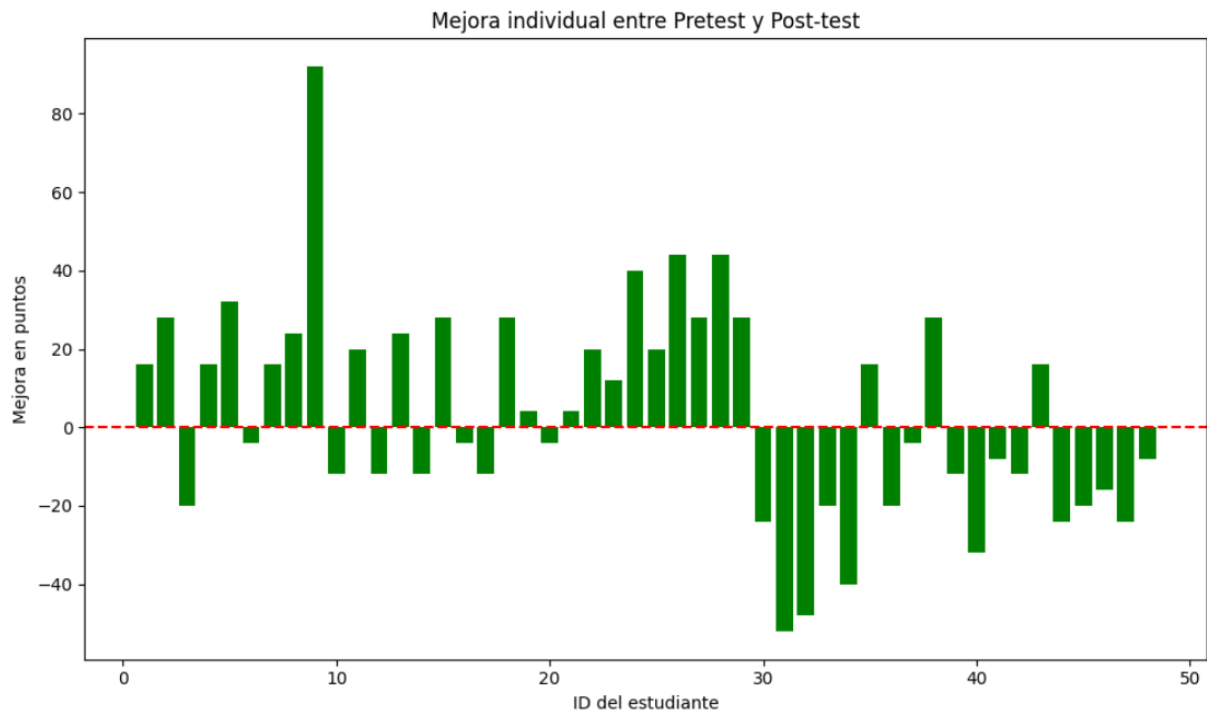


Figura 33. Mejora individual entre resultados Pre-Test y Post-Test.

Análisis descriptivo de los puntajes obtenidos

Para obtener una visión general del rendimiento de los estudiantes antes y después de la intervención con CyberSimU, se calcularon tres métricas estadísticas fundamentales: la media aritmética (μ), la mediana (Me) y la desviación estándar (σ).

Media Aritmética (μ)

La media aritmética representa el valor promedio de los puntajes obtenidos. En la Figura 34, en el Pre-Test, la media fue de **32.29 puntos**, mientras que en el *Post-Test* se elevó a **33.61 puntos**, lo que indica una mejora general en los estudiantes tras el uso de las simulaciones.

$$\mu = \frac{1}{n} \sum_{i=1}^n x_i$$

Figura 34. Formula de media aritmética.

Mediana (Me)

La mediana, que representa el valor central de la distribución de los puntajes, también mostró una mejora. En el *Pre-Test* fue de **31.67 puntos**, y en el *Post-Test* alcanzó los **33.67 puntos**, lo que sugiere que la mayoría de los estudiantes se desplazaron hacia un mejor rendimiento a continuación de describen la formulas usadas cuando n es par e impar Figuras 35 y 36.

$$Me = x_{\frac{n+1}{2}}$$

Figura 35. formula mediana cuando n es impar.

$$Me = \frac{x_{\frac{n}{2}} + x_{\frac{n}{2}+1}}{2}$$

Figura 36. Formula mediana cuando n es par.

Desviación Estándar (σ)

La desviación estándar Figura 37 disminuyó de **7.18** en el *Pre-Test* a **4.89** en el *Post-Test*. Esta reducción es relevante, ya que indica que después de la intervención, los puntajes se concentraron más alrededor de la media, reflejando una menor dispersión y, por tanto, un aprendizaje más uniforme entre los estudiantes.

$$\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \mu)^2}$$

Figura 37. Formula de la desviación estándar.

Análisis Descriptivos de los resultados obtenidos

Para realizar una primera aproximación a los resultados obtenidos por los estudiantes en las evaluaciones de *Pre-Test* y *Post-Test*, se calcularon tres métricas fundamentales de estadística descriptiva: la media aritmética (μ), la mediana (Me) y la desviación estándar (σ), estas métricas son comúnmente utilizadas en estudios del ámbito educativo debido a su capacidad para representar, de manera sintética, la tendencia central y la dispersión de los datos recolectados.

En el *Pre-Test*, la media aritmética fue de 0.53, lo que indica que en promedio los estudiantes obtuvieron un 53% de aciertos, esta cifra sugiere un conocimiento moderado de los temas evaluados, lo cual es esperable dado que aún no se había expuesto a los estudiantes a las simulaciones interactivas de CyberSimU por su parte, la mediana fue de 0.56, ligeramente superior a la media, lo que implica una leve asimetría hacia los valores más bajos, con una parte del grupo que obtuvo puntajes por debajo del promedio. Finalmente, la desviación estándar fue de 0.19, lo que indica una dispersión moderada en los resultados, es decir, los puntajes no se concentraron exclusivamente en torno al promedio, sino que hubo una cierta variabilidad entre los participantes.

Tras la implementación de las simulaciones, se aplicó el *Post-Test* para evaluar el impacto del entorno de aprendizaje, los resultados muestran una mejora considerable, la media aritmética se elevó a 0.76, reflejando un incremento del 23% respecto al *Pre-Test*, la mediana se situó en 0.80, lo que refuerza la observación de que la mayoría de los estudiantes mejoraron notablemente su desempeño, la desviación estándar, en este caso, fue de 0.14, inferior a la obtenida en el *Pre-Test*, lo que indica una mayor homogeneidad en los puntajes. Esto sugiere que no solo

mejoró el rendimiento general, sino que además se redujo la brecha entre los estudiantes con menor y mayor desempeño.

Estos resultados permiten determinar que el uso de la plataforma de simulación CyberSimU generó un efecto positivo en el aprendizaje de los conceptos de ciberseguridad, no solo elevando el conocimiento sino también estandarizando el nivel de comprensión entre los distintos participantes.

En resumen, la comparación entre el *Pre-Test* y el *Post-Test* permite observar una mejora sustancial tanto en la tendencia central como en la dispersión de los datos, consolidando la efectividad de la plataforma CyberSimU como herramienta educativa en ciberseguridad.

Análisis estadístico inferencial

Para determinar si existió una diferencia significativa entre los conocimientos previos y los adquiridos tras el uso de las simulaciones de *CyberSimU*, se aplicó una prueba estadística inferencial *t de Student* para muestras pareadas. Esta prueba ayuda a comparar las medias de dos mediciones realizadas en los mismos participantes antes y después de una intervención.

Hipótesis del análisis

- Hipótesis nula (H_0): No existe una diferencia significativa entre las medias del *Pre-Test* y *Post-Test*.
- Hipótesis alternativa (H_1): Existe una diferencia significativa entre las medias del *Pre-Test* y *Post-Test*.

Resultados

- Estadístico $t = -0.115$
- Valor $p = 0.909$

Dado que el valor p es mayor que 0.05, no se puede rechazar la hipótesis nula. Esto indica que no hubo una diferencia estadísticamente significativa en las medias generales del *Pre-Test* y *Post-Test*.

Interpretación educativa

A pesar de que el valor medio global no mostró una diferencia significativa, este resultado debe interpretarse cuidadosamente. Es posible que:

- Los estudiantes ya contaran con conocimientos previos amplios (como en el caso del grupo de control).
- La duración de la intervención haya sido corta para generar un cambio medible en todos los participantes.
- Algunas preguntas del *test* no hayan sido suficientemente sensibles a los aprendizajes desarrollados en las simulaciones.

Por lo tanto, se recomienda complementar este análisis con evaluaciones específicas por pregunta (ya realizadas), análisis cualitativos de las simulaciones y la percepción de los usuarios (encuestas de funcionalidad), así como estudios longitudinales que midan el aprendizaje a más largo plazo.

Evaluación de la plataforma mediante pruebas de funcionalidad

Para evaluar la calidad funcional de la plataforma CyberSimU desde una perspectiva centrada en el usuario, se aplicó un formulario basado en la norma **ISO/IEC 25010**, la cual establece criterios para medir atributos como funcionalidad, usabilidad, eficiencia y satisfacción del usuario. Esta evaluación consideró a usuarios reales desempeñando los distintos roles en la plataforma (estudiante, experto, administrador), lo cual permitió recoger información directa sobre la experiencia de uso.

Instrumento aplicado

El formulario incluyó preguntas cerradas con escala Likert del 1 al 5, donde **1** representa el menor grado de acuerdo (muy en desacuerdo) y **5** el mayor (totalmente de acuerdo) Véase Figura 38, en torno a los siguientes atributos:

- **Usabilidad:** facilidad de navegación, organización del menú y comprensión de resultados.
- **Funcionalidad:** acceso a simulaciones, autenticación según rol, funcionamiento técnico general.
- **Eficiencia:** tiempos de respuesta, generación de reportes, recomendaciones automáticas.
- **Seguridad:** percepción de protección de datos y cumplimiento de buenas prácticas.
- **Satisfacción general:** utilidad de la plataforma, comentarios libres y sugerencias de mejora.



Figura 38. Evidencia del formulario de pruebas de funcionalidad de CyberSimU.

Análisis de satisfacción por dimensiones según ISO/IEC 25010

Como parte del proceso de validación del sistema CyberSimU, se aplicó una encuesta estructurada en torno al modelo ISO/IEC 25010, evaluando la percepción de calidad

del software en cuatro dimensiones clave: usabilidad, funcionalidad, eficiencia y satisfacción del usuario.

Los resultados obtenidos muestran una evaluación favorable en todas las áreas ver Figura 39 :

- A. En usabilidad se obtuvo un promedio de 4.29, esto refleja una navegación intuitiva, una clara organización del menú, una adecuada percepción de seguridad, y una interfaz amigable. Los resultados sugieren que los usuarios consideran a la plataforma cómoda y accesible a la hora de usarla lo cual es un aspecto esencial en el entorno de la formación educativa.
- B. En el apartado de la funcionalidad, contando con una media de 4.36, se muestra como evidencia de que las funcionalidades que se asignaron a los roles fueron reconocidas por los usuarios además los mismos percibieron una correcta autenticación y cumplimiento de las buenas prácticas de la ciberseguridad. Por lo cual, este resultado resalta la adecuada implementación de la lógica, los permisos y controles del sistema.
- C. Referente a la eficiencia, se obtuvo un promedio de 4.05, esto indica que el rendimiento de la plataforma en la capacidad de respuesta, estabilidad y en los tiempos de carga fue altamente satisfactorio para los usuarios. Claro que en menor medida en comparación con las otras dimensiones, más sin embargo aún se ubica dentro de un alto rango de aceptación.
- D. Por último, algo importante que mencionar es la satisfacción del usuario la cual alcanza una media de 4.37, esto gracias a la claridad de los escenarios simulados, la relevancia educativa de los contenidos, y la utilidad de las recomendaciones, así como también los reportes generados por el sistema. Esta puntuación obtenida reafirma el valor percibido por los participantes en cuanto al aprendizaje práctico en ciberseguridad.

En conjunto, estos resultados sugieren que la plataforma CyberSimU cumple con altos estándares de calidad educativa y técnica, siendo bien valorada por sus usuarios finales, la consistencia en las puntuaciones superiores a 4 en todas las dimensiones también fortalece el argumento de que el sistema es adecuado para ser integrado en contextos formativos de nivel superior.

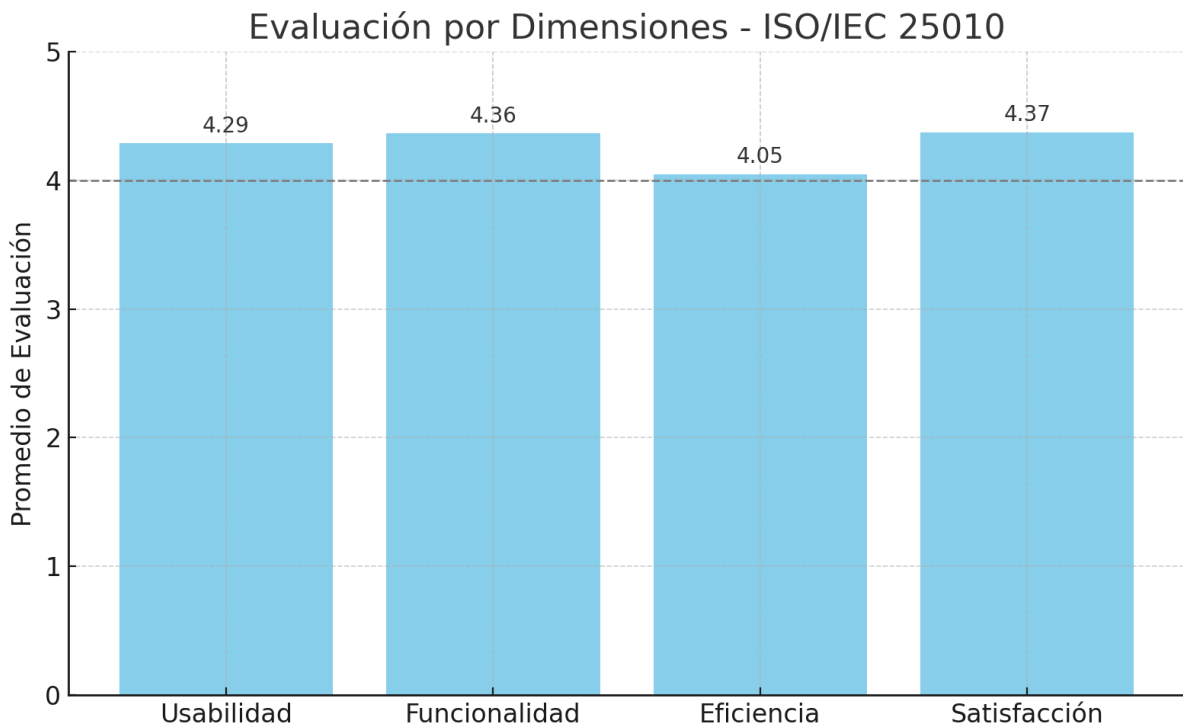


Figura 39. Gráfico de evaluación por dimensiones ISO/IEC 25010.

Análisis Cualitativo de Comentarios Abiertos

Al finalizar la encuesta de evaluación de la funcionalidad de la plataforma CyberSimU, se brindó a los participantes la oportunidad de expresar libremente sus opiniones, sugerencias y comentarios generales, esta sección fue de carácter abierto, lo que permitió recoger impresiones cualitativas más allá de las métricas estructuradas Figura 40. De un total de respuestas, se identificaron comentarios significativos que pueden agruparse en las siguientes categorías:

1. Valoración positiva del simulador: Comentarios como “Es una excelente plataforma para realizar simulaciones de ciberseguridad” y “Muy útil para quienes desean aprender en esta área” muestran que diversos participantes valoran su utilidad educativa.
2. Facilidad de uso y experiencia del usuario: Los usuarios expresan satisfacción con la plataforma, resaltando su interfaz sencilla y la posibilidad de practicar de manera interactiva en un entorno fácil de acceder.

3. Sugerencias y Observaciones Constructivas: Dentro de los comentarios se registraron pocas observaciones destinadas a mejorar la plataforma. Entre estas observaciones se encontraron algunas solicitudes para agregar más niveles de dificultad, incluir otros tipos de simulaciones o mejorar la personalización de los perfiles para usuarios
4. Neutralidad y Respuestas Genéricas: También se lograron identificar respuestas neutras como “ninguno” o “sin comentarios”, dichas respuestas si bien no aportan un contenido concreto, indican que no existen objeciones significativas por parte de algunos de los participantes.

En general, los comentarios que se lograron reunir consolidan la percepción de que CyberSimU cumple con su propósito principal como entorno de simulaciones activas. La evidencia cualitativa refuerza que, en los resultados cuantitativos anteriormente mencionados como el grado de satisfacción, usabilidad y funcionalidad del sistema, también ofrecen oportunidades claras de mejora continua para futuras versiones de la plataforma.

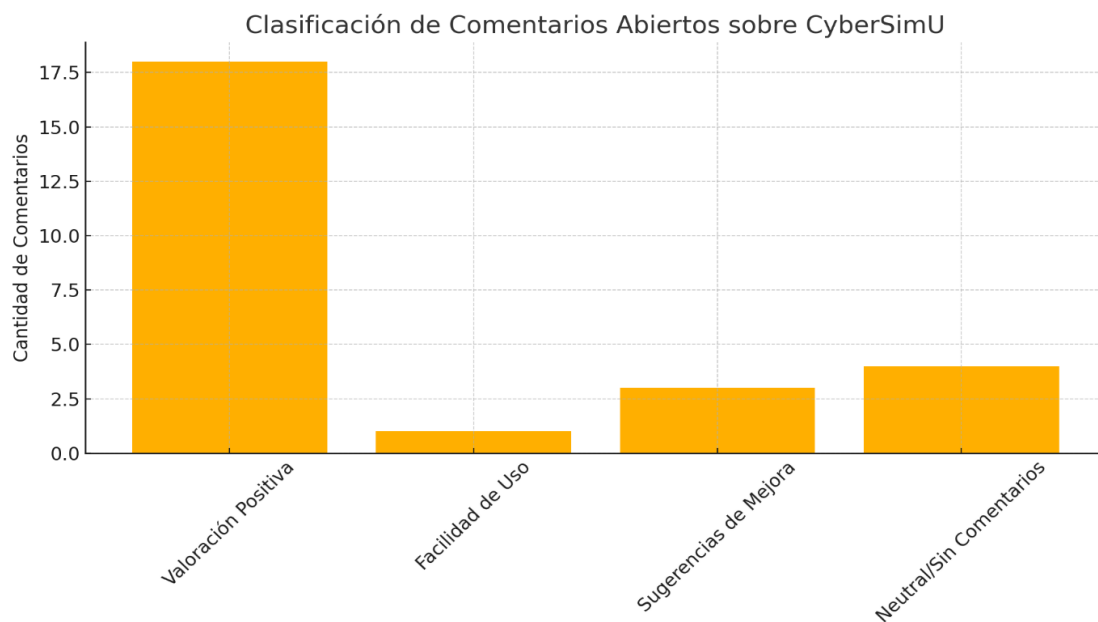


Figura 40. Gráfico de clasificación de comentarios abiertos.

Interpretación de la gráfica

La gráfica que se presenta muestra un análisis cualitativo de los comentarios abiertos que los usuarios compartieron luego de realizar las pruebas de funcionalidad de la plataforma CyberSimU. Los resultados muestran que una parte considerable de los participantes tuvo una valoración positiva del sistema, destacando su utilidad educativa y su contribución al aprendizaje de temas de ciberseguridad. Además, muchos comentarios señalaron que la plataforma es fácil de usar, lo que sugiere que la interfaz y la navegación son accesibles, incluso para aquellos sin experiencia previa en simuladores de este tipo.

A su vez, surgieron propuestas para mejorar, centradas mayormente en añadir nuevas funciones o en pulir ciertos detalles visuales y técnicos, esta clase de feedback es muy útil, pues nos deja entrever oportunidades para mejorar a futuro desde el punto de vista del usuario final. Para terminar, un grupo menor de participantes optó por no comentar o se mostró indeciso, lo que podría indicar una ausencia de puntos críticos importantes a destacar o, simplemente, una falta de ganas de alargar su respuesta. En suma, estos resultados cualitativos complementan el análisis cuantitativo anterior, dando una perspectiva más global de la vivencia del usuario con CyberSimU.

Difusión de los resultados y retribución social

Sumado a los datos cualitativos y cuantitativos recabados gracias a las pruebas de la herramienta CyberSimU, el proyecto ha incidido notablemente en la difusión del saber y la compensación social. Este aspecto es primordial, ya que la investigación no busca solo un provecho académico, sino que anhela contribuir de forma activa a la capacitación y sensibilización de diversos grupos sociales en asuntos de ciberseguridad.

En primer lugar, los hallazgos y aportes derivados de CyberSimU se han difundido a través de artículos de investigación presentados en congresos especializados y publicados en revistas académicas de acceso abierto, estos artículos han abordado tanto el desarrollo tecnológico de la plataforma como su impacto

educativo, contribuyendo al área científica en el área de la educación en ciberseguridad y estableciendo un precedente para investigaciones posteriores.

Se llevaron a cabo diversas acciones de responsabilidad social corporativa a través de ponencias y talleres dirigidos a distintos niveles educativos. En el nivel básico, se realizaron sesiones en escuelas primarias, adaptando los contenidos con un lenguaje sencillo y dinámicas participativas para explicar nociones esenciales sobre seguridad digital y uso seguro de dispositivos. En la educación media superior, se impartieron conferencias en preparatorias enfocadas en la prevención de riesgos cibernéticos, el manejo responsable de redes sociales y la detección de amenazas frecuentes como phishing y *malware*. Finalmente, en el ámbito universitario, se presentó una ponencia magistral en el Centro Universitario UAEM Valle de Chalco, donde se expuso el modelo CyberSimU como caso práctico y herramienta formativa para futuros especialistas en tecnologías de la información.

Las acciones implementadas han posibilitado que el proyecto trascienda su ámbito inmediato, promoviendo el fortalecimiento de la cultura de ciberseguridad en distintos sectores educativos y rangos de edad. Cada una de las intervenciones fue acompañada de un proceso de documentación que incluyó registros fotográficos, programas de actividades, materiales de apoyo visual y constancias de participación. Estos insumos se encuentran integrados en los anexos 4, 5, 6 y 7, lo que asegura la trazabilidad y validación de las actividades realizadas. De esta forma, se consolida el compromiso socialmente responsable del proyecto, garantizando que sus resultados generen un impacto concreto y relevante en la comunidad.

Movilidad académica en la Universidad de Hildesheim

Como parte de las acciones conjuntas al desarrollo del proyecto CyberSimU, se llevó a cabo una estancia académica en la Universidad de Hildesheim, Alemania, en los meses de Abril y Julio de 2025, esta movilidad se dio en el marco del programa de internacionalización del Centro Universitario UAEM Valle de Chalco con el respaldo institucional de la rectoría de Universidad Autónoma del Estado de México (UAEMex).

Durante estos meses, se desarrollaron actividades orientadas a la investigación, docencia y colaboración internacional, en el ámbito académico, se

asistió a seminarios en Analítica de Datos, Procesamiento de Lenguaje Natural y *Big Data Analytics*, los cuales ayudaron en la parte metodológica y técnica y apoyaron el enfoque del proyecto, además se participó en sesiones prácticas y talleres, en donde se aplicaron técnicas de análisis de datos, así como en ejercicios de integración de simulaciones de ciberseguridad, en la parte de colaboración institucional, se establecieron vínculos con investigadores del área de *Computer Science Education* de la Universidad de Hildesheim, ampliando posibilidades de cooperación en un futuro, las actividades incluyeron también visitas a laboratorios de innovación y tecnología educativa, donde se analizaron prácticas para la implementación de entornos virtuales de aprendizaje, además se llevaron a cabo reuniones con coordinadores de programas de intercambio, discutiendo estrategias para la incorporación de simuladores en la formación de estudiantes de ingeniería informática.

En conjunto, esta movilidad académica fortaleció las competencias técnicas e investigativas, aportando una perspectiva internacional que permitió contrastar enfoques, validar estrategias y generar nuevas oportunidades de mejora para el proyecto, la experiencia adquirida durante este periodo se tradujo en la integración de metodologías y herramientas de alcance global, reforzando la pertinencia y proyección del trabajo desarrollado, se anexan las evidencias correspondientes en el Anexo 8.

Cierre de la sección de Resultados

El desarrollo y aplicación de CyberSimU ha permitido constatar, a través de los indicadores obtenidos, que la combinación de metodologías sólidas como el Proceso Unificado Simplificado (SUP) y el modelo ADDIE genera entornos de aprendizaje efectivos y alineados con objetivos educativos claramente definidos según (Moses Adeleke Adeoye et al., 2024) , los incrementos observados en las evaluaciones posteriores a la interacción con las simulaciones, así como las valoraciones positivas de funcionalidad medidas bajo la norma ISO/IEC 25010, reafirman la pertinencia del enfoque adoptado (Estdale & Georgiadou, 2018)

Asimismo, las experiencias derivadas de la estancia académica en la Universidad de Hildesheim y las actividades de difusión en diversos entornos académicos ampliaron el alcance del proyecto más allá de su propósito inicial, aportando un valor añadido tanto en la dimensión formativa como en su potencial de transferencia a otros contextos.

Este grupo de evidencias cuantitativas y cualitativas finaliza la selección de los resultados obtenidos mostrando que no solo se consiguió cumplir los objetivos planificados, sino que también se consiguió obtener la base firme para futuras etapas de implementación, optimización y escalamiento de dicha plataforma tanto en escenarios educativos como en profesionales

5 CONCLUSIONES Y TRABAJOS FUTUROS

El presente proyecto ha significado un avance significativo en desarrollo de entornos educativos; Sin embargo, aún existen diversas líneas de investigación que pueden ser exploradas para potenciar su efectividad, una de las áreas clave es la ampliación del catálogo de las simulaciones, considerando que, si bien CyberSimU actualmente integra nueve escenarios que abordan temáticas como reconocimiento, ataques DDoS, uso de Nmap, *sniffing* de red, post-explotación y *ransomware*, el campo de la ciberseguridad es extenso y evoluciona de manera constante. En este sentido, se propone el desarrollo de simulaciones que incluyan análisis de vulnerabilidades con herramientas avanzadas, pruebas de penetración controladas, ingeniería inversa, análisis forense digital y criptografía, agregando además elementos de gamificación avanzados y retroalimentación mejorada para aumentar la motivación y el compromiso del usuario.

Así mismo, la incorporación de inteligencia artificial para personalizar la experiencia de aprendizaje la cual representa una línea de investigación con éxito en un futuro usando sistemas de recomendación basados en el rendimiento, análisis de errores y tiempos de respuesta, así como motores de evaluación automática respaldados por técnicas de *machine learning*, lo que permitiría generar estrategias de refuerzo y análisis de datos educativos en tiempo real, siguiendo enfoques de *learning analytics* y sistemas tutoriales inteligentes (SIT) (Gomes, 2024),

De la misma manera, se recomienda realizar estudios longitudinales para validar el impacto pedagógico de la plataforma, evaluando el desarrollo de competencias a mediano y largo plazo mediante rúbricas, grupos de control y análisis cualitativos, o bajo marcos de referencia como el modelo de evaluación de Kirkpatrick o el modelo CIPP.

En un contexto internacional, resulta pertinente adaptar CyberSimU a múltiples contextos educativos, llevando contenidos, incorporando estándares globales de seguridad como lo son NIST, OWASP o la norma ISO/IEC 27001, y ajustando los escenarios de acuerdo con las amenazas en cada región del mundo (Ortín et al., 2020).

Desde el punto de vista técnico, el desarrollo de una API y documentación formal permitiría integrar la plataforma con sistemas de gestión del aprendizaje como

Moodle o *Canvas*, fomentando escalabilidad y reutilización por parte de otras instituciones.

Finalmente, este trabajo fortalece y da pauta a nuevas investigaciones de mayor alcance, como un proyecto doctoral enfocado en la simulación y gamificación de ciberseguridad, con posibles enfoques hacia entornos inmersivos de realidad virtual o aumentada, todo esto acompañado de un plan de publicación, escalabilidad y licenciamiento que defina su futuro como herramienta abierta o de distribución controlada, garantizando su difusión y permanencia en el ámbito académico y profesional.

6. REFERENCIAS DE CONSULTA

- Aboaoja, F. A., Zainal, A., Ghaleb, F. A., Al-rimy, B. A. S., Eisa, T. A. E., & Elnour, A. A. H. (2022). Malware Detection Issues, Challenges, and Future Directions: A Survey. *Applied Sciences*, 12(17), 8482. <https://doi.org/10.3390/app12178482>
- Abuhassna, H., Alnawajha, S., Awae, F., Mohamed Adnan, M. A. Bin, & Edwards, B. I. (2024). Synthesizing technology integration within the Addie model for instructional design: A comprehensive systematic literature review. *Journal of Autonomous Intelligence*, 7(5), 1546. <https://doi.org/10.32629/jai.v7i5.1546>
- Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, 2, 100031. <https://doi.org/10.1016/j.csa.2023.100031>
- Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1). <https://doi.org/10.1093/cybsec/tyy006>
- Aiyanyo, I. D., Samuel, H., & Lim, H. (2020). A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning. *Applied Sciences*, 10(17), 5811. <https://doi.org/10.3390/app10175811>
- Alahmadi, A. A., Aljabri, M., Alhaidari, F., Alharthi, D. J., Rayani, G. E., Marghalani, L. A., Alotaibi, O. B., & Bajandouh, S. A. (2023). DDoS Attack Detection in IoT-Based Networks Using Machine Learning Models: A Survey and Research Directions. *Electronics*, 12(14), 3103. <https://doi.org/10.3390/electronics12143103>
- Almelhi, A. M. (2021). Effectiveness of the ADDIE Model within an E-Learning Environment in Developing Creative Writing in EFL Students. *English Language Teaching*, 14(2), 20. <https://doi.org/10.5539/elt.v14n2p20>
- Ashtiani, M., & Abdollahi Azgomi, M. (2014). A distributed simulation framework for modeling cyber attacks and the evaluation of security measures. *SIMULATION*, 90(9), 1071–1102. <https://doi.org/10.1177/0037549714540221>

- Aukstakalnis, S. (2016). *Practical Augmented Reality: A Guide to the Technologies, Applications, and Human Factors for AR and VR*. Addison-Wesley Professional.
- Beuran, R., Pham, C., Tang, D., Chinen, K., Tan, Y., & Shinoda, Y. (2018). Cybersecurity Education and Training Support System: CyRIS. *IEICE Transactions on Information and Systems*, E101.D(3), 740–749. <https://doi.org/10.1587/transinf.2017EDP7207>
- Bobrownicki, R., Carson, H. J., MacPherson, A. C., & Collins, D. (2022). Unloading the dice: selection and design of comparison and control groups in controlled trials to enhance translational impact within motor learning and control research. *International Journal of Sport and Exercise Psychology*, 20(5), 1330–1344. <https://doi.org/10.1080/1612197X.2021.1956567>
- Campos, H. (2017). *adictos al trabajo*. Obtenido de *adictos al trabajo*: <https://www.adictosaltrabajo.com/2017/08/29/aframe-para-hacer-un-videojuego/>
- Conti, M., Dragoni, N., & Lesyk, V. (2016). A Survey of Man In The Middle Attacks. *IEEE Communications Surveys & Tutorials*, 18(3), 2027–2051. <https://doi.org/10.1109/COMST.2016.2548426>
- Czarnocka, M., & Mazurek, M. (2025). Michael Heim's Concept of "Metaphysics" of Virtual Worlds. A Proposal of Improving it. *Foundations of Science*. <https://doi.org/10.1007/s10699-025-09976-1>
- Dieter Schmalstieg, T. H. (2016). *Augmented Reality: Principles and Practice*. EUA: Addison-Wesley Professional.
- Eling, M., Elvedi, M., & Falco, G. (2023). The Economic Impact of Extreme Cyber Risk Scenarios. *North American Actuarial Journal*, 27(3), 429–443. <https://doi.org/10.1080/10920277.2022.2034507>
- Erin Pangilinan, S. L. (2019). *Creating Augmented and Virtual Realities*. O'Reilly Media, Inc.

- Estdale, J., & Georgiadou, E. (2018). Applying the ISO/IEC 25010 Quality Models to Software Product (pp. 492–503). https://doi.org/10.1007/978-3-319-97925-0_42
- Ethical, C. (2014). Introduction to Ethical Hacking. USA: Ec-Council.
- Gomes, D. (2024). A Comprehensive Study of Advancements in Intelligent Tutoring Systems Through Artificial Intelligent Education Platforms (pp. 213–244). <https://doi.org/10.4018/979-8-3693-6170-2.ch008>
- Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, 26(2), 91–108. <https://doi.org/10.1111/j.1471-1842.2009.00848.x>
- Halevi, T., Memon, N., & Nov, O. (2015). Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2544742>
- Hernandez, S. C. (2010). Metodología de la investigacion. Mexico: Mc Graw Hill.
- Iuliia Sergeevna Khukalenko, R. K.-R. (2022). Teachers' perceptions of using virtual reality technology in classrooms: A large-scale survey. *Springer Link*, 11591-11613.
- Kamińska, D., Sapiński, T., Wiak, S., Tikk, T., Haamer, R., Avots, E., . . . Anbarjafari, G. (2019). Virtual Reality and Its Applications in Education: Survey. *MDPI*, 90-924.
- Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97, 101804. <https://doi.org/10.1016/j.inffus.2023.101804>
- Khayretdinova, A., & Kubach, M. (2019). A Methodology for Experimental Evaluation of a Software Assistant for the Development of Safe and Economically Viable Software. *Proceedings of the 15th International Conference on Web Information Systems and Technologies*, 234–241. <https://doi.org/10.5220/0008069102340241>

- Lindwedel, P. C. (2021). Virtual Reality Simulations in Nurse Education: A Systematic Mapping review. *Nurse Education Today*. Obtenido de <https://doi.org/10.1016/j.nedt.2021.104868>
- Lopezosa, L. C. (2023). Inteligencia Artificial y métodos cualitativos de Investigacion: Chat GPT para revisiones de la literatura y analisis de entrevistas semiestructuradas. Jornada "IA para principiantes", (pág. 100). Barcelona, España.
- Luo, X. (2023). Using a virtual reality interview simulator to explore factors influencing people's behavior. Obtenido de <https://arxiv.org/abs/2305.07965>
- Mahjabin, T., Xiao, Y., Sun, G., & Jiang, W. (2017). A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *International Journal of Distributed Sensor Networks*, 13(12), 155014771774146. <https://doi.org/10.1177/1550147717741463>
- Malenkovich, S. (2023). Kaspersky. Obtenido de Kaspersky: <https://latam.kaspersky.com/blog/el-worm-morris-cumplio-25-anos/1644/>
- McCandless, D. (2022). Information is beautiful. Obtenido de Information is beautiful: <https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/#bysensitivity>
- Moses Adeleke Adeoye, Kadek Adrian Surya Indra Wirawan, Made Shania Satya Pradnyani, & Nyoman Intan Septiarini. (2024). Revolutionizing Education: Unleashing the Power of the ADDIE Model for Effective Teaching and Learning. *JPI (Jurnal Pendidikan Indonesia)*, 13(1), 202–209. <https://doi.org/10.23887/jpiundiksha.v13i1.68624>
- Nesenbergs, K., Abolins, V., Ormanis, J., & Mednis, A. (2020). Use of Augmented and Virtual Reality in Remote Higher Education: A Systematic Umbrella Review. *Education Sciences*, 11(1), 8. <https://doi.org/10.3390/educsci11010008>

- Oakley, J. (2022). *Theoretical Cybersecurity*. Berkeley CA: Apress. Obtenido de https://doi.org/10.1007/978-1-4842-8300-4_1
- Ortin, F., Rodriguez-Prieto, O., Pascual, N., & Garcia, M. (2020). Heterogeneous tree structure classification to label Java programmers according to their expertise level. *Future Generation Computer Systems*, 105, 380–394. <https://doi.org/10.1016/j.future.2019.12.016>
- Padilha, J. M., Machado, P. P., Ribeiro, A., Ramos, J., & Costa, P. (2019). Clinical Virtual Simulation in Nursing Education: Randomized Controlled Trial. *Journal of Medical Internet Research*, 21(3), e11529. <https://doi.org/10.2196/11529>
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., ... Moher, D. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, n71. <https://doi.org/10.1136/bmj.n71>
- Parisi, T. (2015). *Learning Virtual Reality*. EUA: O'Reilly Media, Inc.
- Philippe Fuchs, G. M. (2011). *Virtual Reality: Concepts and Technologies*. CRC Press.
- Picard, S., Sun, N., & Botev, J. (2024). XR MUSE: An Open-Source Unity Framework for Extended Reality-Based Networked Multi-User Studies. *Virtual Worlds*, 3(4), 404–417. <https://doi.org/10.3390/virtualworlds3040022>
- Ping Wang, & Peyton Lutchkus. (2023). Psychological Tactics Of Phishing Emails. *Issues In Information Systems*, 71–83. https://doi.org/10.48009/2_iis_2023_107
- Plotzky C, L. U. (2021). Virtual reality simulations in nurse education: A systematic mapping review. *National Library of Medicine*, 15.
- Pramanik, S. (2022). *Cyber Security and Network Security*. Wiley. Obtenido de <https://learning.oreilly.com/library/view/cyber-security-and/9781119812494/>

- Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. *Computers & Security*, 136, 103585. <https://doi.org/10.1016/j.cose.2023.103585>
- Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), e14234. <https://doi.org/10.1016/j.heliyon.2023.e14234>
- Salomon, D. (2010). *Viruses* (pp. 37–97). https://doi.org/10.1007/978-0-85729-006-9_2
- Sandra Dutra Piovesan, L. M. (2012). Virtual Reality as a Tool in the education. *International Conference on Cognition and Exploratory Learning in Digital Age*, (pág. 300).
- Schneier, B. (2000). *Digital Security in a Networked World*. Wiley.
- Scott, A. (2020). Spiceworks. Obtenido de Spiceworks: <https://www.google.com/search?client=firefox-b-d&q=quien+es+el+autor+del+sitio+https%3A%2F%2Fimages.spiceworks.com>
- Sherman, A. B. (2002). *Understanding Virtual Reality*. EUA: Morgan Kaufmann.
- Shin, M. K., Ghosh, S., & Vijayasathy, L. R. (2022). An empirical comparison of four Java-based regression test selection techniques. *Journal of Systems and Software*, 186, 185–189. <https://doi.org/10.1016/j.jss.2021.111174>
- Shojaifar, A., & Järvinen, H. (2021). Classifying SMEs for Approaching Cybersecurity Competence and Awareness. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–7. <https://doi.org/10.1145/3465481.3469200>
- Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333–339. <https://doi.org/10.1016/j.jbusres.2019.07.039>
- Srushtika Neelakantam, T. P. (2017). *Learning Web-based Virtual Reality: Build and Deploy Web-based Virtual Reality Technology*. Apress.

- Steinberg, J. (2019). *Cybersecurity for Dummies. For Dummies*. Obtenido de <https://learning.oreilly.com/library/view/cybersecurity-for-dummies/9781119560326/>
- Thanh Vu, S. N., Stege, M., El-Habr, P. I., Bang, J., & Dragoni, N. (2021). A Survey on Botnets: Incentives, Evolution, Detection and Current Trends. *Future Internet*, 13(8), 198. <https://doi.org/10.3390/fi13080198>
- The NIST Cybersecurity Framework (CSF) 2.0. (2024). <https://doi.org/10.6028/NIST.CSWP.29>
- Tiffany LEUNG, F. Z. (2018). The use of Virtual Reality in Enhancing Interdisciplinary Research and Education. *ARXIV*, 6.
- University, S. V. (2021). Mount Saint Vincent University. Obtenido de Mount Saint Vincent University: https://www.msvu.ca/wp-content/uploads/2017/10/account-termination-phish-2022-09-29_12-05-23.png
- Vanderbilt, U. (2020). Vanderbilt University Medical Center. Obtenido de Vanderbilt University Medical Center: https://www.vumc.org/enterprisecybersecurity/sites/default/files/public_files/Ransomware%20Pic.png
- Vargas, M. (2019). Application of augmented reality as a means of interdisciplinary learning. Obtenido de <https://www.redalyc.org/journal/849/84961239016/html/>
- Veale, M., & Brown, I. (2020). Cybersecurity. *Internet Policy Review*, 9(4). <https://doi.org/10.14763/2020.4.1533>
- Villanueva C, X. J. (2020). Simulation-based surgical education in cardiothoracic training. *ANZ Journal of Surgery*, 978-983.
- Villena-Taranilla, R., Diago, P. D., & Colomer Rubio, J. C. (2025). Virtual Reality as a Pedagogical Tool: Motivation and Perception in Teacher Training for Social Sciences

and History in Primary Education. *Education Sciences*, 15(4), 493.
<https://doi.org/10.3390/educsci15040493>

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research*, 39(1), 93–112.
<https://doi.org/10.1177/0739456X17723971>

Xinyi Luo, Y. W.-H. (2023). Using a virtual reality interview simulator to explore factors influencing people's behavior. *Arxiv*, 12.

Y. A. Mena-Vargas, E. E.-R.-C. (2019). Application of augmented reality as a means of interdisciplinary learning. *Scientia Et Technica*, 479-489.

Yang, C.-N., Kao, C.-L., & Wang, C.-J. (2021). Two-dimensional diagonal layer hash chain based key pre-distribution scheme. *Journal of Information Security and Applications*, 63, 103038. <https://doi.org/10.1016/j.jisa.2021.103038>


Zimmermann, V., Schöni, L., Schaltegger, T., Ambuehl, B., Knieps, M., & Ebert, N. (2024). Human-Centered Cybersecurity Revisited: From Enemies to Partners. *Communications of the ACM*, 67(11), 72–81. <https://doi.org/10.1145/3665665>

ANEXOS

ANEXO 1


Resultados de la encuesta


En el presente Anexo se explican de manera específica las respuestas del formulario aplicado a los estudiantes acerca de necesidades en ciberseguridad y la forma en la que se recopilaron, mostrando las evidencias arrojadas por Google Forms, de esta manera se describen los resultados particulares explicando en contexto estos elementos.



CyberSimU

En CyberSimU, nuestra misión es capacitar a estudiantes universitarios en el campo de la ciberseguridad mediante el uso de simulaciones interactivas y experiencias prácticas. Nos comprometemos a proporcionar una plataforma innovadora y accesible que fomente el aprendizaje efectivo, la experimentación segura y el desarrollo de habilidades necesarias para enfrentar los desafíos emergentes en la seguridad cibernética.

kevin_rv@tesch.edu.mx [Cambiar de cuenta](#) 

 No compartido

*** Indica que la pregunta es obligatoria**

Nombre del Encuestado *

Tu respuesta

Ilustración 1. Encuesta de necesidades de Ciberseguridad.

Tras analizar los resultados de la encuesta sobre la enseñanza de la ciberseguridad en instituciones educativas, se han obtenido varias conclusiones significativas, los

resultados se presentarán de manera grafica de acuerdo con lo que los encuestados fueron respondiendo.

¿Qué tan importante considera la ciberseguridad en su institución educativa?

174 respuestas

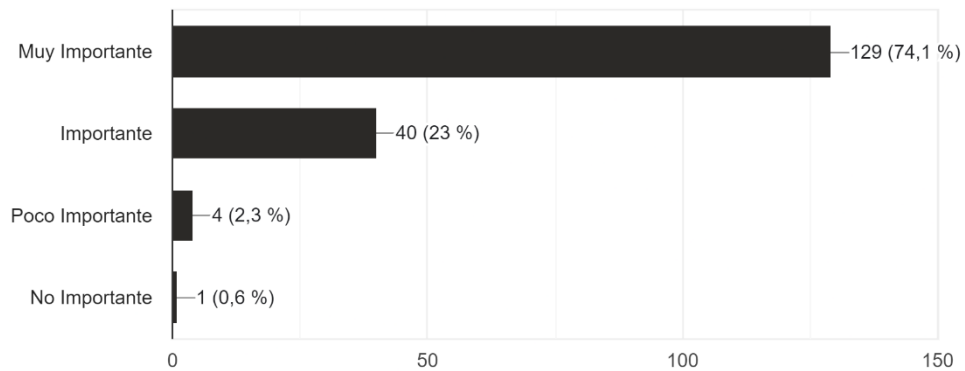


Ilustración 2. Resultados de la pregunta 1.

De las 174 respuestas que se obtuvieron, se puede ver en la anterior grafica que el 74.1% de los encuestados consideran que la ciberseguridad es muy importante en su institución educativa, y un 23% considera que es importante, por lo tanto, se puede observar que la ciberseguridad es un tema de gran importancia en los encuestados.

Actualmente su institución ofrece programas de formación en ciberseguridad

174 respuestas

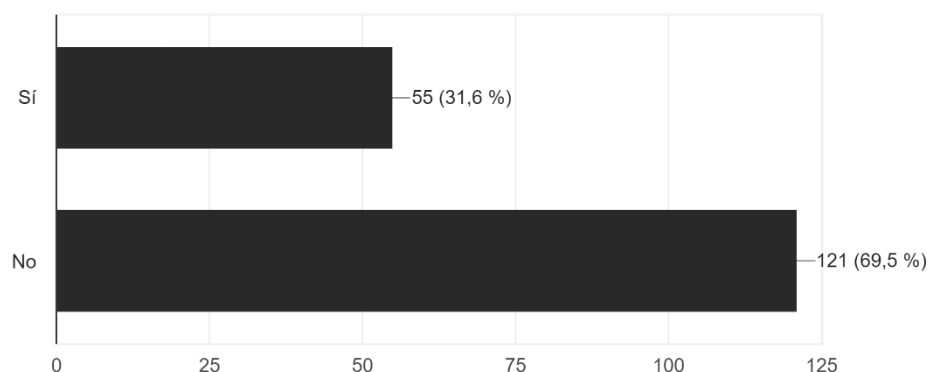


Ilustración 3. Resultados de la pregunta 2.

De la gráfica anterior podemos interpretar que actualmente las instituciones encuestadas no ofrecen una formación sólida en ciberseguridad por lo tanto es un buen nicho el poder lanzar una plataforma que permita a los estudiantes especializarse en temas de seguridad.

¿Cuáles son los principales desafíos que enfrenta su institución en términos de enseñanza de ciberseguridad? (Seleccione todas las que correspondan)

174 respuestas

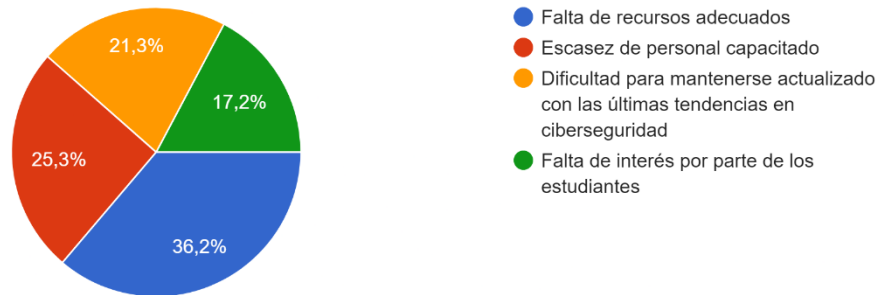


Ilustración 4. Resultados de la pregunta 3.

Se puede observar que dentro de las 174 respuestas se tiene un 36.2% prevaleciendo la respuesta de falta de recursos adecuados, y en segundo lugar la escasez de personal capacitado con un 25.3%, se puede observar la necesidad de tener personal capacitado para poder explicar temas como los relacionados a ciberseguridad.

¿Qué aspectos de la ciberseguridad considera que son más importantes para sus estudiantes? (Seleccione todas las que correspondan)

174 respuestas

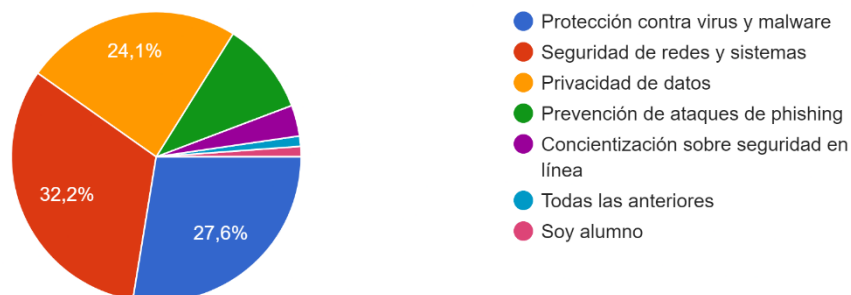


Ilustración 5. Resultados de la pregunta 4.

En la anterior pregunta se busca recabar información relacionada a los aspectos de ciberseguridad importantes y se distribuyeron de la siguiente manera las respuestas, seguridad de redes y sistemas con 32.2%, en segundo lugar, se tiene a protección contra virus y malware con 27.6% y en tercer lugar se ubica la privacidad de los datos, esto nos ayuda a determinar cuáles son las áreas de interés más importantes en tema de capacitación para el simulados.

¿Estarían interesados sus estudiantes en participar en simulaciones interactivas para aprender sobre ciberseguridad?(SOLO DOCENTES)

88 respuestas

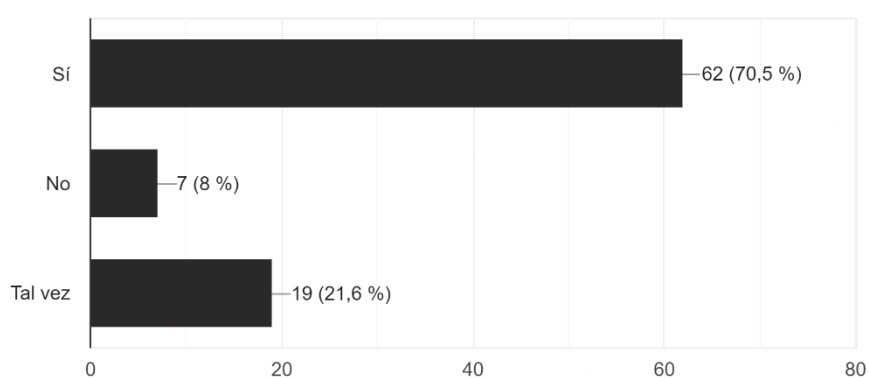


Ilustración 6. Resultados de la pregunta 5.

De la anterior pregunta se puede ver que el 70.5% de encuestados estarían interesados en participar en simulaciones interactivas para aprender sobre ciberseguridad, en segundo lugar, se tiene con un 21.6% que tal vez podrían participar en simulaciones interactivas.

Qué características consideraría más importantes en una plataforma de simulación de ciberseguridad? (Seleccione todas las que correspondan)

174 respuestas

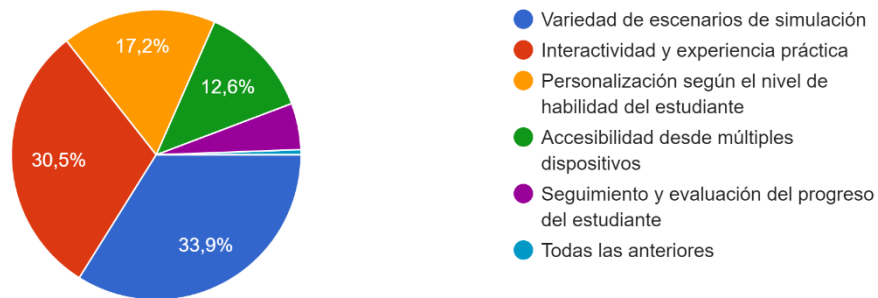


Ilustración 7. Resultados de la pregunta 6.

En la anterior grafica se puede observar que un 33.9% de los encuestados, les interesaría tener variedad de escenarios de simulación, y en segundo lugar, se encuentra la interactividad y experiencia práctica con 30.5% lo que nos permite conocer que es lo que esperan los usuarios relacionados al contenido del simulador.

¿Qué factores consideraría al seleccionar una plataforma de simulación de ciberseguridad para su institución? (Seleccione todas las que correspondan)

174 respuestas

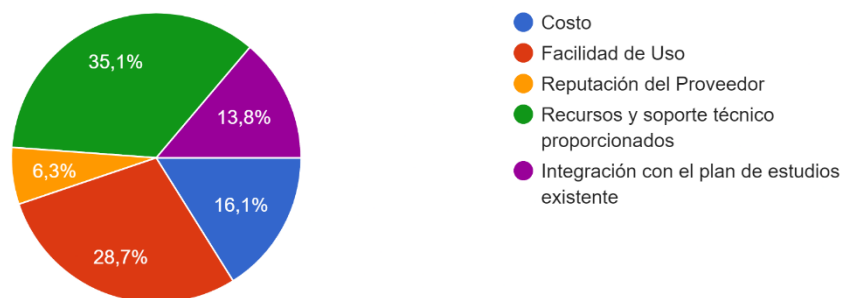


Ilustración 8. Resultados de la pregunta 7.

Una de las preguntas que nos permite determinar la forma en que los usuarios seleccionarían una plataforma recabo los siguientes datos, recursos y soporte técnico proporcionados con 35.1%, en segundo lugar, se encuentra la facilidad de uso con 28.7% y en tercer lugar se encuentra con 16.1% el costo.

¿Qué preocupaciones tendría al implementar una plataforma de simulación de ciberseguridad en su institución? (Seleccione todas las que correspondan)(SOLO DOCENTES)

174 respuestas



Ilustración 9. Resultados de la pregunta 8.

La anterior pregunta muestra las preocupaciones que tendrían para implementar una plataforma de simulación, y los resultados fueron con 29.3% la disponibilidad de tiempo y recursos, en segundo lugar, con 23.6% tiene que ver con el costo de implementación y en tercer lugar se encuentra la seguridad y privacidad de los datos con 19.5%.

¿Cuál es su nivel de familiaridad con las herramientas y recursos disponibles actualmente para la enseñanza de la ciberseguridad?

174 respuestas

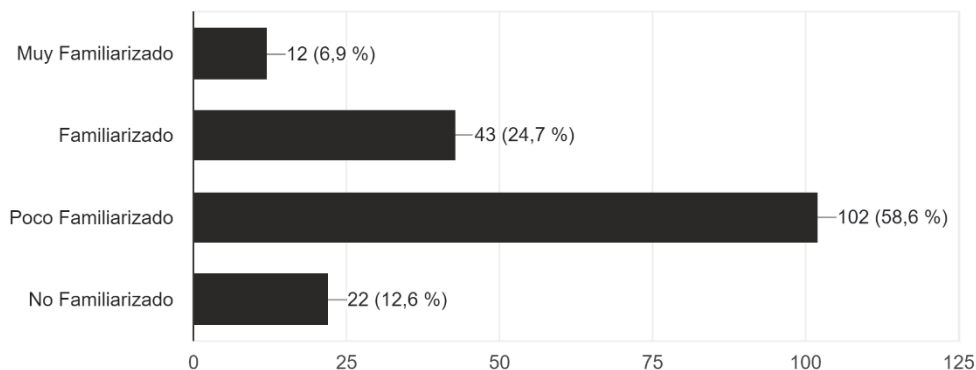


Ilustración 10. Resultados de la pregunta 9.

En la anterior grafica según la pregunta respondida por 174 encuestados respondieron que 58.6% está poco familiarizado con las plataformas de

ciberseguridad y el 24.7% está familiarizado contra un 12.6% que no está familiarizado.

¿Cuánto tiempo y recursos dedica su institución a la enseñanza de la ciberseguridad?

174 respuestas

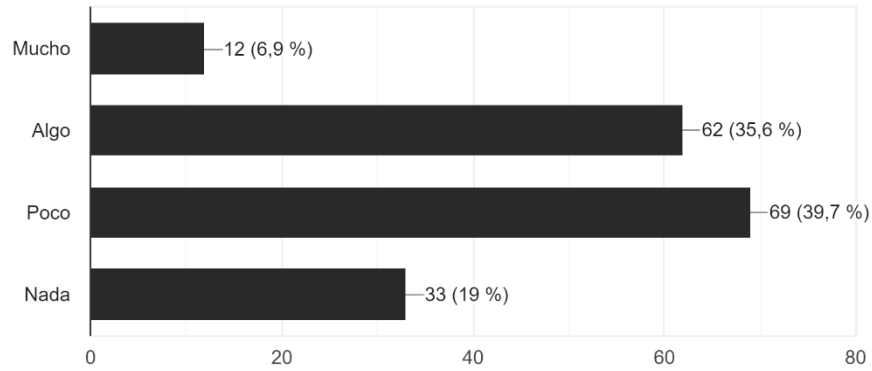


Ilustración 11. Resultados de la pregunta 10.

Notamos en la anterior pregunta las instituciones dedican poco tiempo y recursos para la enseñanza de la ciberseguridad prevaleciendo el 39.7% en segundo lugar con algo un 35.6%.

¿Qué tan satisfecho está con los resultados obtenidos mediante los métodos actuales de enseñanza de la ciberseguridad?

174 respuestas

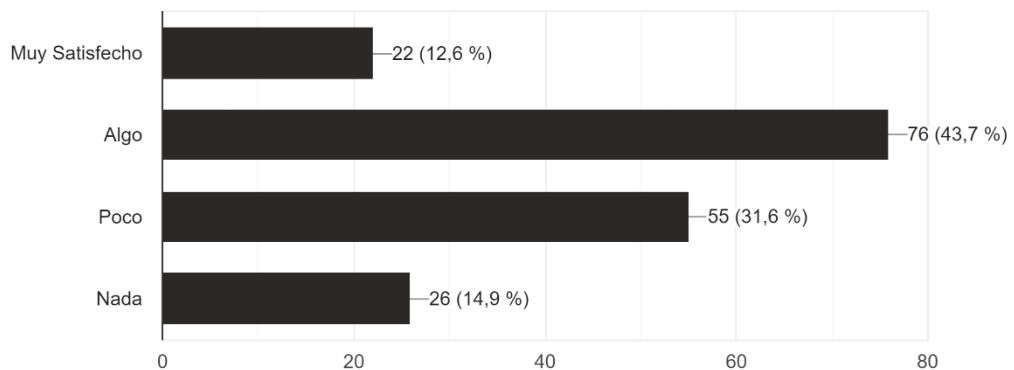


Ilustración 12. Resultados de la pregunta 11.

Esta pregunta es importante porque explora los resultados obtenidos mediante los métodos actuales de enseñanza de la ciberseguridad, y se puede observar que el 43.7% se encuentra algo satisfechos con esos resultados, en segundo lugar con 31.6% se encuentra que es poco y solo 12.6% muy satisfecho.

¿Estaría interesado/a en adquirir un modelo de suscripción institucional para acceder a una plataforma de capacitación en ciberseguridad?

174 respuestas

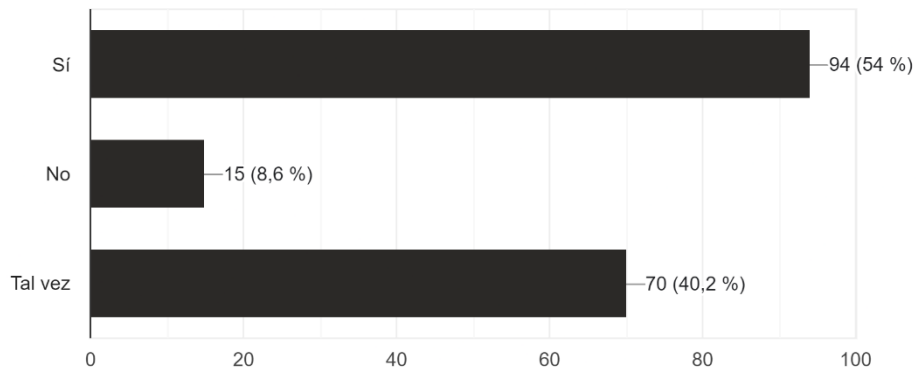


Ilustración 13. Resultados de la pregunta 12.

Se puede observar en la anterior grafica que hay un alto interés se obtener una suscripción institucional de manera que el 54% respondió que si contra un 40.2% que respondió que tal vez, esto es importante ya que uno de los clientes potenciales son las instituciones de educación superior.

¿Estaría interesado/a en un modelo "freemium" donde la plataforma ofrezca una versión básica gratuita con funcionalidades limitadas y opciones de actualización a versiones premium?

174 respuestas

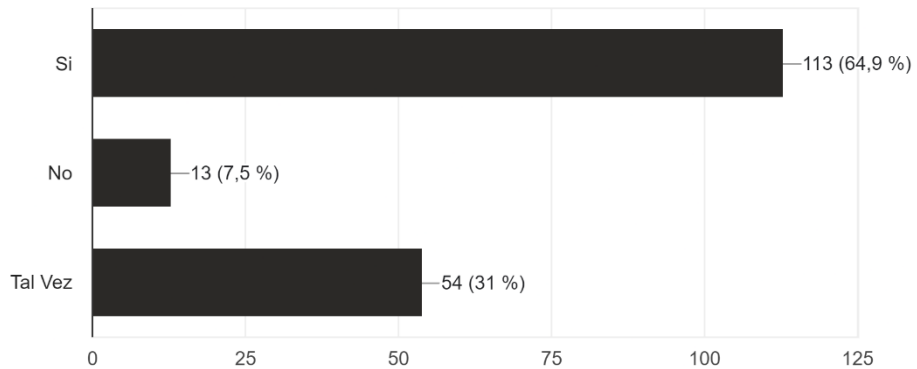
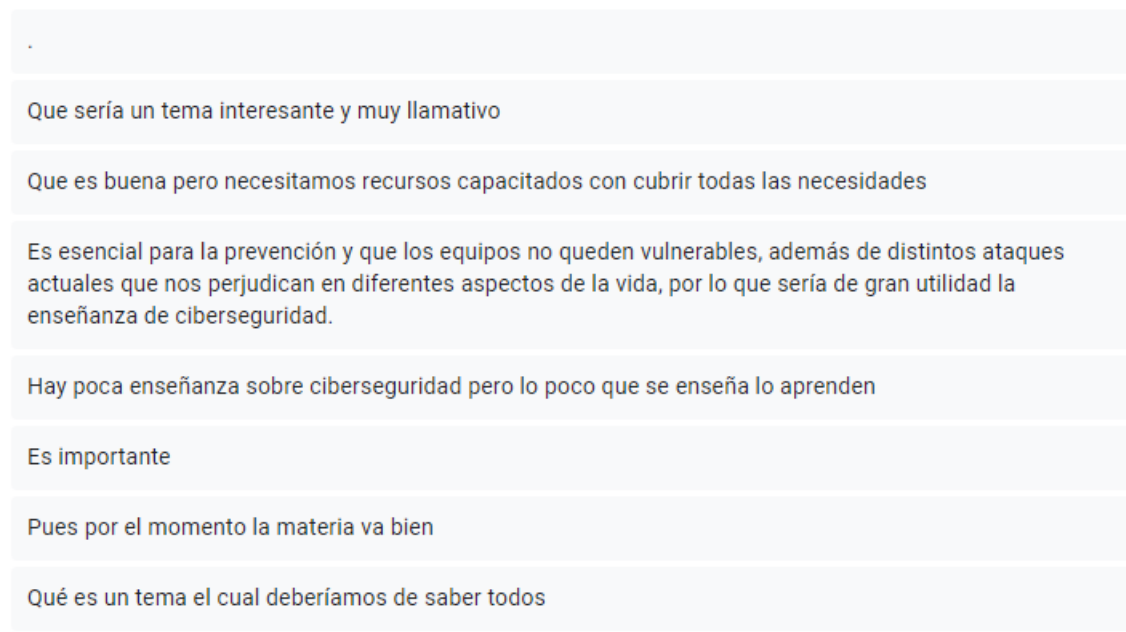


Ilustración 14. Resultados de la pregunta 13.

Esta pregunta al igual que la anterior es importante porque son dos de los modelos de negocios que se tienen planeados y son los modelos *freemium*, donde se pretende que la plataforma ofrezca una versión básica gratuita y después se migre a una versión *premium*, y podemos observar los resultados que el 64.9% si estaría dispuesto a adquirir una versión premium después de probar la plataforma.

¿Qué opinión tienen sus estudiantes sobre la enseñanza de la ciberseguridad en su institución?
(SOLO DOCENTES)

37 respuestas



.
Que sería un tema interesante y muy llamativo
Que es buena pero necesitamos recursos capacitados con cubrir todas las necesidades
Es esencial para la prevención y que los equipos no queden vulnerables, además de distintos ataques actuales que nos perjudican en diferentes aspectos de la vida, por lo que sería de gran utilidad la enseñanza de ciberseguridad.
Hay poca enseñanza sobre ciberseguridad pero lo poco que se enseña lo aprenden
Es importante
Pues por el momento la materia va bien
Qué es un tema el cual deberíamos de saber todos

Ilustración 15. Resultados de la pregunta 14.

Esta penúltima pregunta de la encuesta se realizó de manera abierta, y no se graficó por la diversidad de respuestas así que su pueden observar diferentes sugerencias por parte de los encuestados.

¿Qué recomendaciones tendría para mejorar la enseñanza de la ciberseguridad en su institución?

174 respuestas

.
Ninguna
Que se den esos temas como una materia
Darle un poco mas prioridad a los temas de ciberseguridad por que es muy pobre en eso
Enseñanza personalizada
Tener contenido más actualizado
Apoyar a los estudiantes a aprender a como defenderse de los apartes ciberneticos con herramientas o cursos
Implementar en plan de estudios
Mostrar escenarios reales v cómo resolverlos

Ilustración 16. Resultados de la pregunta 15.

ANEXO 2

Gráficos de Resultados Pre-Test

En el contenido de este anexo se presentan los resultados obtenidos en la fase de evaluación de la plataforma, se incluyen, en primer lugar, los resultados del *pre-test*, acompañados de gráficos individuales para cada una de las preguntas, lo que permite observar el nivel de conocimientos inicial de los estudiantes. Posteriormente, se muestran los resultados del *post-test*, también con sus representaciones gráficas, que reflejan el progreso alcanzado después de la interacción con las simulaciones de CyberSimU. Finalmente, el anexo integra los resultados de la encuesta de pruebas de funcionalidad, donde se recogen las percepciones de los usuarios respecto a la usabilidad, claridad y pertinencia de los simuladores, brindando un panorama integral sobre la efectividad pedagógica y técnica de la herramienta.

4. Pregunta ¿Cuál es el propósito principal del comando ifconfig? (4 puntos)

[Más detalles](#)

83 % de los encuestados respondió correctamente a esta pregunta.

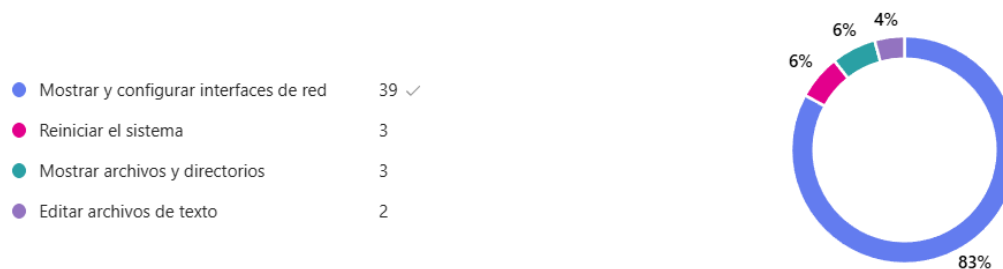


Ilustración 17. Resultados de la pregunta 1 del Pre-Test.

5. ¿Qué significa SSH? (4 puntos)

[Más detalles](#)

38 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 18. Resultados de la pregunta 2 del Pre-Test.

6. ¿Cuál es el objetivo de un ataque DDoS? (4 puntos)

[Más detalles](#)

55 % de los encuestados respondió correctamente a esta pregunta.

● Robar información	11
● Interrumpir servicios	26 ✓
● Instalar malware	3
● Obtener acceso root	7

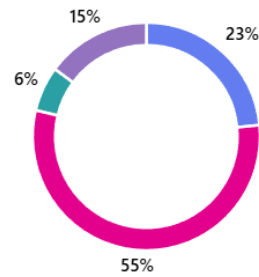


Ilustración 19. Resultados de la pregunta 3 del Pre-Test.

7. ¿Qué protocolo es más seguro contra sniffing? (4 puntos)

[Más detalles](#)

62 % de los encuestados respondió correctamente a esta pregunta.

● HTTP	9
● HTTPS	29 ✓
● FTP	7
● TELNET	2

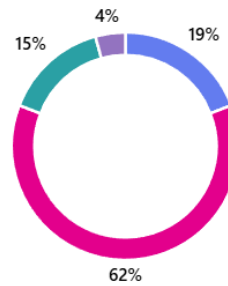


Ilustración 20. Resultados de la pregunta 4 del Pre-Test.

8. El comando 'ps' se utiliza para mostrar los procesos en ejecución. (4 puntos)

[Más detalles](#)

70 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	33 ✓
● Falso	14

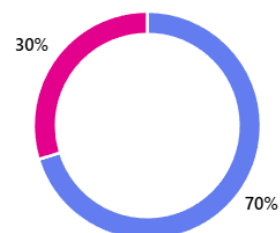


Ilustración 21. Resultados de la pregunta 5 del Pre-Test.

9. ¿Qué hace el comando 'netstat'? (4 puntos)

[Más detalles](#)

74 % de los encuestados respondió correctamente a esta pregunta.

● Muestra conexiones activas	35 ✓
● Borra archivos	1
● Instala software	5
● Edita contraseñas	6

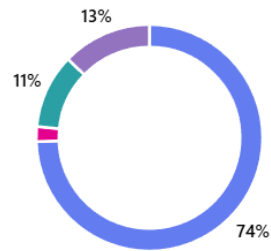


Ilustración 22. Resultados de la pregunta 6 del Pre-Test.

10. ¿Qué comando permite verificar la conectividad de red? (4 puntos)

[Más detalles](#)

83 % de los encuestados respondió correctamente a esta pregunta.

● ping	39 ✓
● dir	1
● whoami	3
● ftp	4

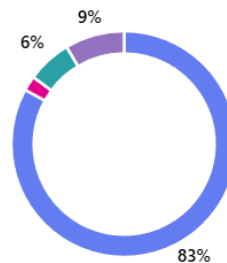


Ilustración 23. Resultados de la pregunta 7 del Pre-Test.

11. ¿Cuál es la principal forma de distribución del ransomware? (4 puntos)

[Más detalles](#)

77 % de los encuestados respondió correctamente a esta pregunta.

● Mensajes de texto	7
● Correos electrónicos de phishing	36 ✓
● Redes sociales	4
● Llamadas telefónicas	0

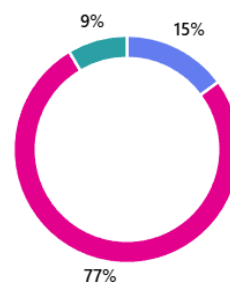


Ilustración 24. Resultados de la pregunta 8 del Pre-Test.

12. ¿Qué puerto se asocia comúnmente con el servicio SSH? (4 puntos)

[Más detalles](#)

45 % de los encuestados respondió correctamente a esta pregunta.

● 21	3
● 22	21 ✓
● 80	15
● 443	8

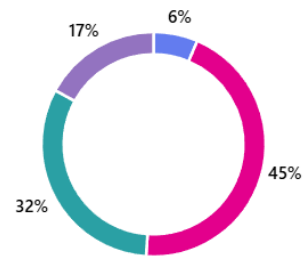


Ilustración 25. Resultados de la pregunta 9 del Pre-Test.

13. Los hashes criptográficos como MD5 son reversibles. (4 puntos)

[Más detalles](#)

62 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	18
● Falso	29 ✓

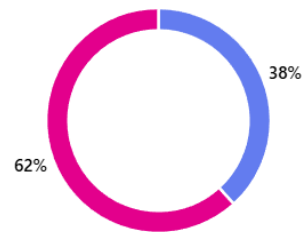


Ilustración 26. Resultados de la pregunta 10 del Pre-Test.

14. El comando 'whoami' muestra: (4 puntos)

[Más detalles](#)

62 % de los encuestados respondió correctamente a esta pregunta.

● Historial de comandos	6
● Usuario actual y contexto	29 ✓
● Tareas programadas	6
● IP pública	6

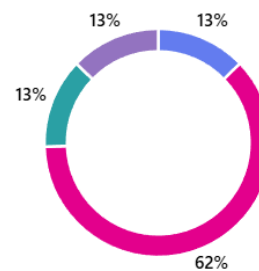


Ilustración 27. Resultados de la pregunta 11 del Pre-Test.

15. ¿Qué hace el comando 'nslookup'? (4 puntos)

[Más detalles](#)

68 % de los encuestados respondió correctamente a esta pregunta.

● Buscar archivos	5
● Consultar registros DNS	32 ✓
● Ver procesos activos	8
● Cerrar sesión	2

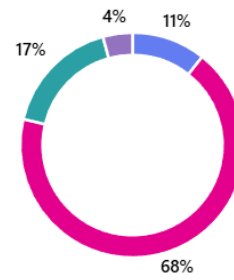


Ilustración 28. Resultados de la pregunta 12 del Pre-Test.

16. El comando 'tasklist' muestra una lista de procesos en ejecución. (4 puntos)

[Más detalles](#)

96 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	45 ✓
● Falso	2

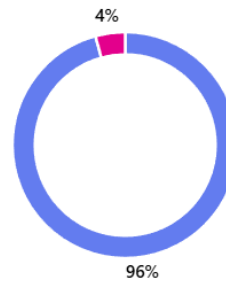


Ilustración 29. Resultados de la pregunta 13 del Pre-Test.

17. ¿Qué tipo de información puede capturar un sniffer? (4 puntos)

[Más detalles](#)

96 % de los encuestados respondió correctamente a esta pregunta.

● Solo imágenes	1
● Solo texto	1
● Solo videos	0
● Contraseñas, mensajes y datos sensibles	45 ✓

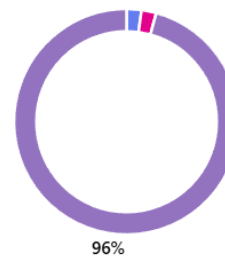


Ilustración 30. Resultados de la pregunta 14 del Pre-Test.

18. La esteganografía busca ocultar información dentro de archivos aparentemente normales. (4 puntos)

[Más detalles](#)

72 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 31. Resultados de la pregunta 15 del Pre-Test.

19. ¿Qué comando muestra la ruta de red hacia un destino? (4 puntos)

[Más detalles](#)

45 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 32. Resultados de la pregunta 16 del Pre-Test.

20. ¿Cuál es el puerto estándar del servicio MySQL? (4 puntos)

[Más detalles](#)

64 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 33. Resultados de la pregunta 17 del Pre-Test.

21. ¿Qué es un rootkit? (4 puntos)

[Más detalles](#)

55 % de los encuestados respondió correctamente a esta pregunta.

● Un tipo de malware que oculta actividades	26 ✓
● Una herramienta de respaldo	13
● Un firewall	5
● Un tipo de antivirus	3

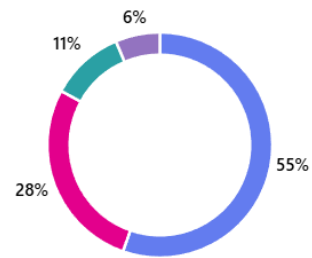


Ilustración 34. Resultados de la pregunta 18 del Pre-Test.

22. ¿Qué comando permite ver la tabla ARP? (8 puntos)

[Más detalles](#)

77 % de los encuestados respondió correctamente a esta pregunta.

● arp -a	36 ✓
● ipconfig	4
● ls	4
● kill	3

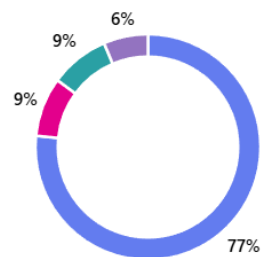


Ilustración 35. Resultados de la pregunta 19 del Pre-Test.

23. La monitorización de tráfico es una medida preventiva contra ataques DDoS. (4 puntos)

[Más detalles](#)

85 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	40 ✓
● Falso	7

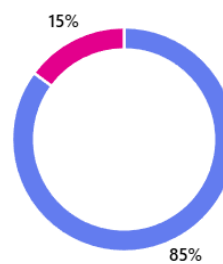


Ilustración 36. Resultados de la pregunta 20 del Pre-Test.

24. Un sistema comprometido debe ser apagado inmediatamente. (4 puntos)

[Más detalles](#)

47 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 37. Resultados de la pregunta 21 del Pre-Test.

25. ¿Qué método de pago exigen usualmente los atacantes de ransomware? (8 puntos)

[Más detalles](#)

51 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 38. Resultados de la pregunta 22 del Pre-Test.

26. Pagar el rescate garantiza la recuperación de archivos cifrados. (4 puntos)

[Más detalles](#)

81 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 39. Resultados de la pregunta 23 del Pre-Test.

Resultados de *Post-Test*

4. ¿Qué comando se usa para asignar manualmente una IP a una interfaz de red? (4 puntos)

[Más detalles](#)

26 % de los encuestados respondió correctamente a esta pregunta.

● ifconfig	14 ✓
● ipconfig	17
● netsh	18
● ping	4

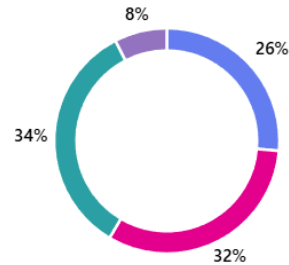


Ilustración 40. Resultados de la pregunta 1 del *Post-Test*.

5. ¿Cuál es el principal uso del protocolo SSH? (4 puntos)

[Más detalles](#)

67 % de los encuestados respondió correctamente a esta pregunta.

● Transferencia de archivos	7
● Instalación de software	9
● Control remoto seguro	35 ✓
● Compartir impresoras	1

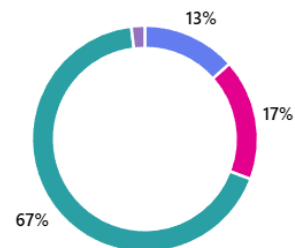


Ilustración 41. Resultados de la pregunta 2 del *Post-Test*.

6. ¿Cuál de las siguientes opciones describe mejor un ataque de denegación de servicio? (4 puntos)

[Más detalles](#)

70 % de los encuestados respondió correctamente a esta pregunta.

● Espiar contraseñas	6
● Suplantar identidad	6
● Inundar un servidor para hacerlo inaccesible	37 ✓
● Acceder al root	4

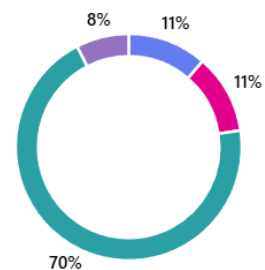


Ilustración 42. Resultados de la pregunta 3 del *Post-Test*.

7. ¿Cuál protocolo previene mejor ataques de tipo sniffing? (4 puntos)

[Más detalles](#)

62 % de los encuestados respondió correctamente a esta pregunta.

● FTP	4
● SMB	5
● HTTP	11
● HTTPS	32 ✓

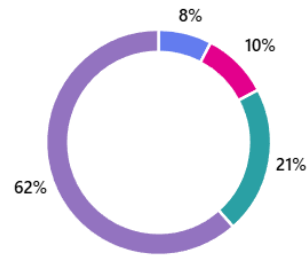


Ilustración 43. Resultados de la pregunta 4 del Post-Test.

8. El comando 'top' se usa para ver procesos activos en tiempo real (4 puntos)

[Más detalles](#)

79 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	42 ✓
● Falso	11

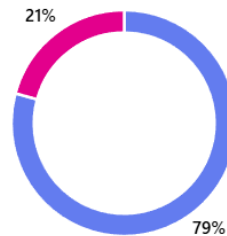


Ilustración 44. Resultados de la pregunta 5 del Post-Test.

9. ¿Cuál es la finalidad del comando 'netstat -an'? (4 puntos)

[Más detalles](#)

70 % de los encuestados respondió correctamente a esta pregunta.

● Reiniciar el sistema	4
● Borrar historial	9
● Mostrar conexiones de red detalladas	37 ✓
● Conectarse a un servidor	3

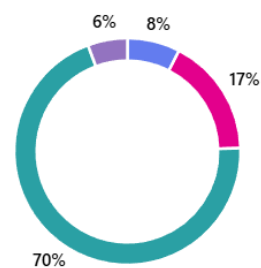


Ilustración 45. Resultados de la pregunta 5 del Post-Test.

10. ¿Qué comando diagnostica problemas de red enviando paquetes ICMP? (4 puntos)

[Más detalles](#)

73 % de los encuestados respondió correctamente a esta pregunta.

● echo	1
● ftp	6
● ping	38 ✓
● mkdir	7



Ilustración 46. Resultados de la pregunta 6 del Post-Test.

11. ¿Qué método es más común para iniciar un ataque de ransomware? (4 puntos)

[Más detalles](#)

64 % de los encuestados respondió correctamente a esta pregunta.

● USB infectado	6
● Anuncios maliciosos	9
● Mensajes de texto	4
● Phishing por correo	34 ✓

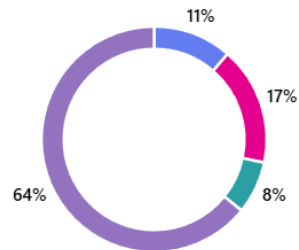


Ilustración 47. Resultados de la pregunta 7 del Post-Test.

12. ¿Qué puerto usa por defecto el protocolo SSH? (4 puntos)

[Más detalles](#)

75 % de los encuestados respondió correctamente a esta pregunta.

● 21	6
● 25	3
● 22	39 ✓
● 110	4

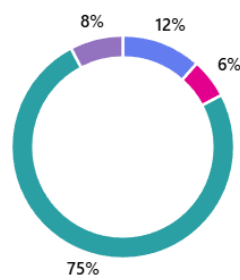


Ilustración 48. Resultados de la pregunta 8 del Post-Test.

13. Los algoritmos hash están diseñados para ser fácilmente reversibles. (4 puntos)

[Más detalles](#)

57 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 49. Resultados de la pregunta 9 del Post-Test.

14. ¿Cuál comando permite saber qué usuario está logueado actualmente? (4 puntos)

[Más detalles](#)

75 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 50. Resultados de la pregunta 10 del Post-Test.

15. ¿Qué herramienta sirve para consultar información DNS de un dominio? (4 puntos)

[Más detalles](#)

63 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 51. Resultados de la pregunta 11 del Post-Test.

16. 'taskkill' permite terminar un proceso desde la línea de comandos. (4 puntos)

[Más detalles](#)

88 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	46 ✓
● Falso	6



Ilustración 52. Resultados de la pregunta 12 del Post-Test.

17. ¿Cuál es el riesgo principal de usar una red WiFi pública sin protección? (4 puntos)

[Más detalles](#)

94 % de los encuestados respondió correctamente a esta pregunta.

● Alta velocidad	2
● Intercepción de datos	49 ✓
● Mayor alcance	0
● Acceso libre	1

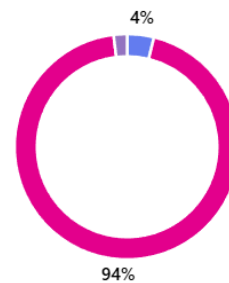


Ilustración 53. Resultados de la pregunta 13 del Post-Test.

18. La esteganografía y la criptografía tienen el mismo objetivo. (4 puntos)

[Más detalles](#)

53 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	25
● Falso	28 ✓

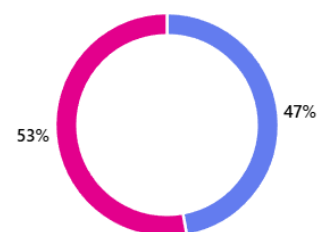


Ilustración 54. Resultados de la pregunta 14 del Post-Test.

19. ¿Qué comando traza la ruta de red hacia un servidor remoto? (4 puntos)

[Más detalles](#)

73 % de los encuestados respondió correctamente a esta pregunta.

● traceroute	38 ✓
● ipconfig	8
● nslookup	4
● netstat	2

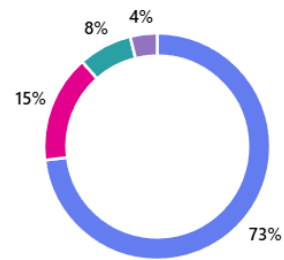


Ilustración 55. Resultados de la pregunta 14 del Post-Test.

20. ¿Qué puerto corresponde al motor de base de datos MySQL? (4 puntos)

[Más detalles](#)

65 % de los encuestados respondió correctamente a esta pregunta.

● 80	7
● 22	6
● 1433	5
● 3306	34 ✓

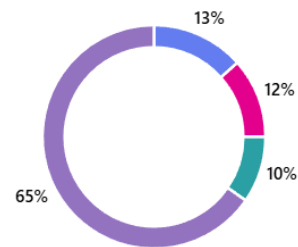


Ilustración 56. Resultados de la pregunta 15 del Post-Test.

21. ¿Qué tipo de malware se caracteriza por ocultar su presencia en el sistema? (4 puntos)

[Más detalles](#)

52 % de los encuestados respondió correctamente a esta pregunta.

● Spyware	12
● Rootkit	27 ✓
● Troyano	11
● Botnet	2

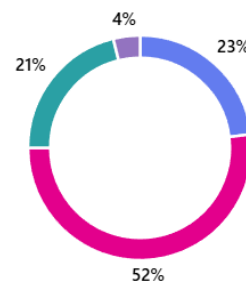


Ilustración 57. Resultados de la pregunta 16 del Post-Test.

22. ¿Qué comando muestra la tabla de direcciones físicas y lógicas? (4 puntos)

[Más detalles](#)

67 % de los encuestados respondió correctamente a esta pregunta.

● ipconfig	7
● netstat -r	6
● arp -a	35 ✓
● whois	4

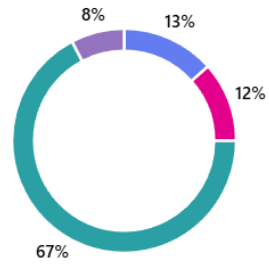


Ilustración 58. Resultados de la pregunta 17 del Post-Test.

23. Monitorear el ancho de banda puede ayudar a detectar ataques inusuales. (4 puntos)

[Más detalles](#)

87 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	46 ✓
● Falso	7

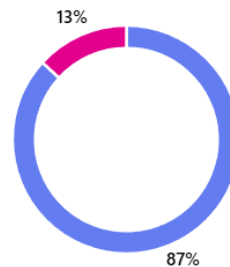


Ilustración 59. Resultados de la pregunta 18 del Post-Test.

24. ¿Qué medida garantiza la recuperación segura tras una intrusión? (4 puntos)

[Más detalles](#)

66 % de los encuestados respondió correctamente a esta pregunta.

● Actualizar drivers	7
● Escanear con antivirus	11
● Restaurar respaldo	35 ✓
● Cerrar sesión	0

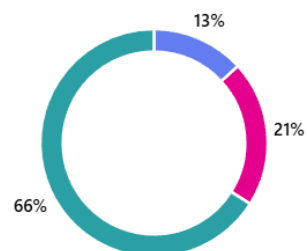


Ilustración 60. Resultados de la pregunta 19 del Post-Test.

25. ¿Cuál es el propósito de la opción '-sS' en Nmap? (4 puntos)

[Más detalles](#)

57 % de los encuestados respondió correctamente a esta pregunta.

● Escaneo de SYN	30 ✓
● Escaneo de versión	7
● Escaneo de OS	11
● Escaneo completo	5

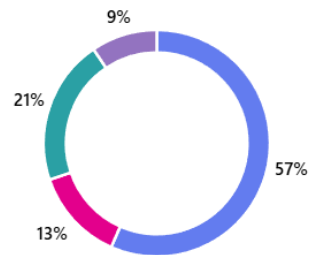


Ilustración 61. Resultados de la pregunta 20 del Post-Test.

26. Apagar un equipo comprometido ayuda a preservar evidencias. (4 puntos)

[Más detalles](#)

43 % de los encuestados respondió correctamente a esta pregunta.

● Verdadero	23 ✓
● Falso	30

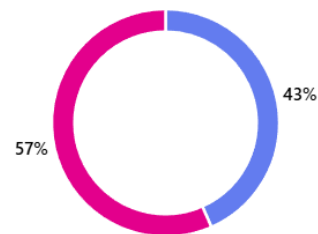


Ilustración 62. Resultados de la pregunta 21 del Post-Test.

27. ¿Qué forma de pago suele solicitar el ransomware para liberar los archivos? (4 puntos)

[Más detalles](#)

73 % de los encuestados respondió correctamente a esta pregunta.

● Paypal	9
● Criptomonedas	38 ✓
● Transferencia bancaria	5
● Efectivo	0

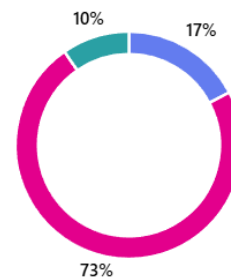


Ilustración 63. Resultados de la pregunta 22 del Post-Test.

28. Pagar el rescate a un atacante es una garantía de recuperar los datos (4 puntos)

[Más detalles](#)

81 % de los encuestados respondió correctamente a esta pregunta.



Ilustración 64. Resultados de la pregunta 23 del Post-Test.

Resultados de Pruebas de Funcionalidad

Selecciona la institución de donde actualmente cursando tus estudios

35 respuestas

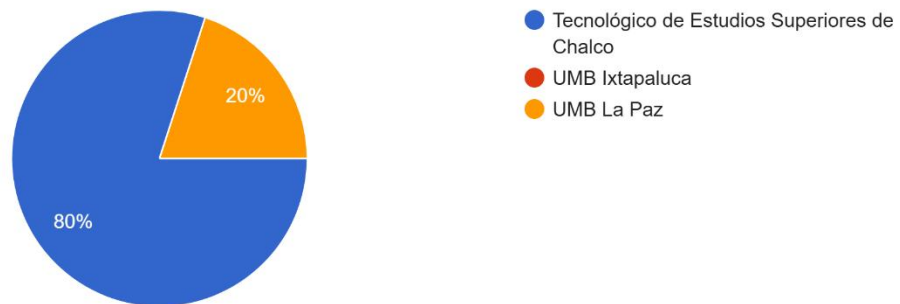


Ilustración 65. Resultados de la pregunta 1 de las pruebas de funcionalidad.

¿Qué semestre estas cursando?

35 respuestas

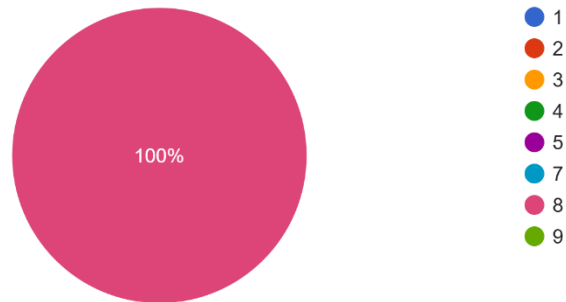


Ilustración 66. Resultados de la pregunta 2 de las pruebas de funcionalidad.

Rol dentro de la plataforma:

36 respuestas

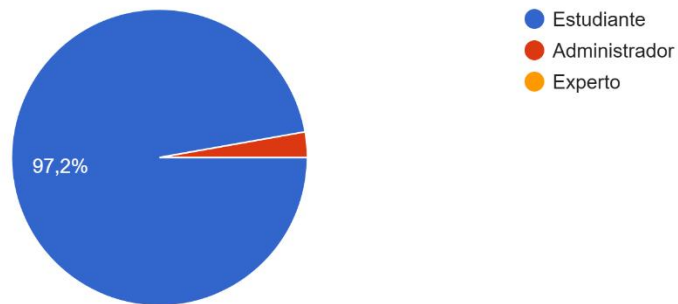


Ilustración 67. Resultados de la pregunta 3 de las pruebas de funcionalidad.

Nivel de experiencia en ciberseguridad:

36 respuestas

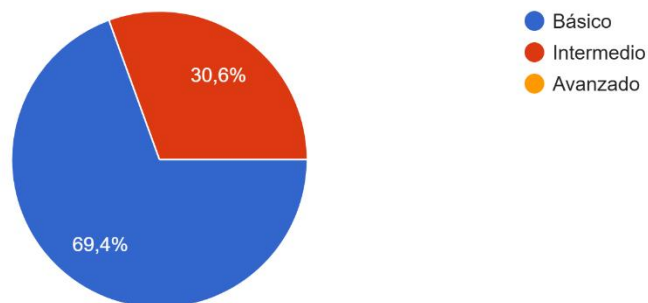


Ilustración 68. Resultados de la pregunta 4 de las pruebas de funcionalidad.

La plataforma es fácil de navegar y acceder a las funciones principales.

36 respuestas

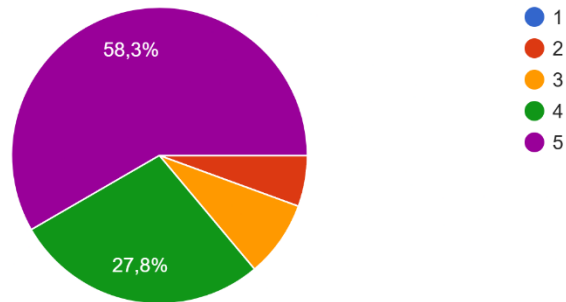


Ilustración 69. Resultados de la pregunta 5 de las pruebas de funcionalidad.

La información y las opciones de menú principal de simulaciones están bien organizadas.

36 respuestas

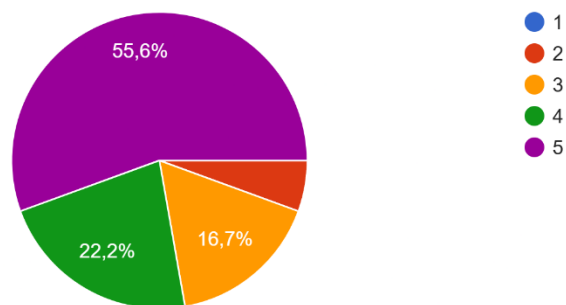


Ilustración 70. Resultados de la pregunta 6 de las pruebas de funcionalidad.

No encontré dificultades técnicas al iniciar sesión y acceder a los módulos.

36 respuestas

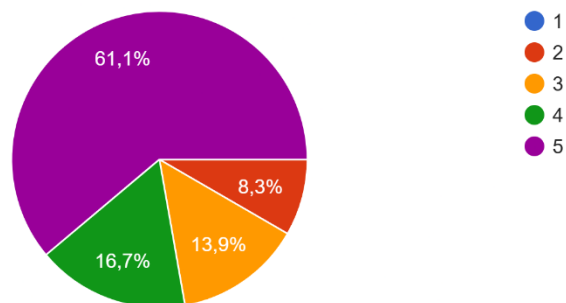


Ilustración 71. Resultados de la pregunta 7 de las pruebas de funcionalidad.

Como estudiante, puedo acceder a mis simulaciones y realizar pruebas sin problemas.
36 respuestas

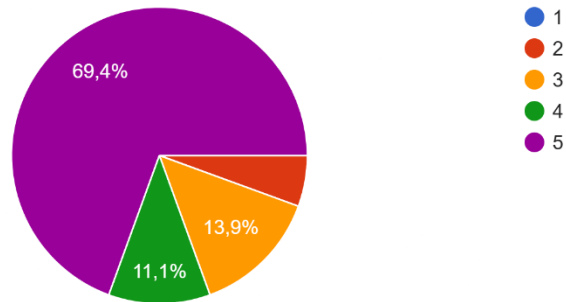


Ilustración 72. Resultados de la pregunta 8 de las pruebas de funcionalidad.

Los escenarios de simulación son realistas y bien estructurados.
36 respuestas

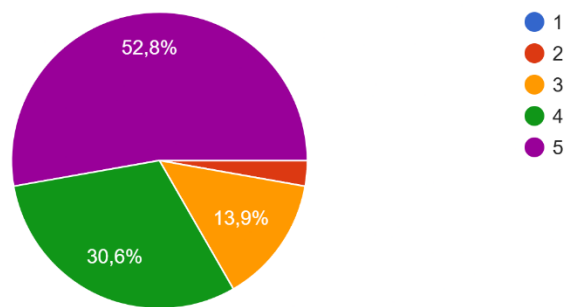


Ilustración 73. Resultados de la pregunta 9 de las pruebas de funcionalidad.

Las simulaciones reflejan ataques reales como phishing, ransomware y DDoS de manera clara.
36 respuestas

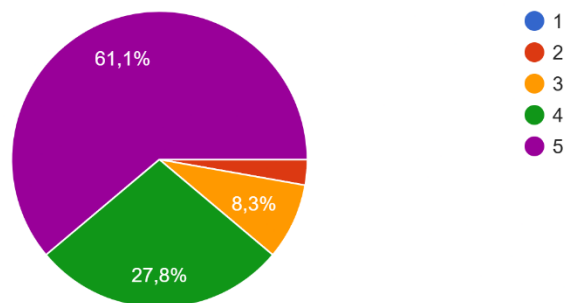


Ilustración 74. Resultados de la pregunta 10 de las pruebas de funcionalidad.

Los ejercicios de práctica son dinámicos y permiten mejorar habilidades en ciberseguridad.
36 respuestas

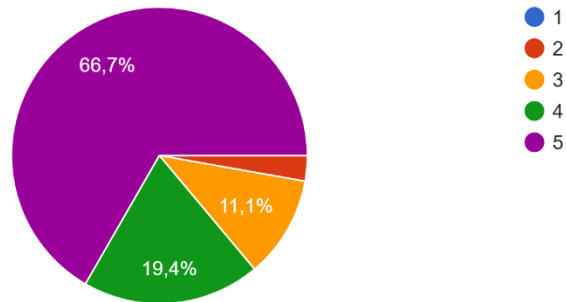


Ilustración 75. Resultados de la pregunta 11 de las pruebas de funcionalidad.

La plataforma responde rápidamente a las acciones realizadas.
36 respuestas

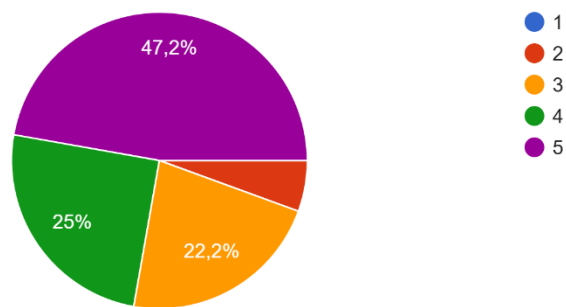


Ilustración 76. Resultados de la pregunta 12 de las pruebas de funcionalidad.

No experimenté fallos o retrasos significativos al ejecutar simulaciones.
36 respuestas

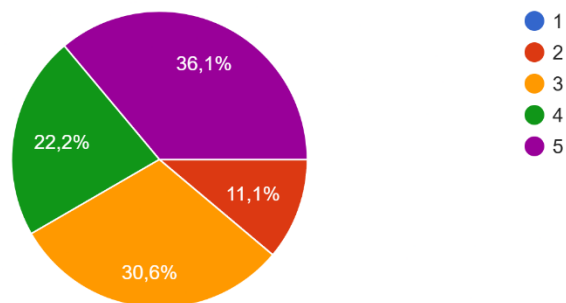


Ilustración 77. Resultados de la pregunta 13 de las pruebas de funcionalidad.

Los tiempos de carga y respuesta fueron adecuados para una experiencia fluida.
36 respuestas

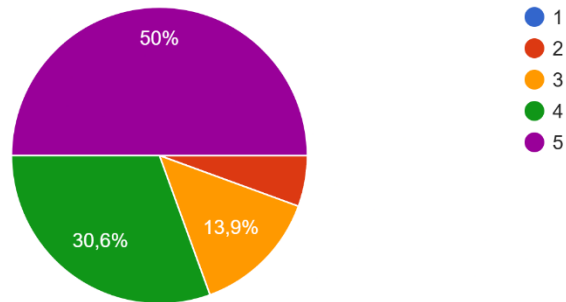


Ilustración 78. Resultados de la pregunta 14 de las pruebas de funcionalidad.

Me siento seguro utilizando la plataforma y compartiendo datos dentro de ella.
36 respuestas

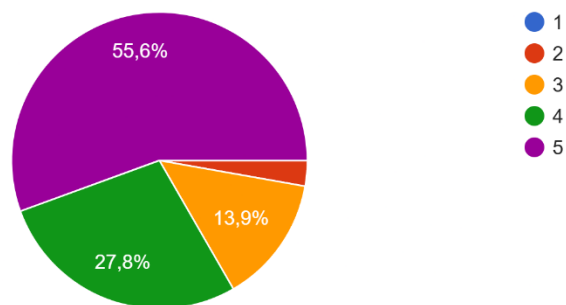


Ilustración 79. Resultados de la pregunta 15 de las pruebas de funcionalidad.

La autenticación y autorización funcionan correctamente según mi rol.
36 respuestas

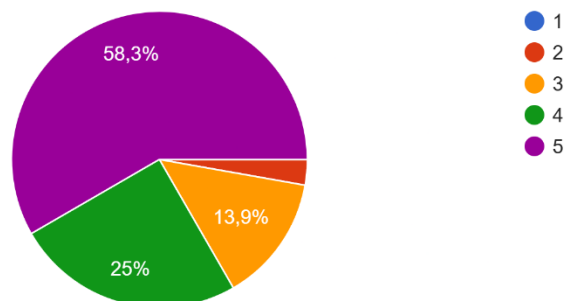


Ilustración 80. Resultados de la pregunta 16 de las pruebas de funcionalidad.

Se respetan las mejores prácticas de ciberseguridad dentro de la plataforma.

36 respuestas

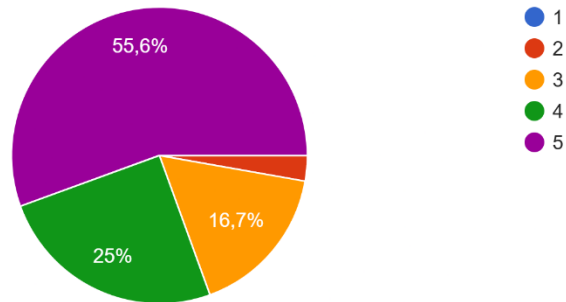


Ilustración 81. Resultados de la pregunta 17 de las pruebas de funcionalidad.

Las recomendaciones de estudio son personalizadas y útiles.

36 respuestas

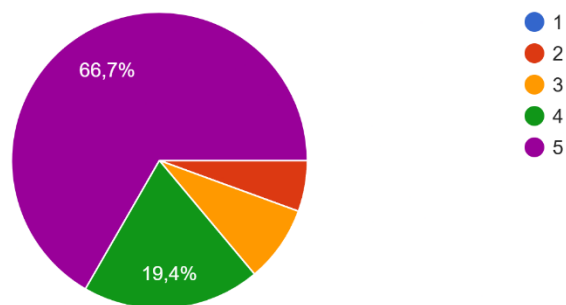


Ilustración 82. Resultados de la pregunta 18 de las pruebas de funcionalidad.

La plataforma me proporciona reportes detallados sobre mi desempeño.

36 respuestas

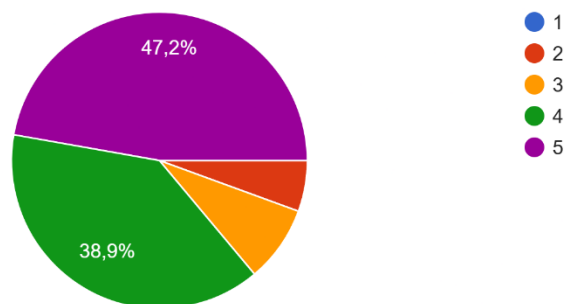


Ilustración 83. Resultados de la pregunta 19 de las pruebas de funcionalidad.

La interfaz para revisar mis resultados es clara y fácil de interpretar.

36 respuestas

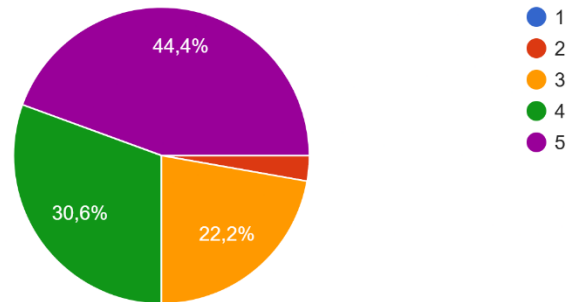


Ilustración 84. Resultados de la pregunta 20 de las pruebas de funcionalidad.

¿Qué funcionalidades mejorarías en la plataforma?

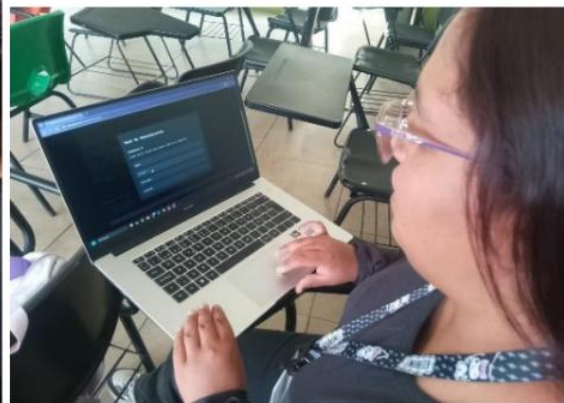
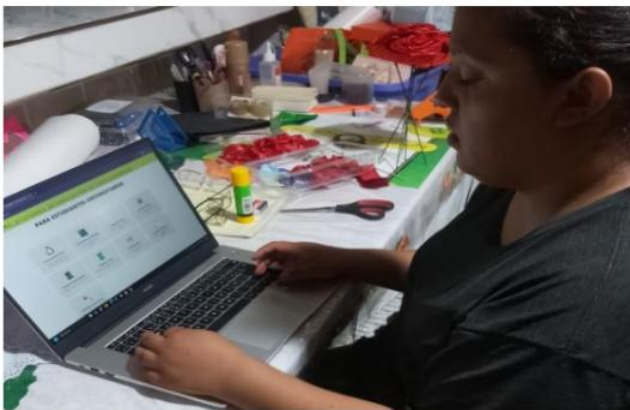
31 respuestas

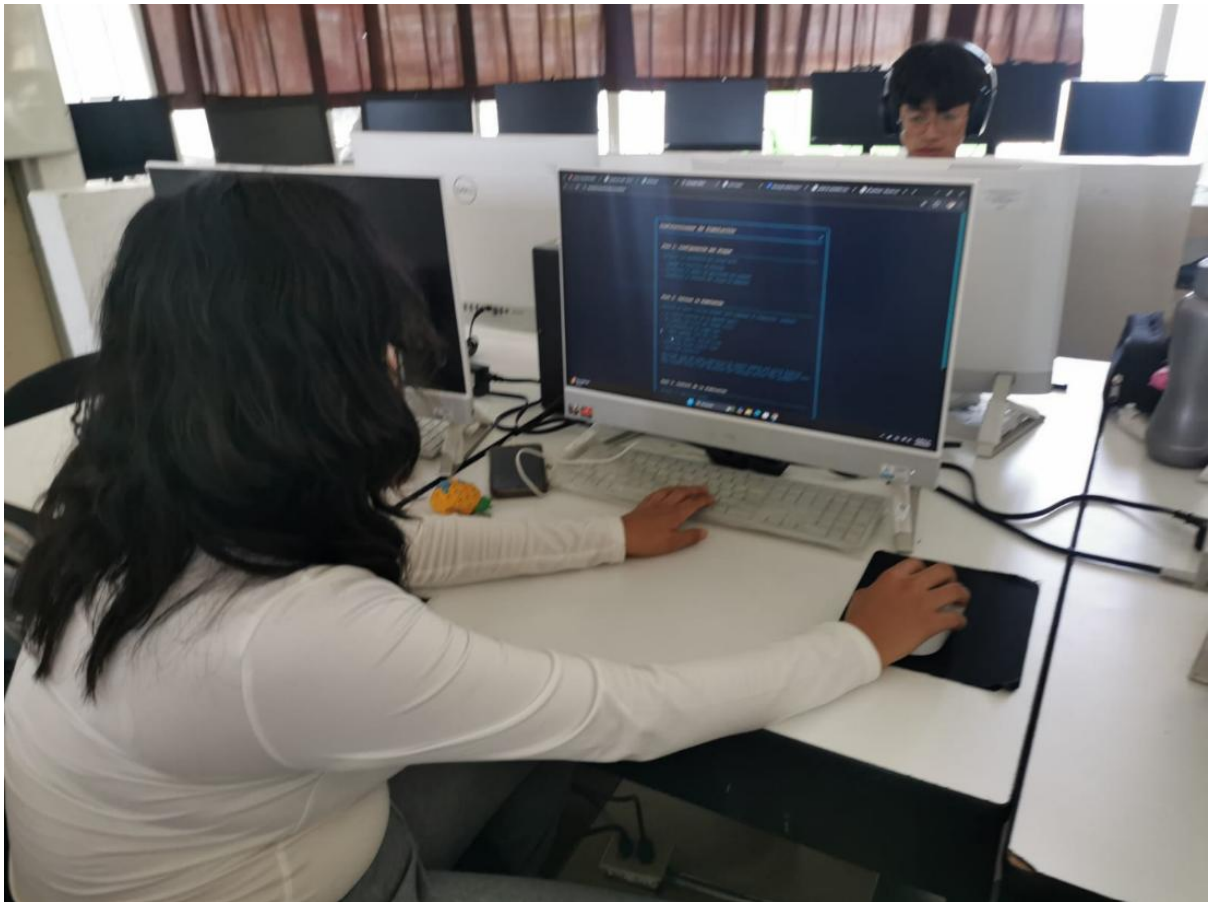
- Ninguna
- Ninguna, todo esta perfecto
- Ninguna está bien
- Ninguna siento que esta completa
- en las evaluaciones mostrar resultados con mas claridad a los usuarios, mostrado sus resultados con una explicación del porque esta bien o mal la respuesta a manera de corregir y retroalimentar al usuario
- Solo en la parte del texto que fuera un poco menos y a lo mejor más dinámico con más imágenes para captar la atención, pero en general las funcionalidades están muy bien explicadas y hechas.
- La mejora del sistema de calificación. Poner las respuestas correctas para un retroalimentación

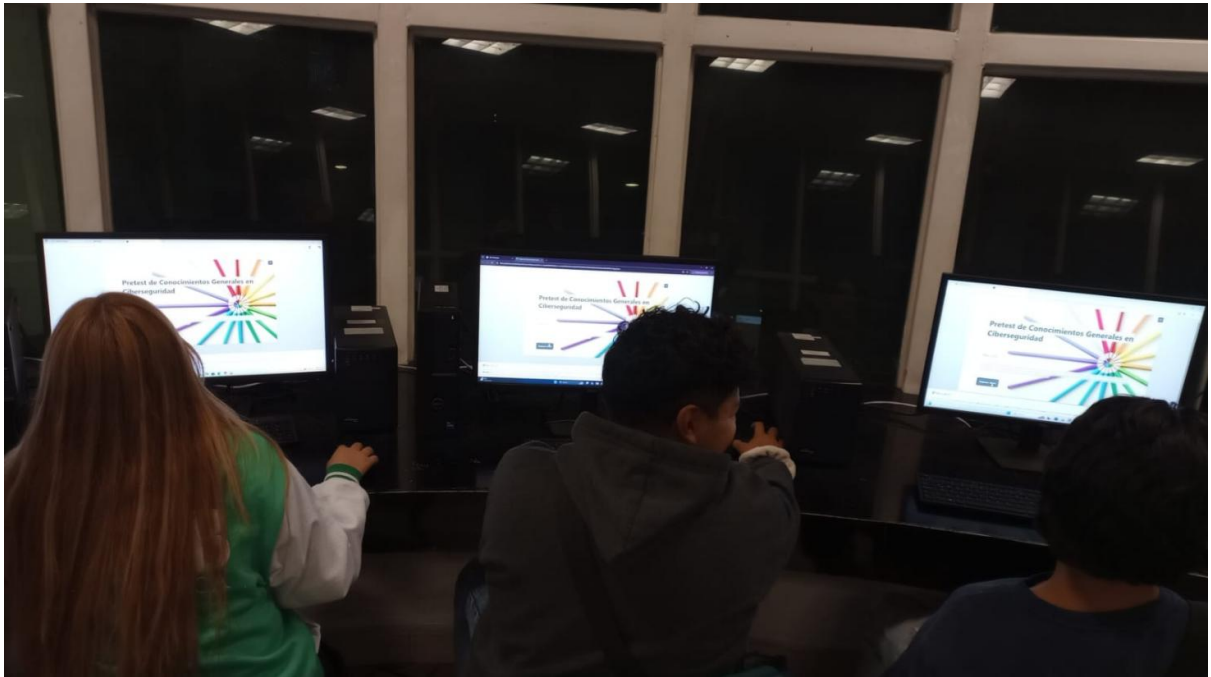
Ilustración 85. Resultados de la pregunta 21 de las pruebas de funcionalidad.

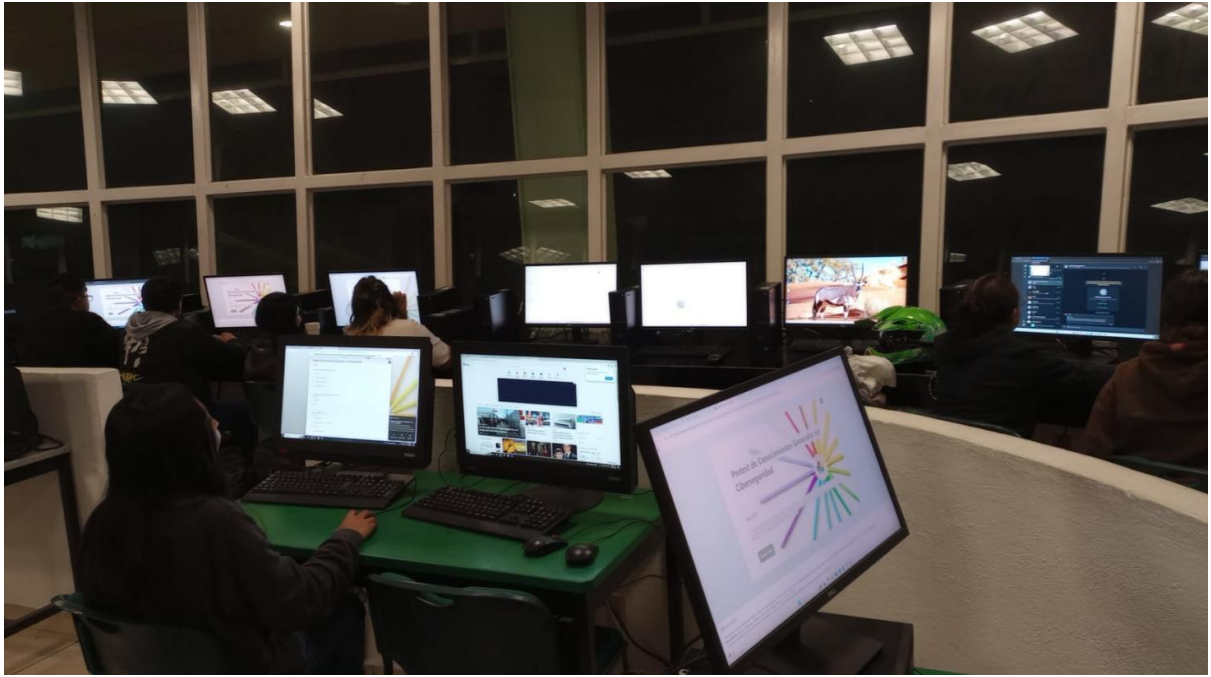
ANEXO 3

En el presente anexo se muestran las evidencias de la utilización del simulador CyberSimU en las diferentes instituciones de educación superior y fotografías de la aplicación de los cuestionarios de *Pre-Test* y *Post-Test* con alumnos de diversos semestres que participaron en las pruebas del simulador.









ANEXO 4

Se participo en dos ponencias tituladas “Propuestas de un sistema de evaluación y recomendación de estudio utilizando lógica difusa en simuladores de ciberseguridad”, y “avances en la capacitación de ciberseguridad: Modelos innovadores para la educación superior”, en el primer congreso de educación científica y tecnológica: Su relación con el trabajo en el Estado de México, el cual se llevó a cabo los días 19 y 20 de junio de 2024 en las instalaciones del Tecnológico de Estudios Superiores de Valle de Bravo, además derivado de las ponencias se publico la memoria de congreso en la revista digital UDEMEX suplemento #15 año 2, Num 7 en Octubre de 2024, con registro ISSN 2992-7056, adjuntado link de evidencia <https://www.udemex.edu.mx/Suplemento23Octubre>





Propuesta de un sistema de evaluación y recomendación de estudio utilizando lógica difusa en simuladores de ciberseguridad.



Eje temático: Ciberseguridad

KEVIN GYOVANI RAMÍREZ VITE

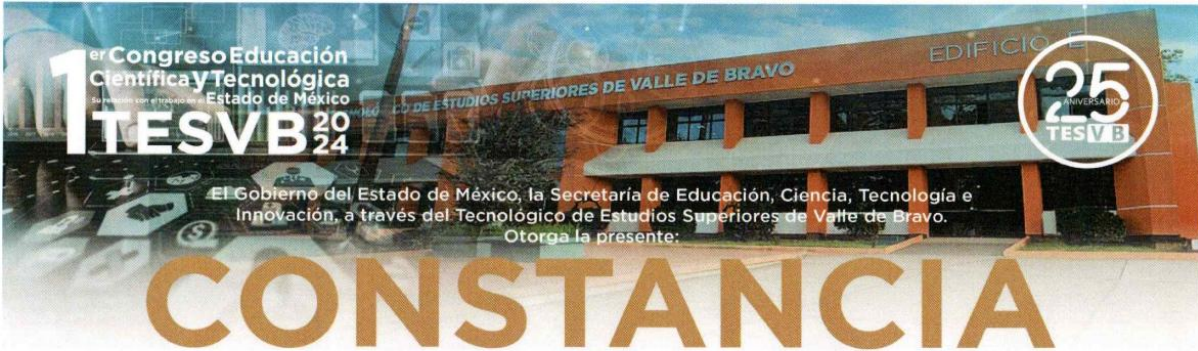
TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHALCO

ANABELEM SOBERANES MARTÍN

CENTRO UNIVERSITARIO UAEMEX VALLE DE CHALCO

RESUMEN

En esta ponencia se presenta el desarrollo de un sistema de evaluación y recomendación de estudio utilizando lógica difusa en simuladores de ciberseguridad. Actualmente, se han definido las reglas de inferencia difusa en una estructura del tipo Sugeno. El objetivo es implementarlo en una plataforma web, por lo que las variables de entrada consideradas son, en primer lugar, el tiempo dentro del simulador; la segunda entrada es la evaluación en el examen final y la tercera es la duración del examen. Por otro lado, las variables de salida son el resultado del examen y las recomendaciones de estudio en términos de tiempo. El modelo ha sido desarrollado en Matlab utilizando la aplicación Fuzzy Logic Designer. Se han realizado las pruebas necesarias para su evaluación y se han obtenido resultados preliminares, los cuales indican que este sistema puede mejorar significativamente la personalización del aprendizaje y la efectividad en cuanto a capacitación en ciberseguridad. Este sistema representa una herramienta dentro del espectro de la Inteligencia Artificial adaptando el conocimiento de la práctica docente para generar las recomendaciones de estudio individuales de los estudiantes. Se destaca su potencial de aplicabilidad en la educación superior en México.



a:

Kevin Gyovani Ramírez Vite

Por su participación con la ponencia titulada "Avances en la capacitación de ciberseguridad: modelos innovadores para la educación superior" en el 1er Congreso de Educación Científica y Tecnológica: su relación con el trabajo en el Estado de México, llevado a cabo los días 19 y 20 de junio de 2024 en las instalaciones del Tecnológico de Estudios Superiores de Valle de Bravo.

Dr. Fidel Argenis Flores Quiroz
Director General

Dr. Lázaro Abner Hernández Reyes
Director Académico

Valle de Bravo, Estado de México, 20 de junio 2024





Avances en la Capacitación de Ciberseguridad: Modelos Innovadores para la Educación Superior.

Eje temático: Ciberseguridad

KEVIN GYOVANI RAMÍREZ VITE

TECNOLÓGICO DE ESTUDIOS SUPERIORES DE CHALCO

ANABELEM SOBERANES MARTÍN

CENTRO UNIVERSITARIO UAEMEX VALLE DE CHALCO



RESUMEN

La capacitación en ciberseguridad en instituciones de educación superior está experimentando avances significativos debido a la adopción de modelos innovadores y herramientas interactivas. Se busca preparar a estudiantes para enfrentar los desafíos de un entorno en constante evolución. Se planteó como objetivo la búsqueda de diferentes modelos a través de un marco de trabajo denominado SALSA Framework, el cual permite revisiones sistemáticas de la literatura, donde los parámetros de búsqueda fueron simulaciones realistas de amenazas cibernéticas, donde los participantes desarrollen habilidades prácticas de detección y respuesta. Además, se incluyeron laboratorios virtuales y entornos de aprendizaje basados en juegos, proporcionando experiencias de aprendizaje envolventes y efectivas. Estas tecnologías permiten a los estudiantes aplicar sus conocimientos teóricos en entornos simulados para resolver problemas de seguridad cibernética. Los resultados han demostrado que estos métodos mejoran significativamente la preparación de los participantes. Se expondrán de manera general los avances logrados, destacando ejemplos concretos de modelos innovadores y herramientas interactivas utilizadas en la capacitación de ciberseguridad, especialmente aplicables en la educación superior en México.

ANEXO 5

Se participo en el “1er Congreso Multidisciplinario de Investigación del TESCH: Difundiendo Ciencia en el Estado de México” con la ponencia “Simuladores de Ciberseguridad, un Enfoque educativo para Universitarios” obteniendo el premio del primer lugar a la mejor ponencia del día.



ANEXO 6

Se participo en la Semana de la Sostenibilidad dentro la Universidad Mexiquense del Bicentenario plantel Ixtapaluca celebrada del 26 de Noviembre al 2 de Diciembre de 2024, con la ponencia denominada “Ciberataques Razones, Técnicas y Objetivos”.



La Universidad Mexiquense del Bicentenario,
a través de la
Unidad de Estudios Superiores Ixtapaluca,
otorgan la presente:

Agradecimiento

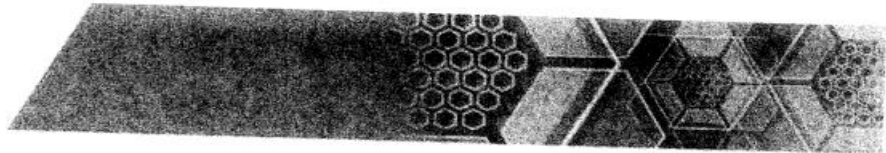
AL: **MTRO. KEVIN GYOVANI RAMÌREZ VITE**

Por impartir el taller “Ciberataques: Razones, Técnicas y Objetivos” en
“LA SEMANA DE LA SOSTENIBILIDAD” llevada a cabo en esta casa de estudios
del 26 Noviembre al 02 de Diciembre del 2024.

MARGARITA GARCIA PEDRAZA
COORDINADORA UES IXTAPALUCA

ANEXO 7

Como parte de las acciones de retribución social se participó con la impartición de tres talleres denominados “Ciberataques, Razones Técnicas y Objetivos” a estudiantes del Centro Universitario Valle de Chalco, celebrado el día 15 de Octubre de 2024.



Otorga la presente

Constancia

Al

Mtro. Kevin Gyovani Ramirez Vite

Por impartir tres talleres denominados “**Ciberseguridad razones técnicas y objetivos**” a estudiantes del Centro Universitario Valle de Chalco, como parte de las acciones de Retribución Social.

Valle de Chalco Solidaridad, a 15 de Octubre de 2024.

Patria, Ciencia y Trabajo

"2024, Conmemoración del 60 Aniversario de la Inauguración de Ciudad Universitaria"

Dra. en A. D. Verónica Lopera Suárez

Coordinadora del Programa Institucional de Tutoría Académica



VALLE DE CHALCO
COORDINACIÓN DE TUTORÍAS

**SOMOS
UAEMéx**

 **CUVCH**

Además, se participó en el taller “Juega con Gestos, Aprendiendo Sin Contacto en el Aula con Media Pipe” a estudiantes del quinto y sexto grado de la Escuela Primaria Paulo Freire Turno Vespertino de Valle de Chalco el día 15 de Octubre de 2024, todo esto también como parte de las acciones de retribución social.



Universidad Autónoma del Estado de México

Centro Universitario Valle de Chalco

Otorga la presente

Constancia

a: Kevin Gyovani Ramírez Vite

Por impartir el taller: “**¡Juega con Gestos! Aprendiendo Sin Contacto en el Aula con MediaPipe**” a estudiantes del quinto y sexto grado de la Escuela Primaria Paulo Freire Turno Vespertino de Valle de Chalco, el día 15 de octubre de 2024, a las 14:00 horas, en las instalaciones del mencionado organismo académico, como parte del programa institucional de posgrado Retribución Social.

Valle de Chalco Solidaridad, Edo. de Méx. a 15 de octubre de 2024

PATRIA, CIENCIA Y TRABAJO

“2024, Conmemoración del 60 Aniversario de la Inauguración de Ciudad Universitaria”

Una firma manuscrita en tinta azul que parece ser la del Sr. Joaquín Morales Alfaro.

M. en C. C. Joaquín Morales Alfaro
Encargado del Despacho de la Dirección
Centro Universitario Valle de Chalco UAEMéx



ANEXO 8

El Anexo 8 reúne las principales evidencias relacionadas con la movilidad académica realizada en la Universidad de Hildesheim durante el semestre de verano 2025. En este apartado se incluye la carta de aceptación oficial, documento que respalda la incorporación al programa de intercambio. Asimismo, se presenta la lista de materias cursadas, lo que permite identificar las áreas de formación abordadas durante la estancia. Finalmente, se integra el certificado de asistencia (Attendance Certificate), que valida formalmente la participación y el cumplimiento de las actividades académicas durante el periodo establecido.

Stiftung Universität Hildesheim



Stiftung Universität Hildesheim | Universitätsplatz 1 | 31141 Hildesheim

To whom it may concern

Letter of Acceptance

It is hereby certified that

Kevin Gyovani Ramirez Vite

Home University: **Universidad Autónoma del Estado de México**

Date of birth: 15.06.1984

Place of birth:

Nationality: Mexiko

Home address: Jose Campos Lt 12
56560 Ayotla
Mexico

is accepted as an exchange student at the University of Hildesheim for the **summer semester 2024/25 (01.04.2025 – 30.09.2025)**.

Please note the study period for exchange students (07.04.2025-31.07.2025).

The language of instruction will be English (B2 level) and the English knowledge has been proven by the home university as sufficient to follow the courses.



Stiftung Universität Hildesheim • Postfach 10 13 63 • D-31141 Hildesheim

Hauptgebäude
Universitätsplatz 1
31141 Hildesheim

To whom it may concern

apl. Prof. Dr. Thomas Mandl
Information Science
University of Hildesheim

Fon: 05121 / 883-30306
E-Mail: mandl@uni-hildesheim.de

16th June 2025

Letter of Confirmation

I hereby confirm that the exchange student

Kevin Gyovani Ramirez Vite

from the Universidad Autónoma del Estado de México, Plantel Valle de Chalco
is currently studying at the University of Hildesheim in Germany.

The student is attending the following courses for:

- Big Data Analytics (3103) – 6 credits
- Natural Language Processing (3113) – 6 credits
- Hauptseminar Information and Society: Information Ethics (4363) – 4 credits
- English for international students (Vollzeit + Erasmus) (0311) – 4 credits
- English conversation and pronunciation (0312) – 2 credits
- Intercultural Workshops for Students (0111) – 2 credits

So far, the student has been working and participating well and has carried out all intermediary tasks. If he continues in this manner, he will pass the courses and receive the credits. However, our university does not confirm participation until the end of the semester for formal reasons.

I am happy to clarify any further questions.

Best regards,

CERTIFICATE OF ATTENDANCE

Kevin Gyovani Ramirez Vite

has participated in the
intercultural incoming workshop and semester-accompanying program

Welcome on Board

Summer semester 2025

Objective of *Welcome on Board* is the promotion of intercultural competencies and sensitization by connecting own experiences with scientific findings in the research field of intercultural communication. Basic knowledge about the dynamism of intercultural communication processes, the promotion of the ability to reflect, as well as developing action prospects for intercultural encounters are the main goals of the training and are worked out together with the participating students. The interactive and experience-oriented structure of the training enables the students to exchange and analyse intercultural experiences.

Contents of the intercultural support program *Welcome on Board*

- Reflection on one's own cultural background
- Analysis of cultural models
- Discussions about cultural differences in the university context
- Reflection on different learning cultures
- Multiperspectivity vs. the process of stereotyping