

UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SANTIAGO - CHILE



Cyber Academy: Diseño e Implementación de una Plataforma Educativa en Unity para el Fortalecimiento de Habilidades en Ciberseguridad en la Educación Media Técnica Profesional de Chile

Joel Darío Domínguez Neira

MEMORIA PARA OPTAR AL TÍTULO DE
Ingeniero Civil Informático

PROFESORA GUÍA : Berioska Contreras Vargas
PROFESOR CORREFERENTE : Pedro Godoy Barrera

Agosto 2025



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: Cyber Academy: Diseño e Implementación de una Plataforma Educativa en Unity para el

Fortalecimiento de Habilidades en Ciberseguridad en la Educación Media Técnica Profesional de Chile

Nombre del candidato(a): Joel Darío Domínguez Neira

Carrera/Grado: Ingeniería Civil Informática

Campus: San Joaquín Departamento: Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Berioska Maureen Contreras Vargas, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por (**marcar una opción**):

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 16/12/2025

Firma:

BERIOSKA
MAUREEN
CONTRERAS
VARGAS

Digitally signed by
BERIOSKA MAUREEN
CONTRERAS VARGAS
Date: 2025.12.16
20:34:01 -03'00'

Estudiante o Candidato(a):

Fecha: 16/12/2025

Firma:

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

AGRADECIMIENTOS

Primeramente, quisiera agradecer a todas las personas que me han apoyando en el transcurso de mi vida universitaria y la personal.

Quisiera agradecer a mis padres por el apoyo en todo el transcurso, brindándome un gran apoyo emocional y por darme la oportunidad de poder estudiar algo que realmente disfruto. A mi hermana Natalia, por acompañarme en todo el recorrido que ha significado esta carrera, desde sus inicios hasta su cierre.

Me gustaría agradecer en especial al sistema PACE, que desde el primer momento me brindó un espacio donde me sentí acogido, como en una segunda familia. Su apoyo fue más allá de lo académico, ayudándome también en lo personal y emocional, permitiéndome crecer y llegar hasta este punto.

También quiero agradecer a mi profesora guía, Berioska Contreras, por acogerme y brindarme de su tiempo para poder llevar a cabo esta memoria, en especial por la paciencia e interés por el proyecto, su guía contribuyó a mi aprendizaje para la consecución de mis objetivos.

Finalmente, y no por ello menos importante, agradezco con mucho cariño a mis amigos Pablo y Sebastián, así como a mis compañeros de ChibiTech, por su amistad, compañerismo y por haber formado parte esencial de esta etapa.

RESUMEN

En un contexto donde la transformación digital ha generado tanto oportunidades como amenazas, la ciberseguridad emerge como una competencia fundamental para el desarrollo social, económico y educativo. En Chile, se han impulsado avances significativos mediante instrumentos como la Ley Marco N.º 21.663 y la Política Nacional de Ciberseguridad 2023–2028. Sin embargo, aún persisten brechas importantes en la formación práctica en seguridad informática, particularmente en la educación secundaria técnico-profesional, etapa clave para la inserción temprana en el ámbito laboral. Esta memoria propone y evalúa CyberAcademy, una plataforma educativa de escritorio desarrollada con el motor de videojuegos Unity, orientada al aprendizaje práctico de ciberseguridad mediante laboratorios interactivos. La propuesta estructura los escenarios de aprendizaje en el modelo Cyber Kill Chain. A través de la simulación de amenazas como phishing, DDoS y worm, los estudiantes analizan las tácticas ofensivas para identificar las vulnerabilidades y aplicar contramedidas defensivas eficaces en cada fase.

Para evaluar su impacto, se aplicó una encuesta a 15 estudiantes de un colegio de secundaria (4to medio en Chile), cuyos resultados reflejan una percepción mayoritariamente positiva: el 74 % de los participantes consideró la interfaz clara y fácil de usar, el 67 % adquirió nuevos conocimientos y mostró interés en profundizar su formación. Por lo tanto, los laboratorios demostraron una progresión formativa medible.

Palabras Clave. ciberseguridad, metodologías de enseñanza y aprendizaje, tecnología educativa, amenazas avanzadas

ABSTRACT

At a time when digital transformation has created both opportunities and threats, cybersecurity is becoming a key skill for social, economic, and educational development. In Chile, significant progress has been made through instruments such as Framework Law No. 21,663 and the National Cybersecurity Policy 2023–2028. However, there are still significant gaps in practical training in computer security, particularly in technical and vocational secondary education, a key stage for early entry into the labor market. This memory proposes and evaluates CyberAcademy, a desktop educational platform developed with the Unity video game engine, geared toward practical cybersecurity learning through interactive labs. Through the simulation of threats such as phishing, DDoS, and worms, students analyze offensive tactics to identify vulnerabilities and apply effective defensive countermeasures at each stage.

To evaluate its impact, a survey was administered to 15 students at a secondary school (12th grade in Chile), whose results reflect a largely positive perception: 74 % of participants considered the interface clear and easy to use, 67 % acquired new knowledge and showed interest in furthering their training. Therefore, the labs demonstrated measurable educational progress.

Keywords. cybersecurity, teaching and learning methodologies, EdTech, advanced threats

ACM CCS Categories: Applied computing (Education, Interactive learning environments); Software and its engineering (Virtual worlds training simulations); Security and privacy (Denial-of-service attacks, Phishing, Malware and its mitigation).

GLOSARIO

ANCI: Agencia Nacional de Ciberseguridad.

API: Un punto de acceso al sistema o una función de biblioteca que tiene una sintaxis bien definida y es accesible desde programas de aplicación o código de usuario para proporcionar una funcionalidad bien definida.

APT: Amenaza avanzada persistente (Advanced Persistent Threat), es cuando un ciberdelincuente utiliza técnicas de hackeo continuas, clandestinas y avanzadas para acceder a un sistema y permanecer allí durante un tiempo prolongado, con consecuencias potencialmente destructivas.

AR: Siglas en inglés de Augmented Reality (Realidad Aumentada), se refiere a un tipo de simulación que implica la superposición de información digital (textos, imágenes o sonidos) en el mundo real a través de una cámara de un dispositivo.

Ciberseguridad: Se refiere a todas las tecnologías, prácticas y políticas para prevenir los ciberataques o mitigar su impacto.

Ciberdelincuente: Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante robo, filtrado de información, deterioro de software o hardware, fraude y extorsión.

CISA: Agencia de Ciberseguridad e Infraestructura Segura (Cybersecurity & Infrastructure Security Agency).

Cobit: Es los Objetivos de control para la información y tecnologías relacionadas (Control Objectives for Information and Related Technologies), es un marco de referencia de ciberseguridad para el gobierno y la gestión de las tecnologías de la información (TI) empresariales y dirigido a toda la empresa.

Cyber Range: Es un tipo de técnica que se basa en un entorno aislado, es decir, que no tiene interacciones externas y se utiliza para impartir formación práctica realista, escenarios, retos y ejercicios en un entorno web de fácil acceso.

DDoS: Es una técnica de denegación de servicio que utiliza numerosos hosts para llevar a cabo el ataque.

DNS (Domain Name System): El sistema mediante el cual se rastrean y regulan los nombres de dominio y las direcciones de Internet, según lo definido por el RFC 1034 del IETF y otros RFC relacionados.

EdTech: Es la aplicación práctica de las tecnologías de la información y comunicación (TIC), para la mejora del aprendizaje.

IP (Internet Protocol): El Protocolo de Internet, según se define en el documento RFC 6864 del IETF, es el protocolo de comunicaciones principal del conjunto de protocolos de Internet del IETF para especificar la información de direcciones del sistema al retransmitir datagramas a través de los límites de la red.

Ludificación (Gamification): Acción y efecto de aplicar técnicas o dinámicas de juego a actividades no recreativas para potenciar la motivación, la participación o facilitar el aprendizaje.

Malware: Un programa que se inserta en un sistema, normalmente de forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de la víctima, o de molestar o perturbar a la víctima de cualquier otra forma.

MITTRE ATT&CK: Es una base de conocimientos sobre tácticas y técnicas de ciberataques, basados en datos compilados reales.

NIST: Es el Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology), este es una agencia de Estados Unidos que se encarga de promover la innovación y la industria.

NNA: Niños, niñas y adolescentes.

Pentesters: Son profesionales de la seguridad expertos en el arte del hackeo ético, que consiste en utilizar herramientas y técnicas de hackeo para arreglar fallas de seguridad en lugar de causar daños.

Phishing: Es una técnica para intentar obtener datos confidenciales, como números de cuentas bancarias, mediante una solicitud fraudulenta por correo electrónico o en un sitio web, en la que el autor se hace pasar por una empresa legítima o una persona de buena reputación.

SOC: Centro de Operaciones de Seguridad (Security Operation Center), es un equipo interno o subcontratado de profesionales de seguridad de TI dedicados a monitorear toda la infraestructura de TI de una organización.

Spear Phishing: Se refiere a un término coloquial, donde se describe como cualquier ataque de phishing que está orientado a un objetivo en específico, siendo este un cargo importante en la empresa víctima.

TTP: El término tácticas, técnicas y procedimientos (Tactics, Techniques and Procedures, TTPs) se refiere al comportamiento observable de un actor (por ejemplo, un atacante). Las tácticas describen las intenciones o metas a un nivel alto; las técnicas detallan los métodos específicos utilizados para alcanzar dichas tácticas; y los procedimientos son descripciones de nivel aún más bajo que explican, paso a paso, cómo se implementa una técnica concreta en la práctica.

VR: Siglas en inglés de Virtual Reality (Realidad Virtual). Hace referencia a un entorno digital simulado que busca generar una experiencia de inmersión realista. Esto se logra mediante el uso de dispositivos especializados, como gafas o cascos de realidad virtual, que se colocan en la cabeza y proyectan el entorno virtual, acompañado de estímulos visuales y sonoros que refuerzan la sensación de presencia dentro del entorno simulado.

Worm: Un programa autorreplicante que se propaga a través de una red a otros sistemas informáticos sin necesidad de un programa anfitrión ni de la intervención del usuario para replicarse.

ÍNDICE DE CONTENIDOS

RESUMEN	II
ABSTRACT	II
GLOSARIO	III
INTRODUCCIÓN	IX
1. CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA	1
1.1. Objetivos	2
1.1.1. Objetivo General	2
1.1.2. Objetivos específicos	2
1.1.3. Árbol del problema	3
2. CAPÍTULO 2: MARCO TEÓRICO	4
2.1. Ciberseguridad	4
2.1.1. Ciberseguridad en Chile	4
2.2. Agencias de Ciberseguridad y Equipos CSIRT	6
2.2.1. INCIBE	6
2.2.2. ANCI	6
2.3. Modelos y Marcos de Referencia (frameworks) de Ciberseguridad	7
2.3.1. Lockheed Martin Cyber Kill Chain	7
2.3.2. Marco de Referencia NICE	8
2.4. Plataformas de Entrenamiento de Ciberseguridad	8
2.4.1. Hack the box	9
2.4.2. Cyberbit	9
2.4.3. RootMe	10
2.4.4. SEED Labs	10
2.5. Motores de creación de videojuegos	10
2.5.1. Unity	10
2.5.2. Unreal Engine	11
2.5.3. Godot	11
2.5.4. GameMaker	12
2.5.5. Construct	12
3. CAPÍTULO 3: PROPUESTA DE SOLUCIÓN	13
3.1. CyberAcademy	13
3.2. Experiencia de Aprendizaje: Desafío Phishing	14
3.3. Experiencia de Aprendizaje: Desafío DDoS	15
3.4. Experiencia de Aprendizaje: Desafío Gusanos	16
3.5. Método de Diseño de Laboratorios	16
3.6. Criterios de Selección y Adopción de Unity	21
3.7. Integración del modelo Cyber Kill Chain de LockHeed Martin	22
3.7.1. Phishing (Laboratorio de prevención)	22
3.7.2. DDoS (Laboratorio de detección)	25
3.7.3. Worm (Laboratorio de análisis)	26

3.8. Diseño de la encuesta	28
3.8.1. Secciones del cuestionario	28
4. CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN Y RESULTADOS	30
4.1. Alcance del Estudio de Percepción de CyberAcademy	30
4.2. Resultados del Estudio	31
4.2.1. Evaluación del perfil de los encuestados	31
4.2.2. Evaluación de los conocimientos previos de ciberseguridad	32
4.2.3. Evaluación de la usabilidad de la aplicación	32
4.2.4. Evaluación del flujo de la aplicación	33
4.2.5. Evaluación de la calidad del contenido	33
4.2.6. Evaluación del aprendizaje percibido	34
4.2.7. Evaluación de la preferencia de los laboratorios	35
4.2.8. Evaluación de datos internos de CyberAcademy	35
4.3. Análisis de Resultados	37
4.3.1. Análisis de dedicación de los estudiantes	37
4.3.2. Análisis de progreso de los estudiantes	39
4.3.3. Discusión de los resultados	40
4.3.4. Limitaciones y Oportunidades de Mejora	41
5. CAPÍTULO 5: CONCLUSIONES	42
5.1. Trabajo Futuro	42
BIBLIOGRAFÍA	45
A. ANEXOS	46
A.1. Anexo: Otras funciones de CyberAcademy	46
A.1.1. Navegación	46
A.1.2. Recursos de Ciberseguridad	47
A.1.3. Personalización	48
A.1.4. Minijuegos	50
A.2. Retroalimentación extra recibidos en la encuesta	50
A.2.1. ¿Cómo calificarías tu nivel de satisfacción general con Cyber Academy?	50
A.2.2. ¿Qué aspecto más te gusto de Cyber Academy?	50
A.2.3. ¿Qué aspectos te gustaría que se mejoraran o se agregaran en futuras versiones?	51

ÍNDICE DE FIGURAS

1.1. Árbol del problema	3
2.1. Cyber kill chain lockheed martin.	8
3.2. Retroalimentación de la aplicación	17
3.3. Página de administración del docente	17
3.4. Capturas del tutorial del laboratorio	18
3.5. Pestaña de sugerencias	18
3.6. Capturas de acciones para acceder al panel de pistas	18
3.7. Panel de salida	19
3.8. Aplicación de notas	19
3.9. Capturas de la aplicación de correo	19
3.10. Panel de tareas	20
3.11. Capturas de la aplicación de Net Tracker	20
3.12. Aplicación de consola DDoS	20
3.13. Aplicación de consola Worm	21
3.14. Panel de preguntas	21
4.1. Gráficos de los perfiles socio-demográfica de los encuestados	31
4.2. Gráfico de la percepción del nivel de conocimientos de ciberseguridad de los encuestados	31
4.3. Gráfico sobre conocimientos previos de redes en los estudiantes	32
4.4. Gráfico sobre la usabilidad de la aplicación	33
4.5. Gráfico sobre el flujo de la aplicación	33
4.6. Gráfico sobre el contenido de la aplicación	34
4.7. Gráfico sobre el aprendizaje percibido por los estudiantes	34
4.8. Gráfico de preferencia de laboratorio según los estudiantes	35
4.9. Gráficas de Tiempos medios acumulados (Dedicación) por Laboratorio	38
4.10. Gráficas de Desviación estándar (Complejidad) por Laboratorio	38
4.11. Gráfico de tiempo de finalización en segundos según el tipo de laboratorio, todos los intentos	38
4.12. Gráficos de Tiempo de finalización en segundos según el tipo de laboratorio e intento	39
4.13. Gráficas de la distribución de Frecuencias de Puntajes por Laboratorio (Radar)	40
4.14. Gráfico de Puntaje de Estudiantes por Instancia de Laboratorio	40
A.1. Parte 1: Interfaz de navegación principal en CyberAcademy.	46
A.2. Parte 2: Interfaz de navegación principal en CyberAcademy.	47
A.3. Parte 1: Recursos educativos de ciberseguridad en CyberAcademy.	47
A.4. Parte 2: Recursos educativos de ciberseguridad en CyberAcademy.	48
A.5. Menú de la tienda	48
A.6. Opciones de personalización disponibles en CyberAcademy.	49
A.7. Sección de minijuegos de CyberAcademy.	50
A.8. Gráfico de calificaciones de CyberAcademy	50

ÍNDICE DE TABLAS

3.1. Indicadores del Laboratorio de Phishing	14
3.2. Indicadores del laboratorio DDoS	15
3.3. Indicadores del laboratorio Worm	16
3.4. Comparación de motores de videojuegos: Unity, Godot, Unreal Engine y GameMaker.	22
3.5. Dimensiones y preguntas del cuestionario aplicado en CyberAcademy	29
4.1. Requisitos Mínimos CyberAcademy	30
4.2. Datos recompilados por la aplicación CyberAcademy	37

INTRODUCCIÓN

En la creciente era digital de los entornos sociales, económicos y educativos se ha transformado la manera en que las personas interactúan, aprenden y acceden a servicios. Si bien, esta transformación ofrece oportunidades sin precedentes, también ha incrementado significativamente la exposición a riesgos cibernéticos, tales como el robo de información, suplantación de identidad, ataques distribuidos de denegación de servicio (DDoS), propagación de malware, entre otros. En este contexto, la ciberseguridad se ha establecido como una disciplina esencial para proteger los activos digitales y garantizar la confianza en el uso de las tecnologías.

En Chile, la necesidad de fortalecer las capacidades nacionales en ciberseguridad ha sido reconocida a través de instrumentos como la Política Nacional de Ciberseguridad 2023–2028 y la Ley Marco N.º 21.663. Estas iniciativas han impulsado la creación de instituciones especializadas con facultades para fiscalizar, sancionar y regular a las empresas que prestan servicios esenciales en el país. En particular, la normativa establece la categoría de operadores de importancia vital, definida por la Agencia Nacional de Ciberseguridad (ANCI) (ANCI, 2025). En el documento “Primer Procedimiento de Calificación de Operadores de Importancia Vital a que se refiere la Ley N.º 21.663” (ANCI, 2023), la ANCI incluye sectores estratégicos como telecomunicaciones, banca, y servicios de generación, transmisión y distribución eléctrica, entre otros, evidenciando la amplitud y relevancia de las infraestructuras críticas que requieren especial protección. En este contexto, las herramientas emergentes orientadas a la enseñanza de la ciberseguridad cobran un alto valor estratégico frente a las exigencias del futuro mercado laboral. La demanda de competencias en esta área ha aumentado, debido al impulso de las empresas de servicios esenciales a reestructurar su infraestructura digital, para alinearse a estas normativas.

Frente a este escenario, surge CyberAcademy, una aplicación educativa de escritorio orientada a la enseñanza de ciberseguridad mediante laboratorios interactivos. Esta plataforma, desarrollada en el contexto de la Feria de Software 2024 de la Universidad Técnica Federico Santa María, tiene como objetivo proporcionar a estudiantes y docentes una herramienta pedagógica que combine aspectos técnicos con elementos lúdicos (gamification), promoviendo un aprendizaje activo centrado en el estudiante. CyberAcademy estructura sus contenidos en torno a tres pilares fundamentales: prevención, detección y análisis de ciberataques. Entre los tipos de ataques abordados se incluyen el phishing, DDoS y worms (gusanos informáticos), seleccionados por su relevancia pedagógica y su representatividad en cada fase.

En el presente documento se propone la incorporación de un modelo de ciberseguridad estructurado y validado para el desarrollo de laboratorios educativos. En particular, se plantea la utilización del modelo Cyber Kill Chain, desarrollado por Lockheed Martin, el cual conceptualiza un ciberataque como una secuencia de fases interrelacionadas. Este enfoque permite descomponer el comportamiento del atacante en pasos claramente definidos, facilitando tanto la comprensión como la simulación de escenarios reales de ataque. La elección de este modelo responde a su valor pedagógico y su aplicabilidad práctica en contextos educativos.

El objetivo de este estudio es analizar el impacto formativo que puede tener la implementación de CyberAcademy, una plataforma educativa orientada a estudiantes de educación secundaria en Chile, evaluando su potencial para desarrollar habilidades fundamentales en ciberseguridad desde una etapa temprana del proceso educativo.

Este documento se organiza de la siguiente manera. El Capítulo 1 se presenta la definición del problema de investigación, junto con los objetivos generales y específicos que guían el estudio. El Capítulo 2 desarrolla el marco teórico necesario para contextualizar el problema, abordando la situación actual de la ciberseguridad a nivel global y nacional, las instituciones responsables de su regulación y los principales marcos de referencia, con énfasis en el análisis del modelo Cyber Kill Chain como metodología seleccionada. También, se revisan las plataformas de entrenamiento en ciberseguridad disponibles en la actualidad y los motores gráficos de desarrollo, justificando la elección de Unity para la propuesta. El Capítulo 3 presenta la solución diseñada, describiendo la construcción de la aplicación, los ataques considerados para la integración de los laboratorios y su organización en función de la metodología Cyber Kill Chain. Además, se detalla el diseño de la encuesta empleada como instrumento de validación. El Capítulo 4 evalúa la aplicación de la propuesta en un liceo de educación secundaria, junto con el análisis de los resultados obtenidos. Finalmente, el Capítulo 5 recoge las conclusiones del trabajo y plantea las proyecciones para investigaciones futuras.

1 | CAPÍTULO 1: DEFINICIÓN DEL PROBLEMA

Chile ha experimentado una notable evolución en su paisaje digital, logrando altos niveles de penetración de internet (Subsecretaría de Telecomunicaciones de Chile, 2024) y posicionándose favorablemente en algunos índices de ciberseguridad a nivel gubernamental (ITU, 2024). Sin embargo, este progreso coexiste con desafíos persistentes en la alfabetización digital (BCN, 2023) y una creciente sofisticación de las amenazas cibernéticas (Al-Sada et al., 2023).

La percepción que tiene la población chilena sobre sus propias habilidades digitales es un factor clave para entender su nivel de preparación ante los desafíos del ciberespacio. Según la encuesta “Chile Nos Habla” de la Universidad San Sebastián (2024), un 34.5 % de los encuestados no sabe cómo proceder o denunciar un ciberataque, y un 53 % desconoce qué es la verificación en dos pasos. Apenas el 18.7 % de los encuestados reportó haber recibido capacitación o educación en ciberseguridad en su lugar de trabajo o estudios.

Desde el ámbito educativo, según CyberMiSTS (Cybersecurity for Middle School Teachers and Students), muchos profesores sienten que carecen de la preparación necesaria para enseñar conceptos de ciberseguridad, debido a la ausencia de recursos didácticos adecuados, currículos accesibles y formación profesional previa en el área (Buchanan et al., 2021).

Además, las barreras de infraestructura y equidad también afectan la implementación de estos contenidos. Las escuelas ubicadas en distritos pequeños, con alta vulnerabilidad o sin acceso a universidades o empresas del sector tecnológico, tienen menor probabilidad de ofrecer contenidos de ciberseguridad a sus estudiantes.

En contextos más avanzados, como lo señala el artículo sobre CyTutor, incluso al integrar tecnologías de inteligencia artificial, los docentes deben contar con conocimientos técnicos mínimos para operar, interpretar y aprovechar estas herramientas, lo que agrega otra capa de complejidad a su labor educativa (Yogarajah y Hossain, 2025).

Estas evidencias configuran un panorama preocupante en torno a la brecha formativa en ciberseguridad, lo que refuerza la urgencia de incorporar esta temática como una competencia transversal dentro del sistema educativo. Según la OEA y CISCO (2023), se estima una escasez de entre 515.000 y 701.000 profesionales calificados en ciberseguridad en América Latina y el Caribe. Esta escasez no solo refleja la falta de talento, sino también una brecha de habilidades que afecta directamente la capacidad de respuesta de las organizaciones: más del 59 % de los encuestados en estudios globales indicaron que su equipo tendría dificultades para reaccionar frente a un incidente por falta de competencias técnicas.

En este escenario, la necesidad de una formación temprana y sistemática en ciberseguridad se hace evidente. La OEA menciona como problema “el débil desarrollo de vocaciones STEM, la falta de conciencia en edades tempranas y la desconexión entre la educación y la industria” (OEA & CISCO, 2023). Por ello, la integración de contenidos de ciberseguridad en la educación secundaria, particularmente en la formación técnico-profesional, constituye una estrategia clave para preparar a los jóvenes entre 16 y 18 años frente a las demandas del mercado laboral y los riesgos del entorno digital.

Por lo tanto, para afrontar esta problemática, este trabajo propone CyberAcademy, una aplicación educativa de escritorio orientada al entrenamiento práctico en ciberseguridad, que ofrece laboratorios interactivos diseñados para simular ciberataques en entornos controlados, adaptados a las competencias del nivel técnico-profesional; El espacio de Formación Diferenciada se comprende dentro de 3° y 4° medio, este permite a los estudiantes adquirir aprendizajes en una especialidad técnica que facilite su inserción laboral y los prepare para adaptarse a los cambios tecnológicos (Ministerio de Educación de Chile, 2016). En este contexto, la implementación de una solución educativa con enfoque

práctico como CyberAcademy podría contribuir significativamente al desarrollo de habilidades técnicas y de conciencia digital en estudiantes de secundaria técnico profesional, fortaleciendo su comprensión de amenazas comunes y motivando su aprendizaje autónomo en entornos digitales seguros.

En particular, las especialidades de Conectividad y Redes, Programación y Telecomunicaciones incluyen en su currículo objetivos de aprendizaje que integran explícitamente la seguridad en las redes como parte de su formación técnica. Un ejemplo concreto es el Objetivo de Aprendizaje OA 2 para Conectividad y Redes, que establece “Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos” (Ministerio de Educación de Chile, 2015a). Este objetivo se repite también como OA 9 en la especialidad de Programación, reconociendo la necesidad de que los futuros técnicos sepan introducir un sistema operativo en una red, siempre bajo parámetros de calidad y seguridad (Ministerio de Educación de Chile, 2015b). Asimismo, aunque no se encuentra el texto literal en los resultados abiertos, el programa de Telecomunicaciones también incluye módulos relacionados con la instalación y configuración de redes y sistemas operativos en red (por ejemplo, en los módulos de "Sistemas operativos de redes") (Ministerio de Educación de Chile, 2015c). Esto sugiere que la seguridad y el cumplimiento de estándares técnicos también forman parte de los aprendizajes esperados en esta especialidad, en consonancia con las demandas del sector tecnológico.

1.1. Objetivos

1.1.1. Objetivo General

Desarrollar una solución educativa orientada al aprendizaje práctico de la ciberseguridad, dirigida a estudiantes de educación media técnico-profesional del área tecnológica, que fortalezca habilidades técnicas y conciencia digital a través de escenarios simulados de prevención, detección y análisis de amenazas comunes. Esta propuesta busca responder a los requerimientos formativos de especialidades como Telecomunicaciones, Programación y Conectividad y Redes, promoviendo el entendimiento de la seguridad en redes y dispositivos, la identificación de códigos maliciosos y la gestión segura de infraestructuras digitales, contribuyendo así a una formación pertinente y contextualizada en entornos digitales seguros.

1.1.2. Objetivos específicos

- Analizar la aplicabilidad de la metodología Cyber Kill Chain como enfoque estructurante para la enseñanza de ciberseguridad en el contexto de la educación técnico-profesional, evaluando su potencial para abordar amenazas relevantes (como phishing, DDoS y worms) desde las perspectivas formativas de las especialidades del área tecnológica.
- Diseñar laboratorios educativos interactivos que simulen escenarios de ciberataques alineados con las etapas de la Kill Chain, permitiendo el desarrollo de habilidades específicas como el análisis de tráfico de red, la identificación de código malicioso y la detección de vulnerabilidades en dispositivos, en concordancia con los aprendizajes esperados del currículo TP en sus tres especialidades.
- Implementar los laboratorios en una plataforma digital educativa (CyberAcademy), garantizando una integración didáctica que fomente la participación activa de los estudiantes, el aprendizaje significativo y el desarrollo de competencias prácticas en ciberseguridad, contextualizadas según el perfil de egreso de cada especialidad TP.
- Evaluar el impacto pedagógico y técnico de la solución propuesta, midiendo su contribución al fortalecimiento de habilidades técnicas, conciencia digital y autonomía en estudiantes de liceos técnico-profesionales, con foco en su aplicabilidad real en las trayectorias formativas de las especialidades del área tecnológica.

1.1.3. Árbol del problema

A continuación se presenta el árbol del problema, el cual contiene el problema principal, al igual que sus causas y consecuencias.

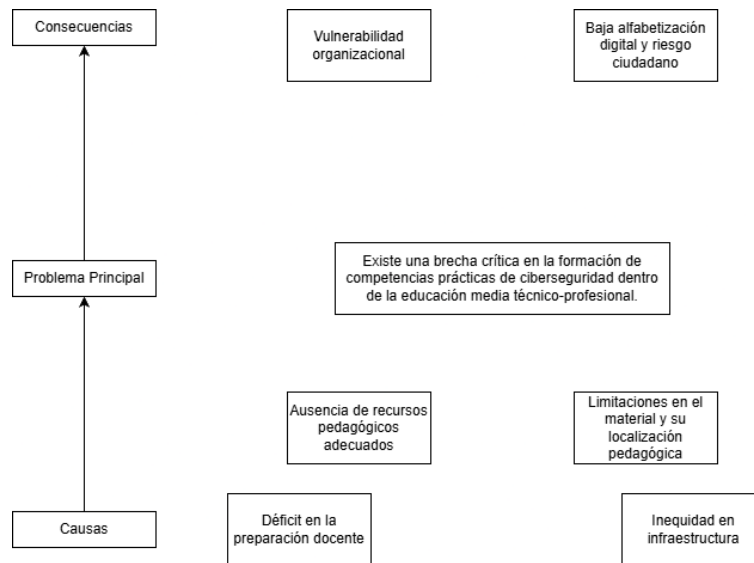


Figura 1.1: Árbol del problema

2 | CAPÍTULO 2: MARCO TEÓRICO

En este capítulo se presentan los pilares teóricos y técnicos de la investigación. Se aborda la ciberseguridad desde su espectro internacional hasta su aplicación en Chile, revisando el rol de las agencias y equipos de respuesta (CSIRT), con el objetivo de dimensionar la brecha local y comprender el ecosistema institucional en el que se inserta el proyecto. Asimismo, se integran los modelos de referencia esenciales para la defensa y las competencias laborales, necesarios para asegurar que los contenidos pedagógicos estén alineados con los estándares de la industria, junto con un estudio de las herramientas de entrenamiento vigentes que permite detectar las carencias actuales en accesibilidad educativa. Finalmente, se incluye una evaluación de los motores gráficos disponibles, cuya selección resulta crítica para viabilizar técnicamente la interactividad y la experiencia de usuario de la solución propuesta.

2.1. Ciberseguridad

La ciberseguridad se ha posicionado como un componente crítico para la estabilidad de las sociedades digitales contemporáneas, definiéndose como el conjunto de tecnologías, prácticas y políticas destinadas a prevenir o mitigar el impacto de los ciberataques (IBM, 2025). Sin embargo, la propia evolución tecnológica; Caracterizada por la creciente interdependencia de sistemas, la expansión de la nube, el Internet de las Cosas y la inteligencia artificial, ha incrementado sustancialmente la complejidad estructural de los entornos digitales. Como advierte Schneier y Vance (2025), “la complejidad es el peor enemigo de la seguridad”, ya que un sistema complejo amplía la superficie de ataque, dificulta la identificación de vulnerabilidades y multiplica los puntos de fallo. Esta complejidad, presente tanto en software como en estructuras organizacionales, no solo introduce nuevos riesgos, sino que transforma cualitativamente la naturaleza de las amenazas, haciendo que la protección de la integridad de los sistemas y los datos sea un desafío continuo y creciente.

La creciente dependencia de los entornos digitales conlleva implicaciones económicas sustanciales. A nivel global, los daños económicos derivados de ciberataques pueden superar el 1 % del Producto Interno Bruto (PIB) en algunos países, y hasta un 6 % del PIB cuando se dirigen a infraestructuras críticas (Banco Interamericano de Desarrollo et al., 2020). El Foro Económico Mundial, en su Global Cybersecurity Outlook 2025, reporta que el 72 % de las organizaciones han experimentado un aumento en los riesgos cibernéticos, siendo el ransomware una de las principales preocupaciones (World Economic Forum, 2025).

2.1.1. Ciberseguridad en Chile

En Chile, al igual que en otras partes del mundo, existe una importante brecha en la formación práctica en ciberseguridad, especialmente en el ámbito educativo. En los liceos técnico profesional, la demanda por programas de formación en ciberseguridad han ido en aumento en los últimos años respondiendo a una brecha de capital humano estimada en miles de especialistas anuales (Talento Digital para Chile, 2022), en un contexto donde estudiantes de entre 12 y 19 años se pueden ver obligados a enfrentar un futuro entorno laboral cada vez más competitivo, con mayores exigencias en términos de conocimientos técnicos y habilidades prácticas.

En respuesta al creciente panorama de amenazas digitales, Chile ha adoptado medidas significativas para fortalecer su ciberseguridad.

La Política Nacional de Ciberseguridad 2023–2028, aprobada mediante el Decreto N.º 164 y publicada en el Diario Oficial el 4 de diciembre de 2023, establece un marco estratégico para proteger la infraestructura crítica, garantizar los derechos de las personas en el ciberespacio y fomentar una cultura de ciberseguridad a nivel nacional (Ministerio del Interior y Seguridad Pública, 2023). Esta Política se estructura en torno a cinco objetivos:

- **Infraestructura Resiliente:** Se basa en fortalecer la infraestructura de la información para resistir y recuperarse de incidentes de ciberseguridad y desastres socioambientales.
- **Derechos de las Personas:** Se refiere a promover y proteger los derechos de las personas en el ciberespacio, asegurando su seguridad y privacidad.
- **Cultura de Ciberseguridad:** Se busca fomentar una cultura de conciencia y responsabilidad en el uso de tecnologías digitales, promoviendo la educación en ciberseguridad desde etapas tempranas.
- **Coordinación Nacional e Internacional:** Se refiere a establecer una gobernanza efectiva que coordine acciones en ciberseguridad a nivel nacional e internacional, promoviendo la cooperación entre sectores públicos y privados.
- **Fomento a la Industria y la Investigación Científica:** Se busca impulsar el desarrollo de la industria de la ciberseguridad y la investigación científica aplicada, fortaleciendo las capacidades nacionales en este ámbito.

Complementando esta política, el 8 de abril de 2024 se promulgó la Ley N.º 21.663: Ley Marco de Ciberseguridad, que establece la institucionalidad, los principios y la normativa general para estructurar, regular y coordinar las acciones de ciberseguridad de los organismos del Estado y entre éstos y los particulares (República de Chile, 2024). La Ley Marco de Ciberseguridad introduce elementos esenciales para la protección del ciberespacio en Chile:

- **Creación de la Agencia Nacional de Ciberseguridad (ANCI):** Establece un organismo autónomo encargado de regular, supervisar y coordinar todas las actividades relacionadas con la ciberseguridad en el país.
- **Definición de Infraestructuras Críticas de la Información (ICI):** Identifica sectores estratégicos que deben implementar medidas de protección obligatorias, con controles de acceso, monitoreo de seguridad y planes de respuesta ante incidentes.
- **Obligaciones para los Operadores de Importancia Vital (OIV):** Establece deberes específicos y el deber de reportar los ciberataques e incidentes que puedan tener impactos significativos, siendo aplicable tanto para los servicios esenciales como para los OIV.
- **Implementación de Normas y Estándares Internacionales:** La ley se alinea con estándares internacionales como ISO/IEC 27001 y marcos de referencia como NIST, obligando a empresas de sectores estratégicos a reforzar sus medidas de protección digital.
- **Establecimiento de Sanciones:** Define un sistema de infracciones y sanciones para garantizar el cumplimiento de las disposiciones en materia de ciberseguridad.

Chile ha logrado posicionarse en el puesto 24 de un total de 175 países evaluados en el National Cyber Security Index (NCSI), un indicador de carácter internacional que mide la capacidad de los Estados para prevenir amenazas cibernéticas, gestionar incidentes de seguridad y desarrollar una infraestructura digital resiliente, según el reporte actualizado el 30 de septiembre de 2025 (e-Governance Academy Foundation, 2025). Sin embargo, esta posición contrasta con el resultado obtenido en el Global Cybersecurity Index (GCI) de la International Telecommunication Union (ITU), donde Chile ocupa el lugar 98 entre 182 países a nivel global. A diferencia del NCSI, el GCI considera un espectro más amplio de dimensiones, incluyendo aspectos legales, técnicos, organizacionales, de desarrollo de capacidades y de cooperación internacional. Esto sugiere que, si bien Chile ha mostrado avances en la formalización de su postura de ciberseguridad. Por ejemplo, a través de la promulgación de nuevas leyes y la creación de la Agencia Nacional de Ciberseguridad (ANCI), persisten desafíos en la implementación práctica, el fortalecimiento de capacidades técnicas de manera generalizada y la articulación efectiva entre actores clave como el sector público, privado, la academia y la sociedad civil (ITU, 2024).

En el área de la formación técnico-profesional, se han actualizado las bases curriculares para incorporar de forma explícita competencias en ciberseguridad, especialmente en especialidades vinculadas al área tecnológica. Las carreras de Conectividad y Redes, Programación y Telecomunicaciones incluyen módulos que abordan la configuración segura de redes, el uso de software responsable para proteger los sistemas, y la comprensión de amenazas comunes en entornos digitales (Ministerio de Educación de Chile, 2016).

El estudio “Kids Online Chile 2022”, que encuestó a 3011 estudiantes desde 4° básico hasta 3° medio, ofrece una visión detallada de las habilidades digitales y la conciencia de riesgos de los NNA en Chile (UNICEF Chile y Universidad de Chile, 2022). En cuanto a la autopercepción de habilidades digitales, los NNA muestran una alta confianza en tareas técnicas básicas: el 71 % se siente “totalmente capaz” de instalar aplicaciones en un celular o tableta, el 57 % de reportar o bloquear a alguien en redes sociales, y el 53 % de reconocer qué información deben evitar compartir en internet. El 50 % sabe cómo configurar su perfil como privado. Sin embargo, esta competencia técnica no se traduce en habilidades de evaluación crítica: solo el 32 % se siente “totalmente capaz” de confirmar la veracidad de la información en línea, y el 41 % de determinar si una fuente en línea es confiable.

También se han implementado planes de capacitación digital, como la entregada por el “Plan Ciudadanía y Alfabetización Digital 2025” (Ministerio Secretaría General de Gobierno (SEGEOB) y Ministerio de Educación (MINEDUC), 2024), busca fortalecer la alfabetización digital e incorporar la alfabetización mediática y la ciudadanía digital en el currículo escolar nacional. Este plan incluye una “Ruta de Alfabetización Digital” con recursos para estudiantes de 1° a 7° básico.

Por ello, resulta necesario contar con herramientas didácticas que faciliten la comprensión y el aprendizaje de los estudiantes, promoviendo una enseñanza accesible, contextualizada y alineada con los desafíos actuales del entorno digital a nivel global y nacional. En particular, se requiere de recursos educativos interactivos, que no solo transmitan contenidos teóricos, sino que además fomenten el desarrollo de habilidades prácticas en un entorno controlado y seguro.

2.2. Agencias de Ciberseguridad y Equipos CSIRT

A nivel global, se han fortalecido las estructuras dedicadas a la protección del ciberespacio mediante la creación de agencias de ciberseguridad y equipos especializados en la gestión de incidentes, comúnmente conocidos como CSIRT (Computer Security Incident Response Team) o CERT (Computer Emergency Response Team). Estos organismos desempeñan funciones clave en la detección, mitigación, coordinación y resolución de ataques cibernéticos, colaborando estrechamente con actores tanto públicos como privados para fortalecer la ciberresiliencia nacional e internacional.

2.2.1. INCIBE

El Instituto Nacional de Ciberseguridad (INCIBE), es un organismo dependiente del Ministerio de Asuntos Económicos y Transformación Digital de España, desempeña un papel fundamental en la promoción de la cultura de la ciberseguridad y en la capacitación de profesionales en este ámbito. A través de diversas iniciativas, INCIBE ofrece recursos y programas formativos adaptados a diferentes perfiles y necesidades.

2.2.2. ANCI

La Agencia Nacional de Ciberseguridad (ANCI) es un organismo creado a partir de la promulgación de la Ley Marco de Ciberseguridad (Ley N.º 21.663). Esta agencia forma parte de la Estrategia de Seguridad del Gobierno de Chile y se alinea con los ejes fundamentales de dicha estrategia, como el fortalecimiento institucional, la lucha contra el crimen organizado —particularmente en lo relativo a los ciberdelitos— y la promoción de acuerdos de Estado en materia de seguridad.

Entre sus principales funciones se encuentran la fiscalización, regulación y sanción de las instituciones que prestan servicios esenciales, tanto públicas como privadas, en lo que respecta a su cumplimiento de las normativas de ciberseguridad. Estas instituciones incluyen sectores estratégicos como la banca, la salud, las telecomunicaciones, entre otros.

2.3. Modelos y Marcos de Referencia (frameworks) de Ciberseguridad

Los marcos de referencia (frameworks), se refiere al conjunto estructurado de las buenas practicas, estándares y guías diseñadas para ayudar al manejo de riesgos de ciberseguridad a las organizaciones (Kidd, 2024).

Los marcos de referencia permiten a las organizaciones establecer políticas coherentes de seguridad, definir responsabilidades claras, evaluar su nivel de madurez en materia de protección digital, y cumplir con regulaciones legales y normativas del sector. Entre los marcos de referencia más utilizados se encuentran NIST, MITRE ATT&CK y Cobit. También, existen normativas y certificaciones como la ISO/IEC 27.001, que son requisitos para implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI). Además, facilitan la toma de decisiones estratégicas en entornos digitales cada vez más complejos y dinámicos, contribuyendo a una postura de seguridad más proactiva y resiliente.

2.3.1. Lockheed Martin Cyber Kill Chain

El modelo Lockheed Martin Cyber Kill Chain, desarrollado por la corporación Lockheed Martin dentro del contexto de seguridad cibernética, es una metodología estructurada para comprender y frenar ataques cibernéticos mediante la identificación y análisis de cada una de las fases que un atacante debe ejecutar para alcanzar su objetivo. Esta metodología es especialmente eficaz para enfrentar amenazas persistentes avanzadas (APT, por sus siglas en inglés), caracterizadas por su nivel de complejidad, persistencia y enfoque estratégico en la obtención de información sensible o el nivel de daño a infraestructuras críticas (Hutchins et al., 2011).

La Cyber Kill Chain se compone de siete fases secuenciales. Como se puede observar en la figura 2.1. Cada una de ellas representa un punto crítico donde es posible aplicar medidas defensivas para detectar, interrumpir o mitigar el avance del ataque:

1. **Reconocimiento (Reconnaissance):** En esta primera fase, el atacante lleva a cabo la recopilación de información sobre el objetivo. Esta información puede incluir direcciones de correo electrónico, infraestructura tecnológica o relaciones sociales. Esta fase es primordial para seleccionar posibles objetivos vulnerables.
2. **Instrumentalización (Weaponization):** Una vez reunida la información, el atacante construye el “arma” que utilizará para comprometer al objetivo. Esto generalmente implica la combinación de código malicioso (como los virus troyanos) con implantaciones de código que explotan vulnerabilidades. Normalmente, se utilizan documentos aparentemente legítimos como archivos PDF o archivos de Microsoft Office.
3. **Entrega (Delivery):** Esta fase corresponde la transmisión del código implantado (payload) al entorno objetivo. Los vectores más comunes incluyen correos electrónicos (phishing), sitios web maliciosos y dispositivos USB comprometidos.
4. **Explotación (Exploitation):** En esta etapa, se activa el código malicioso al explotar una vulnerabilidad en el software del usuario o incluso mediante la manipulación del comportamiento del usuario.
5. **Instalación (Installation):** Tras la explotación exitosa, se continua con la instalación de herramientas que permitan al atacante mantener el acceso al sistema. Esto se logra comúnmente mediante puertas traseras o troyanos, los cuales establecen una presencia persistente en el dispositivo vulnerado.
6. **Comando y Control (C2) (Command and Control):** El atacante establece un canal de comunicación entre el sistema comprometido y su servidor, lo que le permite controlar de manera remota al sistema de la víctima.
7. **Acciones sobre los Objetivos (Actions on Objectives):** Finalmente, el atacante ejecuta sus objetivos específicos, los cuales pueden incluir la exfiltración de datos sensibles, sabotaje de sistemas, modificación de información o desplazamiento lateral dentro de la red para comprometer otros dispositivos.

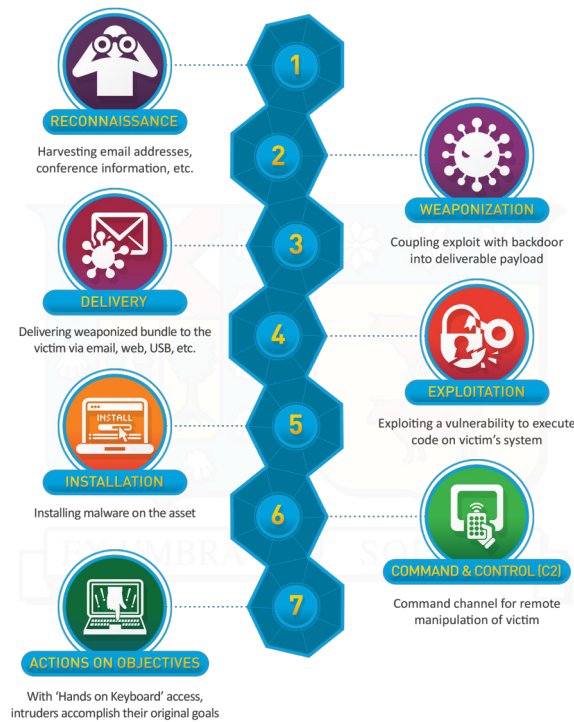


Figura 2.1: Cyber kill chain lockheed martin.

Fuente: [cyber-kill-chain](#)

En este contexto, el modelo Cyber Kill Chain facilita la asociación directa con vectores de ataque específicos, como el phishing, los ataques DDoS y los worms, los cuales han sido seleccionados por su representatividad y relevancia educativa en cada etapa. Esta correspondencia no solo permite estructurar los laboratorios de forma coherente, sino que también ofrece una base sólida para el diseño de nuevos escenarios formativos, alineados con la metodología del modelo y los objetivos de aprendizaje propuestos.

2.3.2. Marco de Referencia NICE

Otro marco de referencia relevante en el ámbito de la ciberseguridad es el NICE Framework (National Initiative for Cybersecurity Education Workforce Framework), promovido por el Instituto Nacional de Estándares y Tecnología (NIST) y gestionado por la CISA. Este estándar “proporciona un lenguaje común para describir el trabajo en ciberseguridad y las competencias necesarias para realizarlo” (National Initiative for Cybersecurity Education (NICE), 2025).

El NICE define tres dimensiones clave de un rol profesional: Tasks (tareas), Knowledge (conocimientos) y Skills (habilidades), o TKS, que se agrupan en Roles de trabajo y Áreas de competencia. Esta estructura permite una interpretación estructurada del trabajo, señalando claramente qué debe saber y poder hacer una persona para desempeñar labores específicas en el ámbito cibernético.

2.4. Plataformas de Entrenamiento de Ciberseguridad

Los campos de entrenamiento en ciberseguridad (Cyber Range) constituyen entornos de simulación seguros diseñados para que los usuarios puedan participar en ejercicios, desafíos y escenarios realistas orientados al desarrollo de habilidades prácticas en el ámbito de la ciberseguridad. Estos espacios reproducen situaciones de ataque, defensa o ambas en un entorno controlado, permitiendo el aprendizaje práctico sin riesgo para sistemas reales. Generalmente, los campos de

entrenamiento en ciberseguridad se implementan de manera online, a través de plataformas web de fácil acceso que integran laboratorios interactivos, métricas de desempeño y retroalimentación inmediata.

De acuerdo con el informe “The Forrester Wave™: Cybersecurity Skills and Training Platforms, Q4 2023” (Burn, 2023), las plataformas de entrenamiento en ciberseguridad deben satisfacer tres criterios fundamentales:

1. **Capacitación basada en roles:** proporcionando contenidos alineados con perfiles como analistas SOC, pentesters, arquitectos de seguridad, entre otros.
2. **Entrenamiento inmersivo:** uso de laboratorios prácticos, simulaciones realistas, escenarios tipo ataque/defensa y ejercicios de respuesta a incidentes.
3. **Medición del rendimiento:** mediante el uso de dashboards, rúbricas y métricas asociadas a la mejora de habilidades y reducción del riesgo humano.

Actualmente, existen diversos enfoques y metodologías para la enseñanza práctica de la ciberseguridad. Uno de los más conocidos es el formato captura la bandera (Capture The Flag, CTF), que consiste en simular escenarios de hacking ético en los que los participantes deben acceder a sistemas vulnerables y recuperar archivos o claves ocultas, completando así los desafíos propuestos.

Otro enfoque ampliamente utilizado es el de Red Team vs. Blue Team, en el que se enfrentan dos equipos: uno encargado de simular ataques (red team) y otro responsable de la defensa y mitigación (blue team), promoviendo la experiencia en situaciones reales de ataque y respuesta. También existen laboratorios centrados en el refuerzo conceptual, que mediante cuestionarios, simulaciones o ejercicios guiados, buscan evaluar y consolidar los conocimientos teóricos adquiridos.

Dada la variedad de metodologías disponibles, resulta fundamental analizar las plataformas actuales y sus enfoques pedagógicos.

2.4.1. Hack the box

Hack The Box, fundada en 2017 con sede en Reino Unido, es una plataforma en línea que ofrece un entorno interactivo para el desarrollo de habilidades en ciberseguridad. A través de laboratorios virtuales y desafíos realistas, los usuarios pueden practicar técnicas de hacking ético, pruebas de captura la bandera (CTF), pruebas de penetración y análisis forense digital (Hack The Box, 2025).

La plataforma se estructura en diferentes modos de aprendizaje:

- **Máquinas:** Entornos virtuales que simulan sistemas operativos con vulnerabilidades específicas para ser explotadas.
- **Desafíos:** Ejercicios enfocados en áreas particulares como criptografía, ingeniería inversa y seguridad web.
- **Academia HTB:** Cursos estructurados que combinan teoría y práctica, diseñados para guiar a los usuarios desde niveles básicos hasta avanzados.

2.4.2. Cyberbit

La plataforma Estado Unidense Cyberbit se posiciona como líder en capacitación en ciberseguridad, ofrecida en tres segmentos: empresa, gobierno y educación superior. Basada en el análisis de Forrester (Burn, 2023), Cyberbit ofrece una combinación robusta de cursos, laboratorios y “live-fire” (fuego real) de simulador de ciberseguridad (Cyber Range), incluyendo simulaciones personalizables. Estas simulaciones permiten que los directivos “observen a los profesionales en tiempo real e introduzcan retos adicionales durante el evento”, lo que refuerza la experiencia de respuesta bajo presión.

En una de sus innovaciones más destacadas, Cyberbit incluye una simulación de crisis que transmite información en tiempo real desde el SOC hasta los ejecutivos, fomentando la colaboración interfuncional y la toma de decisiones en condiciones de alta tensión.

La plataforma también proporciona informes avanzados y dashboards multinivel que utilizan mapas de calor intuitivos para análisis de rendimiento. Estos están alineados con estándares internacionales, incluyendo MITRE ATT&CK® y NIST NICE, facilitando a los equipos medir y demostrar su dominio de habilidades según marcos reconocidos.

2.4.3. RootMe

RootMe es una plataforma de origen francés, que su objetivo es el entrenamiento en ciberseguridad comunitaria y sin ánimo de lucro, con accesibilidad para múltiples idiomas incluyendo hispanohablantes. Permite a los usuarios practicar técnicas de hacking ético a través de más de 500 retos y 178 entornos virtuales, con contenido categorizado por áreas como web, red, forense, criptografía y programación (Root-Me, [s.f.](#)).

La plataforma ofrece cuentas gratuitas, además de una versión RootMe PRO dirigida a instituciones educativas y empresas (Root-Me Pro, [s.f.](#)), que incluye:

- Laboratorios y entornos virtuales bajo demanda.
- Supervisión de progreso del usuario.
- Organización de eventos tipo CTF (Jeopardy y Attack-Defense) para prácticas grupales

2.4.4. SEED Labs

SEED Labs (Security Education) fue fundada en 2002, con origen Estado Unidense, es una plataforma en línea con el objetivo de proporcionar laboratorios prácticos mediante máquinas virtuales para la enseñanza de la seguridad informática (Du, [2025](#)).

Los ejercicios se categorizan en tres tipos principales:

- **Laboratorios de Ataque:** Permiten a los estudiantes explorar y ejecutar ataques informáticos conocidos.
- **Laboratorios de Exploración:** Enfocados en el análisis y comprensión de mecanismos de seguridad.
- **Laboratorios de Diseño e Implementación:** Orientados a la creación y evaluación de soluciones de seguridad.

2.5. Motores de creación de videojuegos

Tras revisar las diversas plataformas de entrenamiento existentes, se observa que la tendencia hacia la gamificación y la simulación práctica requiere de tecnologías capaces de soportar entornos visuales interactivos y dinámicos. Para la construcción de este tipo de software, que busca traducir conceptos técnicos abstractos en experiencias gráficas tangibles, es necesario recurrir a los Motores de Videojuegos (Game Engines).

Tal como lo define Gregory ([2018](#)), un motor de videojuegos es un sistema de software complejo y extensible diseñado para la creación y desarrollo de videojuegos, que proporciona una arquitectura subyacente con componentes reutilizables para gestionar aspectos críticos como el renderizado de gráficos, la simulación de leyes físicas, el sistema de audio y la lógica de programación (scripting). Esta abstracción permite separar la tecnología central (el motor) de los activos y reglas específicas de cada juego (el contenido), facilitando así el prototipado y despliegue eficiente de simulaciones interactivas sin la necesidad de construir el software desde cero para cada nueva aplicación. A continuación, se describen los motores más utilizados en la industria actual, analizando sus características técnicas y su aplicabilidad en el desarrollo de entornos digitales.

2.5.1. Unity

Unity, desarrollado por la empresa Unity Technologies y lanzado oficialmente en 2005 en San Francisco, Estados Unidos (Unity Technologies, [2025](#)), es un motor de desarrollo de aplicaciones interactivas y videojuegos multiplataforma. Su

diseño se orienta a la accesibilidad, la escalabilidad y la flexibilidad, permitiendo crear entornos tridimensionales y bidimensionales tanto para computadores personales como para dispositivos móviles, consolas y experiencias inmersivas de realidad aumentada (AR) y realidad virtual (VR).

El entorno de Unity se compone de un editor visual y un motor de renderizado en tiempo real, que emplea el lenguaje de programación C# para la creación y ejecución de scripts para comportamientos personalizados. Además, incorpora un sistema de administración de recursos denominado “Unity Asset Store”, una biblioteca digital que distribuye modelos, texturas, sonidos y complementos desarrollados por la comunidad o por terceros, facilitando la integración y reutilización de componentes.

Entre sus herramientas complementarias, Unity integra un sistema de control de versiones denominado “Unity Version Control”, perteneciente a la suite de servicios en la nube de la plataforma, que permite la colaboración entre desarrolladores y el seguimiento del ciclo de vida del proyecto de manera similar a herramientas como Git. Asimismo, ofrece funciones de automatización, compilación remota y despliegue multiplataforma mediante “Unity Cloud Build”.

Por su enfoque modular y su ecosistema educativo, Unity ha sido ampliamente adoptado en contextos académicos y de investigación. La plataforma cuenta con programas de apoyo a instituciones educativas, recursos formativos gratuitos y una comunidad internacional activa que promueve la innovación abierta en el ámbito de la simulación interactiva y el aprendizaje basado en proyectos.

2.5.2. Unreal Engine

Desarrollado por la empresa Epic Games y lanzado en 1998 en Carolina del Norte, Estados Unidos (Epic Games, 2025), Unreal Engine es un motor de desarrollo interactivo orientado a la creación de entornos tridimensionales de alta fidelidad visual. Su diseño destaca por la potencia gráfica y la capacidad de producir experiencias inmersivas con un alto nivel de detalle, ampliamente utilizadas en videojuegos, cine digital, visualización arquitectónica y simulaciones.

Una de sus principales características es el sistema “Blueprints”, que permite la programación visual mediante diagramas lógicos sin necesidad de escribir código, facilitando la creación de prototipos complejos. Además, incorpora tecnologías avanzadas como “Nanite” (para renderizado de geometría de alta densidad) y “Lumen” (para iluminación global dinámica), que optimizan el rendimiento gráfico en tiempo real. Otros componentes, como “Metahuman Creator”, posibilitan la generación realista de personajes digitales para entornos interactivos o cinematográficos.

Unreal Engine opera bajo un modelo de licencia gratuito con regalías del 5 % aplicables únicamente a proyectos comerciales que superen un millón de dólares en ingresos. La plataforma cuenta con un amplio ecosistema de apoyo conformado por el “Unreal Marketplace”, foros oficiales, documentación técnica y programas de formación para profesionales y académicos. En contextos educativos, Unreal se valora por su potencia visual y su utilidad en la enseñanza de conceptos de programación visual, diseño interactivo y modelado tridimensional avanzado.

2.5.3. Godot

Godot es un motor de desarrollo de videojuegos y simulaciones de código abierto, creado originalmente por el equipo OKAM en 2014 y actualmente gestionado por la Godot Foundation (Godot Engine Community, 2025). Su principal característica es su arquitectura modular y su compromiso con la filosofía de software libre, que permite a los desarrolladores acceder, modificar y redistribuir el código fuente sin restricciones de licencia.

Godot utiliza un lenguaje de programación propio denominado “GDScript”, diseñado para ser sintéticamente similar a Python, aunque también admite otros lenguajes como C# y C++. El entorno de desarrollo integra herramientas para diseño visual, animación, físicas y scripting, optimizadas tanto para entornos 2D como 3D ligeros. Su estructura jerárquica basada en nodos y escenas facilita la organización lógica de proyectos y promueve una curva de aprendizaje progresiva.

Gracias a su enfoque educativo y su comunidad colaborativa, Godot se ha consolidado como una alternativa accesible para la enseñanza de programación y diseño de videojuegos. La comunidad mantiene una extensa documentación, foros activos, y una biblioteca abierta de recursos digitales que favorecen la experimentación y la innovación pedagógica.

2.5.4. GameMaker

GameMaker, desarrollado originalmente por Mark Overmars en 1999 en los Países Bajos y actualmente administrado por la empresa Opera (YoYo Games, [2025](#)), es un motor de desarrollo especializado en la creación de videojuegos 2D mediante un entorno visual de programación simplificada. Su diseño se orienta a la accesibilidad y a la reducción de la complejidad técnica, lo que lo convierte en una opción idónea para la enseñanza de fundamentos de diseño interactivo y desarrollo de prototipos.

El motor emplea el “GameMaker Language” (GML), un lenguaje de scripting propio que combina programación visual y textual, permitiendo crear comportamientos interactivos sin requerir conocimientos avanzados de código. GameMaker incluye herramientas integradas para diseño de niveles, animaciones, gestión de colisiones y efectos visuales, además de la posibilidad de exportar proyectos a múltiples plataformas como Windows, macOS, Android y HTML5.

La plataforma mantiene un modelo de uso mixto (gratuito y de pago) y ofrece recursos complementarios a través del “GameMaker Marketplace”, donde los desarrolladores pueden acceder a bibliotecas, plantillas y extensiones creadas por la comunidad. En entornos educativos, GameMaker se emplea como un recurso didáctico para enseñar pensamiento lógico, diseño interactivo y nociones básicas de programación.

2.5.5. Construct

Construct, creado por la empresa Scirra Ltd. en 2007 en Londres, Reino Unido (Scirra Ltd, [2025](#)), es un motor especializado en el desarrollo de aplicaciones y videojuegos 2D mediante un enfoque visual basado en eventos. Su diseño elimina la necesidad de conocimientos avanzados de programación, permitiendo que los usuarios construyan dinámicas de juego mediante una interfaz gráfica intuitiva.

El sistema de eventos y acciones constituye el núcleo de Construct: cada elemento del juego responde a condiciones predefinidas que pueden combinarse para generar interacciones complejas. Esta característica lo convierte en una herramienta ideal para la enseñanza de pensamiento lógico, el prototipado rápido y la creación de experiencias educativas interactivas.

Construct permite exportar proyectos a múltiples plataformas, incluyendo sistemas operativos de escritorio, dispositivos móviles y navegadores web mediante soporte nativo para HTML5. Además, cuenta con una biblioteca de recursos predefinidos, un mercado digital de plantillas y una comunidad activa que promueve la colaboración y el aprendizaje entre usuarios de distintos niveles.

En contextos educativos, Construct destaca por su potencial para introducir conceptos de diseño de sistemas, interactividad y programación visual, sin requerir experiencia previa en desarrollo de software. Por su bajo umbral de entrada y enfoque didáctico, se consolida como una alternativa pedagógica eficiente para proyectos de enseñanza creativa y simulación interactiva.

3 | CAPÍTULO 3: PROPUESTA DE SOLUCIÓN

En este capítulo se presenta la propuesta de solución diseñada para mitigar la brecha crítica en la formación de competencias prácticas de ciberseguridad que afecta a la educación media técnico-profesional. Se aborda el desarrollo e implementación de CyberAcademy como respuesta a la necesidad de herramientas educativas accesibles y contextualizadas. Asimismo, se detalla la aplicación del modelo Cyber Kill Chain de Lockheed Martin como la metodología central para estructurar y organizar los escenarios de entrenamiento que conforman la aplicación.

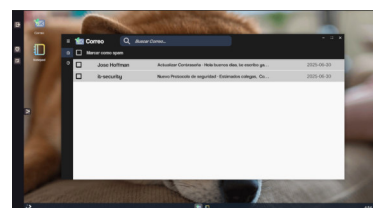
3.1. CyberAcademy

CyberAcademy ¹ es una aplicación de escritorio diseñada para proporcionar laboratorios interactivos y lúdicos. Este proyecto fue presentado dentro del marco de la Feria de Software del año 2024 ² de la Universidad Técnica Federico Santa María, realizado por un grupo de seis estudiantes de Ingeniería Civil Informática.

Esta aplicación, además de crear conciencia sobre ciberseguridad, está diseñada para ser inclusiva dados los distintos estilos de aprendizaje de los estudiantes, ya que proporciona retroalimentación continua y personalizada tras cada intento gracias a la incorporación de instancias dinámicas que se ajustan al nivel de cada usuario, lo que permite reforzar continuamente los conocimientos adquiridos. Además, el sistema trabaja de manera contenida, donde cada laboratorio es una instancia controlada, ofreciendo un control más estricto y seguro en comparación con otras soluciones que pueden ser más vulnerables a riesgos externos, como pueden ser las máquinas virtuales infectadas (Abusaimeh, 2020).



(a) Inicio de CyberAcademy



(b) Laboratorio Phishing de CyberAcademy

CyberAcademy se apoya en tres ejes funcionales:

- **Prevención:** orientado a que los estudiantes desarrollen capacidades analíticas para anticipar ciberataques mediante la identificación de vulnerabilidades.
- **Detección:** enfocado en la formación de habilidades para reconocer patrones maliciosos y señales de ataque en tiempo real.
- **Análisis:** dirigido a la comprensión de la causa del ataque, explorando su comportamiento, impacto y respuesta.

Dado lo anterior, se seleccionaron como ataques representativos para el diseño de los laboratorios los vectores de Phishing, DDoS y Worm, los cuales se alinean con los enfoques de prevención, detección y análisis, respectivamente.

¹CyberAcademy: chibitech.itch.io/cyberacademy

²Feria de software: www.feriadesoftware.cl

3.2. Experiencia de Aprendizaje: Desafío Phishing

El phishing es una técnica de ataque que combina principios de ingeniería social con vulnerabilidades técnicas, con el objetivo de engañar a la víctima para que entregue información confidencial o realice una acción perjudicial (Hajgude y Ragha, 2012). Este tipo de ataque suele ejecutarse a través de correos electrónicos fraudulentos, en los que el atacante suplanta la identidad de entidades legítimas —como instituciones bancarias, empresas tecnológicas o contactos cercanos a la víctima— para generar un falso sentido de urgencia o confianza.

Según Hajgude y Ragha (2012), los correos de phishing generalmente contienen enlaces a sitios falsificados que imitan el aspecto visual de sitios legítimos y utilizan técnicas como la manipulación de enlaces (link spoofing), análisis léxico de URLs y expresiones comunes (e.g. “verifica tu cuenta”, “seguridad”) para engañar al usuario. En muchos casos, se persigue el robo de credenciales o la instalación de malware mediante archivos adjuntos o sitios fraudulentos. La clasificación de estos correos requiere el análisis combinado del contenido textual, la estructura del correo y las propiedades de los enlaces incluidos.

El laboratorio de phishing en CyberAcademy simula un entorno de correo corporativo donde los estudiantes deben analizar mensajes sospechosos. La experiencia se estructura en torno a componentes pedagógicos y técnicos claramente definidos que permiten evaluar el desempeño de manera integral:

Indicador	Descripción
Acción	Seleccionar si un correo es legítimo o sospechoso; abrir, reportar o buscar un correo.
Puntos	El sistema asigna puntaje en función de la precisión de las decisiones: +1 puntos por identificar correctamente un correo de phishing y 0 punto en caso de clasificar erróneamente un correo legítimo como malicioso.
Intentos	En cada interacción los correos presentados varían, de modo que el estudiante no enfrenta siempre los mismos escenarios, favoreciendo así la diversidad de la práctica.
Tiempo	No se establece un límite para responder, pero el tiempo de resolución se registra como parámetro de retroalimentación y análisis del desempeño.
Retroalimentación	Explicación inmediata de los elementos que evidencian el fraude (dominio sospechoso, errores gramaticales, metadatos).
Historial	Registro de decisiones por jugador, que permite evaluar progresión y errores frecuentes.

Tabla 3.1: Indicadores del Laboratorio de Phishing

El ataque de phishing fue seleccionado como representativo para los laboratorios orientados al enfoque de prevención, debido a su carácter formativo en torno a la ingeniería social aplicada a correos electrónicos. Este tipo de amenaza permite trabajar la capacidad de los estudiantes para identificar patrones de suplantación de identidad, como inconsistencias en el dominio del remitente, el lenguaje del mensaje y la metadata asociada al envío.

Esta actividad resulta especialmente pertinente para las especialidades del área tecnológica, ya que refuerza en Telecomunicaciones la comprensión de amenazas a la integridad de los dispositivos y servicios de red, en Conectividad y Redes el análisis del tráfico potencialmente malicioso, y en Programación la interpretación de scripts ocultos o enlaces maliciosos embebidos. En conjunto, el enfoque de prevención permite fortalecer la conciencia digital y las competencias defensivas, coherentes con el perfil de egreso esperado para estudiantes TP en seguridad informática.

3.3. Experiencia de Aprendizaje: Desafío DDoS

La denegación de servicio distribuida —conocida por sus siglas en inglés como DDoS (Distributed Denial-of-Service)— es una forma avanzada de ciberataque que busca impedir el uso legítimo de un servicio mediante la saturación de sus recursos. Este tipo de ataque se considera una extensión del ataque de denegación de servicio tradicional (DoS), ya que en lugar de provenir de un único origen, utiliza múltiples entidades comprometidas que actúan de forma coordinada para amplificar el efecto del ataque.

Existen diversas formas de ejecutar este tipo de ataques. Una de las más comunes es el envío masivo de paquetes hacia un servidor, consumiendo así ancho de banda, capacidad de procesamiento o memoria, lo que resulta en la degradación o interrupción total del servicio. En algunos casos, los atacantes emplean paquetes malformados para causar fallos en los protocolos o aplicaciones del sistema víctima, forzando reinicios o bloqueos del servicio (Mirkovic y Reiher, 2004).

Además, estos ataques pueden clasificarse en dos grandes categorías según la debilidad que explotan:

- **ataques semánticos:** abusan de errores de diseño en protocolos o aplicaciones
- **ataques de fuerza bruta:** se basan en el envío masivo de solicitudes legítimas para agotar recursos

En ambos casos, el objetivo es lograr la inutilidad del servicio, ya sea de forma total (ataques disruptivos) o parcial (ataques degradantes) (Mirkovic y Reiher, 2004).

El laboratorio de DDoS en CyberAcademy simula un entorno de red corporativa donde los estudiantes deben analizar patrones de tráfico para identificar ataques en tiempo real. La experiencia se estructura en torno a componentes pedagógicos y técnicos que permiten evaluar las capacidades de detección y respuesta:

Indicador	Descripción
Acción	Identificación de patrones anómalos en el flujo de paquetes (picos de tráfico, solicitudes recurrentes, caídas de nivel de internet). El estudiante debe marcar si se trata de un comportamiento legítimo o de un posible ataque DDoS, donde se puede bloquear el puerto sospechoso.
Puntos	Se asignan +2 puntos por identificar correctamente un ataque en curso, +1 punto en caso de falsos positivos, y 0 puntos cuando se omite la detección de un ataque real.
Retroalimentación	Retroalimentación inmediata sobre la decisión, mostrando métricas de tráfico y explicaciones pedagógicas que refuerzan la correcta interpretación de los datos.
Intentos	Cada intento presenta variaciones en los patrones de tráfico (legítimo y malicioso), lo que obliga a aplicar criterios de análisis diferenciados en cada simulación.
Tiempo	El tiempo de detección no está limitado, pero se registra como métrica de desempeño para analizar la rapidez de la respuesta frente al ataque.

Tabla 3.2: Indicadores del laboratorio DDoS

El ataque de DDoS fue seleccionado como representativo para los laboratorios orientados al enfoque de detección, debido a su naturaleza reactiva y su manifestación directa en el rendimiento del sistema. Este tipo de ataque se basa en el envío masivo de solicitudes simultáneas hacia un servidor o servicio, con el fin de saturar sus recursos y generar una denegación de acceso a usuarios legítimos.

Esta experiencia es especialmente pertinente para las especialidades del área tecnológica: en Conectividad y Redes, se fortalece la capacidad de analizar flujos de red y aplicar técnicas de supervisión; en Telecomunicaciones, se exploran las implicancias del ataque en la disponibilidad de servicios críticos y la respuesta desde los dispositivos de red; y en Programación, se promueve la comprensión de cómo ciertos scripts o bots automatizados pueden formar parte de estas amenazas.

3.4. Experiencia de Aprendizaje: Desafío Gusanos

Un ataque de gusano, comúnmente denominado Internet Worm, se define como un código malicioso que posee la capacidad de auto-replicarse y propagarse de forma autónoma. Tal como señalan Li, Salour y Su (2008), estos códigos se esparcen sin ninguna intervención humana.

Los gusanos suelen aprovechar vulnerabilidades en sistemas operativos, aplicaciones o protocolos de red para infectar equipos y, a través de ellos, escanear automáticamente y atacar otros dispositivos vulnerables. Este ciclo de replicación automática permite que un único gusano se disemine de forma exponencial, saturando recursos de red o de cómputo, y puede dar lugar a impactos severos en infraestructura crítica —como ocurrió con gusanos históricos como Morris, Code Red y SQL Slammer— debido a su rapidez y alcance.

El laboratorio de gusanos en CyberAcademy simula un entorno de red infectado donde los estudiantes deben analizar los rastros registrados por el código malicioso para identificar su propagación. La experiencia se estructura en torno a componentes pedagógicos que evalúan las capacidades de investigación y análisis:

Indicador	Descripción
Acción	Revisión de registros de sistema, tráfico de red y evidencias digitales para identificar equipos comprometidos, mediante la línea de comando.
Puntos	Se asignan +4 puntos por detectar correctamente todos los dispositivos afectados, +1 por identificar parcialmente la propagación (dispositivo, archivos y puertos), y +0 en caso de conclusiones erróneas que omitan compromisos críticos.
Retroalimentación	Retroalimentación detallada que muestra el mapa de infección completo y explicación de las señales que permitan deducir la propagación del worm.
Intentos	Cada simulación presenta una propagación distinta (diferente número de equipos comprometidos, patrones de infección variados), fomentando la práctica reiterada y el aprendizaje progresivo.
Tiempo	No existe límite de tiempo para el análisis, pero el sistema registra la dedicación de un estudiante al investigar los rastros de propagación de un código malicioso.

Tabla 3.3: Indicadores del laboratorio Worm

El ataque tipo worm fue seleccionado como representativo para los laboratorios orientados a la seguridad en redes, debido a su capacidad de autorreplicación y propagación autónoma entre múltiples dispositivos dentro de una red, sin requerir intervención humana directa. Estas características lo convierten en un escenario idóneo para que los estudiantes investiguen las consecuencias de un incidente posterior a su ocurrencia, mediante la recolección y análisis de evidencias digitales.

En el caso de la especialidad de Conectividad y Redes, se refuerza el análisis de tráfico interno para identificar dispositivos comprometidos. Para Telecomunicaciones, se abordan los efectos del malware en la disponibilidad y calidad de los servicios de red. Por su parte, Programación permite comprender la lógica del código malicioso detrás del worm y sus métodos de persistencia.

3.5. Método de Diseño de Laboratorios

La aplicación CyberAcademy fue desarrollada utilizando el motor de videojuegos Unity, integrando el paquete de assets Dream OS, el cual ofrece un entorno visual que emula el funcionamiento de un sistema operativo real. Este paquete incluye diversas herramientas como consola, navegador, gestor de archivos, cliente de correo, entre otros componentes, lo que facilitó significativamente su adaptación a la visión educativa de los laboratorios.

CyberAcademy implementa un sistema de sesiones de usuario, lo que permite a cada estudiante contar con una cuenta personalizada. Este sistema está diseñado para fomentar la participación a través de elementos lúdicos, tales como la personalización del personaje principal y de la interfaz de usuario, permitiendo a los estudiantes adaptar su experiencia dentro de la plataforma.

Cada laboratorio incorpora un sistema de puntuación y recompensas, donde el desempeño del estudiante se traduce en puntos que incrementan el nivel de su cuenta y le otorgan monedas virtuales. Estas monedas pueden utilizarse en la tienda interna de la aplicación para adquirir distintos cosméticos, promoviendo así una experiencia más interactiva y motivadora.



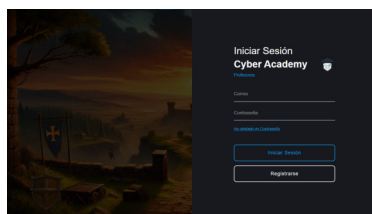
Figura 3.2: Retroalimentación de la aplicación

Durante el desarrollo, se desactivó el sistema de inicio de sesión predeterminado del recurso, y se diseñaron aplicaciones específicas para cada enfoque de los laboratorios, utilizando como base las funcionalidades ya integradas en el paquete Dream OS.

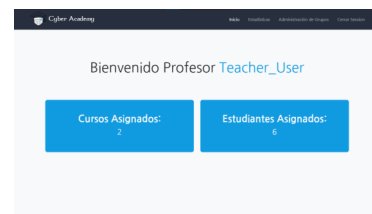
El sistema de laboratorios de CyberAcademy incorpora herramientas específicas que permiten al docente acompañar y potenciar el proceso de aprendizaje de manera integral. A través de una plataforma web centralizada, los educadores pueden acceder a información detallada sobre el desempeño de cada estudiante y del grupo completo.

Entre las funcionalidades disponibles destacan:

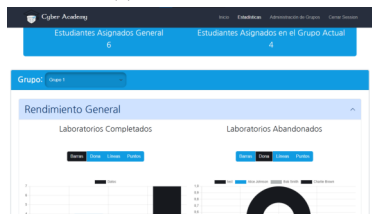
- **Seguimiento del progreso:** Monitoreo en tiempo real del avance individual y grupal mediante dashboards interactivos.
- **Análisis de resultados:** Generación automática de reportes que identifican patrones de error y aspectos que requieren refuerzo.
- **Evaluación continua:** Sistema de métricas que complementa la evaluación tradicional con indicadores de progreso en habilidades específicas.



(a) Inicio de sesión



(b) Página de inicio



(c) Dashboard de estadísticas de los alumnos en la página del profesor



(d) Sección de gestión de los grupos de alumnos

Figura 3.3: Página de administración del docente

La plataforma web recopila y procesa datos detallados de las actividades realizadas por los estudiantes, permitiendo al docente consultar métricas específicas como: porcentaje de correos identificados correctamente en los laboratorios de phishing, tiempo de resolución de cada desafío, efectividad en la detección de dispositivos comprometidos en escenarios de seguridad de redes, entre otros indicadores relevantes. Esta información facilita la identificación de oportunidades de mejora y la personalización de la enseñanza según las necesidades detectadas en cada grupo de aprendizaje.

Al comienzo de cada laboratorio, se presenta un tutorial introductorio que explica el contexto del ejercicio y detalla el funcionamiento de cada uno de sus componentes. Esto permite que los estudiantes, especialmente aquellos que acceden por primera vez, comprendan de manera clara cómo interactuar con el sistema y llevar a cabo correctamente las actividades del laboratorio (ver figura 3.4a y 3.4b).



Figura 3.4: Capturas del tutorial del laboratorio

Adicionalmente, cada laboratorio cuenta con un sistema de sugerencias, pistas contextuales y un menú de salida. Las sugerencias representan ayudas generales siempre visibles, que no afectan el puntaje final. Estas se encuentran disponibles a través de un panel desplegable ubicado en el lado derecho de la interfaz, que al hacer clic sobre la flecha, revela el contenido como se muestra en la Figura 3.5.

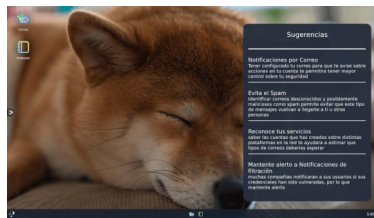


Figura 3.5: Pestaña de sugerencias

Por otra parte, las pistas son ayudas específicas que el usuario puede activar manualmente haciendo clic sobre ellas. A diferencia de las sugerencias, estas sí impactan el puntaje final del laboratorio. Estas pistas se encuentran en el panel izquierdo (ver Figura 3.6a) y, una vez desplegado, muestra un menú con opciones particulares de cada laboratorio y el desbloqueo de pistas (ver Figura 3.6b).



Figura 3.6: Capturas de acciones para acceder al panel de pistas

Finalmente, desde este mismo panel izquierdo, se accede al botón de salida, que ofrece dos opciones: “Abandonar” y “Finalizar” (ver figura 3.7). La opción “Abandonar” está destinada a aquellos casos en los que el estudiante desea

salir del laboratorio sin registrar su desempeño, ya sea por error o por decisión propia. En cambio, la opción “Finalizar” cierra oficialmente la experiencia, calcula el puntaje obtenido, entrega retroalimentación inmediata y actualiza el nivel de la cuenta del usuario.

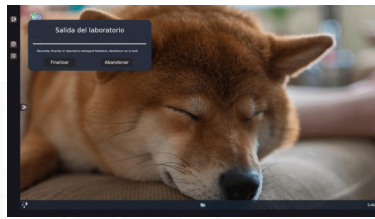


Figura 3.7: Panel de salida

Cada laboratorio incluye una aplicación de notas diseñada para orientar al estudiante durante la actividad. Esta herramienta proporciona indicaciones clave sobre los pasos a seguir, así como información contextual relevante que resulta fundamental para la correcta resolución del laboratorio (ver Figura 3.8).

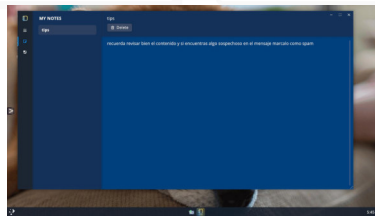
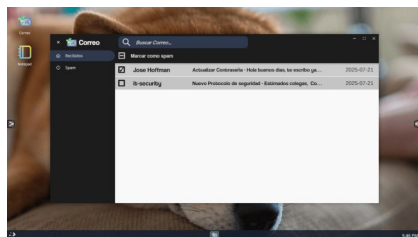
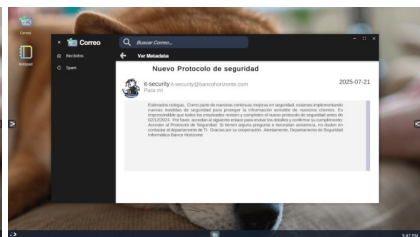


Figura 3.8: Aplicación de notas

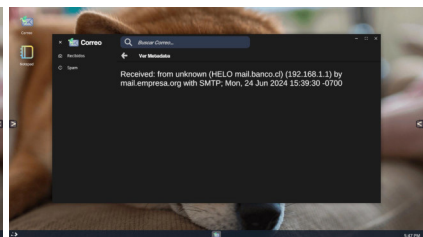
En los laboratorios de enfoque de prevención, se personalizó la aplicación de correos integrando mejoras tanto en el diseño visual como en sus funcionalidades. Entre las nuevas características se incluyeron la búsqueda de mensajes, la opción de marcar o desmarcar correos como spam y la visualización de la metadata asociada a cada correo (ver Figura 3.9a, 3.9b y 3.9c). Estas modificaciones permiten que el estudiante interactúe con la aplicación de forma similar a un cliente de correo real, similar a Gmail, donde es posible visualizar la bandeja de entrada y el contenido de los mensajes dentro de una misma interfaz. El objetivo de esta adaptación es brindar una experiencia más realista y didáctica, fomentando el aprendizaje práctico en la detección de posibles ataques de phishing.



(a) Aplicación de correo, pantalla inicial



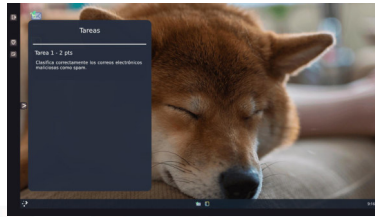
(b) Aplicación de correo, vista correo



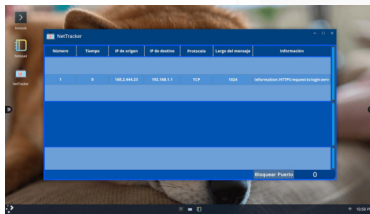
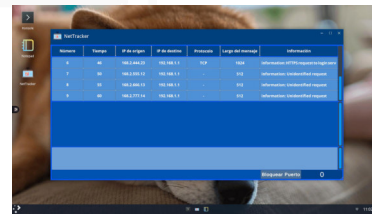
(c) Aplicación de correo, vista metadata

Figura 3.9: Capturas de la aplicación de correo

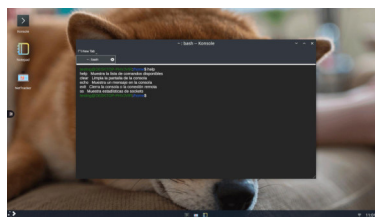
Además, en el enfoque de prevención se incorporó una sección especial denominada 'Tareas' dentro del panel desplegable derecho (ver Figura 3.10). Esta funcionalidad guía al estudiante indicando claramente los objetivos a cumplir dentro del laboratorio. Su propósito es ofrecer apoyo adicional a quienes no hayan visualizado el tutorial inicial o necesiten un recordatorio sobre las acciones requeridas.

**Figura 3.10:** Panel de tareas

En los laboratorios con enfoque en detección, se desarrolló la aplicación 'Net Tracker', una herramienta inspirada en Wireshark que es un analizador de protocolos de red de código abierto que permite a los usuarios capturar y examinar de forma interactiva el tráfico que circula por una red, proporcionando una inspección profunda de cientos de protocolos. A través de esta aplicación, se solicita al estudiante monitorear activamente los paquetes que ingresan al sistema para identificar posibles señales de un ataque DDoS (ver Figuras 3.11a y 3.11b). Una vez detectado, el estudiante tiene la opción de bloquear el puerto comprometido con el fin de mitigar el ataque. Esta dinámica busca fomentar habilidades de respuesta temprana y reconocimiento de patrones anómalos en entornos simulados de red.

**(a)** Aplicación Net Tracker**(b)** Aplicación Net Tracker (en ataque de DDoS)**Figura 3.11:** Capturas de la aplicación de Net Tracker

Además, en este mismo laboratorio se incorporó una versión modificada de la aplicación de consola, la cual fue visualmente adaptada para simular una terminal real (ver Figura 3.12). Esta consola incluye un conjunto de comandos específicos orientados al análisis de red, permitiendo a los estudiantes realizar un diagnóstico más profundo del entorno. El objetivo es fomentar la exploración y el aprendizaje de comandos básicos en un entorno controlado, ya que las funcionalidades están acotadas exclusivamente al contexto del laboratorio.

**Figura 3.12:** Aplicación de consola DDoS

En los laboratorios con enfoque en análisis, también se modificó la aplicación de consola, incorporando comandos específicos diseñados para este escenario (ver Figura 3.13). Entre ellos destaca el uso del protocolo de terminal segura 'ssh', que permite al estudiante conectarse a otra máquina dentro de la red con el fin de analizar su estado, evaluar el uso de recursos y determinar posibles signos de infección. Este laboratorio está orientado a que los estudiantes desarrollen habilidades en la detección de patrones sospechosos y en el uso de la línea de comandos, facilitando la comprensión del impacto que puede tener un ataque tipo worm.

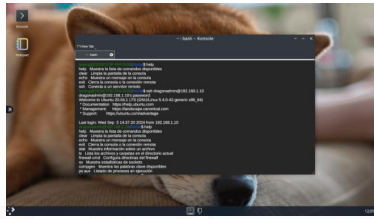


Figura 3.13: Aplicación de consola Worm

También, en este mismo laboratorio se incorporó una sección de preguntas dentro del panel desplegable izquierdo (Ver Figura 3.14). Estas preguntas tienen como objetivo guiar al estudiante en la exploración y análisis de las máquinas, orientando su investigación y ayudándole a identificar los elementos clave necesarios para resolver el laboratorio.

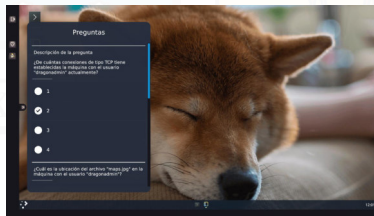


Figura 3.14: Panel de preguntas

3.6. Criterios de Selección y Adopción de Unity

La elección del motor de desarrollo se fundamentó en un análisis comparativo de las principales plataformas disponibles en el mercado, cuyas ventajas y desventajas se sintetizan en la tabla 3.4. Entre las opciones evaluadas, Unity destacó por su equilibrio entre versatilidad, estabilidad y capacidad técnica.

Este motor ofrece un entorno de desarrollo integral que permite la creación de entornos interactivos y simulaciones de diversa complejidad, lo que lo convierte en una herramienta adecuada tanto para proyectos educativos como para aplicaciones de mayor escala. Entre sus atributos más relevantes se encuentran su entorno de edición intuitivo, la amplia documentación técnica disponible y la existencia de una comunidad activa que favorece la resolución colaborativa de problemas y el intercambio de conocimiento.

Asimismo, Unity dispone de un sistema consolidado de recursos y complementos digitales, accesibles a través de su biblioteca oficial, que facilita la integración de elementos visuales y funcionales, optimizando el proceso de desarrollo y diseño de escenarios.

Otro factor determinante en su adopción fue la experiencia previa en el uso de este motor, lo que permitió aprovechar de manera eficiente las herramientas de desarrollo y el dominio del lenguaje de programación C#, reduciendo así los tiempos de implementación y evitando la necesidad de incorporar nuevas curvas de aprendizaje asociadas a otros entornos.

Motor	Pros	Contras
Unity	- Multiplataforma (PC, móvil, consola, VR/AR). - Gran comunidad y documentación extensa. - Amplio <i>Asset Store</i>. - Equilibrio sólido en 2D y 3D. - Lenguaje C# ampliamente usado. - Herramientas robustas para simulaciones y VR.	- Curva de aprendizaje moderada. - Alto consumo de recursos en proyectos grandes. - Cambios recientes en licencias han generado desconfianza.
Godot	- Código abierto y gratuito (MIT). - Muy ligero y eficiente. - Excelente rendimiento en 2D. - Soporta GDScript (similar a Python), C#, C++. - Comunidad activa y transparente. - Ideal para entornos educativos.	- Ecosistema de assets reducido. - Menor adopción en la industria AAA. - Soporte 3D aún inmaduro.
Unreal Engine	- Gráficos de alta calidad (estándar AAA). - Motor de físicas realista. - <i>Blueprints</i> accesibles para no programadores. - Gratis hasta cierto nivel de ingresos. - Amplia comunidad y tutoriales.	- Curva de aprendizaje pronunciada. - Requiere hardware potente. - Excesivo para proyectos simples o educativos.
GameMaker	- Accesible e ideal para principiantes. - Lenguaje propio GML, fácil de aprender. - Excelente para prototipado rápido en 2D. - Exportación a varias plataformas. - Comunidad activa en el ámbito indie.	- Muy limitado en 3D. - Menos versátil frente a Unity o Unreal. - Escasa adopción en grandes producciones. - Modelo de licencias más restrictivo.
Construct	- Desarrollo 2D sin necesidad de programar. - Sistema de eventos visuales muy intuitivo. - Exportación multiplataforma (incluyendo web/HTML5). - Ideal para educación y prototipado rápido. - Marketplace con plantillas y assets.	- No soporta desarrollo 3D. - Funciones avanzadas requieren suscripción de pago. - Limitado para proyectos de gran envergadura. - Menor adopción profesional frente a otros motores.

Tabla 3.4: Comparación de motores de videojuegos: Unity, Godot, Unreal Engine y GameMaker.

3.7. Integración del modelo Cyber Kill Chain de LockHeed Martin

Debido a su naturaleza secuencial y su enfoque en la descomposición de ciberataques, el modelo Cyber Kill Chain de Lockheed Martin se establece como el pilar estructural de esta propuesta. En consecuencia, a continuación se detalla su aplicación práctica en el diseño de los laboratorios, definiendo los componentes específicos de cada fase y explorando su versatilidad para ser adaptados en la generación de nuevas instancias de aprendizaje.

3.7.1. Phishing (Laboratorio de prevención)

El ataque de phishing, dentro del marco del modelo Cyber Kill Chain, se aborda principalmente a través de sus tres primeras fases: reconocimiento (Reconnaissance), instrumentalización (Weaponization) y entrega (Delivery). Esta elección se fundamenta en la estructura pedagógica del laboratorio, cuyo objetivo es desarrollar en los estudiantes la capacidad de identificar patrones y señales tempranas asociadas al ataque, más que simular sus efectos directos sobre el sistema comprometido.

Para cada componente de la kill chain, se identificaron los siguientes aspectos:

- **Reconocimiento:** Si bien esta fase no se simula directamente, se aborda de forma implícita mediante el análisis del origen del correo y la metadata, lo que permite al estudiante inferir la posible obtención previa de información por parte del atacante.
- **Instrumentalización:** Esta fase se representa a través del contenido del correo fraudulento, el cual incluye componentes diseñadas para inducir a la víctima a interactuar con enlaces o archivos maliciosos.
- **Entrega:** Esta fase se implementa directamente mediante la simulación del sistema de correos en la aplicación, donde el estudiante puede examinar los mensajes sospechosos y aplicar criterios de evaluación para identificar posibles ataques de phishing.

Un ejemplo de contexto de instancia de laboratorio puede situar al estudiante en el rol de un técnico de soporte informático en una entidad bancaria. Este escenario resulta especialmente relevante, ya que profesionales en estos cargos suelen tener acceso privilegiado a la red corporativa y, debido al alto volumen de correos que reciben diariamente, son particularmente susceptibles a ataques de phishing. En este contexto, se pueden simular correos fraudulentos que aparentan provenir de departamentos internos, como recursos humanos, o de otras áreas de la organización, con el fin de evaluar la capacidad del estudiante para identificar intentos de suplantación y amenazas potenciales.

Dado este contexto, un ejemplo de correo con un intento de phishing podría estructurarse de la siguiente manera:

```
Received: (qmail 58211 invoked by uid 60001); Wed, 26 Jun 2024 16:25:30 +0000
Received: from [192.168.3.9] by soporte.empresa-soporte.com via HTTP; Wed, 26 Jun 2024 09:25:30 -0700 (PDT)
Date: Wed, 26 Jun 2024 09:25:30 -0700 (PDT)
From: Soporte Técnico <seguridad@empresa-soporte.com>
Subject: Restablecimiento de contraseña requerido
To: carlos.seguridad@empresa.org
Reply-to: soporte@reset-seguro.net
Message-id: <94311.63822.qm@soporte.empresa-soporte.com>
MIME-version: 1.0
X-Mailer: SOPMail/2.5.0
Content-type: multipart/alternative;
boundary="Boundary_(ID_Cy82zAx4wBn3DQvLKcmw2A)"
X-Originating-IP: [192.168.3.9]

--Boundary_(ID_Cy82zAx4wBn3DQvLKcmw2A)
Content-Type: text/plain; charset=ÛTF-8"

Detectamos actividad sospechosa en tu cuenta.
Para evitar bloqueos, restablece tu contraseña inmediatamente desde el siguiente enlace:
<a href="http://reset-seguro.net">Restablecer Contraseña</a>

--Boundary_(ID_Cy82zAx4wBn3DQvLKcmw2A)--
```

Este correo fue enviado el miércoles 26 de junio de 2024. A simple vista, puede parecer legítimo; sin embargo, contiene múltiples componentes que permiten identificarlo como un intento de phishing. A continuación, se destacan los aspectos más relevantes:

- **Dominio sospechoso:** El remitente utiliza el dominio (@empresa-soporte.com), en el cual la palabra “soporte” presenta un error tipográfico (doble p) con respecto al dominio institucional real (@empresa.org). Este pequeño detalle puede pasar desapercibido para un usuario distraído.
- **Dirección IP de origen:** El encabezado muestra una dirección IP de origen (192.168.3.9), perteneciente al rango de direcciones privadas, lo cual sugiere que el correo no fue enviado desde la infraestructura corporativa oficial.
- **Enlace sospechoso:** El mensaje contiene un enlace hacia un sitio externo (http://reset-seguro.net), el cual no es seguro (uso de HTTP en lugar de HTTPS) y tampoco corresponde a un dominio corporativo. Esto podría implicar la existencia de un servidor malicioso utilizado para capturar credenciales o distribuir software malicioso.

- **Ingeniería social en el contenido:** El asunto y el cuerpo del mensaje apelan a la urgencia y al miedo ('Detectamos actividad sospechosa...'), lo cual es una táctica común para forzar al destinatario a actuar sin cuestionamientos.

Este ejemplo se alinea con las tres primeras fases del modelo Cyber Kill Chain:

1. **Reconocimiento (Reconnaissance):** El atacante identifica una posible víctima con privilegios relevantes (por ejemplo, un funcionario del área de seguridad informática), lo que se evidencia por el uso de una dirección específica (carlos.seguridad@empresa.org).
2. **Instrumentalización (Weaponization):** Se construye un payload, en este caso mediante un enlace malicioso que posiblemente redirige a un formulario de captura de credenciales o ejecuta un script malicioso.
3. **Entrega (Delivery):** El correo es enviado con una apariencia legítima, utilizando un remitente falso y un lenguaje que simula una comunicación oficial de la empresa.

Por otra parte, un ejemplo de correo legítimo podría estructurarse de la siguiente manera:

```
Received: (qmail 61122 invoked by uid 60001); Wed, 26 Jun 2024 16:15:10 +0000
Received: from [10.10.1.4] by mail.empresa.org via HTTP; Wed, 26 Jun 2024 09:15:10 -0700 (PDT)
Date: Wed, 26 Jun 2024 09:15:10 -0700 (PDT)
From: Asistente Dirección <asistente.direccion@empresa.org>
Subject: Envío de documento pendiente
To: carlos.seguridad@empresa.org
Reply-to: asistente.direccion@empresa.org
Message-id: <84401.33721.qm@mail.empresa.org>
MIME-version: 1.0
X-Mailer: Outlook 16.0
Content-type: multipart/mixed; boundary="Boundary_(ID_R2KD9w47g7tMbv8WxuNpQQ)"
X-Originating-IP: [10.10.1.4]
```

```
-Boundary_(ID_R2KD9w47g7tMbv8WxuNpQQ)
Content-Type: text/plain; charset=UTF-8"
```

Estimado Carlos,

Por favor revisa el documento adjunto con los resultados del análisis de vulnerabilidades.
No dudes en comunicarte si tienes dudas.

Atentamente,
Asistente Dirección

```
-Boundary_(ID_R2KD9w47g7tMbv8WxuNpQQ)-
```

Este correo también fue enviado el miércoles 26 de junio de 2024. A diferencia del ejemplo anterior, presenta características que permiten identificarlo como legítimo y confiable. Entre los elementos que refuerzan su autenticidad destacan:

- **Dominio institucional:** El remitente utiliza una dirección de correo asociada al dominio oficial de la organización (@empresa.org), sin errores ortográficos ni dominios alternativos sospechosos.
- **Dirección IP de origen:** El encabezado muestra que el correo fue enviado desde una dirección IP interna de la red corporativa (10.10.1.4), lo que refuerza su legitimidad.
- **Contenido del mensaje:** El asunto y el cuerpo del correo mantienen un lenguaje profesional y objetivo, sin apelaciones a la urgencia ni tácticas de ingeniería social. El mensaje es claro, directo y vinculado a una tarea específica dentro del ámbito laboral.

Debido a que este correo no contiene elementos que se alineen con las fases del modelo Cyber Kill Chain, se considera legítimo y no representa una amenaza de seguridad. En el contexto pedagógico, este tipo de correos será incorporado

como contraparte segura dentro del laboratorio de Phishing, permitiendo a los estudiantes distinguir claramente entre comunicaciones legítimas y aquellas que presentan indicios de ataque.

Para la creación de las instancias dentro del laboratorio, se diseñaron diversos contextos que simulan situaciones reales, incorporando correos electrónicos tanto legítimos como potencialmente maliciosos de forma aleatoria. La aplicación utilizada permite descomponer y analizar cada componente del correo como remitente, destinatario, asunto, cuerpo del mensaje y metadatos, facilitando la identificación de señales de alerta. Estas instancias fueron pensadas para ofrecer una experiencia pedagógica completa, promoviendo la capacidad de análisis crítico y el reconocimiento de patrones en un entorno controlado, pero lo suficientemente cercano a escenarios reales.

3.7.2. DDoS (Laboratorio de detección)

En el laboratorio de DDoS, las fases mejor representadas en la cadena de kill chain son Entrega, Explotación y parcialmente Instalación. Estas etapas fueron seleccionadas en función del enfoque del laboratorio, el cual prioriza la detección del ataque a través de la saturación de la red. A lo largo de la actividad, se evidencian las consecuencias de un ataque DDoS mediante la degradación progresiva del rendimiento de la red simulada, lo que permite observar cómo el internet"disminuye su funcionalidad con el tiempo.

- **Entrega:** Se simula a través del tráfico malicioso que llega al sistema en forma de múltiples paquetes de red, replicando el comportamiento de un ataque distribuido.
- **Explotación:** Aunque en un ataque DDoS no existe una explotación de vulnerabilidad en el sentido tradicional, esta fase se interpreta como la saturación intencional de recursos del sistema para degradar o denegar el servicio.
- **Instalación:** Se aborda desde el punto de vista defensivo, ya que el estudiante debe identificar y mitigar el ataque antes de que este afecte gravemente la disponibilidad del sistema.

Un ejemplo de contexto para una instancia de laboratorio sitúa al estudiante en el rol de técnico en redes de una empresa privada. Este escenario es relevante, ya que, ante actividades sospechosas, el técnico tiene la responsabilidad de monitorear y analizar el tráfico de la red local. En este entorno, puede surgir un ataque de tipo DDoS con el objetivo de degradar o interrumpir servicios clave. Este tipo de amenaza es común en situaciones reales, afectando a sitios web, servidores privados y otros servicios críticos, los cuales pueden quedar comprometidos ante este tipo de prácticas maliciosas.

Dado lo anterior, la aplicación recibirá paquetes de red en intervalos de tiempo de hasta 10 minutos como máximo. Cada paquete contiene información estructurada similar al siguiente ejemplo:

```
id: 1
ip_source: 168.2.444.23
ip_dest: 192.168.1.1
port: 443
protocol: TCP
length: 1024
message: "Accessing login portal"
time: 20
```

Cada paquete es procesado en función del parámetro, que indica el momento en que se recibe en segundos. Los campos ip_source y port especifican el origen del paquete, mientras que el campo message representa el contenido del mensaje descriptado. El protocolo (protocol) también cumple un rol importante, ya que será utilizado en la simulación dentro de la consola para representar el tráfico de manera más realista.

Durante la simulación, al iniciar el envío de paquetes, se generará un ataque de denegación de servicio distribuido (DDoS) mediante el envío masivo de múltiples paquetes en un intervalo de tiempo reducido. Cada uno de estos paquetes tendrá una dirección ip_source distinta, simulando distintos atacantes. Este flujo masivo de tráfico será generado de manera aleatoria dentro del tiempo establecido, lo que otorgará mayor dinamismo a la simulación y permitirá identificar visualmente cuándo ocurre un ataque.

Un conjunto de paquetes correspondientes al ataque podría verse de la siguiente forma:

```
id: 15
ip_source: 168.2.555.12
ip_dest: 192.168.1.1
port: 80
protocol: TCP
length: 1024
message: "Repeated access attempts"
time: 50
```

```
id: 16
ip_source: 168.2.555.13
ip_dest: 192.168.1.1
port: 80
protocol: TCP
length: 1024
message: "Repeated access attempts"
time: 55
```

. . .

Este conjunto de paquetes puede ser analizado según el modelo Cyber Kill Chain de la siguiente manera:

- **Entrega:** Los paquetes provenientes de múltiples direcciones IP (por ejemplo, 168.2.555.12 y 168.2.555.13) realizan solicitudes simultáneas al puerto 80 del servidor (192.168.1.1) utilizando el protocolo TCP. Esto simula un intento de sobrecargar el servidor mediante tráfico anómalo.
- **Explotación:** El contenido del mensaje, etiquetado como "Repeated access attempts", representa un intento deliberado de saturar los recursos del sistema aprovechando su apertura al tráfico HTTP.
- **Acciones sobre el Objetivo:** El ataque impacta directamente en la disponibilidad del servidor, afectando su rendimiento a través del alto volumen y frecuencia de las solicitudes, lo cual puede derivar en una denegación total del servicio.

3.7.3. Worm (Laboratorio de análisis)

El laboratorio orientado al ataque tipo worm representa principalmente las fases de Instalación, Comando y Control y Acciones sobre el Objetivo dentro del modelo de la Kill Chain. El propósito es que el estudiante sea capaz de identificar patrones asociados a este tipo de amenaza utilizando herramientas de análisis desde la consola de comandos, accediendo remotamente a otra máquina mediante protocolo SSH. Las fases representadas se abordan de la siguiente forma:

- **Instalación:** Se evidencia en la capacidad del worm de replicarse en múltiples máquinas dentro del entorno simulado, afectando el rendimiento y comportamiento del sistema.
- **Comando y Control (C2):** Si bien no se simula un canal C2 real, se puede inferir mediante el comportamiento autónomo del malware y su propagación.
- **Acciones sobre el Objetivo:** Se manifiesta a través del impacto directo en la infraestructura, como el uso excesivo de recursos, la creación de archivos maliciosos y la alteración de configuraciones.

Un ejemplo de contexto para este laboratorio sitúa al estudiante como analista de ciberseguridad encargado de investigar una red cerrada de servidores sospechosos de haber sido infectados por un worm. La tarea consiste en conectarse a distintas máquinas y, utilizando comandos específicos, determinar cuáles están comprometidas.

En cada una de estas máquinas, los estudiantes podrán examinar parámetros relacionados con el uso de recursos del sistema y la actividad de red, empleando comandos como `compgen`, `iostat` y `ss -tuna`. Las máquinas están configuradas

con una estructura que incluye la dirección IP, los usuarios disponibles y la salida esperada de los comandos mencionados, como se muestra a continuación:

```
ip: 192.168.1.101
users: ["user"]
compgen:
  recent_scripts: [
    "/home/user/run_simulation.sh",
    "/usr/bin/top"
  ]
iostat:
  cpu_user: 8.5%
  cpu_system: 4.2%
  cpu_idle: 87.3%
  disk_read_MB_s: 5.2
  disk_write_MB_s: 1.1
ss -tuna: [
  {
    state: LISTEN
    recv_q: 0
    send_q: 128
    local_address: 0.0.0.0:22
    peer_address: *:*
```

En contraste, una máquina infectada podría presentar la siguiente estructura:

```
ip: 192.168.1.100
users: ["user", "admin_master", "bot"]
compgen:
  recent_scripts: [
    "/tmp/.worm/start.sh",
    "/tmp/.worm/replicate.sh",
    "/home/user/.bash_history"
  ]
iostat:
  cpu_user: 75.3%
  cpu_system: 22.1%
  cpu_idle: 2.6%
  disk_read_MB_s: 120.5
  disk_write_MB_s: 85.7
ss -tuna: [
  {
    state: ESTAB
    recv_q: 0
    send_q: 0
    local_address: 192.168.1.100:4321
    peer_address: 45.12.34.201:8080
  }
  {
    state: ESTAB
    recv_q: 0
    send_q: 0
    local_address: 192.168.1.100:4444
    peer_address: 103.45.67.89:1337
  }
  {
```

```

        state: LISTEN
        recv_q: 0
        send_q: 128
        local_address: 0.0.0.0:22
        peer_address: *:*
    }
]

```

Los indicadores de compromiso en esta máquina son:

- **Consumo excesivo de recursos:** Uso elevado de CPU y disco, sugiriendo actividad maliciosa en segundo plano.
- **Conexiones externas establecidas:** Comunicación activa con direcciones IP desconocidas y puertos inusuales.
- **Usuarios sospechosos:** Presencia de perfiles como admin_master y bot, que no forman parte de la configuración habitual.
- **Ejecución de scripts maliciosos:** Scripts almacenados en rutas ocultas (/tmp/.worm/) con nombres claramente anómalos.

La relación con el modelo de la Kill Chain sería:

- **Instalación:** Reflejada en la ejecución de scripts y la creación de usuarios maliciosos en la máquina.
- **Comando y Control (C2):** Deducible por la persistencia de conexiones externas desde puertos no estándar, y la existencia de usuarios con privilegios elevados posiblemente usados para el control remoto.
- **Acciones sobre el Objetivo:** Evidente en el uso intensivo de recursos del sistema y en la actividad anómala dentro de la red.

3.8. Diseño de la encuesta

Para evaluar la pertinencia pedagógica y técnica de la plataforma CyberAcademy, se elaboró un cuestionario estructurado aplicado a estudiantes de educación secundaria (cuarto medio) de la educación técnico-profesional (TP). El diseño de la encuesta contempló tanto preguntas cerradas con escala Likert como preguntas abiertas de carácter cualitativo, con el fin de obtener una visión integral de la experiencia de uso.

3.8.1. Secciones del cuestionario

La encuesta se organizó en cinco bloques principales:

1. **Datos sociodemográficos:** edad y género de los participantes, permitiendo caracterizar la muestra y analizar patrones diferenciales de percepción.
2. **Conocimientos y actitudes previas sobre ciberseguridad:** se incluyeron preguntas en escala de 1 a 5 sobre el nivel de familiaridad con la ciberseguridad, manejo básico de redes (IP, DNS, puertos), percepción de riesgos en internet y disposición para aprender a protegerse.
3. **Experiencia de uso de CyberAcademy:** se evaluaron aspectos relacionados con la interfaz en una en escala de 1 a 5, claridad del diseño, suficiencia del material de apoyo y representatividad de los laboratorios frente a situaciones reales de ataque.
4. **Impacto en el aprendizaje y percepción de utilidad:** se realizaron preguntas sobre el refuerzo de conocimientos previos con una en escala de 1 a 5, la relevancia de los laboratorios para sus intereses profesionales, y la motivación para seguir aprendiendo sobre ciberseguridad.

5. **Valoración de los laboratorios y satisfacción general:** se preguntó qué laboratorio resultó más útil (Phishing, DDoS o Worm), el nivel de satisfacción general con la plataforma, y qué aspectos se deberían mejorar o incorporar en futuras versiones.

Dimensión	Preguntas asociadas
Datos sociodemográficos	- Edad. - Género. - Nombre del colegio.
Conocimientos y actitudes previas sobre ciberseguridad	- ¿Cuál es tu nivel de familiaridad con la ciberseguridad? (escala 1–5)*³. - ¿Qué tan cómodo te sientes con conceptos básicos de redes (IP, DNS, puertos)? (escala 1–5)**⁴. - ¿Qué tan alto consideras el riesgo de amenazas en Internet? (escala 1–5)**. - ¿Qué tan dispuesto estás a aprender formas de protegerte en línea? (escala 1–5)**.
Experiencia de uso de CyberAcademy	- ¿La interfaz de la plataforma fue clara y fácil de usar? (escala 1–5)**. - ¿El material de apoyo fue suficiente para completar los laboratorios? (escala 1–5)**. - ¿Consideras que los laboratorios representan situaciones reales de ciberataques? (escala 1–5)**.
Impacto en el aprendizaje y percepción de utilidad	- ¿Adquiriste nuevos conocimientos sobre ciberseguridad? (escala 1–5)**. - ¿Reforzaste aprendizajes previos? (escala 1–5)**. - ¿Qué tan relevantes fueron los laboratorios para tus intereses profesionales? (escala 1–5)**. - ¿Te motivó a seguir aprendiendo sobre ciberseguridad? (escala 1–5)**.
Valoración de los laboratorios y satisfacción general	- ¿Qué laboratorio te pareció más útil? (Phishing, DDoS, Worm). - ¿Cómo calificarías tu nivel de satisfacción general con CyberAcademy? (escala 1–5)*. - ¿Qué aspecto más te gustó de CyberAcademy? (respuesta abierta). - ¿Qué aspectos te gustaría que se mejoraran o agregaran en futuras versiones? (respuesta abierta).

Tabla 3.5: Dimensiones y preguntas del cuestionario aplicado en CyberAcademy

^{3*} La escala utilizada corresponde a un rango categórico, donde 1 representa “Muy Poco” y 5 corresponde a “Mucho”

^{4**} La escala utilizada corresponde a un rango categórico, donde 1 representa “Totalmente en desacuerdo” y 5 “Totalmente de acuerdo”

4 | CAPÍTULO 4: VALIDACIÓN DE LA SOLUCIÓN Y RESULTADOS

En este capítulo se describe el proceso de validación de la solución propuesta, cuyo objetivo principal es evaluar el impacto de la aplicación en el aprendizaje de los estudiantes. Para ello, se detalla la metodología empleada para llevar a cabo la evaluación, incluyendo el enfoque utilizado para medir el desempeño de los estudiantes, la estructura y ejecución de los laboratorios, así como el diseño y aplicación de una encuesta orientada a recoger percepciones sobre la experiencia con la plataforma. Finalmente, se analizan los resultados obtenidos a partir de estas instancias, con el fin de determinar si la implementación de la aplicación generó un impacto positivo en términos de aprendizaje, usabilidad e interés por la ciberseguridad.

4.1. Alcance del Estudio de Percepción de CyberAcademy

Para validar la propuesta, se desarrolló una experiencia piloto con estudiantes de enseñanza media en el Liceo Industrial Hardware de San Bernardo, en Santiago de Chile. Este es un establecimiento de educación técnico-profesional que imparte las especialidades de Electrónica y Telecomunicaciones. La actividad se realizó el 20 de mayo de 2025, entre las 13:30 y las 15:30 horas, con la presencia del profesor Ervin Pinto Madariaga, y contó con la participación de 15 estudiantes de cuarto medio B de la especialidad de Telecomunicaciones, quienes respondieron la encuesta previamente descrita.

En la experiencia descrita, las pruebas se realizaron utilizando equipos con las especificaciones técnicas mínimas que se detallan en la Tabla 4.1.

Especificación	Criterio
Sistema Operativo	Windows 10
Almacenamiento	285 MB de espacio disponible
Memoria	1 GB de RAM
Procesador	1 GHz o mayor
Red	Conexión de banda ancha a Internet

Tabla 4.1: Requisitos Mínimos CyberAcademy

La jornada inició con una charla introductoria en la que se presentaron los objetivos del proyecto y se revisaron conceptos básicos de ciberseguridad, junto con una explicación general de los ataques trabajados en los laboratorios. A continuación, los estudiantes participaron en tres experiencias prácticas correspondientes a los ejes de prevención, detección y análisis de amenazas.

Debido a las limitaciones de tiempo, no fue posible realizar una segunda sesión con los estudiantes que permitiera evaluar de manera sistemática la rejugabilidad de los laboratorios. No obstante, se logró recopilar evidencia de algunos reintentos espontáneos en los laboratorios de phishing, DDoS y worm, lo que permitió obtener indicios preliminares sobre este aspecto.

Finalmente, se aplicó una encuesta estructurada para recopilar información relacionada con variables socio-demográficas (edad y género), conocimientos previos en redes, percepciones sobre la usabilidad de la aplicación, fluidez en el uso,

valoración del aprendizaje alcanzado y calidad del contenido ofrecido.

4.2. Resultados del Estudio

4.2.1. Evaluación del perfil de los encuestados

En la Figura 4.1a se presentan las edades de los estudiantes que participaron en la experiencia. La gran mayoría de los encuestados (87 %) tiene 17 años, mientras que el 13 % restante corresponde a estudiantes de 18 años. Esta concentración etaria es coherente con el nivel educativo objetivo (cuarto medio) y representa una ventaja metodológica al reducir variables de confusión relacionadas con la madurez cognitiva.

En la Figura 4.1b se describe la distribución de género de los estudiantes encuestados, esta revela una predominancia masculina del 87 %, frente a un 13 % de participación femenina. Esta distribución refleja una tendencia histórica en las especialidades tecnológicas, donde persiste una baja representación de mujeres, aspecto que debe considerarse al analizar los resultados y proyectar estrategias de inclusión en el área de ciberseguridad.

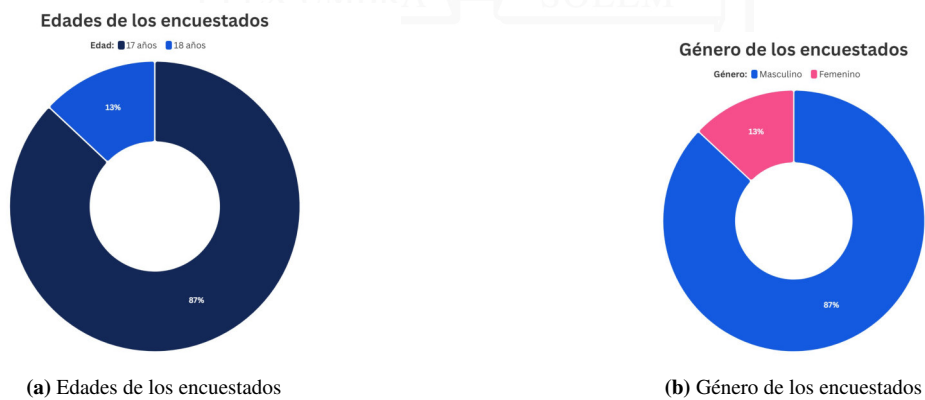


Figura 4.1: Gráficos de los perfiles socio-demográficos de los encuestados

La Figura 4.2 expone los resultados de la autoevaluación realizada por los estudiantes respecto a sus conocimientos previos en ciberseguridad antes de interactuar con la plataforma CyberAcademy. Como se aprecia en los datos, un 60 % de los participantes se autopercibe en un nivel “Regular” de conocimientos, mientras que el 40 % restante se distribuye entre las categorías “Muy poco” y “Poco”. Resulta particularmente revelador que ningún estudiante reportó ubicarse en los niveles superiores (“Bastante” o “Mucho”), lo que configura un panorama de base con importantes oportunidades de desarrollo.

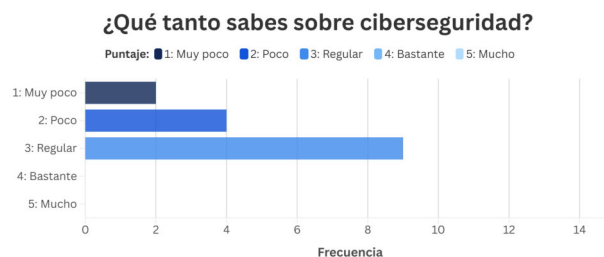


Figura 4.2: Gráfico de la percepción del nivel de conocimientos de ciberseguridad de los encuestados

4.2.2. Evaluación de los conocimientos previos de ciberseguridad

La Figura 4.3 muestra los resultados sobre el dominio autopercebido de conceptos técnicos esenciales para el trabajo en ciberseguridad, medidos mediante una escala Likert de 5 puntos. Los datos revelan un panorama contrastante entre las habilidades digitales básicas y los conocimientos técnicos específicos.

El gráfico muestra que un sólido 87 % de los estudiantes reporta competencia en el uso básico de computadores y navegación web, indicando una base digital adecuada para abordar laboratorios prácticos. Sin embargo, solo el 66 % manifiesta comprender conceptos fundamentales como direcciones IP o DNS, señalando una brecha importante en conocimientos de redes. De manera alentadora, el 93 % reconoce amenazas comunes como malware o correos fraudulentos, demostrando conciencia básica de seguridad. Particularmente relevante es que el 80 % expresa interés activo en aprender sobre protección digital, aunque solo el 60 % declara haber aprendido sobre ciberseguridad en el colegio o fuera de clases.

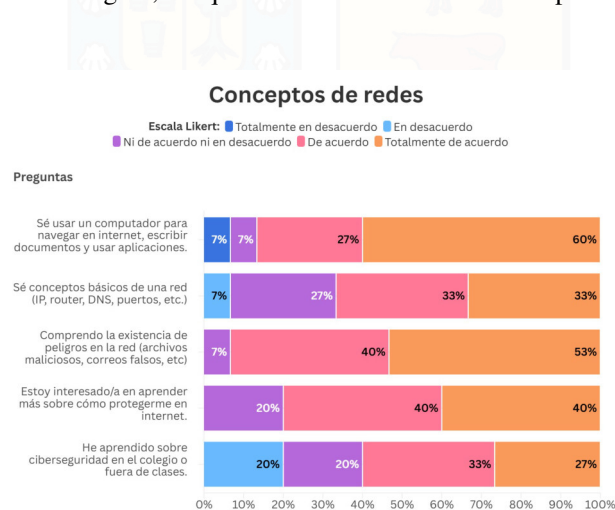


Figura 4.3: Gráfico sobre conocimientos previos de redes en los estudiantes

4.2.3. Evaluación de la usabilidad de la aplicación

La Figura 4.4 presenta los resultados obtenidos en la evaluación de la usabilidad de CyberAcademy, basada en una escala tipo Likert que midió el nivel de acuerdo de los estudiantes con diversos aspectos de la interfaz y la experiencia de uso. Este indicador permite identificar percepciones asociadas a la claridad visual, organización funcional y fluidez en la navegación.

Los datos muestran que el 74 % de los participantes percibe el diseño de la interfaz como claro y comprensible. En relación con la disposición de botones e íconos, el 66 % manifiesta acuerdo, mientras que un 27 % se mantiene neutral y un 7 % expresa desacuerdo, lo que señala posibles variaciones en la interpretación o familiaridad con la estructura visual. La legibilidad de textos y etiquetas alcanza un 80 % de respuestas positivas, lo que refleja una adecuada correspondencia entre los elementos gráficos y la terminología utilizada. Finalmente, el 73 % de los encuestados considera intuitiva la navegación entre pantallas, evidenciando una experiencia de interacción funcionalmente coherente.

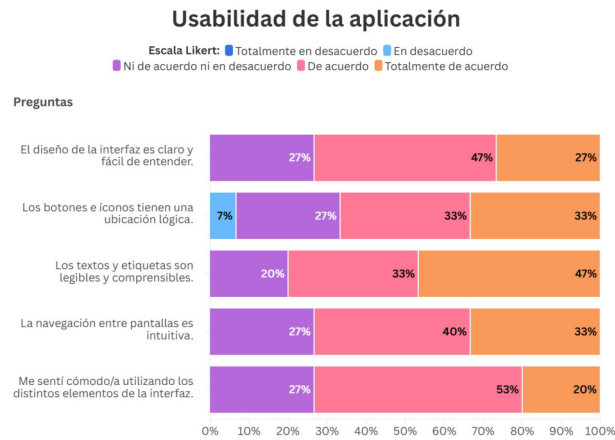


Figura 4.4: Gráfico sobre la usabilidad de la aplicación

4.2.4. Evaluación del flujo de la aplicación

La Figura 4.5 presenta los resultados asociados a la percepción de los estudiantes sobre el flujo y el rendimiento general de CyberAcademy, medidos mediante una escala tipo Likert. Este indicador permite examinar la coherencia secuencial de las actividades, la orientación del sistema durante el uso y la eficiencia técnica en la ejecución de los laboratorios.

Los datos indican que un 80 % de los participantes percibe una secuencia de pasos coherente y bien estructurada dentro de los laboratorios. De igual modo, un 80 % manifiesta que el sistema proporciona una guía adecuada a lo largo de cada fase del proceso, lo que refleja una interacción lineal y comprensible. Por otra parte, un 20 % de respuestas neutrales sugiere la posibilidad de fortalecer los mecanismos de orientación o asistencia contextual durante etapas específicas de la experiencia. En relación con el rendimiento técnico, el 67 % de los encuestados considera satisfactorio el tiempo de respuesta del sistema, mientras que un 14 % reporta demoras eventuales, evidenciando un área de seguimiento para mejorar la estabilidad del entorno interactivo.

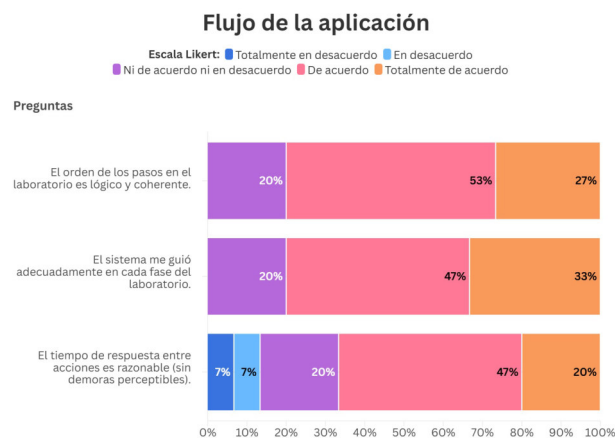


Figura 4.5: Gráfico sobre el flujo de la aplicación

4.2.5. Evaluación de la calidad del contenido

La Figura 4.6 presenta la percepción de los estudiantes respecto a la calidad y el realismo del contenido desarrollado en los laboratorios, evaluada mediante una escala tipo Likert. Este indicador permite analizar la pertinencia pedagógica de

los escenarios, el grado de correspondencia con situaciones reales y la claridad del material de apoyo proporcionado durante las actividades.

La evaluación del realismo de los laboratorios muestra que el 53 % de los participantes considera que los laboratorios representan adecuadamente casos reales de ataque, mientras que el 47 % restante se mantiene en una posición neutral. En cuanto al material de apoyo, se observa que el 60 % de los estudiantes valora positivamente las instrucciones, pistas y contexto proporcionados, frente a un 33 % que se muestra neutral y un 7 % que expresa insatisfacción.

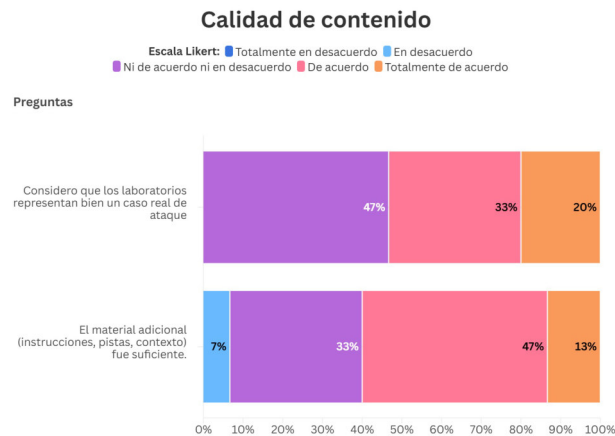


Figura 4.6: Gráfico sobre el contenido de la aplicación

4.2.6. Evaluación del aprendizaje percibido

La Figura 4.7 muestra la percepción de los estudiantes respecto a los aprendizajes alcanzados y la relevancia formativa de la plataforma CyberAcademy, evaluada mediante una escala tipo Likert. Este indicador permite examinar la autoevaluación del progreso cognitivo de los participantes, así como la correspondencia entre los contenidos trabajados y sus intereses formativos o profesionales.

El análisis de los datos muestra que el 67 % de los estudiantes declara haber adquirido nuevos conocimientos a través de la plataforma, mientras que un 60 % reporta que los laboratorios contribuyeron al refuerzo de aprendizajes previos. Asimismo, el 60 % de los encuestados considera que los contenidos abordados guardan relación con sus intereses profesionales, y un 67 % manifiesta interés en seguir profundizando en temáticas de ciberseguridad.

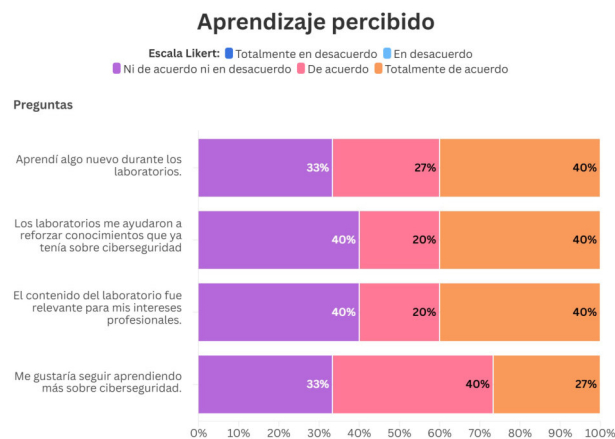


Figura 4.7: Gráfico sobre el aprendizaje percibido por los estudiantes

4.2.7. Evaluación de la preferencia de los laboratorios

La Figura 4.8 presenta la distribución de preferencias de los estudiantes en relación con los tres tipos de laboratorios implementados en CyberAcademy, representada mediante un gráfico de barras que compara la frecuencia de elección de cada modalidad. Este indicador permite identificar la percepción de utilidad práctica que los participantes asignan a cada tipo de laboratorio dentro del proceso de aprendizaje.

Los resultados muestran que 12 de los 15 estudiantes (80 %) seleccionaron el laboratorio de phishing como el más útil, mientras que 2 participantes (13 %) optaron por el laboratorio de DDoS, y ninguno eligió el laboratorio de gusanos (worms). Esta disparidad significativa en las preferencias evidencia variaciones sustanciales en la percepción de valor entre los diferentes tipos de ejercicios.

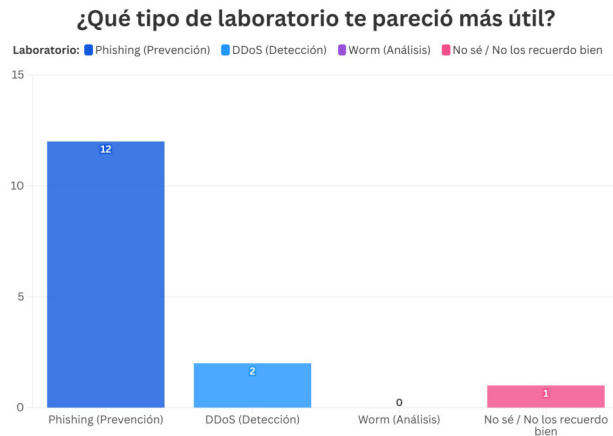


Figura 4.8: Gráfico de preferencia de laboratorio según los estudiantes

4.2.8. Evaluación de datos internos de CyberAcademy

En esta sección se presentan los datos recopilados por la aplicación mediante una API, con el objetivo de realizar un análisis más específico que pueda servir como recurso para los docentes en la evaluación de la dedicación y progreso de cada estudiante en cada laboratorio. Los resultados se detallan en la siguiente tabla 4.2 para facilitar su interpretación y comparación. A continuación, se describen las columnas incluidas en el conjunto de datos, junto con su significado operativo y valor analítico:

- **typeLab:** Indica la categoría del laboratorio ejecutado por el estudiante en un intento determinado (por ejemplo, *phishing*, *DDoS* o *worm*).
- **subInstanceId:** Identificador único de la subinstancia del laboratorio correspondiente al intento realizado por el estudiante.
- **try:** Representa el número acumulativo de intentos efectuados por el mismo estudiante en un laboratorio del mismo tipo.
- **score:** Puntaje obtenido por el estudiante en el intento específico del laboratorio.
- **time:** Duración total del intento, expresada en segundos, calculada como la diferencia entre el tiempo de inicio y el de finalización de la actividad.
- **studentId:** Identificador único asignado al estudiante dentro del sistema de la aplicación.
- **createdAt:** Marca temporal que registra el momento exacto en que el estudiante inició la ejecución del laboratorio.

typeLab	subInstanceId	try	score	time	studentId	createdAt
phishing	1	1	3	222	32	2025-05-20 14:50:39.873368
phishing	1	1	2	228	26	2025-05-20 14:50:29.405026
phishing	1	1	1	231	17	2025-05-20 14:52:38.247969
phishing	1	1	3	235	16	2025-05-20 14:52:22.171969
phishing	1	1	3	239	20	2025-05-20 14:51:07.096805
phishing	1	1	3	241	30	2025-05-20 14:50:37.901401
phishing	1	1	1	245	36	2025-05-20 14:57:10.283602
phishing	1	1	2	248	29	2025-05-20 14:50:41.672667
phishing	1	1	2	252	25	2025-05-20 14:50:29.041883
phishing	1	1	1	255	22	2025-05-20 14:56:10.412861
phishing	1	1	1	259	23	2025-05-20 14:56:09.006455
phishing	1	1	1	263	24	2025-05-20 14:51:36.583369
phishing	1	1	2	267	31	2025-05-20 14:50:58.847884
phishing	1	1	3	272	28	2025-05-20 14:51:28.285493
phishing	1	1	1	278	33	2025-05-20 14:50:44.844402
DDOS	1	1	2	321	16	2025-05-20 15:02:36.722829
DDOS	1	1	0	334	36	2025-05-20 15:02:37.81785
DDOS	1	1	2	342	20	2025-05-20 15:02:43.297232
DDOS	1	1	1	355	25	2025-05-20 15:02:43.957422
DDOS	1	1	0	363	17	2025-05-20 15:02:57.3002
DDOS	1	1	1	371	30	2025-05-20 15:03:14.024071
DDOS	1	1	1	378	31	2025-05-20 15:03:23.069143
DDOS	1	1	2	386	29	2025-05-20 15:03:26.570801
DDOS	1	1	1	395	26	2025-05-20 15:03:46.052724
DDOS	1	1	2	404	22	2025-05-20 15:03:56.868359
DDOS	1	1	1	412	33	2025-05-20 15:03:57.754226
DDOS	1	1	0	419	23	2025-05-20 15:04:00.6325
DDOS	1	1	2	425	36	2025-05-20 15:06:01.704112
DDOS	1	1	1	433	24	2025-05-20 15:06:20.773538
DDOS	1	1	2	420	28	2025-05-20 15:05:40.547277
worm	1	1	1	452	24	2025-05-20 15:08:41.670347
worm	1	1	4	465	36	2025-05-20 15:08:59.694174
worm	1	1	3	478	25	2025-05-20 15:09:30.240798
worm	1	1	4	484	30	2025-05-20 15:09:58.144162
worm	1	1	0	491	16	2025-05-20 15:10:45.870756
worm	1	1	3	499	20	2025-05-20 15:10:50.317796
worm	1	1	3	507	22	2025-05-20 15:11:54.360071
worm	1	1	4	516	39	2025-05-20 15:17:28.387615
worm	1	1	3	522	26	2025-05-20 15:10:45.870757
worm	1	1	0	535	29	2025-05-20 15:10:50.317797
worm	1	1	1	543	32	2025-05-20 15:11:54.360072
worm	1	1	1	558	28	2025-05-20 15:17:28.387616
worm	1	1	4	565	31	2025-05-20 15:10:45.870758
worm	1	1	2	577	33	2025-05-20 15:10:50.317798
worm	1	1	3	589	23	2025-05-20 15:11:54.360073
phishing	2	2	4	205	26	2025-05-20 15:20:33.703670
phishing	2	2	4	210	20	2025-05-20 15:21:33.370368
phishing	3	2	3	215	29	2025-05-20 15:18:25.987654
phishing	2	2	4	220	23	2025-05-20 15:21:13.703702
phishing	3	2	3	225	31	2025-05-20 15:20:43.036703
phishing	3	2	2	230	33	2025-05-20 15:18:05.123456
DDOS	3	2	2	310	16	2025-05-20 15:21:23.037035

DDOS	3	2	2	320	30	2025-05-20 15:20:13.037034
DDOS	2	2	2	330	25	2025-05-20 15:18:55.109876
DDOS	2	2	2	340	28	2025-05-20 15:21:03.670369
DDOS	3	2	2	350	33	2025-05-20 15:20:23.370367
DDOS	2	2	2	360	20	2025-05-20 15:18:35.012345
worm	2	2	3	420	36	2025-05-20 15:20:03.703701
worm	2	2	3	430	17	2025-05-20 15:21:43.703701
worm	3	2	4	440	24	2025-05-20 15:18:15.654321
worm	3	2	4	450	22	2025-05-20 15:20:53.367036
worm	2	2	4	460	32	2025-05-20 15:21:53.037034
worm	3	2	4	470	26	2025-05-20 15:18:45.543210

Tabla 4.2: Datos recopilados por la aplicación CyberAcademy

4.3. Análisis de Resultados

4.3.1. Análisis de dedicación de los estudiantes

Las Figuras 4.11, 4.12a y 4.12b presentan un análisis comparativo de los tiempos de ejecución requeridos por los estudiantes para completar los diferentes laboratorios de CyberAcademy, distribuidos por tipo de ejercicio y número de intento. Los gráficos de caja permiten visualizar la distribución, dispersión y valores atípicos del tiempo invertido en cada escenario, proporcionando una visión valiosa sobre la complejidad percibida y la curva de aprendizaje. Las Figuras 4.9 y 4.10 complementan este análisis, detallando los tiempos medios y la desviación estándar, respectivamente.

La Figura 4.12a (Intento 1), junto con los datos de la Figura 4.9, muestra que los laboratorios de Phishing presentan la menor dedicación temporal media, con 249 segundos, y una desviación estándar baja (16.7) (Figura 4.10), lo que indica una dificultad ajustada y consistente para los estudiantes. Los laboratorios de DDOS exhiben una distribución más amplia y asimétrica, con una media de 377 segundos y una mayor desviación (35.4), reflejando diferencias individuales en la comprensión de los conceptos de detección de tráfico malicioso. Por su parte, los laboratorios de Worm concentran los tiempos más elevados, con una media de 520 segundos y la dispersión más alta (41.7) lo que sugiere la naturaleza compleja del análisis de amenazas de red requerido.

Esta jerarquía temporal se mantiene en la Figura 4.12b (Intento 2), donde se observan reducciones generalizadas en los tiempos de ejecución: Phishing presenta una media de 218 segundos y una desviación de 9.4, lo que representa una mejora del 12 % respecto al primer intento y evidencia una rápida familiarización con la mecánica de juego del laboratorio; DDOS muestra una media de 335 segundos y una desviación de 18.7, la mejora más pronunciada con un 15 % de reducción temporal, lo que indica una efectiva asimilación de técnicas de monitoreo de saturación de la red; y Worm tiene una media de 445 segundos y una desviación de 18.7, con una mejora del 10 %, confirmando que, aunque persiste la complejidad, los estudiantes desarrollaron habilidades analíticas más efectivas.

La Figura 4.11 consolida ambos intentos, revelando que las medias globales de tiempo de dedicación (Figura 4.9) son de 233.5 segundos para Phishing, 356 segundos para DDOS, y 482.5 segundos para Worm. En cuanto a la dispersión total (Figura 4.10), los valores son 20.7 para Phishing, 38.4 para DDOS y 49.7 para Worm. La baja desviación total en Phishing confirma una distribución simétrica y homogénea, donde la mayoría de estudiantes mostró desempeños similares. En DDOS y, especialmente, en Worm, las desviaciones superiores indican una mayor heterogeneidad en el abordaje de estos laboratorios más complejos. Esta relación valida la progresión coherente de dificultad entre los tres tipos de laboratorios y la fiabilidad de las métricas obtenidas.

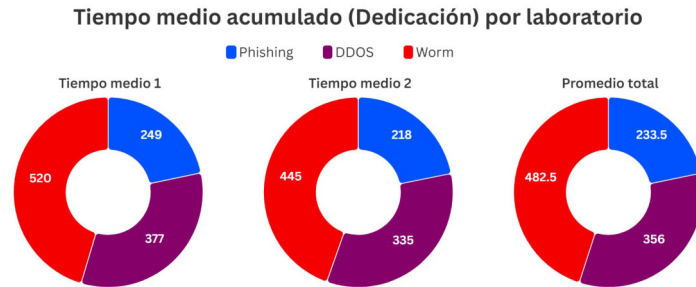


Figura 4.9: Gráficas de Tiempos medios acumulados (Dedicación) por Laboratorio

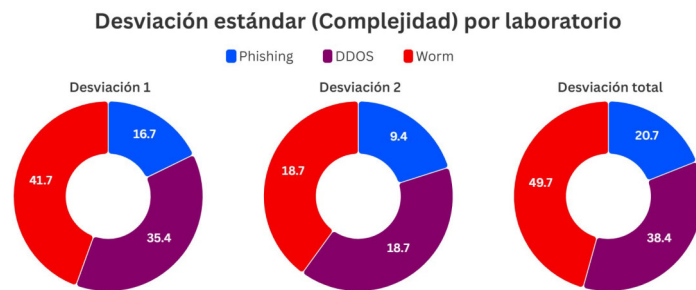


Figura 4.10: Gráficas de Desviación estándar (Complejidad) por Laboratorio

Al correlacionar el grado de utilidad otorgada por cada estudiante al laboratorio seleccionado y los tiempos de ejecución, se demuestra una relación directa. Los laboratorios de Phishing, siendo los más rápidos de completar (media total de 233.5 s), coinciden con los mejor evaluados en términos de usabilidad y claridad. Por el contrario, los laboratorios de Worm, que demandan más del doble de tiempo que los de Phishing (media total de 482.5 s) y exhiben la mayor desviación (49.7), reflejan la complejidad asociada al rastreo de código malicioso y la interpretación de estos hallazgos. La mejora consistente observada entre el primer y segundo intento en todos los laboratorios sugiere una efectiva curva de aprendizaje, siendo más pronunciada en DDOS (15 % de reducción temporal), lo que indica que la plataforma facilita la adquisición progresiva de competencias. Estas métricas temporales proporcionan una validación cuantitativa de los desafíos identificados cualitativamente y refuerzan la necesidad de ajustes instruccionales en los laboratorios de mayor complejidad.

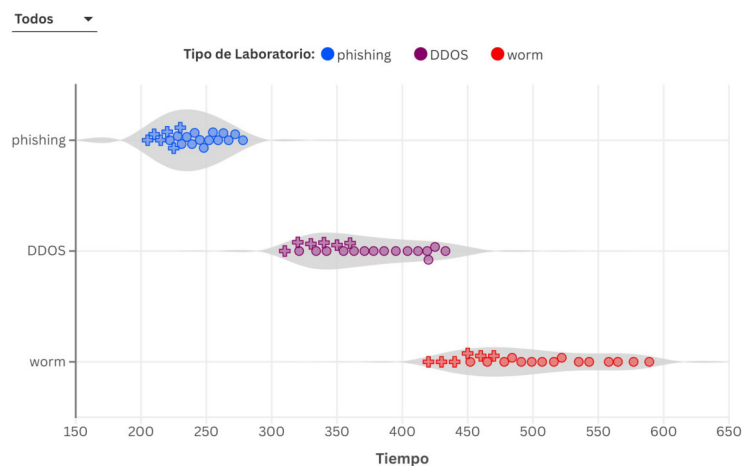


Figura 4.11: Gráfico de tiempo de finalización en segundos según el tipo de laboratorio, todos los intentos

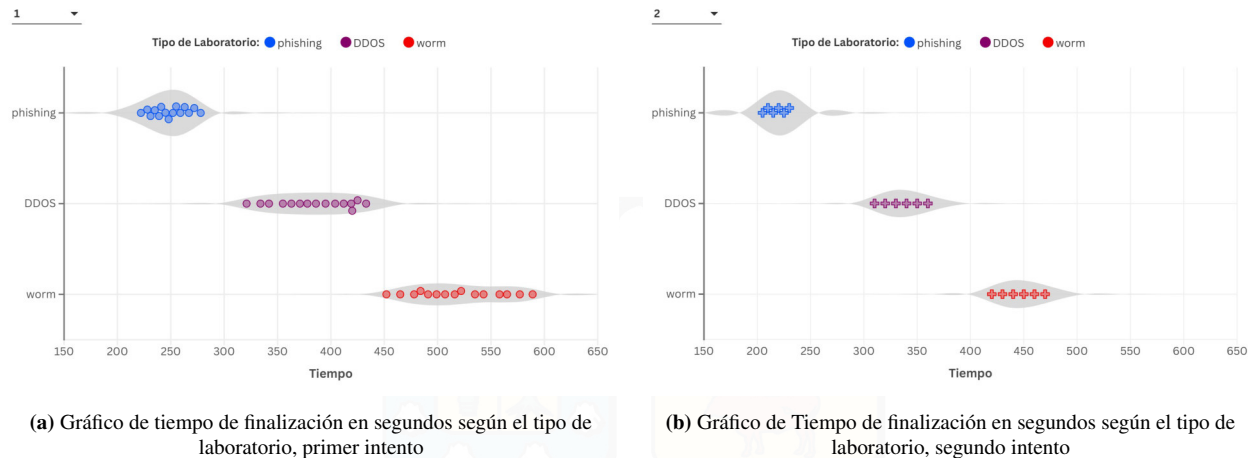


Figura 4.12: Gráficos de Tiempo de finalización en segundos según el tipo de laboratorio e intento

4.3.2. Análisis de progreso de los estudiantes

La Figura 4.14 expone la distribución de puntajes obtenidos por los estudiantes en las diferentes instancias del laboratorio de phishing, DDOS y worm, utilizando una escala de 0 a 4 puntos. El gráfico de barras agrupadas permite visualizar la frecuencia de cada puntuación para las tres instancias evaluadas de cada laboratorio (por ejemplo, phishing - 1, phishing - 2 y phishing - 3). La Figura 4.13 complementa este análisis, ilustrando la distribución porcentual de las puntuaciones obtenidas por tipo de laboratorio mediante gráficos de radar.

Para la instancia Phishing - 1, los datos muestran una distribución relativamente equilibrada: el 40 % de los estudiantes (6/15) obtuvo 1 punto, el 26.7 % (4/15) alcanzó 2 puntos, y el 33.3 % (5/15) logró 3 puntos. Ningún estudiante obtuvo puntuaciones mínimas (0) o máximas (4), indicando un primer acercamiento a este tipo de laboratorios, tal como se refleja en el radar de Phishing (Figura 4.13), donde las frecuencias más altas se encuentran en los puntajes 1, 2 y 3. En contraste, la instancia Phishing - 2 presenta un rendimiento notablemente superior, donde el 100 % de los estudiantes (3/3) alcanzó la puntuación máxima de 4 puntos. Esta mejora sugiere una efectiva curva de aprendizaje o una mejor adaptación de la mecánica de juego del laboratorio. La instancia Phishing - 3 muestra una distribución más concentrada: el 33.3 % (1/3) obtuvo 2 puntos y el 66.7 % (2/3) logró 3 puntos, manteniéndose en rangos intermedios-altos pero sin alcanzar el máximo.

En la instancia DDoS - 1, se observa una distribución dispersa, evidenciada en el radar de DDoS (Figura 4.13) por una alta concentración en el puntaje 2 y un notable pico en el puntaje 1: 20 % (3/14) en puntaje 0, 40 % (6/14) en puntaje 1, y 40 % (6/14) en puntaje 2. Esta variabilidad inicial sugiere una dificultad significativa en la comprensión de los conceptos de detección de ataques DDoS. Sin embargo, las instancias posteriores muestran una mejora significativa: en DDoS - 2 y DDoS - 3, el 100 % de los estudiantes (3/3 en cada caso) alcanza puntaje 2, indicando una efectiva consolidación de las habilidades de análisis de tráfico y reconocimiento de patrones de ataque.

En Worm - 1, la distribución es amplia, como lo indica el radar de Worm (Figura 4.13), que muestra puntajes distribuidos desde el 0 hasta el 4: 13.3 % (2/15) en puntaje 0, 20 % (3/15) en puntaje 1, 6.7 % (1/15) en puntaje 2, 33.3 % (5/15) en puntaje 3, y 26.7 % (4/15) en puntaje 4. Esta dispersión refleja la naturaleza compleja del análisis de amenazas de red que es requerido por el laboratorio a primeras impresiones. No obstante, las instancias Worm - 2 y Worm - 3 muestran una notable mejora: en Worm - 2, 66.7 % (2/3) logra puntaje 3 y 33.3 % (1/3) puntaje 4; en Worm - 3, el 100 % (3/3) alcanza la máxima puntuación, demostrando una excelente asimilación de las técnicas de investigación digital. Los radares de DDOS y Worm confirman que, a diferencia de Phishing, donde las puntuaciones son más altas y concentradas, estos laboratorios presentan una mayor dispersión inicial y requieren instancias posteriores para que los estudiantes desarrollen la competencia en alto grado.



Figura 4.13: Gráficas de la distribución de Frecuencias de Puntajes por Laboratorio (Radar)

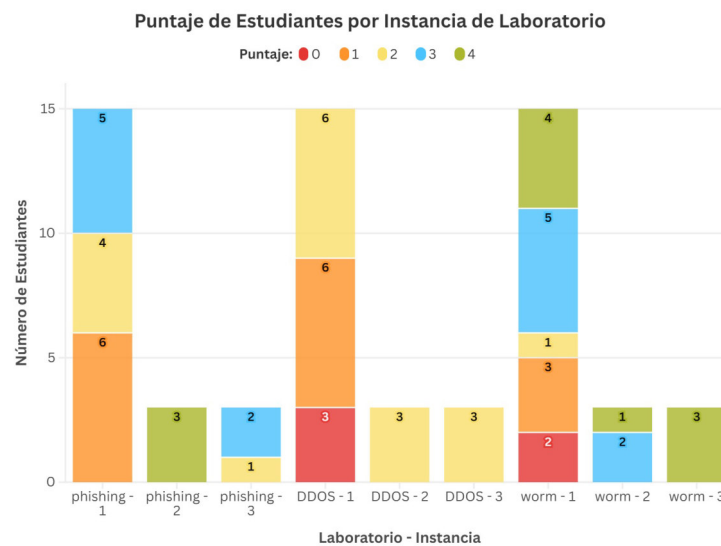


Figura 4.14: Gráfico de Puntaje de Estudiantes por Instancia de Laboratorio

4.3.3. Discusión de los resultados

Los hallazgos obtenidos demuestran que CyberAcademy posee un potencial significativo para la formación en ciberseguridad de estudiantes de secundaria técnico profesional, validación que se sustenta en cuatro dimensiones críticas analizadas a continuación: la usabilidad del sistema, la coherencia del flujo pedagógico, la calidad del contenido y, fundamentalmente, el progreso medible en el aprendizaje.

La efectiva integración de la metodología Cyber Kill Chain de LockHeed Martin se manifestó no solo en la estructura pedagógica (secuencia de pasos considerada coherente por el 80 % de los participantes), sino en los resultados concretos de aprendizaje. La progresión desde el laboratorio de Phishing (donde el 100 % de los estudiantes alcanzó puntajes altos en segundas instancias) hacia los laboratorios más complejos de DDoS y Worms (que mostraron mejoras del 15 % en tiempos de ejecución y 100 % de efectividad en terceras instancias, respectivamente), evidencia una asimilación progresiva de competencias alineada con las fases de un ciberataque real.

La valoración positiva en usabilidad con un 74 % de aprobación en claridad de interfaz y 73 % en navegación intuitiva constituye un factor clave para la adopción tecnológica en contextos educativos técnico profesionales, donde la accesibilidad práctica es fundamental. Esta usabilidad es crucial para sortear la brecha de conocimientos previos

observada, ya que si bien un 87 % de los estudiantes maneja el uso básico de computadores, solo el 66 % comprende conceptos fundamentales de redes como IP o DNS, y únicamente el 60 % había recibido formación previa. La alta aceptación en legibilidad de textos (80 %) y la coherencia del flujo de trabajo (80 % de acuerdo) compensaron estas limitaciones de base, permitiendo una experiencia de aprendizaje guiada.

Sin embargo, la disparidad en la preferencia de laboratorios (80 % de selección por Phishing frente al 0 % por Worms) señala la necesidad de un enfoque diferenciado según la complejidad técnica. Los datos temporales revelan que esta brecha no responde necesariamente a deficiencias conceptuales, sino a la carga cognitiva y esfuerzo que se traduce en un tiempo de dedicación significativamente mayor: una mediana de 475 segundos para Worms, en comparación con los 230 segundos para Phishing. Este mayor esfuerzo se reflejó también en la valoración del contenido, donde el 53 % considera que los laboratorios representan adecuadamente casos reales (lo que indica un amplio espacio para mejorar la contextualización), y el 60 % aprueba el material de apoyo (instrucciones, pistas, etc.). Esto explica que la preferencia se incline hacia el Phishing debido a la familiaridad con esta amenaza, frecuente en la vida cotidiana, a diferencia de los gusanos, asociados a contextos técnicos más avanzados.

Los resultados en aprendizaje percibido (67 % adquisición de nuevos conocimientos, 60 % reforzamiento de previos) se correlacionan directamente con las métricas de desempeño, particularmente en la curva de aprendizaje acelerada observada en DDoS y Worms. Este fenómeno sugiere que, aunque inicialmente complejos, estos laboratorios lograron desarrollar competencias técnicas sólidas mediante la práctica iterativa, respaldando la efectividad del diseño pedagógico. La ligera demora reportada por el 14 % de los usuarios en el tiempo de respuesta del sistema, aunque minoritaria, es un punto de optimización a considerar para mejorar la percepción de rendimiento técnico (67 % de evaluación positiva).

Finalmente, la motivación de los estudiantes (67 % de interés en continuar aprendiendo y 60 % de relevancia profesional percibida) surge como un resultado de igual relevancia que los indicadores cognitivos. Esta disposición activa, observada tanto en los estudiantes como en el docente, refleja un escenario oportuno para impulsar nuevos proyectos formativos. Estos deben orientarse no solo a fortalecer competencias para la vida laboral, sino a consolidar los hábitos de protección digital en la vida cotidiana, especialmente considerando el alto interés inicial (80 % activo en aprender sobre protección digital) que justifica plenamente la inversión en este tipo de herramientas educativas.

4.3.4. Limitaciones y Oportunidades de Mejora

Entre las limitaciones del estudio destaca el tamaño reducido de la muestra: solo 15 alumnos participaron en la evaluación. Esto impone restricciones a la generalización estadística de los resultados y motiva la necesidad de repetir la prueba con grupos más amplios y diversos.

Otro aspecto importante es la diferencia en la acogida de los laboratorios: mientras el 80 % de los estudiantes valoró positivamente el laboratorio de phishing, la aceptación fue mucho menor para DDoS (13 %) y nula para el de gusanos (worms) (0 %). Esta brecha podría atribuirse a la “limitada contextualización práctica” de los ataques más complejos y a su “mayor complejidad técnica”. En consecuencia, las oportunidades de mejora se centran en reforzar el contexto y el apoyo pedagógico en estos casos: por ejemplo, incluir ejemplos más claros de la vida real y simplificar los pasos técnicos (o explicar mejor los comandos) en los laboratorios de DDoS y gusanos (worms).

La evaluación puso de manifiesto que una fracción importante de los alumnos partió sin experiencia en ciberseguridad. Los resultados señalan que “el 60 % de los estudiantes declaró que aprendió antes algo de ciberseguridad incluso fuera del colegio”. Esta carencia contribuyó a las dificultades observadas en los laboratorios más técnicos, ya que los participantes sin conocimientos previos encontraban más abstracto el análisis de tráfico y el uso de comandos. Por lo tanto, se sugiere reforzar los fundamentos de seguridad antes de los laboratorios prácticos: por ejemplo, introducir un módulo inicial que cubra conceptos básicos (como tipos de ataques o fundamentos de redes) ayudaría a nivelar la base de conocimientos de todos los estudiantes y facilitaría su desempeño en los laboratorios avanzados.

5 | CAPÍTULO 5: CONCLUSIONES

CyberAcademy responde a la crítica carencia de herramientas en español para el desarrollo de habilidades prácticas en ciberseguridad en la educación técnico-profesional. La evaluación con 15 estudiantes de educación secundaria demostró una acogida mayoritariamente positiva: el 70 % de los participantes encontró la interfaz clara y fácil de navegar, mientras que el 67 % adquirió nuevos conocimientos y el 60 % reforzó aprendizajes previos. La plataforma, basada en laboratorios interactivos de phishing, DDoS y worm, demostró efectividad comprobada no solo en la adquisición de conocimientos sino también en la motivación generada, con un 67 % de los estudiantes expresando interés en profundizar su formación en ciberseguridad. Estos resultados validan su capacidad para generar aprendizaje significativo y motivación sostenida desde la perspectiva de los usuarios.

La integración del modelo Cyber Kill Chain de Lockheed Martin como estructura pedagógica central evidenció una progresión formativa medible a través de métricas cuantitativas concretas. En el laboratorio de phishing, alineado con las fases iniciales de prevención, los estudiantes mostraron un desempeño consistentemente alto con el 100 % alcanzando puntajes máximos en segundas instancias y una media temporal de 234 segundos. El laboratorio de DDoS, correspondiente a fases intermedias de detección, exhibió una curva de aprendizaje más pronunciada con mejoras del 15 % en tiempos de ejecución entre intentos y una progresión desde puntajes iniciales dispersos (21.4 % en nivel 0) hacia consistentes puntajes de 2 puntos. Finalmente, el laboratorio de worm mostró la evolución más significativa, comenzando con una distribución amplia de puntajes (13.3 % con puntaje 0, 26.7 % con puntaje 4) y culminando con el 100 % de efectividad en la tercera instancia, a pesar de requerir los mayores tiempos de ejecución (mediana de 475 segundos). En esta perspectiva, CyberAcademy transforma conceptos abstractos en competencias prácticas concretas mediante un enfoque pedagógico progresivo y medible.

5.1. Trabajo Futuro

El trabajo futuro para CyberAcademy se centrará en cuatro ejes estratégicos interconectados:

- **Validación expandida:** Extensión de la plataforma a un mayor número de instituciones de educación secundaria técnico-profesional para consolidar los resultados iniciales y optimizar los laboratorios existentes.
- **Fortalecimiento del marco pedagógico:** Validación rigurosa de la efectividad del modelo Cyber Kill Chain en el progreso de aprendizaje estudiantil en distintos contextos educativos.
- **Herramientas docentes:** Desarrollo de sistemas avanzados de monitoreo, configuración y retroalimentación que faciliten una supervisión más detallada y una intervención pedagógica oportuna por parte del docente.
- **Diversificación de contenido:** Incorporación progresiva de nuevos escenarios de ataque alineados con los planes de estudio vigentes, para enriquecer la experiencia de aprendizaje.

BIBLIOGRAFÍA

- Abusaimh, H. (2020). Virtual machine escape in cloud computing services. *International Journal of Advanced Computer Science and Applications*, 11(7).
- Al-Sada, B., Sadighian, A., & Oligeri, G. (2023). Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database. *IEEE Access*, PP, 1-1. <https://doi.org/10.1109/ACCESS.2023.3344680>
- ANCI. (2023, junio). *Documento DD-2777819-250603 P* (Technical Report). ANCI – Agencia Nacional de Ciberseguridad, Chile. https://anci.gob.cl/documents/4712/DD_2777819_250603_P.pdf
- ANCI. (2025). ANCI – Agencia Nacional de Ciberseguridad [Organismo técnico público para fiscalizar, regular y promover la ciberseguridad en Chile]. <https://anci.gob.cl>
- Banco Interamericano de Desarrollo, Organización de los Estados Americanos & Universidad de Oxford. (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe [Publicado bajo licencia Creative Commons IGO 3.0 BY-NC-ND]. <https://www.observatoriociberseguridad.com>
- BCN. (2023). *Construyendo la ciberseguridad en Chile: Una mirada desde el ecosistema 2.0 (2ª ed.)* (Technical Report). Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/89176/4/Construyendo_la_Ciberseguridad_en_chile_2ed_V2.pdf
- Buchanan, L., Scarlatos, L., & Telendii, N. (2021). Curriculum to Broaden Participation in Cybersecurity for Middle School Teachers and Students. *2021 IEEE Integrated STEM Education Conference (ISEC)*, 63-70. <https://doi.org/10.1109/ISEC52395.2021.9763930>
- Burn, J. (2023, diciembre). The Forrester Wave™: Cybersecurity Skills And Training Platforms, Q4 2023 [(Wave™ Report N.º RES178480). (Evaluación basada en 21 criterios sobre proveedores de plataformas de formación en ciberseguridad). Forrester Research, Inc.]. <https://reprints2.forrester.com/%5C#/assets/2/2565/RES178480/report>
- Du, W. (2025). SEED Project: Hands-on Labs for Security Education [SEED Security Labs]. <https://seedsecuritylabs.org/>
- e-Governance Academy Foundation. (2025, septiembre). National Cyber Security Index: Chile [Informe actualizado el 30 de septiembre de 2025]. <https://ncsi.ega.ee/>
- Epic Games. (2025). Unreal Engine [Consultado en 2025-09-23]. <https://www.unrealengine.com/es-ES>
- Godot Engine Community. (2025). Godot Engine [Consultado en 2025-09-23]. <https://godotengine.org/es>
- Gregory, J. (2018). *Game Engine Architecture* (3.ª ed.). CRC Press.
- Hack The Box. (2025). Hack The Box: The 1 Cybersecurity Performance Center [Plataforma líder en laboratorios y formación práctica en ciberseguridad]. <https://www.hackthebox.com/>
- Hajgude, J., & Ragha, L. (2012). “Phish mail guard: Phishing mail detection technique by using textual and URL analysis”. *2012 World Congress on Information and Communication Technologies*, 297-302. <https://doi.org/10.1109/WICT.2012.6409092>
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research*, 1(1), 80-106. <https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf>
- IBM. (2025). ¿Qué es la ciberseguridad? [Consultado el 21 de mayo de 2025]. <https://www.ibm.com/es-es/topics/cybersecurity>
- ITU. (2024). *Global Cybersecurity Index 2024* (inf. téc.) (Accedido en: 2025-06-30). ITU. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx>
- Kidd, C. (2024, octubre). Cybersecurity Frameworks: What They Are & How to Use Them [Consultado el 28 de mayo de 2025]. https://www.splunk.com/en_us/blog/learn/cybersecurity-frameworks.html

- Ministerio de Educación de Chile. (2015a, octubre). *Programa de Estudio: Especialidad Conectividad y Redes (Formación Diferenciada Técnico-Profesional, 3.º y 4.º medio)* (Technical Report) (Decreto Exento n.º 0954/2015; ISBN 978-956-292-517-4). Ministerio de Educación de Chile, Unidad de Currículum y Evaluación. https://www.curriculumnacional.cl/sites/default/files/newtenberg/614/articles-34335_programa.pdf
- Ministerio de Educación de Chile. (2015b, octubre). *Programa de Estudio: Especialidad Programación (Formación Diferenciada Técnico-Profesional, 3.º y 4.º medio)* (Technical Report) (Decreto Exento n.º 0954/2015; ISBN 978-956-292-515-0). Ministerio de Educación de Chile, Unidad de Currículum y Evaluación. https://www.curriculumnacional.cl/sites/default/files/newtenberg/614/articles-34336_programa.pdf
- Ministerio de Educación de Chile. (2015c, octubre). *Programa de Estudio: Especialidad Telecomunicaciones (Formación Diferenciada Técnico-Profesional, 3.º y 4.º medio)* (Technical Report) (Decreto Exento n.º 0954/2015). Ministerio de Educación de Chile, Unidad de Currículum y Evaluación. https://www.curriculumnacional.cl/sites/default/files/newtenberg/614/articles-34340_programa.pdf
- Ministerio de Educación de Chile. (2016). Bases Curriculares para Formación Diferenciada Técnico-Profesional [Decreto Supremo de Educación N.º 452/2013]. https://www.curriculumnacional.cl/sites/default/files/newtenberg/614/articles-70892_bases.pdf
- Ministerio del Interior y Seguridad Pública. (2023, diciembre). Decreto Supremo N.º 164: Aprueba Política Nacional de Ciberseguridad 2023–2028 [Publicado en el Diario Oficial de la República de Chile, N.º 43.717]. <https://www.diariooficial.interior.gob.cl/publicaciones/2023/12/04/43717/01/2415658.pdf>
- Ministerio Secretaría General de Gobierno (SEGEGOB) y Ministerio de Educación (MINEDUC). (2024). Plan Ciudadanía y Alfabetización Digital 2025 [Accedido en: 2025-06-27]. <https://www.segegob.gob.cl/media/2024/05/Plan-Ciudadani%CC%81a-y-Alfabetizacio%CC%81n-Digital-2025.pdf>
- Mirkovic, J., & Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2), 39-53.
- National Initiative for Cybersecurity Education (NICE). (2025). NICE Workforce Framework for Cybersecurity (NICE Framework) [Establece un lenguaje común para describir el trabajo y competencias en ciberseguridad; versión actualizada incluye categorías de roles, tareas y áreas de competencia]. <https://niccs.cisa.gov/tools/nice-framework>
- OEA & CISCO. (2023, junio). *Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades* (Technical Report) (América Latina y el Caribe). OEA / CISCO. https://www.oas.org/es/sms/cicte/docs/Reporte_sobre_el_desarrollo_de_la_fuerza_laboral_de_ciberseguridad_en_una_era_de_escasez_de_talento_y_habilidades.pdf
- República de Chile. (2024). Ley N.º 21.663: Ley Marco de Ciberseguridad [Publicada en el Diario Oficial el 8 de abril de 2024]. <https://www.bcn.cl/leychile/navegar?i=1202434>
- Root-Me. (s.f.). Root-Me: Plataforma de Hacking Ético y Retos de Ciberseguridad [Accedido en: 2025-06-29]. <https://www.root-me.org/?lang=es>
- Root-Me Pro. (s.f.). Root-Me Pro: Advanced Ethical Hacking and Cybersecurity Challenges [Accedido en: 2025-06-29]. <https://pro.root-me.org/?lang=en>
- Schneier, B., & Vance, A. (2025). Guest Editorial: “Complexity is the Worst Enemy of Security”: Studying Cybersecurity Through the Lens of Organizational Complexity.
- Scirra Ltd. (2025). Construct [Consultado en 2025-09-23]. <https://www.construct.net/en>
- Subsecretaría de Telecomunicaciones de Chile. (2024, marzo). El 94,3 % de los hogares en Chile declara tener acceso propio y pagado a Internet según datos de la SUBTEL [Información oficial proveniente de la décima encuesta “Acceso, usos y usuarios de Internet en Chile” realizada por SUBTEL y CADEM]. <https://www.subtel.gob.cl/el-943-de-los-hogares-en-chile-declara-tener-acceso-propio-y-pagado-a-internet-segun-datos-de-la-subtel/>
- Talento Digital para Chile. (2022). La urgencia de talento digital [Accedido: 13-12-2025]. <https://talentodigitalparachile.cl/la-urgencia-de-talento-digital/>
- UNICEF Chile y Universidad de Chile. (2022). *Kids Online Chile 2022: Usos, Oportunidades y Riesgos del uso de TIC en NNA de Chile* (inf. téc.) (Accedido en: 2025-06-27). UNICEF. <https://www.unicef.org/chile/media/9376/file/Informe%20kids%20online.pdf>
- Unity Technologies. (2025). Unity [Consultado en 2025-09-23]. <https://unity.com>
- Universidad San Sebastián. (2024). Encuesta Chile Nos Habla: Ciberseguridad [Accedido en: 2025-06-27]. <https://www.uss.cl/noticias/encuesta-chile-nos-habla-ciberseguridad/>
- World Economic Forum. (2025). Global Cybersecurity Outlook 2025 [Accedido en: 2025-06-27]. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

- Yogarajah, J., & Hossain, G. (2025). The Concept of Cognitive CyTutor Utilizing Federated Learning for Cybersecurity Education. *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC)*, 00681-00690. <https://doi.org/10.1109/CCWC62904.2025.10903809>
- YoYo Games. (2025). GameMaker [Consultado en 2025-09-23]. <https://gamemaker.io/en>



A | ANEXOS

A.1. Anexo: Otras funciones de CyberAcademy

A.1.1. Navegación



Figura A.1: Parte 1: Interfaz de navegación principal en CyberAcademy.



Figura A.2: Parte 2: Interfaz de navegación principal en CyberAcademy.

A.1.2. Recursos de Ciberseguridad

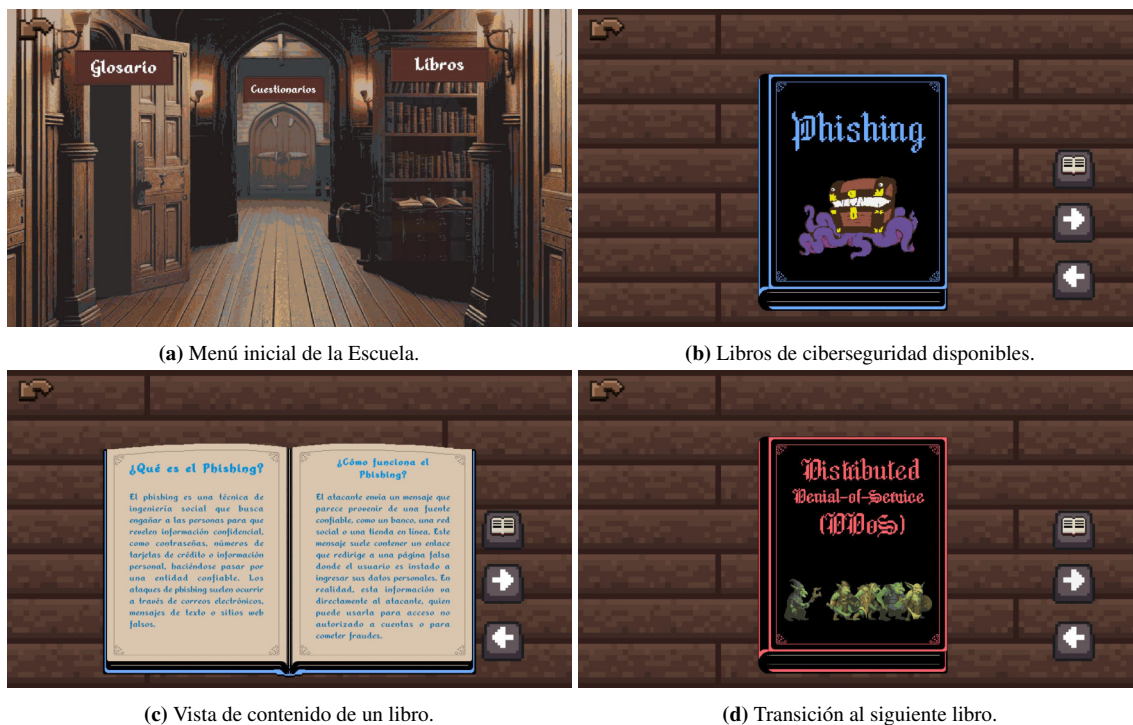


Figura A.3: Parte 1: Recursos educativos de ciberseguridad en CyberAcademy.



Figura A.4: Parte 2: Recursos educativos de ciberseguridad en CyberAcademy.

A.1.3. Personalización



Figura A.5: Menú de la tienda



(a) Casa del caballero: selección de personalización.



(b) Perfil de usuario y logros.



(c) Personalización de interfaz (banner y fondo).



(d) Personalización de la armadura.



(e) Selección de color de la armadura.

Figura A.6: Opciones de personalización disponibles en CyberAcademy.

A.1.4. Minijuegos

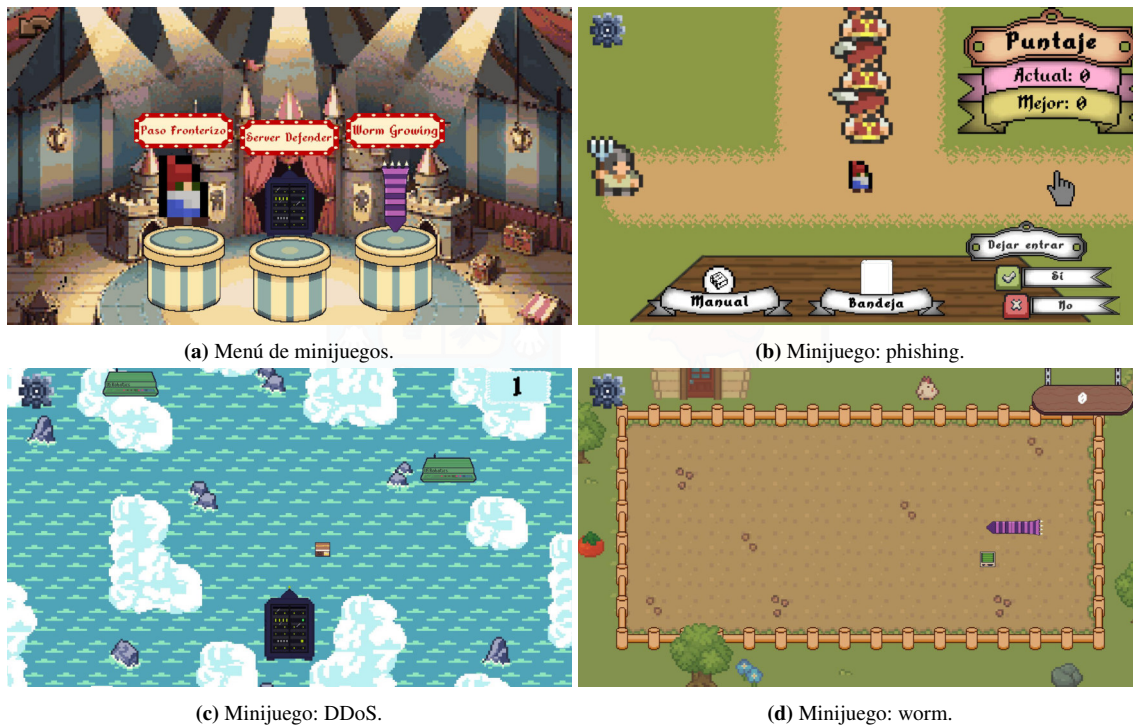


Figura A.7: Sección de minijuegos de CyberAcademy.

A.2. Retroalimentación extra recibidos en la encuesta

A.2.1. ¿Cómo calificarías tu nivel de satisfacción general con Cyber Academy?

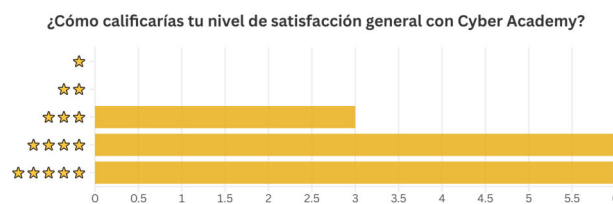


Figura A.8: Gráfico de calificaciones de CyberAcademy

A.2.2. ¿Qué aspecto más te gusto de Cyber Academy?

- La interfaz como un juego
- Todo
- Los juegos
- Los minijuegos
- El tema sobre Phishing

- Todo
- La forma rápida y eficiente de realizar tareas y resolver problemas de ciberseguridad a través de minijuegos creados por la página
- Los juegos
- El juego en general
- La interfaz
- Los mini juegos
- Los juegos
- Los juegos

A.2.3. ¿Qué aspectos te gustaría que se mejoraran o se agregaran en futuras versiones?

- Distintos tipos de ataques como malware
- Nada
- Se congela mucho la pantalla, no sé por qué
- Que haya más objetos en la tienda y más minijuegos
- Ninguna
- Mmm, no sé
- Me gustaría un escenario de cableado estructurado en el que aparezca un virus durante la actividad y enseñar cómo detenerlo
- Que le agreguen más juegos
- Que se bajen los precios en la tienda
- Una explicación de los minijuegos
- Que tengan más variedad de juegos
- Que no todo el juego sea en forma de cuadritos