

CTF en escuelas secundarias 2.0: una plataforma para la organización de competencias de ciberseguridad escolares

Benjamin Freccero Starnari[0009-0005-9640-0168], Claudia
Queiruga[0009-0004-1612-4902], Paula Venosa[0009-0004-0878-5305], Francisco
Javier Díaz[0000-0002-4225-3829]

LINTI - Facultad de Informática UNLP (Universidad Nacional de La Plata) La Plata,
Argentina

benjamin.freccero175916@alumnos.info.unlp.edu.ar, claudiaq, pvenosa,
javierd@{info.unlp.edu.ar}

Resumen. Este artículo se enmarca en las actividades del proyecto "Extensión en vínculo con escuelas secundarias" de la Universidad Nacional de La Plata, cuyo objetivo es promover y debatir la incorporación de la ciberseguridad como área de conocimiento en las escuelas secundarias, específicamente en el área de influencia del proyecto (La Plata, Berisso y Ensenada). La estrategia didáctica empleada consiste en el desarrollo de competencias de ciberseguridad bajo la metodología de juegos conocida como CTF (Captura la Bandera), fomentando el abordaje de estas problemáticas mediante la búsqueda de soluciones a desafíos cognitivos situados, la experimentación de los estudiantes mediante la formulación de conjeturas, la investigación y el trabajo colaborativo. Este trabajo presenta una nueva versión de la herramienta "CTF en escuelas secundarias" orientada a la organización y gestión de competencias de ciberseguridad en las escuelas, promoviendo la autonomía y participación de los equipos escolares. La mejora de la experiencia de usuario es un lineamiento de diseño de esta nueva versión. A su vez, en este trabajo se presenta una primera evaluación de su uso en dos escuelas, en la que se analiza la facilidad de instalación, las dificultades técnicas encontradas y la viabilidad de creación de una competencia de ciberseguridad. La información recopilada de esta evaluación proporciona datos valiosos sobre los requisitos tecnológicos, las implicancias pedagógicas y las mejoras necesarias para una integración fluida en los currículos de la escuela secundaria. Los hallazgos de este trabajo contribuyen a una mejor comprensión de cómo promover la educación en ciberseguridad desde un enfoque práctico, apoyando a los educadores y las instituciones escolares en la adopción de esta metodología didáctica.

Palabras claves: educación en informática, ciberseguridad, CTF, escuelas, software libre, rediseño de software.

CTF in High Schools 2.0: A Platform for Organizing School Cybersecurity Competitions

Abstract. This article is contextualized in the activities carried out in the project "Extensión en vínculo con escuelas secundarias"(Extension in link with high schools) of the UNLP (National University of La Plata), which aims is to make known and discuss the incorporation of Computer Science as a field of knowledge in high schools, specifically in the area of influence of the project (La Plata, Berisso and Ensenada). The didactic strategy employed involves developing cybersecurity competencies through the use of Capture the Flag (CTF) games, encouraging the exploration of these topics through the resolution of situated cognitive challenges, student experimentation, conjecture formulation, research, and collaborative work. This paper presents a new version of the tool "CTF in high schools," designed to support the organization and management of cybersecurity competitions in high schools, promoting autonomy and active participation among school teams. Enhancing the user experience was a key design principle of this new version. Furthermore, the paper includes an initial evaluation of the tool's use in two schools, analyzing aspects such as installation ease, encountered technical difficulties, and the feasibility of creating a cybersecurity competition. The findings from this evaluation provide valuable insights into technological requirements, pedagogical implications, and necessary improvements for a smooth integration into high school curricula. The results of this study contribute to a deeper understanding of how to promote cybersecurity education through a practical approach, supporting educators and educational institutions in adopting this didactic methodology.

Keywords: computer science education, cybersecurity, Capture The Flag (CTF), schools, open-source software, software redesign.

1 Introducción

El trabajo aquí presentado se enmarca en el proyecto “Extensión en vínculo con escuelas secundarias” de la Universidad Nacional de La Plata (UNLP), cuyo objetivo es discutir y visibilizar la Informática como campo de conocimiento en la escuela secundaria, entendiéndola como una disciplina fuertemente vinculada al desarrollo socio-productivo y al ámbito laboral. En este sentido, el proyecto impulsa prácticas educativas basadas en el aprendizaje contextualizado y orientado a la resolución de problemas (Barrows H., 1986) (Hmelo-Silver C.E, 2004), centradas en la construcción de artefactos digitales en sus diversas dimensiones. Una de ellas está relacionada con la ciberseguridad y su articulación con la programación de aplicaciones, el uso de servicios de Internet y la exposición de información personal.

Preguntas como: ¿para qué enseñar ciberseguridad en la escuela secundaria?, ¿qué contenidos son relevantes? y ¿cómo enseñarlos, es decir, con qué estrategias didácticas y materiales?, orientan esta línea de trabajo dentro del proyecto. La estrategia didáctica adoptada se basa en un enfoque de resolución de problemas contextualizados, a través de desafíos o retos de ciberseguridad desarrollados con la metodología conocida como Capture The Flag (CTF). Este enfoque promueve la participación activa de los estudiantes mediante la formulación de conjeturas, la investigación y el trabajo colaborativo. Los desafíos se centran, fundamentalmente, en problemáticas vinculadas con la exposición de datos personales, con el doble propósito de sensibilizar e introducir a los estudiantes en un campo de conocimiento nuevo dentro de las tecnologías digitales: la seguridad informática. Se busca así no solo desarrollar conciencia crítica, sino también abrir la puerta al conocimiento de un área profesional y laboral específica del campo de la informática.

En el marco de esta línea de trabajo del proyecto “Extensión en vínculo con escuelas secundarias”, la metodología CTF se implementa mediante la herramienta “CTF en escuelas secundarias” (Suárez G. et al., 2020) (Suárez G. et al., 2023) (Bolino P. et al., 2021). Este trabajo presenta los avances en el desarrollo de la versión 2.0 de dicha herramienta, a partir del rediseño realizado recientemente (Freccero B. et al., 2024).

2 Herramientas para enseñar ciberseguridad en la escuela

Hoy en día, resulta relevante incorporar la ciberseguridad en las etapas tempranas de la formación de los jóvenes. Por este motivo, es importante contar con plataformas o herramientas que apoyen este proceso. La estrategia Capture The Flag (CTF) es una opción para acompañar la formación en ciberseguridad mediante un enfoque lúdico. Esta metodología de enseñanza resulta atractiva, ya que permite a los participantes aprender divirtiéndose y trabajando en equipo (Leune et al., 2017) (McDaniel et al., 2016).

Si bien existen distintas alternativas para implementar CTFs, pocas herramientas son de software libre y adaptables a escuelas. En la Tabla 1 se describen las

características de un conjunto de herramientas analizadas en el marco del presente trabajo.

Table 1. Herramientas y plataformas para la enseñanza de ciberseguridad. Características.

CTFd	
URL	https://github.com/CTFd/CTFd
Descripción	Plataforma de código fuente abierto diseñada para la creación y gestión de competencias de tipo Capture The Flag (CTF), utilizada ampliamente en contextos educativos y profesionales. Es altamente personalizable y permite a instituciones, docentes o comunidades construir sus propias competencias de ciberseguridad de forma autónoma.
Características	Permite la creación de desafíos personalizados y categorías temáticas. Soporta modos de competencia individual o en equipos, con un sistema de puntuación automática y paneles de clasificación en tiempo real. Es de código abierto y desplegable localmente por el usuario, lo que facilita su adaptación a distintos entornos educativos. Su flexibilidad la convierte en una herramienta ideal para ser adaptada con fines pedagógicos, como en el caso de implementaciones orientadas a escuelas.
Público objetivo	Estudiantes y profesionales.
Enfoque	CTF educativo
Hack The Box	
URL	https://academy.hackthebox.com/
Descripción	Plataforma de aprendizaje online orientada a la formación profesional en ciberseguridad. Combina teoría estructurada con laboratorios prácticos y simulaciones realistas.
Características	Ofrece rutas de aprendizaje progresivas, con contenidos altamente guiados y orientados a la práctica. Cada módulo incluye teoría, ejercicios interactivos, conexión a máquinas virtuales y evaluaciones. Permite al usuario aprender a su propio ritmo, con un enfoque realista. Al finalizar una de estas rutas de aprendizaje, se otorga un certificado.
Público objetivo	Profesionales

Enfoque	Plataforma de aprendizaje on-line para capacitación en ciberseguridad.
PicoCTF	
URL	https://picoctf.org/
Descripción	Plataforma educativa gratuita de tipo Capture The Flag (CTF), desarrollada por la Universidad Carnegie Mellon (https://www.cmu.edu/), orientada principalmente a estudiantes de nivel secundario. Su objetivo es introducir a los jóvenes en el mundo de la ciberseguridad a través de desafíos interactivos, con un enfoque lúdico y progresivo.
Características	Diseñada como una competencia gamificada de ciberseguridad, incorpora desafíos reales de hacking ético presentados en un entorno accesible y amigable. Incluye tutoriales y materiales introductorios para acompañar el aprendizaje de principiantes. Se organiza en torno a eventos anuales, aunque parte del contenido puede explorarse fuera de competencia. No permite la creación de desafíos o competencias propias por parte de los usuarios. Se puede participar individualmente o en equipos.
Público objetivo	Estudiantes especialmente de escuelas secundarias.
Enfoque	CTF educativo
TryHackMe	
URL	https://tryhackme.com/
Descripción	Plataforma online de aprendizaje práctico en ciberseguridad, diseñada tanto para principiantes como para usuarios avanzados. Su enfoque principal es el aprendizaje activo, a través de la interacción con máquinas virtuales y desafíos en tiempo real. Combina contenidos teóricos con laboratorios prácticos en un entorno accesible y gamificado.
Características	Ofrece rutas de aprendizaje temáticas y progresivas con contenido guiado. Incorpora desafíos interactivos, máquinas virtuales y evaluaciones. La plataforma permite crear salas públicas o privadas, aunque solo creadores de contenido pueden publicar contenido abierto. Las salas privadas pueden ser utilizadas por docentes para diseñar actividades personalizadas. Posee un entorno amigable para principiantes, fuerte componente de gamificación y ofrece certificados al completar

	rutas de aprendizaje.
Público objetivo	Profesionales
Enfoque	Plataforma de aprendizaje on-line para capacitación en ciberseguridad.

3 CTF en escuelas secundarias 2.0

En el trabajo de Freccero Starnari B. et al (2024) se plantearon una serie de mejoras destinadas a readaptar la plataforma CTFd para su implementación efectiva en el contexto del proyecto “Extensión en vínculo con escuelas secundarias” y su uso en escuelas secundarias. Estas mejoras surgieron a partir del análisis de las limitaciones detectadas en múltiples instancias de uso en el proyecto, entre las que se identifican: la necesidad de carga manual de los desafíos o retos que los estudiantes deben resolver durante la competencia; los inconvenientes en el proceso de registración de los equipos participantes; y la escasa flexibilidad para que las escuelas, a través de los docentes, intervengan en el armado de la competencia de ciberseguridad tanto en relación a los contenidos de los desafíos y sus niveles de complejidad como en la gestión de la competencia.

A partir de las problemáticas identificadas en la versión 1.0 de “CTF en escuelas secundarias”, que concretamente es una instancia personalizada de la herramienta CTFd¹ (Freccero Starnari B. et al, pp. 3, 2024), se propusieron líneas de diseño centradas en la automatización, la mejora de la experiencia de usuario, y la autonomía de las instituciones escolares para organizar sus propias competencias de ciberseguridad. En la Tabla 2 se describen los lineamientos de diseño de “CTF en escuelas secundarias 2.0”.

Tabla 2. Lineamientos de diseño de “CTF en escuelas secundarias 2.0”.

Meta de diseño	Descripción
Experiencia de usuario	Se pretende mejorar la experiencia del usuario a partir de: <ul style="list-style-type: none"> • Disponer de un acceso directo para unirse a un equipo, evitando tener que recordar el nombre del mismo. • Crear un rol “Autor” orientado a docentes, que facilite la colaboración en la selección de contenidos y la carga de desafíos. Este rol no colisiona con el de administrador de la competencia, pero sí favorece la participación de los docentes en

¹ CTFd es un framework de código fuente abierto orientado a la creación de competencias “Capture The Flag”, centrado en la facilidad de uso y la personalización.
<https://github.com/CTFd/CTFd>

Meta de diseño	Descripción
	la elaboración del contenido. <ul style="list-style-type: none"> • Automatizar la carga de desafíos desde ctfcli.
Autonomía de las escuelas para organizar sus propias competencias CTF	Se pretende que las escuelas logren autonomía en la organización de sus propias competencias CTF, para ello se propone: <ul style="list-style-type: none"> • Dockerizar² esta versión de la herramienta para facilitar su instalación. • Ofrecer un repositorio de desafíos para utilizar y así contar con una base sólida de contenidos sobre ciberseguridad. • Facilitar, a cada escuela, la elaboración de contenido propio de ciberseguridad, a través del nuevo rol “Autor”.

A partir de los lineamientos de diseño definidos se desarrollaron las funcionalidades que los implementan. A continuación se describen y presentan las mismas.

2.1 Funcionalidades que mejoran la experiencia de usuario

La carga de desafíos se identificó como una limitación en la versión 1.0 de la plataforma “CTF en escuelas secundarias” dado que la plataforma CTFd provee una interfaz web en la cual los desafíos deben cargarse uno por uno y en caso de querer crear una nueva instancia para otro CTF, debe repetirse la carga de todos los desafíos. Por ello, en esta nueva versión, se incorpora una funcionalidad que facilita a los usuarios, tanto administradores como contenidistas, la carga masiva de desafíos teniendo en cuenta el tipo de contenido y grado de dificultad. Esta funcionalidad está disponible en la versión 2.0 de la plataforma a partir de un script escrito en Python que usa el comando de ctfcli³ de CTFd.

A modo de ejemplo, en la Fig. 1 se muestra una carga de desafíos de dificultad intermedia sobre la temática Criptografía. Esta carga masiva, donde con un simple comando se cargan 5 desafíos, mejora significativamente los tiempos de preparación de la plataforma para una competencia.

² Dockerizar significa empaquetar una aplicación junto con todo lo que necesita para funcionar (por ejemplo, el sistema operativo, librerías y configuraciones) en un contenedor. Un contenedor es como una “caja” que guarda todo lo necesario para que la aplicación funcione igual, sin importar en qué computadora la ejecutes.

³ ctfcli es una herramienta para la gestión de desafíos de la herramienta CTFd.
<https://github.com/CTFd/ctfcli>

```
bemyi@debian:~/ctfcli$ python3 ctfcli.py instalar ctfcli-challenges/Criptografía intermedio

Installing 'A1 B2 C3' (ctfd-challenges/Criptografía/A1 B2 C3/challenge.yml) ...
Success! All challenges installed!

Installing 'Lenguaje de puntos y rayas' (ctfd-challenges/Criptografía/Lenguaje de puntos
y rayas/challenge.yml) ...
Success! All challenges installed!

Installing 'Espejito espejito' (ctfd-challenges/Criptografía/Espejito espejito/challenge.
yml) ...
Success! All challenges installed!
```

Fig. 1. Carga masiva de desafíos de Criptografía y grado de dificultad intermedia usando un script en Python.

Otra de las mejoras introducidas en esta nueva versión, destinada a los estudiantes que participan de la competencia, es la de “unirse a un equipo”. Para ello, los estudiantes, previamente registrados, disponen de accesos directos a los equipos como se muestra en la Fig. 2. Esta funcionalidad agiliza notablemente el inicio de la competencia, sobre todo cuando se trata de eventos en los que participan muchos equipos, eliminando tiempos de espera y frustraciones al requerir que cada estudiante recuerde el nombre del equipo (esto ocurría en la versión 1.0)

The screenshot shows a web interface for joining a team. On the right, there is a 'Join Team' section with a 'Team Name' input field containing 'Escuela Secundaria Num 2' and a 'Team Password' field with masked characters. A green 'Join' button is at the bottom right of this section. On the left, there is a 'Teams' section with a search bar and a table of teams. The table has columns for 'Team', 'Website', 'Affiliation', 'Country', and 'Actions'. One team is listed: 'Escuela Secundaria Num 2'. A red arrow points from the 'Join' button in the 'Actions' column of this team to the 'Join' button in the 'Join Team' section.

Fig. 2. Unirse al equipo “Escuela Secundaria Num 2”.

En relación al rol “Autor”, introducido en esta versión de la plataforma, la intención es ofrecer a los docentes de las escuelas una participación activa en el uso de la herramienta. Este rol tiene por propósito que el docente sea contenidista sin necesidad de requerir permisos de administración de la plataforma. En la Fig. 3 se muestran las funcionalidades disponibles desde el rol “Autor”, a partir del cual se puede crear, editar y borrar desafíos. Para cada desafío se especifica el área temática a la que corresponde (criptografía, OSINT, etc), los puntos (columna value) que se obtienen al resolver el desafío, el tipo (type) que indica si los puntos que se obtienen son fijos o







dinámicos en función de su resolución por parte de otros equipos y la visibilidad del mismo para la competencia.

Create Challenge

Name:
The name of your challenge

Category:
The category of your challenge

Message:
Use this to give a brief introduction to your challenge.

B I H      



lines: 1 words: 0 0:0

Value:
This is how many points are rewarded for solving this challenge.

Create

Challenges

Q

<input type="checkbox"/>	ID ↕	Name ↕	Category ↕	Value ↕	Type ↕	State ↕
<input type="checkbox"/>	6	A1 B2 C3	Criptografia	50	standard	visible
<input type="checkbox"/>	7	Lenguaje de puntos y rayas	Criptografia	50	standard	visible
<input type="checkbox"/>	8	Espejito espejito	Criptografia	50	standard	visible
<input type="checkbox"/>	9	Se nos corrió el abecedario	Criptografia	50	standard	visible
<input type="checkbox"/>	10	Base 64	Criptografia	50	standard	visible

Fig. 3. Rol Autor: pantallas de carga y edición de desafíos nuevos

En la Tabla 3 se sistematizan las principales características de las funcionalidades incorporadas en la plataforma “CTF escuelas secundarias 2.0” cuyo propósito es mejorar la experiencia del usuario en el uso de la herramienta.

Tabla 3. Funcionalidades implementadas en “CTF en escuelas secundarias 2.0. Mejoras en la experiencia de usuario

Funcionalidad	Consiste en	Se usa	Destinado a
Automatización de la carga de desafíos	Facilitar la carga masiva y organizada de desafíos por categoría de contenido y nivel de dificultad.	Mediante un script en Python que integra la herramienta ctfcli (ofrecida por CTFd)	Organizadores y Contenidistas
Unirse a equipos	Simplificar la incorporación de estudiantes a equipos de la competencia sin necesidad de recordar el nombre del equipo.	Mediante un acceso directo	Estudiantes
Rol Autor	Cargar y gestionar desafíos sin necesidad de contar con privilegios administrativos en la plataforma	Mediante permisos específicos de acceso	Docentes y Contenidistas

2.2 Funcionalidades que ofrecen autonomía a las escuelas para crear competencias CTF

A continuación se describen las funcionalidades desarrolladas en la versión 2.0 de “CTF en escuelas secundarias” orientadas a ofrecer a las escuelas autonomía en la organización de competencias y en general de uso de la herramienta. Como se describió en el trabajo de Freccero Starnari B. et al (2024), en la primera versión de la herramienta, la organización del evento CTF y la elección del contenido se centraliza en el equipo desarrollador de la herramienta. Aunque se dialoga con las escuelas en tanto edades de los estudiantes que participan y nivel de conocimientos previos, las escuelas no influyen por ejemplo en el contenido de los desafíos. Es por ello que se consideró que disponer de una versión de la herramienta, simple de instalar y configurar, aporta autonomía a la escuela tanto para organizar competencias a partir de los recursos que las propias escuelas disponen (computadoras, acceso a Internet) como para seleccionar los contenidos que desean trabajar en cada evento y con qué grupo de estudiantes.

Disponer de un repositorio público de 37 desafíos organizado por los temas considerados relevantes en la campo de la ciberseguridad: criptografía, OSINT,

esteganografía e ingeniería social, es un punto de partida para comenzar a trabajar en ciberseguridad en la escuela. La Fig. 4 se muestra el repositorio público, disponible en <https://github.com/Bemyi/ctfd-challenges/>

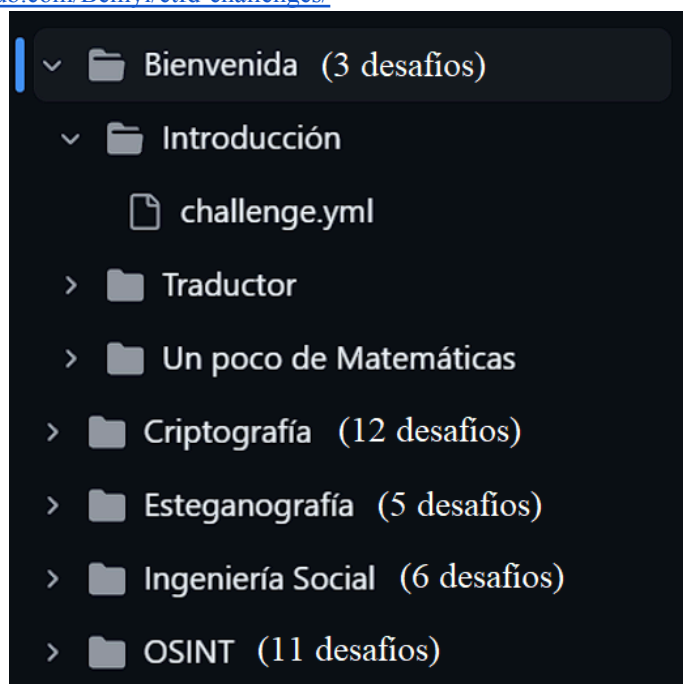


Fig. 4. Repositorio de desafíos de “CTF en escuelas secundarias 2.0”, disponible en <https://github.com/Bemyi/ctfd-challenges/>

En la Tabla 4 se sistematizan las principales características de las funcionalidades incorporadas en la plataforma “CTF escuelas secundarias 2.0” cuyo propósito es ofrecer autonomía a las escuelas para el uso de la herramienta.

Tabla 4. Funcionalidades implementadas en “CTF en escuelas secundarias 2.0”.
Mejoras en la autonomía de las escuelas para el uso de la plataforma

Funcionalidad	Consiste en	Se usa	Destinado a
Dockerización	Facilitar la instalación y puesta en marcha de CTfD en entornos escolares.	Mediante una versión dockerizada que permite desplegar la plataforma con una configuración mínima. No requiere conocimientos	Administradores de laboratorios de computación o de áreas de soporte técnico de las escuelas.

		técnicos. avanzados.	
Repositorio base de desafíos	Disponer de un punto de partida sobre contenidos de seguridad informática para facilitar la creación de la competencia en las escuelas.	Mediante un acceso a un repositorio pública en GitHub [https://github.com/Bemyi/ctfd-challenges/]	Docentes y Contenidistas
Documentación	Disponer de documentación simple sobre la configuración de la plataforma.	Mediante un documento en formato pdf.	Administradores de laboratorios de computación y Docentes

En conjunto, las funcionalidades ofrecidas en esta nueva versión de “CTF en escuelas secundarias” buscan fortalecer una versión libre, accesible y personalizable de CTFd, capaz de adaptarse a las necesidades particulares de la escuela en el nivel secundario, brindando a docentes, estudiantes y equipos de gestión una herramienta útil, de bajo costo de implementación dado que es adaptable a los recursos que dispone la escuela, versátil en tanto puede usarse en otros campos de conocimiento y fundamentalmente adaptable a los contenidos de ciberseguridad que las escuelas deseen enseñar.

4. Evaluación de “CTF en escuelas secundarias 2.0” para la creación de competencias en la escuela

Esta nueva versión de “CTF en escuelas secundarias” fue evaluada por tres docentes de escuelas secundarias técnicas: dos a cargo del dictado la materia “Matemáticas orientadas a la programación”, del Instituto Politécnico Superior General San Martín dependiente de la Universidad Nacional de Rosario (UNR), de la ciudad de Rosario (provincia de Santa Fe) y, uno a cargo del dictado de un taller de “Concientización en Ciberseguridad” de la escuela preuniversitaria de la UNLP “Liceo Víctor Mercante” de la ciudad de La Plata (provincia de Buenos Aires). Se trata de tres docentes varones, con formación en Informática dado que son estudiantes avanzados en carreras universitarias en Informática, dos de ellos de la UNR y el tercero de la UNLP. En este último caso se trata de un estudiante que está realizando su Práctica Profesional Supervisada en el marco del proyecto “Extensión en Vínculos con escuelas secundarias”.

Los tres docentes que participaron de la evaluación de la herramienta no cuentan con experiencia previa en la creación y gestión de un CTF de ciberseguridad con la herramienta “CTF en escuelas secundarias 2.0” ni con otras herramientas para tal fin.

El propósito de la evaluación es relevar información acerca de la experiencia de instalar, configurar y usar la herramienta “CTF en escuelas secundarias 2.0”, para luego realizar las adecuaciones necesarias con el propósito que resulte en una herramienta útil para su uso en las escuelas. Para ello se realizó una sesión de prueba de forma online en la que se requirió a los docentes participantes, que:

- a) Instalen CTF en escuelas secundarias 2.0.
- b) Instalen y configuren la herramienta ctfcli para la carga de desafíos.
- c) Carguen de modo masivo desafíos con el script de Python que integra ctfcli.
- b) Califiquen/caractericen al rol Autor

Al finalizar la sesión de prueba, se administró a los docentes participantes una encuesta semiestructurada, con preguntas de respuesta cerrada y otras abiertas que nos permitieran conocer con más profundidad los motivos de algunas elecciones, específicamente que ayuden a identificar los problemas a los que se enfrentaron los docentes en la instalación y configuración de la herramienta. La misma se estructuró en ocho secciones: datos demográficos, sistema operativo y versión de Python usada para instalar CTF en escuelas secundarias 2.0, instalación de CTF en escuelas secundarias 2.0, instalación y configuración de CTFcli para la carga de desafíos, escritura de comandos en ctfcli, escritura de desafíos en YML, opinión sobre el rol Autor y comentarios generales.

En la Tabla 5 se sintetizan los resultados más relevantes de la encuesta.

Tabla 5. Resultados de la encuesta de evaluación de “CTF en escuelas secundarias 2.0”

Instalación de CTFd adaptado	La experiencia fue valorada como buena o muy buena. Se identificó un conflicto con la versión usada de Python.
Instalación y configuración de ctfcli	La experiencia fue valorada como buena o muy buena. Se identificaron algunos errores al conectar ctfcli con la instancia de CTFd, al cargar o modificar los desafíos y con alguna versión de Python (Python 3.7). La falta de feedbacks ante errores de instalación de ctfcli, la escasa documentación sobre cómo usar ctfcli y la falta de detalles, fueron los problemas descriptos.
Carga masiva de desafíos	La experiencia fue valorada como muy buena. Los docentes participantes pudieron cargar y actualizar desafíos durante la sesión de prueba. Los docentes manifestaron sentirse más

	<p>cómodos con la carga manual de desafíos (ofrecida en CTFd) que la carga automática con ctfcli. Entre las razones se encuentran que sienten más control de la tarea de carga y que les resulta más cómodo, a pesar de ser más lento.</p> <p>La falta de feedbacks de la herramienta (escasos mensajes de error o con falta de detalles), la documentación del instructivo poco clara y escasa documentación respecto de cómo usar los archivos YML para crear desafíos, fueron los problemas identificados con el script para la carga masiva de desafíos.</p>
Caracterización del rol Autor	<p>El rol Autor es valorado positivamente. Entre los argumentos más relevantes se hace referencia a que ofrece a los docentes la posibilidad de gestionar y crear desafíos en la plataforma para un evento determinado, realizar actividades en el aula, analizar las estadísticas de las respuestas (evaluación) y el promedio de intentos por desafíos, e identificar los desafíos que resultaron más difíciles de resolver.</p>

En esta sesión de prueba los docentes participantes usaron computadoras con el sistema operativo Linux y las versiones de Python usadas fueron la 3.7, la 3.10 y la 3.11 o superior.

5. Conclusiones

CTF en escuelas secundarias 2.0 es una herramienta que aporta a la educación en ciberseguridad en las escuelas, desde un enfoque didáctico basado en la resolución de problemas o desafíos con característica de gamificación, es decir, con una dinámica propia de los juegos como la inclusión de reglas, interactividad, retroalimentación, niveles, recompensas, insignias, etc.

La automatización de la instalación de la herramienta mediante un archivo Docker (Docker image), la facilidad de carga masiva de desafíos, categorizados por tema y nivel de dificultad, la disponibilidad de un repositorio público y abierto de desafíos, sumado a la definición de roles con función de contenidista de desafíos para favorecer la participación activa de los docentes en la construcción de competencias CTF, facilitan a los educadores e instituciones escolares la adopción de “CTF en escuelas secundarias 2.0” como metodología didáctica para acercar temas de ciberseguridad al ámbito escolar y ganar autonomía para organizar sus propias competencias.

La primera evaluación de “CTF en escuelas secundarias 2.0” realizada con docentes de dos escuelas secundarias, arrojó resultados alentadores en tanto pudieron instalar la herramienta, cargar y editar desafíos. Se identificaron algunos conflictos con las versiones de Python que resultaron útiles para establecer requerimientos de instalación. En relación a la preferencia de carga manual de desafíos sobre la posibilidad de carga automática y masiva, es posible que se deba a que los docentes al responder esta pregunta consideraron un escenario de una competencia CTF y no en múltiples eventos. Por otro lado, el manual de instalación se actualizó a partir de las devoluciones de los docentes participantes de la evaluación y se agregaron ejemplos para definir desafíos con YML.

A su vez, a partir de los problemas identificados en la primera evaluación se planifica incorporar mejoras en la herramienta y realizar una próxima evaluación con docentes en la que se releve información acerca de los contenidos de ciberseguridad que se enseña en las materias y si participaron u organizaron CTFs previamente.

Referencias

- Barrows H. (1986). Taxonomy of problem-based learning methods. *Medical education*: 20(6), 1986.
- Bolino P., Suárez G., Pretto J., Venosa P. y Queiruga C. (2021). CTFs en escuelas: una plataforma para acercar la ciberseguridad a la educación secundaria. *Actas de las Primeras Jornadas Argentinas de Didáctica de Ciencias de la Computación (JADiCC)*, pp 54-64.
- Hmelo-Silver C.E (2004). Problem-Based Learning: What and How Do Students Learn?. *Educational Psychology*, Vol. 16, N° 3. September 2004, pp. 235-266. <https://doi.org/10.1023/B:EDPR.0000034022.16470.f3>
- Leune Kess, Petrilli Salvatore J. (2017). Using Capture The Flag to enhance to effectiveness of cybersecurity education. Adelphi University, Garden City, New York, SIGITE '17, Rochester, NY, USA, 2017.
- McDaniel L., Talvi E. and Hay B. (2016). Capture the Flag as Cyber Security Introduction," 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA, 2016, pp. 5479-5486, doi: 10.1109/HICSS.2016.677.
- Freccero Starnari B., Suárez G., Queiruga C. y Venosa P. (2024). The CTFd Tool Adapted to Cybersecurity Teaching in Schools. 2024 L Latin American Computer Conference (CLEI), Buenos Aires, Argentina, 2, pp. 1-7, doi: 10.1109/CLEI64178.2024.10700203.
- Suárez G., Bolino P., Venosa P. y Queiruga C. (2023). Acercando la ciberseguridad a la escuela secundaria desde una perspectiva lúdica. *Memorias De Las JAIIO*, 9(9), pp. 207-220.
- Suárez G. y Bolino P. (2020). “Capture the Flag” aplicada a la enseñanza de Ciberseguridad en escuelas. SEDICI, <http://sedici.unlp.edu.ar/handle/10915/118187>.