UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

TÍTULO: "Capture the Flag" aplicada a la enseñanza de Ciberseguridad en escuelas.

AUTORES: Gabriela Yanina Suárez y Patricio Emilio Bolino.

DIRECTOR: Lic. Paula Venosa y Lic. Einar Lanfranco.

CODIRECTOR:

ASESOR PROFESIONAL:

CARRERA: Gabriela Suárez: Licenciatura en Sistemas. Patricio Bolino: Licenciatura en Informática.

Resumen

Hoy en día se ha incorporado a la ciberseguridad en las etapas tempranas de formación estudiantil. En Europa y América del Norte se han desarrollado competencias Capture The Flag dirigidas a alumnos de colegios primarios y secundarios para interiorizar a los estudiantes en esta temática mediante un enfoque lúdico. Esta metodología de enseñanza resulta atractiva ya que los alumnos aprenden divirtiéndose y trabajando en equipo. Por lo que en el presente trabajo de grado se propone adaptar esta idea al contexto local, realizando una competencia Capture The Flag dirigida a estudiantes de escuelas secundarias que aborde temáticas de Ciberseguridad acordes al nivel educativo de nuestro contexto.

Palabras Clave

Capture the flag, ciberseguridad, escuelas secundarias, juego, seguridad informática, competencia, enseñanza, gamificación

Conclusiones

Se ha podido desarrollar satisfactoriamente una competencia de ciberseguridad dirigida a los estudiantes de escuelas secundarias que posibilitó, mediante un enfoque lúdico, que los alumnos aprendan conocimientos en el área de seguridad informática.

Consideramos que integrar este tipo de actividades en el aula resultó motivador para los estudiantes, debido que se involucraron rápidamente en la competencia y que el 100% de encuestados contestó que volvería a participar.

Trabajos Realizados

Se realizó un análisis del contexto global, regional y local con respecto a proyectos de seguridad informática dirigidos a alumnos de escuelas secundarias. Se investigaron competencias CTF dirigidas a estudiantes de escuelas secundarias y proyectos similares a esta tesina. Se seleccionó la plataforma a utilizar para desarrollar la competencia posteriormente a haber realizado una investigación y evaluación de las disponibles hoy en día. Se seleccionó el contenido teórico a incorporar en los retos planteados, luego de haber realizado una investigación de las temáticas que se abordan comúnmente en este tipo de competencias. Se desarrolló la competencia y se puso en práctica. Finalmente se analizaron los resultados de su implementación y se realizaron conclusiones a partir del análisis.

Trabajos Futuros

Los trabajos futuros que se proponen son:

1. *Proveer a los docentes la competencia configurada de manera que puedan utilizarla en el aula.*
2. *Adaptar la competencia y aplicarla en la Facultad para motivar a los alumnos a perfilarse al área de seguridad informática.*
3. *Realizar una introducción previa a la competencia para nivelar a los participantes.*
4. *Enriquecer con nuevo contenido teórico a la plataforma.*
5. *Realizar cambios en la modalidad de juego como por ejemplo, permitir el acceso online a la plataforma o prolongar su duración.*

Fecha de la presentación: Enero 2020

UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

“Capture the Flag” aplicada a la enseñanza de Ciberseguridad en escuelas secundarias

---

Gabriela Yanina Suárez - Patricio Emilio Bolino

Directores: Paula Venosa y Einar Lanfranco

Agradecimientos

A nuestras familias, a nuestros amigos y compañeros,
que nos acompañaron en todo el recorrido de la carrera hasta su culminación.

A nuestros directores Paula y Einar,
que nos acompañaron y guiaron constantemente durante el desarrollo de la tesina.

A todos los profesores y profesoras de la Facultad,
que nos ayudaron a concretar nuestra propuesta.

A los profesores de los colegios secundarios y a los alumnos,
que han participado activamente en el taller y
que nos han dado una devolución de nuestro trabajo.

A la Facultad,
que nos ha permitido realizarnos profesionalmente.

Índice

1. Introducción **5**
1.1 Objetivo 5
1.1.1 Objetivo General 5
1.1.2 Objetivos Específicos 5
1.2 Motivación 6
1.3 Estructura de la Tesina 7

2. Estado del Arte **9**
2.1 Capture The Flag (CTF) 9
2.2 CTF como herramienta para la enseñanza mediante un enfoque lúdico 11
2.2.1 Enfoque lúdico 11
2.2.2 Métodos alternativos de enseñanza 12
2.2.3 Utilización de CTF como pedagogía alternativa de enseñanza 12
2.3 CTF para niños y adolescentes 13
2.3.1 Contexto Global 13
2.3.2 Contexto Regional 13
2.3.3 Contexto Local 14
2.3.4 Limitaciones encontradas 15
2.4 Conclusión del Análisis del Contexto 16

3. Investigación **17**
3.1 Análisis de CTF para niños y adolescentes 17
3.1.1 Hack in the Class 17
3.1.2 picoCTF 19
3.1.3 TJCTF 20
3.1.4 HSCTF 21
3.1.5 NeverLAN CTF 22
3.1.6 Tech CTF 22
3.1.7 NACTF 23
3.1.8 InCTF 24
3.2 Documentación provista por los CTFs evaluados 24
3.3 Tesis y Proyectos similares 25
3.3.1 Universidad de Extremadura 25
3.3.2 Universidad de Catalunya 25
3.3.3 Universidad de Cantabria 26
3.3.4 MIT - Lincoln Laboratory 26
3.4 Cuadro comparativo 27
3.5 Conclusión de la investigación 28
3.5.1 Limitaciones de los CTFs evaluados 28
3.5.2 Conclusiones generales 29

4. Investigación de la Plataforma **30**
4.1 Análisis de las plataformas 30
4.1.1 Mellivora 30
4.1.1.1 Características 30
4.1.1.2 Ventajas de la plataforma 32
4.1.1.3 Desventajas de la plataforma 33
4.1.2 CTFd 34
4.1.2.1 Características 34
4.1.2.2 Ventajas de la plataforma 36
4.1.2.3 Desventajas de la plataforma 37
4.1.3 Facebook CTF 38
4.1.3.1 Características 38
4.1.3.2 Complicaciones con la plataforma 39
4.1.4 Easy CTF 39
4.1.5 Libre CTF 39
4.2 Conclusión del análisis de las plataformas 40
4.3 Evaluación de Calidad de CTFd y Mellivora 40
4.3.1 Comparación de Plataformas 40
4.3.2 ISO 25000 41
4.3.2 Aplicación de la evaluación 43
4.3.2.1 Determinación de los requisitos de evaluación 44
4.3.2.2 Especificación de la Evaluación 47
4.3.2.3 Diseño de la evaluación 49
4.3.2.4 Ejecución de la evaluación 50
4.3.2.5 Conclusión de la evaluación 51
4.4 Selección de la plataforma 54

5. Desarrollo del CTF **55**
5.1 Contenido teórico seleccionado 55
5.2 Configuración general del CTF 57
5.3 Modalidad del juego 58

6. Puesta en Práctica **61**
6.1 Primera evaluación 61
6.1.1 Configuración del CTF 61
6.1.2 Descripción de la competencia 61
6.1.3 Desempeño de los participantes 62
6.1.4 Dificultades 63
6.1.5 Conclusiones 65
6.1.5.1 Devolución de los alumnos 66
6.1.5.2 Mejoras efectuadas 66
6.2 Segunda evaluación 68
6.2.1 Configuración del CTF 68

6.2.2 Descripción de la competencia 69
6.2.3 Desempeño de los participantes 70
6.2.4 Dificultades 70
6.2.5 Conclusiones 71
6.2.5.1 Devolución de los alumnos 72
6.3 Análisis de los Resultados de las Encuestas 73

7. Conclusiones y Trabajo Futuro 76
7.1 Conclusiones 76
7.2 Trabajo a Futuro 77
7.2.1 Utilización de la plataforma en el aula 77
7.2.2 Utilización de la plataforma en la Facultad 77
7.2.3 Introducción previa a la competencia 77
7.2.4 Enriquecer con nuevo contenido teórico a la plataforma 78
7.2.5 Cambios en la Modalidad del Juego 79

8. Anexos 80
8.1 Instalación de Mellivora 80
8.1.1 Instalación con LAMP (Ubuntu, Apache, MySQL, PHP) 80
8.1.2 Instalación con Docker 82
8.2 Instalación de CTFd 84
8.3 Métricas Utilizadas 85
8.4 Matriz de Calidad 89
8.5 Especificación de las mediciones tomadas en Mellivora 94
8.5.1 Características que hacen a la usabilidad del software 94
8.5.2 Características que hacen a la seguridad del software 101
8.5.3 Características hacen a la portabilidad del software 102
8.6 Especificación de las mediciones tomadas en CTFd 104
8.6.1 Características que hacen a la usabilidad del software 104
8.6.2 Características que hacen a la seguridad del software 113
8.6.3 Características hacen a la portabilidad del software 114
8.7 Análisis de accesibilidad de Mellivora 116
8.8 Análisis de accesibilidad de CTFd 118
8.9 Encuestas de la primera evaluación 120
8.9.1 Encuestas de los alumnos de la escuela técnica número 5 120
8.10 Encuestas de la segunda evaluación 126
8.10.1 Encuestas de los alumnos de la escuela número 14 126
8.10.2 Encuestas de los alumnos de la escuela número 50 132
8.10.3 Encuestas de los alumnos del colegio Liceo Victor Mercante 138

9. Índice de tablas 142

10. Índice de figuras 143

11. Bibliografía 144

1. Introducción

1.1 Objetivo

1.1.1 Objetivo General

El objetivo principal de la tesina es elaborar una plataforma web dirigida a los estudiantes de escuelas secundarias que les posibilite, mediante un enfoque lúdico, aprender o interiorizar conocimientos en el área de seguridad informática. Dicha plataforma se destinará a aquellos estudiantes que posean o no conocimientos en programación.

1.1.2 Objetivos Específicos

- Hacer una investigación sobre los proyectos existentes hoy en día que se utilizan para motivar a los alumnos de colegios secundarios a interiorizarse en conocimientos de seguridad informática. Luego evaluar sus virtudes y falencias.
- Analizar y comparar las distintas plataformas existentes que se utilizan para crear desafíos de seguridad informática.
- Elegir una de las plataformas anteriormente evaluadas para el desarrollo del proyecto en función de características que consideremos convenientes.
- Implementar una plataforma que sea inclusiva, tanto para alumnos con conocimientos en informática como para aquellos que no han tenido la posibilidad de cursar una materia de computación.
- Cuidar las expresiones del lenguaje utilizadas en los contenidos de la plataforma de manera de abarcar a todos los alumnos dejando de lado cualquier tipo de discriminación.
- Desarrollar ejercicios prácticos que sean desafiantes para los alumnos pero que no excedan el grado de dificultad para evitar que los mismos se frustren.

1.2 Motivación

La Seguridad Informática es una rama de la ciencia computacional que se enfoca en la protección de las infraestructuras de redes de computadoras y de la información que reside en una máquina o que circula a través de las redes. Se encarga de identificar y eliminar vulnerabilidades para evitar ataques malintencionados. Los ataques pueden darse en las distintas capas en las que se organizan las tecnologías de red: en aplicaciones web, dispositivos de red, dispositivos IoT, servidores, o en las computadoras personales de los usuarios finales de las aplicaciones. Por lo tanto la seguridad informática comprende software, hardware, redes de computadoras y activos de información.

A causa de la enorme expansión de las tecnologías informáticas, existe hoy en día una preocupación a nivel global por aplicar medidas seguridad a las mismas debido a los numerosos ataques que han sufrido las organizaciones y que han impactado negativamente en su economía, en la integridad de la información que gestionan y en su reputación. Por este motivo se ha incrementado la demanda de personal encargado de la seguridad informática por lo que se ha empezado a motivar a las personas a acercarse al campo de la seguridad desde las etapas de formación secundaria.

Desde el año 2015, la Facultad de Informática de la Universidad Nacional de La Plata está llevando a cabo un proyecto de extensión en vínculo con escuelas secundarias que tiene por finalidad acercar a los jóvenes a la disciplina Informática a través de diferentes propuestas y actividades que les permitan comprender e intervenir el mundo digital que los rodea. En el marco de este proyecto se realizan charlas y talleres dirigidos a alumnos de escuelas secundarias que participan en el mismo, en las que se introducen conceptos básicos sobre distintas ramas de la informática como seguridad, desarrollo de aplicaciones, entre otras.

Una manera muy frecuente de interiorizar a los estudiantes respecto a la seguridad informática es explicando las amenazas a las que una persona está expuesta y dando algunas recomendaciones de las buenas prácticas a la hora de utilizar las tecnologías, como por ejemplo la creación de contraseñas fuertes para evitar el robo de identidad, la utilización de pantallas de bloqueo, utilización de antivirus, etc. Si bien esta modalidad teórica de enseñanza es de gran utilidad, la seguridad informática es más abarcativa.

Como participantes del proyecto de extensión de la Facultad de Informática estamos interesados en motivar a los alumnos de los colegios secundarios a interiorizarse en la seguridad aplicando una metodología de enseñanza que sea más atractiva que la teórica que se utiliza normalmente. Creemos que mediante un enfoque práctico y/o lúdico se podría incrementar su motivación al hacerlos partícipes en las actividades.

1.3 Estructura de la Tesina

- En el capítulo 1 se detallan, como puntapié inicial, los objetivos que se persiguen en la realización de la tesina, una pequeña introducción a la problemática actual y la solución que se propone. Finalmente, en esta misma sección se realiza una descripción del contenido de cada uno de los capítulos.
- En el capítulo 2 se describe el estado del arte con respecto a las competencias de seguridad informática “Capture The Flag” haciendo hincapié en el uso de las mismas como herramienta para la enseñanza con un enfoque lúdico. Se realiza un análisis del contexto global, regional y local en relación al uso de los CTFs donde se describen las modalidades de enseñanza existentes hoy en día en el ámbito de la seguridad.
- En el capítulo 3 se detallan las investigaciones realizadas sobre un conjunto de competencias CTFs dirigidas a alumnos de colegios secundarios de distintos países del mundo. Luego se expone un cuadro comparativo que resume las características más importantes. También se describen tesinas de otros países que han realizado un trabajo similar al propuesto en el presente documento y que se han aplicado en un marco académico.
- En el capítulo 4 se realiza una descripción de las plataformas que se utilizan hoy en día para implementar las competencias CTFs. Allí se exponen sus principales características, sus ventajas y desventajas. Luego se detalla el análisis de calidad realizado sobre aquellas plataformas que se han destacado en el análisis previo. Finalmente se explica qué plataforma se ha seleccionado para la realización de los objetivos propuestos y se realiza una justificación de la elección.
- En el capítulo 5 se describe la secuencia de pasos que se han realizado para desarrollar el CTF: en primera instancia se hace una explicación de qué temas teóricos se incluyeron en la competencia y la justificación de la selección de los temas elegidos. Luego se realiza una descripción general de la disposición de los desafíos en la plataforma. Finalmente se detalla la modalidad del juego desarrollado, es decir, una descripción de cómo los alumnos deben acceder al juego, de cómo deben utilizar la plataforma para resolver los ejercicios y de qué reglas deben respetar para no ser descalificados o penalizados.
- En el capítulo 6 se detalla la puesta en práctica del CTF en el marco de las actividades del proyecto de extensión en vínculo con escuelas secundarias. Se hace una descripción de la configuración de los desafíos y de las páginas de la plataforma al momento de realizar la prueba, de las características de la competencia (cantidad de participantes, cantidad de desafíos dados, composición de los equipos, etc.), del desempeño de los participantes, y de

las problemáticas que surgieron durante la puesta en práctica. Finalmente se detalla una conclusión elaborada en la cual se incorpora la devolución de los alumnos a partir del análisis de la encuestas.

- En el capítulo 7 se exponen las conclusiones a las que se llegaron con respecto a los objetivos propuestos (detallados en los capítulos iniciales) y los posibles trabajos futuros que se pueden desarrollar a partir de la labor realizada en esta tesina.

2. Estado del Arte

2.1 Capture The Flag (CTF)

"Capture The Flag" (capturar la bandera) es un tipo de competencia de seguridad informática en donde ciertas piezas de información llamadas "flags" (banderas) se colocan en servidores, se encriptan, se ocultan o se almacenan en lugares de difícil acceso. Durante la competencia, se liberan distintos desafíos en donde los equipos participantes aplican diferentes técnicas de ingeniería inversa, hacking, desencriptación y lo que sea necesario para hacerse con las flags. Cuando un equipo envía una flag al servidor de puntuaciones y la misma es correcta, obtiene los puntos correspondientes para esa flag [1] [2] [3] [4].

El objetivo de un CTF es encontrar y capturar todas las flags para el equipo y hacerlo de la manera más rápida posible. Cada flag suma puntos al puntaje total del equipo. Al finalizar el juego, el equipo que tenga mayor cantidad de puntos será el ganador.

Cada desafío tiene su propia flag y un input para ingresarla y enviarla al servidor de puntuaciones. Cuando se obtiene la flag (una vez completado un desafío), se la debe ingresar en el input y enviar al servidor para obtener los puntos correspondientes.

Algunas flags valen más puntos que otras. Por ejemplo, un desafío que es más difícil y tomará mucho tiempo completarlo generalmente vale más que uno que es fácil y se resuelve rápido.

Existen tres tipos de estilos de CTFs:

- **Jeopardy**: este tipo de competición CTF es el más habitual. Se juega en equipos formados por 1 o N personas donde cada equipo obtiene puntos por cada prueba que resuelve. La puntuación de las pruebas es proporcional a su dificultad y al finalizar la competición ganará el equipo que haya logrado más puntos. En algunas ocasiones el primer equipo en resolver un reto, obtiene una bonificación extra conocida como "First Blood" [1].

  Los CTF de estilo Jeopardy se caracterizan por dividir las pruebas en un rango de categorías. Las categorías que conforman este estilo son [5]:

  - **Análisis Forense**: se brindan archivos con imágenes de memoria, de discos duros o capturas de red, las cuales almacenan diferentes tipos de información.
  - **Criptografía**: se utilizan textos cifrados mediante un criptosistema determinado.

- **Esteganografía**: imágenes, sonidos o vídeos que ocultan información en su interior.
- **Explotación**: descubrimiento de vulnerabilidades en un servidor. Normalmente este tipo de desafíos vienen con un ejecutable, una dirección IP y un número de puerto del servidor que está corriendo ese programa. Se tiene que encontrar la manera de explotar el programa y lograr ejecutarlo remotamente. Se desarrolla un exploit[1] de manera local y posteriormente se usa contra el servidor donde luego se podrá leer el archivo que contiene la flag.
- **Ingeniería Inversa**: inferir en el funcionamiento del software. Generalmente se utilizan archivos binarios de Windows y Linux. Normalmente estos tipos de desafíos contienen un ejecutable, para descargarlo y ejecutarlo localmente. El programa descargado implementa algún tipo de algoritmo que chequea una clave de entrada, y al encontrar la clave correcta se resuelve el desafío. Para encontrar la clave correcta se debe hacer ingeniería inversa, entender el algoritmo del programa y a raíz de eso deducir la clave correcta.
- **Programación**: también conocida como PPC (Professional Programming & Coding), son desafíos en los que se requiere desarrollar un programa o script que realice una determinada tarea.
- **Web**: descubrimiento de vulnerabilidades en una aplicación Web.
- **Reconocimiento**: búsqueda de la flag en distintos sitios de Internet. Para resolverlo se ofrecen pistas, tal como el nombre de una persona.
- **Trivial**: diferentes preguntas relacionadas con la seguridad informática.
- **Misceláneo**: retos aleatorios que pueden pertenecer a distintas categorías sin especificar.

Normalmente los desafíos tienen un título, una descripción corta, y tal vez información sobre cómo acceder a un servicio o un archivo para descargar. Los tópicos más comunes son ingeniería inversa, explotación, criptografía, forensia y programación.

- **Ataque y defensa**: en las competiciones de Ataque - Defensa cada equipo dispone de una red o host con servicios vulnerables en ejecución y tiene un tiempo determinado para parchear dichos servicios vulnerables y desarrollar los exploits. Una vez transcurrido dicho tiempo, los organizadores interconectan los equipos de los participantes y la competencia inicia. La puntuación se divide en puntos de ataque y puntos de defensa, los cuales se obtendrán protegiendo los servicios y atacando al resto de oponentes [1].

[1] Exploit: Secuencia de comandos utilizados para provocar un comportamiento no deseado o imprevisto en un sistema aprovechándose de un fallo o vulnerabilidad en el mismo.

- **Mixto**: puede tener muchas variaciones puede ser una mezcla de ataque y defensa con retos especiales. Hay tipos como “King of the hill” donde varios equipos luchan para obtener el control de un servidor vulnerable y mantener ese control. O CTFs donde se comienza por ataque y defensa y, mientras esto ocurre, se liberan retos o flags especiales [2] [4].

Además de los CTFs existen los denominados “Wargames” que constan de pruebas sobre seguridad informática, preparadas para ser resueltas de forma individual y sin límite de tiempo. Los retos propuestos suelen ser más sencillos que los que se encuentran en los CTF, puesto que no están preparados para ser resueltos por equipos. Los “Wargames” sirven para entrenarse y prepararse para las competencias CTF.

2.2 CTF como herramienta para la enseñanza mediante un enfoque lúdico

2.2.1 Enfoque lúdico

La Gamificación es una técnica de aprendizaje que traslada la mecánica de los juegos al ámbito educativo - profesional con el fin de conseguir mejores resultados, ya sea para absorber mejor algunos conocimientos o mejorar alguna habilidad.

Este tipo de aprendizaje ha ganado terreno en las metodologías de formación ya que facilita la interiorización de conocimientos de una forma divertida, generando una experiencia positiva en el usuario.

El concepto de gamificación involucra técnicas de aprendizaje mediante la utilización de juegos en el aula para motivar a los estudiantes en diferentes habilidades como la resolución de problemas, el alcance de objetivos, el trabajo en equipo, entre otros.

Uno de los motivos por los cuales los estudiantes no se involucran en el aprendizaje es por la falta de relación entre las actividades estudiadas y su aplicación en la vida real. La gamificación enfoca a los estudiantes en el contenido relevante, proporciona retroalimentación, mejora la retención y soporta múltiples estilos de aprendizaje [6].

2.2.2 Métodos alternativos de enseñanza

Hoy en día existe la denominada “Red Global de Aprendizajes” [7] que es una iniciativa de colaboración internacional que integra nuevas pedagogías de aprendizaje en 8 países a través de un marco común de acciones e investigación. Es una red profesional que busca cambiar las maneras de enseñar y aprender. Los países que participan en la red son: Uruguay, Australia, Canadá, Estados Unidos, Finlandia, Holanda, Nueva Zelanda y Hong Kong.

Esta red ofrece un espacio para llevar adelante las iniciativas de los docentes tomando a los estudiantes como centro. Las prácticas pedagógicas se basan en aprender haciendo en torno a proyectos vinculados a experiencias de la vida real con el estudiante como protagonista y el docente como activador. Esta metodología busca evaluar el desarrollo de seis competencias: creatividad, pensamiento crítico, carácter, comunicación, colaboración y ciudadanía. El ambiente de aprendizaje se extiende al patio, al barrio y también a espacios virtuales de acceso al conocimiento. También se utilizan las herramientas digitales como acelerador de los aprendizajes.

2.2.3 Utilización de CTF como pedagogía alternativa de enseñanza

Extendiendo el enfoque lúdico de enseñanza, las competencias de estilo CTF generan una variedad de conocimientos técnicos en los participantes al introducir los conceptos de seguridad informática como desafíos dentro de un ambiente competitivo [8].

Teniendo en cuenta que hoy en día se están aplicando metodologías alternativas de enseñanza en varios países del mundo y que la gamificación es una metodología de formación que facilita la interiorización de conocimientos, consideramos que las competencias CTF pueden ser utilizadas como una herramienta educacional en el ámbito escolar.

Creemos fehacientemente que la implementación de un CTF en el aula mejorará el aprendizaje debido a su carácter lúdico, lo que motivará a los estudiantes a colaborar entre ellos, y permitirá que los mismos desarrollen una comprensión más profunda de los temas y tomen acciones para resolver problemas del mundo real.

Por lo tanto, concluímos que los CTF sirven para complementar todo estudio teórico de la seguridad de la información.

2.3 CTF para niños y adolescentes

2.3.1 Contexto Global

En la actualidad se realizan competencias online denominadas “Capturar la Bandera” o CTF de forma abreviada (del inglés “Capture the Flag”), en las que participan personas de distintos países del mundo y que sirven como un ejercicio educacional para los competidores. Los participantes pueden ser aprendices o expertos en seguridad informática, y estas competencias les brindan conocimientos sobre vulnerabilidades y ataques conocidos de la actualidad para poder hacer frente a los mismos.

Países desarrollados y aquellos con una buena base informática han empezado a motivar a los alumnos de colegios secundarios a interiorizarse en la seguridad informática mediante competencias CTF para niños [6] [9] [10], como por ejemplo “Hack in the Class” [11] de Holanda, “InCTF” [12] de la India, “picoCTF” [13], “TJCTF” [14], “HSCTF” [15] y “NeverLAN CTF” [16] de Estados Unidos.

También se han desarrollado competencias CTF en el ámbito académico en las que han participado tanto estudiantes de grado como profesionales de la seguridad. Algunas de las experiencias más relevantes son “Cybersecurity Challenge” de la Universidad de Extremadura [19] [20], “CTF utilizando la plataforma de Facebook” de la Universidad de Catalunya [21], “CTF para implementar en la asignatura Garantía y Seguridad en Sistemas y Redes” de la Universidad de Cantabria [22] y “MIT/LL CTF” del Laboratorio Lincoln del Instituto Tecnológico de Massachusetts (MIT) [23].

2.3.2 Contexto Regional

Nos resultó interesante la modalidad práctica de motivación que se utilizan en los países europeos o de América del Norte comentados anteriormente. Por ende, decidimos hacer una investigación sobre CTFs para chicos existentes en el contexto regional y local.

La Unión Internacional de Telecomunicaciones (UIT) ha publicado un índice que especifica un ranking de los países más comprometidos en la seguridad informática ordenados por área geográfica [24]. En función de este índice hemos investigado qué actividades de seguridad se realizan en aquellos países de América Latina que figuran por encima de Argentina. Como resultado de la investigación, hemos encontrado campañas y actividades aplicadas en los colegios secundarios que tienen por finalidad la concientización de los alumnos en temas asociados a la

seguridad informática pero no hemos hallado información respecto de competencias CTFs o de alguna actividad similar. También hemos encontrado la aplicación de metodologías alternativas de enseñanza en el ámbito escolar. Por ejemplo:

- UNICEF Paraguay en el 2017 lanzó la campaña #LoDigitalEsReal que se basó en instar a padres y madres a acompañar a sus hijos e hijas en el uso de las redes, de modo a prevenir casos de captación, acoso y abuso a través de la red [25] [26].
- La fundación Paraguay Ciberseguro trabaja en capacitaciones en escuelas y colegios públicos sobre seguridad en internet, enfocados en los peligros que se encuentran en internet como ciberbullying, grooming, y el acoso a menores [27].
- Uruguay forma parte de la denominada “Red Global de Aprendizajes” [7] que es una iniciativa de colaboración internacional que integra nuevas pedagogías de aprendizaje a través de un marco común de acciones e investigación. Uruguay, a través de ANEP y Plan Ceibal, participa de esta red junto con otros siete países: Australia, Canadá, Estados Unidos, Finlandia, Holanda, Nueva Zelanda y Hong Kong.

2.3.3 Contexto Local

En Argentina se encuentra la asociación civil Argentina Cibersegura [28] que realiza charlas sobre navegación segura por Internet, orientadas a niños, adolescentes y adultos, y también se encuentra la Fundación Dr. Manuel Sadosky [29] que es una institución público privada que ofrece cursos de programación en colegios secundarios para incentivar a estudiantes a cursar carreras vinculadas con el campo de la informática.

La Fundación Sadosky también desarrolló en septiembre del 2019 la competencia “Capture the flag junior” [30] dirigido a aquellas personas interesadas en la seguridad informática pero que no posean conocimientos específicos en la seguridad y que no hayan participado previamente en un CTF. La competencia exigía que los participantes posean conocimientos generales de computación como manejo de entorno Linux y programación básica. Los desafíos brindados podían pertenecer a las siguientes categorías: web, criptografía, redes, inyección SQL, informática forense e ingeniería inversa. Si bien, el CTF brindado tenía un carácter introductorio en la ciberseguridad, apuntaba a un público técnico.

La Fundación Sadosky, a través de su iniciativa Program.AR, brinda manuales de Ciencias de la Computación para docentes de primer y segundo ciclo de primaria [31] [32], y primer ciclo de secundaria [33]. Los mismos se pueden acceder y descargar desde la página oficial de Program.AR. Estos manuales

abarcan temáticas básicas de programación y de hardware de las computadoras. Además, incluyen actividades prácticas que los docentes pueden utilizar a la hora de explicar estos conceptos en el aula.

Docentes e investigadores del Laboratorio de Investigación en Nuevas Tecnologías Informáticas (LINTI) de la Facultad de Informática de la UNLP junto con la Fundación Sadosky desarrollaron el Manual de Ciencias de la Computación para docentes de segundo ciclo de educación secundaria que tiene por finalidad proveer de material útil para asistir a los docentes a la hora de dictar contenidos asociados a programación, sistemas operativos, redes y seguridad informática. Este manual (que se encuentra en proceso de edición y será publicado próximamente) provee material teórico correspondiente a las temáticas anteriormente mencionadas y ejercicios prácticos que tienen por finalidad que los alumnos interioricen estos conceptos en el aula de una forma divertida mediante el trabajo en equipo.

También hemos encontrado sitios web de concientización en seguridad como segu-kids [34] fundada por Cristian F. Borghello.

Si bien hemos encontrado proyectos en Argentina que buscan involucrar a los alumnos de colegios secundarios en temas de seguridad informática, no hemos hallado una modalidad de enseñanza similar a las competencias CTFs.

2.3.4 Limitaciones encontradas

En función de lo investigado podemos observar que se está comenzando a implementar CTFs para chicos en determinados países europeos y de América del Norte, pero no en América Latina. Si bien esta modalidad práctica de enseñanza nos resultó muy atractiva, hemos encontrado algunas limitaciones para aplicarla directamente en el contexto regional:

- La mayoría de las competencias están en idioma inglés, por lo que sólo aquellas personas que dominan ese idioma pueden comprender la totalidad de los desafíos.
- Los niveles de dificultad de los desafíos en la mayoría de los CTFs se incrementan de manera abrupta. La resolución de los ejercicios iniciales demandan conocimientos básicos en seguridad; mientras que a medida que se avanza en la competencia, se requieren de conocimientos más específicos y técnicos. De esta manera, se llega a una instancia en la que el nivel es tan elevado que causa frustración en los competidores por no poder avanzar. La dificultad se debe principalmente al desconocimiento y/o porque el desafío es realmente complejo aunque la temática sea accesible.
- En la mayoría de los desafíos se otorga una pista para orientar su resolución pero no se brinda una introducción a los temas abordados.

- Algunas competencias impiden continuar hacia las instancias finales porque exigen su resolución de manera presencial.
- En muchos casos hay contenido de la cultura propia de cada país relacionado con el desafío, lo que incrementa la dificultad en la resolución.

2.4 Conclusión del Análisis del Contexto

En resumen, debido a los numerosos ataques que han sufrido las organizaciones y que han impactado fuertemente en su economía, reputación y en la integridad de la información que gestionan, se ha incrementado enormemente la demanda de profesionales especializados en seguridad informática. Por esta razón se ha comenzado a motivar a las personas a interiorizarse en la seguridad desde las etapas de formación secundaria mediante diferentes metodologías de enseñanza.

En Europa y América del Norte se ha empezado a utilizar una modalidad de enseñanza práctica incorporando competencias CTFs para chicos pero esta modalidad no existe hoy en día en América Latina. En consecuencia, proponemos realizar un CTF que se aplique en el marco del proyecto de extensión en vínculo con las escuelas secundarias y que se adapte al contexto regional para superar las limitaciones analizadas.

Consideramos que un enfoque lúdico de enseñanza es una forma muy atractiva de difundir las carreras de informática en los secundarios ya que creemos que el aprendizaje mediante el juego y la competencia en equipo motivará a los estudiantes y despertará la curiosidad en instruirse más sobre estos temas [35] [36].

Queremos diseñar una plataforma que sea lo más inclusiva posible, por lo que los ejercicios estarán al alcance de los estudiantes sin importar el nivel de conocimientos en programación que posean, y opcionalmente brindaremos material en idioma español para orientar a los alumnos en la resolución de los desafíos con explicaciones teóricas de los conceptos.

3. Investigación

3.1 Análisis de CTF para niños y adolescentes

En esta sección se detallan las características de las competencias CTF para escuelas secundarias halladas durante el análisis del contexto global descrito en la sección 2.3.1. Estas competencias son: Hack in the Class, PicoCTF, TJCTF, HSCTF, NeverLAN CTF, Tech CTF, NACTF e InCTF.

El análisis de las competencias lo realizamos durante el transcurso del mes de abril hasta octubre del 2019 por lo que hemos estudiado más en detalle a aquellas competencias que se encontraron online durante el período de investigación.

3.1.1 Hack in the Class

La Fundación Hack in the Class se estableció con el objetivo de promover la educación de los estudiantes en torno a la tecnología, la privacidad y la seguridad. Al introducir a los estudiantes en la tecnología, se les fomentan habilidades como la curiosidad y la investigación. Por este medio, los creadores del CTF intentan que los jóvenes se den cuenta de que el hacking es una forma de aprender cómo funcionan las cosas y, al mismo tiempo, formarlos con este conocimiento para el futuro [11].

Al crear conciencia, desarrollar el conocimiento y estimular la curiosidad en torno a la seguridad informática y el hacking en una edad temprana, se espera estimular en estas temáticas a la próxima generación.

Los niños están creciendo en una sociedad digital. La educación está luchando para proporcionar los conocimientos y habilidades necesarias para que los niños puedan comprender e interactuar con las nuevas tecnologías, pero tener éxito en esto muchas veces depende de la dedicación y el conocimiento del docente.

Basándose en la filosofía de "Mantener el conocimiento libre", el hackerspace Randomdata y la conferencia de seguridad “Hack in the Box” lanzaron la iniciativa "Hack in the Class" en Ámsterdam del 2016, que luego se formalizó en una fundación en el 2018.

El primer paquete de enseñanza es el entorno de hacking "Capture The Flag (CTF)" para niños en el cual, a través de varias tareas, los estudiantes tienen un primer acercamiento a las técnicas de hacking para principiantes.

Debido a que vulnerar computadoras y sitios web ajenos es ilegal, tienen preparado un entorno de laboratorio propio donde los niños pueden comenzar a practicar esas técnicas.

Actualmente tienen disponibles 4 tipos de ejercicios:

- Inicio de sesión: los estudiantes intentan hallar las credenciales de un usuario mediante la inspección de las páginas html.

    - Los ejercicios se presentan en múltiples idiomas, incluído el español.
    - Los desafíos están dispuestos en 6 niveles, en los cuales se va incrementando la dificultad.
    - Se brinda una ayuda cuando las credenciales de login son incorrectas.
    - Cuando se termina el desafío se da información sobre el mismo.
    - Falta algún indicio de por dónde empezar a encarar el desafío.

- Códigos ocultos: los estudiantes utilizan varias formas de codificación y cifrado.

    - Estos ejercicios sólo están disponibles en idioma inglés.
    - Está armado por niveles, en los cuales cada uno contiene un mensaje encriptado en algún criptosistema de los más conocidos (Morse, César, Vigenere).
    - Al terminar el desafío se brinda información del mismo.
    - Para encontrar los mensajes cifrados, los jugadores deben buscarlos inspeccionando la página html, por lo que se agrega una complicación extra que no hace a la finalidad del ejercicio. Podrían haberse otorgado los mensajes encriptados directamente en el enunciado.

- Conceptos básicos de la web: aquí se combina información teórica y ejercicios prácticos. A través de una presentación interactiva, los estudiantes se interiorizan en los conceptos básicos de los servidores web y aprenden a utilizar técnicas de hacking cada vez más difíciles.

    - El material está disponible sólo en idioma inglés.
    - Está estructurado como una presentación en diapositivas en donde se recorre desde los temas más básicos como HTTP, arquitectura cliente-servidor y aplicación web hasta temáticas más complejas relacionadas con vulnerabilidades web como SQL Injection, path transversal y file inclusion.
    - Los desafíos se presentan a continuación de su respectiva explicación teórica.

- Análisis Forense: los estudiantes utilizan comandos para recuperar información oculta del tráfico de red. Estos desafíos son menos adecuados para principiantes.

- Los ejercicios están solamente en idioma holandés.
- Los desafíos constan de una explicación y un link para descargar un archivo con extensión .pcap.
- Estos ejercicios se encuentran en desarrollo ya que no hay forma de ingresar la solución.

3.1.2 picoCTF

PicoCTF es un juego de seguridad informática dirigido a estudiantes de secundaria y preparatoria que fue creado por la Universidad de Carnegie Mellon. El juego consiste en una serie de desafíos centrados en una historia en donde los participantes deben aplicar ingeniería inversa, hacking, desencriptación y otras técnicas para resolver los desafíos [13]. Todos los desafíos se configuran con la intención de ser hackeados, de manera que los estudiantes adquieran experiencia práctica de forma legal.

Este CTF posee las siguientes características:

- Sólo está disponible en idioma inglés.
- Tiene la opción para registrarse como estudiante o profesor/instructor.
- Permite crear “classrooms” como profesor para agrupar varios alumnos en una clase.
- La vista completa de la administración de un “classroom” sólo es accedida por quién lo crea.
- La lista de desafíos está ordenada de menor a mayor por el nivel de dificultad y puntaje otorgado.
- Se definen 6 categorías: análisis forense, ingeniería inversa, criptografía, explotación web, explotación de binarios y habilidades generales.
- Las distintas categorías se mezclan en el listado de desafíos.
- Todos los desafíos están legibles y no hay dependencia entre ellos.
- Cuando se resuelve un desafío, el mismo se oculta pero opcionalmente se puede visualizar.
- Hay una opción para calificar al desafío con un “like” o “dislike” como feedback del usuario.
- Las pistas están contenidas en una solapa aparte, lo que hace que se pierda el foco en el desafío.

- Presenta una shell[2] contenida en una página web aparte para resolver algunos desafíos. Por un lado, esta shell se comporta de manera inestable y por otro, se pierde el listado de los desafíos por cambiar de página.

La competencia picoCTF2019 se llevó a cabo desde el viernes 27 de septiembre hasta el viernes 11 de octubre.

3.1.3 TJCTF

TJCTF es una competencia CTF organizada por el Club de Seguridad Informática de la escuela "Thomas Jefferson High School for Science and Technology" del estado de Virginia. Se trata de un CTF online estilo jeopardy dirigido a estudiantes de escuelas secundarias que están interesados en las ciencias de la computación y en la ciberseguridad. Los participantes forman equipos de hasta 5 integrantes y resuelven problemas de diferentes categorías relacionadas con seguridad informática como ingeniería inversa, forensia, criptografía y explotación web. Los equipos que consigan los puntajes más altos obtienen premios al final de la competencia [14].

Este CTF posee las siguientes características:

- Sólo está disponible en idioma inglés.
- Tiene la opción para registrarse como observador o estudiante.
- Presenta la opción para crear equipos y enviar invitaciones a los usuarios.
- Sólo quién crea el equipo puede administrarlo y enviar las invitaciones.
- Se definen 6 categorías: web, criptografía, ingeniería inversa, forensia, análisis de binarios y una categoría con retos variados.
- La lista de desafíos está ordenada de menor a mayor por el nivel de dificultad.
- Todos los desafíos están visibles y no hay dependencia entre desafíos.
- Las categorías se mezclan en el listado de desafíos.
- Hay una opción para filtrar por categorías y que la lista de desafíos quede ordenada por la dificultad para esas categorías.

La competencia TJCTF 2019 se realizó en el mes de abril desde el viernes 5 al martes 9.

[2] Shell: es un término utilizado para referirse al intérprete de comandos que es una interfaz entre el usuario y el sistema operativo.

3.1.4 HSCTF

Es el primer CTF para estudiantes de escuelas secundarias realizado por estudiantes de escuelas secundarias. Es una competencia internacional de hacking online diseñada para enseñar computación a los alumnos [15].

Equipos de 4 estudiantes deben resolver retos en 4 categorías:

1. Crack de códigos
2. Ingeniería inversa
3. Diseño de algoritmos
4. Maestro de Internet

HSCTF no se trata solamente de seguridad informática sino que extiende el modelo de competencia de los CTF a otras áreas dentro de las ciencias de la computación tales como diseño y análisis de algoritmos y lenguajes de programación. HSCTF es un CTF diseñado para jóvenes estudiantes que pueden estar interesados en las ciencias de la computación.

La competencia está abierta a estudiantes de escuelas primarias y secundarias (de 6to grado a 5to año) de Estados Unidos. Los equipos deben estar compuestos por un máximo de 4 estudiantes.

HSCTF es organizado por estudiantes de “West Windsor-Plainsboro High School North” de New Jersey como parte de las actividades del Club de Ciencias de la Computación.

Este CTF posee las siguientes características:

- Sólo está en idioma inglés
- Define 7 categorías: criptografía, explotación de binarios, análisis forense, ingeniería inversa, web y misceláneo.
- Los desafíos están ordenados por categoría y, dentro de la categoría, por puntaje. El puntaje de un desafío define su dificultad.
- Hay desafíos que contienen una pista y otros que no incluyen pista.
- Existe la opción de crear un equipo y elegir un capitán para el mismo.

La competencia HSCTF 6 estuvo online en el mes de junio en la semana del lunes 3 al viernes 7.

3.1.5 NeverLAN CTF

NeverLAN CTF es un CTF de estilo jeopardy. Este evento fue creado con el objetivo de enseñar ciencias de la computación a las generaciones más jóvenes para fomentarles los valores del pensamiento crítico y las habilidades para resolver problemas [16].

La idea nació de 5 estudiantes que participaron de la SAINTCON, una conferencia de ciberseguridad que se hace en UTAH desde el 2015. Con esta experiencia, pensaron en mostrar a otros estudiantes la importancia de la seguridad informática sobre todo al estar conectados en Internet. Para esto, comenzaron realizando un evento en su comunidad local. Luego del increíble éxito y los comentarios positivos del primer año, el proyecto se convirtió en un evento anual donde se le enseña a los más jóvenes conceptos y temas relacionados con la ciberseguridad.

Como el CTF se realizó entre el 31 de enero y el 3 de febrero, no pudimos probarlo y evaluarlo en su totalidad. Su registración se encuentra cerrada, pero presenta ejercicios pre-ctf que poseen las siguientes características:

- Son 6 ejercicios divididos en 3 desafíos web y 3 desafíos criptográficos.
- Todos los desafíos están habilitados y no hay dependencia entre ellos.
- No se brinda ninguna pista para la resolución de los desafíos.

3.1.6 Tech CTF

Tech CTF es un evento internacional de Capture The Flag destinado a enseñar ciencias de la computación a la generación más joven. Es una competencia pensada para estudiantes de escuelas secundarias y fue creada por participantes de ediciones anteriores de NeverLAN CTF. Los participantes aprenden criptografía, forensia, programación e investigación. Todo lo que un participante necesita es una computadora, paciencia y habilidades para resolver problemas [17].

Este CTF posee las siguientes características:

- Está disponible sólo en idioma inglés.
- Presenta la opción de armar equipos, eligiendo un capitán por equipo.
- Opcionalmente permite configurar una contraseña para el equipo.
- Se establecen varias categorías: comandos, criptografía, análisis forense, trivia, OSINT[3], reconocimiento, seguridad web.

[3] OSINT: “Open Source Intelligence” o “Inteligencia de fuentes abiertas” hace referencia al conocimiento recopilado a partir de fuentes de acceso público. El proceso incluye la búsqueda,

- La lista de desafíos está ordenada por categorías. Dentro de una categoría los desafíos se ordenan por puntaje.
- Todos los desafíos están visibles y no hay dependencia entre ellos.
- Las pistas restan puntaje. Hay desafíos con varias pistas con distintos valores y desafíos que no contienen pistas.
- Hay desafíos con límite de intentos para ingresar la flag.
- En algunos desafíos no se respeta el formato de la flag ya que la respuesta se debe ingresar directamente.

La competencia Tech CTF se realizó en el mes de abril entre los días viernes 12 y lunes 22.

3.1.7 NACTF

NACTF es una competencia de ciberseguridad de tipo CTF estilo jeopardy para estudiantes de secundaria y preparatoria organizada por el Club de Ciencias de la Computación de la "Newark Academy". Los estudiantes pueden formar equipos de hasta 5 miembros y participar online de forma gratuita.

Los equipos compiten para resolver los desafíos aplicando descifrado, hacking e ingeniería inversa en temas como criptografía, análisis forense y explotación binaria. Los participantes envían flags o cadenas ocultas de texto para sumar puntos [18].

Este CTF posee las siguientes características:

- Está disponible sólo en idioma inglés.
- Presenta la opción de armar equipos de hasta 5 integrantes, eligiendo un capitán por cada uno.
- Opcionalmente permite configurar una contraseña para un equipo.
- Define 6 categorías: criptografía, ingeniería inversa, habilidades generales, explotación de binarios, análisis forense y explotación web.
- Los desafíos se encuentran separados por categorías. Dentro de una categoría, los desafíos están ordenados por puntaje que se corresponde con el nivel de dificultad.
- Todos los desafíos se encuentran visibles y no hay dependencia entre ellos.
- Hay desafíos que no contienen pistas y otros que tienen una o más.
- Todas las pistas se encuentran visibles y no restan puntaje.
- En todos los desafíos se respeta el formato de la flag.

selección y adquisición de la información, así como un posterior procesado y análisis de la misma con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

La competencia NACTF transcurrió en el mes de octubre desde el jueves 17 hasta el martes 22.

3.1.8 InCTF

InCTF es la principal competencia CTF de la India desarrollada exclusivamente para estudiantes y preparada por el team bi0s. Este equipo participa en concursos internacionales de ciberseguridad desde el año 2007 [12].

InCTF se plantea como meta generar conciencia e interés en la ciberseguridad en la comunidad estudiantil y busca fomentar en los estudiantes habilidades para que elijan carreras en este sector, proporcionándoles capacitación práctica y brindándoles el conocimiento y la experiencia de los expertos de la industria.

Por medio de esta competencia se buscan fomentar la pasión e interés a todos los estudiantes del país, permitiéndoles asumir los desafíos de un mundo digital que cambia rápidamente.

La competencia InCTF 2019 se realizó en el mes de septiembre desde el sábado 21 hasta el lunes 23.

Este CTF no pudo ser probado debido a que para registrarse en el mismo hay que abonar y, además, sólo se permite la participación de estudiantes de la India.

3.2 Documentación provista por los CTFs evaluados

De los CTFs que evaluamos en la sección anterior, verificamos si contenían algún tipo de explicación embebida en la competencia o si ofrecían algún material de referencia para su resolución. De la investigación que realizamos concluimos que:

- Hack in The Class: dentro de la misma competencia provee diapositivas con los contenidos teóricos necesarios para resolver ejercicios. Las diapositivas son largas porque explican temas que lo demandan como por ejemplo vulnerabilidades web. Los conceptos están descritos de manera concisa y el diseño es agradable al lector.
- PicoCTF: aporta documentación en su página oficial pero no embebido en la competencia. La documentación provee explicaciones de cada una de las categorías de los desafíos. A nuestro parecer no nos resultaron explicativas: en cada documento se hace una breve introducción a los temas de una categoría y luego redirige al lector a otras páginas de Internet para más

información. Tampoco incorporan imágenes que ayuden a una mejor comprensión de los contenidos.

- TJCTF: no provee documentación para los desafíos. Como método de entrenamiento recomienda picoCTF, la plataforma “Smash the Stack” y utilizar Google en la realización de cualquier CTF.
- HSCTF: no provee documentación teórica pero sí ejercicios prácticos con sus respectivas soluciones para entrenar.
- TechCTF: no ofrece documentación teórica.
- NACTF: no ofrece material extra para consultar.

3.3 Tesis y Proyectos similares

3.3.1 Universidad de Extremadura

El Cybersecurity Challenge fue una actividad tipo CTF llevada a cabo en la Universidad de Extremadura que contó con la participación de 132 personas, principalmente estudiantes y miembros de las Fuerzas de Seguridad. El CTF consistió en la superación de 5 retos y tuvo una duración de 72 hs. Para el desarrollo del mismo, se utilizó la plataforma Moodle que se utiliza en la universidad aprovechando las herramientas y recursos que ésta provee y, así, adaptar el aula virtual a un escenario de competición CTF [19] [20].

Las categorías elegidas fueron ingeniería inversa, exploiting, hacking web, análisis forense y esteganografía. Los retos se presentaron en bloques haciendo uso de etiquetas, URLs y archivos. La comunicación entre los participantes se realizó utilizando los foros. La validación y el registro de la solución de los retos se comprobaron a través de distintos cuestionarios.

3.3.2 Universidad de Catalunya

La Universidad de Catalunya desarrolló un CTF utilizando la plataforma de Facebook en donde participaron los alumnos de la carrera Ingeniería de Software de la Universidad Rey Juan Carlos de Madrid que en total formaron 12 equipos de 4 integrantes cada uno [21]. La competencia tuvo una duración de 1 hora y 40 minutos en la cual todos los equipos pudieron resolver al menos 2 desafíos como mínimo. El CTF consistió en 12 retos que incluyeron las categorías esteganografía, criptografía, ingeniería inversa y vulnerabilidades web. Cada reto estaba representado por un país y tenía un puntaje asociado según su dificultad.

3.3.3 Universidad de Cantabria

La Universidad de Cantabria realizó un proyecto para acercar las competencias CTF de los congresos de seguridad informática al entorno docente. El resultado fue generar un CTF para implementar en la asignatura “Garantía y Seguridad en Sistemas y Redes” en la cual se estudian los conceptos relacionados con la seguridad informática [22].

Para implementar el entorno de desarrollo de pruebas de CTF se analizaron distintas tecnologías y plataformas. El entorno final se compone de una serie de máquinas virtuales o de acceso remoto que se les proporcionan a los participantes. Entre estas máquinas se encuentra la que contiene al framework CTF donde se definen los retos y se hace un seguimiento del progreso de los participantes. El resto de las máquinas se comportan como víctimas y forman parte de la infraestructura a atacar para obtener las flags y conseguir los puntos para avanzar en la competencia.

3.3.4 MIT - Lincoln Laboratory

En el año 2011, para celebrar el 60° aniversario del Laboratorio Lincoln del Instituto Tecnológico de Massachusetts (MIT) se hizo una experiencia educacional en ciberseguridad. El MIT/LL CTF contó con la participación de 53 estudiantes provenientes de 6 universidades de Boston y tuvo una duración de 2 días. Los distintos retos hicieron foco en la seguridad sobre las aplicaciones web cubriendo múltiples niveles tanto en el cliente como en el servidor [23].

La semana anterior al evento se realizaron diferentes talleres en donde se capacitó a los alumnos en distintas temáticas relacionadas con la seguridad en aplicaciones web y las competencias CTF. Cada equipo contó con una máquina virtual para utilizar en la competencia que les fue distribuida un mes antes de la misma para que puedan familiarizarse con ella y practicar.

El CTF se desarrolló con la modalidad ataque - defensa donde cada alumno conectaba su computadora contra la máquina virtual de su equipo para realizar las tareas defensivas. Las máquinas virtuales tenían instalado el stack LAMP (Linux, Apache, MySQL y PHP) junto con una serie de plugins de Wordpress. Las flags estaban almacenadas dentro de los sistemas de archivos y la base de datos de las máquinas virtuales.

Los resultados de las encuestas realizadas luego de la competencia fueron positivos ya que la mayoría de los encuestados afirmaron que volverían a participar en un CTF y que incrementó su interés en la seguridad informática.

3.4 Cuadro comparativo

CTF	Modalidad de Juego	Clasificación de Desafíos	Idioma	Documentación
Hack in The Class	Individual	Inicio de Sesión, Códigos ocultos, Conceptos básicos de la Web, Análisis Forense	La mayoría de los desafíos están en Inglés y Holandés. Sólo algunos en Español.	Aporta presentaciones con los contenidos teóricos necesarios para resolver los ejercicios.
PicoCTF	Registración individual o grupal	Análisis forense, Ingeniería inversa, Criptografía, Explotación web, Explotación de binarios, Habilidades generales	Inglés	Provee documentación con explicaciones de cada una de las clasificaciones de los desafíos.
TJCTF	Grupal	Explotación de Binarios, Ingeniería Inversa, Explotación Web, Forensia, Criptografía	Inglés	No provee documentación para los desafíos.
HSCTF	Grupal	Criptografía, Explotación de Binarios, Análisis Forense, Ingeniería Inversa, Lenguajes de Programación, Web, Reconocimiento	Inglés	No provee documentación teórica pero sí ejercicios prácticos para entrenar.
Tech CTF	Grupal	Comandos, Criptografía, Análisis Forense, Osint, Reconocimiento, Web, Crack de Contraseñas	Inglés	No ofrece documentación teórica.
NACTF	Grupal	Criptografía, Ingeniería Inversa, Habilidades generales, Explotación de binarios, Análisis forense, Explotación web	Inglés	No ofrece material extra para consultar.

Tabla 1 - Cuadro comparativo de los CTFs investigados

Tesis	Lugar	Público	Clasificación de Desafíos
Cybersecurity Challenge	Universidad de Extremadura	Estudiantes y miembros de las Fuerzas de Seguridad	Ingeniería inversa, Exploiting, Hacking web, Análisis forense, Esteganografía
El aprendizaje basado en juegos a través de la plataforma Facebook CTF	Universidad de Catalunya	Alumnos de la carrera Ingeniería de Software de la Universidad Rey Juan Carlos de Madrid	Esteganografía, Criptografía, Ingeniería Inversa y Vulnerabilidades Web
Class Capture The Flag	Universidad de Cantabria	Alumnos de la Universidad de Cantabria	Fuerza Bruta, SQL Injection, XSS, Sniffing.
MIT LL CTF	Laboratorio Lincoln del Instituto Tecnológico de Massachusetts	Estudiantes de Universidades de Boston	Modalidad ataque - defensa

Tabla 2 - Cuadro comparativo de las tesis y los proyectos similares investigados

3.5 Conclusión de la investigación

3.5.1 Limitaciones de los CTFs evaluados

De acuerdo al análisis realizado de los CTFs orientados a los alumnos de escuelas secundarias existentes, podemos detallar algunas limitaciones que hemos encontrado y por las cuales no podemos aplicarlos directamente en el contexto local:

- En primer lugar, la mayoría de las competencias no están disponibles en idioma español por lo que se nos presenta una barrera idiomática que imposibilita la comprensión de los desafíos para el alumnado.
- Uno de los principales problemas que nos encontramos en los CTFs evaluados fue que la complejidad de los desafíos se incrementan de manera abrupta al avanzar en la competencia requiriendo conocimientos específicos y técnicos sobre seguridad informática. Esto provoca que algunos participantes se traben en la competencia generando una sensación de frustración.
- Con respecto a las temáticas abordadas en los CTFs, se otorgan pistas para orientar en la resolución de los desafíos. Muchas veces estas pistas

descuentan gran cantidad de puntos en el desafío y el contenido de la mismas es prácticamente la resolución del mismo. En casi todos los casos analizados no se brinda una introducción teórica a los temáticas que les sirva a los participantes que se encuentran por primera vez con ellas.

- En muchos de los desafíos el contenido de los mismos es propio de la cultura del país que desarrolla el CTF, como por ejemplo referirse al monstruo de las cookies de plaza sésamo en los desafíos de vulnerabilidades web que incluyen alguna interacción con las cookies del navegador o referencias a la serie “Mr. Robot” en desafíos en los cuales se involucra al archivo robots.txt. Esto incrementa la dificultad en la resolución debido al desconocimiento de esos contenidos culturales que sirven como pistas.

3.5.2 Conclusiones generales

En referencia a los proyectos y tesis encontrados que se asemejan a nuestra tesina podemos concluir que las mismas fueron dirigidas a otro tipo de público ya que los participantes de las competencias fueron estudiantes universitarios, docentes o miembros de fuerzas de seguridad que conocían las temáticas de antemano por lo que los desafíos exigieron conocimientos técnicos para su resolución.

Por este motivo no nos hemos basado en estos proyectos para el desarrollo de nuestro CTF, sino que nos hemos guiado con los CTFs dirigidos a los estudiantes de colegios secundarios analizados en la sección 3.1.

De la evaluación de los CTFs mencionados anteriormente extrajimos los tipos de categorías utilizadas comúnmente en las competencias de hoy en día y las temáticas que abarcan. A partir de allí hemos realizado una selección de las categorías de los desafíos en función de lo que consideramos más conveniente para cumplir con los objetivos propuestos. La justificación de la selección de las temáticas se encuentra detallada en el capítulo 5.

Una de las características que nos resultó útil del CTF “Hack in the Class” fue la disposición de diapositivas explicativas dentro de la misma competencia para orientar a los alumnos en la resolución de los desafíos. Por lo que hemos decidido utilizar esta idea en la competencia que desarrollamos y adaptarla a los temas que seleccionamos.

Si bien no es posible aplicar directamente alguno de los CTFs en el contexto local debido a las limitaciones detalladas anteriormente, pudimos adaptar y traducir algunos de los desafíos de menor complejidad para tomarlos como insumo en el desarrollo del CTF implementado en la tesina.

4. Investigación de la Plataforma

4.1 Análisis de las plataformas

Luego de haber realizado una investigación acerca de plataformas que permiten crear competencias CTFs, encontramos el siguiente conjunto de sistemas disponibles: Mellivora, CTFd, Facebook CTF, Easy CTF y Libre CTF. En esta sección se describe el análisis que hemos realizado de cada una de las plataformas encontradas.

4.1.1 Mellivora

Mellivora es un motor de CTF ligero escrito en PHP [37]. Pudimos instalar la plataforma de manera eficaz por lo que hemos realizado un análisis exhaustivo de la misma. Los detalles de la instalación de Mellivora se pueden consultar en el anexo 8.1.

A continuación se detallan las características de Mellivora teniendo en cuenta las pruebas que realizamos sobre el sistema y la información que se incluye en el proyecto oficial en GitHub. También hemos concluido ventajas y desventajas que encontramos a la hora de utilizar el sistema.

4.1.1.1 Características

- Presenta una consola de administración que brinda una visión general de la competencia y permite la realización de las siguientes operaciones:
    - Crear y editar las notificaciones que se visualizan en la página home.
    - Crear categorías con nombre, descripción y fechas de inicio y fin en las que estarán disponibles.
    - Crear desafíos con nombre, descripción, flag, puntos, número de intentos, cantidad de segundos entre intentos, dependencia con otro desafío, archivos adjuntos y fechas de inicio y fin en las que estarán disponibles.
    - Añadir MD5 de forma automática a los archivos que componen un desafío.
    - Administrar soluciones, permitiendo cambiar la corrección de las mismas.
    - Gestionar usuarios con la correlación de la dirección IP.

    - Utilizar correo electrónico SMTP.
    - Crear pistas para los desafíos con una descripción y la opción de visibilidad.
    - Crear contenido dinámico que abarca elementos del menú y páginas internas.
    - Gestionar logs internos para la captura de excepciones.
    - Realizar búsquedas por usuario, email o dirección IP.

- Presenta una página principal con las notificaciones listadas por orden de publicación.
- Posee una página general de desafíos separados por categorías y dentro de cada categoría la lista de desafíos con el título, puntaje, tiempo restante y, si está visible, el resto de las características.
- Expone un listado de pistas ordenadas por categorías y fecha de creación.
- Presenta una tabla de puntuaciones que está separada por equipos y por desafíos individuales.

    - Las puntuaciones por equipo están ordenadas por puntaje y se muestra el nombre del equipo y el país de origen.
    - La lista de desafíos resueltos está ordenada por categoría y dentro de cada categoría cada desafío por porcentaje de resolución. Para cada desafío se muestran el nombre, los puntos y los 3 primeros equipos que resolvieron el desafío.

- Mantiene una página de progreso por cada equipo participante que contiene el porcentaje de resolución para cada categoría y una lista de desafíos resueltos ordenada por la fecha de resolución más reciente.
- Permite configurar el perfil privado del usuario para gestionar el cambio de contraseña y la opción de segundo factor de autenticación.
- Tiene soporte para:

    - reCaptcha de Google.
    - integración con Docker.

- Tiene Licencia GNU General Public License V3 (GPL-3) [38].

4.1.1.2 Ventajas de la plataforma

- Desde la perspectiva del usuario común:

    - Al iniciar Mellivora se muestra la página Home que contiene las notificaciones. Si bien no hay una alerta de notificaciones, se ordenan por las más recientes por lo que se visualiza primero la última notificación añadida.
    - En la solapa de los desafíos, los mismos están separados por categorías y se ordenan según el puntaje, de menor a mayor.
    - Cuando se resuelve un desafío se marca como resuelto pudiéndose distinguir gráficamente de los desafíos no resueltos.
    - En la vista de los puntajes se presenta la tabla de desafíos, ordenados por categoría, junto el nombre, el puntaje, el porcentaje de resolución según la cantidad de participantes y el nombre de los equipos que fueron los primeros en resolverlo.
    - Al hacer click en el nombre del desafío se muestra información detallada con respecto a la resolución del mismo por parte de los equipos o avisa que no fue resuelto por ningún equipo.

- Desde la perspectiva del administrador:

    - Se pueden crear noticias para mostrar en la página principal.
    - Se puede crear contenido dinámico como ítems de menú y páginas nuevas. A un ítem del menú se le puede asociar una página. Las páginas nuevas sólo permiten un título y un cuerpo en el que se puede ingresar contenido con formato BBcode.
    - En la sección “Submissions” se visualizan las respuestas de cada participante en cada desafío, y se puede modificar la devolución por parte de la plataforma, es decir si la respuesta es correcta o incorrecta.
    - Se permite visualizar la competencia de una forma gráfica a través de la representación de un grafo de dependencias. Los elementos del grafo están compuestos por las categorías junto con los desafíos. Para cada elemento se indica su estado, de acuerdo a la disponibilidad, en color verde o rojo.
    - Para un desafío se pueden definir la cantidad de intentos y los segundos entre envíos para una flag.

4.1.1.3 Desventajas de la plataforma

- Desde la perspectiva del usuario común:

    - Un participante puede ver un listado de las hints, lo cual nos pareció innecesario porque no hay ningún link hacia el desafío asociado.
    - Si hay dependencias entre los desafíos y las hints de los desafíos están configurados como visibles, no se pueden ver los desafíos dependientes pero sí sus hints.
    - Si un equipo responde acertadamente un desafío del cual dependen otros, los desafíos dependientes se destraban para el resto de los equipos. Un usuario de otro equipo puede resolver un desafío dependiente sin haber resuelto los desafíos previos.
    - En la tabla de puntajes hay un ícono que al hacerle click brinda la misma información en formato JSON. Esta información es irrelevante para el usuario común y no aporta para su experiencia con la plataforma.
    - Si el desafío tiene definido un contador entre submits, se permite ingresar una flag lo cual redirige a otra página que avisa del contador en curso. Este comportamiento de la plataforma es confuso porque no se entiende si la flag fue enviada o no al servidor de puntuaciones.
    - Cuando se termina el tiempo del desafío, queda habilitada la opción de enviar una flag. Si se envía la flag se notifica al usuario que el tiempo del desafío finalizó. Si en vez de enviar la flag se refresca la página, entonces el desafío se bloquea.

- Desde la perspectiva del administrador:

    - Al crear una categoría o un desafío se debe configurar una fecha de inicio y de fin. Con respecto a las fechas, no se hace ningún tipo de validación por lo que se puede configurar una fecha de fin menor a la fecha de inicio o ingresar un formato inválido lo que genera la fecha 1970-01-01 00:00:00.
    - El formato de las fechas es de tipo YYYY-MM-DD HH:MM:SS y se ingresa de forma manual lo que facilita que se cometan errores.
    - La categoría se guarda al hacer click en el botón “create category” pero no hay feedback de la plataforma que nos avise de la creación. Al editar la categoría y hacer click en “save changes” aparece un mensaje de confirmación.
    - Cuando se guarda una categoría recién creada se visualiza un alerta avisando que la categoría ya existe y que en caso de eliminarla se

borrarán los desafíos y las resoluciones asociados a la misma. Esto es confuso porque la categoría ya fue creada pero el mensaje de éxito aparece al clickear el botón “save changes”.
    - A la hora de guardar un desafío recién creado se da el mismo error que con las categorías y además da la opción de agregar las pistas y adjuntos una vez que el desafío fue creado.
    - Al crear una hint se abre una ventana aparte para configurarla y una vez guardada aparece la opción para eliminarla. El comportamiento de creación es el mismo que en las categorías y desafíos.
    - Se puede habilitar o deshabilitar la visibilidad de una hint pero no se permite definir los puntos a penalizar por acceder a la misma, ni darle la opción al participante de visualizarla o no.

4.1.2 CTFd

CTFd es un framework CTF que se enfoca en la facilidad de uso y la personalización. Proporciona todo lo necesario para ejecutar un CTF y es posible personalizarlo fácilmente mediante plugins y temas [39].

Hemos podido instalar la plataforma de manera eficaz, lo que nos permitió realizar un análisis más exhaustivo de la misma. Los detalles de la instalación de CTFd se pueden consultar en el anexo 8.2.

A continuación se detallan las características de CTFd teniendo en cuenta las pruebas que hicimos sobre el sistema y la información que hemos encontrado en el proyecto oficial en GitHub. También concluímos ventajas y desventajas que hemos encontrado a la hora de utilizar el sistema.

4.1.2.1 Características

- Permite la creación de categorías, desafíos, pistas y flags desde la interfaz del administrador, pudiendo así realizar las siguientes acciones:

    - Configurar desafíos con puntuación dinámica: estos tipos de desafíos disminuyen su valor a medida que reciben soluciones. Cuanto más se resuelva un desafío dinámico, menor será su valor para todos los que lo resuelvan.
    - Definir dependencias entre desafíos.
    - Crear desafíos personalizados mediante la utilización de una arquitectura de plugins.
    - Definir de múltiples flags.

    - Utilizar flags basadas en expresiones regulares o expresiones estáticas, permitiendo elegir en ambos casos si serán Case Sensitive o Insensitive.
    - Definir múltiples pistas en un mismo desafío.
    - Asignar un puntaje a las pistas para poder desbloquearlas.
    - Subir archivos al servidor.
    - Limitar la cantidad de intentos y ocultar los desafíos.

- Posibilita configurar competencias individuales o grupales , es decir que los usuarios participen por su cuenta o armen equipos para jugar juntos.
- Presenta una tabla de puntuaciones con resolución automática de empates que permite:

    - Ocultar puntuaciones al público.
    - Congelar los puntajes por un tiempo determinado.

- Dispone de gráficos de puntuaciones que comparan el top 10 de los equipos y gráficos de progreso por equipo.
- Tiene soporte para correo electrónico que permite:

    - Confirmar el email.
    - Restaurar la contraseña.

- Permite configurar la fecha de inicio, de congelamiento y de fin de la competencia: se puede especificar una fecha de inicio de la competencia y una fecha de fin en la que los desafíos se cerrarán automáticamente y los usuarios no podrán enviar respuestas. También se puede especificar una fecha de congelamiento que implica que se mostrarán todas las soluciones hechas antes del tiempo de congelación, pero no se mostrarán nuevas soluciones a los usuarios.
- Permite administrar los equipos.
- Posee la capacidad de personalizar la plataforma a través de plugins y temas.
- Protege a la plataforma de ataques de fuerza bruta.
- Permite exportar e importar los datos de una competencia CTF configurada.
- Tiene licencia propia que detalla los términos de uso [40].

4.1.2.2 Ventajas de la plataforma

- Desde la perspectiva del usuario común:
    - Se presenta la capacidad de visualizar las notificaciones ordenadas de forma descendente por fecha de publicación.
    - Se permite acceder a estadísticas individuales de los usuarios participantes de la competencia y de cada equipo registrado en la plataforma.
    - Se visualiza la tabla de puntuaciones que mantiene el listado de equipos o usuarios con sus respectivos puntajes.
    - Se muestra la tabla de puntuaciones de manera gráfica como líneas de tiempo independientes para el top 10 de los equipos/usuarios con mayor puntuación.
    - Se puede acceder al perfil del usuario que presenta sus estadísticas junto con su historial de desafíos resueltos.
    - Se representan todas las estadísticas en forma de gráficos de torta cuando se muestran porcentajes de resolución y en líneas de tiempo para los historiales de puntuación.
    - Se permite distinguir gráficamente los desafíos resueltos de aquellos que todavía no han sido contestados correctamente, ya que cuando se resuelve un desafío el mismo cambia de color de negro a verde.
    - Se visualizan los desafíos ordenados dentro de cada categoría de acuerdo al puntaje de menor a mayor.

- Desde la perspectiva del administrador:
    - Se permite acceder a las estadísticas generales de la competencia con gráficos que representan el porcentaje de resolución de los desafíos, de las categorías y el porcentaje de respuestas correctas e incorrectas enviadas al servidor.
    - Se pueden crear notificaciones y páginas con formato HTML.
    - Se presenta la posibilidad de ocultar equipos, usuarios y desafíos.
    - Se puede asociar una o más flags a un mismo desafío.
    - Se permiten crear flags estáticas o dinámicas que utilizan expresiones regulares.
    - Se pueden configurar las flags sensibles o insensibles a las mayúsculas y minúsculas.
    - Se presenta la opción de previsualización del desafío que permite probar las flags.

- Se muestra el listado de respuestas enviadas al servidor (filtradas por correctas e incorrectas) junto con las opciones de eliminación de las mismas.
- Se le puede otorgar visibilidad pública o privada a la página de desafíos, la tabla de puntuaciones, la registración y las cuentas de usuarios y equipos.
- Se permite realizar backups para exportar toda la configuración y la información del CTF, importar un backup que fue exportado con anterioridad y descargar en formato CSV las tablas de la base de datos.

4.1.2.3 Desventajas de la plataforma

- Desde la perspectiva del usuario común:
  - Al iniciar CTFd se muestra la página Home y al iniciar sesión redirige al usuario a la página de los desafíos. Esto produce que pasen desapercibidas las notificaciones ya que no se dispone de ningún tipo de alerta que avise de nuevas notificaciones.
  - Si un desafío ya fue resuelto y se vuelve a hacer click sobre el mismo se habilita el input para ingresar la flag nuevamente. Al ingresar cualquier cadena de caracteres en el input, la plataforma avisa que el desafío fue resuelto.
  - Si un desafío se resolvió sin la utilización de la pista dada, la plataforma permite pedir la hint decrementando el puntaje correspondiente a la misma a pesar de que el desafío ya se encuentre resuelto.
  - No se muestra el número de intentos posibles para un desafío.

- Desde la perspectiva del administrador:
  - Una vez elegida la modalidad del juego (individual o grupal) la única manera de cambiarla es reiniciando el CTF perdiendo toda la información relacionada con los usuarios.
  - La creación de las categorías se realiza a través de la creación de los desafíos: al crear un desafío se debe indicar el nombre de la categoría a la que corresponde. Si es la primera vez que se usa ese nombre, se crea la categoría y si se desean crear nuevos retos asociados a la misma, se debe especificar su nombre exactamente igual.

4.1.3 Facebook CTF

Facebook CTF es una plataforma para alojar competiciones CTF de estilos Jeopardy y “King of the Hill” [41].

La plataforma Facebook CTF se presenta como un mapa interactivo en donde los participantes de la competencia van conquistando bases y países a medida que resuelven los distintos desafíos.

No hemos podido instalar la plataforma de manera eficaz por lo que a continuación sólo se detallan las características de Facebook CTF que hemos encontrado en la documentación oficial del proyecto.

4.1.3.1 Características

- Presenta una página de configuración del administrador a partir de la cual se pueden realizar las siguientes acciones:
    - Registrar usuarios en modo público o mediante tokens que se utilizarán luego para registrar a un equipo.
    - Configurar el login con Active Directory / LDAP.
    - Configurar el tiempo de inicio y fin de la competencia con posibilidad de pausarla en cualquier momento.
    - Definir el puntaje de un desafío según el orden de resolución de los equipos.
    - Establecer el idioma de la competencia y cambiarlo a posteriori.
    - Enviar mensajes en forma global a los participantes del evento.
    - Crear cuestionarios en formato pregunta y respuesta.
    - Incluir archivos adjuntos y links en los desafíos.
    - Crear categorías para agrupar los distintos tipos de desafíos.
    - Añadir pistas tanto a los cuestionarios como a los desafíos.
    - Habilitar o deshabilitar países y asignar desafíos y cuestionarios a los mismos.
    - Administrar las bases que representan sistemas objetivos que deben ser comprometidos por los equipos para obtener puntos de captura. Las bases son usadas en las competencias tipo King of the Hill en donde los participantes compiten por tomar el control de esos sistemas objetivos.

- Tiene Licencia Attribution-NonCommercial Creative Commons License (CC BY-NC 4.0) [42].

4.1.3.2 Complicaciones con la plataforma

Como se mencionó anteriormente, no hemos podido realizar una instalación eficaz de la plataforma Facebook CTF. Con la versión parcialmente funcional que obtuvimos al instalarla logramos probar cómo se crean los desafíos junto con sus pistas y flags, lo cual nos resultó bastante burocrático y poco intuitivo. No pudimos probar la competencia ya que tuvimos problemas para visualizar el mapa principal del juego.

La plataforma ha sido utilizada en varias competencias internacionales en el transcurso del año 2019, como la International CyberEx [43] desarrollada el miércoles 11 de septiembre y la OEA Cyberwomen Challenge [44] realizada el viernes 28 de junio. Sin embargo, Facebook utilizó la plataforma CTFd para llevar a cabo su propio CTF que se realizó en el mes de junio del 2019 entre los días sábado 1 y lunes 3 [45]. Esta decisión de Facebook de elegir CTFd sobre su propia plataforma sumado al resto de las complicaciones que tuvimos a la hora de probarlo, fue un determinante para descartar la prueba de esta plataforma.

4.1.4 Easy CTF

En primera instancia tuvimos en cuenta a la plataforma Easy CTF debido que había sido utilizada en la competencia TJCTF 2019, pero al investigar el proyecto oficial en GitHub [46] nos encontramos con la notificación de que el proyecto ha sido discontinuado, que la última actualización fue en realizada hace 2 años, que no posee ningún tipo de documentación tanto para su instalación como para su utilización y que han dado de baja su página oficial [47]. Por estos motivos, descartamos la prueba de la plataforma Easy CTF.

4.1.5 Libre CTF

Libre CTF es un framework para crear competencias CTF que ha sido desarrollado por los mismos creadores de Easy CTF. Anteriormente este proyecto se denominó Open CTF, que luego fue reescrito en Rust. Esta plataforma fue creada con la idea de que sea performante y al mismo tiempo lo más flexible posible [48].

En el proyecto oficial en Github se especifica que actualmente LibreCTF está en desarrollo y que todavía no está listo para entrar en producción.

El método recomendado para ejecutar esta plataforma es a través de un contenedor de Docker que será construido con versiones. Esta plataforma tiene

muchas partes móviles que pueden romperse si no se tiene el debido cuidado. Por lo tanto, se desaconseja ejecutar la plataforma en un entorno diferente al proporcionado a menos que se sepa lo que se está haciendo.

El proyecto utiliza las licencias:

- Apache License, Version 2.0 [49].
- MIT License [50].

Dado que la plataforma se encuentra en desarrollo y que la documentación provista es breve [51] [52], hemos decidido no realizar un análisis más exhaustivo de la misma ni probar su funcionalidad.

4.2 Conclusión del análisis de las plataformas

Luego de investigar y analizar las plataformas anteriormente mencionadas hemos llegado a la conclusión de que las plataformas que se podrían aplicar para la realización del objetivo de la tesina son CTFd y Mellivora, ya que hemos podido instalar ambas correctamente y, en líneas generales, las dos permiten crear una competencia CTF de manera eficaz.

Como se mencionó en la sección anterior, decidimos descartar a EasyCTF porque es un proyecto discontinuado, a LibreCTF porque todavía se encuentra en fase de desarrollo y a Facebook CTF porque su instalación no nos resultó sencilla, su interfaz nos resultó poco intuitiva y porque la misma empresa optó por utilizar otra plataforma en la competencia que organizó en el 2019.

Para poder tomar una determinación final sobre qué plataforma utilizar entre CTFd y Mellivora, hemos optado por hacer una evaluación de la calidad de ambas. En la siguiente sección se detalla el proceso de evaluación que hemos realizado y la conclusión a la que hemos llegado en función de los resultados obtenidos.

4.3 Evaluación de Calidad de CTFd y Mellivora

4.3.1 Comparación de Plataformas

A la hora de analizar las plataformas hemos optado por hacer una valoración de su calidad para poder compararlas. El concepto de calidad del software es subjetivo por lo que muchas empresas desarrolladoras de software utilizan

estándares o modelos que les permiten hacer una valoración más objetiva del producto a partir de medidas cuantitativas que se toman del mismo [53].

Para hacer la valoración de la calidad de las plataformas nos hemos basado en la ISO/IEC 25000 conocida como SQuaRE (System and Software Quality Requirements and Evaluation). La ISO/IEC 25000 es una familia de normas que tiene por objetivo la creación de un marco de trabajo común para evaluar la calidad del producto software [54].

4.3.2 ISO 25000

La norma ISO 25000 provee una guía para evaluar la calidad del software interna, externa y en uso:

- Calidad Interna: se valora cuando el producto software se encuentra en desarrollo.
- Calidad Externa: se valora cuando el producto software se encuentra en funcionamiento.
- Calidad en Uso: se valora cuando el producto software se encuentra en uso.

En nuestro caso particular, hemos hecho hincapié en la evaluación de la calidad externa de las plataformas CTF.

La ISO/IEC 25010 (denominada “System and software quality models”) describe un modelo de calidad para el producto software (interna y externa) y para la calidad en uso. Un modelo de calidad categoriza la calidad del producto en características y subcaracterísticas. La calidad del producto de software se puede interpretar como el grado en que dicho producto satisface estas características aportando de esta manera un valor [55].

Para hacer la evaluación de las plataformas nos hemos concentrado en el modelo de calidad del producto de software, el cual se encuentra representado en el siguiente esquema:

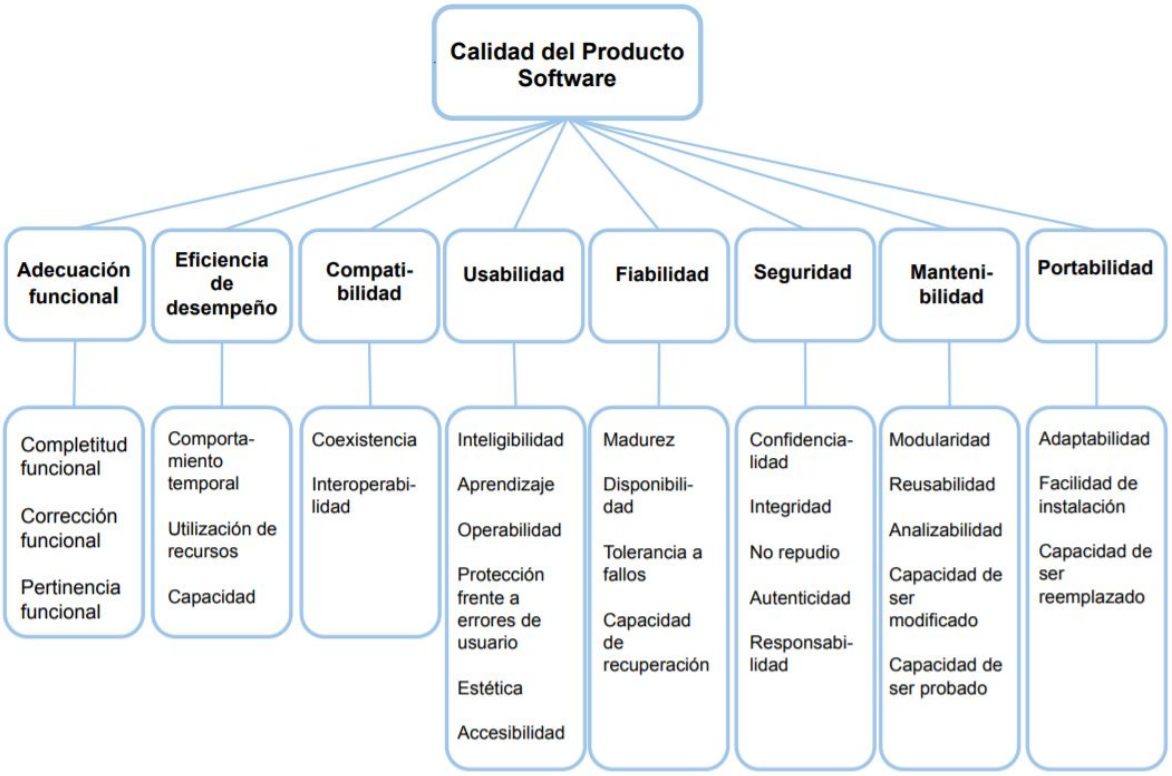


Figura 1 - Calidad del Producto de Software

Dependiendo del tipo de sistema a evaluar, las características presentadas en la norma tendrán un grado de importancia mayor o menor que otros, por lo tanto las características de calidad que se apliquen a un producto software deben definirse por el tipo de producto.

Las normas ISO/IEC 25023 e ISO/IEC 25022, proveen un conjunto de métricas para la calidad interna, externa y en uso, que son usadas con el modelo de calidad ISO/IEC 25010. Estas métricas pueden utilizarse directamente o pueden ser modificadas. También pueden emplearse métricas que no están definidas, siempre y cuando se especifique cómo se relacionan con el modelo de calidad ISO/IEC 25010 o con el modelo de calidad que vaya a sustituir al especificado en la norma.

La ISO/IEC 25040 (denominada “Evaluation reference model and guide”) [56] define el proceso para llevar a cabo la evaluación de la calidad del producto de software. Dicho proceso de evaluación consta de un total de cinco actividades:

1. **Determinar los requisitos de evaluación:** en esta instancia se determina el propósito de la evaluación, se especifican los requisitos de calidad del producto utilizando un determinado modelo de calidad, se especifica el tipo de producto a evaluar (especificación de requisitos, diagramas de diseño, etc.) dependiendo de la fase en el ciclo de vida en que se realiza la evaluación y del propósito de ésta, y se define el rigor de la evaluación.

2. **Especificar la evaluación:** en esta tarea el evaluador selecciona las métricas de calidad, técnicas y herramientas que cubran todos los requisitos de la evaluación y los criterios de decisión que se aplicarán en la evaluación.
3. **Diseñar la evaluación:** en esta actividad se define el plan con las actividades de evaluación que se deben realizar teniendo en cuenta la disponibilidad de los recursos, tanto humanos como materiales, que puedan ser necesarios. En la planificación se debe tener en cuenta el presupuesto, los métodos de evaluación y estándares adaptados, las herramientas de evaluación, etc.
4. **Ejecutar la evaluación:** en esta actividad se ejecutan las actividades de evaluación obteniendo las métricas de calidad y aplicando los criterios de evaluación.
5. **Concluir la evaluación:** en esta actividad se concluye la evaluación de la calidad del producto software, realizando el informe de resultados que se entregará al cliente y revisando con éste los resultados obtenidos.

La evaluación de calidad puede ser realizada durante o después del proceso de desarrollo o adquisición, desde el punto de vista de los desarrolladores, de los adquirentes o de evaluadores independientes.

Para llevar a cabo el proceso de evaluación de las plataformas nos hemos basado en la Tesina “Evaluación de calidad de productos software en empresas de desarrollo de software aplicando la norma ISO/IEC 25000” [57] en la cual se hace una evaluación de calidad de una página web desde la perspectiva de un evaluador independiente externo a la empresa proveedora del producto de software. Para el desarrollo de la evaluación Evelyn Balseca (la autora de la tesina) se basó en la norma ISO/IEC 25041 (denominada “Evaluation guide for developers, acquirers and independent evaluators”) que describe los requisitos y recomendaciones para la implementación práctica de la evaluación del producto software desde el punto de vista de los desarrolladores, de los adquirentes y de evaluadores independientes.

4.3.2 Aplicación de la evaluación

En esta sección se detalla cómo hemos realizado la evaluación de la calidad de las plataformas CTFd y Mellivora en función del proceso de evaluación definido en la ISO/IEC 25040 y de la aplicación práctica de la norma realizada en la tesina que hemos analizado.

4.3.2.1 Determinación de los requisitos de evaluación

Realizamos la evaluación de calidad sobre un producto de software final para compararlo con productos competitivos. Para ello hemos decidido evaluar sólo la calidad externa, es decir el análisis del funcionamiento del sistema.

A cada característica y sub-característica definida en la norma le hemos asignado un nivel de importancia según el tipo de producto de software a evaluar y en función de nuestros requerimientos para desarrollar un CTF acorde a los objetivos de la tesina.

Luego ponderamos cada una de las características en función del nivel de importancia que les asignamos. La ponderación la realizamos distribuyendo el 100% entre las características a evaluar. Aquellas características que definimos con un nivel de importancia bajo las ponderamos con un 0%. Este porcentaje fue utilizado para realizar el cálculo final de la calidad externa.

Para definir los niveles de importancia hemos utilizado la siguiente escala:

Nivel de importancia	Simbología	Significado
Alto	A	El grado de importancia de la característica o subcaracterística es alto por ende se realizarán las mediciones
Medio	M	La característica o subcaracterística no es tan relevante pero puede o no ser medida dependiendo del criterio del evaluador
Bajo	B	La característica o subcaracterística no tiene relevancia y no será medida.

Tabla 3 - Nivel de importancia de las características y subcaracterísticas

Las características de calidad externa las hemos nivelado y ponderado de la siguiente manera:

Características de Calidad Externa			
Características	**Descripción**	**Nivel de Importancia**	**Ponderación de la importancia**
Adecuación Funcional	Capacidad del producto software para proporcionar funciones que satisfacen las necesidades declaradas e implícitas, cuando el producto se usa en las condiciones especificadas.	B	0%
Eficiencia en el Desempeño	Desempeño relativo a la cantidad de recursos utilizados bajo determinadas condiciones.	B	0%
Compatibilidad	Capacidad de dos o más sistemas o componentes para intercambiar información y/o llevar a cabo sus funciones requeridas cuando comparten el mismo entorno hardware o software.	B	0%
Usabilidad	Capacidad del producto software para ser entendido, aprendido, usado y resultar atractivo para el usuario, cuando se usa bajo determinadas condiciones.	A	45%
Fiabilidad	Capacidad de un sistema o componente para desempeñar las funciones especificadas, cuando se usa bajo unas condiciones y periodo de tiempo determinados.	B	0%
Seguridad	Capacidad de protección de la información y los datos de manera que personas o sistemas no autorizados no puedan leerlos o modificarlos.	M	15%
Mantenibilidad	Capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidades evolutivas, correctivas o perfectivas.	B	0%
Portabilidad	Capacidad del producto o componente de ser transferido de forma efectiva y eficiente de un entorno hardware, software, operacional o de utilización a otro.	A	40%

Tabla 4 - Características de calidad externa

Luego determinamos el nivel de importancia de las subcaracterísticas correspondientes a aquellas características que hemos decidido evaluar:

Características y Subcaracterísticas de Calidad Externa			
Característica	**Sub Característica**	**Descripción**	**Nivel de Importancia**
Usabilidad	Inteligibilidad	Capacidad de permitir al usuario entender si el software es adecuado para sus necesidades.	A
	Aprendizaje	Capacidad de permitir al usuario aprender su aplicación.	B
	Operabilidad	Capacidad de permitir al usuario operarlo y controlarlo con facilidad.	A
	Protección frente a errores de usuario	Capacidad de proteger a los usuarios de cometer errores.	A
	Estética de la interfaz	Capacidad de la interfaz de usuario de agradar y satisfacer la interacción con el usuario.	M
	Accesibilidad	Capacidad de permitir que sea utilizado por usuarios con determinadas características y discapacidades.	A
Seguridad	Confidencialidad	Capacidad de protección contra el acceso de datos e información no autorizados, ya sea accidental o deliberadamente.	A
	Integridad	Capacidad de prevenir accesos o cambios no autorizados a datos o programas de ordenador.	B
	No repudio	Capacidad de demostrar las acciones o eventos que han tenido lugar, de manera no puedan ser repudiados posteriormente.	B
	Autenticidad	Capacidad de demostrar la identidad de un sujeto o un recurso.	A
	Responsabilidad	Capacidad de rastrear de forma inequívoca las acciones de una entidad.	B
Portabilidad	Adaptabilidad	Capacidad de adaptarse de forma efectiva y eficiente a diferentes entornos determinados de hardware, software, operacionales o de uso.	A
	Facilidad de Instalación	Facilidad con la que el producto se puede instalar y/o desinstalar de forma exitosa en un determinado entorno.	A
	Capacidad de ser reemplazado	Capacidad del producto para ser utilizado en lugar de otro producto software determinado con el mismo propósito y en el mismo entorno.	B

Tabla 5 - Características y subcaracterísticas de calidad externa

Como resultado de la nivelación anteriormente descrita, hemos seleccionado las siguientes características y subcaracterísticas a evaluar:

- Usabilidad:
  - Inteligibilidad.
  - Operabilidad.
  - Protección frente a errores de usuario.
  - Estética de la interfaz.
  - Accesibilidad.
- Seguridad:
  - Confidencialidad.
  - Autenticidad.
- Portabilidad:
  - Adaptabilidad.
  - Facilidad de Instalación.

A la usabilidad le hemos otorgado una importancia del 45% porque nos importa evaluar las interfaces de las plataformas teniendo en cuenta la perspectiva de los usuarios y administradores con respecto a la practicidad y la intuitividad de las mismas. Nuestro interés se enfoca en que tanto la creación como el acceso a los desafíos sea sencillo.

A la seguridad le dimos una importancia del 15% porque consideramos que el riesgo de que la plataforma sea atacada es mínimo. Esto se debe a que una de las reglas del juego prohíbe el ataque a la plataforma ya que de ser así los equipos serán descalificados.

A la portabilidad le asignamos una importancia del 40% porque consideramos muy relevante que las plataformas se puedan instalar de manera eficaz y eficiente. Además realizamos una evaluación de la adaptabilidad de las plataformas desde el punto de vista del usuario final ya que nos resulta fundamental que las mismas se mantengan operativas indistintamente del navegador o del dispositivo desde el cual se acceda.

4.3.2.2 Especificación de la Evaluación

En esta instancia definimos las métricas de las características que hemos decidido evaluar (usabilidad, seguridad y portabilidad) junto con sus respectivos valores deseados. Las mismas pueden encontrarse en el anexo 8.3.

Para evaluar la accesibilidad de las plataformas (sub-característica de la usabilidad) decidimos utilizar una herramienta automatizada que nos brinde valores cuantificables que complementen nuestras métricas. Para ello utilizamos SiMor, un validador robusto, completo, actualizado y que está disponible online.

SiMor es una herramienta que ha sido presentada por dos estudiantes de la Facultad de Informática de la UNLP como trabajo final de grado en el año 2015 [58] [59]. SiMor es una validador de accesibilidad web basado en las reglas WCAG[4] de la W3C[5] que permite analizar el código HTML estático de un sitio web con el objetivo de identificar problemas en el mismo.

Para realizar el análisis de la calidad del producto de software de una manera completa y concisa utilizamos una matriz de calidad que se muestra en la siguiente figura:

Matriz de calidad								
Característica	**Subcaracteristica**	**Métrica**	**Valor Deseado**	**Valor Obtenido (x)**	**Ponderación (/10)**	**Valor Parcial Total (/10)**	**Porcentaje de Importancia**	**Valor Final**
Seguridad	Confidencialidad	Capacidad de control de acceso						
	Autenticidad	Métodos de autenticación						
Portabilidad	Adaptabilidad	Adaptabilidad en entorno hardware						
		Adaptabilidad en entorno software						
	Facilidad de Instalación	Eficiencia en el tiempo de instalación						
		Eficacia de la Instalación						
		Economía de pasos de instalación						

Figura 2 - Matriz de calidad

Como se puede visualizar en la imagen, la matriz de calidad posee los siguientes campos:

- Característica: nombre de la característica.
- Subcaracterística: nombre de la sub-característica.
- Métrica: nombre de la métrica.
- Valor deseado: umbrales esperados de medida.

[4] Las pautas WCAG (Web Content Accessibility Guidelines) se han desarrollado mediante el proceso del W3C en cooperación con individuos y organizaciones en todo el mundo, con el fin de proporcionar un estándar compartido para la accesibilidad del contenido web que satisfaga las necesidades de personas, organizaciones y gobiernos a nivel internacional. Seguir estas pautas permite crear un contenido más accesible para un mayor número de personas con discapacidad y puede ayudar a que el contenido Web sea más usable para cualquier tipo de usuario.

[5] La W3C (World Wide Web Consortium) es una comunidad internacional donde las organizaciones miembros, un equipo de profesionales y el público general trabajan juntos para desarrollar guías y estándares para la Web.

- Valor obtenido: valor que se obtiene a partir de la aplicación de la fórmula de la métrica.
- Ponderación: valor obtenido de la métrica que es representado en la escala del 1 al 10.
- Valor parcial total: promedio de los valores obtenidos de las métricas de una misma característica.
- Porcentaje de importancia: porcentaje de importancia de la característica.
- Valor final: representa el valor de la característica que se calcula realizando el producto su valor parcial por el porcentaje de importancia de la característica.

A partir de la resolución de la matriz de calidad pudimos calcular la calidad externa del sistema, la cual se determinó realizando la suma de los valores finales de las características que hemos evaluado. A partir del valor final obtenido es posible determinar el grado de satisfacción que tiene el producto de software en cuanto a su calidad externa.

Para analizar el resultado final de la calidad externa utilizamos la siguiente escala de medición:

Escala de Medición	Niveles de Puntuación	Grado de Satisfacción
8.75 - 10	Cumple con los requisitos	Muy Satisfactorio
5 - 8.74	Aceptable	Satisfactorio
2.75 - 4.9	Mínimamente aceptable	Insatisfactorio
0 - 2.74	Inaceptable	

Tabla 6 - Escala de medición de la calidad

4.3.2.3 Diseño de la evaluación

Esta instancia del proceso de evaluación propuesto por la norma no la hemos aplicado debido que realizamos el análisis de un producto final (no en una fase de desarrollo), siempre contamos con la disponibilidad del software (ya que hemos descargado las plataformas de GitHub) y del hardware (ya que los instalamos en servidores propios). Esto nos permitió realizar la evaluación sin necesidad de establecer un plan de trabajo que especifique la programación de las tareas a realizar.

4.3.2.4 Ejecución de la evaluación

Para la realización de la evaluación de calidad de las plataformas hemos resuelto las matrices de calidad (las cuales se pueden encontrar en el anexo 8.4). En dichas matrices se aplicaron las métricas de las características referenciadas en el anexo 8.3. Los valores obtenidos de las métricas se encuentran justificadas en en los anexos 8.5 y 8.6.

Los resultados de las evaluaciones de la accesibilidad en Mellivora y CTFd se pueden consultar en los anexos 8.7 y 8.8 respectivamente.

Los resultados finales que hemos obtenido son los siguientes:

Resultado Final de la Calidad Externa de CTFd				
Característica	**Valor Final**	**Calidad del Sistema**	**Nivel de Puntuación**	**Grado de Satisfacción**
Usabilidad	3,77	9,11	Cumple con los requisitos	Muy Satisfactorio
Seguridad	1,5			
Portabilidad	3,84			

Tabla 7 - Resultado de calidad de CTFd

Resultado Final de la Calidad Externa de Mellivora				
Característica	**Valor Final**	**Calidad del Sistema**	**Nivel de Puntuación**	**Grado de Satisfacción**
Usabilidad	2,52	7,54	Aceptable	Satisfactorio
Seguridad	1,5			
Portabilidad	3,52			

Tabla 8 - Resultado de calidad de Mellivora

4.3.2.5 Conclusión de la evaluación

Las siguientes tablas muestran en detalle los valores obtenidos de las características que fueron aplicadas en la evaluación de calidad:

Valor Total de las características de Mellivora				
Característica	**Valor Parcial Total (/10)**	**Porcentaje de Importancia**	**Valor Final**	**Calidad Total del sistema**
Usabilidad	5,62	45 %	2,52	7,54
Seguridad	10	15 %	1,5	
Portabilidad	8,8	40 %	3,52	

Tabla 9 - Valor de las características de Mellivora

Valor Total de las características de CTFd				
Característica	**Valor Parcial Total (/10)**	**Porcentaje de Importancia**	**Valor Final**	**Calidad Total del sistema**
Usabilidad	8,39	45 %	3,77	9,11
Seguridad	10	15 %	1,5	
Portabilidad	9,6	40 %	3,84	

Tabla 10 - Valor de las características de CTFd

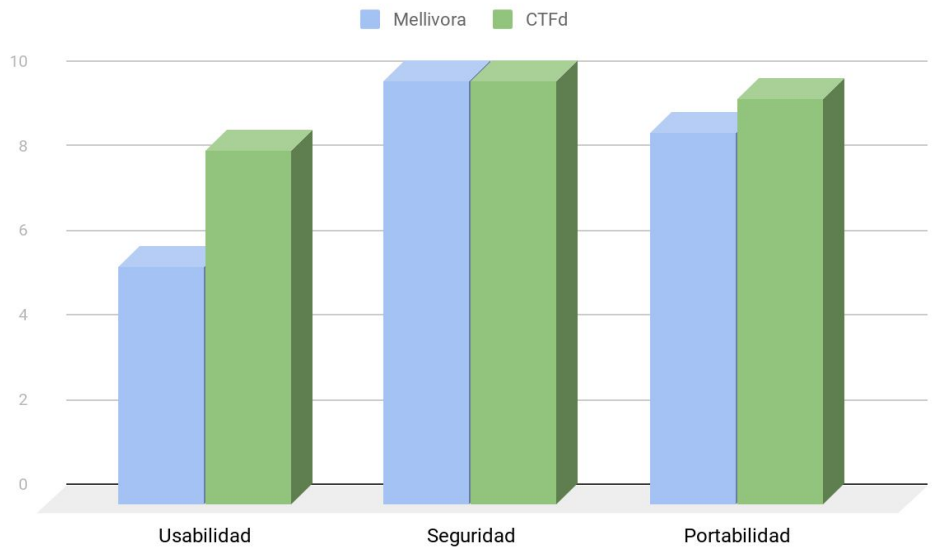


Figura 3 - Evaluación de calidad externa de Mellivora y CTFd

Como se puede apreciar en las tablas y en el gráfico, la diferencia en los resultados entre Mellivora y CTFd se hace notable en la usabilidad que es la característica con mayor porcentaje de importancia de acuerdo con la ponderación que hemos realizado en la sección 4.3.2.1.

A continuación se analizan las subcaracterísticas de usabilidad en donde CTFd ha superado con ventaja a Mellivora:

- Operabilidad
    - La cantidad de pasos que se debe realizar al momento de crear un desafío es un punto importante en el cual se dió una disparidad que se refleja en la diferencia de resultados. En Mellivora la creación de un desafío es bastante burocrática, se establecen dependencias entre operaciones lo cual lo hace menos eficiente. En CTFd este proceso se resume en 2 pasos y no genera ningún tipo de dependencia con otras operaciones.
    - A la hora de acceder a un desafío, la cantidad de pasos que tiene que hacer el usuario es mayor en Mellivora que en CTFd.
- Protección frente a errores de usuario
    - En este apartado es donde CTFd le ha sacado más ventaja a Mellivora. En CTFd de 47 campos que requieren validación, 43 alertan al usuario cuando se ingresa un dato erróneo mientras que en Mellivora de 44 campos que requieren validación sólo 12 alertan al usuario. Esta es una sub-característica muy importante que hace al manejo de errores en la plataforma.
- Estética de la interfaz
    - Ambas plataformas obtuvieron un puntaje bajo a la hora de evaluar la personalización de la apariencia.
- Accesibilidad
    - La evaluación de accesibilidad realizada con SiMor resultó en un 77% de reglas válidas para CTFd contra un 65% para Mellivora. Con estos resultados podemos afirmar que CTFd es más accesible que Mellivora y esta característica es fundamental si queremos incorporar alumnos con discapacidades para que puedan participar en la competencia CTF. Para más detalle se pueden consultar los anexos 8.7 y 8.8.

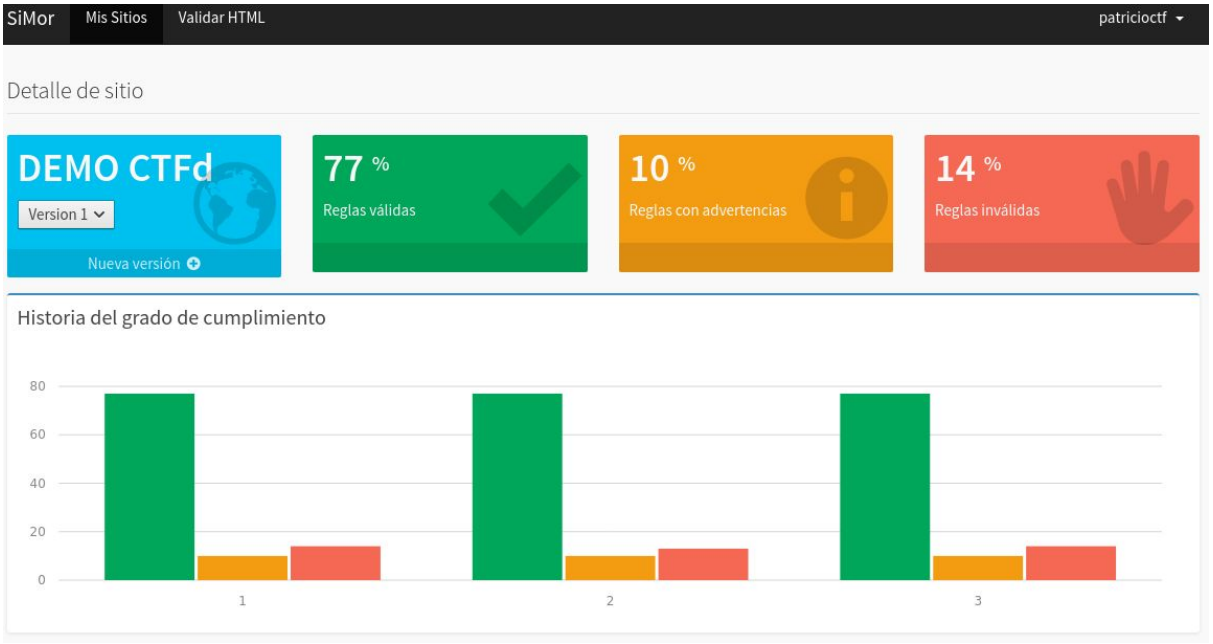


Figura 4 - Análisis global de accesibilidad de CTFd

Con respecto al resto de las características de usabilidad y los valores obtenidos mediante métricas, Mellivora y CTFd tuvieron un comportamiento óptimo en todos los casos:

- Las interfaces son inteligibles debido que la gran mayoría de las funciones provistas al usuario son fáciles de localizar e iniciar. Además las mismas proveen características adicionales que le permiten al usuario entender si el software es adecuado para sus necesidades.
- Las funciones que proveen las plataformas son en su mayoría auto explicativas ya que un mínimo porcentaje de las mismas han resultado inconsistentes respecto a las expectativas de los usuarios.
- Las operaciones provistas por los sistemas son en su mayoría eficientes ya que permiten llevarse a cabo con facilidad.

En el análisis de la seguridad, ambas plataformas respondieron de forma óptima de acuerdo con las sub-características evaluadas. Tanto Mellivora como CTFd proveen más de un método de autenticación y controlan de manera eficaz el acceso no autorizado a funcionalidades sólo provistas al perfil de administrador.

En relación al análisis de la portabilidad se evaluaron dos características:

- En cuanto a la adaptabilidad ambas tienen un buen nivel, habiéndose adaptado a más de dos dispositivos hardware y 3 navegadores diferentes. Si bien ambas superaron las expectativas, Mellivora no logra visualizarse correctamente en celulares.
- La diferencia dada en la facilidad de instalación se produjo dado que la cantidad de pasos de instalación es mayor en Mellivora pero de todas

maneras la instalación se ha podido realizar de manera eficaz en ambas plataformas. Es decir que la diferencia en los valores finales de la portabilidad se debió a que el proceso de instalación es menos eficiente en Mellivora que en CTFd, pese a que ambas pueden instalarse de manera eficaz.

El puntaje total obtenido de CTFd lo ubica con un grado de satisfacción por encima de Mellivora, por lo que concluímos que CTFd es la plataforma más adecuada para implementar la competencia CTF.

4.4 Selección de la plataforma

Luego de haber realizado el análisis de las plataformas y evaluado su facilidad de uso, su seguridad y su portabilidad hemos optado por utilizar CTFd.

Una de las características de CTFd que tuvo mucha relevancia a la hora de decantarnos por esta plataforma fue la posibilidad de hacer backups de la misma. Esta característica permite exportar una competencia ya configurada y luego fácilmente importarla en un servidor que tenga instalada la plataforma.

Otra de las características que nos resultó realmente atractiva de CTFd fue la capacidad de generar estadísticas globales de la competencia y específicas de los usuarios y equipos participantes. Consideramos que estas medidas nos serán de utilidad a la hora de evaluar el desempeño de los alumnos al momento de poner en funcionamiento la competencia.

CTFd permite visualizar listados de respuestas correctas e incorrectas enviadas al servidor. Esta característica es de mucha utilidad para determinar si los participantes están teniendo problemas al ingresar una flag en particular.

CTFd actualmente está siendo muy utilizada por la comunidad:

- De los CTFs evaluados en el capítulo 3, CTFd se utilizó en:
  - HSCTF
  - Tech CTF
  - NACTF
- Facebook utilizó la plataforma CTFd para llevar a cabo su propio CTF que se realizó en el mes de junio del 2019 entre los días sábado 1 y lunes 3 [45].
- La Fundación Sadosky implementó con CTFd la competencia PRECTF 2019 [60] que sirvió de preparación y capacitación para las personas interesadas en participar en el CTF Junior que se desarrolló en septiembre de 2019.
- En la Ekoparty[6] de 2019 se utilizó CTFd como la plataforma elegida para la competencia CTF principal por sobre Facebook CTF utilizada en la edición de 2018.

[6] Ekoparty: es la conferencia de Seguridad Informática más importante de Latinoamérica y se realiza desde hace 15 años en la Ciudad Autónoma de Buenos Aires.

5. Desarrollo del CTF

5.1 Contenido teórico seleccionado

A la hora de seleccionar qué temas tratar en el CTF propuesto hicimos un análisis de las categorías incluidas en los distintos CTFs que evaluamos en la sección 3.1, y concluimos que los temas que se utilizan generalmente son:

- Ingeniería inversa.
- Vulnerabilidades Web.
- Análisis forense.
- Esteganografía.
- Criptografía.
- Explotación de Binarios.
- OSINT o Reconocimiento.
- Programación.
- Habilidades Generales.

El contenido que abordan estas temáticas ha sido detallado en el capítulo 2. Para implementar una competencia que resulte realizable para todos los alumnos participantes, tuvimos en cuenta nuestro contexto educacional, donde podíamos encontrarnos tanto con alumnos que hayan cursado alguna materia de computación como con estudiantes que nunca lo hubieran hecho. Es por ello que de los temas mencionados anteriormente seleccionamos cuatro: OSINT, Ingeniería Social, Criptografía y Esteganografía. Elegimos las temáticas anteriormente mencionadas debido a que nos pareció que podríamos hacer una introducción a estos conceptos planteando desafíos que no requieran poseer conocimientos técnicos previos para su resolución.

Pensamos que al añadir la temática de Ingeniería Social los alumnos pueden tomar noción de las amenazas a las que se enfrenta en la vida cotidiana al momento de utilizar los dispositivos tecnológicos. Mediante la incorporación de desafíos de OSINT pretendemos que los alumnos comprendan la importancia de la privacidad de la información.

La Criptografía es un concepto que se utiliza en el día a día sin siquiera percatarnos de ello, el simple hecho de acceder a una página web que posee https implica la utilización de métodos criptográficos. Por este motivo, hemos decidido introducir esta temática en el CTF de manera que los alumnos empiecen a familiarizarse con el concepto mediante retos que demanden la utilización de métodos criptográficos sencillos que puedan ser resueltos tanto con herramientas online como simplemente de forma manual.

Decidimos integrar la Esteganografía ya que nos pareció que sería una temática atractiva para los alumnos y que nos permitiría hacer desafíos sencillos sin demandar mucho conocimiento técnico para sus resoluciones.

El resto de las temáticas fueron descartadas debido a que para lograr el entendimiento de las mismas se requiere de un alto grado de conocimientos técnicos que en nuestro contexto local se adquieren en la universidad. Aún los desafíos más fáciles para estas categorías necesitan de conocimientos previos por parte de los participantes. Por ejemplo, para resolver los ejercicios de ingeniería inversa se requiere del manejo de conceptos relacionados con programación a bajo nivel, o si quisiéramos realizar un desafío de vulnerabilidades web, deberíamos primero introducirlos en el concepto de la web, de la arquitectura cliente - servidor, etc., para que sea accesible para todos, lo cual atentaría contra la dinámica de la competencia.

Los desafíos fueron planteados de manera que puedan ser resueltos con herramientas online. Nos independizamos de las herramientas del sistema operativo subyacente para disminuir la dificultad de los ejercicios por falta de conocimiento técnico en el uso de los mismas.

Dentro de la plataforma de competencia brindamos una breve explicación teórica introductoria a las temáticas para que el alumno pueda utilizarla para orientarse en la resolución de los desafíos. La idea de la utilización de material explicativo surgió como una crítica a los CTFs convencionales que sólo proveen desafíos sin ningún tipo de orientación. Nuestro objetivo fue proveer a los alumnos de un material extra para ponerlos en contexto y que comprendan la finalidad del ejercicio.

Todos los desafíos fueron armados de manera que sean accesibles para todos los participantes. Para el desarrollo de los mismos tuvimos en cuenta que sería la primera vez en que los alumnos participaban en una competencia de seguridad informática, por lo que podían desconocer tanto las temáticas como la modalidad del juego.

En la temática OSINT, incluimos ejercicios que tienen como objetivo que los alumnos aprendan a realizar búsquedas avanzadas para obtener resultados más precisos. Para ello debían utilizar herramientas online como Google Hacking[7], Internet Archive[8] [61], y el buscador de imágenes de Google. También planteamos ejercicios en los que los alumnos tenían que pensar la secuencia de búsquedas a realizar para obtener información específica a partir de un conjunto dado de datos reducidos.

[7] Google Hacking: es una herramienta que provee Google para optimizar las búsquedas y obtener información específica mediante el uso de operadores.

[8] Internet Archive: es una biblioteca digital dedicada a la preservación de archivos digitales, capturas de sitios de la Web, recursos multimedia y software.

Para la categoría de Ingeniería Social hicimos una descripción de la temática junto con una breve explicación de los conceptos Phishing[9], y Punycode[10]. Nuestro objetivo fue generar conciencia en los alumnos de los peligros de estas técnicas utilizadas por personas malintencionadas.

En Criptografía hicimos hincapié en los métodos de criptografía clásica ya que nos pareció una buena manera de introducirlos en la temática y que comprendan el concepto básico. Dentro de los métodos de criptografía clásica desarrollamos ejercicios que implican el uso de dos tipos de cifrado: ellos son el cifrado por sustitución y por transposición.

En la temática de Esteganografía desarrollamos ejercicios en los que se utilizaron distintos métodos para ocultar objetos dentro de otros: un texto dentro de una imagen, una imagen dentro de otra imagen, un texto dentro de una imagen con contraseña y un mensaje dentro de un archivo de audio.

5.2 Configuración general del CTF

Como mencionamos en el capítulo 4, para el desarrollo del CTF utilizamos la plataforma CTFd. La competencia que realizamos la pusimos en práctica dos veces dentro del marco del proyecto de extensión. Para cada instancia de prueba realizamos distintos configuraciones, pero en ambas mantuvimos las mismas categorías de los ejercicios: OSINT, Ingeniería Social, Criptografía, y Esteganografía.

En ambas pruebas comenzamos el CTF con un ejercicio de muestra, para que los alumnos puedan comprender con facilidad cómo utilizar la plataforma para resolver los desafíos. El flujo de ejecución de los ejercicios lo configuramos de manera que los alumnos puedan acceder a los desafíos desde los más fáciles hasta los más difíciles de manera progresiva, es decir, que ordenamos los ejercicios en función de su dificultad.

[9] Phishing: es un tipo de ingeniería social que utiliza elementos técnicos para engañar a un usuario y lograr que éste entregue involuntariamente información confidencial a usuarios malintencionados.

[10] Punycode: Es una técnica que permite traducir un conjunto de caracteres de un alfabeto a caracteres del alfabeto latino.

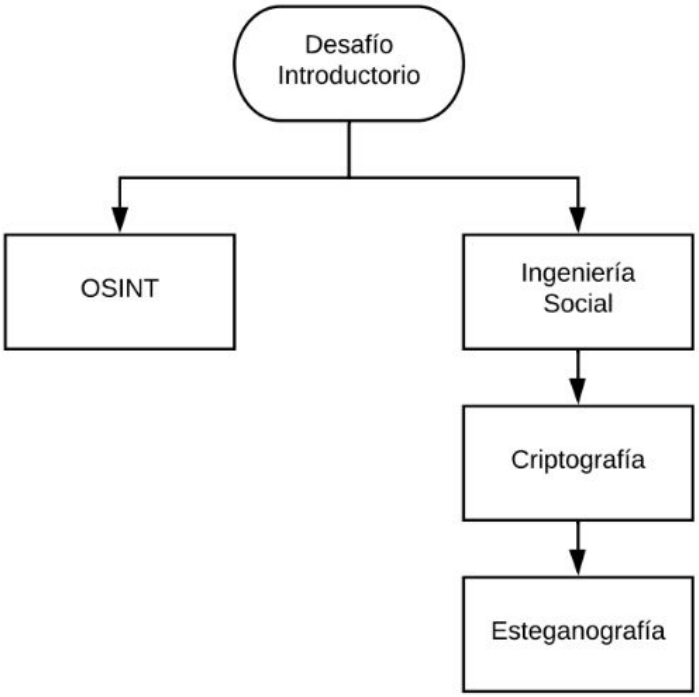


Figura 5 - Dependencias entre categorías

5.3 Modalidad del juego

La competencia se realiza entre equipos. Cada equipo puede estar constituido por una persona o un grupo de participantes. En primera instancia los alumnos deben registrarse en la plataforma y luego unirse a un equipo ya existente, ingresando el nombre del equipo y la contraseña del mismo. Para agilizar la registración de los equipos, los creamos antes de que inicie la competencia de manera que los alumnos sólo tengan adherirse a uno de ellos.

La competencia se configura con un horario de comienzo, por lo que una vez registrados y habiendo iniciado sesión en la plataforma, los alumnos deben esperar a que comience el juego. Se configura de tal forma para evitar que los alumnos que ingresen primero comiencen a jugar y saquen ventaja sobre los que todavía no lo hicieron. Mientras que el juego se encuentra deshabilitado no se pueden visualizar los desafíos.

Una vez iniciada la competencia, dentro de la página “Challenges”, los alumnos pueden acceder a los desafíos. Todos los retos poseen un puntaje. Si uno de los participantes responde correctamente un desafío, el mismo se resuelve para todo su equipo, sumándole puntos al mismo. Si la respuesta es incorrecta, sólo se alerta al usuario que su respuesta no es válida, no se decrementan puntos ni se penaliza al equipo de ninguna manera. La cantidad de intentos para responder es ilimitada.

Figura 6 - Desafíos del CTF

Dentro de los desafíos pueden haber ayudas, denominadas “hints”, que pueden o no costar puntos. El alumno puede decidir utilizar la ayuda o no. Si decide utilizarla se le resta al puntaje del equipo el valor de la misma.

Cada desafío se presenta como un botón que posee un nombre. Al hacer click sobre uno de los botones se abre una nueva ventana que especifica qué debe realizarse y un campo para ingresar la respuesta. La respuesta debe respetar un determinado formato.

Algunos desafíos contaron con filminas explicativas que los alumnos podían utilizar de manera opcional para guiarse en la resolución de los ejercicios.

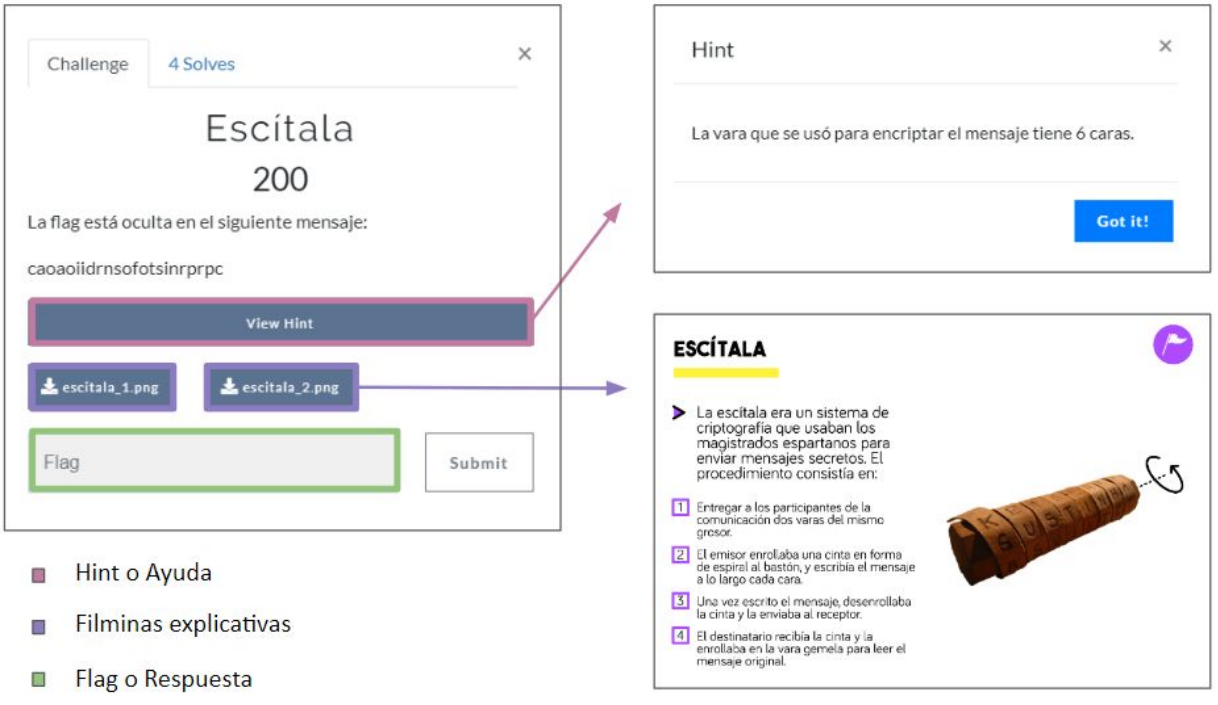


Figura 7 - Desafío de la Escítala

Todos los participantes de la competencia deben respetar y adherirse a las siguientes reglas del juego:

- No deben pasarse las flags o dar pistas entre equipos.
- El ataque a la plataforma está totalmente prohibido.
- Si se cambia o arregla un reto se avisará en el momento.
- En caso de romper las reglas, el equipo será penalizado perdiendo puntos.

El equipo ganador es aquel que posee el puntaje más alto al finalizar el juego, y en caso de haber un empate, el ganador es el que resolvió los ejercicios más rápidamente.

6. Puesta en Práctica

6.1 Primera evaluación

La primer instancia de evaluación fue realizada el día viernes 18 de octubre del 2019 a las 9:00 hs en el aula 7 de la Facultad de Informática y contó con la presencia de 6 alumnos pertenecientes a las escuelas N° 14 de La Plata y la Técnica N° 5 de VIlla Elvira.

6.1.1 Configuración del CTF

El flujo de resolución de los ejercicios se configuró de la siguiente manera:

- En primera instancia los alumnos sólo podían visualizar un único desafío de prueba, cuya finalidad era que comprendan cómo utilizar la plataforma.
- Una vez resuelto el desafío inicial se habilitaban los ejercicios de OSINT e Ingeniería Social.
- Uno de los ejercicios de Ingeniería Social habilitaba los ejercicios de Criptografía y uno de los ejercicios de Criptografía habilitaba los ejercicios de Esteganografía.

En la página principal de la plataforma detallamos las reglas del juego a las que debían adherirse los participantes. En esta página explicamos que las respuestas debía escribirse con un formato específico para ser consideradas válidas.

Dentro de la plataforma creamos una página denominada “Temas” donde explicamos los conceptos básicos de OSINT, Ingeniería Social, Criptografía y Esteganografía para poner a los alumnos en contexto y orientarlos en la resolución de los ejercicios.

6.1.2 Descripción de la competencia

En esta instancia participaron 6 alumnos: 1 alumno de la escuela N° 14 de La Plata y 5 alumnos de la escuela técnica N°5 de Villa Elvira.

Información de los participantes:

- Edad: entre 15 y 16 años.
- Año que cursan: 4to.

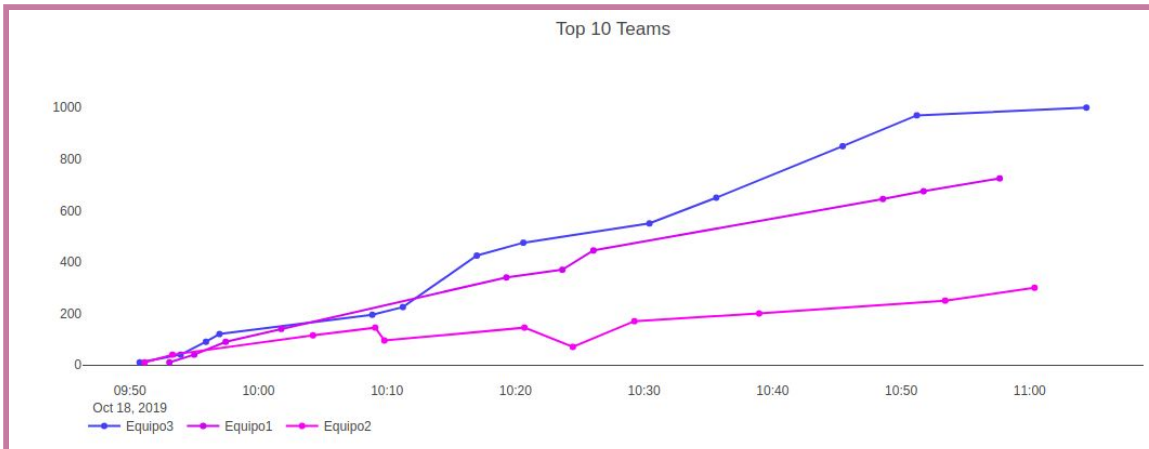
La competencia contó con las siguientes características:

- Duración de la Competencia: 1 hora y 20 minutos.
- Cantidad de Grupos: 3.
- Cantidad total de participantes: 7 (6 alumnos y una profesora).
- Cantidad de desafíos: 16.
- Valor de los desafíos: desde 30 hasta 200 puntos.
- Costo de las ayudas: desde 50 hasta 75 puntos.
- A cada participante se le brindó una computadora durante la competencia.

Los alumnos conformaron 3 grupos distintos:

- El equipo número 1 se compuso de 3 alumnos de la escuela técnica N°5.
- El equipo número 2 se compuso de 2 alumnos de la escuela técnica N°5.
- El equipo número 3 se compuso del alumno de la escuela N° 14 y su profesora.

6.1.3 Desempeño de los participantes



Place	Team	Score
1	Equipo3	1000
2	Equipo1	725
3	Equipo2	300

Figura 8 - Tabla de puntuaciones finales de la primer evaluación

Como resultado se obtuvieron:

- Cantidad de respuestas correctas: 32 (19.5 %).
- Cantidad de respuestas incorrectas: 132 (80.5 %).
- Puntaje más alto: 1000 (resolución de 13 desafíos sin ayudas).
- Puntaje más bajo: 300 (resolución de 9 desafíos con 2 ayudas que restaron 125 puntos).

6.1.4 Dificultades

Por lo general, se nos presentaron las siguientes dificultades:

- A los alumnos se les complicó el formato de las flags debido a que establecimos respuestas estáticas, por lo cual si ingresaban un espacio o una coma de más en la respuesta, la plataforma la interpretaba como incorrecta a pesar de que la resolución estuviera bien.
- Durante la competencia, pudimos observar que los chicos no utilizaron la página “Temas”, en la cual se hacía una breve introducción a cada una de las categorías. Esto provocó que en muchos ejercicios no comprendieran el contexto y como consecuencia no supieran cómo encarar el desafío.
- Los alumnos realizaron las búsquedas de las herramientas online en idioma español lo que generó que los resultados obtenidos no contengan dichas herramientas. Las búsquedas en inglés son mucho más precisas, por lo que aquí se nos presentó una barrera idiomática.
- Notamos que los alumnos tuvieron complicaciones a la hora de interpretar cuál era la flag dentro de la respuesta obtenida. Por ejemplo, en varios ejercicios, se devolvía un texto similar al siguiente: “Bien hecho! Pudiste descifrar el mensaje! La flag es ***” y los alumnos ingresaban todo el texto en vez de sólo la flag.
- En algunos desafíos las ayudas costaban mucho puntaje porque brindaban el enlace a la herramienta con la cual podían resolver el ejercicio. Esto provocó que los alumnos, además de no entender cómo encarar el desafío por no haber leído la página “Temas”, no quisieran utilizar la ayuda porque les restaba mucho puntaje. En estos casos en particular detectamos que no se presentaba un punto intermedio: por un lado, no comprendían qué es lo que debían hacer y por el otro, la ayuda les daba directamente la respuesta.

También tuvimos complicaciones en desafíos puntuales:

- Dentro de la categoría de Criptografía hicimos un ejercicio en el que los alumnos debían descifrar un mensaje encriptado con el método de la Escítala. Este procedimiento es difícil de entender rápidamente sin ningún

tipo de explicación. En esta instancia no brindamos material teórico para la resolución de este ejercicio por lo que a los alumnos les resultó difícil resolverlo.

- En la categoría de Ingeniería Social tuvimos las siguientes dificultades:
    - Hicimos un desafío denominado “Sitios falsos” donde brindamos un conjunto de sitios en el cual los alumnos debían identificar y responder cuáles eran falsos. Pero el formato de la respuesta que exigimos era complicado: para que la flag sea considerada correcta, los alumnos debían transcribir los sitios falsos manualmente para evitar ingresar caracteres extraños, por lo que no podían copiar y pegar. Además, la gran mayoría de los sitios eran falsos, por lo cual la resolución se complicó por el formato y la longitud de la respuesta, no por la dificultad del ejercicio.

Figura 9 - Desafío sitios falsos

Figura 10 - Flag del desafío sitios falsos

    - Realizamos un desafío en el que los alumnos debían descifrar un mensaje escrito en formato Punycode y pasarlo al alfabeto latino. Este desafío les resultó difícil de resolver porque en esta instancia no habíamos brindado una explicación del concepto.

- En la categoría de OSINT hicimos un ejercicio denominado “Búsqueda difícil” en el que a partir de la foto de una persona los alumnos debían encontrar su nombre completo y su DNI. Uno de los percances que tuvimos fue que contabamos con la disponibilidad de la página dateas.com para la resolución del ejercicio, pero en el momento de la competición, no se encontraba accesible. Y el segundo percance fue que a los alumnos se les complicó el formato de la flag.
- En todos los ejercicios de Esteganografía los alumnos no comprendieron cuál era la finalidad de los mismos al no haber leído la pequeña introducción al concepto dada en la página “Temas”. Por otro lado hubo muchas dificultades para encontrar las herramientas online para resolverlos.

6.1.5 Conclusiones

En esta primera instancia notamos que los alumnos comprendieron rápidamente la modalidad del juego y que estaban motivados con la competencia. Unas de las estrategias de motivación que utilizamos fue proyectar en la pared la tabla de posiciones y ofrecer premios para el equipo que terminara en el primer puesto.

Al ser la primera vez que pusimos en práctica la plataforma, la actividad fue bastante guiada para que los alumnos puedan resolver los ejercicios pese a las dificultades que fueron surgiendo. Como el foco siempre estuvo puesto en la motivación, estuvimos siempre atentos a las dudas que les fueron surgiendo a los alumnos para que no se frustren y los incentivamos a que intenten con otros desafíos cuando se trababan con la resolución de alguno en particular. Al tratarse de una competencia en la cual el equipo ganador es el que obtiene la mayor cantidad de puntos, los alumnos encaraban aquellos desafíos con puntaje más alto dejando de lado aquellos más simples que por sumatoria de puntaje les permitirían subir posiciones en la tabla de puntuaciones.

En esta primera prueba, actuamos como mentores durante la competencia para guiar a los alumnos en la resolución de los desafíos. Decidimos adoptar este rol debido que era el primer CTF en el que participaban los alumnos y que la duración del juego era corta comparado con los CTFs evaluados en la sección 3.1 los cuales duraron entre 3 y 14 días permitiendo que los participantes pudieran resolver los desafíos con mayor comodidad.

Las ayudas las hemos brindado de manera equitativa a todos los equipos participantes, de manera que todos se encontraran en igualdad de condiciones y puedan resolver la mayor cantidad de desafíos.

La revisión constante de las respuestas enviadas al servidor fue de gran ayuda para avisar a los alumnos si estaban por el camino correcto en la resolución. Por ejemplo, si habían ingresado todo el mensaje con la flag incluída.

6.1.5.1 Devolución de los alumnos

Luego de la competencia les solicitamos a los alumnos que respondan una breve encuesta que se encuentra en el anexo 8.9. De ellas concluimos que:

- Era la primera vez en que los alumnos participaban en una competencia de seguridad informática.
- La plataforma les resultó fácil de usar.
- Los alumnos respondieron que el nivel de dificultad de los desafíos fue intermedio, lo cual, desde nuestro punto de vista, fue una devolución positiva ya que no queríamos que los ejercicios fueran fáciles al punto de que resulten aburridos ni tampoco muy difíciles y que se frustren a la hora de resolverlos.
- El tiempo de duración de la competencia no les pareció suficiente.
- Les gustó el taller y les gustaría volver a participar.

6.1.5.2 Mejoras efectuadas

Hemos perfeccionado la competencia para una segunda instancia de prueba solucionando aquellas dificultades que hemos detallado en la sección 6.1.4 y teniendo en cuenta la devolución obtenida por parte de los alumnos descritas en la sección 6.1.5.1. En la tabla 11 se describen los problemas surgidos en la primer evaluación y la soluciones planteada para la segunda prueba. También realizamos mejoras a la plataforma que se describen en la tabla 12.

Problema	Solución
A los alumnos les resultó corto el tiempo de duración del CTF.	Prolongar la duración de la competencia.
Barrera idiomática a la hora de realizar las búsquedas.	Poner un desafío de traducción del español al inglés en la plataforma. La idea es que se acostumbren a realizar las búsquedas en inglés para que encuentren fácilmente las herramientas online.
Dificultad del formato de las flags. Utilización de respuestas estáticas, que debían respetar la sintaxis flag{respuesta}.	Quitar el formato “flag{respuesta}” y que los alumnos sólo tengan que introducir el resultado obtenido del desafío. Utilizar expresiones regulares, de manera de evitar que los espacios en blanco, las comas u otros caracteres invaliden la respuesta dada por el alumno.
Los estudiantes no utilizaron la página “Temas”, en la cual se hacía una breve introducción a las distintas categorías de los desafíos. Al no comprender el contexto de los ejercicios se les complicó entender la finalidad de los mismos.	Sacar la página “Temas” y embeber el contenido teórico en desafíos dentro de la competencia. Crear un desafío introductorio en cada una de las categorías, el cual contiene una infografía con una descripción de la temática.
Dificultad en la resolución de los desafíos de Punycode, Escítala, y en los ejercicios de Esteganografía.	Agregar filminas explicativas en aquellos ejercicios en que los alumnos no supieron comprender la finalidad del ejercicio.
Algunas ayudas brindaban el enlace a la herramienta con la cual podían resolver el ejercicio. No había punto medio: los alumnos no comprendían qué se debía hacer y la ayuda les daba directamente la respuesta.	Modificar las ayudas de manera que no provean las herramientas sino las palabras claves que simplifiquen su búsqueda.

Tabla 11 - Mejoras efectuadas para la segunda instancia de prueba

Estado de la Plataforma	Mejoras efectuadas
Utilizamos un logo de la Facultad de Informática de la UNLP.	Cambiamos el logo de la facultad por el logo del Proyecto de Extensión y agregamos una descripción del mismo en la página principal de la plataforma.
En la primer instancia de prueba, instalamos al CTF en un servidor que alquilamos a la empresa Digital Ocean.	Para la segunda prueba, lo instalamos en un servidor de la facultad con el nombre de dominio ctf-escuelas.linti.unlp.edu.ar.
Utilizamos http.	Utilizamos https.

Tabla 12 - Mejoras efectuadas a la plataforma para la segunda evaluación

6.2 Segunda evaluación

La segunda instancia de evaluación fue realizada el día miércoles 13 de Noviembre del 2019 a las 10:00 hs en el aula 1 de la Facultad de Informática y contó con la presencia de 18 alumnos pertenecientes a las escuelas N° 14 de La Plata, Liceo Víctor Mercante y N° 50 de Tolosa.

6.2.1 Configuración del CTF

En función de los percances que tuvimos en la primer instancia, creamos dos ejercicios iniciales: uno para mostrarle a los alumnos cómo ingresar las respuestas en la plataforma, y otro ejercicio donde les pedíamos que utilicen el traductor de Google para que comprendan cómo realizar búsquedas en inglés y así puedan encontrar las herramientas necesarias para resolver los ejercicios de forma rápida.

Dado que en la primer instancia los alumnos no utilizaron la página “Temas” para orientarse en la resolución de los ejercicios, decidimos embeber el contenido teórico en los mismos desafíos. Para ello desarrollamos filminas que explicaban los conceptos básicos de OSINT, Ingeniería Social, Criptografía y Esteganografía. Las filminas fueron desarrolladas por un diseñador gráfico de manera que sea agradable y legible para los alumnos. Nos aseguramos de que las filminas contengan conceptos puntuales, concisos y que su redacción sea de fácil interpretación, evitando el uso de un lenguaje técnico y utilizando un lenguaje más coloquial.

Dentro de cada una de las categorías, creamos un desafío inicial que contenía una filmina (a la cual se podía acceder de manera opcional) en la que se explicaba los conceptos básicos de la categoría. Una vez resuelto el ejercicio inicial se habilitaban el resto de los ejercicios de la misma categoría.

El flujo de resolución de los ejercicios se configuró de la siguiente manera:

- En primera instancia habilitamos el ejercicio de muestra y el de traducción.
- Una vez resueltos los desafíos iniciales se habilitaba la categoría de OSINT y la de Ingeniería Social.
- Uno de los ejercicios de Ingeniería Social habilitaba la categoría de Criptografía y uno de los ejercicios de Criptografía habilitaba la categoría de Esteganografía.

También incorporamos filminas en aquellos desafíos en los cuales los alumnos habían tenido dificultades de interpretación en la primer instancia de prueba. Todas las filminas se podían utilizar de manera opcional.

Modificamos la página principal de la plataforma y allí pusimos una descripción del Proyecto de Extensión en Vínculo con Escuelas junto con su logo.

Dentro de la plataforma creamos una página denominada “Reglas” donde detallamos las reglas del juego a las que debían adherirse los participantes.

Agregamos más desafíos en las categorías de OSINT, Criptografía y Esteganografía teniendo en cuenta que el tiempo de la competencia iba a ser mayor en esta segunda instancia y teniendo el antecedente de que en la instancia previa los alumnos tuvieron una muy buena performance en la resolución.

6.2.2 Descripción de la competencia

En esta instancia participaron 18 alumnos: 3 del colegio Liceo Víctor Mercante, 10 de la escuela N° 14 de La Plata y 5 de la escuela N° 50 de Tolosa.

Información de los participantes:

- Edad: entre 14 y 17 años.
- Año que cursan: 3ro.

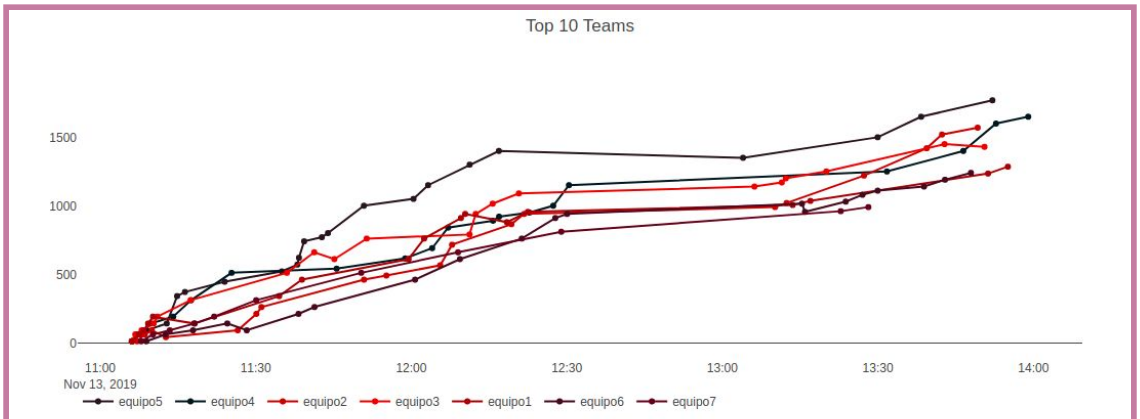
La competencia contó con las siguientes características:

- Duración de la Competencia: 3 hs con un recreo de media hora.
- Cantidad de Grupos: 7.
- Cantidad total de participantes: 18.
- Cantidad de desafíos: 25.
- Valor de los desafíos: desde 30 hasta 200 puntos.
- Costo de las ayudas: desde 20 hasta 110 puntos.
- Se repartieron 2 computadoras por equipo.

Los alumnos conformaron 7 grupos distintos:

- El equipo número 1 se compuso de 2 alumnos de la escuela N°14.
- El equipo número 2 se compuso de 2 alumnos de la escuela N°14.
- El equipo número 3 se compuso de 3 alumnos del Liceo Víctor Mercante.
- El equipo número 4 se compuso de 3 alumnos de la escuela N° 14.
- El equipo número 5 se compuso de 3 alumnos de la escuela N° 14.
- El equipo número 6 se compuso de 2 alumnos de la escuela N° 50.
- El equipo número 7 se compuso de 3 alumnas de la escuela N° 50.

6.2.3 Desempeño de los participantes



Place	Team	Score
1	equipo5	1775
2	equipo4	1655
3	equipo2	1575
4	equipo3	1435
5	equipo1	1290
6	equipo6	1245
7	equipo7	995

Figura 11 - Tabla de puntuaciones finales de la segunda evaluación

Los resultados obtenidos fueron:

- Respuestas correctas: 122 (17 %).
- Respuestas incorrectas: 595 (83 %).
- Puntaje más alto: 1775 (21 desafíos resueltos con una ayuda que les descontó 50 puntos).
- Puntaje más bajo: 995 (11 desafíos resueltos sin ayudas).

6.2.4 Dificultades

En esta segunda instancia de evaluación de la plataforma pudimos superar la mayoría de los problemas que surgieron en la primera prueba. Pero tuvimos dificultades con desafíos puntuales:

- En el ejercicio de cifrado Vigenere, no especificamos qué método se había utilizado para encriptar el mensaje original, sino que incluimos la imagen de la tabla que se utiliza en este cifrado para que los alumnos utilicen Google Imágenes y así descubran que método se había utilizado. Pero al ingresar esa imagen en el buscador de imágenes de Google el resultado de la búsqueda devolvía “sopa de letras tema excel” confundiendo a los alumnos en la resolución del desafío.
- A los alumnos les costó mucho entender el ejercicio de OSINT que consistía en utilizar Internet Archive para buscar el precio de un pendrive en deremate.com en el año 2005. Por lo que decidimos hacer una explicación en el aula que sirva como ayuda en la resolución del desafío. A partir de esta ayuda, los alumnos pudieron lograr la resolución del desafío en cuestión y del siguiente que consistía en buscar en cuáles cines de La Plata se estrenó la película de batman del 2008.
- Con el desafío de Google Hacking pasó algo similar que con el de Internet Archive. En este caso preparamos una filmina explicativa pero los alumnos no terminaron de entender el concepto y, si bien se les brindó ayuda, les costó bastante llegar a la resolución. Como una mejora a implementar, se podría utilizar un ejercicio introductorio en el que se realice una búsqueda menos compleja y que el mismo habilite a este desafío.
- Se volvió a presentar el problema a la hora de interpretar cuál es la flag dentro de la respuesta obtenida. Porque muchas respuestas dadas por los alumnos contienen todo el mensaje descifrado en vez de la flag incluída en dicho mensaje.

6.2.5 Conclusiones

En esta segunda etapa se triplicaron tanto la cantidad de alumnos como el tiempo de duración de la competencia por lo que esta experiencia fue más enriquecedora que la primera. Se pudo armar un mayor número de equipos y los alumnos tuvieron más tiempo para resolver los desafíos.

En general los alumnos pudieron resolver los ejercicios más fáciles, pero en la resolución de los desafíos de OSINT y Criptografía se notó mucha diferencia entre las distintas escuelas.

Si bien adoptamos el rol de mentores durante la competencia, tratamos de que los alumnos intenten resolver los desafíos de manera independiente, apoyándose en el contenido teórico provisto en las filminas.

Para nivelar la tabla de posiciones focalizamos las ayudas en aquellos equipos que iban más rezagados minimizando las mismas para los equipos que estaban en el podio.

Los dos equipos que sumaron menos puntos fueron los de la escuela N° 50 de Tolosa que es un colegio con muchas vulnerabilidades sociales, que no ha dictado clases durante un período de tiempo prolongado y en el que los alumnos se encuentran en estado de reescolarización. Observamos que los estudiantes tenían muchos problemas de interpretación de lectura, por lo que los acompañamos durante todo el proceso para que puedan resolver algunos retos y no se sientan excluidos o frustrados al no poder avanzar. Notamos que prestaron mucha atención a las explicaciones que les brindamos, y así pudieron entender los conceptos y relacionarlos con situaciones de la vida diaria (por ejemplo asociar el phishing con el fraude con las tarjetas de crédito).

Uno de los equipos participantes estaba integrado por el alumno que había salido ganador en la primer instancia de prueba. Por lo que minimizamos las ayudas brindadas al mismo para lograr equidad entre los equipos. Al final de la competencia el equipo terminó en el primer puesto. Analizando esta situación podemos confirmar que para este alumno fue mucho más fácil la resolución de los desafíos y esto se refleja en el desempeño del participante dentro del equipo ya que acertó 16 desafíos de los 21 retos resueltos. A partir de estas observaciones concluimos que el estudiante logró incorporar el conocimiento de las temáticas y el manejo de la plataforma en su primer experiencia con el CTF por lo que esto lo aventajó en la segunda competencia.

Un apartado positivo fue que todos los alumnos contaron con el apoyo de sus respectivos docentes escolares que los ayudaron y motivaron en la resolución de los desafíos.

Hemos notado una mejora respecto a la primer instancia de prueba ya que la mayoría de las consultas realizadas por los alumnos tuvieron que ver con las temáticas planteadas y no con el formato de las flags.

6.2.5.1 Devolución de los alumnos

Luego de la competencia les solicitamos a los alumnos que respondan una breve encuesta que se encuentra en el anexo 8.10. De ellas concluimos que:

- Era la primer vez que los alumnos participaban en una competencia de seguridad informática.
- La plataforma les resultó fácil de usar.
- El tiempo de duración de la competencia les pareció suficiente.
- Les gustó el taller y les gustaría volver a participar.

6.3 Análisis de los Resultados de las Encuestas

Obtuvimos 11 encuestas en total:

- De la primera instancia de prueba tenemos:
    - 3 encuestas de los alumnos de la escuela Técnica N° 5.
- De la segunda instancia de prueba tenemos:
    - 3 encuestas de los alumnos de la escuela N° 14.
    - 2 encuestas de las alumnas del Liceo Víctor Mercante.
    - 3 encuestas de los alumnos la escuela N° 50.

A continuación exponemos los datos que resultaron de nuestro mayor interés. Las medidas evaluadas tienen en cuenta la totalidad de las encuestas obtenidas, tanto de la primera instancia de prueba como de la segunda.

¿La plataforma te resultó fácil de usar?

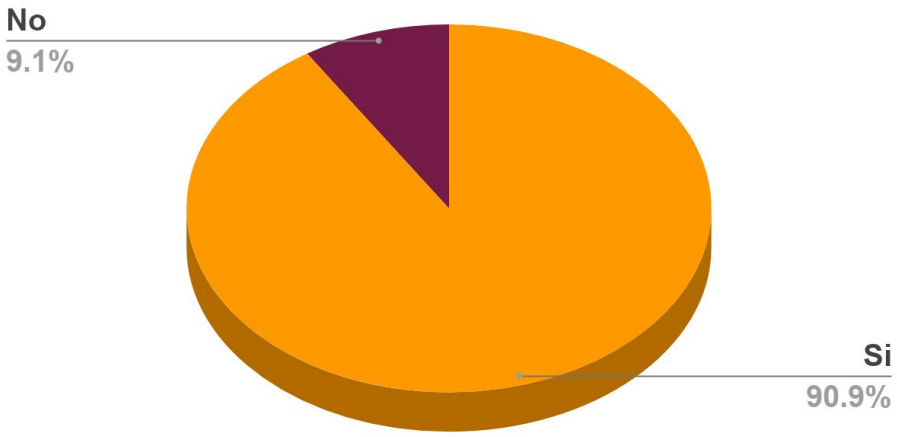


Figura 12 - Resultados encuesta: Facilidad de la plataforma

Del total de los encuestados, 10 alumnos respondieron que la plataforma fue fácil de usar. Sólo un alumno de la escuela número 50 respondió que no le resultó sencilla.

¿Qué te parecieron los retos del CTF? (Muy fáciles, fáciles, intermedios, difíciles, Muy difíciles).

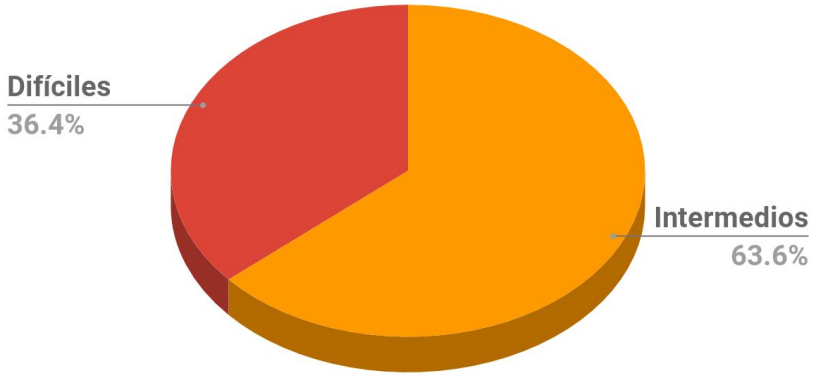


Figura 13 - Resultados encuesta: Dificultad de los desafíos

7 alumnos contestaron que la complejidad de los desafíos les resultaron de nivel intermedio y otros 4 que les resultaron difíciles. Los alumnos a los que se les dificultó la resolución fueron: uno de la escuela N° 14, un alumno del Liceo y dos de la escuela N° 50.

¿Conocías alguno de los temas relacionados a los desafíos?

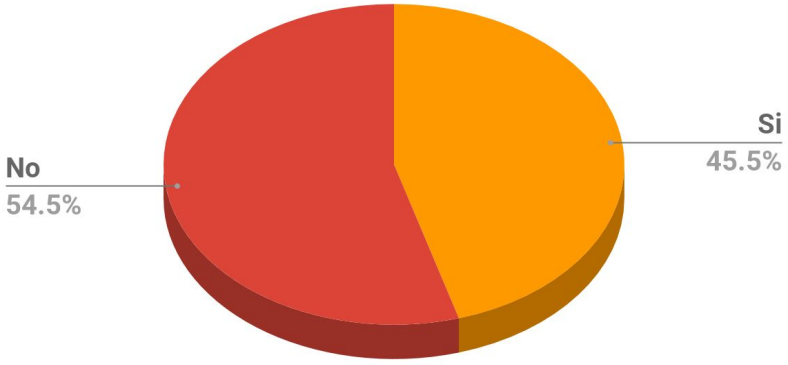


Figura 14 - Resultados encuesta: Conocimiento de las temáticas

6 alumnos contestaron que no conocían los temas abordados en los desafíos y otros 5 contestaron que conocían algunos temas de videos e información publicados en internet, de amigos con más conocimiento y de los scouts.

¿Te gustaría volver a participar?

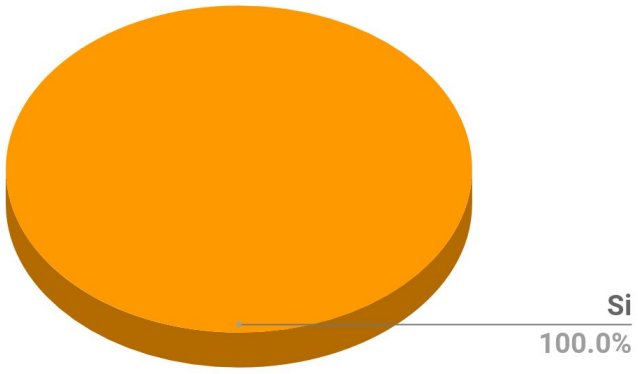


Figura 15 - Resultados encuesta: Volver a participar

Todos los alumnos que completaron las encuestas contestaron que les gustaría volver a participar. Las encuestas se encuentran en los anexos 8.9 y 8.10.

7. Conclusiones y Trabajo Futuro

7.1 Conclusiones

Luego de haber investigado y desarrollado esta tesina, consideramos que hemos logrado la gran mayoría de los objetivos propuestos: desarrollamos una competencia de ciberseguridad dirigida a los estudiantes de escuelas secundarias que se ha puesto en práctica en el marco del proyecto de extensión y que posibilitó, mediante un enfoque lúdico, que los alumnos aprendan conocimientos en el área de seguridad informática. Hemos aplicado una modalidad de enseñanza utilizada hoy en día en Europa y América del Norte adaptándola a nuestro contexto local.

La plataforma seleccionada para el desarrollo del CTF no nos ha generado ningún tipo de inconveniente a la hora de instalarla, configurarla y usarla. Una desventaja de la plataforma es que sólamente se encuentra en idioma inglés, pero independientemente del lenguaje, al tener una interfaz gráfica tan intuitiva, nos resultó fácil de administrar y a los alumnos fácil de utilizar.

Una de las críticas que resaltamos sobre las competencias CTF investigadas es que no proveen ningún tipo de introducción a las temáticas. En nuestro CTF hemos provisto de material teórico dentro de la misma competencia para poner en contexto a los alumnos y guiarlos en la resolución de los desafíos. Esto sirvió como punto de partida a la hora de encarar la resolución de los retos y facilitó la comprensión de los objetivos planteados en los mismos.

A partir de la experiencia vivida en la puesta en práctica del CTF y de la devolución que obtuvimos de los estudiantes, consideramos que integrar este tipo de actividades en el aula resultará motivador para los alumnos. Los estudiantes se involucraron rápidamente en la competencia y la dificultad de los desafíos que les propusimos no los desanimó en ningún momento.

Pese a la diferencia en el nivel educativo de las distintas escuelas, los alumnos tuvieron una performance más que aceptable en ambas experiencias y, como lo reflejan las encuestas, el 100% de encuestados volvería a participar. Por estos motivos, concluimos que esta herramienta ha significado un aporte muy valioso para el proyecto de extensión en vínculo con escuelas. Teniendo esto en mente, pensamos continuar involucrados brindando soporte y actualizando los desafíos una vez culminada la realización de esta tesina.

7.2 Trabajo a Futuro

7.2.1 Utilización de la plataforma en el aula

Al desarrollar ambas experiencias notamos mucho interés de parte de los docentes escolares ya que se involucraron en la competencia formando parte del equipo o ayudando a resolver los desafíos.

Muchas de las consultas recibidas durante la competencia tuvieron que ver en cómo aplicar la plataforma en el ámbito del aula.

Para futuras competencias se podría preparar una plataforma dirigida a los docentes para que los mismos la evalúen durante el desarrollo del juego. En dicha plataforma, cada docente tendría el rol de administrador para acceder a todas las funcionalidades.

Por otra parte, se les puede proveer a los docentes la competencia configurada de manera que puedan utilizarla en el aula. El docente como administrador tendría la capacidad de generar nuevos ejercicios o adaptar los existentes al contexto escolar. También se les podría brindar una página aparte en la misma plataforma con las soluciones de los desafíos para guiar a los docentes en la resolución de los mismos.

También consideramos que esta plataforma puede ser fácilmente adaptada y utilizada por los docentes a la hora de enseñar cualquier tipo de temáticas, más allá de la ciberseguridad. Ello les permitirá aplicar una metodología de enseñanza lúdica que motive a los alumnos a aprender jugando.

7.2.2 Utilización de la plataforma en la Facultad

Esta plataforma podría adaptarse para ser utilizada en materias de la misma Facultad de Informática de la UNLP a la hora de presentar las optativas. Así se podría interiorizar a los alumnos en conceptos de seguridad y en las modalidades de competencia utilizadas hoy en día. Esta plataforma podría motivar a los alumnos a perfilarse al área de seguridad informática y seleccionar las materias relacionadas a estas temáticas.

7.2.3 Introducción previa a la competencia

A modo de disminuir desigualdades entre los participantes respecto al conocimiento en las temáticas, se podría realizar una actividad de capacitación previa a la competencia y así poner a los alumnos en contexto.

Esta idea fue aplicada en la experiencia educacional del MIT/LL CTF [23] en la cual se realizaron diferentes talleres la semana anterior al evento, donde se capacitó a los alumnos en distintas temáticas relacionadas con la seguridad en aplicaciones web y en las modalidades de competencias CTF.

Utilizando las estadísticas que nos provee CTFd de las experiencias que llevamos a cabo, se puede definir en qué categorías hacer hincapié en las capacitaciones.

7.2.4 Enriquecer con nuevo contenido teórico a la plataforma

En estas primeras experiencias presentamos las temáticas con un alto nivel de abstracción de manera de simplificar la complejidad de los desafíos, utilizando un lenguaje coloquial y evitando utilizar un lenguaje técnico.

Considerando la propuesta detallada en la sección 7.2.3, se podrían realizar talleres introductorios al CTF donde se hagan explicaciones de temáticas más avanzadas (como vulnerabilidades Web) y como consecuencia proveer desafíos de mayor complejidad. Creemos fehacientemente que los talleres facilitarían la comprensión de las temáticas ya que esta situación la hemos experimentado con el alumno que participó en ambas competencias: en la primera instancia de prueba el alumno resolvió 13 desafíos en el lapso de aproximadamente 50 minutos con ayuda provista por los mentores y en la segunda instancia el alumno se desempeñó de la misma manera con la diferencia de que no obtuvo ayuda durante la resolución de los ejercicios. Los siguientes gráficos reflejan la situación descrita anteriormente:

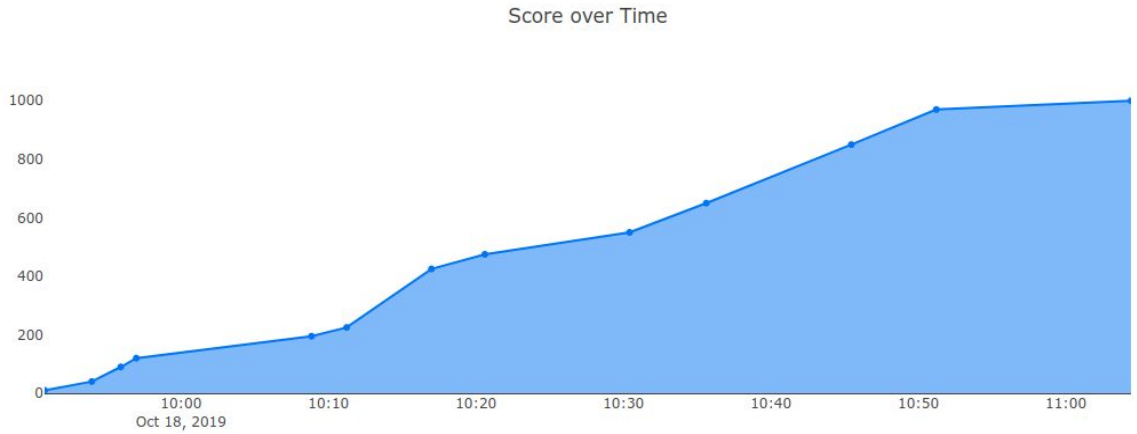


Figura 16 - Desempeño del Alumno en la Primera Instancia

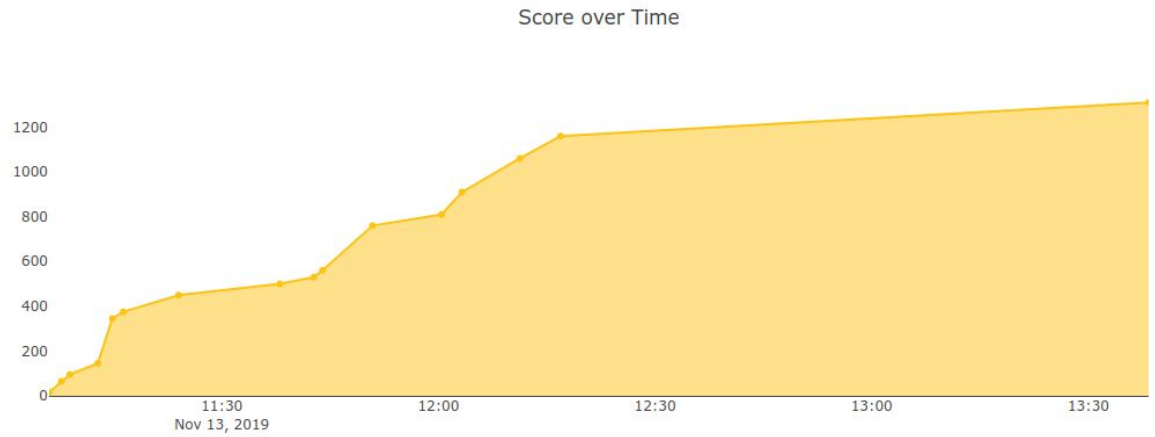


Figura 17 - Desempeño del Alumno en la Segunda Instancia

7.2.5 Cambios en la Modalidad del Juego

Se pueden plantear las siguientes modificaciones:

- Para una futura competencia se puede considerar formar equipos constituidos con alumnos de diferentes colegios mezclando a los estudiantes que tengan conocimientos en computación con aquellos que no han tenido esa posibilidad. El objetivo es nivelar el desempeño de los equipos participantes.
- Aplicar la modalidad de los CTFs investigados permitiendo el acceso online a la plataforma y prolongando la duración de la competencia.

8. Anexos

8.1 Instalación de Mellivora

Mellivora permite instalarse sobre varias configuraciones. Para probar la plataforma lo hicimos de dos formas posibles:

8.1.1 Instalación con LAMP (Ubuntu, Apache, MySQL, PHP)

Primeramente intentamos instalar Mellivora sobre una máquina física que tenía instalada la versión de escritorio de Ubuntu 18.04. Pero al ejecutar el programa tasksel y elegir la versión LAMP server, el mismo comenzó a borrar todo programa que no cumpla con el stack LAMP por lo que interrumpimos el proceso y perdimos la integridad del sistema operativo de esa computadora.

Con los problemas surgidos de la experiencia anterior, nos dispusimos a instalar Mellivora sobre una máquina virtual con Ubuntu Server 18.04 recién instalado.

La idea fue tener una máquina virtual que sea un servidor ejecutando Mellivora y otra máquina virtual cliente que visualice Mellivora en el navegador web. Para que esto sea posible configuramos los adaptadores de red de ambas máquinas en una red NAT definida en las preferencias de Virtual Box.

En la documentación oficial del repositorio GitHub de Mellivora se recomienda instalar en una instancia limpia de Ubuntu 16.04 por conexión SSH.

Los pasos para instalar Mellivora con LAMP son los siguientes:

1. Actualizar el sistema, instalar tasksel y elegir la opción LAMP server
   a. `sudo apt-get update && sudo apt-get -y upgrade`
   b. `sudo apt-get -y install tasksel && sudo tasksel`
2. Instalar las extensiones PHP
   a. `sudo apt-get install php-curl php-pear php-mbstring`
3. Instalar Composer
   a. `curl -sS https://getcomposer.org/installer | php`
   b. `sudo mv composer.phar /usr/local/bin/composer`
4. Agregar permisos de escritura al directorio /var/www
   a. `sudo chown -R $(whoami):$(whoami) /var/www/`
   b. `cd /var/www/`
5. Instalar git y clonar el repositorio de Mellivora
   a. `sudo apt-get install -y git`

    b. `git clone https://github.com/Nakiami/mellivora.git`
6. Buscar las dependencias requeridas usando Composer
    a. `cd /var/www/mellivora/`
    b. `composer install`
7. Copiar y editar los archivos de configuración
    a. `cp /var/www/mellivora/include/config/config.default.inc.php /var/www/mellivora/include/config/config.inc.php`
    b. `cp /var/www/mellivora/include/config/db.default.inc.php /var/www/mellivora/include/config/db.inc.php`
    c. `vim /var/www/mellivora/include/config/config.inc.php`
8. Agregar permisos de escritura al directorio writable
    a. `sudo chown -R www-data:www-data /var/www/mellivora/writable/`
9. Copiar y editar el archivo de configuración de Apache2
    a. `sudo cp /var/www/mellivora/install/lamp/mellivora.apache.conf /etc/apache2/sites-available/mellivora.conf`
    b. `sudo vim /etc/apache2/sites-available/mellivora.conf`
10. Deshabilitar el sitio por defecto de Apache, activar Mellivora y reiniciar Apache
    a. `sudo a2dissite 000-default`
    b. `sudo a2ensite mellivora`
    c. `sudo service apache2 restart`
11. Crear la base de datos e importar la estructura provista
    a. `echo "CREATE DATABASE mellivora CHARACTER SET utf8 COLLATE utf8_general_ci;" | mysql -u root -p`
    b. `mysql mellivora -u root -p < /var/www/mellivora/install/sql/001-mellivora.sql`
    c. `mysql mellivora -u root -p < /var/www/mellivora/install/sql/002-countries.sql`
12. Crear un nuevo usuario de MySQL
    a. `echo "GRANT ALL PRIVILEGES ON mellivora.* TO 'UserName'@'%' IDENTIFIED BY 'Password';" | mysql -u root -p`
13. Actualizar las preferencias de configuración para usar la base de datos y el usuario creado en el paso anterior.
    a. vim /var/www/mellivora/include/config/db.inc.php
14. Desde el cliente visitar la interfaz web de Mellivora y registrar un nuevo usuario.
15. Hacer al usuario moderador del sitio

    a. `echo "UPDATE users SET class = 100 WHERE id = 1;" | mysql mellivora -u root -p`
16. Loguear al usuario administrador en el sitio.

Problemas que surgieron durante la instalación:

1. En el paso 2.a no se encontró la extensión php-mbstring en los repositorios por lo que tuvimos que editar el archivo /etc/apt/sources.list con la opción universe.
2. En el paso 3 tuvimos que instalar curl ya que tasksel lo desinstaló.
3. Entre el paso 6.a y 6.b tuvimos que instalar unzip para que funcione composer install y la instalación siga su curso normal.
4. Antes de poder realizar el paso 11 tuvimos que setear la contraseña del usuario root de MySQL, esto nos llevó a realizar otra serie de pasos
    a. `sudo /etc/init.d/mysqld stop`
    b. `sudo vim  /lib/systemd/system/mysql.service`
    c. Comentamos con un # la linea del ExecStart
    d. Escribimos ExecStart=/usr/sbin/mysqld --skip-grant-tables
    e. `sudo systemctl start mysql`
    f. `sudo mysql -u root mysql`
    g. `mysql> UPDATE user SET authentication_string=password('my_password') where User='root';`
    h. `mysql> FLUSH PRIVILEGES;`
5. El paso 12 no nos anduvo porque con la configuración anterior podemos entrar a la base pero no nos deja crear al usuario y cambiando la configuración a como viene por defecto no podemos entrar a la base con el usuario root y la password configurada.

Pese a lo trillado de la instalación y a los problemas surgidos, tuvimos éxito en obtener una versión de Mellivora usable para realizar las primeras pruebas.

8.1.2 Instalación con Docker

La instalación manual de Mellivora fue bastante compleja debido a problemas en la configuración que requieren editar varios archivos. Para evitar estos problemas existe Docker que resuelve estos inconvenientes.

Mellivora es fácil de usar con docker-compose ya que se incluye una configuración destinada a ser usada en un entorno de desarrollo.

Los pasos para instalar Mellivora con Docker son:

1. Instalar docker y docker-compose
    a. `sudo apt install docker`
    b. `sudo apt install docker-compose`
2. Ejecutar Mellivora con Docker
    a. `sudo service docker start`
    b. `sudo docker-compose -f docker-compose.dev.yml up`
3. Agregar permisos de escritura al directorio writable
    a. `sudo docker exec -i -t mellivora_container_id bash`
    b. `chown -R www-data:www-data writable/`
4. Visitar la interfaz web de Mellivora en http://localhost y registrar un nuevo usuario.
5. Ir a http://localhost:18080 y loguearse en Adminer con las credenciales
    a. Server: db
    b. Username: root
    c. Password: password
    d. Database: mellivora
6. Para hacer al usuario administrador, ir a “SQL Command” en el menú y ejecutar
    a. `UPDATE users SET class = 100 WHERE id = 1;`
7. Loguear al usuario administrador en el sitio.

Observaciones:

1. La primera vez que se ejecuta el comando 2.b se construyen 3 containers de Docker: El container de la base de datos MySQL, el container del manejador de la base de datos Adminer y el container de Mellivora. Esto suele tardar un tiempo razonable al principio, pero en los siguientes usos es inmediato el tiempo de arranque de los containers.
2. Si por alguna razón hay que reconstruir los contenedores simplemente se debe ejecutar docker-compose -f docker-compose.dev.yml up --build.
3. En caso de modificar algún parámetro como puertos se debe editar el archivo docker-compose.dev.yml y reconstruir los contenedores.

Como se puede observar, la instalación de Mellivora con Docker fue más sencilla y no se produjeron problemas en la configuración.

8.2 Instalación de CTFd

Teniendo en cuenta que la instalación de Mellivora con Docker fue más sencilla, decidimos seguir los mismos pasos para el caso de CTFd.

Los pasos para la instalación de CTFd con Docker son:

1. Instalar docker y docker-compose
    a. `sudo apt install docker`
    b. `sudo apt install docker-compose`
2. Instalar git y clonar el repositorio de CTFd
    a. `sudo apt-get install -y git`
    b. `git clone https://github.com/CTFd/CTFd.git`
3. Ejecutar CTFd con Docker
    a. `sudo service docker start`
    b. `sudo docker-compose up`

También se puede utilizar la imagen de Docker autogenerada por CTFd y ejecutarla con el comando `sudo docker run -p 8000:8000 -it ctfd/ctfd`

Métricas de Usabilidad				
Subcaracterística	**Métrica**	**Propósito**	**Fórmula**	**Valor Deseado**
Inteligibilidad	Funciones evidentes	¿Qué cantidad de funciones del producto son evidentes al usuario?	X = A/B A= C + D , B = E + F C = Número de funciones evidentes al usuario común. D = Número de funciones evidentes al administrador. E = Número total de funciones provistas al usuario común. F = Número total de funciones provistas al administrador.	0<=X<=1 El valor más cercano a 1 es el mejor
	Funcionalidades complementarias	¿Qué cantidad de funciones extras posee el producto?	X = A A = Cantidad de características adicionales.	X>=0 El valor mayor o igual a 2 es el mejor
Operabilidad	Consistencia operacional	¿Cuán auto explicativas son las funciones que provee el producto?	X = A/B A= C + D , B = E + F C = Número de funciones que el usuario común encontró inconsistentes según sus expectativas. D =Número de funciones que el administrador encontró inconsistentes según sus expectativas. E = Número total de funciones provistas al usuario común. F = Número total de funciones provistas al administrador.	0<=X<=1 El valor más cercano a 0 es el mejor
	Economía de movimientos del administrador	¿Qué cantidad de pasos deben realizarse para ejecutar una función?	X = A A = Cantidad de pasos que un administrador debe realizar para crear un desafío.	X>=2 El valor más cercano a 2 es el mejor
	Economía de movimientos del usuario común	¿Qué cantidad de pasos deben realizarse para ejecutar una función?	X = A A = Cantidad de pasos que un usuario común debe realizar para acceder a un desafío.	X>=2 El valor más cercano a 2 es el mejor
	Eficiencia en las operaciones	¿Qué cantidad de operaciones no pueden llevarse a cabo con facilidad?	X = A/B A= C + D , B = E + F C = Cantidad de operaciones que son difíciles de controlar para el usuario común.	0<=X<=1 El valor más cercano a 0 es el mejor

			D = Cantidad de operaciones que son difíciles de controlar para el administrador. E = Número de funciones evidentes al usuario común. F = Número de funciones evidentes al administrador.	
	Eficiencia en las operaciones jerárquicas	¿Cuán alto es el árbol de operaciones de una determinada función?	X = A A = Cantidad máxima de dependencias entre funcionalidades del sistema a la hora de crear un desafío.	X>=0 El valor más cercano a 0 es el mejor
Protección frente a errores de usuario	Alerta al usuario	¿Qué cantidad de campos de entrada son validados?	X = A/B A= C + D , B = E + F C = Cantidad de campos de entrada que requieren ser validados y que alertan el ingreso de un dato erróneo al usuario común. D = Cantidad de campos de entrada que requieren ser validados y que alertan al administrador. E = Cantidad de campos que requieren ser validados provistos al usuario común. F = Cantidad de campos que requieren ser validados provistos al administrador.	0<=X<=1 El valor más cercano a 1 es el mejor
Estética de la interfaz	Personalización de la apariencia	¿Cuántas páginas pueden ser personalizadas en apariencia?	X = A/B A = Número de páginas que son personalizables. B = Número de páginas totales.	0<=X<=1 El valor más cercano a 1 es el mejor
Accesibilidad	Verificación código HTML estático	¿Pueden utilizar la plataforma usuarios con discapacidades visuales?	X = A A = Porcentaje de reglas WCAG válidas.	0<=X<=1 El valor más cercano a 1 es el mejor

Tabla 13 - Métricas de usabilidad

Métricas de Seguridad				
Subcaracterística	**Métrica**	**Propósito**	**Fórmula**	**Valor Deseado**
Confidencialidad	Capacidad de control de acceso	¿Qué tan controlables son los accesos al sistema?	X = A/B A = Número de operaciones ilegales detectados. B = Número de operaciones evaluadas.	0<=X<=1 El valor más cercano a 0 es el mejor
Autenticidad	Métodos de autenticación	¿Qué tan bien el sistema autentica la identidad de un sujeto?	X = A A = Número de métodos de autenticación provistos.	X>=0 El valor igual o mayor a 2 es el mejor

Tabla 14 - Métricas de seguridad

Métricas de Portabilidad				
Subcaracterística	**Métrica**	**Propósito**	**Fórmula**	**Valor Deseado**
Adaptabilidad	Adaptabilidad en entorno hardware	¿Es el sistema capaz de visualizarse de manera eficaz en distintos dispositivos?	X = A A = Cantidad de dispositivos tecnológicos en los que se visualiza sin problemas.	X>=0 El valor igual o mayor a 2 es el mejor
	Adaptabilidad en entorno software	¿Es el sistema capaz de visualizarse de manera eficaz en distintos navegadores?	X = A A = Cantidad de navegadores en los que se visualiza la plataforma sin problemas.	X>=0 El valor igual o mayor a 2 es el mejor
Facilidad de Instalación	Eficiencia en el tiempo de instalación	¿Cuánto tiempo es requerido para realizar una instalación?	X = A A = Tiempo de instalación expresada en minutos.	X>=0 El valor menor a 30 minutos es el mejor
	Eficacia de la Instalación	¿Puede instalarse el software de manera eficaz?	X = A/B A = Número de casos exitosos de instalación. B = Número total de intentos de instalación.	0<=X<=1 El valor más cercano a 1 es el mejor
	Economía de pasos de instalación	¿Cuántos pasos son requeridos para realizar una instalación?	X = A A = Cantidad de pasos a realizar durante la instalación.	X>=0 El valor menor a 10 es el mejor

Tabla 15 - Métricas de portabilidad

8.4 Matriz de Calidad

Evaluación de Calidad Externa de Mellivora								
Característica	**Subcaracteristica**	**Métrica**	**Valor Deseado**	**Valor Obtenido (x)**	**Ponderación (/10)**	**Valor Parcial Total (/10)**	**Porcentaje de Importancia**	**Valor Final**
Usabilidad	Inteligibilidad	Funciones Evidentes	1	X = A/B A= C + D , B = E + F C = 11 , D = 58 E = 11 , F = 60 X = 69/71 = 0,97	9,7	5,62	45%	2,52
		Funcionalidades que complementan al objetivo del sistema	Deseado: >= 2 Peor caso: <1	X = 3	10			
	Operabilidad	Consistencia operacional	0	X = A/B A= C + D , B = E + F C = 0 , D = 2 E = 11 , F = 60 X = 2/71	9,7			
		Economía de movimientos del administrador	Deseado: 2 Peor caso: >= 4	X = 7	0			
		Economía de movimientos del usuario común	Deseado:2 Peor caso: >= 4	X = 3	5			
		Eficiencia en las operaciones	0	X = A/B A= C + D , B = E + F C = 0 , D = 1 E = 11 , F = 58 X = 1/69	9,8			
		Eficiencia en las operaciones jerárquicas	Deseado: 0 Peor caso: >=2	X = 2	0			
	Protección frente a errores de usuario	Alerta al usuario	1	X = A/B A= C + D , B = E + F C = 7 , D = 5	2,7			

				E = 11 , F = 33 X = 12 / 44				
	Estética de la interfaz	Personalización de la apariencia	1	X = A/B A= 2 , B = 7 X = 2/7 = 0,28	2,8			
	Accesibilidad	Verificación código HTML estático	1	X = 0,65	6,5			
Seguridad	Confidencialidad	Capacidad de control de acceso	0	X = A/B A= 0 , B = 22 X=0	10	10	15%	1,5
	Autenticidad	Métodos de autenticación	Deseado: >=2 Peor caso: < 1	X = 2	10			
Portabilidad	Adaptabilidad	Adaptabilidad en entorno hardware	Deseado: >=2 Peor caso: <2	X = 2	10	8,8	40%	3,52
		Adaptabilidad en entorno software	Deseado: >=2 Peor caso: <2	X = 3	10			
	Facilidad de Instalación	Eficiencia en el tiempo de instalación	Deseado: < 30 minutos Peor caso: >= 30 minutos	X = 15	10			
		Eficacia de la Instalación	1	X = A/B A = 2 , B = 2 X = 1	10			
		Economía de pasos de instalación	Deseado: 1 Peor caso: > 10	X = 7	4			

Tabla 16 - Evaluación de calidad externa de Mellivora

Evaluación de Calidad Externa de CTFd								
Característica	**Subcaracteristica**	**Métrica**	**Valor Deseado**	**Valor Obtenido (x)**	**Ponderación (/10)**	**Valor Parcial Total (/10)**	**Porcentaje de Importancia**	**Valor Final**
Usabilidad	Inteligibilidad	Funciones Evidentes	1	X = A/B A= C + D , B = E + F C= 12 , D= 64 E=13 , F=65 X = 76/78	9,7	8,39	45%	3,77
		Funcionalidades que complementan al objetivo del sistema	Deseado: >= 2 Peor caso: < 1	X = 5	10			
	Operabilidad	Consistencia operacional	0	X = A/B A= C + D , B = E + F C=1 , D=2 E= 13 , F= 65 X= 3/78= 0,038	9,6			
		Economía de movimientos del administrador	Deseado: 2 Peor caso: >= 4	X = 3	5			
		Economía de movimientos del usuario común	Deseado: 2 Peor caso: >= 4	X = 2	10			
		Eficiencia en las operaciones	0	X = A/B A= C + D , B = E + F C = 0 , D = 1 E = 12 , F = 64 X = 1/76 = 0.01	9,8			
		Eficiencia en las operaciones jerárquicas	Deseado: 0 Peor caso: >=2	0	10			
	Protección frente a errores de usuario	Alerta al usuario	1	X = A/B A= C + D , B = E + F C = 12 , D = 31	9,1			

				E = 12 , F = 35 X=43/47				
	Estética de la interfaz	Personalización de la apariencia	1	X = A/B A= 3 , B = 10 X=0,3	3			
	Accesibilidad	Verificación código HTML estático	1	0,77	7,7			
Seguridad	Confidencialidad	Capacidad de control de acceso	0	X = A/B A= 0 , B = 16 X=0	10	10	15%	1,5
	Autenticidad	Métodos de autenticación	Deseado: >=2 Peor caso: < 1	2	10			
Portabilidad	Adaptabilidad	Adaptabilidad en entorno hardware	Deseado: >=2 Peor caso: < 2	X = 3	10	9,6	40%	3,84
		Adaptabilidad en entorno software	Deseado: >=2 Peor caso: < 2	X = 3	10			
	Facilidad de Instalación	Eficiencia en el tiempo de instalación	Deseado: < 30 minutos Peor caso: >= 30 minutos	X = 10 minutos	10			
		Eficacia de la Instalación	1	X = A/B A = 5 , B = 5 X = 1	10			
		Economía de pasos de instalación	Deseado: 1 Peor caso: > 10	X = 3	8			

Tabla 17 - Evaluación de calidad externa de CTFd

Resultado Final de la Calidad Externa de Mellivora				
Característica	**Valor Final**	**Calidad del Sistema**	**Nivel de Puntuación**	**Grado de Satisfacción**
Usabilidad	2,52	7,54	Aceptable	Satisfactorio
Seguridad	1,5			
Portabilidad	3,52			

Tabla 18 - Resultado final de la calidad externa de Mellivora

Resultado Final de la Calidad Externa de CTFd				
Característica	**Valor Final**	**Calidad del Sistema**	**Nivel de Puntuación**	**Grado de Satisfacción**
Usabilidad	3,77	9,11	Cumple con los requisitos	Muy Satisfactorio
Seguridad	1,5			
Portabilidad	3,84			

Tabla 19 - Resultado final de la calidad externa de CTFd

8.5 Especificación de las mediciones tomadas en Mellivora

8.5.1 Características que hacen a la usabilidad del software

1. **Inteligibilidad**

    a. **Funciones Evidentes**

    Una función es evidente si es fácil de localizar e iniciar.

    i. Número total de funciones provistas al usuario común (11):

        1. Registrar un equipo en la plataforma (se comparte la cuenta).
        2. Iniciar sesión en la plataforma.
        3. Modificar los datos del equipo configurados en la registración.
        4. Visualizar la tabla de posiciones.
        5. Visualizar la información de los equipos participantes de la competencia (desafíos resueltos y estadísticas de su desempeño).
        6. Visualizar las notificaciones realizadas por los administradores.
        7. Visualizar las páginas creadas por los administradores.
        8. Acceder a los desafíos.
        9. Visualizar la información de resolución de un desafío.
        10. Visualizar el listado de pistas.
        11. Responder los desafíos.

    ii. Número de funciones evidentes al usuario común (11).
    iii. Número total de funciones provistas al administrador (60)

        1. Registrar un equipo en la plataforma (se comparte la cuenta).
        2. Iniciar sesión en la plataforma.
        3. Modificar los datos del equipo configurados en la registración.
        4. Visualizar la tabla de posiciones.
        5. Visualizar la información de los equipos participantes de la competencia (desafíos resueltos y estadísticas de su desempeño).

6. Visualizar las notificaciones realizadas por los administradores.
7. Visualizar las páginas creadas por los administradores.
8. Acceder a los desafíos.
9. Visualizar la información de resolución de un desafío.
10. Visualizar el listado de pistas.
11. Responder los desafíos.
12. Crear una notificación.
13. Editar una notificación.
14. Borrar una notificación.
15. Listar las notificaciones.
16. Agregar una categoría.
17. Editar una categoría.
18. Borrar una categoría.
19. Listar las categorías.
20. Agregar un desafío.
21. Editar un desafío.
22. Borrar un desafío.
23. Listar los desafíos.
24. Listar todas las respuestas enviadas por los equipos.
25. Borrar una respuesta.
26. Marcar una respuesta correcta como incorrecta.
27. Marcar una respuesta incorrecta como correcta.
28. Listar las respuestas que necesitan marcarse.
29. Listar los usuarios.
30. Modificar un usuario.
31. Borrar un usuario.
32. Restablecer la contraseña de un usuario.
33. Agregar un tipo de usuario.
34. Modificar un tipo de usuario.
35. Borrar un tipo de usuario.
36. Listar los tipos de usuarios.
37. Agregar reglas para restringir cuentas de email.
38. Modificar una regla.
39. Borrar una regla.
40. Listar las reglas.
41. Probar una regla.
42. Enviar un mail único.
43. Enviar un mail a todos los usuarios.
44. Agregar una pista.
45. Modificar una pista.
46. Borrar una pista.

47. Listar las pistas.
48. Agregar un nuevo item personalizado para el menú.
49. Modificar un item personalizado del menú.
50. Borrar un item personalizado del menú.
51. Listar los ítems personalizados del menú.
52. Agregar una página personalizada.
53. Modificar una página personalizada.
54. Borrar una página personalizada.
55. Listar las páginas personalizadas.
56. Listar las excepciones que se producen en la ejecución de la plataforma.
57. Borrar todas las excepciones de los logs de la plataforma.
58. Buscar usuarios.
59. Buscar direcciones IPs.
60. Visualizar el CTF de forma gráfica.

iv. Número de funciones evidentes al administrador (58)

1. Funciones totales (60) - Funciones inconsistentes (2)

b. Funcionalidades que complementan al objetivo del sistema

i. Cantidad de características adicionales (3)

1. Agregar contenido dinámico.
2. Envío de mails.
3. Reglas de filtrado de cuentas de mail.

2. Operabilidad

a. Consistencia operacional

i. Número total de funciones provistas al usuario común (11)
ii. Número total de funciones provistas al administrador (60)
iii. Número de funciones que el usuario común encontró inconsistentes según sus expectativas (0).
iv. Número de funciones que el administrador encontró inconsistentes según sus expectativas (2):

1. Listar las excepciones que se producen en la ejecución de la plataforma.
2. Agregar un tipo de usuarios.

b. Economía de movimientos del administrador

i. Cantidad de pasos que un administrador debe realizar para crear un desafío (7)

1. Acceder a la opción del menú superior “Manage”.
2. Click en la solapa “Categories”.
3. Elegir la opción “Add category” y completar los campos.
4. Click en la solapa “Challenges”.
5. Elegir la opción “Add Challenge” y completar los campos.
6. Click en la solapa “Hints”.
7. Elegir la opción “New Hint” y completar los campos.

c. Economía de movimientos del usuario común

i. Cantidad de pasos que un usuario común debe realizar para acceder a un desafío (3):

1. Ir a la opción “Challenges” del menú superior.
2. Elegir la categoría del menú de categorías.
3. Hacer click en el desafío.

d. Eficiencia en las operaciones

i. Cantidad de operaciones que son difíciles de controlar para el usuario común (0)
ii. Cantidad de operaciones que son difíciles de controlar para el administrador (1)

1. Nuevo item de menú

iii. Número de funciones evidentes al usuario común (11)
iv. Número de funciones evidentes al administrador (58)

e. Eficiencia en las operaciones jerárquicas

i. Cantidad máxima de dependencias entre funcionalidades del sistema a la hora de crear un desafío (2):

1. Crear la categoría.
2. Crear el desafío.
3. Crear la pista.

3. **Protección frente a errores de usuario**

    a. **Alerta al usuario**

        i. Cantidad de campos de entrada que requieren ser validados provistos al usuario común (11):

            1. Datos de registro:

                a. Nombre del equipo.
                b. Dirección de mail.
                c. Contraseña.
                d. País.

                4 campos requieren validación: 2 generan alertas (Nombre del equipo y Dirección de mail).

            2. Iniciar sesión

                a. Dirección de mail.
                b. Contraseña.

                2 campos requieren validación: 2 generan alertas.

            3. Modificar los datos:

                a. País.
                b. Contraseña actual.
                c. Nueva contraseña.
                d. Re ingresar nueva contraseña.

                4 campos requieren validación: 2 generan alertas (Contraseña actual y Re ingresar nueva contraseña).

            4. Desafío:

                a. Flag para el desafío.

                1 campo requiere validación: 1 genera alertas.

        ii. Cantidad de campos de entrada que requieren ser validados que alertan al usuario común el ingreso de un dato erróneo (7).

        iii. Cantidad de campos de entrada que requieren ser validados provistos al administrador (33):

            1. Crear una notificación:

                a. Título.

b. Cuerpo.

2 campos requieren validación: 1 genera alertas (Título).

2. Crear una categoría:

    a. Títiulo.
    b. Descripción.
    c. Fecha de Inicio.
    d. Fecha de Fin.

    4 campos requieren validación: 1 genera alertas (Título).

3. Crear un desafío:

    a. Título.
    b. Descripción.
    c. Flag.
    d. Puntos.
    e. Categoría.
    f. Fecha de inicio.
    g. Fecha de fin.

    7 campos requieren validación: 1 genera alertas (Título).

4. Crear un tipo de usuario:

    a. Título.
    b. Descripción.

    2 campos requieren validación: Ninguno genera alertas.

5. Editar un usuario:

    a. Email.
    b. Nombre del equipo.
    c. País.

    3 campos requieren validación: 1 genera alertas (Email).

6. Crear regla para restringir cuentas de email:

a. Regla.
b. Prioridad.

2 campos requieren validación: Ninguno genera alertas.

7. Crear un nuevo email:

    a. Destinatario.
    b. Asunto.
    c. Cuerpo.

    3 campos requieren validación: 1 genera alertas (Destinatario).

8. Crear una pista:

    a. Cuerpo.
    b. Desafío.

    2 campos requieren validación: Ninguno genera alertas.

9. Crear un item del menú:

    a. Título.
    b. Página interna.
    c. Tipo de visibilidad.

    3 campos requieren validación: Ninguno genera alertas.

10. Crear una página:

    a. Título.
    b. Cuerpo.
    c. Tipo de visibilidad.

    3 campos requieren validación: Ninguno genera alertas.

11. Búsqueda:

    a. Contenido a buscar.
    b. Tipo de búsqueda.

2 campos requieren validación: Ninguno genera alertas.

iv. Cantidad de campos de entrada que requieren ser validados que alertan al administrador el ingreso de un dato erróneo (5).

4. **Estética de la interfaz**

   a. **Personalización de la apariencia**

      i. Número de páginas que son personalizables (2):

         1. Home.
         2. Challenges.

      ii. Número de páginas totales (7):

         1. Home.
         2. Challenges.
         3. Hints.
         4. Scores.
         5. Profile.
         6. Login.
         7. Manage.

5. **Accesibilidad**

   a. **Verificación código HTML estático**

      i. La plataforma Mellivora tuvo un resultado del 65% de reglas WCAG válidas.

         Los detalles del análisis de accesibilidad se pueden consultar en el anexo 8.7 Análisis de accesibilidad de Mellivora.

8.5.2 Características que hacen a la seguridad del software

1. **Confidencialidad**

   a. **Capacidad de control de acceso**

      i. Número de operaciones ilegales detectados (0).
      ii. Número de operaciones evaluadas (22):

         1. /admin/
         2. /admin/new_news
         3. /admin/list_news

4. /admin/new_category
5. /admin/new_challenge
6. /admin/list_submissions?only_needing_marking=1
7. /admin/list_submissions
8. /admin/list_users
9. /admin/new_user_type
10. /admin/list_user_types
11. /admin/new_restrict_email
12. /admin/list_restrict_email
13. /admin/test_restrict_email
14. /admin/new_hint
15. /admin/list_hints
16. /admin/new_dynamic_menu_item
17. /admin/list_dynamic_menu
18. /admin/new_dynamic_page
19. /admin/list_dynamic_pages
20. /admin/list_exceptions
21. /admin/edit_exceptions
22. /admin/search

2. **Autenticidad**

    a. **Métodos de autenticación**

        i. Número de métodos de autenticación previstos (2):

            1. Login.
            2. Segundo factor de autenticación.

8.5.3 Características hacen a la portabilidad del software

1. **Adaptabilidad**

    a. **Adaptabilidad en entorno hardware**

        i. Cantidad de dispositivos tecnológicos en los que se visualiza sin problemas (2):

            1. Tablets.
            2. Notebooks.

    b. **Adaptabilidad en entorno software**

        i. Cantidad de navegadores en los que se visualiza la plataforma sin problemas (3)

1. Mozilla Firefox.
2. Google Chrome.
3. Microsoft Edge.

2. Facilidad de Instalación

Los detalles de los resultados de la instalación están analizados en el anexo 8.1 Instalación de Mellivora**.**

a. Eficiencia en el tiempo de instalación

i. La instalación demoró en promedio 15 minutos.

b. Eficacia de la Instalación

i. Se instaló Mellivora 2 veces en diferentes servidores mediante la utilización de Docker.
ii. Todas las instalaciones resultaron exitosas.

c. Economía de pasos de instalación

i. La instalación con Docker demandó 7 pasos.

8.6 Especificación de las mediciones tomadas en CTFd

8.6.1 Características que hacen a la usabilidad del software

1. **Inteligibilidad**

    a. **Funciones Evidentes**

    Una función es evidente si es fácil de localizar e iniciar.

    i. Número total de funciones provistas al usuario común (13):

    1. Registrarse en la plataforma.
    2. Iniciar sesión en la plataforma.
    3. Registrar un equipo.
    4. Unirse a un equipo.
    5. Unirse a una liga mayor.
    6. Modificar los datos personales configurados en la registración.
    7. Visualizar la tabla de posiciones.
    8. Visualizar la información de los usuarios participantes de la competencia (desafíos resueltos y estadísticas de su desempeño).
    9. Visualizar información de los equipos participantes (integrantes del equipo, estadísticas del desempeño individual y grupal).
    10. Visualizar las notificaciones realizadas por los administradores.
    11. Acceder a los desafíos.
    12. Acceder a las ayudas de los desafíos.
    13. Responder los desafíos.

    ii. Número de funciones evidentes al usuario común (12):

    1. Todas menos la de unirse a la liga mayor que no se puede iniciar si no se encuentra configurada y tampoco se le provee la opción de invisibilizar el botón en caso de que no se haya configurado.

    iii. Número total de funciones provistas al administrador (65):

1. Registrarse en la plataforma.
2. Configurar al CTF como juego grupal o individual.
3. Iniciar sesión en la plataforma.
4. Registrar un equipo.
5. Unirse a un equipo.
6. Unirse a una liga mayor.
7. Modificar los datos personales configurados en la registración.
8. Visualizar la tabla de posiciones.
9. Visualizar la información de los usuarios participantes de la competencia (desafíos resueltos y estadísticas de su desempeño).
10. Visualizar información de los equipos participantes (integrantes del equipo, estadísticas del desempeño individual y grupal).
11. Visualizar el perfil del usuario donde se detalla el desempeño del mismo en la competencia.
12. Visualizar la composición del equipo del cual forma parte el usuario, como también el desempeño grupal e individual.
13. Acceder a estadísticas globales de la competencia (donde se especifica, por ejemplo, el ejercicio más resuelto, el menos resuelto, los porcentajes de respuestas correctas e incorrectas, etc.).
14. Crear notificaciones.
15. Visualizar las notificaciones realizadas por los administradores.
16. Eliminar notificaciones.
17. Agregar páginas al sitio.
18. Editar páginas.
19. Eliminar páginas.
20. Acceder a la información del desempeño de todos los usuarios registrados (visibles o no).
21. Modificar la información del desempeño de los usuarios (por ejemplo, borrar respuestas correctas o incorrectas que hayan ingresado).
22. Crear usuarios (comunes o administradores).
23. Buscar usuarios por nombre, identificador, email, afiliación o dirección IP.
24. Modificar los datos de registración de los usuarios.
25. Eliminar usuarios.
26. Crear equipos.

27. Buscar equipos por nombre, identificador, email o afiliación.
28. Modificar los datos de registración de los equipos.
29. Elegir al capitán del equipo.
30. Eliminar equipos.
31. Invisibilizar equipos.
32. Visibilizar equipos.
33. Acceder a la información del desempeño de todos los equipos registrados (visibles o no).
34. Modificar la información del desempeño de los equipos (por ejemplo, borrar respuestas correctas o incorrectas que hayan ingresado).
35. Crear desafíos.
36. Modificar los desafíos.
37. Borrar los desafíos.
38. Invisibilizar desafíos.
39. Visibilizar desafíos.
40. Resolver los desafíos.
41. Crear ayudas para los desafíos.
42. Modificar las ayudas.
43. Eliminar las ayudas.
44. Utilizar las ayudas de los desafíos.
45. Crear flags.
46. Modificar flags.
47. Eliminar flags.
48. Adjuntar archivos al desafío.
49. Eliminar los archivos.
50. Agregar dependencias entre desafíos.
51. Eliminar dependencias.
52. Agregar tags a los desafíos.
53. Borrar los tags.
54. Visualizar todas las respuestas ingresadas por los participantes.
55. Borrar respuestas de los participantes.
56. Configurar la apariencia de la página principal.
57. Configurar características de las cuentas (definir una lista blanca de los dominios de correo electrónico en los que los usuarios pueden registrarse, controlar si los usuarios deben confirmar sus direcciones de correo electrónico antes de jugar, controlar si los usuarios pueden cambiar sus nombres).
58. Configurar la liga mayor.

59. Configurar la visibilidad (pública, privada o sólo administradores) de los desafíos, de la tabla de posiciones, de las cuentas y de la registración.
60. Configurar servidor de emails.
61. Configurar el tiempo de inicio, de fin y de congelación de la competencia.
62. Exportar la configuración de la competencia.
63. Importar una configuración existente.
64. Descargar tablas de la base de datos.
65. Resetear la configuración de la competencia.

iv. Número de funciones evidentes al administrador (64):

1. Cantidad total de funciones menos 1 (se descuenta la característica de unirse a la liga mayor que no se puede iniciar si no se encuentra configurada y tampoco se le provee la opción de invisibilizar el botón en caso de que no se haya configurado).

b. Funcionalidades que complementan al objetivo del sistema

i. Cantidad de características adicionales (5):

1. Estadísticas.
2. Backups.
3. Creación de Páginas.
4. Creación de Notificaciones.
5. Configuración de modalidad del CTF (individual o grupal).

2. Operabilidad

a. Consistencia operacional

i. Número total de funciones provistas al usuario común (13).
ii. Número total de funciones provistas al administrador (65).
iii. Número de funciones que el usuario común encontró inconsistentes según sus expectativas (1):

1. Unirse a una liga mayor.

iv. Número de funciones que el administrador encontró inconsistentes según sus expectativas (2):

1. Unirse a una liga mayor.
2. Agregar tags a los desafíos.

b. Economía de movimientos del administrador

i. Cantidad de pasos que un administrador debe realizar para crear un desafío (3):

1. Acceder a la solapa “Admin”.
2. Hacer click en la solapa “Challenges”.
3. Apretar el botón “Create Challenge” y completar los campos. En la misma página se puede configurar el desafío, el nombre de la categoría, las pistas, las flags y se pueden adjuntar archivos al desafío.

c. Economía de movimientos del usuario común

i. Cantidad de pasos que un usuario común debe realizar para acceder a un desafío (2):

1. Hacer click en la solapa “Challenges”.
2. Hacer click sobre el desafío que se quiere resolver.

d. Eficiencia en las operaciones

i. Cantidad de operaciones que son difíciles de controlar para el usuario común (0).
ii. Cantidad de operaciones que son difíciles de controlar para el administrador (1):

1. A la hora de configurar un pre-requisito se dispone de un listado de desafíos a elegir y un botón para confirmar la operación que se llama “Add prerequisite”. No queda en claro que primero hay que elegir el desafío y luego apretar el botón, por lo que si primero se aprieta el botón, el sistema agrega el pre-requisito vacío.

iii. Número de funciones evidentes al usuario común (12).
iv. Número de funciones evidentes al administrador (64).

e. Eficiencia en las operaciones jerárquicas

i. Cantidad máxima de dependencias entre funcionalidades del sistema a la hora de crear un desafío (0):

1. El administrador puede crear un desafío directamente sin tener que crear previamente una categoría o posteriormente sus atributos (como las ayudas). En la misma página se configura el desafío, el nombre de la categoría a la que pertenece, sus flags, las ayudas y los archivos adjuntos.

3. **Protección frente a errores de usuario**

    a. **Alerta al usuario**

        i. Cantidad de campos de entrada que requieren ser validados provistos al usuario común (12):

            1. Registración de un usuario:

                a. Nombre del usuario.
                b. Dirección de email.
                c. Contraseña.

                3 campos requieren validación: 3 generan alertas.

            2. Inicio de sesión:

                a. Nombre de usuario o dirección de email.
                b. Contraseña.

                2 campos requieren validación: 2 generan alertas.

            3. Registración de un equipo:

                a. Nombre del equipo.

                1 campo requiere validación: 1 genera alertas.

            4. Unión a un equipo existente:

                a. Nombre del equipo.
                b. Contraseña.

                2 campos requieren validación: 2 generan alertas.

            5. Modificar los datos personales configurados en la registración:

                a. Nombre de usuario.
                b. Dirección de email.
                c. Contraseña actual.

                3 campos requieren validación: 3 generan alertas.

            6. Responder los desafíos:

a. Flag del desafío.

1 campo requiere validación: 1 genera informes.

ii. Cantidad de campos de entrada que requieren ser validados que alertan al usuario común el ingreso de un dato erróneo (12).
iii. Cantidad de campos de entrada que requieren ser validados provistos al administrador (35):

1. Registración del administrador:

    a. Nombre de usuario.
    b. Dirección de email.
    c. Contraseña.

    3 campos requieren validación: 1 alerta (email).

    Si la registración se hace vacía la acepta, pero a la hora de modificar los datos del administrador la página exige esos 3 campos.

2. Iniciar sesión en la plataforma:

    a. Nombre de usuario.
    b. Contraseña.

    2 campos requieren validación: 2 generan alertas.

3. Registración de un equipo:

    a. Nombre del equipo.
    b. Contraseña.

    1 campo requiere validación: 1 genera alertas (nombre del equipo).

    Un administrador puede crear un grupo al momento al momento de unirse a uno, o dentro de la solapa “admin”. En el primer caso se puede no poner contraseña. Si se crea un grupo desde la solapa “admin” hay que ponerle contraseña (si bien la registración permite no ponerle una contraseña al momento de unirse al equipo el servidor devuelve un error 500).

4. Unión a un equipo:

    a. Nombre del equipo.
    b. Contraseña.

    2 campos requieren validación: 2 generan alertas.

5. Modificar los datos personales configurados en la registración:

    a. Nombre de usuario.
    b. Dirección de email.
    c. Contraseña actual.

    3 campos requieren validación: 2 generan alertas (nombre de usuario y dirección de email).

6. Crear usuarios (comunes o administradores):

    a. Nombre de usuario.
    b. Dirección de email.
    c. Contraseña.

    3 campos requieren validación: 2 generan alertas (nombre de usuario y dirección de email).

    Si la registración se hace sin contraseña la acepta, pero a la hora de querer iniciar sesión con ese usuario el servidor devuelve un error 500.

7. Modificar los datos de registración de los usuarios:

    a. Nombre de usuario.
    b. Dirección de email.

    2 campos requieren validación: 2 generan alertas.

8. Modificar los datos de registración de los equipos:

    a. Nombre del equipo.

    1 campos requiere validación: 1 genera alertas.

9. Crear desafíos:

    a. Valor del desafío.

    1 campo requiere validación: 1 genera alertas.

10. Modificar desafíos:

    a. Valor del desafío.

    1 campo requiere validación: 1 genera alertas.

11. Resolver los desafíos:

    a. Flag del desafío.

    1 campo requiere validación: 1 genera informes.

12. Configurar el tiempo de inicio, de fin y de congelación de la competencia:

    a. Mes.
    b. Día.
    c. Año.
    d. Hora.
    e. Minuto.

    15 campos requieren validación: 15 generan alertas.

iv. Cantidad de campos de entrada que requieren ser validados que alertan al administrador el ingreso de un dato erróneo (31).

4. Estética de la interfaz

a. Personalización de la apariencia

i. Número de páginas que son personalizables (3):

1. Home.
2. Notifications.
3. Challenges.

ii. Número de páginas totales (10):

1. Home.

2. Notifications.
3. Users.
4. Teams.
5. Scoreboard.
6. Challenges.
7. Login.
8. Team.
9. Profile.
10. Admin.

5. **Accesibilidad**

a. Verificación código HTML estático

i. La plataforma CTFd tuvo un resultado del 77% de reglas WCAG válidas.

Los detalles del análisis de accesibilidad se pueden consultar en el anexo 8.8 Análisis de accesibilidad de CTFd

8.6.2 Características que hacen a la seguridad del software

1. **Confidencialidad**

a. Capacidad de control de acceso

i. Número de operaciones ilegales detectados (0).

ii. Número de operaciones evaluadas (16):

1. /admin/statistics
2. /admin/notifications
3. /admin/pages
4. /admin/pages/new
5. /admin/users
6. /admin/users/new
7. /admin/teams
8. /admin/teams/new
9. /admin/scoreboard
10. /admin/challenges
11. /admin/challenges/new
12. /admin/submissions
13. /admin/submissions/correct
14. /admin/submissions/incorrect
15. /admin/config
16. /admin/reset

2. **Autenticidad**

    a. **Métodos de autenticación**

        i. Número de métodos de autenticación previstos (2):

            1. Login.
            2. Integración del ID de Cliente de MajorLeagueCyber.

8.6.3 Características hacen a la portabilidad del software

1. **Adaptabilidad**

    a. **Adaptabilidad en entorno hardware**

        i. Cantidad de dispositivos tecnológicos en los que se visualiza sin problemas (2):

            1. Tablets.
            2. Celulares.
            3. Notebooks.

    b. **Adaptabilidad en entorno software**

        i. Cantidad de navegadores en los que se visualiza la plataforma sin problemas (3):

            1. Mozilla Firefox.
            2. Google Chrome.
            3. Microsoft Edge.

2. **Facilidad de Instalación**

    Los detalles de los resultados de la instalación están analizados en el anexo 8.2 Instalación de CTFd.

    a. **Eficiencia en el tiempo de instalación**

        i. La instalación demoró en promedio 10 minutos.

    b. **Eficacia de la Instalación**

i. Se instaló CTFd 5 veces en diferentes servidores mediante la utilización de Docker.
ii. Todas las instalaciones resultaron exitosas.

c. Economía de pasos de instalación

i. La instalación con Docker demandó 3 pasos.

8.7 Análisis de accesibilidad de Mellivora

Como la herramienta SiMor analiza sitios web que están online, utilizamos la plataforma Trinity del Libre Lab de la Universidad Complutense de Madrid que fue desarrollada con Mellivora. Este CTF se encuentra disponible en https://trinity.librelabucm.org [62].

El análisis global de accesibilidad del sitio realizado con SiMor arrojó los siguientes resultados:

- 65% de Reglas válidas
- 11% de Reglas con advertencias
- 25% de Reglas inválidas

Simor también detectó 25 enlaces del sitio para los cuales el análisis de accesibilidad resultó en un porcentaje que oscila entre 67% y el 80% para las reglas válidas, entre el 6% y el 12% para las reglas con advertencias y entre el 8% y el 34% para el caso de las reglas inválidas.

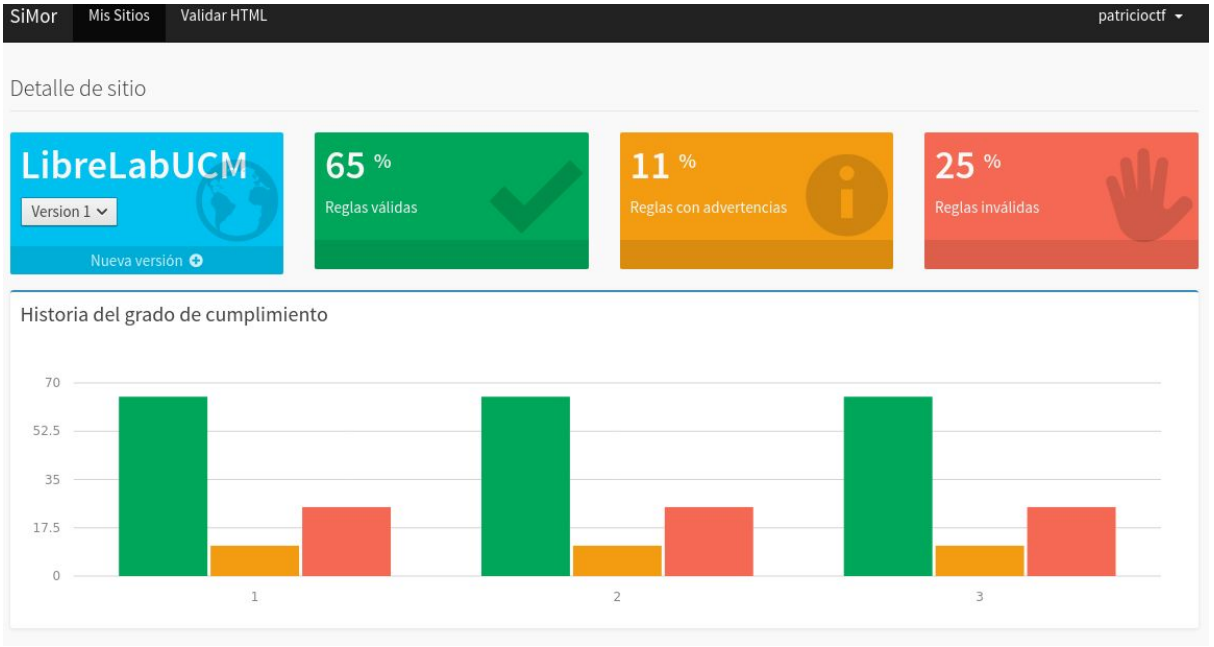


Figura 18 - Análisis global de accesibilidad de Mellivora

Enlaces del sitio

#	URL	Elementos analizados
1	ROOT_LINK	80% 12% 8%
2	/scores	53% 13% 34%
3	/content?show=	67% 11% 22%
4	/register	78% 11% 11%
5	/challenge?id=94	80% 12% 7%
6	/challenge?id=49	66% 12% 22%
7	/challenge?id=37	62% 13% 25%
8	/challenge?id=91	69% 12% 19%
9	/challenge?id=93	66% 12% 22%
10	/challenge?id=92	73% 11% 16%

Figura 19 - Análisis de accesibilidad de los enlaces de Mellivora

8.8 Análisis de accesibilidad de CTFd

Para el caso del análisis de accesibilidad sobre la plataforma CTFd con la herramienta SiMor utilizamos la demo que provee la página oficial del proyecto y que se encuentra disponible en https://demo.ctfd.io/ [63].

El análisis global de accesibilidad del sitio realizado con SiMor arrojó los siguientes resultados:

- 77% de Reglas válidas
- 10% de Reglas con advertencias
- 14% de Reglas inválidas

Simor analizó 25 enlaces del sitio para los cuales el análisis de accesibilidad resultó en un porcentaje que ronda entre 54% y el 90% para las reglas válidas, entre el 6% y el 24% para las reglas con advertencias y entre el 2% y el 22% para el caso de las reglas inválidas.

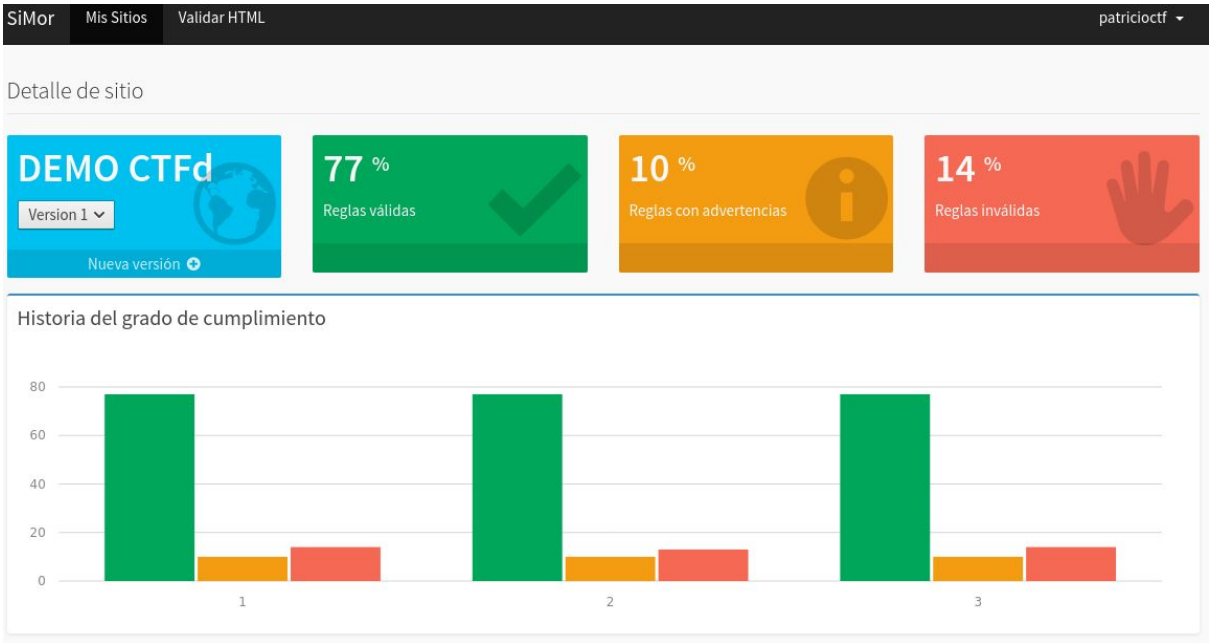


Figura 20 - Análisis global de accesibilidad de CTFd

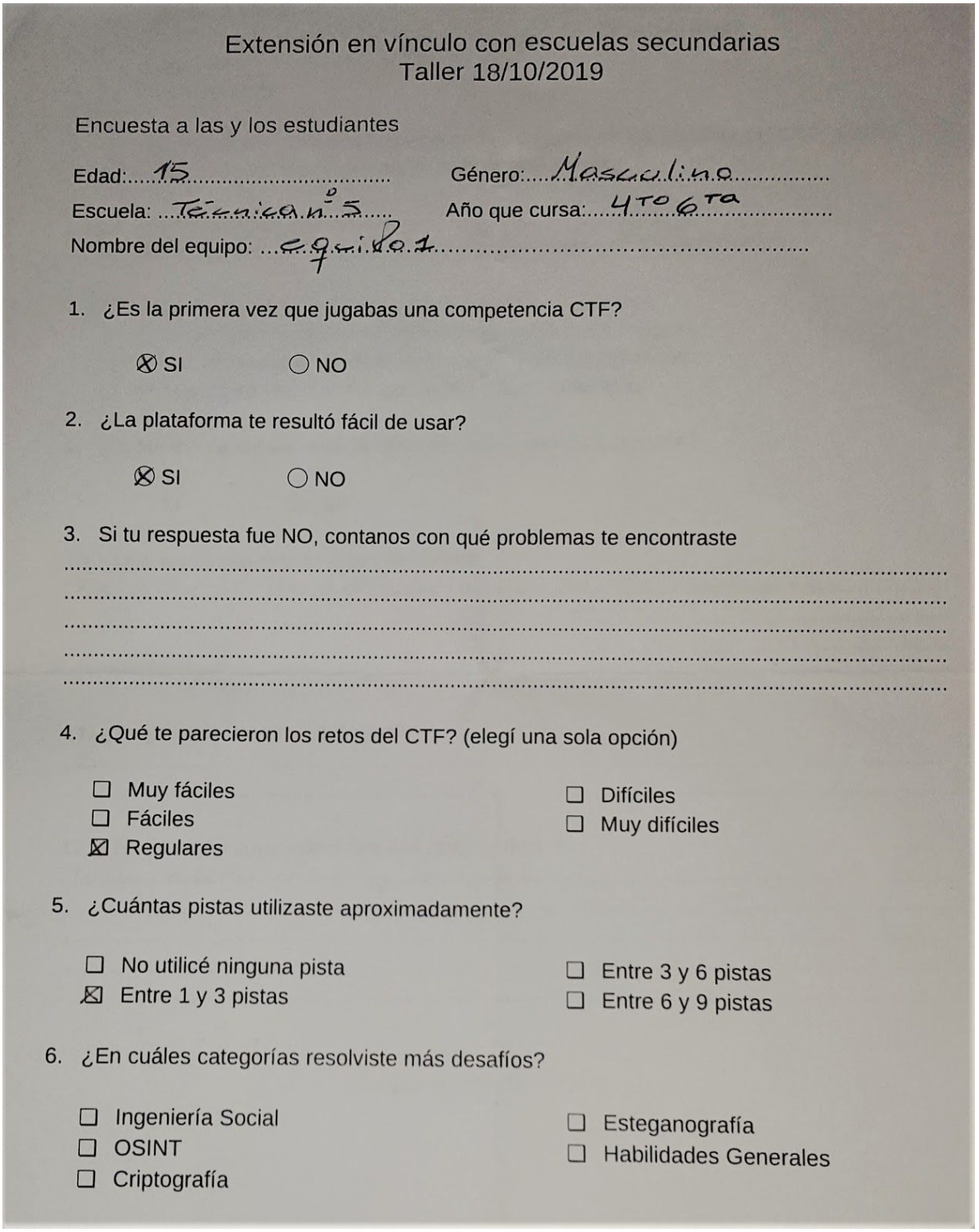
Enlaces del sitio

#	URL	Elementos analizados
1	ROOT_LINK	70% 24% 6%
2	/admin	78% 18% 4%
3	/team	74% 23% 3%
4	/user	54% 24% 22%
5	/settings	84% 14% 2%
6	/logout	70% 24% 6%
7	/oauth	83% 15% 2%
8	/teams/join	75% 19% 6%
9	/teams/new	75% 19% 6%
10	/reset_password	75% 21% 3%

Figura 21 - Análisis de accesibilidad de los enlaces de CTFd

8.9 Encuestas de la primera evaluación

8.9.1 Encuestas de los alumnos de la escuela técnica número 5



Extensión en vínculo con escuelas secundarias
Taller 18/10/2019

Encuesta a las y los estudiantes

Edad: 15 Género: Masculino

Escuela: Técnica n° 5 Año que cursa: 4to 6ta

Nombre del equipo: Equipo 1

1. ¿Es la primera vez que jugabas una competencia CTF?

⊗ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

⊗ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

.....
.....
.....
.....
.....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

- ☐ Muy fáciles
- ☐ Fáciles
- ☒ Regulares
- ☐ Difíciles
- ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?

- ☐ No utilicé ninguna pista
- ☒ Entre 1 y 3 pistas
- ☐ Entre 3 y 6 pistas
- ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

- ☐ Ingeniería Social
- ☐ OSINT
- ☐ Criptografía
- ☐ Esteganografía
- ☐ Habilidades Generales

7. ¿Conocías alguno de los temas relacionados a los desafíos?

- ☐ Ingeniería Social
- ☐ OSINT
- ☐ Criptografía
- ☐ Esteganografía
- ☐ Habilidades Generales
- ☐ Otros.¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- ☐ Me los enseñan en la escuela.
- ☐ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad

.....

- ☐ A través de videos e información publicados en Internet.
- ☐ En mi familia me hablan de estos temas porque los conocen.
- ☐ Tengo amigos que conocen más que yo y me los transmiten.
- ☐ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

◯ SI ⊗ NO

10. ¿Qué fue lo que más te gustó del taller?

Me gustó las explicaciones de los profesores

11. ¿Te gustaría volver a participar?

Si

12. ¿Tenés algún comentario que nos quieras dejar?

Que estuvo muy bueno

¡¡MUCHAS GRACIAS!!

Extensión en vínculo con escuelas secundarias
Taller 18/10/2019

Encuesta a las y los estudiantes

Edad: 15 Género: MASCULINO

Escuela: TÉCNICA 5 Año que cursa: 4TO 4TA

Nombre del equipo: EQUIPO 2 :'V

1. ¿Es la primera vez que jugabas una competencia CTF?

   ◉ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ◉ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   .....
   .....
   .....
   .....
   .....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ☐ Muy fáciles
   ☐ Fáciles
   ☑ Regulares
   ☐ Difíciles
   ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?

   ☐ No utilicé ninguna pista
   ☑ Entre 1 y 3 pistas
   ☐ Entre 3 y 6 pistas
   ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   ☐ Ingeniería Social
   ☐ OSINT
   ☐ Criptografía
   ☐ Esteganografía
   ☑ Habilidades Generales

7. ¿Conocías alguno de los temas relacionados a los desafíos?

- ☐ Ingeniería Social
- ☐ OSINT
- ☑ Criptografía
- ☐ Esteganografía
- ☑ Habilidades Generales
- ☐ Otros.¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- ☐ Me los enseñan en la escuela.
- ☑ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad
  SCOUT
- ☑ A través de videos e información publicados en Internet.
- ☐ En mi familia me hablan de estos temas porque los conocen.
- ☐ Tengo amigos que conocen más que yo y me los transmiten.
- ☐ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

○ SI ◉ NO

10. ¿Qué fue lo que más te gustó del taller?
LA ANFORA

11. ¿Te gustaría volver a participar?
SI

12. ¿Tenés algún comentario que nos quieras dejar?
ESTUVO MUY BUENO GRACIAS POR EL TALLER

¡¡MUCHAS GRACIAS!!

Extensión en vínculo con escuelas secundarias
Taller 18/10/2019

Encuesta a las y los estudiantes

Edad: 15 Género: Femenino

Escuela: Técnica N°5 Año que cursa: 4to 6to

Nombre del equipo: .....

1. ¿Es la primera vez que jugabas una competencia CTF?

   ⊘ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ⊘ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   .....
   .....
   .....
   .....
   .....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ☐ Muy fáciles
   ☐ Fáciles
   ☑ Regulares
   ☐ Difíciles
   ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?

   ☐ No utilicé ninguna pista
   ☑ Entre 1 y 3 pistas
   ☐ Entre 3 y 6 pistas
   ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   ☑ Ingeniería Social
   ☐ OSINT
   ☑ Criptografía
   ☐ Esteganografía
   ☐ Habilidades Generales

7. ¿Conocías alguno de los temas relacionados a los desafíos?

- ☐ Ingeniería Social
- ☐ OSINT
- ☐ Criptografía
- ☐ Esteganografía
- ☐ Habilidades Generales
- ☐ Otros.¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- ☐ Me los enseñan en la escuela.
- ☐ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad
.....
- ☐ A través de videos e información publicados en Internet.
- ☐ En mi familia me hablan de estos temas porque los conocen.
- ☐ Tengo amigos que conocen más que yo y me los transmiten.
- ☑ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

⊘ SI ○ NO

10. ¿Qué fue lo que más te gustó del taller?
El buen trato y el juego entre grupos

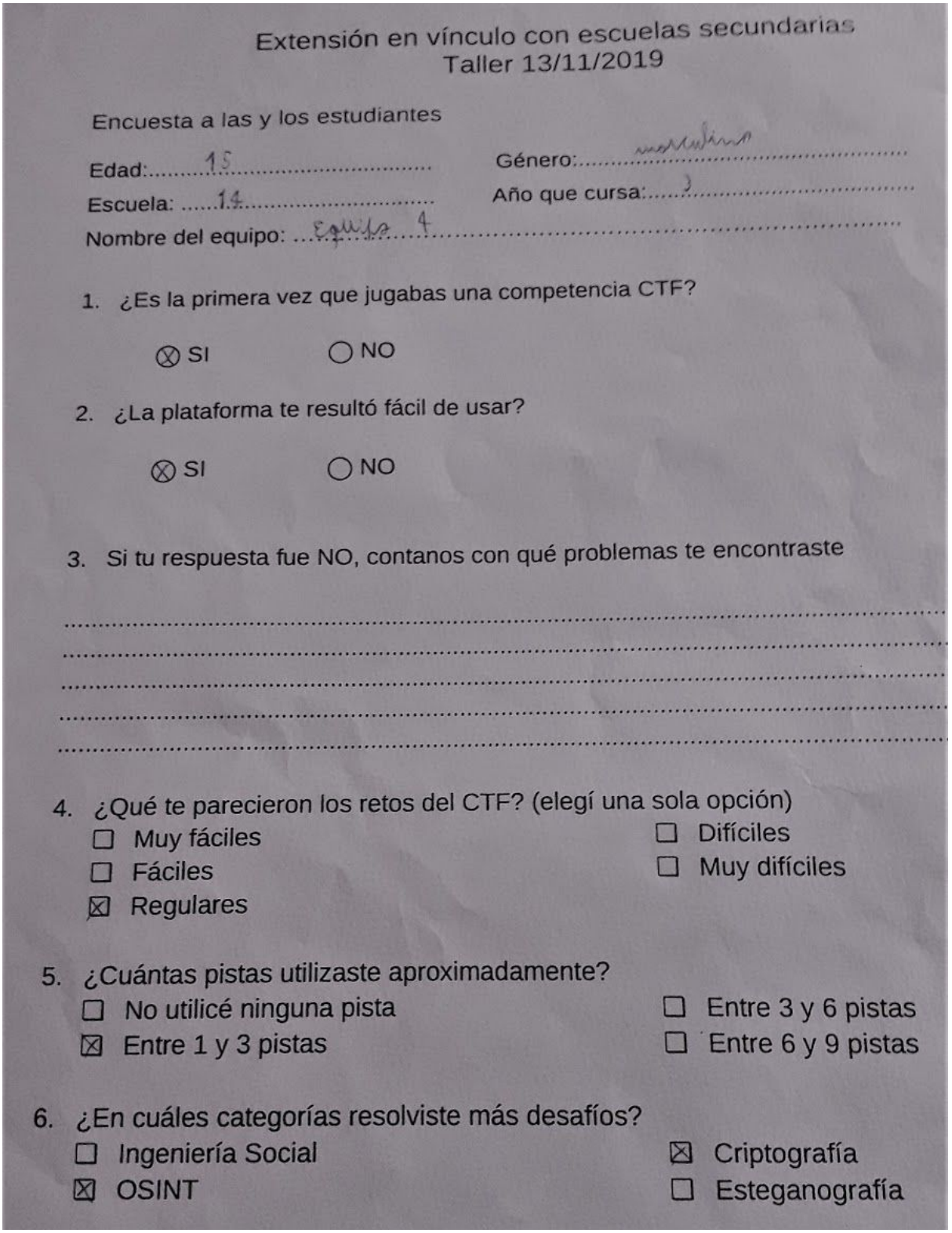
11. ¿Te gustaría volver a participar?
Sí

12. ¿Tenés algún comentario que nos quieras dejar?
Estuvo muy bueno

¡¡MUCHAS GRACIAS!!

8.10 Encuestas de la segunda evaluación

8.10.1 Encuestas de los alumnos de la escuela número 14



Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 15 Género: masculino

Escuela: 14 Año que cursa: 3

Nombre del equipo: Equipo 4

1. ¿Es la primera vez que jugabas una competencia CTF?

⊗ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

⊗ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

.....
.....
.....
.....
.....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

☐ Muy fáciles ☐ Difíciles
☐ Fáciles ☐ Muy difíciles
☒ Regulares

5. ¿Cuántas pistas utilizaste aproximadamente?

☐ No utilicé ninguna pista ☐ Entre 3 y 6 pistas
☒ Entre 1 y 3 pistas ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

☐ Ingeniería Social ☒ Criptografía
☒ OSINT ☐ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos?

- ☐ Ingeniería Social
- ☒ Criptografía
- ☒ OSINT
- ☐ Esteganografía
- ☐ Otros. ¿Cuáles?..............................

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- ☐ Me los enseñan en la escuela.
- ☐ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad ....
- ☒ A través de videos e información publicados en Internet.
- ☐ En mi familia me hablan de estos temas porque los conocen.
- ☐ Tengo amigos que conocen más que yo y me los transmiten.
- ☐ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

(✓) SI ◯ NO

10. ¿Qué fue lo que más te gustó del taller?

todo

11. ¿Te gustaría volver a participar?

si

12. ¿Tenés algún comentario que nos quieras dejar?

Con el tema de los premios me parece que debería de haber 1 por cada participante del equipo

¡¡MUCHAS GRACIAS!!

Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 14 Género: masculino

Escuela: Carlos N. Vergara Año que cursa: tercero

Nombre del equipo: equipo 4

1. ¿Es la primera vez que jugabas una competencia CTF?

   ⊗ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ⊗ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

.....
.....
.....
.....
.....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)
   - ☐ Muy fáciles
   - ☐ Fáciles
   - ☐ Regulares
   - ☒ Difíciles
   - ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?
   - ☒ No utilicé ninguna pista
   - ☐ Entre 1 y 3 pistas
   - ☐ Entre 3 y 6 pistas
   - ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?
   - ☒ Ingeniería Social
   - ☒ OSINT
   - ☐ Criptografía
   - ☐ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos?

☐ Ingeniería Social
☐ Criptografía
☐ OSINT
☒ Esteganografía

☐ Otros. ¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

☐ Me los enseñan en la escuela.
☐ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad
.....

☒ A través de videos e información publicados en Internet.
☐ En mi familia me hablan de estos temas porque los conocen.
☐ Tengo amigos que conocen más que yo y me los transmiten.
☐ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

⊗ SI ○ NO

10. ¿Qué fue lo que más te gustó del taller?
me gusta que trabajaramos con netbooks
.....
.....
.....

11. ¿Te gustaría volver a participar?
Si, me parecio muy entretenido
.....

12. ¿Tenés algún comentario que nos quieras dejar?
no, me parecio todo bien
.....
.....
.....
.....

¡¡MUCHAS GRACIAS!!

Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 16 Género: masculino

Escuela: Carlos Vergara N°1 Año que cursa: 3°

Nombre del equipo: .....

1. ¿Es la primera vez que jugabas una competencia CTF?

   (✓) SI ( ) NO

2. ¿La plataforma te resultó fácil de usar?

   (✓) SI ( ) NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   .....
   .....
   .....
   .....
   .....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)
   - ☐ Muy fáciles
   - ☐ Fáciles
   - ☑ Regulares
   - ☐ Difíciles
   - ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?
   - ☐ No utilicé ninguna pista
   - ☑ Entre 1 y 3 pistas
   - ☐ Entre 3 y 6 pistas
   - ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?
   - ☑ Ingeniería Social
   - ☑ OSINT
   - ☑ Criptografía
   - ☐ Esteganografía

☐ Otros. ¿Cuáles? TV, diario, internet

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

☐ Me los enseñan en la escuela.
☐ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad

.....

☐ A través de videos e información publicados en Internet.
☐ En mi familia me hablan de estos temas porque los conocen.
☐ Tengo amigos que conocen más que yo y me los transmiten.
☑ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

◉ SI ○ NO

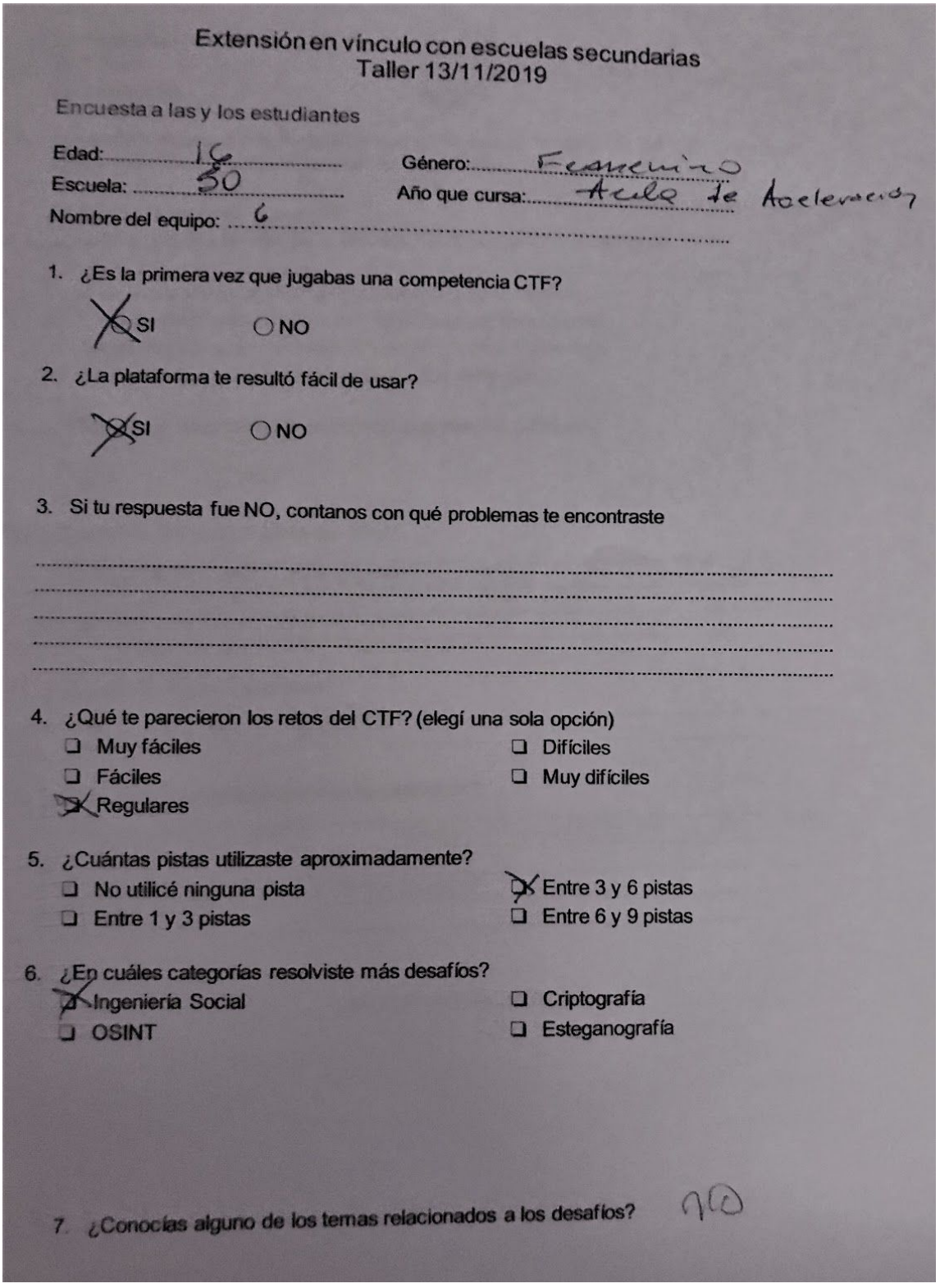
10. ¿Qué fue lo que más te gustó del taller?
pasar hacerlo con un amigo, competir con mis otros amigos y los premios (también el premio)

11. ¿Te gustaría volver a participar?
definitivamente !si!

12. ¿Tenés algún comentario que nos quieras dejar?
muy buenos desafíos y espero los próximos ganar hasta los premios (W.W.W)

¡¡MUCHAS GRACIAS!!

8.10.2 Encuestas de los alumnos de la escuela número 50



Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 16 Género: Femenino

Escuela: 50 Año que cursa: Aula de Aceleración

Nombre del equipo: 6

1. ¿Es la primera vez que jugabas una competencia CTF?

   ☒ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ☒ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   .....
   .....
   .....
   .....
   .....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ❑ Muy fáciles ❑ Difíciles
   ❑ Fáciles ❑ Muy difíciles
   ☒ Regulares

5. ¿Cuántas pistas utilizaste aproximadamente?

   ❑ No utilicé ninguna pista ☒ Entre 3 y 6 pistas
   ❑ Entre 1 y 3 pistas ❑ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   ☒ Ingeniería Social ❑ Criptografía
   ❑ OSINT ❑ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos? NO

- ❑ Ingeniería Social
- ❑ OSINT
- ❑ Criptografía
- ❑ Esteganografía
- ❑ Otros. ¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- ❑ Me los enseñan en la escuela.
- ❑ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad

.....

- ❑ A través de videos e información publicados en Internet.
- ❑ En mi familia me hablan de estos temas porque los conocen.
- ❑ Tengo amigos que conocen más que yo y me los transmiten.
- ❑ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

X SI ○ NO

10. ¿Qué fue lo que más te gustó del taller?

Me gusto mucho ingenieria social, todo en si.

11. ¿Te gustaría volver a participar?

Si, POR FAVOR

12. ¿Tenés algún comentario que nos quieras dejar?

SIGAN ASI, VAN A VENIR A LA ESCUELA TAMBIEN?

¡¡MUCHAS GRACIAS!!

Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 13 Género: F

Escuela: 50 Año que cursa: 4A

Nombre del equipo: 7

1. ¿Es la primera vez que jugabas una competencia CTF?

   (●) SI ( ) NO

2. ¿La plataforma te resultó fácil de usar?

   ( ) SI (●) NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   ~ co use mo nokbac

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ❑ Muy fáciles
   (●) Difíciles
   ❑ Fáciles
   ❑ Muy difíciles
   ❑ Regulares

5. ¿Cuántas pistas utilizaste aproximadamente?

   ❑ No utilicé ninguna pista
   ❑ Entre 3 y 6 pistas
   ❑ Entre 1 y 3 pistas
   (●) Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   (●) Ingeniería Social
   ❑ Criptografía
   ❑ OSINT
   ❑ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos?

❑ Ingeniería Social
❑ OSINT
❑ Criptografía
❑ Esteganografía
❑ Otros. ¿Cuáles? .....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

❑ Me los enseñan en la escuela.
❑ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad
.....
❑ A través de videos e información publicados en Internet.
❑ En mi familia me hablan de estos temas porque los conocen.
❑ Tengo amigos que conocen más que yo y me los transmiten.
❑ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

● SI ○ NO

10. ¿Qué fue lo que más te gustó del taller?

todo

11. ¿Te gustaría volver a participar?

Si mucho. Quiero seguir aprendiendo

12. ¿Tenés algún comentario que nos quieras dejar?

Gracias por la oportunidad

¡MUCHAS GRACIAS!

Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 17 Género: M

Escuela: 80 Año que cursa: Aceleración

Nombre del equipo: 7

1. ¿Es la primera vez que jugabas una competencia CTF?

   ◉ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ◉ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

.....
.....
.....
.....
.....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ❑ Muy fáciles ☒ Difíciles
   ❑ Fáciles ❑ Muy difíciles
   ❑ Regulares

5. ¿Cuántas pistas utilizaste aproximadamente?

   ❑ No utilicé ninguna pista ☒ Entre 3 y 6 pistas
   ❑ Entre 1 y 3 pistas ❑ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   ❑ Ingeniería Social ☒ Criptografía
   ❑ OSINT ❑ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos?

   NO.

- ❑ Ingeniería Social
- ❑ OSINT
- ❑ Criptografía
- ❑ Esteganografía
- ❑ Otros. ¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- ❑ Me los enseñan en la escuela.
- ❑ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad

.....

- ❑ A través de videos e información publicados en Internet.
- ❑ En mi familia me hablan de estos temas porque los conocen.
- ❑ Tengo amigos que conocen más que yo y me los transmiten.
- ❑ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

◉ SI ○ NO

10. ¿Qué fue lo que más te gustó del taller?

ME GUSTO CONOCER COSAS DE INFORMÁTICA, SEGURIDAD. NUNCA HABÍA SALIDO A NINGUN LUGAR CUANDO ESTUVE EN LA ESCUELA HASTA AHORA

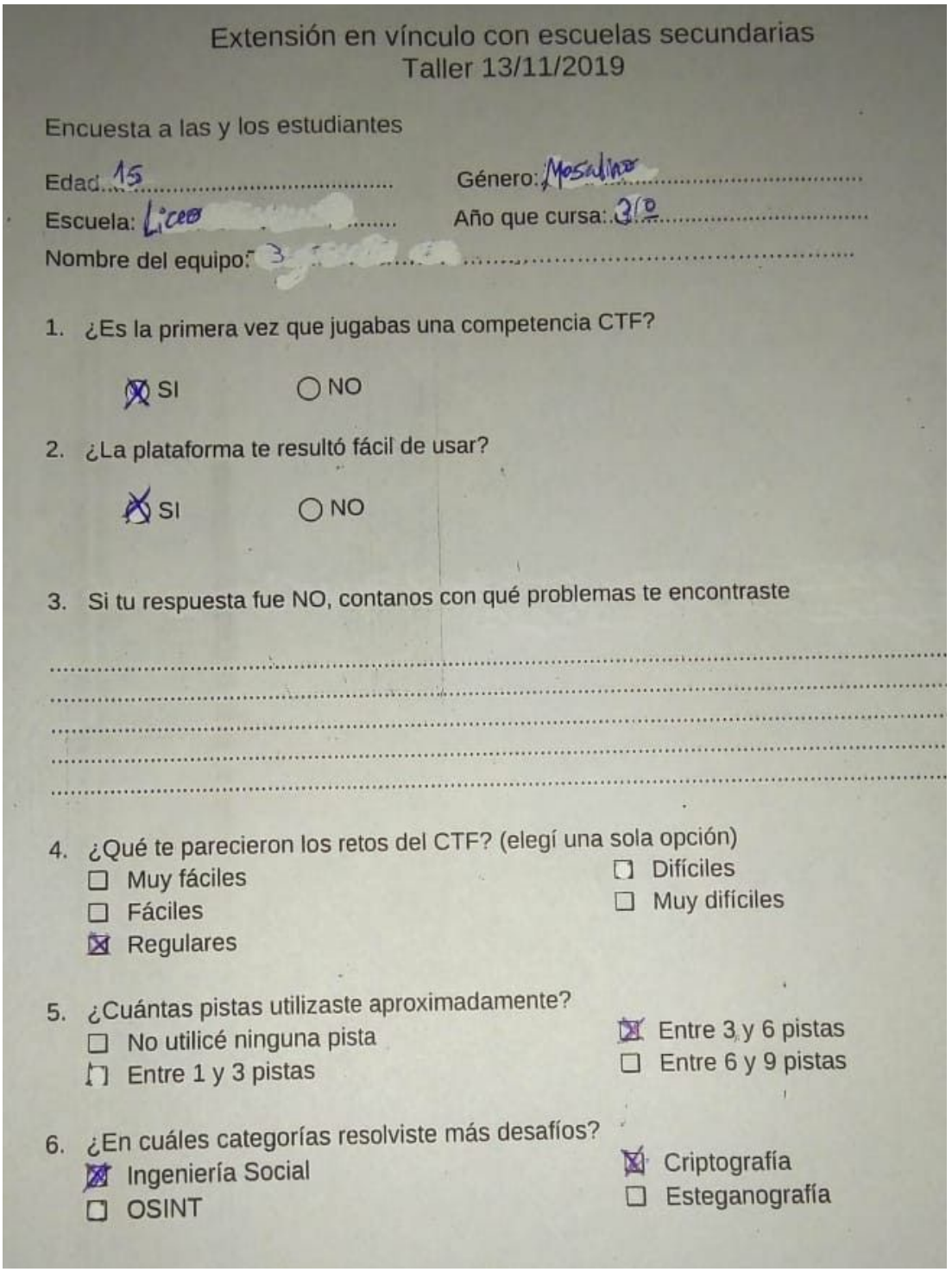
11. ¿Te gustaría volver a participar?

SI CLARO

12. ¿Tenés algún comentario que nos quieras dejar?

¡¡MUCHAS GRACIAS!!

8.10.3 Encuestas de los alumnos del colegio Liceo Victor Mercante



Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 15 Género: Masculino

Escuela: Liceo ... Año que cursa: 3/0

Nombre del equipo: 3 [illegible]

1. ¿Es la primera vez que jugabas una competencia CTF?

   ☒ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ☒ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   .....
   .....
   .....
   .....
   .....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ☐ Muy fáciles
   ☐ Fáciles
   ☒ Regulares
   ☐ Difíciles
   ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?

   ☐ No utilicé ninguna pista
   ☐ Entre 1 y 3 pistas
   ☒ Entre 3 y 6 pistas
   ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   ☒ Ingeniería Social
   ☐ OSINT
   ☒ Criptografía
   ☐ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos?

- [x] Ingeniería Social
- [ ] OSINT
- [x] Criptografía
- [ ] Esteganografía

- [ ] Otros. ¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

- [ ] Me los enseñan en la escuela.
- [ ] Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad .....
- [x] A través de videos e información publicados en Internet.
- [ ] En mi familia me hablan de estos temas porque los conocen.
- [x] Tengo amigos que conocen más que yo y me los transmiten.
- [ ] Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

- [x] SI
- ○ NO

10. ¿Qué fue lo que más te gustó del taller?

la actividad con los conductores

11. ¿Te gustaría volver a participar?

Sí

12. ¿Tenés algún comentario que nos quieras dejar?

Me gustó mucho, sigan haciéndolo

¡¡MUCHAS GRACIAS!!

Extensión en vínculo con escuelas secundarias
Taller 13/11/2019

Encuesta a las y los estudiantes

Edad: 15 Género: Femenino

Escuela: Liceo Víctor Mercante Año que cursa: 3°

Nombre del equipo: Tony Stark (?) N°3

1. ¿Es la primera vez que jugabas una competencia CTF?

   ☒ SI ○ NO

2. ¿La plataforma te resultó fácil de usar?

   ☒ SI ○ NO

3. Si tu respuesta fue NO, contanos con qué problemas te encontraste

   .....
   .....
   .....
   .....
   .....

4. ¿Qué te parecieron los retos del CTF? (elegí una sola opción)

   ☐ Muy fáciles
   ☐ Fáciles
   ☐ Regulares
   ☒ Difíciles
   ☐ Muy difíciles

5. ¿Cuántas pistas utilizaste aproximadamente?

   ☐ No utilicé ninguna pista
   ☒ Entre 1 y 3 pistas
   ☐ Entre 3 y 6 pistas
   ☐ Entre 6 y 9 pistas

6. ¿En cuáles categorías resolviste más desafíos?

   ☒ Ingeniería Social
   ☒ OSINT
   ☐ Criptografía
   ☐ Esteganografía

7. ¿Conocías alguno de los temas relacionados a los desafíos?

   ☐ Ingeniería Social
   ☐ OSINT
   ☒ Criptografía
   ☐ Esteganografía

☐ Otros. ¿Cuáles?.....

8. Si conocías alguno de los contenidos que se trataron en los desafíos del CTF, ¿cómo los habías aprendido? (podés elegir más de una opción)

☐ Me los enseñan en la escuela.
☐ Asistí a una charla fuera de la escuela. Contanos cuál fue la actividad
.....

☒ A través de videos e información publicados en Internet.
☐ En mi familia me hablan de estos temas porque los conocen.
☒ Tengo amigos que conocen más que yo y me los transmiten.
☐ Es la primera vez que me transmiten estos contenidos.

9. ¿El tiempo de duración de la competencia te pareció suficiente?

○ SI ⊗ NO

10. ¿Qué fue lo que más te gustó del taller?
Fue divertido estar en grupo con la presión del tiempo y de gritos y el reto que fue para nosotros adivinar las pistas.....
.....
.....

11. ¿Te gustaría volver a participar?
Si.....
.....

12. ¿Tenés algún comentario que nos quieras dejar?
No.....
.....
.....
.....
.....

¡¡MUCHAS GRACIAS!!

9. Índice de tablas

Tabla 1 - Cuadro comparativo de los CTFs investigados 27

Tabla 2 - Cuadro comparativo de las tesis y los proyectos similares investigados 28

Tabla 3 - Nivel de importancia de las características y subcaracterísticas 44

Tabla 4 - Características de calidad externa 45

Tabla 5 - Características y subcaracterísticas de calidad externa 46

Tabla 6 - Escala de medición de la calidad 49

Tabla 7 - Resultado de calidad de CTFd 50

Tabla 8 - Resultado de calidad de Mellivora 50

Tabla 9 - Valor de las características de Mellivora 51

Tabla 10 - Valor de las características de CTFd 51

Tabla 11 - Mejoras efectuadas para la segunda instancia de prueba 67

Tabla 12 - Mejoras efectuadas a la plataforma para la segunda evaluación 67

Tabla 13 - Métricas de usabilidad 86

Tabla 14 - Métricas de seguridad 87

Tabla 15 - Métricas de portabilidad 88

Tabla 16 - Evaluación de calidad externa de Mellivora 90

Tabla 17 - Evaluación de calidad externa de CTFd 92

Tabla 18 - Resultado final de la calidad externa de Mellivora 93

Tabla 19 - Resultado final de la calidad externa de CTFd 93

10. Índice de figuras

Figura 1 - Calidad del Producto de Software 42

Figura 2 - Matriz de calidad 48

Figura 3 - Evaluación de calidad externa de Mellivora y CTFd 51

Figura 4 - Análisis global de accesibilidad de CTFd 53

Figura 5 - Dependencias entre categorías 58

Figura 6 - Desafíos del CTF 59

Figura 7 - Desafío de la Escítala 59

Figura 8 - Tabla de puntuaciones finales de la primer evaluación 62

Figura 9 - Desafío sitios falsos 64

Figura 10 - Flag del desafío sitios falsos 64

Figura 11 - Tabla de puntuaciones finales de la segunda evaluación 70

Figura 12 - Resultados encuesta: Facilidad de la plataforma 73

Figura 13 - Resultados encuesta: Dificultad de los desafíos 74

Figura 14 - Resultados encuesta: Conocimiento de las temáticas 74

Figura 15 - Resultados encuesta: Volver a participar 75

Figura 16 - Desempeño del Alumno en la Primera Instancia 78

Figura 17 - Desempeño del Alumno en la Segunda Instancia 79

Figura 18 - Análisis de accesibilidad global de Mellivora 116

Figura 19 - Análisis de accesibilidad de los enlaces de Mellivora 117

Figura 20 - Análisis global de accesibilidad de CTFd 118

Figura 21 - Análisis de accesibilidad de los enlaces de CTFd 119

11. Bibliografía

[1] Blanco Parajón Manuel, Batlle Adrián M., “Iniciación a los CTF”, Cyberworking Ponferrada, 2018.

[2] Comunidad EphorSec. (23 de septiembre de 2017). Que es un CTF | Tienes que capturarlas todas - EphorSec. Recuperado el 17 de abril de 2019, de http://www.ephorsec.co/que-es-un-ctf/

[3] Collado, P. (17 de julio de 2015). Capture The Flag - Security Artwork, un blog de la compañía S2 Grupo. Recuperado el 15 de abril de 2019, de https://www.securityartwork.es/2015/07/17/capture-the-flag/

[4] CTFtime team. (s.f.). CTFtime.org / All about CTF (Capture The Flag). Recuperado el 16 de abril de 2019, de https://ctftime.org/ctf-wtf/

[5] Centro de respuesta a incidentes de seguridad INCIBE. (26 de febrero de 2014). CTF: Entrenamiento en seguridad informática | INCIBE-CERT. Recuperado el 15 de abril de 2019, de https://www.incibe-cert.es/blog/ctf-entrenamiento-seguridad-informatica

[6] Leune Kess, Petrilli Salvatore J., “Using Capture The Flag to enhance to effectiveness of cybersecurity education”, Adelphi University, Garden City, New York, SIGITE '17, Rochester, NY, USA, 2017.

[7] Proyecto Internacional Red Global de Aprendizajes. (s.f.). Red Global de Aprendizajes. Recuperado el 30 de abril de 2019, de https://redglobal.edu.uy/

[8] Mc Daniel Lucas, Talvi Erik, Hay Brian, “Capture the Flag as Cyber Security Introduction” en IEEE Computer Society Washington, “Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS)”, University of Alaska Fairbanks, 2016.

[9] Cheung Ronald S., Cohen Joseph P., Lo Henry Z., Elia Fabio, “Challenge Based Learning in Cybersecurity Education”, Department of Computer Science, University of Massachusetts, Boston, MA, USA, 2011.

[10] Eagle Chris, Clark John L., “Capture The Flag: Learning Computer Security Under Fire”, Naval Postgraduate School, 2004.

[11] Fundación Hack in the Class. (s.f.). Hack in the Class. Recuperado el 6 de mayo del 2019, de http://hackintheclass.nl/

[12] Amrita School of Engineering & School of Arts and Sciences. (s.f.). InCTF. Recuperado 24 de julio de 2019, de https://inctf.in/

[13] Universidad Carnegie Mellon. (s.f.). picoCTF - CMU Cybersecurity Competition. Recuperado el 4 de junio de 2019, de https://picoctf.com/

[14] Club de Seguridad Informática de Thomas Jefferson High School for Science and Technology. (s.f.). Home - TJCTF 2019, High School CTF Competition. Recuperado el 3 de junio de 2019, de https://www.tjctf.org/

[15] West Windsor-Plainsboro High School North. (s.f.). HSCTF - The First CTF by High Schoolers, for High Schoolers. Recuperado el 6 de junio de 2019, de https://hsctf.com/

[16] Durkin, Z., Pace, P., Purves, T., Daggett, D. y Weaver, M. (s.f.). NeverLAN CTF 2020. Recuperado el 16 de julio de 2019, de https://neverlanctf.com/

[17] Vu, T., Sea, D., y Mendoza A. (s.f.). Tech CTF - Home. Recuperado el 19 de julio de 2019, de https://techctf.com/

[18] Club de Informática de la Academia Newark. (s.f.). NACTF. Recuperado el 20 de septiembre de 2019, de https://nactf.com/

[19] Martín Sanchez Laura, Sancho Nuñez José C., Durán Domínguez Arturo, “Capture The Flag - Prácticas de Ciberseguridad mediante técnicas de e-learning” en Valverde Berrecoso Jesús, “Libro del I Congreso Internacional de Campus Digitales en la Educación Superior”, Universidad de Extremadura, 2018.

[20] Sancho Nuñez José C., Caro Lindo Andrés, Martín Sanchez Laura, Félix de Sande José A, “CyberSecurity Challenge: Detección de talento en ciberseguridad mediante una competición virtual de Capture The Flag” en Zurutuza Urko, Iturbe Mikel, Ezpeleta Enaitz, Garitano Iñaki “Actas de las IV Jornadas Nacionales de Investigación en Ciberseguridad”, Mondragon Unibertsitatea, 2018.

[21] González Mejías Sergio, “El aprendizaje basado en juegos a través de la plataforma Facebook Capture The Flag”, Universitat Oberta de Catalunya, 2018.

[22] Rey Betancourt Leonardo E., “Class Capture The Flag: una nueva manera de aprender seguridad informática”, Trabajo de Fin de Grado, Universidad de Cantabria, 2015.

[23] Werther Joseph, Zhivich Michael, Leek Timothy, Zeldovich Nickolai, “Experiences in Cyber Security Education: The MIT Lincoln Laboratory Capture The Flag Exercise”, 2011.

[24] International Telecommunication Union, “Global Cybersecurity Index (GCI) 2018 Draft”, Ginebra, Suiza, 2018.

[25] UNICEF Paraguay. (7 de junio de 2018). Campaña de UNICEF Paraguay gana premio Inspire en Holanda. Recuperado el 30 de abril de 2019, de https://www.unicef.org/paraguay/comunicados-prensa/campaña-de-unicef-paraguay-gana-premio-inspire-en-holanda

[26] UNICEF Paraguay. (3 de enero de 2018). Campaign #DigitalIsReal - YouTube. Recuperado el 30 de abril de 2019, de https://www.youtube.com/watch?v=kSatdXGEvmY&feature=youtu.be

[27] Diario La Nación Paraguay. (4 de agosto de 2018). Ciberseguridad en niños: Control de padres es clave | La Nación. Recuperado el 30 de abril de 2019, de https://www.lanacion.com.py/pais/2018/08/04/ciberseguridad-en-ninos-control-de-padres-es-clave/

[28] Organización Argentina Cibersegura. (s.f.). Trabajamos para prevenir riesgos que afectan a las personas en Internet | Argentina Cibersegura. Recuperado el 3 de mayo de 2019, de https://www.argentinacibersegura.org/

[29] Fundación Dr. Manuel Sadosky. (s.f.). Fundación Sadosky | Investigación y Desarrollo en TIC. Recuperado el 3 de mayo de 2019, de http://www.fundacionsadosky.org.ar/

[30] Fundación Dr. Manuel Sadosky. (s.f.). Capture The Flag Junior | Fundación Sadosky. Recuperado el 8 de junio de 2019, de http://www.fundacionsadosky.org.ar/ctf-junior/

[31] Fundación Dr. Manuel Sadosky. (noviembre de 2018). Manual Docente | Primer Ciclo de Primaria | Program.AR Recuperado el 18 de julio de 2019, de http://program.ar/manual-primer-ciclo-primaria/

[32] Fundación Dr. Manuel Sadosky. (agosto de 2018). Manual Docente | Segundo Ciclo de Primaria | Program.AR. Recuperado el 18 de julio de 2019, de http://program.ar/manual-segundo-ciclo-primaria/

[33] Fundación Dr. Manuel Sadosky. (abril de 2019). Manual Docente | Primer Ciclo de Secundaria | Program.AR. Recuperado el 18 de julio de 2019, de http://program.ar/manual-primer-ciclo-secundaria/

[34] Borghello, C. (s.f.). Segu Kids - Juntos en la Red - Seguridad para menores, padres y docentes. Recuperado el 18 de abril de 2019, de www.segu-kids.org

[35] Chacón Paula, "El juego didáctico como estrategia de enseñanza y aprendizaje", Departamento de Educación Especial, Instituto Pedagógico de Caracas, Universidad Pedagógica Experimental Libertador, 2008.

[36] Andrés Andreu María Ángeles, García Casas Miguel, "Actividades lúdicas en la enseñanza de LFE: el juego didáctico", Universidad Politécnica de Valencia en "Actas del Primer Congreso Internacional de Español para Fines Específicos", Ámsterdam, 2000.

[37] GitHub - Nakiami/mellivora: Mellivora is a CTF engine written in PHP. (21 de noviembre de 2019). Recuperado el 13 de mayo de 2019, de https://github.com/Nakiami/mellivora

[38] Free Software Foundation. (18 de noviembre de 2016). The GNU General Public License v3.0 - GNU Project - Free Software Foundation. Recuperado el 13 de mayo de 2019, de https://www.gnu.org/licenses/gpl-3.0.en.html

[39] Chung, K. (20 de diciembre de 2019). GitHub - CTFd/CTFd: CTFs as you need them. Recuperado el 9 de septiembre de 2019, de https://github.com/CTFd/CTFd

[40] Chung, K. (4 de febrero de 2019). CTFd: The Easiest Capture The Flag Platform. Recuperado el 9 de septiembre de 2019, de https://ctfd.io/terms-of-use/

[41] Facebook. (14 de septiembre de 2018). GitHub - facebook/fbctf: Platform to host Capture the Flag competitions. Recuperado el 27 de mayo de 2019, de https://github.com/facebook/fbctf

[42] Creative Commons. (s.f.). Creative Commons — Attribution-NonCommercial 4.0 International — CC BY-NC 4.0. Recuperado el 27 de mayo de 2019, de https://creativecommons.org/licenses/by-nc/4.0/

[43] International CyberEx. (s.f.). International CyberEx | INCIBE-CERT. Recuperado el 10 de octubre de 2019, de https://www.incibe-cert.es/international-cyberex

[44] OEA Cyberwomen Challenge. (28 de junio de 2019) - Llega a la Argentina el "OEA CyberWomen Challenge" | Ministerio de Relaciones Exteriores y Culto. Recuperado el 1 de julio de 2019, de https://www.cancilleria.gob.ar/es/actualidad/noticias/llega-la-argentina-el-oea-cyberwomen-challenge

[45] Facebook CTF. (1 de junio de 2019). Facebook CTF 2019 - Welcome to Facebook's first-ever global CTF! Recuperado el 15 de septiembre de 2019, de https://web.archive.org/web/20190601004931/https://fbctf.com/

[46] GitHub - easyctf/easyctf-iv-platform: EasyCTF IV. (21 de febrero de 2018). Recuperado el 3 de junio de 2019, de https://github.com/EasyCTF/easyctf-iv-platform

[47] Easy CTF. (3 de abril de 2018). Home - EasyCTF IV, High School CTF Competition. Recuperado el 3 de junio de 2019, de https://web.archive.org/web/20180403083343/https://easyctf.com/

[48] GitHub - easyctf/librectf: CTF in a box. Minimal setup required. (not production-ready yet). (17 de febrero de 2019). Recuperado el 3 de junio de 2019, de https://github.com/easyctf/librectf

[49] Apache Software Foundation. (enero de 2004). Apache License, Version 2.0. Recuperado el 3 de junio de 2019, de https://www.apache.org/licenses/LICENSE-2.0

[50] Open Source Initiative. (s.f.). The MIT License | Open Source Initiative. Recuperado el 3 de junio de 2019, de https://opensource.org/licenses/MIT

[51] Intro - OpenCTF. (s.f.). Recuperado el 3 de junio de 2019, de https://easyctf.github.io/librectf/v0.0.0-8/

[52] librectf/docs at develop - easyctf/librectf - GitHub. (20 de noviembre de 2018). Recuperado el 3 de junio de 2019, de https://github.com/easyctf/librectf/tree/develop/docs

[53] Roger S. Pressman, Ph.D. , "Ingeniería del software: un enfoque práctico", Séptima Edición, Universidad de Connecticut, 2010.

[54] NORMAS ISO 25000. (s.f). Recuperado el 21 de diciembre de 2019, de https://iso25000.com/index.php/normas-iso-25000

[55] ISO 25010. (s.f.). Recuperado el 22 de diciembre de 2019, de https://iso25000.com/index.php/normas-iso-25000/iso-25010

[56] ISO 25040. (s.f.). Recuperado el 22 de diciembre de 2019, de https://iso25000.com/index.php/normas-iso-25000/iso-25040

[57] Balseca Chisaguano Evelyn A., “Evaluación de calidad de productos software en empresas de desarrollo de software aplicando la norma ISO/IEC 25000”, Facultad de Ingeniería de Sistemas, Escuela Politécnica Nacional, Quito, 2014.

[58] Defalco Magalí E., Rajoy Gaspar, “Analizador intensivo de accesibilidad basado en reglas”, Facultad de Informática, Universidad Nacional de La Plata, 2015

[59] Defalco Magalí E., Rajoy Gaspar. (s.f.). SiMor - Validador de Accesibilidad Web. Recuperado el 14 de diciembre de 2019, de http://simor.linti.unlp.edu.ar/

[60] Fundación Dr. Manuel Sadosky. (s.f.). PRECTF 2019. Recuperado el 8 de junio de 2019, de https://ctf.fundacionsadosky.org.ar/prectf

[61] Librería Digital Internet Archive (s.f.). Wayback Machine. Recuperado el 3 de noviembre de 2019, de https://web.archive.org/

[62] Libre Lab UCM - Universidad Complutense de Madrid (s.f). Home: Trinity - Mellivora, the CTF engine. Recuperado el 22 de diciembre de 2019, de https://trinity.librelabucm.org/home

[63] CTFd (s.f). This is a fully functional demo of CTFd platform. Recuperado el 22 de diciembre de 2019, de https://demo.ctfd.io/