Fundación Universitaria
SAN MATEO

INGENIERÍA DE SISTEMAS

FACULTAD DE INGENIERIA Y AFINES
INGENIERIA DE SISTEMAS

PLATAFORMA PARA EL FORTALECIMIENTO DE CONOCIMIENTOS EN SEGURIDAD INFORMATICA A NIVEL ACADEMICO

TRABAJO DE GRADO MODALIDAD DE OPCIÓN DE GRADO

JORGE REINALDO LINARES PINEDA
LEANDRO ALBERTO GARCIA

DIRECTOR (A)
LUIS GUILLERMO MOLERO SUAREZ

BOGOTA D.C. COLOMBIA
2018

NOTA DE SALVEDAD DE RESPONSABILIDAD INSTITUCIONAL

"La Fundación Universitaria San Mateo NO se hace responsable de los conceptos emitidos en el presente documento, el departamento de investigaciones velará por el rigor metodológico de la investigación".

CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

DEDICATORIA

Esta tesis va dedicada con todo nuestro amor a las mujeres más hermosas que han logrado sacar lo mejor de nosotros apoyándonos y acompañándonos en este largo camino que con ayuda de este proyecto culminamos y damos paso a nuevas aventuras, gracias a ellas que nos han dado su cariño en los momentos más difíciles, su apoyo y compresión, estos seres tan hermosos son nuestras esposas, madres, hermanas e hija gracias de todo corazón y por ustedes vamos por mucho mas

AGRADECIMIENTOS

Agradecemos de todo corazón a cada profesor que ha aportado en nuestra formación durante toda nuestra vida, a ellos que sin pensar en formar grandes cuidados nos han hecho lo que somos hoy en día, a mi profesor de colegio Jerson Alonso Alvares que me apoyo en esa etapa tan crucial en mi formación motivándome a ser mejor persona sin con lo más mínimo, a nuestro profesor de inicios de programación Edward Reyes quien gracias a sus consejos en programación y su gran talento por enseñar esta área nos motivó y genero una pasión sobre una rama de la informática que pocos suelen manejar.

ABREVIATURAS

Abreviatura	Palabra	Definición
C.T.F.	Capture the flag	Se define como capturar la bandera a cada punto alcanzado sobre un reto expuesto al jugador
I.O.T	Internet Of Things	Se define como internet de las cosas, donde todo dispositivo que esté conectado a la red de redes puede ser encontrado
F.U.S.	Fundación Universitaria San Mateo	Fundación a la cual se presenta el proyecto de investigación.
MIT/LL CTF	MIT Lincoln Laboratory Capture-the-Flag	Laboratorio fundado por the MIT (Institute technology Massachuset)

RESUMEN

Las plataformas de CTF (Capture The Flag) por sus siglas en inglés "Capturar la bandera", fueron implementadas por la milicia un tiempo atrás, hoy en día se usan para prácticas de hacking en eventos importantes de seguridad informática. Estas plataformas permiten a las personas que las usan estar en un entorno seguro y manejable para poder usar sus conocimientos en pro de su fortalecimiento y madurez, permitiendo poder competir con otros usuarios y demostrar su capacidad de razonamiento.

Comentado [1]: Palabras claves?

Palabras Claves:

- Capturar la bandera
- Seguridad Informática
- Juegos de Guerra
- Hacking
- Aprendizaje
- Conocimiento

ABSTRACT

The platforms of CTF (Capture The Flag) by its abbreviations in English "Capture the flag", were implemented by the militia some time back, nowadays they are used for practices of hacking in important events of computer security.

These platforms allow the people who use them to be in a safe and manageable environment in order to use their knowledge for their strengthening and maturity, allowing them to compete with other users and demonstrate their reasoning ability.

KEY WORDS:

- Capture the flag
- Informatic security
- War games
- Hacking
- Learning
- Knowledge

Comentado [2]: Abstract

INTRODUCCIÓN

El término hacking ético hace referencia a una persona que con sus conocimientos avanzados en informática y seguridad realiza pruebas en sistemas complejos para encontrar vulnerabilidades para luego generar un informe y entregar a una entidad para que tome las medidas suficientes sin generar daños.

El uso de técnicas de hacking en sistemas fue la solución que empresarios de alto rango le dieron a sus redes al ver que muchas veces eran vulnerados, con el fin de solucionar este tipo de problemas decidieron contratar a hacker's experimentados a los cuales por medio de temas éticos y morales les atribuyó el nombre de Hacker Ético, esto dio un gran inicio a que todo tipo de gobierno tuviera dentro de sus filas a expertos en sistemas computacionales para proteger sus redes.

Según Emanuel Abraham, Ethical Hacker de la empresa Security Solutions & Education (SSE), representantes para Colombia de EC Council (Consejo Internacional de Comercio Electrónico): "el hacker ético trabaja en encontrar estas vulnerabilidades para que no sean explotadas por otros hackers. Trata de adelantarse e identificarlas antes que los criminales".

Esto recrea una vista mucho más amplia sobre que es capaz de realizar un hacker ético y sobre las medidas de seguridad con lo cual puede apoyar desde una gran empresa internacional hasta una empresa pequeña.

Los juegos de guerra es una estrategia que las fuerzas militares usaron para poder fortalecer sus conocimientos y habilidades en sistemas, estos juegos consisten en crear grupos de personas con altos conocimientos en computación para crear un escenario donde los participantes intentarán acceder al sistema que los contrincantes intentan defender, gana el equipo que pueda acceder al sistema del adversario y tomar posesión de este.

Eli Fashka, presidente de Soluciones Seguras comentó sobre la importancia de las competencias, 'la idea es darles a los asistentes una noción práctica de seguridad informática sobre cuáles son los riesgos, cómo un atacante podría entrar a su página y cómo protegerla'. 'Uno necesita tener el conocimiento de cómo se pueden hacer las cosas malas para prevenirlas', añadió

En la actualidad muchos grupos han tomado este tipo de eventos para generar eventos que permiten ahora no solo a militares sino a personas del común y corriente acceder a estos tipos de eventos y generar una cultura en seguridad informática, el mayor evento de warGames se lleva a cabo en la ciudad de las Vegas en Estados Unidos el cual se llama "DEFCON".

Esta investigación quiere dar a conocer el uso de las plataformas de aprendizaje en seguridad informática tipo WarGames para generar en el estudiante un interés adicional por fomentar su auto aprendizaje y superación personal.
.

Comentado [3]: Donde se cierra la introducción con el aporte de esta investigación.

CAPITULO I

DESCRIPCIÓN DEL PROYECTO

I.Presentación del problema de investigación

La seguridad informática es un área de conocimiento que está en crecimiento constante, durante los años pasados se ha podido evidenciar la necesidad de mejorar técnicas, procesos o estrategias para poder mitigar al ciber delincuente.

Con la falla de seguridad presentada el año pasado (WannaCry) se evidencio la falta de seguridad en las empresas, de este modo al analizar los ataques de ciber delincuentes en Bogotá podemos llegar a una cifra alarmante que debe preocupar al gobierno y a las empresas privadas.

Todo se evidencia a la falta de conocimientos o de técnicas de seguridad informática sobre los profesionales que hoy en día se forman en nuestra ciudad Bogotá.

Para realizar una buena formación en seguridad informática, las empresas especialistas en esta rama utilizan una plataforma para capacitar a sus profesionales dándoles a conocer las nuevas técnicas o reforzando las existente.

En la fundación Universitaria san mateo existe una materia en la carrera de Ingeniería de Sistemas e Ingeniería en Telecomunicaciones que se llama Seguridad informática, en esta carrera del pensum se dan a conocer técnicas, procedimientos y leyes que son aplicables al momento de sufrir un ataque cibernético pero debido al corto tiempo de cada semestre, esta materia se olvida y se pasa sin tener en cuenta la importancia que tiene para la vida laboral.

Después de tener en cuenta estos factores que se han explicado anteriormente, la pregunta problema de esta tesis de investigación es ¿Como fortalecer el conocimiento en seguridad informática en estudiantes de la fundación universitaria san mateo?

Comentado [4]: Mejorar redacción

Comentado [5]: arreglado

II.Justificación

El fomentar y cultivar en una persona una cultura de auto aprendizaje sobre un área específico es la mayor hazaña que un docente puede tener, en seguridad informática con ayuda de nuestra plataforma el estudiante se ve retado a superar cada desafío que este demande con el fin de superarse a el mismo y a sus competidores.

Cada desafío obliga al estudiante a consultar sobre un tema en específico ayudando a que el estudiante maneje sus propias herramientas con las cuales cumple cada desafío y se capacita ante cualquier prueba que en la vida real se pueda presentar, de esta manera se puede mejorar la calidad del profesionalismo de cada ingeniero que sea egresado de la Fundación universitaria San Mateo para abrir campo a una mejora constante entre calidad e innovación.

III.Objetivos

A. Objetivo General

- Diseñar una plataforma de entrenamiento para el aprendizaje y fortalecimiento de habilidades en seguridad informática en la Fundación universitaria San Mateo (F.U.S.)

B. Objetivos Específicos

- Realizar el diseño estructural de la base de datos relacional para la plataforma de entrenamiento para el aprendizaje y fortalecimiento de habilidades en seguridad informática
- Desarrollar la arquitectura basada en el Modelo Vista Controlador para la plataforma de entrenamiento para el aprendizaje y fortalecimiento de habilidades en seguridad informática
- Diseñar la interfaz gráfica de la plataforma de entrenamiento para el aprendizaje y fortalecimiento de habilidades en seguridad informática
- Realizar la documentación de pruebas de la plataforma de entrenamiento para el aprendizaje y fortalecimiento de habilidades en seguridad informática

Comentado [6]: No veo un objetivo donde se evalué la situación actual de la investigación.

La investigación sin bases formales establece que hay un problema, pero no lo demuestra con hechos factibles, estadísticas, metodologías aplicadas, encuestas, entrevistas, etc, etc.

Cual es el sustento de la investigación? donde se estudia? se dice? se concluye? que hay falencias en el área de la seguridad informática en la Universidad San Mateo?

Comentado [7]: No se pueden utilizar dos verbos en un objetivo especifico

Comentado [8]: El Mock-Up es un bosquejo, por ende, esta de mas colocarlo. Asimismo, se usa un lenguaje genérico para que el lector que desconoce la investigación la entienda.

Toda plataforma didáctica debe tener una interfaz amigable, se sugiere revisar este objetivo.

CAPITULO II

MARCO TEÓRICO

IV.Antecedentes de la investigación

En los últimos diez años, la docencia apoyada con los medios tecnológicos actuales ofrece un sin número de posibilidades al mundo de la educación ya que pueden facilitar ampliamente la enseñanza de conceptos y materias, apoyando la resolución de problemas y contribuyendo ampliamente al desarrollo de habilidades cognitivas. Marqués Aldo [1] plantea, "Los buenos recursos educativos multimedia tienen un alto potencial didáctico ya que su carácter audiovisual e interactivo resulta atractivo y motivador para los estudiantes, que además pueden conocer inmediatamente los resultados de sus actuaciones ante el ordenador y muchas veces incluso pueden configurar los programas según sus intereses o necesidades (niveles de dificultad, itinerarios, tiempo disponible para las respuestas...". Han pasado 18 años desde que Márquez manifiesta que las ayudas multimedia proporcionan gran valor a la catedra ya que genera a los estudiantes mayor interés al momento de explicar temas complejos, al igual en su postura transforma una computadora en una maquina con fines netamente educativos brindando de esta manera un gran aporte al desarrollo de competencias y aprendizajes en una diversidad de población con características socioculturales.

Los estudios que anteceden sobre CTF generalmente se han dividido en básicamente en dos categorías. La primera categoría trata de la utilidad de los CTF. En general, se acepta que los juegos de CTF son herramientas pedagógicas útiles. Por ejemplo, Dabrowski manifestó que el uso de desafíos similares a CTF como parte de una clase de seguridad motivó a los estudiantes a esforzarse más en su aprendizaje [2] Además, Carlisle compartió que la incorporación de CTF en un currículo en la academia de la fuerza aérea de los Estados Unidos condujo a un mayor interés de los estudiantes en los estudios de ciberseguridad, una mayor colaboración entre los estudiantes y una mayor disposición hacia los estudios auto dirigidos [3]. Chothia también encontró una correlación entre los estudiantes que se desempeñan bien en CTF al estilo de riesgo y que se desempeñan bien en evaluaciones más formales [4].

La segunda categoría trata más sobre la mecánica de organizar y ejecutar un CTF, y generalmente incluye lecciones aprendidas de anteriores CTF e ideas sobre cómo mejorar las realizadas en el futuro. Por ejemplo, Chung describió las

deficiencias y fortalezas de varios eventos CTF en términos de diseño del juego y su eficacia pedagógica [5], y Davis [6] y Vigna [7], respectivamente, escribieron sobre la arquitectura del MIT/LL CTF e iCTF, así como sus experiencias en la organización de estos eventos CTF. Si bien los equipos participantes narran sus experiencias en varios eventos CTF (como [8], [9] y [10]), no se conocemos ningún estudio sistemático que se haya realizado sobre cómo los participantes juegan el juego CTF. Tampoco se conoce ningún estudio sistemático que examine la relación entre las tácticas de los participantes del CTF y sus correspondientes clasificaciones finales.

Los CTF son beneficiosos para los investigadores de seguridad y académicos que pueden utilizar los datos del atacante y el tráfico de red generado durante las competencias como casos de estudio para ayudar a modelar, predecir y prevenir incidentes de seguridad en el mundo real [11]. Además, en un estudio realizado por IBM Security en noviembre del 2016 manifiesta que estos ejercicios son una herramienta de evaluación para ayudar a las organizaciones a entender el panorama de amenazas y para probar la capacidad de respuesta ante un ataque cibernético.

Tren Micro es una entidad especializada en seguridad informática la cual realiza una competencia anual denominada cature of flag de trend micro, entre los objetivos de esta competencia esta una labor social la cual consiste en fomentar estos torneos para que cada vez más personas en especialmente apasionados de la ciber seguridad cuenten con un espacio simulado, controlado y con una excelente infraestructura para que exploten, adquieran y fortalezcan sus conocimientos y habilidades. Esta compañía también hace mención en una publicación de junio de 2017 sobre el problema potencial que tiende hace una crisis debido al déficit de especialistas en el sector, basándose en una investigación realizada por el gobierno británico, la asociación ISACA la cual prevé una escasez global de dos millones de profesionales de la seguridad informática y en cinco años de 1.8 millones, sumándole a esto la falta de habilidades en los jóvenes para ocupar cargos relacionados y las personas mayores las cuales son especialistas se retiran. La investigación también arroja un panorama desalentador por genero ya que solo el 14 por ciento en Estados Unidos son mujer un poco mayor comparado con en el promedio mundial que es de un 11 por ciento.

El problema es muy grave ya que día a día aumentan los atacantes, ciber delincuentes y el crimen organizado en el mundo digital, sin mencionar las diferentes técnicas de penetración y ataque que surgen en el transcurrir de los días, dejándonos a la intemperie de un sistema en el cual somos vulnerables no solo digital sino físicamente a este nivel ha evolucionado y sigue evolucionando este flagelo, de ahí el llamado a fomentar el fortalecimiento en conocimiento y habilidades en la seguridad informática las cuales se pueden adquirir con una mayor interacción en plataformas de entrenamiento como los ctf.

V.Bases teóricas o fundamentos conceptuales

A. CTF

Son competencias de seguridad cibernética donde los equipos participantes compiten entre sí para capturar banderas virtuales. Según la clasificación las banderas se pueden obtener resolviendo acertijos relacionados con seguridad informática o bien comprometiendo la infraestructura de los contrincantes del evento la cual se encuentra en ambientes controlados. CTFTime.org [12] clasifica en su blog los ctf en tres tipos de eventos a partir de ciertas características particulares como se muestran a continuación:

- Jeopardy: este tipo de eventos cuenta con varias subcategorías de desafíos los cuales mediante que se resuelven su dificultad aumenta y proporciona banderas o puntos directamente proporcional a la dificultad del desafío. Habitualmente este tipo de evento cuenta con las siguientes categorías:
  - Pwnables, estos desafíos solicitan la explotación de vulnerabilidades, pero a aplicaciones de la compañía.
  - Criptografía: Suele trabajar temas de mensajes ocultos en textos previamente encriptados.
  - Esteganografía: Es la detección de texto sobre imágenes, se le da acceso al usuario a una imagen por defecto, el usuario debe poder obtener el texto en claro en la imagen.
  - Web: Se debe conocer sobre programación web, en esta parte el usuario debe encontrar la bandera en una página web especifica publicada por el usuario.
  - IoT: El usuario debe obtener la bandera en base a los logs generados por conexiones de IoT, estas conexiones pueden ser SSH, FTP, Protocolos de almacenamiento Bin.
  - Malware: El usuario debe saber de dónde proviene el malware publicado, y que acciones realiza el malware, apoyándose en uso de herramienta de análisis de malware.
  - Lenguaje de Programación: En esta parte se publican programas codificados con un lenguaje de programación especifico, lo que se requiere es poder aprovecharse de ellos e ingresar a la bandera que este almacena.
  - Ingeniería Inversa: Se da un archivo el cual es el resultado de una ejecución en el sistema, se debe saber quién origino este archivo y la forma en como lo origino es la bandera.

- Defensa y ataque: en este tipo de desafíos cada participante o equipo recibe una red o host con varios servicios o puertos que son vulnerables los cuales deben defender, de igual manera también deben comprometer las vulnerabilidades de sus oponentes para poder obtener un archivo que contiene la bandera. El juego se desarrolla acumulando puntos cuando se penetra la seguridad del oponente y se deducen puntos si el sistema es vulnerado.
- CTF mixtos: Esta categoría agrupa un sin número de formatos, los cuales proponen tareas las cuales requieren de tiempo y dedicación para lograr el desafío.

B. Seguridad Informática

Consiste en proteger los recursos de un sistema de información en una organización para que este no sea accedido de una forma fraudulenta y que los accesos sean controlados, con el fin de salva guardar los principios básicos de la seguridad de la información:

- Confidencialidad: Permite que solo personas con autorización puedan acceder a la información.
- Integridad: Consiste en mantener datos fidedignos y garantizar la no modificación de estos sin consentimiento del usuario autorizado.
- Disponibilidad: Consiste en mantener de manera concurrente en cualquier momento y lugar la información.
- Autenticidad: Consiste en la validación de los parámetros presentados los cuales otorgan o niegan una acción frente al sistema de información.
- Autorización: Consiste en la otorgación de las credenciales asignadas al perfil validando los privilegios con los que cuenta el usuario, para realizar determinadas acciones en el sistema o con la información.
- Auditabilidad: Consiste en mantener un log con las acciones transaccionales en el sistema frente a los datos.
- No repudio: Consiste en llevar controles que permitan comprobar las acciones que se realice un usuario en el sistema.

En este proyecto se resguardarán los principios básicos la seguridad de la información implementando técnicas y metodologías como son el cifrado de datos sensibles, acceso al sistema únicamente por medio de un usuario y contraseña, manteniendo la trazabilidad de los procesos y acciones que realice el usuario dentro del sistema entre otros.

C. Cifrado de Credenciales

El cifrado de credenciales se realizará por medio de un algoritmo de cifrado hash como SHA 2 con la diferencia que la contraseña no se almacena en la base de datos, esta solo existe para realizar comparaciones de autenticación, así si una persona con conocimientos en informática logra ingresar a nuestra base de datos no podrá utilizar las credenciales de acceso.

D. Log de Eventos

Para evitar el no repudio en nuestro sistema, se contará con un control de logs por cada acción que el usuario tome sobre la plataforma, aprovechando el control de log podemos contribuir a la auditoria y a la falsificación de información.

E. OWASP

El proyecto abierto de seguridad en las aplicaciones web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a solicitar que las diferentes organizaciones estatales o privadas desarrollen, adquieran y mantengan aplicaciones y APIs confiables. Esta institución define la seguridad en aplicaciones como un problema el cual es transversal a los procesos, tecnología y personas debido a que los enfoques más contundentes en cuanto a temas de seguridad deben comenzar con el fortalecimiento de estas [13]. Con base a los seguimientos que la fundación owasp realiza a las diferentes vulnerabilidades reportadas en todo el mundo ellos realizan una publicación donde las clasifican dándoles top con base a su nivel de incidencia e impacto, en este documento se describe cada vulnerabilidad con su descripción, forma de prevenirla y ejemplos en escenarios de ataque. La última publicación la realizaron en el año 2017 donde se exponen las 10 principales vulnerabilidades. Este top 10 es muy utilizado como lista de chequeo en las pruebas que realizan compañías auditoras de seguridad.

La versión de owasp 2017 fue todo un reto para los colaboradores de la fundación ya que rescribieron todas las vulnerabilidades de su antigua versión y más aun asumiendo retos con las nuevas tecnologías ya que la evolución en tecnología de desarrollo en 4 años avanzo a pasos agigantados el evaluar los nuevos frameworks, las nuevas tecnologías para acceso a la información como son los microservicios, los servicios resfull tecnologías que son la tendencia del momento.

Los diez riesgos más críticos en las aplicaciones web:

- A1 Inyección: una inyección de código SQL, NoSQL, LDAP, XPath entre otros pueden causar una divulgación de información sensible para la organización.
- A2 Perdida de autenticación: este tipo de ataque permite al atacante que con una credencial de acceso al sistema penetrarlo sin causar ruido a los sistemas de alerta esta técnica es silenciosa, al igual existe otra técnica que es un poco más ruidosa y es la implementación de fuerza bruta la cual consiste en tener un sin número de contraseñas y de manera persistente tratar de penetrar al sistema.
- A3 Exposición de datos sensibles: En las organizaciones es muy habitual que los usuarios no recuerden sus contraseñas y como medida optan por guárdalas en block de notas o un papelito debajo del monitor, este tipo de descuidos son utilizados por el atacante para lograr su cometido.
- A4 Entidades externas XML (XML): estos son defectos de procesadores antiguos donde el atacante utiliza una técnica de negación de servicio para realizar un desbordamiento para acceder a datos grabados en memoria.
- A5 Perdida de control de acceso: la falta de controles que permitan la validación de credenciales de acceso al sistema da una mayor facilidad para que el atacante pueda utilizarla y acceder sin que el usuario se percate.
- A6 Configuración de seguridad incorrecta: Es habitual que al momento de configurar archivos claves para el arranque de una aplicación no conozcamos la mejor forma de hacerlo o la configuración más optima y optamos por mantener la configuración por defecto dejando una brecha de seguridad a favor del atacante.
- A7 Cross-site Scripting (XSS): Es la ejecución de comandos en el DOM del navegador para explorar variables o cookies que revelen información sensible del usuario.
- A8 Deserialización insegura: La utilización de algoritmos de cifrado inseguro permiten al atacante poder acceder a datos cifrados explotando estas vulnerabilidades.
- A9 Uso de componentes con vulnerabilidades conocidas: En la web surgen a diario nuevos frameworks que prometen ser eficientes y mejores los cuales carecen de una muy buena documentación y más aun sin una comunidad fuerte que permita el crecimiento de estos. Es muy recomendable en estos casos verificar el número de personas que hacen parte de la comunidad que apoyan el framework.
- A10 Registro y monitoreo insuficientes: los atacantes aprovechan la falta de monitoreo y de respuesta oportuna para logar sus objetivos sin ser detectados [13].

VI.Bases legales de la investigación

A. *LEY 1273 DE 2009*

En Colombia, El Congreso de la República aprobó la ley 1273 de 2009, sobre los delitos informáticos. Esta ley básicamente introduce un ajuste al código penal colombiano en cuanto a la protección de la información y de los datos impone penas de prisión de hasta 120 meses y multas hasta por 1500 salarios mínimos legales mensuales legales vigentes.

Los delitos tipificados en esta ley son los siguientes:

1. Acceso abusivo a un sistema informático.
2. Obstaculización ilegitima de un sistema informático o red de telecomunicación
3. Interceptación de datos informáticos
4. Daño informático
5. Uso de software malicioso
6. Violación de datos personales
7. Suplantación de sitios web para capturar datos personales
8. Hurto por medios informáticos y semejantes
9. Transferencia no consentida de activos

CAPITULO III

DISEÑO METODOLÓGICO

Se abordó en cuatro fases. Las tres primeras corresponden específicamente al diseño de la plataforma y la cuarta fase hace relación a la prueba de funcionamiento de esta:

Fase 1: Estructuración de la base de datos: en 5 sesiones, para un total de 20 horas, donde se definieron entidades para la clasificación de la información, los procesos de almacenamiento de la información, hasta obtener el modelo de base de datos con la que se construyó la plataforma.

Fase 2: Desarrollo el back-end: En esta etapa se construyó la lógica de negocio e interfaces que dan alcance a los requerimientos de la aplicación donde la información se expone por medio de servicios rest al cliente, esta fase tuvo un costo en tiempo de 32 horas.

Fase 3: Desarrollo del front-end: El diseño de la aplicación implementa el concepto de **mobile first** por medio de la plantilla bootstrap la cual permite crear vistas para dispositivos móviles, tableas y posteriormente acoplarlos a pantallas de ordenadores, la renderización de pantallas se realiza utilizando framework radioactivos como vue.js el cual trabaja con programación modular bajo el del patrón observador.

Fase4: Implementación prueba piloto: para la prueba piloto de uso de la plataforma, se seleccionó un grupo de 20 estudiantes de Ingeniería de Sistemas de décimo semestre, de los cuales 14 participaron de la misma.

VII.Tipo de investigación

Consideramos que el presente trabajo de investigación corresponde a una investigación aplicada en función del contexto formativo de los estudiantes de ingeniería de sistemas de la Fundación Universitaria San Mateo, que responde a la necesidad de tener una herramienta de entrenamiento (plataforma) en el área de seguridad informática, que a su vez incentive en los estudiantes un ejercicio de competencia sana, que les permita cotejar sus conocimientos y habilidades con sus compañeros.

VIII.Población

Estudiantes de decimo semestre del programa de ingeniería y afines de la Fundación Universitaria San Mateo.

IX.Técnicas e instrumentos de recolección de datos

Para la construcción de la plataforma pedagógica en seguridad informática, se aprovechó el conocimiento, habilidades, prácticas y experiencia con otro tipo de plataformas, producto de la formación académica y profesional durante los 10 semestres en la Fundación Universitaria San Mateo.

En la prueba piloto de la plataforma participaron el 70% de los estudiantes 14 de 20 invitados a la realización del ejercicio

Los estudiantes se enfrentaron a diferentes retos en las siguientes categorías:

1- Lógica
2- Cracked
3- Análisis web
4- Sistemas operativos
5- Estenografía

CAPITULO III

RESULTADOS DE LA INVESTIGACIÓN

X.Resultados del objetivo específico no. 1

El modelo relacional aportado al proyecto de investigación cumple con cada característica con la que la plataforma contara permitiendo un ágil desarrollo y fácil acceso a los datos, el diseño relacional aportado para el proyecto cumple con todas las normas de normalización de base de datos relacionales y conserva una sintaxis que permite su fácil lectura.

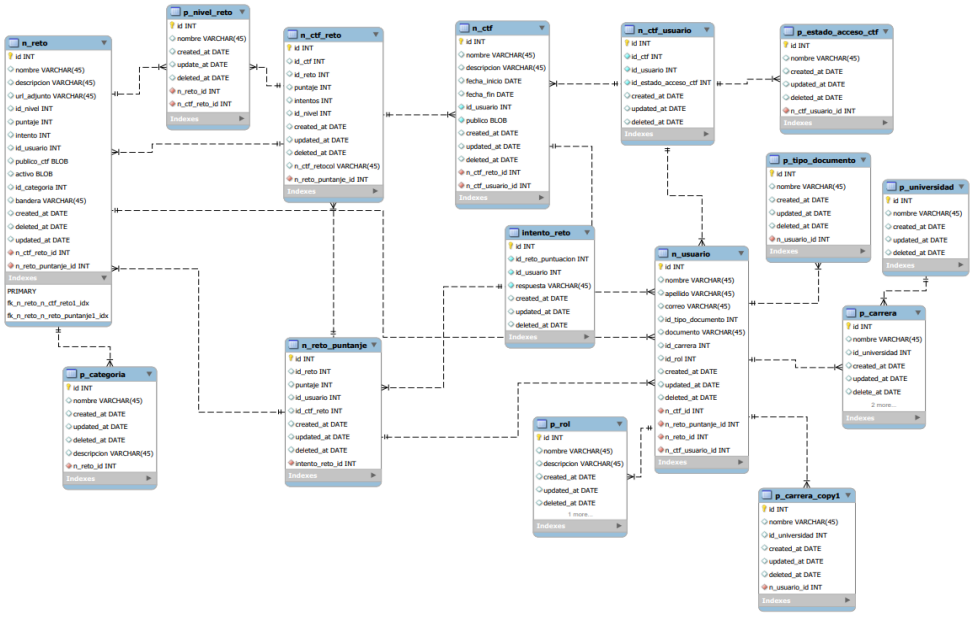

Fig. 1 Modelo de base de datos de la aplicación donde se visualiza la estructura y relación entre tablas.
Fuente propia.

XI.Resultados del objetivo específico no. 2

A nivel de manejo de datos se desarrolló una arquitectura MVC dada por los siguientes componentes

- Common : Administra las funcionalidades que son comunes en todas las vistas del proyecto back end.
- Config : Archivo de configuración que se ejecuta al iniciar el Spring Boot dando cualidades específicas al usuario final como el manejo de webtoken o configuración de servicios rest
- Controller : Esta es la vista de los servicios rest en el modelo MVC, con ella es que interactúa la aplicación Front End, en este paquete se encuentran todas las funcionalidades que la herramienta puede manejar con el fin de garantizar una navegacion fluida de los datos.
- Entities : Package correspondiente a administrar todos los objetos que se utilizaran en el manejo de datos, una cualidad importante en este paquete es que la base de datos se mapea (DDL) administrando de mejor manera las conexiones concurrentes a la base de datos
- Exceptions : En este package se encuentras archivos que dan control a las posibles fallas que el sistema puede encontrar garantizando que cada exception se administre de forma personalizada.
- Repository : En este sitio se administra todas las conexiones y consultas sobre la base de datos (DML), al utilizar persistencia de datos con Spring Boot no es necesario crear nosotros mismo los scripts de manejo de datos, estos scripts los crea el ORM que en este caso es Hibernate con el cual el manejo de la información es un poco más fluida y permite concentrarse más en la capa de negocio
- Services : Los servicios aprovechan las interfaz aportada por los repositorios para dar cara a los controladores que son quienes dan la información al usuario final.
- Utilities : Este package maneja todas aquellas funcionalidades que son aprovechadas en diferentes momentos por diferentes clases, un ejemplo claro de esta función puede ser la validación de un campo null o el saber si un número es mayor a otro, volver un texto a mayúscula, obtener la fecha del sistema entre otros.

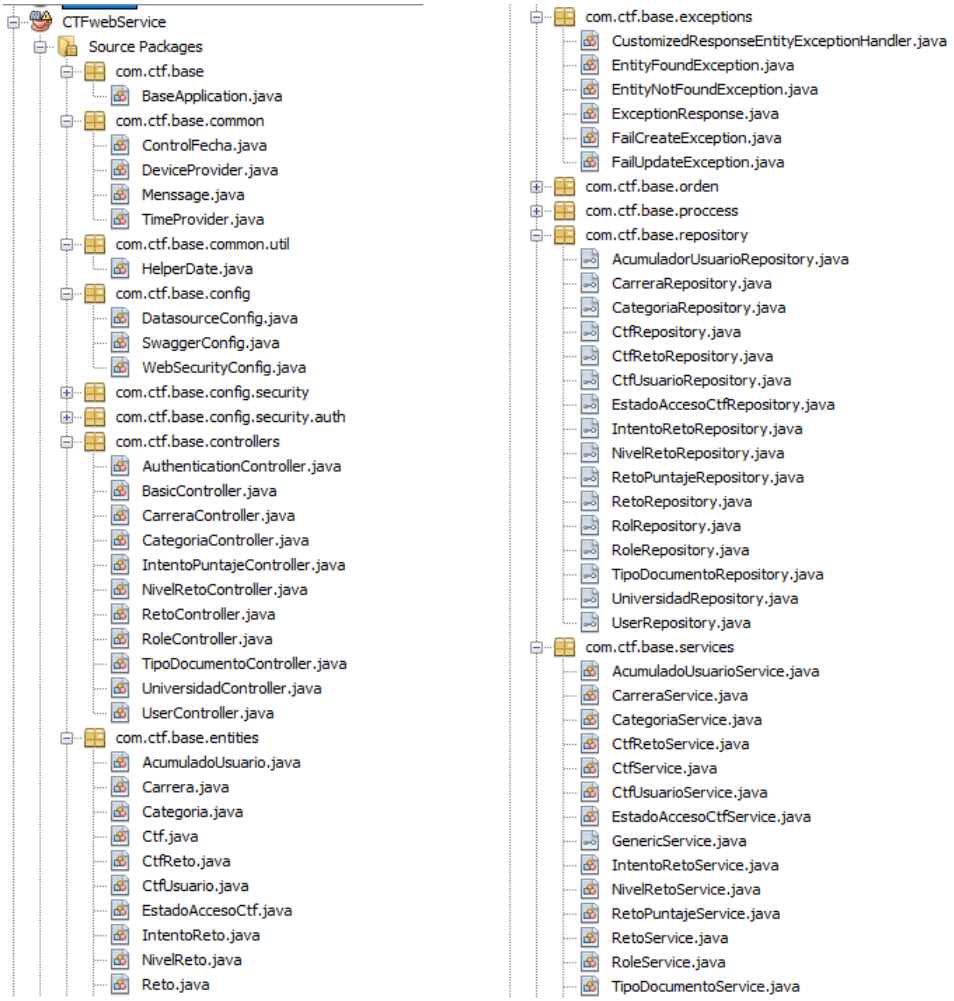

Fig. 2 Arquitectura en capas que contiene la lógica de negocio de la aplicación.

XII.Resultados del objetivo específico no. 3

La construcción de la interfaz gráfica se llevó acabo realizando inicialmente los diseños en papel para evaluar las posiciones y dimensiones de los formularios que se emplearon, posteriormente se realizó la maquetación implementando framework responsivos como lo es Bootstrap.

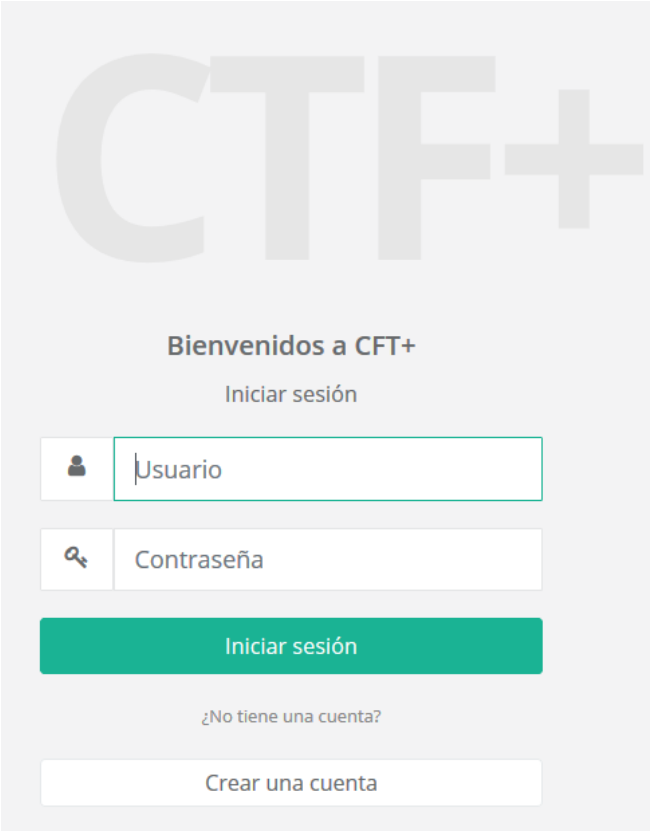

Fig. 3 Imagen del módulo de login de la plataforma visualizado desde un navegador web.

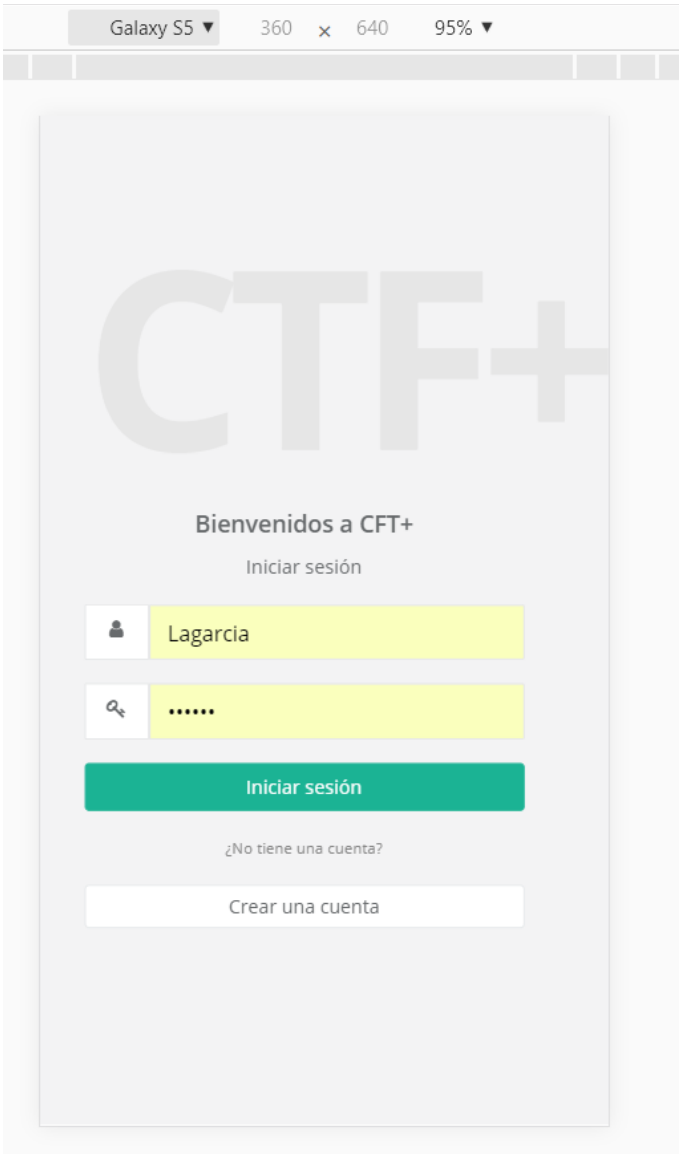

Fig. 4 Modulo de login de acceso a la plataforma, visualizado desde un emulador de dispositivo móvil.

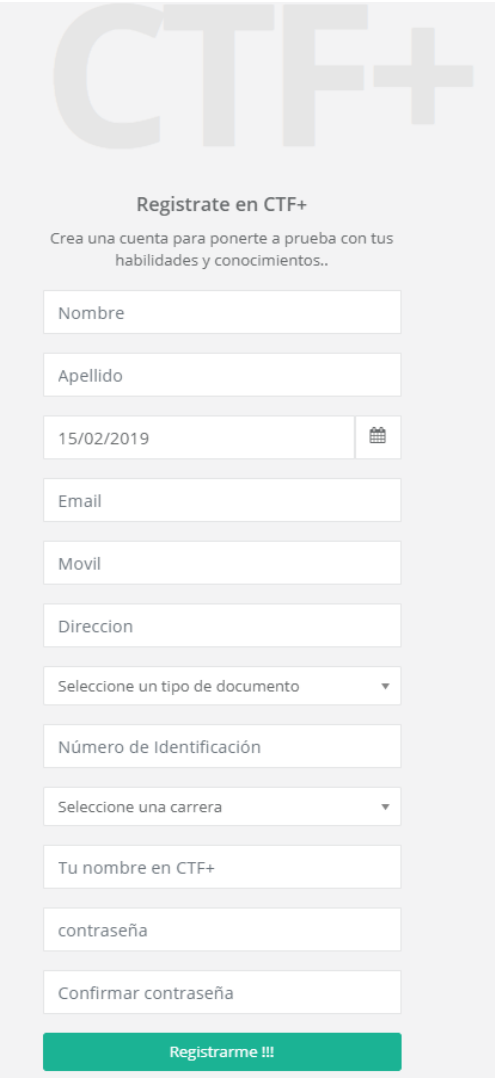

Fig. 5 Modulo de registro de usuario

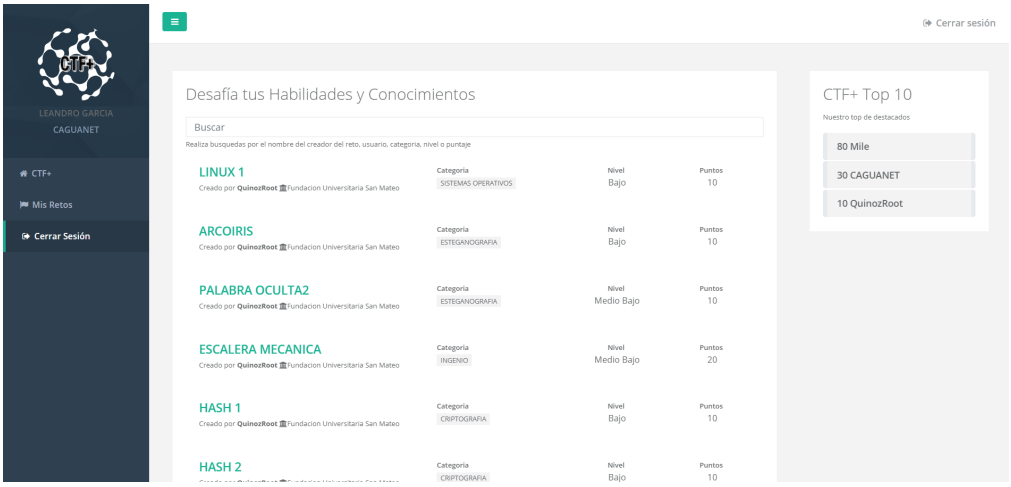

Fig. 6 Visualización de retos en módulo principal.

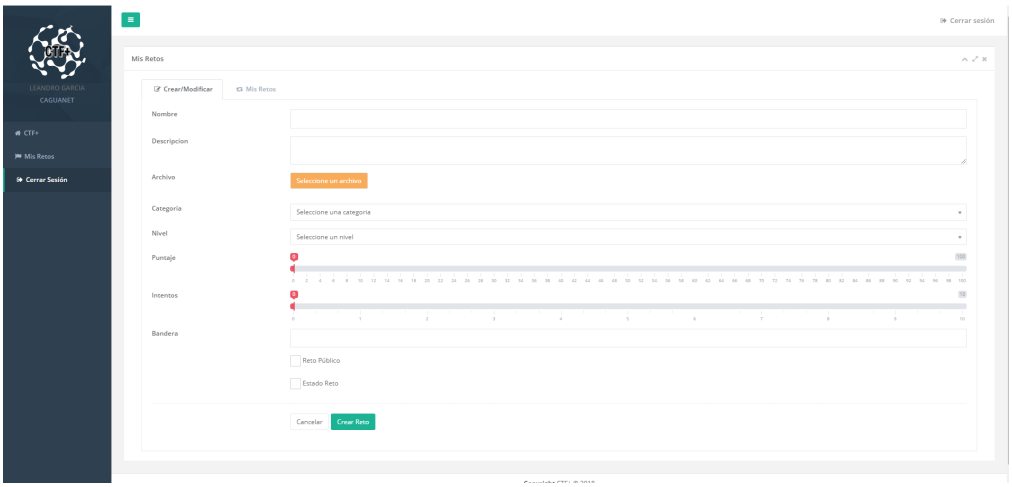

Fig. 7 Módulo de creación de retos.

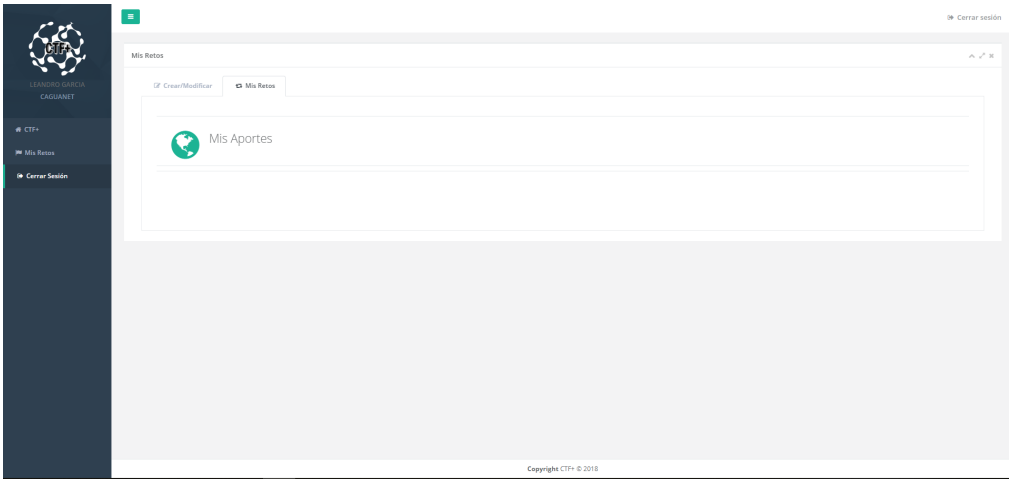

Fig. 8 Visualización de los aportes o retos creados por el usuario en la plataforma.

XIII.Resultados del objetivo específico no. 4

Se realizaron pruebas con un grupo de estudiantes de X semestre de Ingeniería en Sistemas de la jornada nocturna, en la prueba participaron 19 de los 20 estudiantes que se encontraban en la lista, en las pruebas se habló sobre la plataforma, se contó el tipo de pruebas que podían realizar en ella y se realizó pruebas de funcionalidad, se realizó una en cuentas apoyándonos en Google Forms y se obtuvieron los siguientes resultados a las preguntas presentadas en la misma, pueden encontrar el formulario en la url https://docs.google.com/forms/d/1u_tpWQDCxocNi39TTAyA2Qpl38QXUvD68nG-srJXZNk/prefill

¿A cual carrera pertenece?

19 respuestas

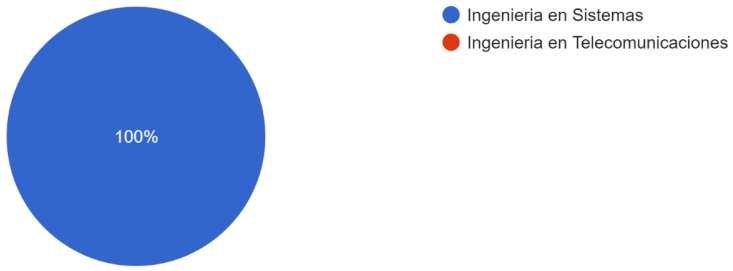

Fig. 9 Primer pregunta realizada en la encuentra, donde el 100% de los encuestados pertenecen a la carrera de ingeniería de sistemas.

¿La plataforma cuenta con una fácil navegación?

19 respuestas

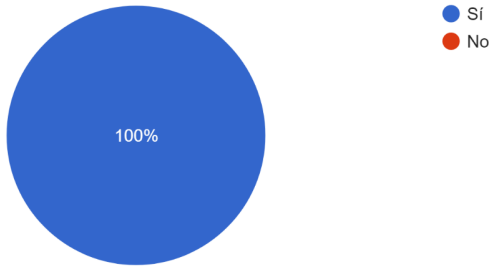

Fig. 10 Segunda pregunta realizada en la encuesta en donde el 100% de los encuestados respondieron que la plataforma cuenta con una fácil navegación.

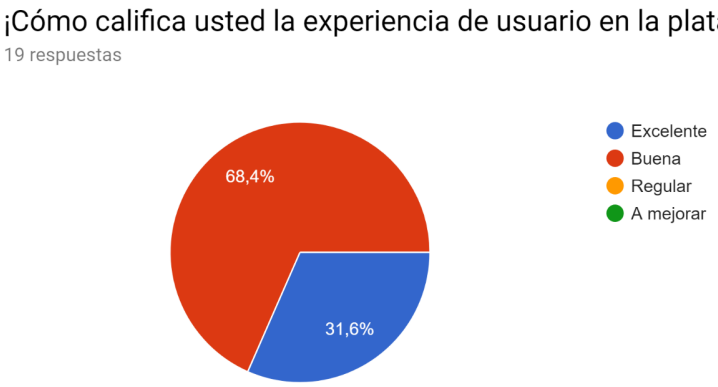

Fig. 11 Tercer pregunta realizada en la encuesta, en donde el 71,4% califica la plataforma como buena.

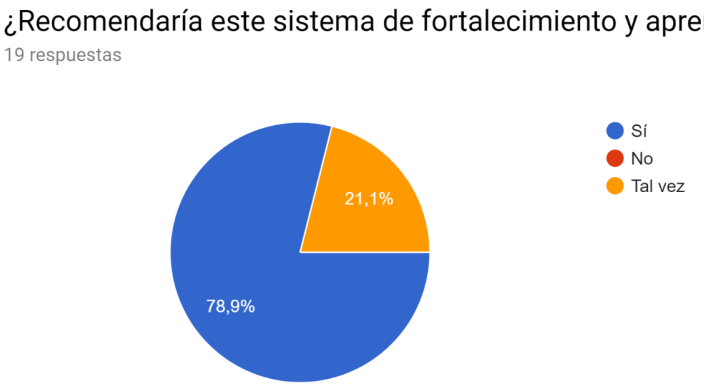

Fig. 12 Cuarta pregunta realizada en la encuesta, en donde el 85.7% recomendaría la plataforma con un sistema de fortalecimiento y aprendizaje.

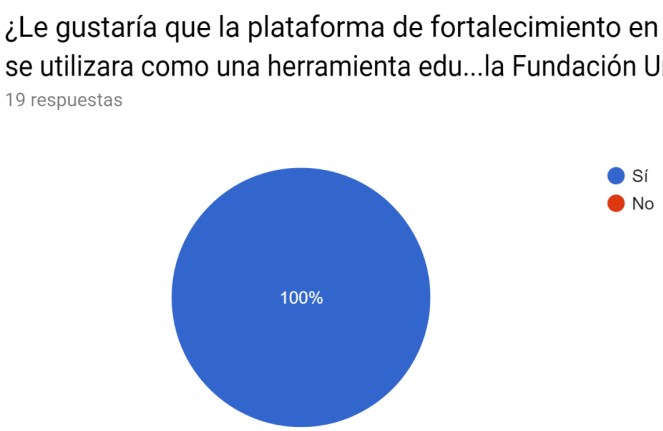

Fig. 13 Quinta pregunta realizada en la encuesta, en donde la totalidad de los encuestados les gustaría una plataforma de fortalecimiento en seguridad informática en la institución.

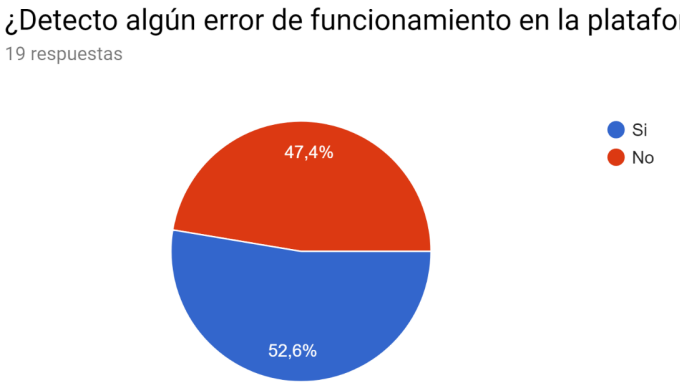

Fig. 14 Sexta pregunta realizada en la encuesta, en donde el 47.4% de los encuestados detectaron algún error de funcionamiento de la plataforma.

¿El cargue de archivos presenta inconvenientes?

19 respuestas

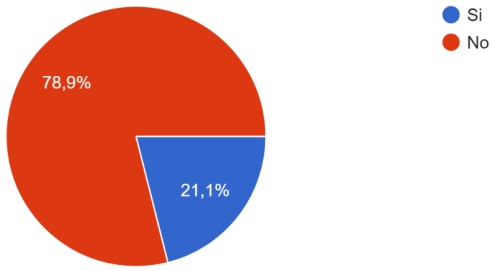

Fig. 15 Séptima pregunta realizada en la encuesta, en donde el 78.9% de la población encuestada no tuvieron inconvenientes al cargar el archivo a la plataforma.

La barra de búsqueda de la página principal filtra los registros de acuerdo a los parámetros brindados.

19 respuestas

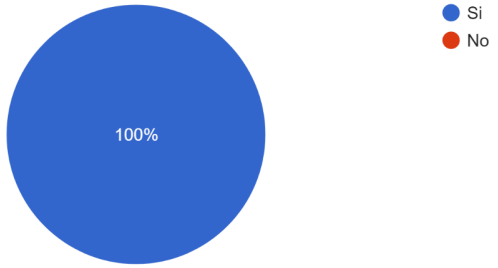

Fig. 16 Octava pregunta realizada en la encuesta, en donde la totalidad de los encuestados obtuvieron los resultados esperados el filtrar la información en la barra de búsqueda.

CAPÍTULO V.

CONCLUSIONES Y RECOMENDACIONES

El desarrollo de la plataforma en seguridad informática requiere el tener conocimientos sólidos y claros en seguridad informática como también requiere un muy buen nivel en programación (JAVA, .NET, C#, ANGULAR JS, VUE.JS).
El tomar como ejemplo las plataformas que hoy en día están en producción como puede ser YASHIRA o CTFChangerd es de gran ayuda ya que permite aclarar el concepto de lo que se quiere realizar.

En cuanto a la plataforma desarrollada en este documento de investigación, se quiso que los mismos usuario pudieran crear los retos y que entre sus mismo compañeros los pudieran resolver, se encontró que esto no puede ser del todo posible ya que esto abre la puerta a posible fraudes en la toma de puntaje y dificulta el poder medir el nivel de cada usuario correctamente, se decide que los usuarios crean retos pero el reto tiene que pasar a verificación de un administrador de contenido el cual aprueba o rechaza el reto según las indicaciones entregadas por el usuario que lo solicita, esto puede no garantizar al 100% el resultado de los puntajes de cada reto pero si atrasa y garantiza que no pueden haber fraudes en competiciones.

Al grupo de investigación o a la persona que desee continuar en este asombroso mundo de la seguridad informática le recomendamos empaparse bien del tema antes de querer modificar o anexar nuevas funcionalidades en la plataforma, el trabajo que puede continuar sobre el proyecto de investigación puede ser el anexo de una red física para realizar pruebas de penetración a sitio web reales, ataques de inyección SQL a sitios reales controlados en nuestra red, el uso de una VPN para garantizar la conexión y con nuevos tipos de pruebas como las puede brindar IoT

BIBLIOGRAFÍA

[1] A. Dabrowski, M. Kammerstetter, E. Thamm, E. Weippl y W. Kastner, «https://www.usenix.org,» 2015. [En línea]. Available: https://www.usenix.org/system/files/conference/3gse15/3gse15-dabrowski.pdf. [Último acceso: 28 Agosto 2018].

[2] M. Carlisle, M. Chiaramonte y D. Caswell, «Using CTFs for an Undergraduate Cyber Education,» 2015 . [En línea]. Available: https://www.usenix.org/system/files/conference/3gse15/3gse15-carlisle.pdf. [Último acceso: 28 Agosto 2018].

[3] T. Chothia y C. Novakovic, «An Offline Capture The Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education,» 2015. [En línea]. Available: https://www.usenix.org/system/files/conference/3gse15/3gse15-chothia.pdf. [Último acceso: 26 Agosto 2018].

[4] A. Dabrowski, M. Kammerstetter, E. Thamm, E. Weippl y W. Kastner, «Learning Obstacles in the Capture The Flag Model,» 2014. [En línea]. Available: https://www.usenix.org/system/files/conference/3gse15/3gse15-dabrowski.pdf. [Último acceso: 26 Agosto 2018].

[5] A. Davis , T. Leek, M. Zhivich, K. Gwinnup y W. Leonard, «The fun and future,» 2014. [En línea]. Available: https://www.usenix.org/system/files/conference/3gse14/3gse14-davis.pdf. [Último acceso: 27 Agosto 2018].

[6] G. Vigna, K. Borgolte, J. Corbetta, A. Doupe, Y. Fratantonio, L. Invernizzi, D. Kirat y. Shoshitaishvili, «www.usenix.org,» 2014. [En línea]. Available: https://www.usenix.org/system/files/conference/3gse14/3gse14-vigna.pdf. [Último acceso: 27 Agosto 2018].

[7] O. Tsai, «blog.orange,» Orange Tsai, 26 Agosto 2014. [En línea]. Available: http://blog.orange.tw/2014/08/hitcon-win-2nd-in-defcon-22-ctf-final.html. [Último acceso: 26 Agosto 2018].

[8] Jeffxx , «Jeffxx.com,» Jeffxx Blog, 13 Agosto 2014. [En línea]. Available: http://www.jeffxx.com/blog/2014/08/13/2014-defcon-22-final-can-sai-xin-de-shang/. [Último acceso: 27 Agosto 2018].

[9] chengtc , «Ddaa.logdown.com,» Ddaa.logdown.com, 13 Agosto 2014. [En línea]. Available: http://ddaa.logdown.com/posts/220500-defcon-22-ctf-diaries. [Último acceso: 27 Agosto 2018].

[10] . A. Knowles, «Security Intelligence,» IBM, 8 Diciembre 2016. [En línea]. Available: https://securityintelligence.com/behind-the-scenes-at-a-capture-the-flag-ctf-competition/. [Último acceso: 3

Septiembre 2018].

[11] C. team, «ctftime,» ctftime, 12 Septiembre 2015. [En línea]. Available: https://ctftime.org/ctf-wtf/. [Último acceso: 6 Septiembre 2018].

[12] OWASP, «owasp.org,» 2017. [En línea]. Available: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf. [Último acceso: 5 Septiembre 2018].