TRABAJO DE GRADO

PROPUESTA DE UNA PLATAFORMA WEB DE RETOS TIPO HACKING ÉTICO PARA LA UNIVERSIDAD CATÓLICA DE COLOMBIA, DONDE EL CONTENIDO SEA CREADO POR LOS PROPIOS INTEGRANTES

INTEGRANTES

JOHN FREDY PEREZ JIMENEZ

YULIET STEPHANY RUIZ BENAVIDES

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020
1

TRABAJO DE GRADO

PROPUESTA DE UNA PLATAFORMA WEB DE RETOS TIPO HACKING ETICO PARA LA UNIVERSIDAD CATOLICA DE COLOMBIA, DONDE EL CONTENIDO SEA CREADO POR LOS PROPIOS INTEGRANTES

JOHN FREDY PEREZ JIMENEZ

YULIET STEPHANY RUIZ BENEVIDES

Trabajo de grado presentado para optar al título de Especialista en Seguridad de la Información

Docente

DIEGO OSORIO REINA
Magister en Seguridad de las Tecnologías de la Información y las Comunicaciones

UNIVERSIDAD CATÓLICA DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN

BOGOTÁ D.C

2020

DEDICATORIA

El presente proyecto está dedicado a Dios por ser quien me ha guiado y me ha dado la fortaleza de seguir adelante, ya que gracias a él he logrado culminar mi especialización, a mi esposa y a mi hijo por sus palabras de aliento, amor, comprensión, apoyo, también por su sacrificio al brindarme el tiempo necesario para realizarme profesionalmente y por ser mi mayor motivación para nunca rendirme en los estudios y poder llegar a ser un ejemplo para ellos, a mis padres por su mejor trabajo y sacrificio en todos estos años y a mis hermanos, al Ingeniero Diego Osorio Reina por su confianza y dedicación hacia nosotros sus estudiantes, y todas aquellas personas que de una u otra manera han contribuido para alcanzar mis objetivos.

John Fredy Pérez Jiménez

Quiero dedicar este proyecto de grado primero a Dios que me ha dado la vida y fortaleza para terminar este trabajo, a SIETE24 por la confianza y la oportunidad de culminar otro logro en mi vida, a mi esposo por apoyarme en cada momento que lo he necesitado, a mi hija que me acompaño cada segundo de esta especialización hasta su nacimiento y ahora está junto a mí, siendo mi motor para salir adelante y luchar por ella, a mi mamá que siempre ha estado ahí en los momentos más difíciles dándome constantemente su comprensión y amor infinito, a mi papá que está en el cielo mirándome orgullosamente, a mi abuelita que me ha acompañado toda su vida y a mis hermanos, al Ingeniero Diego Osorio Reina porque siempre con su conocimiento y confianza en cada uno de nosotros mostró su apoyo incondicional y a todos mis compañeros de la Especialización de Seguridad de la Información que han sido el centro de este nuevo reto… Cada una de estas personas antes mencionadas puso su grano de arena en mi vida contribuyendo incondicionalmente para lograr una de mis metas y objetivos propuestos para este nuevo proceso.

Yuliet Stephany Ruiz Benavides

Queremos darle gracias a Dios por permitirnos estar aquí, por habernos acompañado a lo largo de nuestra especialización, por ser nuestro guía y fortaleza en los momentos de debilidad.

Agradecemos a la Universidad Católica de Colombia por brindarnos los medios para la culminación de este nuevo ciclo, a los docentes por la disposición, el seguimiento y la verificación continua de la misma, pero sobre todo por la enseñanza y el apoyo recibido a lo largo de este año, a nuestros padres, hermanos e hijos por estar ahí apoyándonos en todo momento.

A todos Muchas Gracias

TABLA DE CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

1. INTRODUCCIÓN

La ciberseguridad es una parte de la seguridad de la información que se enfoca en la protección de los activos de información del ciberespacio, al preocuparse por las amenazas a la información que se procesa, almacena y transporta a través de los sistemas de información que trabajan sobre la Internet. [1]

El presente proyecto de Grado está motivado por una necesidad dentro del ámbito estudiantil de reforzar y adquirir conocimientos, sobre las diferentes herramientas, técnicas y métodos existentes y actuales empleados en la disciplina de Hacking Ético, de forma adicional a las brindadas por la Universidad dentro de la malla curricular.

El hacking ético es una disciplina dentro de la informática, que permite a través de pruebas de penetración, buscar vulnerabilidades dentro de los sistemas informáticos, redes y dispositivos electrónicos. El nivel de especialización de esta disciplina cada vez es mayor, debido a las diferentes ramas tecnológicas, ya que las nuevas tecnologías emergen o cambian de un momento a otro, y esto permite abrir una brecha a las vulnerabilidades de dicha tecnología.

A pesar de que existen numerosos recursos en internet acerca de Hacking Ético, incluso de hacking a nivel general, estos no se encuentran centralizados, no están en español, en algunos casos desactualizados o sin veracidad de la información, muchos de estos recursos no siguen una línea educativa, ni una trazabilidad lógica, por lo que no son apropiados debido al nivel de complejidad. Además una de las barreras para los estudiantes, profesionales y egresados de carreras a fines en nuestro país es la fluidez en el idioma inglés, recalcando que la mayoría de recursos y sitios web se encuentran en dicho idioma, dejando de un lado la posible vinculación a sitios tales como HACKER 101 (es una plataforma para hackers con un esquema legal permitiendo que los involucrados reciban recompensas al encontrar vulnerabilidades a diferentes empresas), también hay otras como se mencionan en la encuesta del presente proyecto.

Por ende, en este trabajo presentamos una propuesta que pretende no solo reforzar los procesos de conocimiento, capacitación y dominio de los temas, previamente otorgados por los docentes de la universidad, sino además de las herramientas y tecnologías más usadas en la disciplina del hacking ético, a través de la practica constante y del involucramiento activo en las actividades propuestas en el laboratorio.

El objetivo del laboratorio de retos informáticos se basa en la construcción de conocimiento y competencias por medio de un espacio compartido que permita albergar a estudiantes con los mismos intereses en el cual se creen sinergias que conlleven a desafiar al estudiante para que piense de manera diferente y se enfrente

a situaciones que se pueden presentar en el ámbito profesional, que logre ubicar dichas falencias en los programas, que descubra las metodologías de ataque y se prepare de una manera más integral y práctica, todo ello por medio de diferentes simulaciones en eternos prácticos y controlados, dentro del cual se usarían diferentes metodologías, así como la identificación y uso de algunas de las fases del ethical Hacking.

Con el tiempo se busca que el laboratorio sea una ayuda y una oportunidad de mejora para el encuentro de los diferentes integrantes, permitiendo que la herramienta eleve las competencias en hacking ético de los integrantes y de forma adicional ayude en la preparación de exámenes de certificación de entes reconocidos en la materia.

Para la actual sociedad es crítico y vital que más profesionales remedien la actual brecha de expertos en la temática, permitiendo así elevar el nivel de protección de los individuos y las organizaciones.

2. GENERALIDADES

2.1 LÍNEA DE INVESTIGACIÓN

Siendo estudiantes de la Especialización en Seguridad de la Información, usaremos la Línea de Investigación llamada: Software Inteligente y Convergencia Tecnológica.

2.2 PLANTEAMIENTO DEL PROBLEMA

Las evoluciones tecnológicas, conllevan cambios no solo a nivel de infraestructura, equipos de seguridad, políticas y/o procedimientos, sino, además, de personal calificado, profesionales en el área de informática responsables de crear, modificar, lanzar y evaluar dichos sistemas informáticos, profesionales capaces de detectar falencias, errores de programación y puntos débiles que requieran medidas para evitar pérdidas de información, por medio de acciones preventivas y correctivas.

Según el Consorcio Internacional de certificación de Seguridad de Sistemas de Información (ISC²), la escasez de la fuerza de trabajo en materia de seguridad cibernética a nivel mundial sigue siendo un problema para las empresas de todas las industrias y de todos los tamaños. De hecho, esta escasez sigue siendo la principal preocupación laboral para los que trabajan en el campo. Esto no es sorprendente ya que 2018 fue “el año de la Mega Brecha”. Las ciudades se están viendo muy afectadas por los rescates y los ataques de malware móvil se han duplicado. Actualmente se conoce que la fuerza de trabajo de la ciberseguridad global necesita crecer en un 145% para satisfacer la demanda de talento cualificado en materia de Ciberseguridad. [2]

Solo en Colombia en el último reporte del Estudio de Escasez de Talento 2020 [3], de la compañía Manpower, sitúa el rol de Ciberseguridad dentro de los 10 más demandados a nivel Nacional, La principal causa que está generando dicha cifra y que ha sido una constante es la falta de experiencia por lo cual no se encuentra el personal adecuado. (Javier Echeverri, presidente Manpower) [4]

En la mayoría de los casos los profesionales con apetito de esta disciplina se instruyen por medio de la lectura, libros, ensayos, video tutoriales, proporcionando un nivel de madurez sobre lo teórico pero sin oportunidad de aplicar esto en entornos prácticos, ya que las plataformas actuales como cursos, diplomados y certificaciones tienen un costo que en la mayoría de ocasiones es muy elevado, impidiendo a la mayoría de la población de estudiantes acceder a ellos, sin mencionar que muchas de las plataformas no están en español, sumando una problemática adicional a las ya mencionadas anteriormente, tomando como una de las bases de la teoría de aprendizaje experiencial, la cual nos dice que no es suficiente aprender nuevos conceptos, estos deben ser probados en nuevas situaciones, que permitan al estudiante hacer el vínculo entre teoría y práctica, debe

planearse una acción, llevarse a cabo y luego reflexionar sobre ello y comparar nuevamente con la teoría dada [5]; sin la experiencia y la reflexión lo que se aprendió puede ser rápidamente olvidado. Desde esta perspectiva, como lo expresa Gómez Pawelek “el aprendizaje es el proceso por medio del cual construimos conocimiento mediante un proceso de reflexión y de dar sentido a las experiencias” [6]. Existen varios modelos cíclicos que explican cómo aprendemos desde la experiencia, pero todos comparten características importantes del modelo de Kolb. El aprendizaje experiencial está compuesto por 4 etapas que se siguen una a la otra en un ciclo [7], ver figura 1.

Ilustración 1 Ciclo de Kolb
Fuente: http://biblioteca.galileo.edu/tesario/handle/123456789/778

En internet se puede encontrar diferentes recursos para la preparación autónoma en diferentes temas, como por ejemplo Udemy (es una plataforma de aprendizaje en línea, enfocada para adultos profesionales, que permite el mejoramiento de habilidades y practica de las mismas, otorgando en algunos casos una certificación técnica de los cursos realizados) sin embargo a pesar de que en el mercado se encuentran estas plataformas, no existe una hoja de ruta para adquirir este tipo de conocimientos.

Por otro lado, existen academias para la formación de estudiantes – profesionales, otorgando recompensas por labores realizadas, sin embargo, una de las limitaciones es el miedo a enfrentarse con el propio conocimiento, puesto que muchos(as) no se sienten preparados para ejercer con los conocimientos previos, en algunas ocasiones el profesional se siente limitado y no da continuación, y en

muy pocos casos utilizan este mecanismo de autoaprendizaje especializado.
Partiendo de esta teoría, la práctica de algunos profesionales es realizar intentos de intrusión a páginas y aplicaciones que se encuentran en internet, esto con el fin de medir sus capacidades pero obviando la implicación legal que esto puede tener, como por ejemplo la Ley 1273 de 2009 Ley de Delitos Informáticos en Colombia [8], la cual estipula de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, o la reciente política de Seguridad Digital CONPES 3854 de 2016, en la cual se establece una política de seguridad y defensa contra posibles ataques digitales a las entidades del Estado [9], debido a esto se plantea mitigar esta problemática por medio de un ambiente virtual y controlado, que permita al estudiante ejecutar actividades de hacking, sin incurrir en actividades delincuenciales, todo dentro de la norma ética.

2.2.1 ANTECEDENTES DEL PROBLEMA

Todos los países del mundo están entendiendo poco a poco que el rol del profesional de Ciberseguridad y hacking ético es un bien valioso para cada una de las regiones, tanto así que algunas grandes naciones han iniciado planes carrera y han incluido dentro de su presupuesto temas relacionados con ciberseguridad tanto para defensa como para educación, como es el caso de India, Ucrania, Rusia, estados unidos, entre otros; Estados unidos por ejemplo desde el año 2016 por medio del presidente Barack Obama, decreto la implementación del Plan de acción Nacional de Ciberseguridad, el cual implementa medidas a corto plazo y establece estrategias a largo plazo para mejorar la conciencia y la protección de la seguridad cibernética, proteger la privacidad, mantener la seguridad publica así como la seguridad económica y nacional [10]. Hoy en día en estados unidos existen múltiples programas de pregrado en ciberseguridad.

India siendo uno de los países pioneros y líderes en temas de ciberseguridad, implemento su política Nacional de Ciberseguridad desde el año 2013, planteando como objetivos principales, la creación de un centro nacional de protección de infraestructura de información crítica, el incentivo por promover la investigación y el desarrollo de vanguardia de la tecnología de seguridad cibernética y el desarrollo de recursos humanos a través de programas de educación y capacitación para desarrollar capacidades en ciberseguridad. [11]

En Latinoamérica tenemos países como México, Argentina y Chile, que dentro de sus universidades poseen carreras de ciberseguridad, con titulaciones como técnicos, licenciados e ingenieros.

En Colombia, la Corporación Universitaria Minuto de Dios es actualmente la única entidad universitaria que brinda un programa para tecnólogos referente al Hacking ético, el cual lleva por nombre Tecnología en Gestión de seguridad en redes de computadores [12], donde una de sus áreas va enfocada a la seguridad informática, promoviendo las asignaturas de Hacking Ético y gestión de seguridad informática,

Adicional a esta entidad para optar por una carrera en Ciberseguridad, Seguridad de la información/informática o de Hacking ético debemos aspirar a una especialización o maestría, ya que no se cuenta con plan carrera desde nuestro bachillerato o pregrado. Existen universidades que plantean un esquema de convenio con empresas y entes certificadores, como es el caso del Politécnico Gran Colombiano que en noviembre de 2019, firmo una alianza con Fortinet empresa líder en el sector de dispositivos Firewall y de seguridad de última Generación, Dicho convenio consiste en brindar entrenamientos en los cursos de Network Security Expert (NSE) y ofrecer acceso a la certificación internacional en Ciberseguridad, así como el Politécnico Gran Colombiano, este programa ya ha sido implementado en otras ciudades como Manizales, Cali y Medellín. [13]

Grandes empresas como Cisco están haciendo énfasis en el involucramiento de mujeres en Hacking Ético, y a su vez fabricantes de diferentes marcas y gremios apoyan e incentivan aún más este tema, como es el caso de una comunidad llamada Women Tech Network, que promueve la diversidad de género, en especial incentivando a la mujer a unirse a la tecnología, realizando eventos, entrevistas, conexión de talentos femeninos tecnológicos y así brindando la oportunidad de inclusión en diferentes áreas.

2.3 PREGUNTA DE INVESTIGACION

Entendiendo que el Hacking Ético es una disciplina con alta demandada corporativa que, sumado a la falta de competencias y habilidades en dicha temática de los aficionados, estudiantes y profesionales de seguridad de la información en Colombia, se permite plantear ¿cómo una plataforma de retos informáticos podría promover la adquisición y construcción de dichas competencias?

2.4 VARIABLES DEL PROBLEMA

- Se espera que con el diseño del laboratorio propuesto se logre aumentar las competencias prácticas en Hacking Ético.
- Aumentar el porcentaje de retención de estudiantes en la facultad de ingeniería, más precisamente en alumnos de Ingeniería de Sistemas, ingeniería de Telecomunicaciones y especialización en seguridad de la información.
- Apoyar a los docentes por medio de un espacio que contenga herramientas prácticas que permitan afianzar la adquisición de competencias referentes a hacking ético.

3. JUSTIFICACIÓN

El incremento en las tecnologías de la información y comunicación, la facilidad de acceso a servicios de internet, la curiosidad y la falta de plataformas prácticas que impidan que los usuarios infrinjan de manera voluntaria o involuntaria ley por querer realizar acciones prácticas de hacking.

Conociendo la necesidad y la actual brecha de profesionales capaces, con competencias técnicas y practicas sobre el Hacking Ético, un espacio dedicado para que puedan recurrir a realizar sus prácticas bajo un ambiente controlado permitirá no solo influir en el desarrollo profesional del estudiante, sino que este mismo será un aporte para la sociedad.

Para ello buscamos aportar a la solución por medio del desarrollo de un Diseño Web en la Universidad Católica de Colombia, en el cual se fomentaría la investigación por medio de nuevas metodologías, y retos informáticos, además de conocer y descubrir nuevas herramientas de Hacking ético que permitan alcanzar el logro dentro del reto, además de tener la oportunidad de educar y fomentar la cultura de seguridad sobre los futuros profesionales de la Universidad.

Este diseño de laboratorio permitirá capacitar por medio retos prácticos a los estudiantes de educación formal y continua de las diferentes carreras de ingeniería de la universidad católica de Colombia, aprovechando la totalidad de recursos disponibles de la plataforma.

Con las diferentes temáticas practicas del laboratorio web de hacking ético se estimulará al estudiante en la metodología de Aprendizaje Basado en Problemas (ABP), en donde se le permite desarrollar la capacidad del estudiante de resolver situaciones de la vida real a partir de la aplicación de funciones cognitivas, el desarrollo de actitudes y la apropiación del conocimiento. [14]

Este espacio impulsara a los estudiantes de pregrado, permitiendo involucrarse en las temáticas y orientándose por medio de la ruta de aprendizaje que permita en mayor capacidad ser productivo para el estudiante, incluso siendo este un bien valioso para los estudiantes de postgrado ya que al tener un espacio donde permitan promover y fortalecer sus conocimiento técnicos, tanto así, que se vea reflejado este espacio como el impulso para la consecución de certificaciones referentes al Ethical Hacking.

Justificamos nuestro proyecto como una necesidad de la comunidad de seguridad de la información colombiana y una oportunidad para abordar el requerimiento por parte de la universidad católica de Colombia.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Desarrollar una propuesta que permita por medio de una plataforma web, construir un ambiente controlado de aprendizaje a través de retos informáticos, que permita la autoalimentación del contenido por parte de los integrantes, para la UNIVERSIDAD CATOLICA DE COLOMBIA.

4.2 OBJETIVOS ESPECIFICOS

1. Definir el diseño adecuado del laboratorio web de retos hacking, con rutas claras de aprendizaje para los diferentes roles laborales de hacking ético.

2. Estructurar la metodología de los retos por medio de las diferentes ramas de especialidad del Hacking ético.

3. Diseñar la arquitectura técnica y tecnológica de la plataforma, soportada en virtualización.

4. Desarrollar una prueba de concepto de la implementación de la plataforma, alimentada con al menos un reto.

5. Diseñar un mecanismo de motivación en el aprendizaje a través de estatus y rankings a los participantes que logren superar los niveles, otorgando adicionalmente los permisos para alimentar la plataforma con un reto propio.

5 MARCOS DE REFERENCIA

Para entender un poco sobre los diferentes enfoques que puede tener la palabra Hacker o incluso la palabra Hacker ético, tomaremos algunas definiciones de profesionales e investigadores, como es el caso de Pekka Himanen, que en su libro La ética del hacker y el espíritu de la era de la información, que define a los hackers, a las personas que se dedican a programar de forma entusiasta y creen que poner en común la información constituye un extraordinario bien [15], Por otra parte Federico Gacharna, en su artículo llamado Mitos del hacking menciona que el hacking, ha sido confundido injustamente relacionado con ilícitos y los hackers confundidos con delincuentes, debido a diversos mitos que resultan equívocos, toda vez que ser hacker implica desarrollar un pensamiento diferente, y hacking, una actitud loable hacia la creación y el conocimiento compartido, en cualquier campo [16], por su parte Héctor Jara y Federico Pacheco**,** En su libro Ethical Hacking 2.0 definen la palabra hacker como un neologismo, que en informática se utiliza para referirse a un gran experto en alguna área de dominio. Si bien lo relacionamos más con los conocimientos técnicos e informáticos, es posible extender el concepto hacia otras disciplinas. De esta manera, definimos así a cualquiera persona a la que le apasiona el conocimiento, el descubrimiento, el aprendizaje y el funcionamiento de las cosas. [17]

Actualmente alrededor del mundo, se realizan diferentes actividades y conferencias con el fin de dar a conocer productos de Seguridad informática, actividades de hacking ético, charlas, incentivos, becas referentes a estudios de Hacking Ético y además se presentan famosos personajes catalogados como Hackers como es el caso de Kevin Mitnick, famoso por lograr penetrar sistemas de gran magnitud y grandes empresas como Nokia y Motorola, se cataloga como Ex-Hacker ya que en la actualidad se dedica a la consultoría desde la óptica particular de la ingeniería social. [18]

Un ejemplo de estas presentaciones es la Edición #2 de la Conferencia Internacional Sobre Ciencias Técnicas (ICTS2019) Realizada en la ciudad de Benghaz, Libya, la cual es una conferencia con expertos y es la segunda que acoge la Junta Nacional de Enseñanza Técnica y Profesional después de la primera conferencia que se celebró en 2018, que tuvo una aceptación muy amplia a nivel local e internacional y fue apoyada por muchos patrocinadores locales. [19]

En ella se realizó la conferencia llamada Enseñanza del Ethical Hacking: Evaluando los niveles de logros y motivaciones de los estudiantes, en la cual describen, que el Ethical Hacking o las pruebas de penetración es el acto de utilizar técnicas, habilidades y herramientas de piratería para descubrir vulnerabilidades y localizar debilidades de los sistemas de información. Se ha utilizado para obtener mejores profesionales de la seguridad que puedan protegerse a sí mismos y a su información personal de los ataques a la seguridad. Así pues, la enseñanza y la práctica de la piratería ética pueden considerarse un componente necesario de un programa de

estudios sobre seguridad informática y un método de enseñanza de técnicas defensivas. Sin embargo, hay una considerable escasez de documentos técnicos que describan la aplicación de técnicas de piratería ética para ejercicios prácticos de laboratorio que puedan llevarse a cabo en un entorno de laboratorio aislado, que se ajuste a limitaciones como los presupuestos y el espacio físico. en este documento se presenta el uso de la versión virtual de la plataforma de seguridad de cyBer basada en la nube (VIBRANT) para ejecutar ejercicios prácticos de piratería ética basados en escenarios. El análisis de los resultados de las evaluaciones mostró que más del 85% de los estudiantes encuestados habían encontrado que la plataforma VIBRANT les daba más libertad para experimentar y mejoraba la accesibilidad a través de la plataforma VirtualBox. [20]

Por otra parte, el trabajo de grado denominado Implantación De Técnicas Y Administración De Laboratorio Para Investigación De Ethical Hacking, realizado por Lucia Carolina Sandoval y Andrea Estefanía Vaca, resaltan la necesidad de un laboratorio físico En la Escuela Politécnica del Ejercito, que fomente la investigación y el uso de herramientas de hacking para poner a prueba la seguridad de los sistemas de información, este trabajo de grado parte de la misma necesidad visualizada en la universidad, pero con un enfoque diferente, ya que lo que se pretende es tener un espacio dedicado físicamente para poder realizar los talleres sobre maquinas ya preestablecidas. [21]

Otra conferencia importante a mencionar fue la realizadas en Oaxaca en Octubre de 2014, la conferencia llamada: Técnicas de Hacking Ético en un Laboratorio de Pentesting Virtualizado, esto en el 1er Congreso de Informática e innovación Tecnológica (CIIT 2014), en donde este trabajo muestra la implementación de un laboratorio de Pentesting virtualizado con la utilización de Kali Linux y Virtual Box donde se instalaron varios sistemas operativos que sirvieron de soporte para instalar servicios de red que fueron los objetivos de ataques de intrusión, siguiendo una metodología ordenada, y utilizando técnicas y herramientas de hacking. Los ataques realizados resultaron exitosos y se pudo probar la efectividad de las herramientas y técnicas de hacking cuando existen vulnerabilidades y debilidades en la configuración de los servicios de red, dentro de nuestro punto de vista, a pesar de ser un impulso y un gran avance, las maquinas prediseñadas allí se encuentran en plataformas de fácil acceso y son bien conocidas en el mundo del Hacking Ético para los inicios. [22]

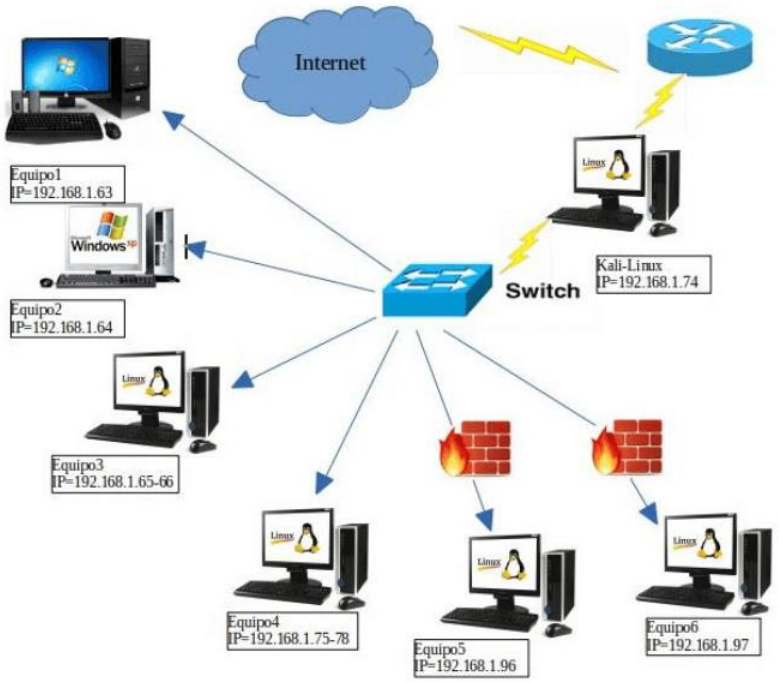

Ilustración 2 Laboratorio Pentesting Virtualizado
Fuente: Tecnicas_de_Hacking_Etico_en_un_Laboratorio_de_Pentesting_Virtualizado[22]

Adicional de conocer las definiciones acerca de los conceptos como Hackers y el tema de Hacking ético, de conocer proyectos referentes a la temática y metodología propuesta en nuestro proyecto de grado, queremos dar a conocer las normas, políticas y leyes colombianas que acobijan, respaldan o aplican a los infractores y/o acusados por delitos informáticos en Colombia, como es el caso de la norma técnica colombiana NTC-ISO/IEC 27001, tecnología de la información. Técnicas de Seguridad. Sistemas de Gestión de la seguridad de la información (SGSI), por la cual el ICONTEC, que es el organismo nacional de normalización, opto por acobijarla para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento, y mejora de un sistema de gestión de la seguridad de la información (SGSI) [23], Esta norma permite a las empresas definir su plan de seguridad de la información, por medio de una guía que contempla los factores fundamentales para resguardar los datos y la información de las mismas, y a su vez permite mantener por medio de controles los 3 pilares de la seguridad, como lo son la disponibilidad, integridad y confidencialidad de la información. Como caso puntual existe una norma que trata sobre estos temas denominada “De la protección de la información y de los datos” la cual es la Ley 1273 de 2009, que consta de dos capítulos que permiten a los entes regulatorios y a los entes jurídicos conocer las penas que acarrean los actos delincuenciales contenidos allí, y a presentar las penas que van desde 48 hasta 120 Meses de prisión y en multas que oscilan de 200 a los 1500 salarios mínimos legales mensuales vigentes. muy cerca de la publicación de esta ley el presidente de la época Álvaro Uribe Vélez, decreto la ley 1341 la cual garantiza a Colombia un marco

normativo por el cual se modifica el código penal, se crea un nuevo régimen tutelado denominado “de la protección de la información y de los datos” [24], años después se decreta la ley estatutaria 1581 del 17 de octubre de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, también conocida como Habeas data, en donde se desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos [25], por último el 11 de abril de 2016, a través del consejo nacional de política económica y social, aprobó la nueva política de seguridad Digital CONPES 3854 de 2016, en el cual se establece una política de seguridad y defensa contra posibles ataques digitales a las entidades del estado. [26]

6 ESTADO DEL ARTE

El hacker ha sido una palabra, mal catalogada por muchas empresas y entes, que lo describen como personas que infringen la ley, y que se dedican a entorpecer, o destruir la labora de muchas empresas, por medio de ataques y filtraciones de datos, pero los hackers no son más que personas apasionadas por la tecnología, aquellos que se dedican a realizar ataques se les conoce como ciberdelincuentes.

El termino Hacker ético, se dio para mitigar estos errores de comprensión, debido a señalamientos erróneos sobre personas que se dedican a encontrar y reparar errores dentro de los sistemas informáticos.

Actualmente muchas personas se apasionan por esta rama de la seguridad informática, y encuentran disponibles plataformas que, en muchas ocasiones, terminan desmotivándolos, ya que el nivel se encuentra muy elevado, o no existe una ruta de aprendizaje dentro de dichas plataformas.

En algunas universidades se han realizado proyectos con una temática similar, pero con espacios reservados (Físicos) o con metodologías ya preestablecidas de máquinas vulnerables, o entornos vulnerables, que no permiten ir más allá a los estudiantes más que de errores conocidos, o de solucionarios por medio de guías.

Algunos gremios individuales, o empresas de formación, ofrecen un amplio portafolio de aprendizaje, con muy buenos caminos y lineamientos a seguir para enfocarse en un área especifico de la seguridad o del hacking ético, por medio de cursos cortos o intensivos y planes de carrera que permiten cubrir todo el camino deseado por muchos profesionales, pero el mayor inconveniente de este punto es el valor económico al que no todos tienen la oportunidad ya que en la mayoría de los casos son muy costosos, o al segmentar la formación los costos se multiplican al igual que el tiempo invertido.

Es común que existan foros de la temática del hacking que intentan ayudar a sus participantes en el autoaprendizaje, pero sigue faltando la disposición de entornos prácticos que fortalezcan los conocimientos.

7 METODOLOGIA

7.1 FASES DEL TRABAJO DE GRADO

Para llevar a cabo el desarrollo de los objetivos propuestos del proyecto, se planteó una metodología por fases, las cuales son las siguientes:

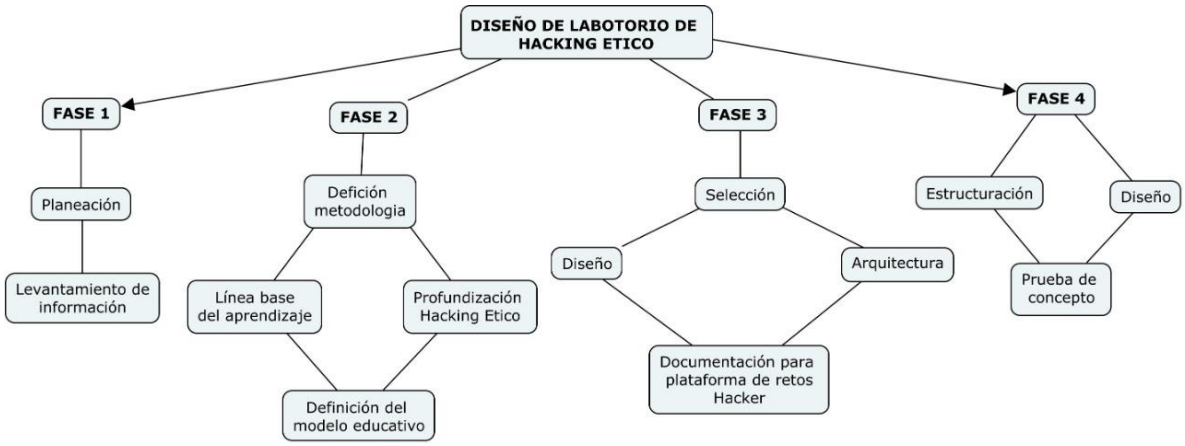

Ilustración 3 Fases del Trabajo de Grado
Fuente: Autores

Fase 1.
Como primera fase, Realizaremos la planeación y levantamiento de la información para el desarrollo del diseño laboratorio.

Fase 2.
Como Segunda Fase, definiremos la metodología interna del laboratorio, la cual tomaremos como punto de partida la línea base del aprendizaje o la hoja de ruta adecuada para el estudio y profundización del Hacking ético, así como la definición del mejor modelo educativo.

Fase 3.
La Tercera Fase estudiaremos y seleccionaremos el diseño y la arquitectura técnica o tecnológica de la plataforma a usar, siguiendo los lineamientos de las mejores prácticas para estos laboratorios de entrenamiento.

Fase 4.
Como cuarta Fase, realizaremos por medio de un diseño previamente estructurado una prueba de concepto del laboratorio, la cual permitirá demostrar el planteamiento de la solución.

8 INSTRUMENTOS O HERRAMIENTAS UTILIZADAS

Como instrumento de recolección de los datos en la investigación, se utilizó una encuesta que consta de 13 preguntas, de las cuales 9 son cerradas y 4 abiertas, reconociendo la encuesta como un método de investigación social, cuya aplicación significa el seguimiento de un proceso de investigación en toda su extensión, destinado a la recogida de los datos de la investigación, pero en el que se involucra un conjunto diverso de técnicas que combinadas, en una sintaxis propia y coherente, que se orienta y tienen como objetivo la construcción de un objeto científico de investigación. [27]

Dicha encuesta se aplicó a un total de 56 estudiantes y egresados, de los programas de ingeniería en telecomunicaciones, ingeniería en Sistemas, Postgrados de Seguridad de la Información y Egresados de este mismo postgrado, por medio de un formulario suministrado a través de correo electrónico y diligenciado por Google Forms

9 POBLACIÓN Y MUESTRA

Estudiantes de las ingenierías de Sistemas y Computación e Ingeniería Electrónica y Telecomunicaciones, adicionalmente la Especialización en Seguridad de la Información y Egresados de este mismo postgrado, de la Universidad Católica de Colombia.
Fecha de recolección de la información: del 30 marzo 2020 al 01 mayo 2020.

Marco Muestral: Se realiza selección de una muestra representativa debido a la cantidad de estudiantes de las diferentes carreras mencionadas anteriormente, se toma como primera base del proyecto la cantidad de encuestados que fueron 90 Estudiantes.

Técnica de recolección: Cuestionario estructurado vía online, por medio de Google forms.

Error muestral: +/- 10%
Nivel De Confianza: 95%

Encuestas diligenciadas por los estudiantes.

Pregrado: 14
Postgrado 1er Semestre: 15
Postgrado 2do Semestre: 12
Egresados: 15

10 ALCANCES Y LIMITACIONES

El Alcance global de este proyecto se define como el desarrollo de la propuesta de una plataforma web de Ethical Hacking para la universidad católica de Colombia

En cuanto a las limitaciones nos encontramos con la planeación inicial del proyecto, además del diseño de la estructura, modelos, métodos y lineamientos, mas no de la solución, ni ejecución del laboratorio.

Este proyecto no pretende ser la solución final, ni la implementación de la plataforma.

11 PRODUCTOS A ENTREGAR

A. Encuesta De Diagnostico

Documento el cual contiene las preguntas y respuestas que se realizaron en la encuesta a los estudiantes de pregrado de Ingeniería de Sistemas e ingeniería en Telecomunicaciones, postgrado en Seguridad de la información y Egresados del postgrado en Seguridad de la información, con su respectivo análisis de las respuestas obtenidas.

B. Metodología del Laboratorio de Retos de Hacking ético

Documento que contendrá la línea base para el aprendizaje del Hacking ético, los módulos internos del laboratorio, con sus respectivas áreas de aprendizaje, la estructura interna para el desarrollo de los retos Hacking y la estructura de la bandera la cual dará el aval de resuelto del laboratorio.

C. Diseño Técnico y Tecnológico del Laboratorio

Recomendaciones fundamentadas de la elección de software y hardware para la puesta en marcha del laboratorio web de retos Hacker, mostrando los beneficios, ventajas y desventajas de la lógica y lenguajes de programación existentes, además de la postulación de plataformas de virtualización o hardware recomendado para la implementación del laboratorio.

D. Prueba de Concepto

Se realiza una prueba de concepto en donde se evidenciará la metodología, fases y consecución para la aprobación del laboratorio, mostrando la consecución de la bandera, para dar por logrado el reto y obteniendo los beneficios de dicho logro.

12 ENTREGA DE RESULTADOS E IMPACTOS

12.1 ENCUESTA DE DIAGNOSTICO

A continuación, revisaremos las respuestas otorgadas por los estudiantes y egresados que participaron en la encuesta, la cual permitió afianzar la necesidad de un apoyo y motivación adicional para los estudiantes de la universidad católica de Colombia.

- Condición Estudiantil.

En esta pregunta vemos muy equilibrado la condición estudiantil de las personas que participaron en el diligenciamiento de la encuesta.

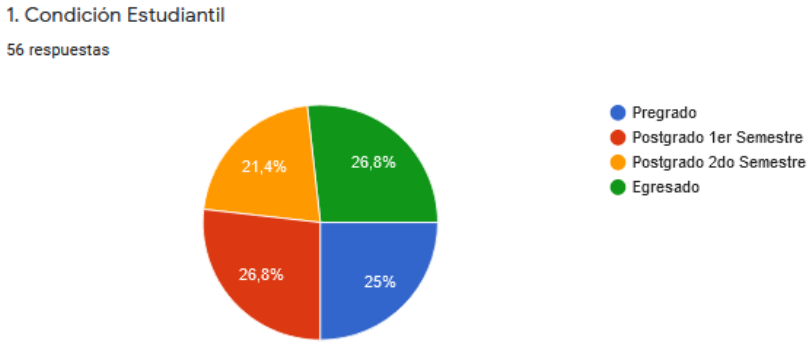

Ilustración 4 Encuesta. Pregunta 1
Fuente: Autores

- Dentro de su experiencia, ¿la colegiatura impartida en la Especialización de Seguridad de la Información cumplió sus expectativas en lo referente a Hacking Ético? (Solo Para Egresados y Segundo Semestre de especialización)

A pesar de que no se ve muy marcado, existe un ligero sentimiento, que algo hace falta en la especialización.

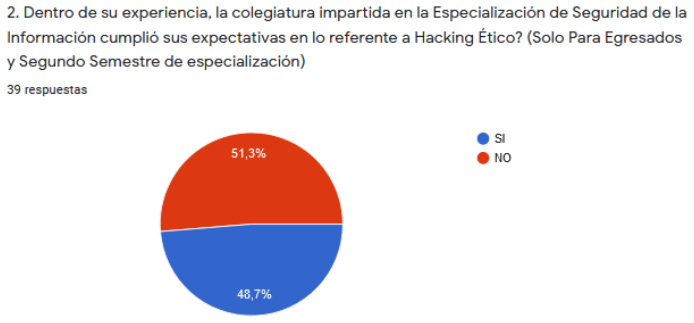

Ilustración 5 Encuesta. Pregunta 2
Fuente: Autores

- ¿Cuál de las siguientes plataformas de entrenamiento Hacking conoce?

Aquí nos encontramos que el 44,6% de las personas que diligenciaron la encuesta no conoce, alguna plataforma de retos informáticos bien sea por desinterés o porque aún no se ha interesado en el tema.

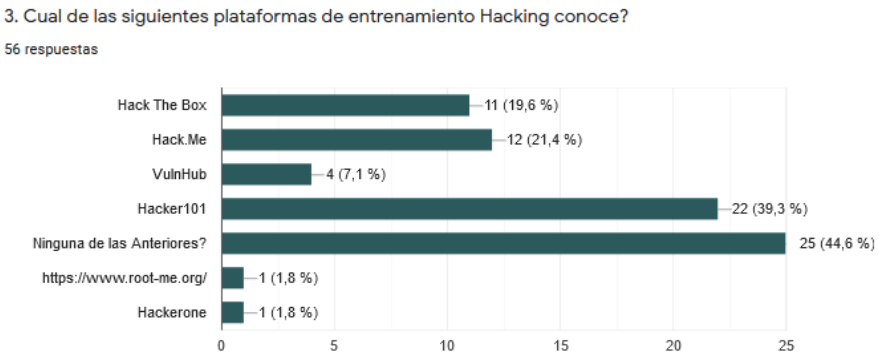

Ilustración 6 Encuesta. Pregunta 3
Fuente: Autores

- De las anteriores plataformas de entrenamiento, ¿cuál cree usted que es el mayor impedimento para participar en ellas?

Parte de la necesidad, incluso de los autores del proyecto, es que la mayoría de las plataformas de entrenamiento que existen están sobre el idioma inglés, lo cual, refleja un miedo, una brecha para poder usarlas al máximo.

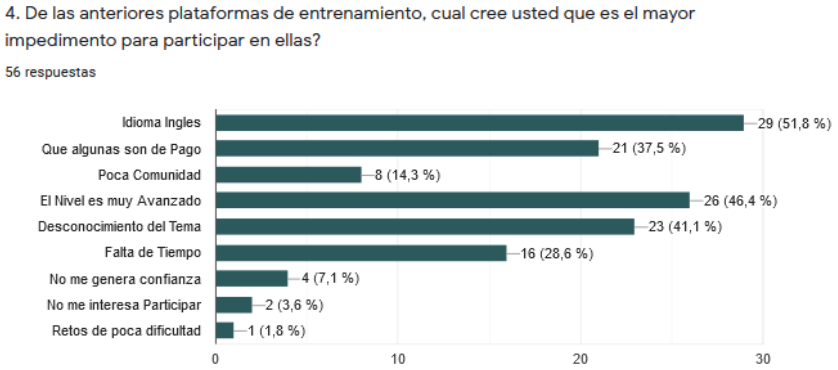

Ilustración 7 Encuesta. Pregunta 4
Fuente: Autores

- Conoce usted plataformas de retos hackers colombianas que permitan adquirir conocimientos y competencias en la temática.?

Consultamos a los encuestados, sobre plataformas colombianas, que puedan conocer sobre entrenamiento en seguridad informática.

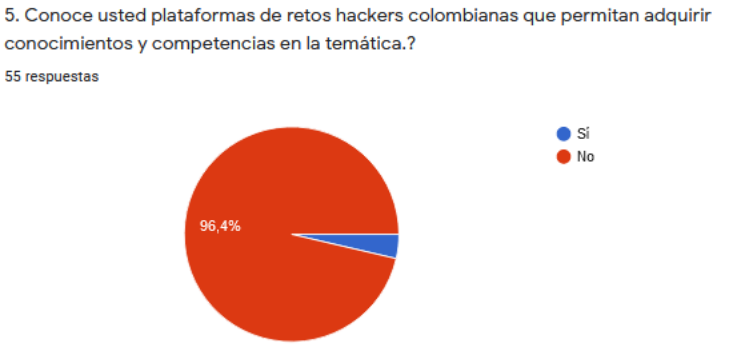

Ilustración 8 Encuesta. Pregunta 5
Fuente: Autores

- Si la anterior pregunta fue afirmativa, mencione la plataforma

De las 55 Personas que dieron respuesta a la pregunta anterior, les solicitamos compartir dicha plataforma, para poder consultarla y dar veredicto de aquella afirmación. Obteniendo 2 respuestas, pero ninguna de ellas catalogada como una plataforma de entrenamiento, sino más bien como entidades o empresas dedicadas a la labor de seguridad.

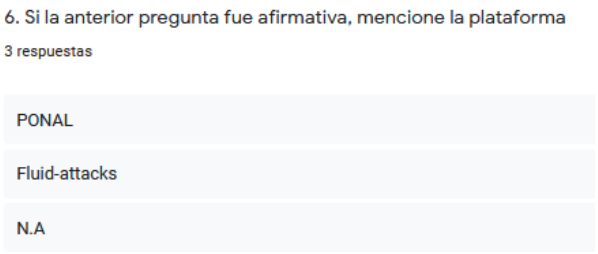

Ilustración 9 Encuesta. Pregunta 6
Fuente: Autores

- Considera usted que una plataforma Web de retos hackers promovida por la Universidad Católica, aportaría a su crecimiento profesional?

En la siguiente pregunta, evidenciamos el querer de los estudiantes de una plataforma que sume a su crecimiento dentro de la universidad.

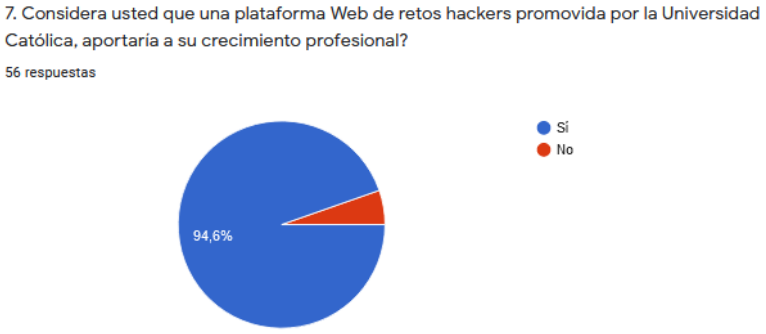

Ilustración 10 Encuesta. Pregunta 7
Fuente: Autores

- ¿Se vincularía a una plataforma Web de Retos hackers auspiciada por la Universidad Católica de Colombia?

Los estudiantes sienten curiosidad por el proyecto, y parte de este es la afirmación de querer participar de la plataforma.

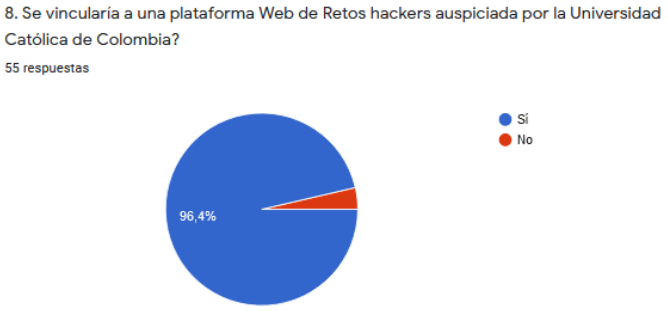

Ilustración 11 Encuesta. Pregunta 8
Fuente: Autores

- ¿Cuáles de las siguientes temáticas le gustaría que se incluyeran en el diseño de la plataforma?

Evidenciando el querer de los estudiantes, les solicitamos conocer las temáticas que preferirían si existiera una plataforma para el entrenamiento de estos campos

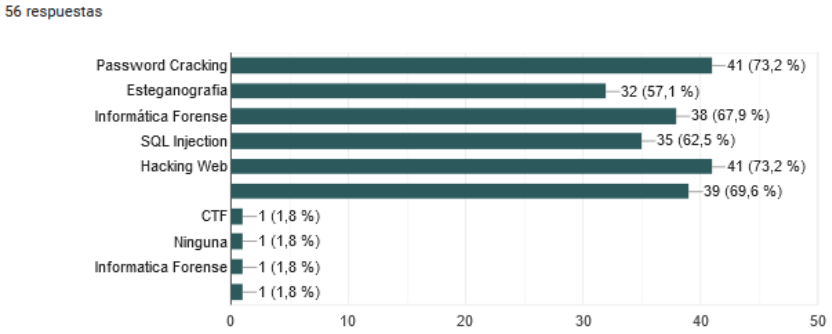

Ilustración 12 Encuesta. Pregunta 9
Fuente: Autores

- ¿Sabía Usted que existen plataformas intermediarias que entregan retribuciones económicas por encontrar vulnerabilidades en compañías?

Esta pregunta está orientada a despertar el interés por la plataforma, para que los estudiantes se incentiven a estudiar, prepararse y pensar en las posibilidades que la plataforma puede brindarles.

Ilustración 13 Encuesta. Pregunta 10
Fuente: Autores

- ¿Si tuviera la oportunidad de agregar desafíos en la plataforma de retos, lo haría?

Parte del deseo del proyecto es que los estudiantes se apropien de la plataforma y la mantengan viva, por tal razón, una de las características de esta, es la posibilidad de agregar retos.

Ilustración 14 Encuesta. Pregunta 11
Fuente: Autores

- ¿Usted sabía que en Colombia existe una gran demanda de vacantes enfocadas a roles relacionados con Hacking?

La industria y la tecnología cambia cada día, y la demanda de personal que sepa atacar y defender las infraestructuras de las compañías, suman un valor importante a las mismas.

Ilustración 15 Encuesta. Pregunta 12
Fuente: Autores

- ¿Si usted mejorara sus competencias en Hacking Ético, consideraría cambiar su rol laboral?

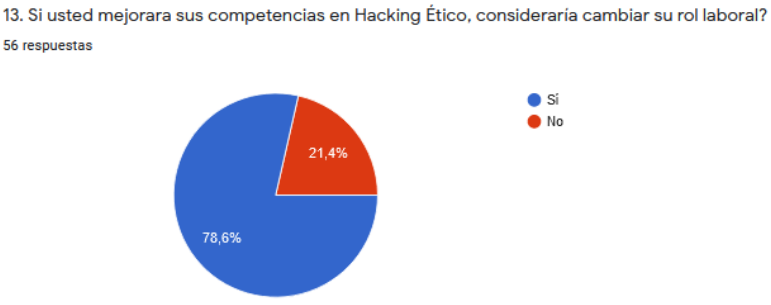

Ilustración 16 Encuesta. Pregunta 13
Fuente: Autores

- Si tienen Comentarios, Ideas, Sugerencias, Felicitaciones, los pueden compartir a continuación.

La plataforma es un proyecto que se realizara por y para los estudiantes, por ello, solicitamos en la encuesta dar un punto de vista y comentarios acerca del proyecto.

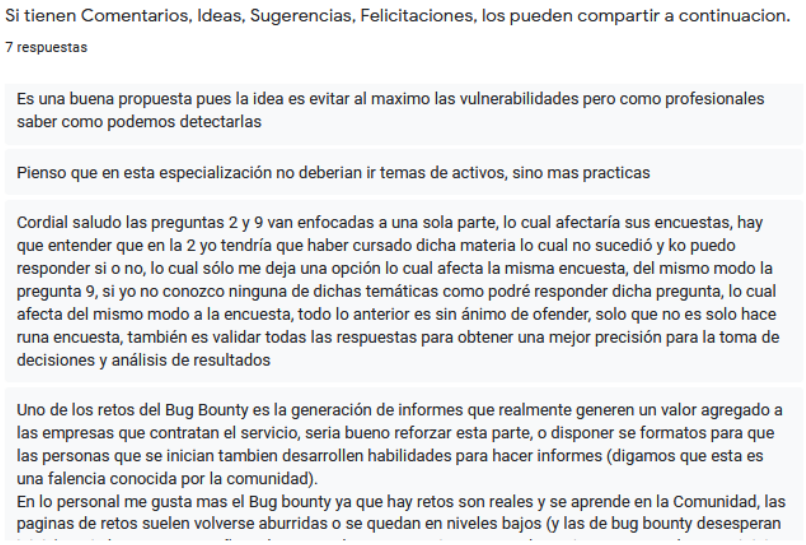

Ilustración 17 Encuesta. Comentarios
Fuente: Autores

12.2 METODOLOGÍA DEL LABORATORIO DE RETOS DE HACKING ÉTICO

Como parte de la estructuración y diseño de la propuesta del laboratorio de retos tipo Hacking ético, este se realizará por medio de distintas modalidades que permitan a los estudiantes y egresados, desenvolverse mediante diferentes metodologías usadas en competencias y certificaciones de seguridad informática, las cuales, permitirán adquirir conocimiento, destrezas y experiencia para ser aplicadas en un futuro.

Este diseño se centra en 3 modalidades las cuales son:

1. **Instancias.**
    a. Permite desplegar por medio de una ventana emergente, o una pestaña en el navegador un ambiente controlado y único por usuario, para ser utilizado en la consecución y resolución del reto.

2. **Máquinas Virtuales**
    a. Estas permiten ser descargadas, y por medio de instrucciones se enviarán la o las actividades a culminar para dar por finalizado el reto.

3. **Descarga de Evidencias.**
    a. Los archivos que se podrán descargar serán capturas de tráfico, imágenes de disco, dumps de Memoria ram, fotos y demás archivos que pueden ser usados para adquirir información o como evidencia, para dar finalizado el reto.

Ilustración 18 Modalidades Retos Plataforma
Fuente: Autores

Estas modalidades vienen acompañadas de sus líneas de ruta y aprendizaje, las cuales permitirán a los estudiantes perfilarse y enfocarse profesionalmente, mediante ejercicios que se asemejan a la realidad de estas líneas de ruta.

Las líneas de aprendizaje se centran en 3 perfiles profesionales los cuales son:

- Red Team
- Blue Team
- Purple Team

Para el desarrollo de la propuesta, nos centraremos en los dos primeros ya que, su perfil técnico y profesional es más demandado en las empresas y el tercero de forma general es la unión de los dos primeros

Una de las definiciones más precisas para describir lo que realiza cada equipo, lo

menciono Daniel Miessler en su artículo The Difference between Red, Blue, and Purple Teams. [28]

Red Team.
Los Red Team, son entidades internas o externas dedicadas a probar la efectividad de un programa de seguridad emulando las herramientas y técnicas de los probables atacantes de la manera más realista posible. La práctica es similar, pero no idéntica, a la Prueba de Penetración, e implica la persecución de uno o más objetivos, normalmente ejecutados como una campaña.

Blue Team
Los Blue Team, se refieren al equipo de seguridad interna que defiende tanto a los atacantes reales como a los Red Team. Los Blue Team deben distinguirse de los equipos de seguridad estándar en la mayoría de las organizaciones, ya que la mayoría de los equipos de operaciones de seguridad no tienen una mentalidad de vigilancia constante contra los ataques, que es la misión y la perspectiva de un verdadero Blue Team.

Cada uno de estos perfiles poseen categorías Preestablecidas, permitiendo realizar un diseño metodológico por medio de los roles laborales más demandados en seguridad informática, en Colombia.

Para cada perfil, hemos seleccionado 2 categorías, las cuales describiremos a continuación

Red Team

Penetration Testing
Esta categoría permitirá al estudiante descubrir y familiarizarse con el reconocimiento, análisis y explotación de vulnerabilidades, a través de diferentes metodologías para evadir sistemas de seguridad.

Web Penetration Testing
Esta categoría retará al estudiante por medio retos sobre plataformas en diferentes motores y aplicaciones web, aprenderá a detectar vulnerabilidades, inyectar código malicioso, y tomar el control de estas aplicaciones.

Blue Team

Incident Response
Esta categoría, retará al estudiante a pensar como primer respondiente y/o parte del equipo forense, revisando dumps de memoria, análisis de tráfico, trazas y capturas de tráfico, y así encontrar evidencias para hallar la causa del incidente presentado.

Security Analist

Esta categoría, permitirá al estudiante a reconocer debilidades sobre la infraestructura informática de una empresa, por medio de la captura de logs, el reconocimiento del tráfico malicioso y la obtención de información importante para alcanzar el objetivo.

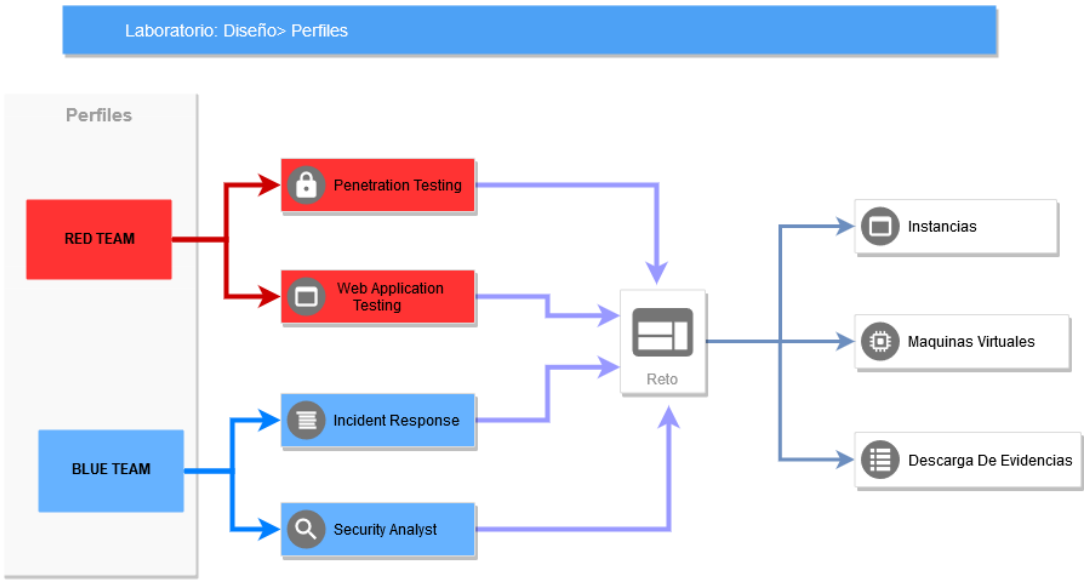

Ilustración 19 Perfiles Plataforma
Fuente: Autores

12.3 ESTRUCTURAR LA METODOLOGÍA DE LOS RETOS POR MEDIO DE LAS DIFERENTES RAMAS DE ESPECIALIDAD DE HACKING ÉTICO

La metodología de los retos parte de la categorización del reto, dentro de las categorías, se encontrarán niveles, los cuales permitirán al estudiante conocer el grado de dificultad de los retos, los estudiantes iniciaran con los niveles de menor complejidad para poder avanzar a los niveles superiores, ya que en aquellos será más complicado encontrar la resolución del reto.

Adicional los niveles inferiores permitirán construir las bases para los siguientes niveles, con ello se garantiza que el estudiante cuente con los conocimientos necesarios para poder afrontar estos retos de mayor complejidad.

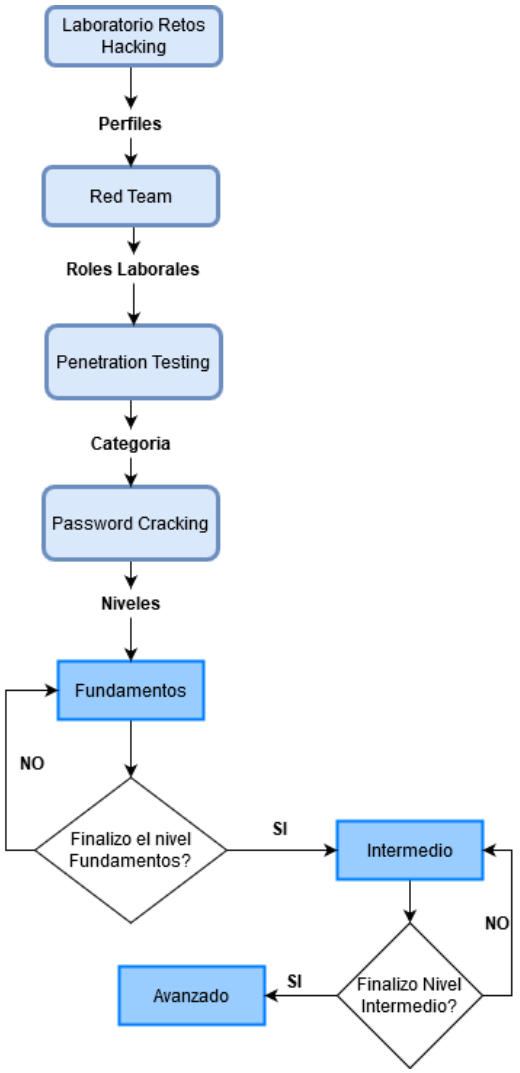

Ilustración 20 Niveles Reto. Ejemplo Categoría Password Cracking
Fuente: Autores

Cada reto para resultar satisfactorio deberá pasar por una comprobación de lo solicitado en el mismo, usualmente una bandera de tipo: **UCatolica{f_L_4_G_encontrada},** esta mostrara que es correcto el parámetro (Flag) y asignara una puntuación por alcanzar el desarrollo de este, ya que cada reto asignara una puntuación acorde a su complejidad y el nivel en donde se encuentra cada reto dentro de la plataforma.

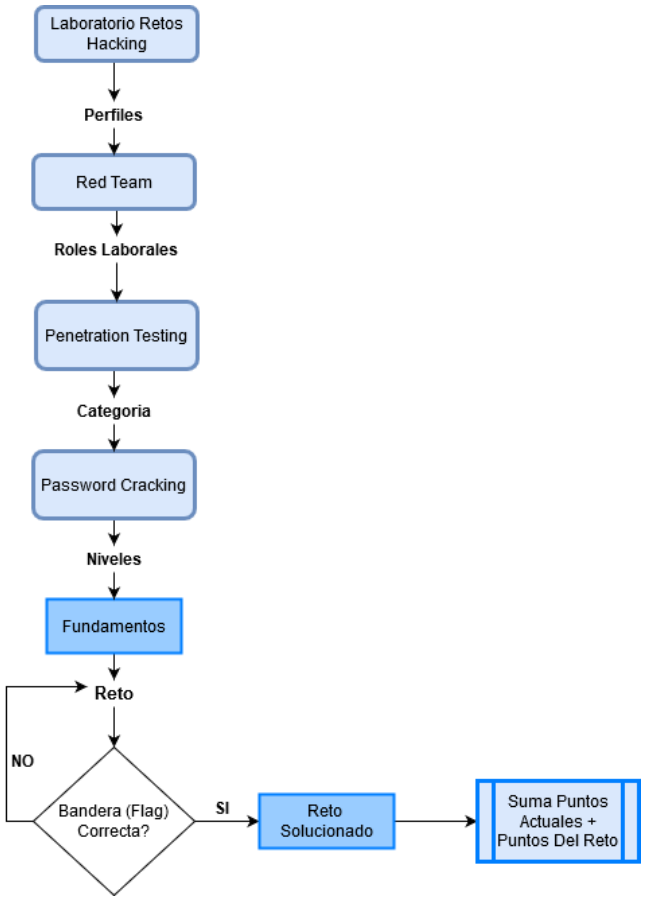

Ilustración 21 Comprobación Flag, Categoría Password Cracking
Fuente: Autores

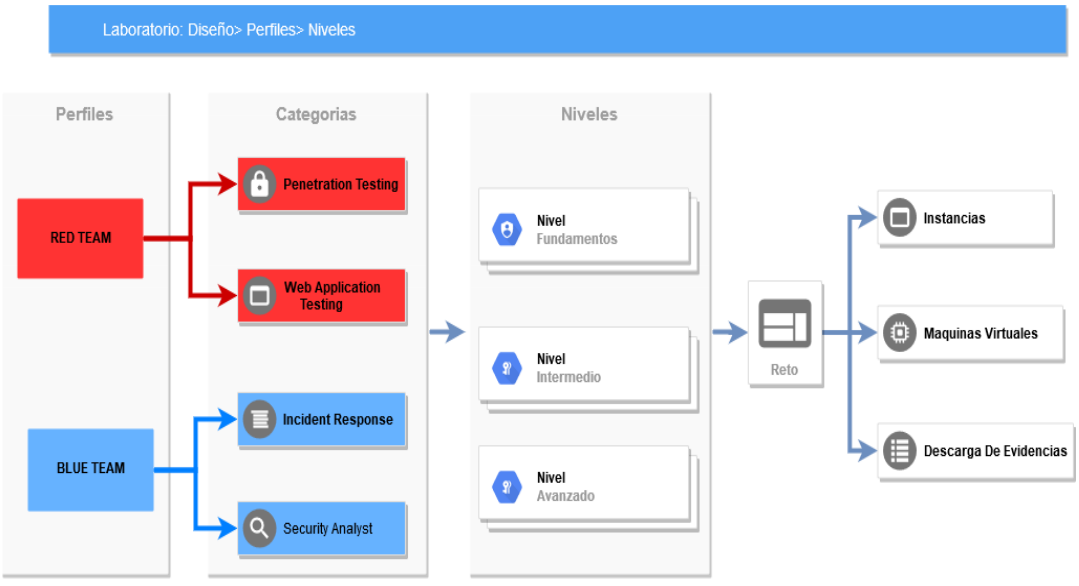

Ilustración 22 Esquema General Plataforma
Fuente: Autores

12.4 DISEÑO TÉCNICO Y TECNOLÓGICO DEL LABORATORIO

Generalidades

Dentro de la propuesta técnica y tecnología de la aplicación, nos basaremos en la realización del modelo de programación por capas, las cuales son:

Capa de Presentación. También conocida como Front end, es la encargada de la visualización de la información, presenta el sistema al usuario, le comunica la información y captura de la misma.

Capa de Negocio. También conocida como Back end, es la encargada de mantener los programas que se ejecutan, se reciben las peticiones del usuario y envían las respuestas tras finalizar el proceso.

Capa de Datos. También conocida como Base de Datos, en esta residen los datos, y es la encargada de acceder a los mismos.

Estas capas permitirán acceder a la información en un menor tiempo, y los retos cargaran y descargaran información de una manera más eficiente, permitiendo trabajar en un modelo tipo cliente/servidor, en donde la distribución y división de las capas hará más eficiente y fluida la plataforma. [29]

A continuación, se visualizará la topología seleccionada para el desarrollo de la propuesta del laboratorio

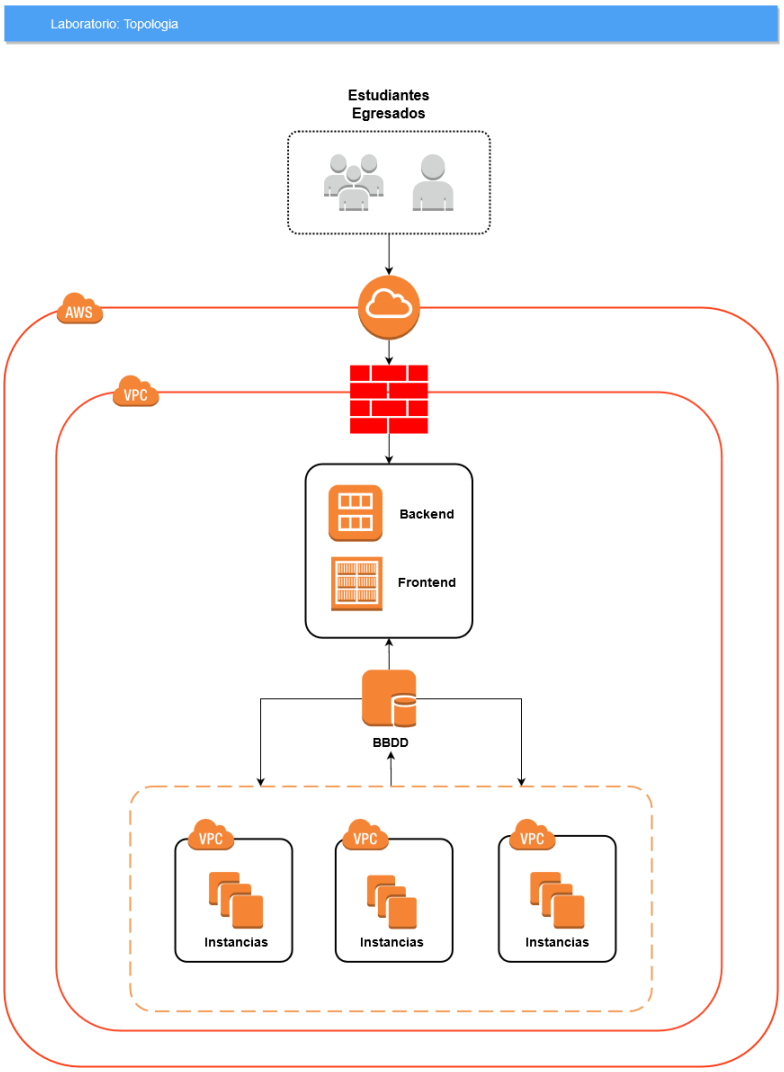

Ilustración 23 Topología Plataforma
Fuente: Autores

Esta arquitectura y topología permitirá la implementación de redes privadas sobre la plataforma de virtualización, permitiendo que las instancias se ejecuten según las necesidades de los usuarios, con ello, no se mantendrán en ejecución hasta que se requiera.

Los retos tipo Máquinas Virtuales y Descarga almacenaran los enlaces de descarga sobre la base de datos de la aplicación, con ello, se mantendrán en ejecución mientras el motor de base de datos se mantenga activo, significando ahorro en costes de instancias adicionales no requeridas.

Dentro de los elementos seleccionados para la implementación de la arquitectura técnica se encuentra el Framework de CTF, la tecnología de virtualización, los entornos de despliegue de los diferentes escenarios del laboratorio, bases de datos,

entre otros.

Dentro de esta arquitectura prima la independencia de los elementos, permitiendo deshacerse de la dependencia de uno u otro recurso dentro de la plataforma, con ello las instancias se basarán en entornos bajo el esquema de dockers, lo cual permite, desplegar con mayor rapidez y seguridad, ya que cada elemento es independiente del anterior. Los contenedores basan su estructura por medio de imágenes, las cuales comparten una aplicación o servicios, en varios entornos simultáneamente, pero de forma aislada e independiente.

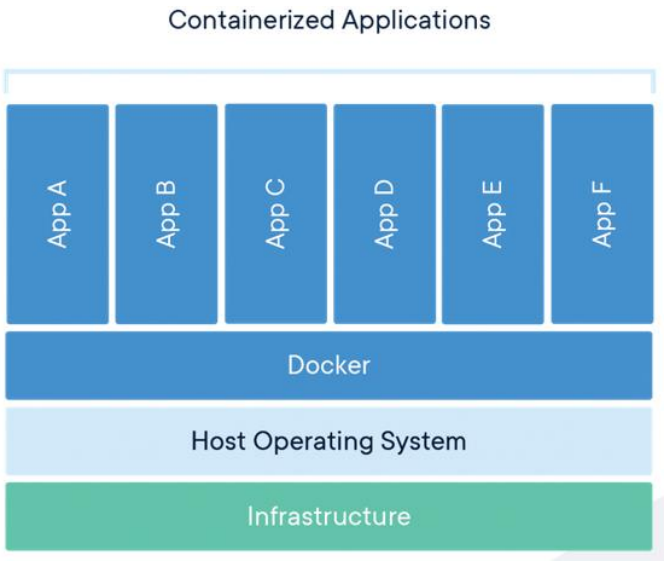

Ilustración 24 Infraestructura Docker
Fuente: www.docker.com

Componentes.

La elección de los componentes para el desarrollo de la propuesta del laboratorio de retos tipo Hacking ético, se basa en las investigaciones realizadas anteriormente.

Framework: Dentro de las opciones existentes en el mercado, hemos seleccionado el framework CTFd, por su nivel de personalización, sus características, la gestión de usuarios consumidores y administradores, por su facilidad de uso y adaptación, permitiendo consultar resultados y estadísticas en tiempo real por los participantes.

Base de Datos: Para el desarrollo de la propuesta, se decidió separar la base de datos de las capas de Front end y Back end, esto debido a la elección de una mayor capacidad de almacenamiento y procesamiento de este recurso. El Framework mencionado anteriormente posee la característica de configuración de una base de datos externa, y recomienda para esta labor MySQL o MariaDB, debido a rendimiento y licenciamiento se recomienda el uso del motor de Datos MariaDB.

Cache: El Framework CTFd usa la característica de Flask-Caching, esto con el fin

de reducir los tiempos de respuesta en su lógica de cache, con esta característica se desplegará una base de datos en memoria redis para aprovechar esta característica disponible.
Cada uno de estos componentes será independiente, por lo tanto, será un contenedor por separado, interconectado entre sí, por medio de una VPC (Red Privada) segura, con ello se garantiza su integridad al aislarse de las demás VPC.

Para garantizar esta integridad se separan las redes en 2 tipos, los cuales son:

Red Pública: Esta red es la que se puede acceder al ingresar a la plataforma, donde se observaran la unión de las capas de Front y Back end, aquí los estudiantes y egresados ingresaran para visualizar sus puntos, los retos de la plataforma, categorías, metodologías y demás características que la plataforma les ofrezca.

Red Privada: Esta red es la lógica de la plataforma, ya que en esta se interconectan los componentes descritos anteriormente, se distingue por ser una red independiente, usada para el consumo de los componentes entre sí.

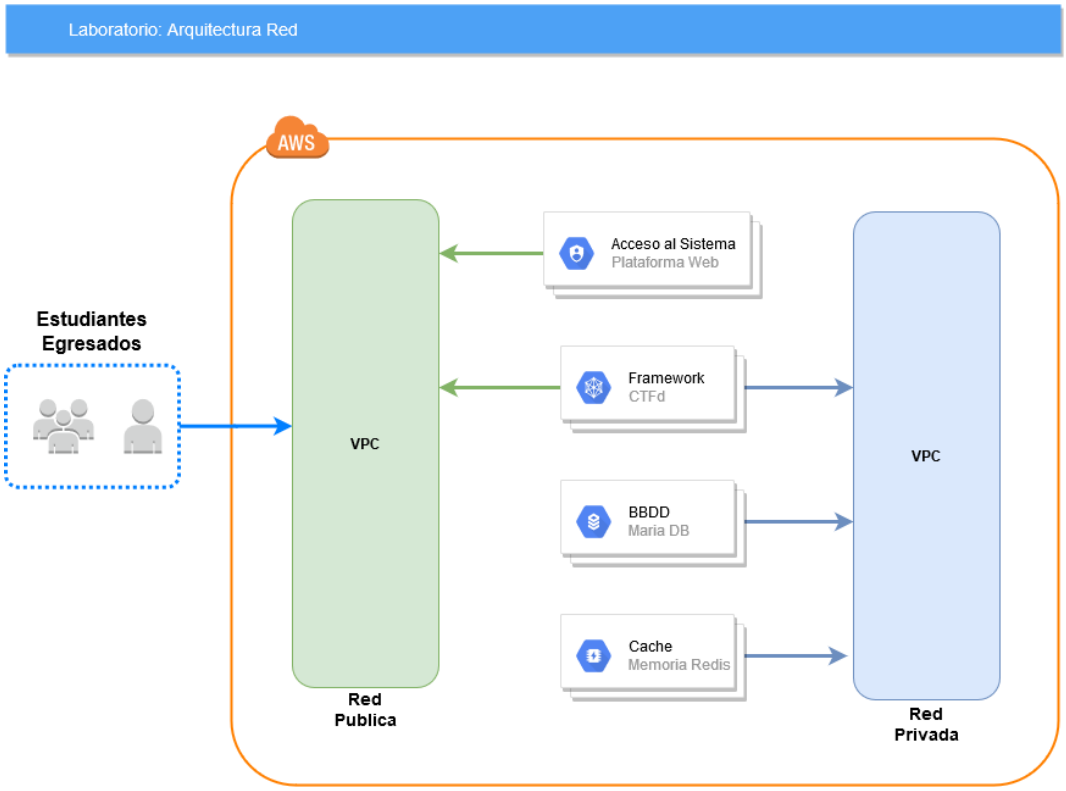

Ilustración 25 Arquitectura Pública y Privada Laboratorio.
Fuente: Autores

12.5 PRUEBA DE CONCEPTO

Existen 2 maneras de desplegar instancias del Framework CTFd, en nuestra infraestructura.

Una de ellas, es por medio de la clonación del repositorio del proyecto, instalando manualmente sus dependencias, por medio de la aplicación pip en nuestro servidor, adicional a esto se deben configurar las bases de datos MySQL/MariaDB y la memoria Redis.

Por otra parte, existe las tecnologías de Docker o contenedores, las cuales por medio del archivo Docker-compose.yml, presente en el repositorio del framework, permite desplegar cada componente requerido en contenedores separados, permitiendo como mencionamos anteriormente mayor rapidez de despliegue y mejor rendimiento.

Cabe aclarar que una migración futura será menos traumática por medio de los contenedores que una instalación dependiente en un servidor, por tal motivo, además de las características, funciones y ventajas descritas acerca de los contenedores, recomendamos el uso de esta tecnología para el despliegue del proyecto y por tal motivo se realizará para la prueba de concepto.

Para realizar la prueba de concepto, realizaremos la instalación desde cero del framework CTFd, por esta razón, haremos login dentro del servidor para proceder a instalar lo requerido.

Ilustración 26 Servidor Prueba de Concepto
Fuente: Autores

Iniciaremos removiendo las aplicaciones que puedan estar obsoletas, puntualmente el caso de Docker, y actualizando la lista de paquetes disponibles para el servidor, en este caso un Ubuntu Server 20.10.

sudo apt-get remove docker docker-engine docker.io containerd runc && sudo apt-get update

```
ec2-user@ip-172-31-20-12:~$
ec2-user@ip-172-31-20-12:~$ sudo apt-get remove docker docker-engine docker.io containerd runc
[sudo] password for ec2-user:
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package docker-engine
ec2-user@ip-172-31-20-12:~$ sudo apt-get update
Hit:1 http://co.archive.ubuntu.com/ubuntu groovy InRelease
Hit:2 http://co.archive.ubuntu.com/ubuntu groovy-updates InRelease
Hit:3 http://co.archive.ubuntu.com/ubuntu groovy-backports InRelease
Hit:4 http://co.archive.ubuntu.com/ubuntu groovy-security InRelease
Reading package lists... Done
ec2-user@ip-172-31-20-12:~$
```

Ilustración 27 Eliminación Aplicaciones y Actualización Repositorios.
Fuente: Autores

Terminada la actualización, procederemos a instalar algunos paquetes necesarios para la configuración a futuro del servidor con las aplicaciones del contenedor.

sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent software-properties-common

```
ec2-user@ip-172-31-20-12:~$ sudo apt-get install apt-transport-https ca-certificates curl gnupg-agent softw
are-properties-common
Reading package lists... Done
Building dependency tree
Reading state information... Done
curl is already the newest version (7.68.0-1ubuntu4).
curl set to manually installed.
software-properties-common is already the newest version (0.99.3).
software-properties-common set to manually installed.
ca-certificates is already the newest version (20201027ubuntu0.20.10.1).
ca-certificates set to manually installed.
The following NEW packages will be installed:
  apt-transport-https gnupg-agent
0 upgraded, 2 newly installed, 0 to remove and 5 not upgraded.
Need to get 6940 B of archives.
After this operation, 209 kB of additional disk space will be used.
```

Ilustración 28 Instalación Paquetes Sistema Operativo.
Fuente: Autores

Agregamos la key y el repositorio de Docker para el servidor Ubuntu

curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -

sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"

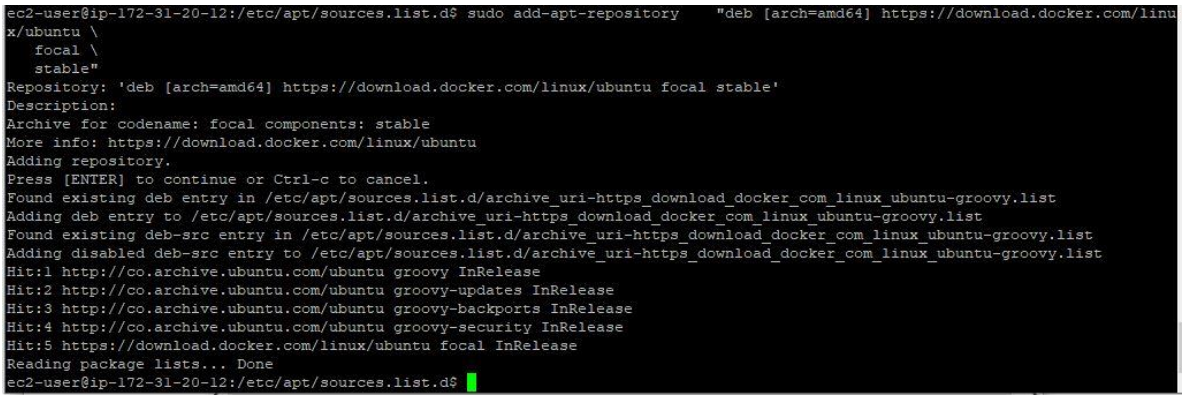

Ilustración 29 Key y Repositorio Docker.
Fuente: Autores

Realizamos la instalación del contenedor donde agregaremos la plataforma de retos

sudo apt-get install docker-ce docker-ce-cli containerd.io docker-compose

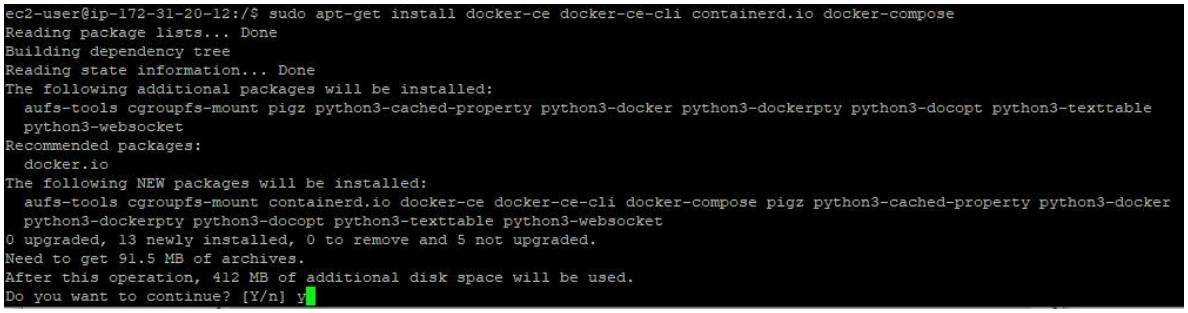

Ilustración 30 Instalación Contenedores.
Fuente: Autores

Finalizada la instalación de Docker, procederemos a descargar el git del framework CTFd para desplegarlo y poder realizar la configuración de la plataforma.

Sudo git clone https://github.com/csivitu/ctfd && cd CTFd

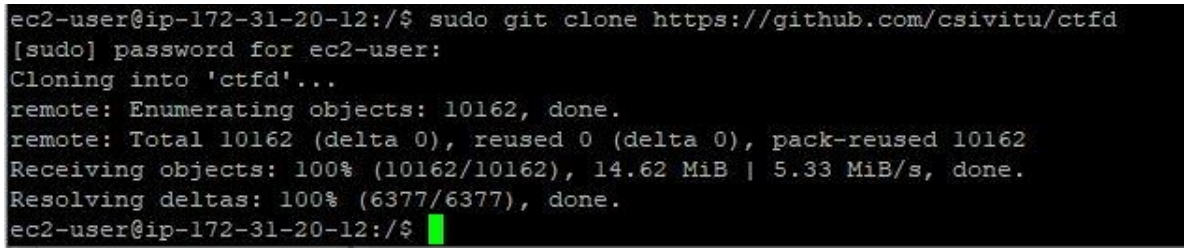

Ilustración 31 Descarga Framework.
Fuente: Autores

Sudo docker-compose up -d

```
ec2-user@ip-172-31-20-12:/ctfd$ cd CTFd/
ec2-user@ip-172-31-20-12:/ctfd/CTFd$
ec2-user@ip-172-31-20-12:/ctfd/CTFd$ sudo docker-compose up -d
[sudo] password for ec2-user:
Creating network "ctfd_internal" with the default driver
Creating network "ctfd_default" with the default driver
Pulling db (mariadb:10.4.12)...
10.4.12: Pulling from library/mariadb
23884877105a: Extracting [==================================================>]  26.69MB/26.69MB
bc38caa0f5b9: Download complete
2910811b6c42: Download complete
36505266dcc6: Download complete
e69dcc78e96e: Download complete
222f44c5392d: Download complete
efc64ea97b9c: Download complete
9912a149de6b: Download complete
7ef6cf5b5697: Download complete
8a05be3688e0: Download complete
c09ffdc1b660: Download complete
2eb7fe288fc8: Downloading [======>                                            ]  10.19MB/80.02MB
b41d1cc4d40f: Download complete
a92376500910: Download complete
```

Ilustración 32 Despliegue Framework sobre el Contenedor.
Fuente: Autores

Finalizada el despliegue del framework sobre el contenedor, nos debe mostrar los siguientes mensajes, confirmándonos que el despliegue se realizó con éxito.

```
40e134f79af1: Pull complete
Digest: sha256:2e03fdd159f4a08d2165calc92adde438ae4e3e6b0f74322ce013a78ee81c88d
Status: Downloaded newer image for redis:4
Creating ctfd_db_1    ... done
Creating ctfd_cache_1 ... done
Creating ctfd_ctfd_1  ... done
Creating ctfd_nginx_1 ... done
ec2-user@ip-172-31-20-12:/ctfd/CTFd$
```

Ilustración 33 Finalización del despliegue del framework
Fuente: Autores

El framework CTFd, trabaja sobre el puerto por defecto :8000, por tal razón, realizamos la apertura desde cualquier navegador, para realizar los siguientes pasos.

Agregamos un Nombre, descripción y modo de usuario (el cual se puede cambiar en cualquier momento), adicional de la cuenta administradora, estilos, uso horario e integraciones necesitemos en ese momento.

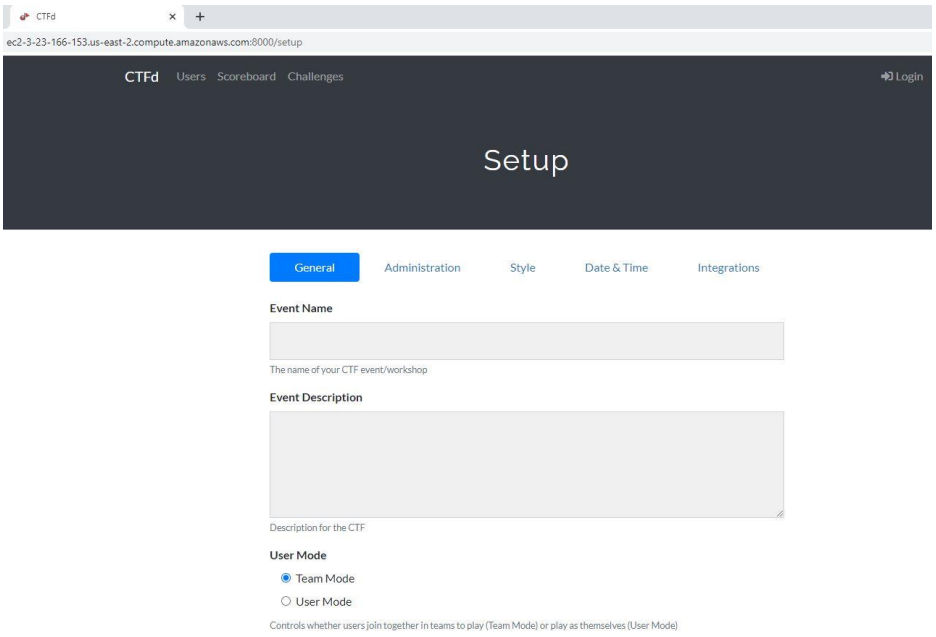

Ilustración 34 Inicio Configuración Web Framework.
Fuente: Autores

Finalizada la configuración inicial, podremos ingresar a la plataforma para proceder con la configuración de los perfiles y el reto para la prueba de concepto.

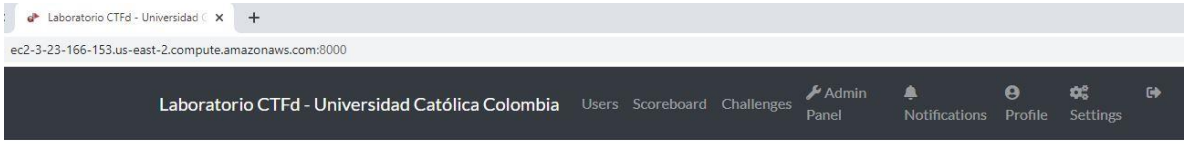

Ilustración 35 Visualización Panel Usuario Administrador.
Fuente: Autores

Adicional a la configuración mínima que se puede realizar, existen otros parámetros adicionales que se pueden configurar y de los cuales recomendamos aplicar en el momento de la implementación de la plataforma, los cuales son, la lista blanca de dominios de correo y la opción de verificación de este.

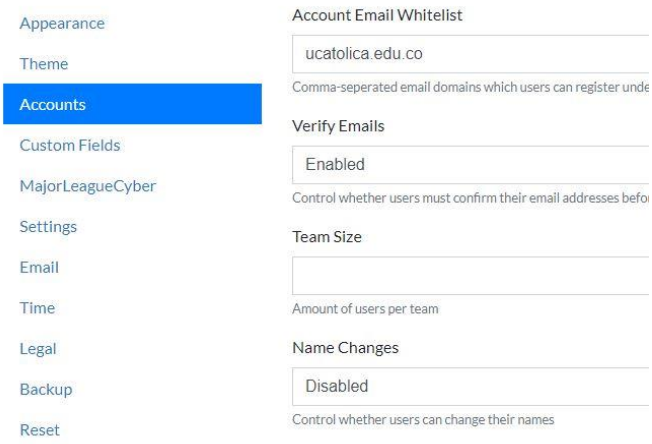

Ilustración 36 Recomendaciones Configuración.
Fuente: Autores

Después de realizar las configuraciones mínimas iniciales y recomendadas, procedemos a la prueba de concepto, sobre una categoría y nivel especifico las cuales son.

Laboratorio -> **Perfil** (Blue Team) -> **Categoría** (Security Analyst) -> **Nivel** (Fundamentos)

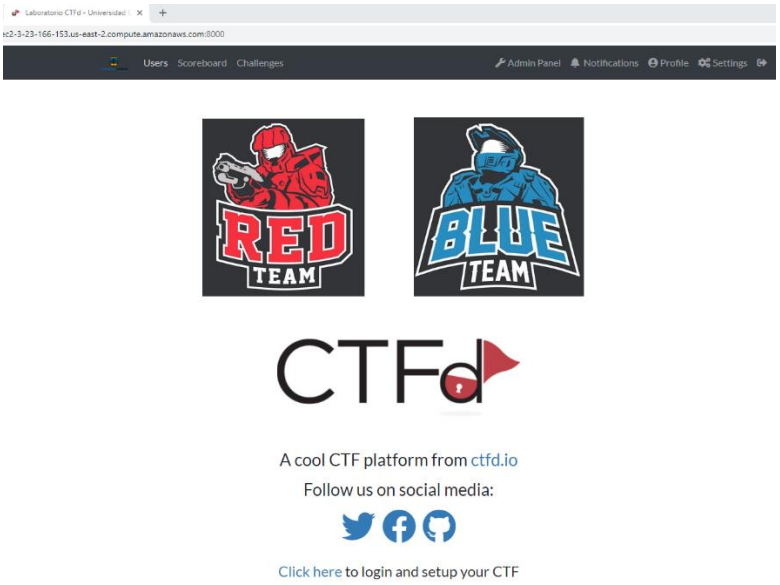

Ilustración 37 Index Plataforma (Perfiles).
Fuente: Autores

Al ingresar a la plataforma, el estudiante, se encontrará con los 2 perfiles descritos anteriormente, los cuales son Red Team y Blue Team, esto permitiendo que el estudiante pueda decidir, no solo por donde iniciar, ya que lo recomendado es poder participar en ambos perfiles, y con ello se garantiza que, por medio de los retos, defina su línea de aprendizaje sobre el rol que quiere para su futuro profesional.

Se recomienda, dar una introducción sobre estos perfiles definidos en la plataforma, para que los estudiantes tengan claro el perfil al que se van a enfrentar, comprendan el por qué y para que de este perfil y con ello se minimice la deserción, por falta de claridad sobre el perfil al que se ingresa.

Continuando con la prueba de concepto y dejando claro los perfiles y sobre que puede brindar cada uno de estos al perfil profesional de cada estudiante, nos dirigiremos a la sección de Blue Team, en donde encontraremos las 2 categorías iniciales de la plataforma las cuales son Incident Response y Security Analist.

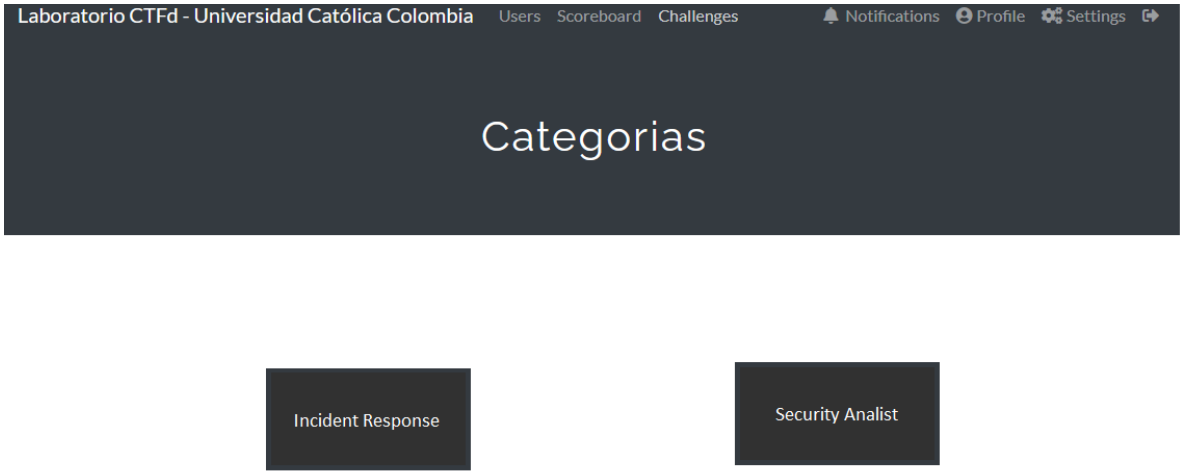

Ilustración 38 Categorías Blue Team..

Fuente: Autores

Estas categorías parten de preparar a los estudiantes frente a las adversidades que puedan encontrarse en sus profesiones y sobre todo pueda ser su día a día, ya que estas se enfocan en verificar eventos inusuales sobre la red y actuar sobre estas si se materializan.

Como lo mencionamos en capítulos anteriores la ruta de aprendizaje sobre las distintas categorías se apoya en un modelo de niveles, en donde, el estudiante aprende las nociones básicas en los niveles inferiores, y esto a su vez lo preparara para los niveles que exijan una mayor destreza y habilidad, llegando al nivel avanzado que permita asemejar entornos empresariales, con sus retos, amenazas y brechas de seguridad latentes.

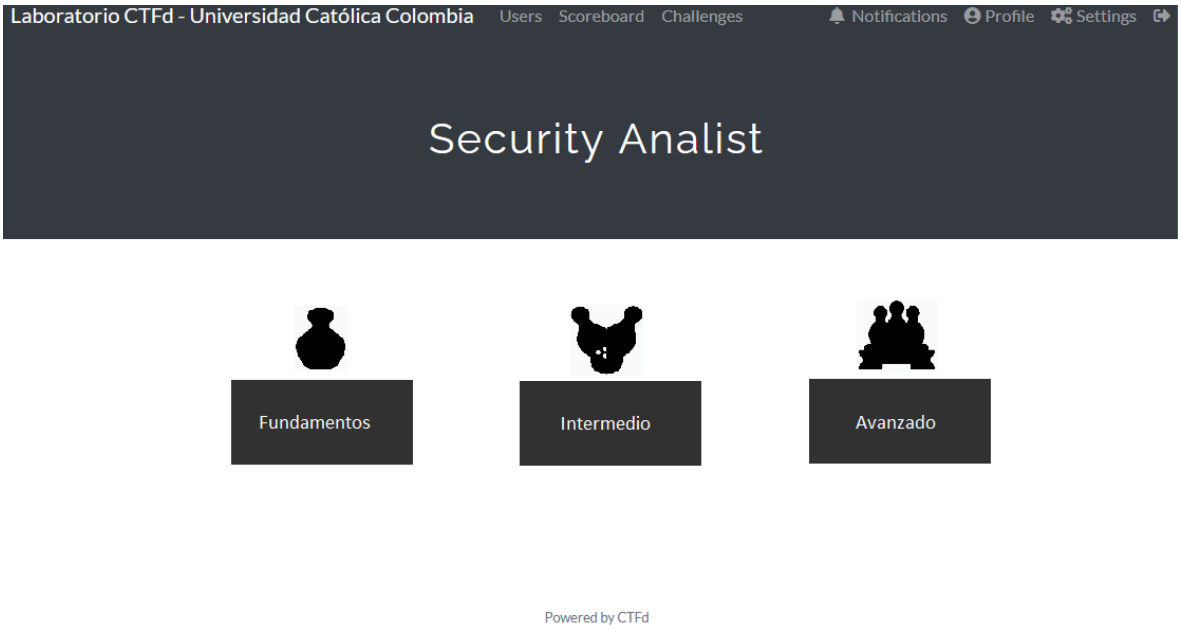

Ilustración 39 Niveles de la Plataforma.

Fuente: Autores

El nivel seleccionado para el desarrollo de la prueba de concepto es el de fundamentos en donde encontraremos diferentes retos, que deben ser cumplidos para obtener la puntuación necesaria con el fin de avanzar al siguiente nivel y/o aportar un reto dentro de la plataforma.

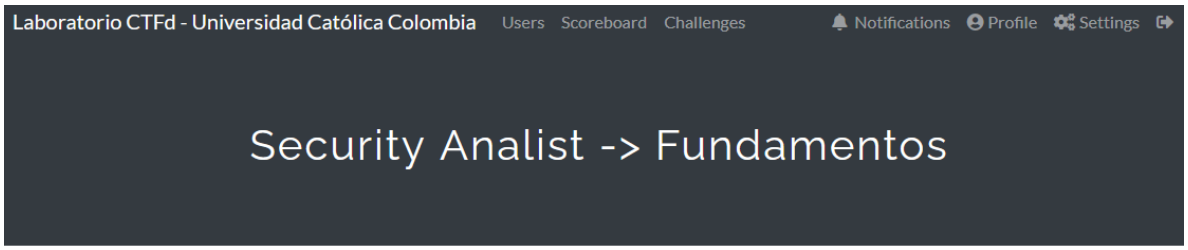

Ilustración 40 Nivel Fundamentos Blue team

Fuente: Autores

Este nivel no solo permite al estudiante comprender y afianzar conceptos, sino adicional a esto, familiarizarse con la plataforma, comprendiendo la funcionalidad

de esta, la metodología, el significado de la flag y, por ende, el descubrimiento de los objetivos alcanzados en cada reto.

Cada reto independiente del nivel podrá proporcionar una descripción de este, una historia, algo que permita identificar y sumergir al estudiante a imaginar que lo que se está solicitando encontrar y/o explotar, fue algo que le sucedió o que le está sucediendo, o simplemente por algún motivo se le solicito realizar en sus labores diarias.

A continuación, dentro del nivel fundamentos, se encuentra uno de los retos el cual consiste en calcular la función Hash de un archivo ubicado el día del incidente, esto permitiendo a los estudiantes a identificar las diferentes funciones criptográficas que existen y que le servirán para identificar firmas de seguridad por medio de estas funciones, al calcular la función esta debe ser introducida con una cadena tipo: Ucatolica{HASH SHA1}

Ilustración 41 Reto Prototipo

Fuente: Autores

Para la realización del reto y obtener el hash correspondiente, debemos identificar con que programas o aplicaciones podemos descubrir los diferentes tipos de Hash, en este caso usaremos la aplicación PowerShell y el comendo Get-FileHash, el cual nos permite por medio de diferentes parámetros obtener las firmas de los diferentes tipos de hash, en este caso SHA1, esto realizándolo de la siguiente manera.

```
PS C:\Users\FredySnake\Downloads> Get-FileHash .\UmbrellaPharm.pcapng.zip -Algorithm SHA1

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA1            C4172695CB785A9626C092CBEA42E0B9E6082510                               C:\Users\FredySnake\Downloads...
```

Ilustración 42 Obtención de Flag del Reto.

Fuente: Autores

Ya con nuestro hash, en este caso de tipo SHA1, nos dirigiremos al reto y lo

agregaremos en el campo solicitado, con la estructura definida en la plataforma.

Ilustración 43 Estructura Flag solicitada por la Plataforma.

Fuente: Autores

Comprobamos que la Flag, sea correcta, por medio del botón, submit.

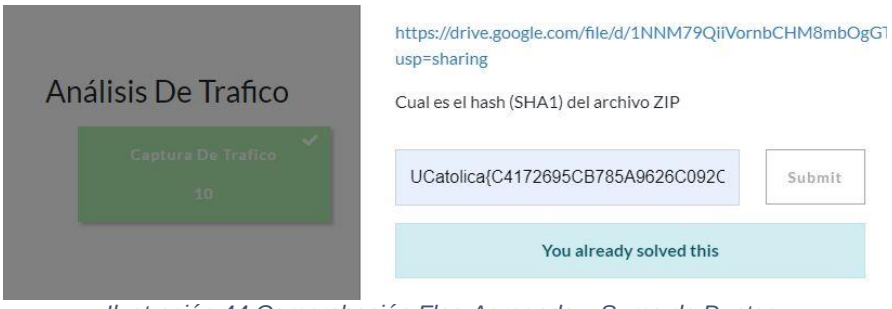

Ilustración 44 Comprobación Flag Agregada y Suma de Puntos.

Fuente: Autores

En donde nos muestra que el resultado es satisfactorio, comentando que es correcto el parámetro ingresado, y otorgando los puntos del reto.

Cada vez que se concluya un reto y aprobando este, la casilla correspondiente al reto será marcada y otorgado los puntos definidos bajo su nivel de complejidad, esto definido por el creados y/o administrador de la plataforma

Ilustración 45 Retos Aprobados.
Fuente: Autores

Como se mencionó en capítulos anteriores, cada estudiante podrá observar sus estadísticas dentro de la plataforma, sus retos culminados, puntos obtenidos, categorías con mayor y menor participación y a su vez los errores presentados al introducir la bandera de finalización del reto, permitiendo no solo medirse en sus aspectos positivos, sino fortalecer sus puntos negativos.

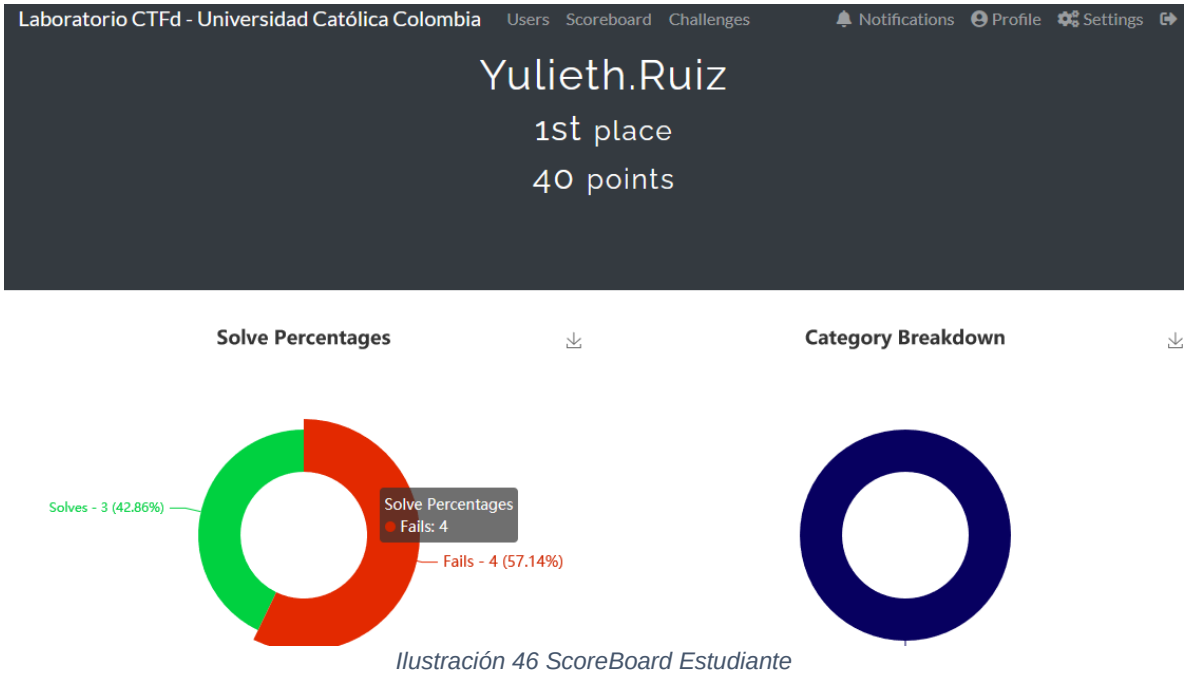

Ilustración 46 ScoreBoard Estudiante
Fuente: Autores

12.6 MECANISMO Y MOTIVACIÓN

En el desarrollo de la propuesta del laboratorio, se ha parametrizado un sistema que permita al estudiante/egresado conocer su desempeño en la plataforma, esto mediante un scoreboard o tablero de puntuación.

Este ScoreBoard, tendrá un límite de participantes en el, y el reto e incentivo de los estudiantes es estar dentro de las 10 primeras posiciones, adicional, los estudiantes que se encuentren en las 10 primeras posiciones se esforzaran para poder escalar cada vez más en el top de la plataforma.

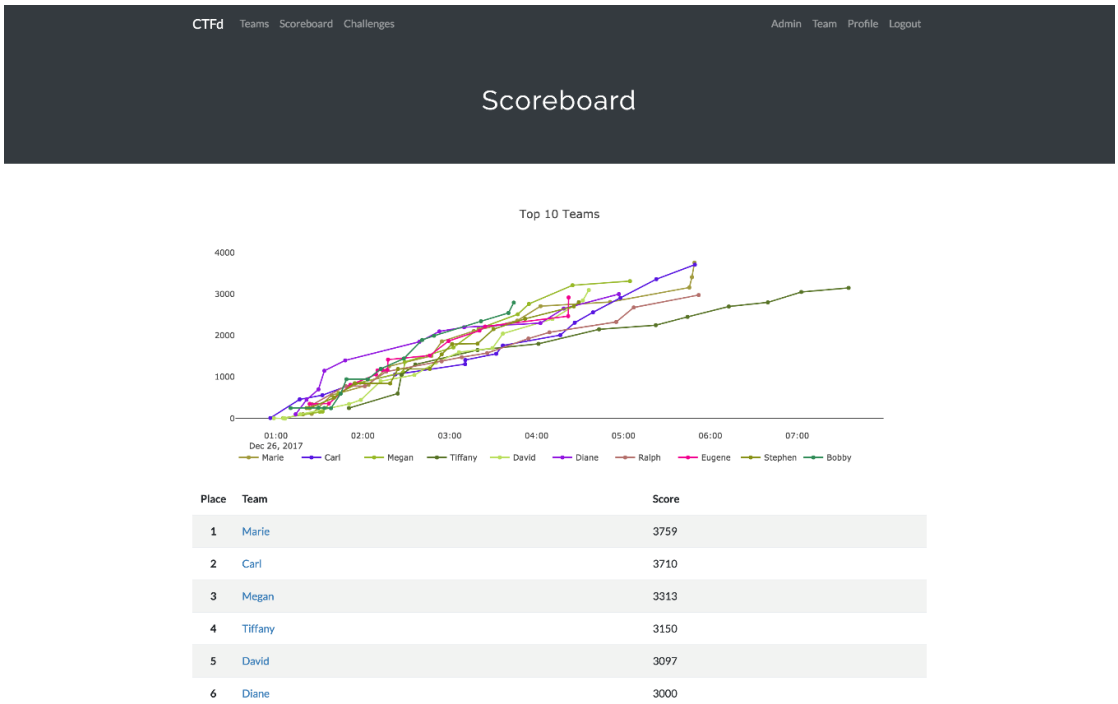

Ilustración 47 ScoreBoard Framework.
Fuente: Autores

La plataforma brinda un reporte dentro del perfil del usuario que permite conocer su desempeño individual, visualizando las categorías que mejor se ha desempeñado, sus respuestas erróneas y correctas de los retos, su puntuación total y su ranking dentro de la plataforma, si este no se encuentra dentro del Top 10.

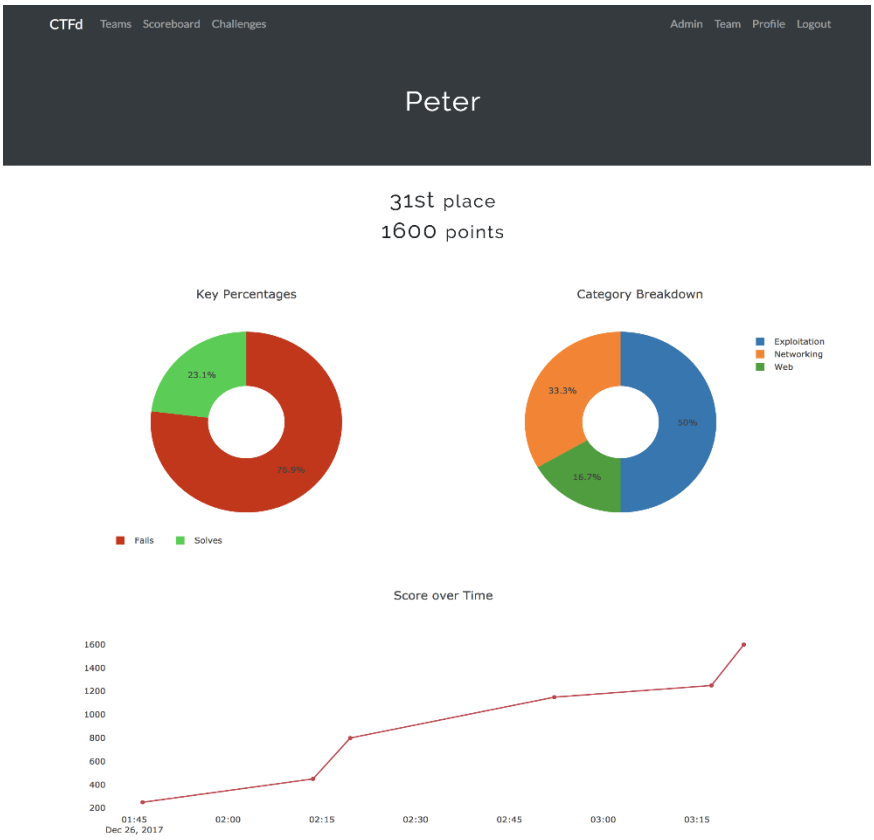

Ilustración 48 Reporte Usuario Framework.

Fuente: Autores

Los usuarios que avancen en la plataforma, que completen los retos de forma satisfactoria se les permitirá bajo ciertos criterios la posibilidad de cargar retos a la plataforma, alguno de los criterios abordados en esta propuesta son los siguientes:

- Completar los retos del nivel donde se quiere realizar el aporte.
- El reto que se quiera agregar debe pertenecer a la categoría completada.
- Diligenciamiento de la plantilla, que permita medir si el reto corresponde o no al nivel de dificultad.
- Solución del reto, donde se evidencie la Flag, que debe ser ingresada para completar el reto.
- Aprobación de un administrador o moderador de la plataforma.

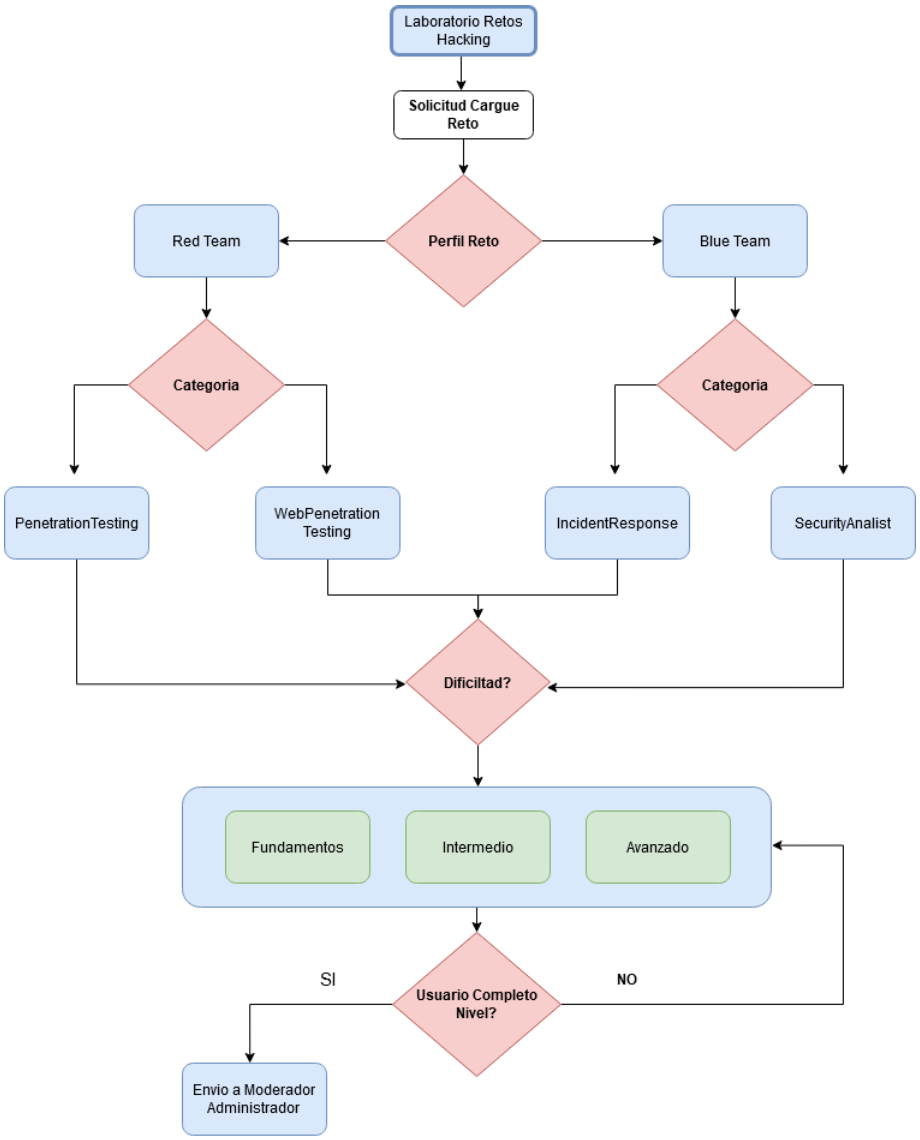

Ilustración 49 Pasos Cargue Reto.

Fuente: Autores

12.7 PLANTILLA CARACTERIZACIÓN DEL RETO

La siguiente plantilla permitirá en principio medir el reto y categorizarlo para poder cargarlo sobre la plataforma.

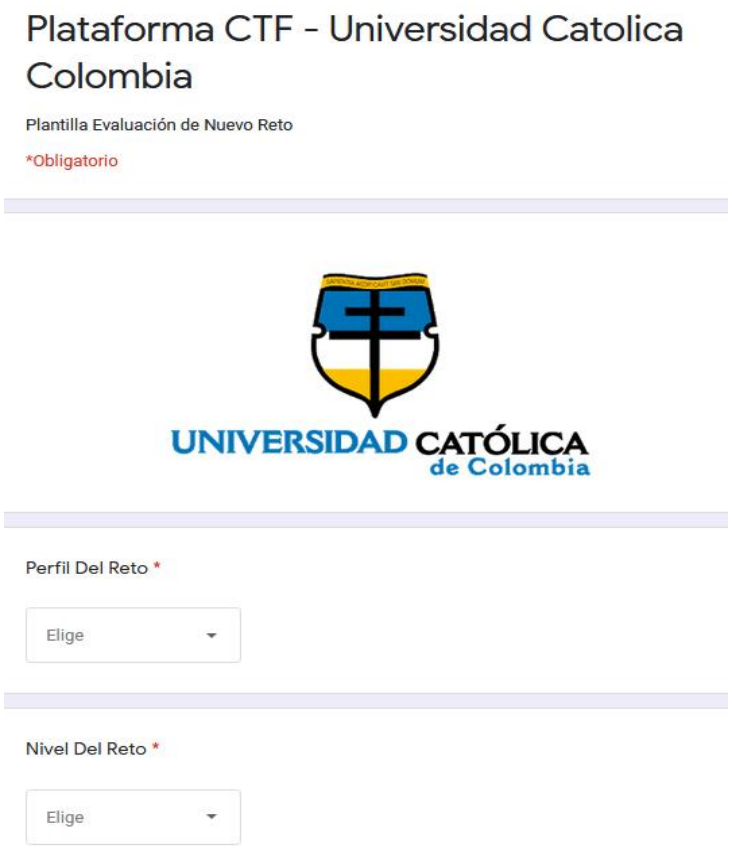

Ilustración 50 plantilla de caracterización del reto

Fuente: Autores

Categoría Red Team

- Seleccione La categoría Del Reto

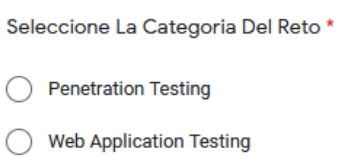

Ilustración 51 Red Team, Pregunta 1

Fuente: Autores

- Mencione la/las Fases que posee el Reto

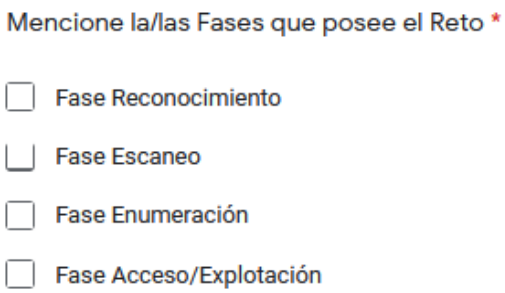

Ilustración 52 Red Team, Pregunta 2

Fuente: Autores

- Herramientas Necesarias Para la obtención de la Flag

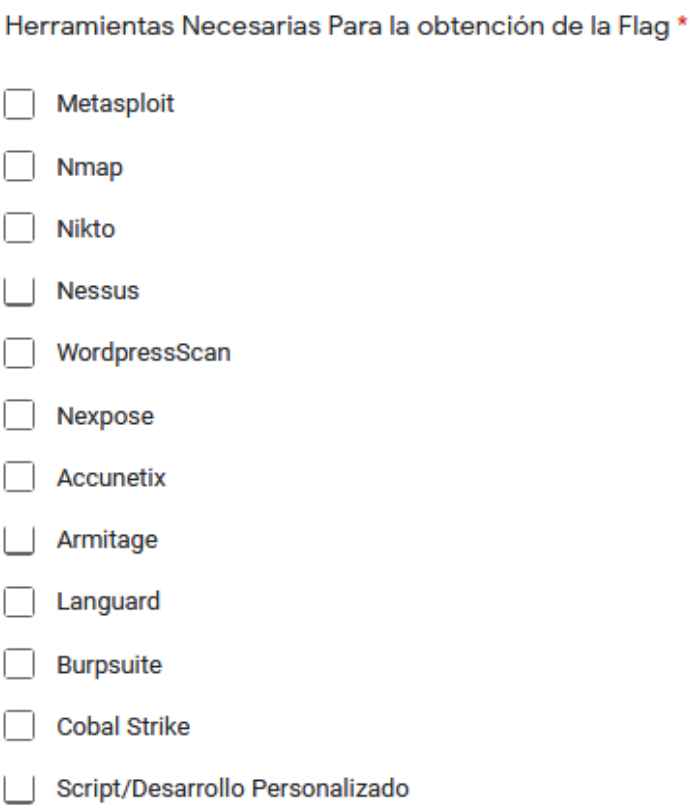

Ilustración 53 Red Team, Pregunta 3

Fuente: Autores

- Menciones El/Los Servicios Vulnerables

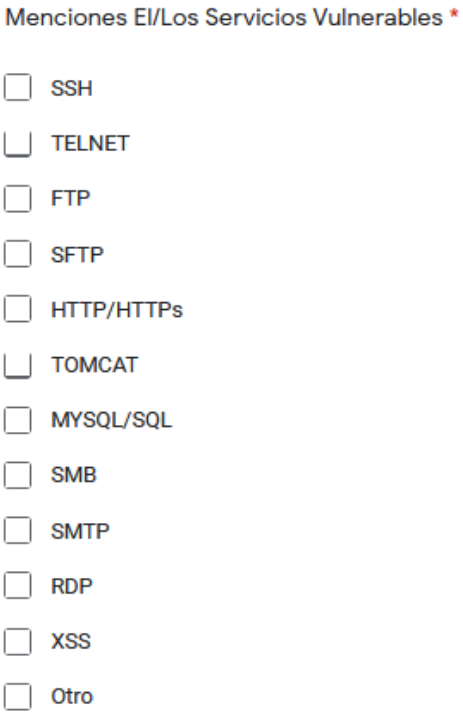

Ilustración 54 Red Team, Pregunta 4

Fuente: Autores

- Existe un Exploit para esta vulnerabilidad?

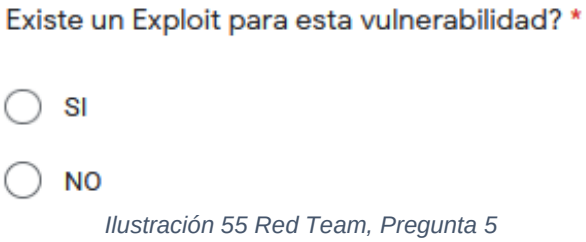

Ilustración 55 Red Team, Pregunta 5

Fuente: Autores

- El Reto requiere evasión de Antivirus?

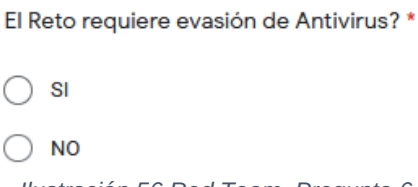

Ilustración 56 Red Team, Pregunta 6

Fuente: Autores

- Requiere escalamiento de Privilegios?

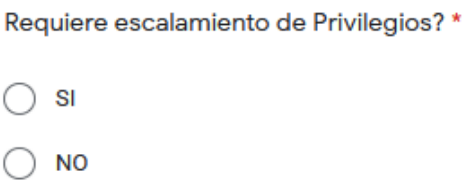

Ilustración 57 Red Team, Pregunta 7

Fuente: Autores

- Describa el reto, de una introducción, y nombre al reto.

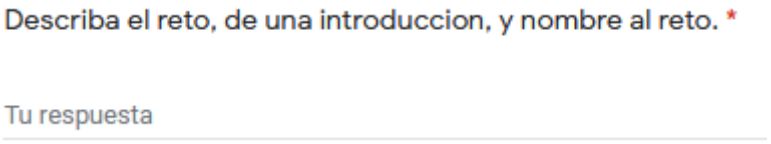

Ilustración 58 Red Team, Pregunta 8

Fuente: Autores

Categoría Blue Team

- Seleccione La categoría Del Reto

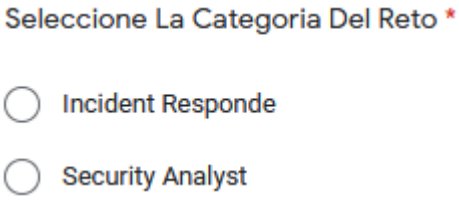

Ilustración 59 Blue Team, Pregunta 1

Fuente: Autores

- Mencione la/las Fases que posee el Reto

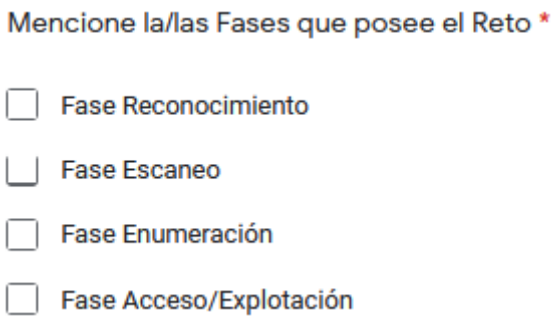

Ilustración 60 Blue Team, Pregunta 2

Fuente: Autores

- Escenario Del Reto

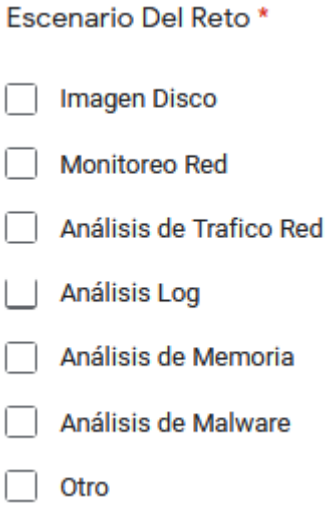

Ilustración 61 Blue Team, Pregunta 3

Fuente: Autores

- Herramientas Usadas en el Reto

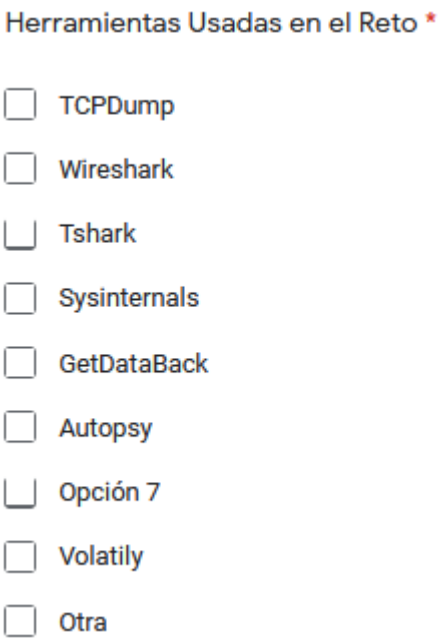

Ilustración 62 Blue Team, Pregunta 4

Fuente: Autores

* Describa el reto, de una introducción, y nombre al reto.

Ilustración 63 Blue Team, Pregunta 5

Fuente: Autores

13 NUEVAS ÁREAS DE ESTUDIO

El desarrollo de la propuesta pretende poder culminar el proyecto, por medio de unas fases adicionales y lineamientos a seguir que describiremos a continuación, para ser apropiados por los futuros compañeros que decidan continuar con la implementación del laboratorio de retos.

a. La implementación del proyecto por medio del modelo por capas permite que los recursos sean administrados de una manera eficiente, lo cual garantiza una mayor rapidez, escalabilidad y uso de los recursos.
b. El uso de contenedores permite una migración más ágil, rápida y segura, ya que todas sus dependencias se mantienen de un contenedor a otro.
c. La propuesta se basó en los perfiles más demandados y estándar de la industria en seguridad, los más requeridos por las compañías.
d. Las categorías agregadas al inicio de la propuesta son un inicio de la plataforma, pero se recomienda complementarlas, ya que las necesidades de la industria cambian cada día, temas especializados en forense y caza de amenazas, son las recomendaciones para nuevas fases de la implementación.
e. El uso de tecnologías en la nube, son una necesidad latente en las nuevas instalaciones e implementaciones para las empresas y proyectos, siguiendo las mejores prácticas en temas de seguridad, se fortifican los servicios expuestos y se minimizan las brechas de seguridad.
f. El uso de instancias bajo demanda garantiza que los recursos se usen cuando se requieren, por lo tanto, retos que impliquen un nivel de dificultad mayor, se recomienda sean implementados bajo esta modalidad.
g. La plataforma es por y para los estudiantes, por tal motivo, recomendamos se agregue única y exclusivamente el uso del dominio de la universidad para el login de la plataforma.
h. La plantilla de medición de los retos sirve como medida de control para el insumo de retos de la plataforma, se debe incentivar su uso, para medir el entusiasmo de la plataforma con los estudiantes.

14 CONCLUSIONES

Con la realización del presente proyecto y la investigación que se llevó a cabo, se pudo identificar que por medio del desarrollo de la propuesta de una plataforma web de retos de hacking ético y la prueba de concepto definida en el desarrollo, se puede concluir que:

A. La metodología propuesta brinda a los estudiantes, la oportunidad de ser profesionales multidisciplinarios, permitiendo desenvolverse en diferentes ramas, dando así un valor adicional a sus carreras.

B. La segmentación de las categorías por niveles brinda la oportunidad a los estudiantes, de adquirir conocimiento necesario para avanzar a un ritmo propio.

C. La oportunidad de ser parte de la plataforma, no solo como usuario, sino como creador de contenido, permite generar mayor expectativa y aceptación dentro de la comunidad estudiantil.

D. El uso de tecnologías por medio de contenedores permite mayor control, eficiencia y facilidad a la hora de implementar proyectos de cualquier índole, permitiendo una migración en menor tiempo y esfuerzo.

E. Las ventajas que nos brinda la virtualización de los proveedores en la nube a través de las instancias por demanda permiten un ahorre de costos y mayor eficiencia de recursos a usar dentro del proyecto.

15 BIBLIOGRAFÍA

[1] ISACA. CSX Cybersecurity Fundamentals Study Guide, 2nd Edition. 2017. 200p.

[2] ISC². “Stategies for Building and Growing Strong Cybersecurity Teams. Cibersecurity Workforce Study 2019”. [En Línea]. Disponible desde Internet en: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482 [Con acceso el 26-03-2020]

[3] ManpowerGroup. “Escasez de Talento 2020: Cerrando la brecha de habilidades: lo que los trabajadores quieren”. [En Línea]. Disponible desde internet en: https://manpowergroupcolombia.co/wp-content/uploads/dlm_uploads/Estudio-Escasez-de-Talento-2020-final-1.pdf [Con acceso el 15-04-2020]

[4] Educación/Vida. Los Talentos que requieren urgentemente los empresarios del país. En: El Tiempo. Bogotá: (14, febrero, 2020). Disponible desde internet en: https://www.eltiempo.com/vida/educacion/los-talentos-que-requieren-urgentemente-los-empresarios-del-pais-segun-manpowergroup-460674 [Con acceso el 27-03-2020]

[5] KOLB, A. and KOLB D. A. “The Theory of Experiential Learning”. [En Línea]. Disponible desde Internet en: https://www.scss.tcd.ie/disciplines/information_systems/crite/crite_web/lpr/teaching/kolb.html [Con acceso el 12-03-2020]

[6] GOMEZ, Pawelek Jeremías, “El aprendizaje Experiencial” Universidad de Buenos Aires, Facultad de Psicología. Materia: Capacitación y Desarrollo en las Organizaciones” Disponible desde internet en: https://www.ecominga.uqam.ca/PDF/BIBLIOGRAPHIE/GUIDE_LECTURE_5/1/3.Gomez_Pawelek.pdf [Con acceso el 18-03-2020]

[7] DE LA ROCA, Mónica. 01-03-2019. Vinculando teoría y práctica a través de una secuencia de actividades de aprendizaje en un MOOC. [En Línea]. Disponible desde Internet en: http://biblioteca.galileo.edu/tesario/handle/123456789/778 [Con acceso el 05-02-2020]

[8] CONGRESO DE LA REPUBLICA. COLOMBIA, «LEY 1273 DE 2009» De la Protección de la información y de los datos. [En Línea]. Disponible desde Internet en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_

2009.pdf [Con acceso el 02-04-2020]

[9] MINTIC. 11, abril 2016. «Política Nacional de Seguridad Digital, CONPES 3854» [En Línea]. Disponible desde Internet en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf [Con acceso el 30-03-2020]

[10] The White House. 09, febrero 2016. FACT SHEET: Cybersecurity National Action Plan. [En Línea]. Disponible desde Internet en: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan [Con acceso el 18-04-2020]

[11] MINISTRY, Communication and Information Technology. 02, Julio 2013. «National Cyber Security Policy - 2013» [En Linea]. Disponible desde Internet en: https://meity.gov.in/sites/upload_files/dit/files/National%20Cyber%20Security%20Policy%20%281%29.pdf [Con acceso el 18-04-2020]

[12] UNIMINUTO, Tecnología en Gestión de Seguridad en Redes de Computadores. [En Linea]. Disponible desde Internet en: http://www.uniminuto.edu/web/programasacademicos/tecnologias/-/programa/Bogot%C3%A1+calle+80+Presencial/tgsc-104929 [Con acceso el 28-04-2020]

[13] Technocio. 12, noviembre 2019. Fortinet y el Politécnico Gran Colombiano firman alianza para suplir escasez de Profesionales en Ciberseguridad. [En Linea]. Disponible desde Internet en: http://technocio.com/fortinet-y-el-politecnico-grancolombiano-firman-alianza-para-suplir-escasez-de-profesionales-en-ciberseguridad/ [Con acceso el 10-04-2020]

[14] VARGAS, Gladys. El Aprendizaje basado en problemas: Una Metodología basada en la vida real. [En Linea]. Disponible desde Internet en: https://www.magisterio.com.co/articulo/el-aprendizaje-basado-en-problemas-una-metodologia-basada-en-la-vida-real [Con acceso el 19-03-2020]

[15] HIMANEN, Pekka. La ética del hacker y el espíritu de la era de la información. 2001. 166p.

[16] Revista GAHCARNA GACHARNA, Federico. ACIS. Mitos del Hacking. En: Asociación Colombiana De Ingenieros de Sistemas. Bogotá. 2012. [En Linea] Disponible desde Internet en: http://acistente.acis.org.co/typo43/fileadmin/Revista_123/Dos.pdf [Con acceso el 12-04-2020]

[17] HECTOR Jara y PACHECO Federico. Ethical Hacking 2.0: Implementación de un sistema para la gestión de la seguridad. P19. [En Linea]. Disponible desde Internet en: https://books.google.com.co/books?id=PkDCIzakkB4C&lpg=PA4&ots=B4A85NA58y&dq=significado%20hacker%20%2B%20articulo%20cientifico&lr&hl=es&pg=PA1#v=onepage&q&f=false [Con acceso el 20-03-2020]

[18] BCC, Conferenciantes. Kevin Mitnick: El más famoso Hacker del Mundo. [En Linea]. Disponible desde Internet en: https://grupobcc.com/co/speakers/kevin-mitnick/ [Con acceso el 15-04-2020]

[19] LIBYA. International Conferencia on Technical Sciences. [En Linea]. Disponible desde Internet en: https://icts2019.tve.gov.ly/2019/en/index [Con acceso el 18-04-2020]

[20] A Younis, Younis & Kifayat, Kashif & Topham, Luke & Shi, Qi & Askwith, Bob. (04-06 marzo 2019). Teaching Ethical Hacking: Evaluating Students Levels of Achievements and Motivations. [En Lina]. Disponible desde Internet en: https://icts2019.tve.gov.ly/2019/PDF/PDFCI/CI3014.pdf [Con acceso el 18-04-2020]

[21] SANDOVAL, Lucia y VACA, Andrea. Implantación De Técnicas Y Administración De Laboratorio Para Investigación De Ethical Hacking. SANGOLQUI, 2013, 128p. Trabajo de Grado (Ingeniero en Sistemas e informática). Escuela Politécnica Del Ejercito. Departamento de Ciencias de la Computación.

[22] Méndez Gijón, Florentino y Robles, Adrián y Ronquillo, Armando y Valdez Besares, José. Técnicas de Hacking Ético en un Laboratorio de Pentesting Virtualizado. OAXACA, 2014. [En Linea]. Disponible desde Internet en: https://www.researchgate.net/publication/308312418_Tecnicas_de_Hacking_Etico_en_un_Laboratorio_de_Pentesting_Virtualizado [Con acceso el 20-04-2020]

[23] ICONTEC, 22, marzo 2006. Norma Técnica Colombiana. NTC-ISO/IEC 27001. [En Linea]. Disponible desde Internet en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf [Con acceso el 19-04-2020]

[24] CONGRESO DE LA REPUBLICA. COLOMBIA, «LEY 1341 DE 2009» Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC -, se crea la agencia nacional de espectro y se dictan otras disposiciones. [En Línea]. Disponible desde Internet en: https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_

2009.pdf [Con acceso el 02-04-2020]

[25] CONGRESO DE LA REPUBLICA. COLOMBIA, «LEY 1581 DE 2012» Por la cual se dictan disposiciones generales para la protección de datos personales. [En Linea]. Disponible desde Internet en: https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf [Con acceso el 02-04-2020]

[26] CANCILLERIA, COLOMBIA. «CONPES 3854 DE 2016» Política Nacional de Seguridad Digital. [En Linea]. Disponible desde Internet en: https://www.cancilleria.gov.co/sites/default/files/planeacion_estrategica/conpes_3854_-_seguridad_digital.pdf [Con acceso el 04-04-2020]

[27] LOPEZ, Pedro y FACHELLI, Sandra. Metodología de la investigación social cuantitativa. 2015. [En Linea]. Disponible desde Internet en: https://ddd.uab.cat/pub/caplli/2016/163567/metinvsoccua_a2016_cap2-3.pdf [Con acceso el 18-04-2020]

[28] MIESSLER, Daniel. The Difference Netween Red, Blue, And Purple Teams. 2020 [En Linea]. Disponible desde Internet en: https://danielmiessler.com/study/red-blue-purple-teams/ [Con acceso el 04-09-2020]

[29] S. D. M. Henríquez, «Programación en N capas,» 2010. [En línea]. Available: https://d1wqtxts1xzle7.cloudfront.net/40842810/a07v7n2.pdf?1450791046=&response-content-disposition=inline%3B+filename%3DProgramacion_por_capas.pdf&Expires=1605461295&Signature=WEvG8-lzvFb0PRb99UiP1SnifUk~3jdyiJ37PJjIgthqyLOTPaybqteZ8x0CHrKFjBRqyoKRaHiJgF.