Retos y competiciones

Doris Londoño
Master en seguridad de las TIC
TFM

Nombre Consultor/a
Nombre Profesor/a responsable de la asignatura

04/06/2018

C) Copyright

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Retos y competiciones*
Nombre del autor:	*Doris Londoño Londoño*
Nombre del consultor/a:	Victor Garcia Font
Nombre del PRA:	Trabajo final del Master
Fecha de entrega (mm/aaaa):	06/2018
Titulación::	*Master en seguridad de las TIC*
Área del Trabajo Final:	*Memorias*
Idioma del trabajo:	*Español*
Palabras clave	*Restos y competiciones*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

La ciberseguridad se ha convertido en una de las áreas con mayor acogida por los profesionales de las TIC; la formación competente es uno de los propósitos de cada uno de estos profesionales, por ello, los eventos, congresos y concursos de seguridad ahora son fuentes de formación, con seguidores de todo tipo.

Durante los últimos 20 años, el aumento de las competiciones ha sido significativa, beneficiando así, a las grandes industrias de seguridad informática.

Los juegos o retos llevados a cabo en las competiciones tienen como objetivo principal, probar las capacidades de cada uno de los competidores en forma práctica, poniendo en juego la experiencia y conocimientos previos. Estos retos, están diseñados para todo tipo de personas, aunque casi siempre se necesita tener un mínimo de habilidades generales en ciberseguridad o en algunas una de sus divisiones para afrontar estos desafíos.

En las entrevistas realizadas a profesionales de la ciberseguridad que compiten en los retos, se afirma que la gamificación en los diferentes entornos competitivos, es una forma de motivar a los participantes comprometidos con la superación profesional y personal; además de ser una gran experiencia de vida, los retos dan la oportunidad de fortalecer las competencias profesionales y en otros casos, un participante puede ser reclutado parte de grandes compañías de ciberseguridad como resultado de su desempeño en la competición.

Abstract (in English, 250 words or less):

Training is one of the purposes of these professionals, therefore, events, congresses and security competitions are now sources of training with followers of all kinds.

During the last 20 years, the increase in competitions has been significant, benefiting the large IT security industries.

Games or challenges carried out in the competitions have as main objective, to test the capabilities of each competitor in a practical way, putting in play the their previous experience and knowledge. These contests are designed for all types of people, although almost always is needed to have a minimum of general skills in cybersecurity or in some of its divisions to face them.

In the interviews carried out with cybersecurity professionals who compete in the challenges, it is affirmed that the gamification in the different competitive environments is a way of motivating the participants committed to professional and personal improvement. In addition to being a great experience of life, challenges give the opportunity to strengthen professional skills and in other cases, a contestant can be recruited from large cybersecurity companies as a result of their performance in the competition.

Índice

1. Introducción

Una de las áreas de la tecnología que más fuerza ha venido adquiriendo es la seguridad de TI. El incremento de ataques y amenazas del ciberespionaje son los que más han alertado a las compañías, lo que los obliga a invertir en profesionales de seguridad con las capacidades de enfrentar el día a día y evitar caer en las manos de criminales informáticos.

La seguridad en tecnología se ha convertido en inversión de competencia y un punto clave en la continuidad del negocio.

La seguridad de las tecnologías de la información comprende categorías, tales como: criptografía, programación, hacking web, esteganografía, análisis forense, explotación, auditoria, reversing, comercio electrónico, análisis de tráfico, vulnerabilidades, aspectos legales, entre otros; muchas de estas categorías hacen parte de los retos que se llevan a cabo en las competiciones de ciberseguridad, profesionales y principiantes se enfrentan para demostrar sus habilidades, ganar créditos y en alguno casos hasta lograr una certificación como es el caso de Offensive Security (creadores de Kali) que utilizan retos de Capture the Flag para certificar profesionales en pentesting (Certificaciones OSCP, OSCE).

La profundidad y aporte del aprendizaje que se obtiene en los juegos de ciberseguridad o CTF pueden ser métodos de preparación de profesionales que aspiran llegar a ser parte de las grandes compañías de seguridad de TI.

1.1. Contexto y justificación del Trabajo

Los retos de ciberseguridad para mí son un tema de gran importancia porque aun siendo llamados "juegos" que traduce diversión, tienen como objetivo entregar conocimiento que se convierte en una herramienta para enfrentar uno de los grandes problemas que nos amenaza en la actualidad como son los ataques de ciberseguridad.

1.1.1. Alcance

Este trabajo final de Master inicia con la investigación y consultas en la web que me permitan profundizar e incursionar en el mundo de los retos de ciberseguridad que son llevado a cabo en las diferentes competiciones, aclarar panoramas, dudas y supuestos existentes en cuanto a lo que a estos se refiere, conocer su historia, identificar las categorías que son tenidas en cuenta para este tipo de eventos y cuáles no, investigar lo que logra un profesional de seguridad en TI cuando toma la decisión

de hacer parte de esta experiencia, así como indagar en qué sucede con su perfil profesional después de esta gran experiencia.

1.1.2. **Entregables/Logros**

Los resultados que espero obtener al final del TFM de consulta e investigación son los siguientes:

- ✓ Habré logrado mi propósito de conocer los diferentes retos de ciberseguridad que se llevan a cabo en las competiciones, además de los eventos, congresos y organizaciones en las que se reúnen personas con ideas y mundos diferentes pero que abordan un solo propósito de ser los mejores porque es una competencia.

- ✓ Conoceré la diferencia entre cada uno de los retos, podré interactuar con personas que han vivido estás experiencias y tal vez en un futuro no muy lejano con la motivación adquirida en este proceso, me estaré animando a hacer parte de esta gran experiencia.

- ✓ Finalmente tendré información muy importante para elaborar un entregable a la asignatura, incluyendo las conclusiones y vídeo de los momentos más emotivos del desarrollo del TFM.

1.2. **Objetivos del Trabajo**

Los objetivos propuestos para este TFM, están enfocados en la investigación a profundidad que llevará a resolver las inquietudes de lo "qué son" y "para qué son" los retos de ciberseguridad; los principales objetivos son:

- ✓ Identificar cada uno de los retos de ciberseguridad.

- ✓ Investigar a fondo sobre la experiencia que se vive en las competiciones de los diferentes retos de ciberseguridad.

- ✓ Identificar si existen áreas de conocimiento sobreutilizadas en estos retos de ciberseguridad y si hay áreas de conocimiento en seguridad que no tienen retos aún.

- ✓ Conocer qué tipo de personas son las que se animan a participar de estos retos de ciberseguridad y que es lo que más los motiva a hacerlo.

- ✓ Clasificar su nivel de importancia y que tanto podrán influir en un futuro tanto para los participantes como para las industrias que tienen relación directa con la seguridad de las TI, así como los clientes que hacen uso de sus servicios.

1.3. **Enfoque y método seguido**

Obtener la información necesaria para cumplir los logros propuestos, requiere de la aplicación de una metodología direccionada a resultados positivos; ésta metodología será desarrollada en las siguientes etapas:

- ✓ Levantamiento exhaustivo de información, obtenido desde los diferentes retos de ciberseguridad organizados en eventos y conferencias como el DEFCON.

- ✓ Consultar en la web sobre los retos de ciberseguridad que los que se encuentran en los diferentes sitios destinados para este fin.

- ✓ Investigar sobre los retos de ciberseguridad que tienen como objetivo formar profesionales con certificaciones competentes en la industria de seguridad de las TI.

- ✓ Tener un acercamiento con participantes de retos de ciberseguridad que han tenido la experiencia de participar en os diferentes retos.

- ✓ Categorizar y clasificar la información para obtener las conclusiones requeridas en el objetivo general propuesto para el TFM desde la asignatura

1.4. **Planificación del Trabajo**

1.4.1. **Tareas**

Las tareas que se llevarán a cabo para el desarrollo de la metodología descrita y alcanzar os objetivos propuestos son las siguientes:

1. Realizar las consultas en la Web sobre los diferentes tipos de retos de ciberseguridad.

2. Clasificar la información obtenida y detallar cada uno de los retos de ciberseguridad identificados en las investigaciones.

3. Consultar e identificar las áreas de seguridad en las que son desarrollados los retos de ciberseguridad.

4. Clasificar las diferentes áreas obtenidas en la investigación de la tarea anterior, para determinar si existen algunas de estas que están siendo sobreutilizadas y en cuales aún no existen retos de ciberseguridad.

5. Realizar un cuestionado basado en la información obtenida y entrevistar participantes de retos de ciberseguridad.

6. Sacar las conclusiones de la investigación.

7. Clasificar información y material para el video entregable.

8. Realizar el vídeo solicitado por la asignatura del TFM.

1.4.2. **Recursos necesarios**

Para el correcto desarrollo de la TFM elegida "retos y competiciones", será necesario contar con la disponibilidad de los siguientes recursos:

- ✓ Computador funcional
- ✓ Navegación a Internet
- ✓ Participantes con experiencia en los diferentes retos de ciberseguridad
- ✓ Editores de texto
- ✓ Software multimedia
- ✓ Dispositivo de vídeo

1.4.3. **Riesgos/limitaciones**

En todos los proyectos existen riesgos y limitaciones que deberán ser enfrentados, y para ello se deben tener planes de contingencia, recursos opcionales que permitan llevar a cabo los objetivos propuestos; algunos de estos pueden ser:

- ✓ Información insuficiente en los diferentes recursos de la Web.
- ✓ Limitaciones para contactar los participantes de los retos de ciberseguridad para realizar las entrevistas.
- ✓ Daño o pérdida del hardware disponible para el desarrollo de las actividades.
- ✓ Daño o perdida de la información recolectada.
- ✓ Limitación de tiempo para cumplir las metas propuestas en el desarrollo de las tareas.

1.4.4. **Plan de trabajo**

El archivo anexo incluye las tareas, fechas de entrega y demás detalles del plan de trabajo.

DorisLondono-TFM_PEC4\DorisLondono-PlanDeTrabajo.xlsx

2. **Breve sumario de productos obtenidos**

La cultura de la seguridad de TI ha crecido en todo el mundo los últimos años, la época de esperar que se llegue el momento de tener grandes eventos de seguridad ya pasó a la historia; para hoy, hablar de eventos, capacitaciones, congresos y concursos de seguridad se ha convertido en un tema fácil, entretenido e interactivo en cualquier mesa.
Retos como CTF que es totalmente legal y está dirigido a hackers que quieran demostrar sus habilidades, mejorar técnicas enfrentados a profesionales del mismo nivel, aun siendo costoso es de los más reconocidos en el mundo.
Sitios como ATENEA están diseñados para demostrar destrezas y habilidad en los desafíos de seguridad; su aporte al conocimiento está basado en permitir que todos los que tengan inquietudes de ciberseguridad pongan a prueba sus conocimientos.
Algo que sin duda tiene que ser resaltado en este punto son aquellos retos de ciberseguridad, que además de poner a prueba los conocimientos de los competidores, da la oportunidad a profesionales de fortalecer su perfil, con certificaciones en pentesting, como es el caso de Offensive Security con retos de Capture the Flag.
Sin embargo, no siempre las cosas se hacen bien en estos retos, eventos, congresos o competiciones, como es el caso de los que cobran al participante, pues se debería conseguir patrocinadores que se encarguen del financiamiento, premios y demás gastos del Wargame, CTF o reto de seguridad; las bases no son claras o tienen un foco perdido de la realidad, los participantes encuentran un información en la metodología y retos que da pie a equivocaciones; no se preocupan por la seguridad, siendo un reto de seguridad hay que tener conciencia de que muchos de los participantes, curiosos o interesados son expertos en seguridad y que los sitios expuestos para ofrecer el evento es vulnerable a ataques, y ellos podrán llegar al punto de ganar ventajas en el juego.

2.1. **Información clasificada**

Hace más de 20 años el aumento de las competiciones en seguridad informática ha sido significativo, beneficiando así a las grandes industrias de seguridad con los participantes de los diferentes retos.

El objetivo principal de los diferentes tipos de restos de ciberseguridad, es probar las capacidades sobre la seguridad informática de cada uno de los participantes, en forma práctica poniendo en juego la experiencia y conocimientos previos. Por lo tanto, se requiere que el participante tenga un mínimo de habilidades de ciberseguridad o alguna base en las ramas de conocimiento, que le permita el entendimiento y desarrollo de los diferentes retos.

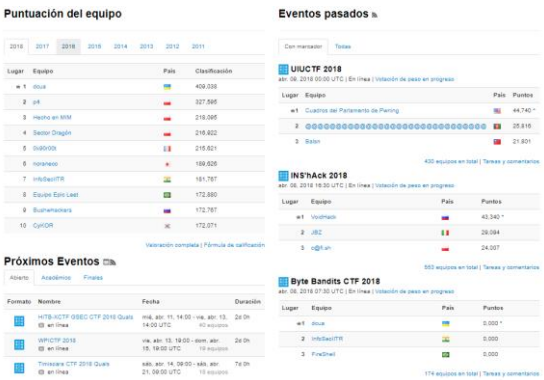
Para los menos experimentados hay competiciones que incluyen ideas o pistas de los desafíos.

2.2. **Retos/juegos de ciberseguridad**

2.2.1. **Capture The Flag (CTF)**

La gamificación dentro de este entorno competitivo es una forma de incentivar y motivar a los participantes a continuar con su formación comprometidos con la superación profesional y personal. Las competiciones de estilo Capture The Flag (CTF) han sido la forma adecuada de inducir a los estudiantes que apenas comienzan en conceptos técnicos bastante diversos. (1)

Para este tipo de juegos los participantes se apoyan en los sitios donde se alberga información subida por los participantes, éstos suministran material valioso con las soluciones de los problemas. Uno de estos sitios es el CTF Time (2), siendo el más conocido, incluye competiciones al estilo CTF públicas, privadas, activas, próximas y archivadas.



Los recursos presentados para el CTF deben ser muy atractivos, debido a que hay alumnos con diversos niveles de conocimientos, interés y habilidades.
Los modos de juego son:

ESTILO	DESCRIPCION/TEMATICA	DIFICULTAD
Jeopardy	Este estilo es el más extendido de todos, incluye una cantidad de retos con temáticas variadas, ya sea de individual o en equipo, se deben encontrar banderas ocultas en un entorno parcialmente conocido y dar evidencia del logro del objetivo, el tiempo de acceso es limitado, el indicador de que la bandera que se ha alcanzado es legitima suele ser una cadena de caracteres que siguen un orden concreto, p.e. "flag{ [random key] }" y cuya clave sea lo suficientemente extensa para garantizar que no fue obtenida mediante la fuerza bruta. Cuando se obtiene la clave se confirma con la herramienta de puntuación y se asignan los puntos del reto superado, sumándolos al marcador que le corresponde; el ganador es quién adquiere más puntos al finalizar la competición. La solución de los retos es de todo o nada, al finalizar la mayoría de los participantes publican sus resultados, lo que genera mucha sinergia entre los participantes haciendo que las competiciones crezcan al igual que la formación que adquieren los participantes. Las temáticas más utilizadas en este tipo de reto de ciberseguridad son: ingeniería inversa, criptografía, forense, explotación web, redes, scrpting, esteganografia.	Avanzada
Attack-Defense	Es una modalidad de juego en equipos, el organizador de la competición proporciona una red cerrada y un servidor por equipos que contiene vulnerabilidades deliberadamente, la configuración inicial de todos los equipos es igual y ejecutan una serie de servicios personalizados, en éstos es donde se encuentran las fallas, cada uno de los equipos defiende su servidor encontrando las fallas para corregirlas y ataca las fallas no parcheadas de sus rivales, el objetivo del reto es hurtar las bandejas alojadas en los servidores de los rivales y entregarlas a los jurados para que las validen	Media
King of the Hill	En este reto de ciberseguridad, los equipos participantes intentan ganar el control de un servidor vulnerable y mantenerlo bajo su propiedad frente a los demás participantes por el mayor tiempo que le sea posible, con el fin de obtener mayor puntaje.	Media

(3)

2.2.3. **Role play**

Este tipo de competición basada en ciberejercicios en los que participan diferentes países, son considerados ambientes simulados para la enseñanza. Son herramientas que permiten evaluar el estado de la preparación de los participantes para enfrentar la crisis de origen cibernético, fortaleciendo el aprendizaje con lecciones valiosas y recomendaciones que son útiles para el día a día.
Los sectores involucrados adquieren ganancia en el aumento de la defensa frente a ataques es una de las fortalezas de mejora en la concienciación y formación.
Entre los años 2002 y 2004 los ciberejercicios realizados redujeron, sin embargo, en los últimos años se ha incrementado.
La mayoría de los ciberejercicios que se han realizado tienen mayor fuera a nivel nacional. Esto es debido a que los primeros lanzamientos se realizan en una sola nación y no son extendidos a otras hasta no comprobar su grado de madurez.

Modalidad	Descripción	Dificultad
Tabletop	consisten en debates sobre hipotéticos escenarios en un ambiente informal, con el objetivo de evaluar los planes, las políticas y los procedimientos, o los sistemas necesarios para la prevención, respuesta y recuperación ante un determinado incidente	Baja
Escala real	Estos son más complejos, ya que involucran a diversas organizaciones y jurisdicciones, con el objetivo de validar muchos aspectos, como la implementación y el análisis de los planes, políticas, procedimientos y acuerdos de cooperación desarrollados en los ejercicios basados en debates	Avanzada

(4)

2.3. **Sitios para demostrar destrezas y habilidades**

Realizando una exploración en la Web, se encuentran múltiples de sitios que son diseñados para todo tipo de participantes de retos de ciberseguridad, a continuación, se mencionan los más populares.

ATENEA

- Es una plataforma de desafíos de seguridad del CCN-CERT que básicamente tiene como objetivos:
  - Concienciar
  - Involucrar
  - Atraer

GFoS

- Es un sitio web no comercial dirigido a todos los que están iniciando en el mundo de la seguridad informática. Presenta tres ejercicios con diferentes temáticas que tienen como objetivo ir incrementado el nivel de dificultad a medida que se avanza; estos son:
  - Comprometer un servidor FTP
  - Sitio privado y archivo cifrado
  - Rastreo digital

Captf

- Es un sitio web de enlaces de prácticas que permite encontrar una lista de sitios y herramientas al estilo CTF, tales como:
  - Juegos en línea en vivo
  - Juegos fuera de línea descargables
  - Máquinas virtuales
  - Archivados o históricos

Hacking Lab

- Es una plataforma online de piratería ética, redes informáticas y desafíos de seguridad dedicado a encontrar y educar talentos de ciberseguridad. Hacking Lab tiene como objetivo crear conciencia sobre el aumento de la educación y la ética en la seguridad de la información a través de una serie de competiciones cibernéticas que abarcan:
  - Ciencia forense
  - Criptografía
  - Ingeniería inversa
  - Piratería ética
  - Defensa

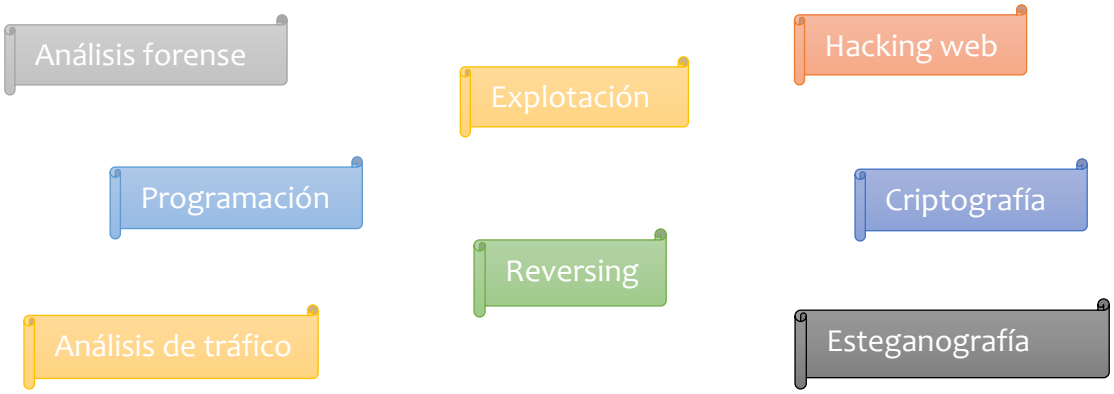
Ctf365

- Este sitio tiene claramente definidos sus objetivos dependiendo según los siguientes perfiles:
- Profesionales en seguridad: mejorar las habilidades defensivas, desarrollar nuevas estrategias de ataque, probar herramientas ofensivas o sus propios scripts, entre otros.
- Administradores de sistemas: entrenamiento de sus habilidades de seguridad defensiva, mitigación de riesgos, análisis de detección, entre otros.
- Desarrolladores de sitios de internet: ayudar a detectar vulnerabilidades en las aplicaciones web de código abierto, escribir códigos con buenas prácticas en seguridad, así como aplicaciones web más seguras.
- Es una plataforma de entrenamiento de seguridad que pone a prueba:
  - La piratería
  - Defensa de servidores propios
  - Ataques contra otros servidores

(5) (6) (7) (8) (9)

2.4. **Áreas implicadas**

Como se puede comprobar en la categorización de la información recopilada en las investigaciones, las áreas de la Seguridad de TI más empleadas en cada uno de los diferentes retos de ciberseguridad son:



3. **Entrevista**

Para conocer un poco más sobre los restos de ciberseguridad, se realizó una entrevista a Giovanni Chacón, auditor de seguridad informática de EPM y docente de Catedra de universidades de la ciudad de Medellín Colombia.

3.1 **Cuestionario**

- ¿Qué te motivó a participar en los retos de ciberseguridad?

"La motivación para participar en estos juegos de ciberseguridad o CTF´s, yo creo que las podría resumir en dos, es básicamente pasión, cuando estás motivado, cuando te gusta este tema a un nivel lo suficientemente alto, en el que termines involucrado en este tipo de juegos eso va a ser inevitable, porque son oportunidades de aprendizaje muy valiosas. Entonces, primero que todo por pasión, por gusto y segundo por conocimiento, porque una vez juegas uno, te das cuenta que el camino que se requiere para llegar a una respuesta te entrega una cantidad de conocimiento que de otra forma hubiera sido muy difícil"

- ¿Desde cuándo participas en retos de ciberseguridad?

"Yo creo que, desde hace más de ocho años, unos diez años atrás, no soy un participante lo suficientemente activo como otros, pero si me gusta, en lo medianamente posible siempre que puedo y tengo el suficiente tiempo participo"

- ¿Cuál era la expectativa que tenías antes de participar en los retos? ¿Sientes que se cumplió dicha expectativa?

"Yo creo que, uno se monta en este cuento sin ni siquiera a veces tener una expectativa muy clara, pero digamos, yo lo siento desde mi concepto muy personal, lo mío retrospectivamente ha sido una cuestión transparente, es decir, la comunidad de las personas con las que te rodeas, que están relacionados con todo ese tema de ciberseguridad, digamos que usted termina inverso en todo ese tema de juegos o CTF´s, juegos de ciberseguridad, War games de forma inevitable. Esto sin esperar nada a cambio a parte de conocimiento. En la mayoría de los casos la expectativa siempre se consigue al 100%, siempre hay un gana, gana"

- Giovanni, ¿Hablando de tus comienzos recuerdas tus primeros CTF´s, los hacías solo o fue en un equipo? ¿Recuerdas cómo fue manejar la frustración al comienzo de no poderlos solucionar rápidamente, cómo tú los esperabas, o que no eran tan fáciles cómo pensabas, o tal vez la dificultad era más alta de la que esperabas?

"Si, yo recuerdo en los inicios, incluso antes de entrar a la universidad, digamos que los seguía muy de forma individual, posteriormente al ingresar a la universidad empecé a conocer personas que estaban relacionados con el tema y que ahí ya se empieza a construir comunidad, a construir ese equipos de trabajo, ese grupo de amigos… Vagamente recuerdo uno en el que participé en Manizales, "Easy", un evento patrocinado por un grupo de personas del área de seguridad acá en Colombia, que recuerde, fue el primero que hicimos en grupo, fue muy emocionante, estuvimos a punto de ganar, al final nos ganó otro equipo por muy poco, quedamos de segundos, ese evento fue bastante grato, tengo muy buenos recuerdos. Efectivamente lo que dices acerca de la frustración, acerca de tratar de encontrar la mejor salida, la mejor forma de ver ese reto que te están poniendo, todo eso en algún momento te explota la mente, y uno definitivamente no vuele a ser la misma persona, ya después cambia la estructura mental, para abordar algún problema, es un poco adictivo porque esto, si bien es muy difícil y uno de los principales skill para enfrentarlo es la paciencia, el manejo de la frustración, es de las cosas que uno más aprecia y que uno puede desarrollar en este tipo de eventos"

- ¿Entonces según, esa experiencia prefieres los retos en equipo o individuales?

"Yo prefiero los retos grupales, pero la verdad es que es más complicado organizar un grupo y trabajar en equipo por cuestiones laborales, de tiempo, que la universidad, el estudio, todo eso, son muchos factores que evitan que uno pueda reunirse… Cuando se pueda y la medida de lo posible es mejor grupal, porque se comparte información, estás con todo el equipo, uno piensa de una forma el otro de otra y desde cada punto de vista se trata de solucionar, hasta que alguien encuentra una forma, la comparte y ya todos nos beneficiamos de ese conocimiento… No obstante, los individuales también son importantes, en la medida de que no pueda participar en los grupales lo importante es no perder el ritmo… Gracias a la tecnología de cierta forma también puedes hacerlo

grupal, pero lo importante es evitar perder el ritmo y compartir con las personas que quieren entrar a ese mundo y con los que tienen experiencia, aún más"

- Existen retos de larga y corta duración ¿Cuál ha sido el máximo y el mínimo de tiempo en el que has competido? ¿Cuál prefieres?

"Personalmente, me parecen mejor los retos cortos, tipo un día, dos días, tres días porque el 80% del equipo con el que he jugado trabaja… Entonces es interesante en los que se puede intercambiar de forma masiva con los compañeros. Los que son continuos también son muy importantes por el conocimiento, pero si es por hobbie prefiero los cortos"

- ¿Has usado tu experiencia y conocimiento para explorar maliciosamente los sitios web de las competiciones?

"Personalmente no… No quiere decir que no se le ocurra a uno, mientras está en un CTF evaluar dos tres cosas, pues, pruebas muy básicas, por ejemplo, que no exista un listado de directorios, o que puedas hacer la enumeración de usuarios, pues una cosa muy básicas, pero es algo muy puntual, incluso para protección de uno mismo, pero digamos de ahí a hacerlo algo más profundo, con más detalle no, eso necesariamente inmediatamente cambia el foco de los que estás haciendo, porque ya estás es atacando, evaluando o auditando… Yo personalmente me pongo a jugar un CTF, estoy es jugando, digamos que no lo haría, en ese momento con la presión y el tiempo encima, la mente está 100% enfocada en el reto"

- Sitios como CTF Time, alojan información valiosa de los diferentes retos que es suministrada por participantes. ¿Te gusta publicar los resultados en sitios como éste?

"Valoro mucho la información que se comparte, pero personalmente no lo he hecho"

- Desde tu punto de vista; ¿Crees que los retos son hechos para curiosos, estudiantes o profesionales? ¿Porqué?

"Digamos que la estructura de estos juegos, el objetivo permite que esa metodología se pueda aplicar a todo tipo de ambiente o de campo del saber, incluso en la ingeniería civil ingeniería química, vas resolviendo una seria de preguntas relacionada con el tema y de acuerdo a eso tienes unos puntos, no creo que existan límites para estos, veo los CTF´s como una metodología de enseñanza, de aprendizaje, de camarería, de construir conocimiento en equipo, creo que se puede utilizar cualquier otro campo "

- ¿Recomendarías a un estudiante ingresar al mundo de los retos de ciberseguridad?

"Absolutamente si, incluso creo que los docentes deberían utilizar esta técnica de enseñanza"

- En los últimos años, los ataques y amenazas del ciberespionaje se ha incrementado ¿Consideras que la formación en los retos de ciberseguridad, entrega valor para enfrentar dichos ataques y amenazas?

"*Para enfrentarlos si, hay diferentes tipos de CTF, desde el punto de vista de atacante, de personas que defienden, desde el punto de vista del análisis forense incluso, entonces, digamos que eso está englobado a todo el campo de la tecnología, entonces dependiendo del campo en el que seas experto, como jugador, vas a obtener una serie de herramientas y elementos que vas a replicar después en el lugar donde trabajas, por ejemplo si estás jugando en un War game y haces parte del* blue time *, entonces toda esa cantidad de conocimiento, destrezas y habilidades efectivamente las vas a poder utilizar en tu lugar de trabajo, lo mismo desde el punto de vista de los red time, también pueden ser utilizados para hacer evaluaciones y auditar la infraestructura donde laboras e incluso la propia"*

- ¿Podrías definir blue time y red time?

"*Hace un tiempo se ha venido trabajando con un concepto que se llama war games, por ejemplo, la firma Unix, dentro de sus recomendaciones incluyen la creación de procesos incluso dentro de las empresas que gestionan todos estos juegos de cyber guerra, entonces dentro de estos juegos como proceso organizacional están los blue time´s y red time´s. Los blue time´s, son grupo de personas que se dedican a detectar, analizar, contener todos los ataques que hacen los red time´s; entonces en consecuencia los red time´s, son grupo de personas que se dedican a realizar una serie de pruebas y de ataques desde todos los puntos de vista posibles... ataques en cualquiera de los elementos de una infraestructura tecnológica, digamos que son un grupo de expertos de un alto nivel que utilizan una gran cantidad de herramientas para poder hacer una intrusión u obtener algún tipo de información dentro de una empresa, pero todo enmarcado entre un ejercicio del gato y el ratón.*

- ¿Cuál de los sitios web diseñados para demostrar destrezas y habilidades en los retos de seguridad recomiendas?

"*Hay demasiados, en este momento se me viene a la mente hackthis.co.uk, que me parece muy didáctico…Incluso en Internet encuentras listas de sitios, para entrenamiento…"*

Para una persona de nivel introductorio se recomienda este sitio por ser muy didáctico, viene por niveles y vas subiendo a medida que vas avanzando.

- ¿Qué opinas de los organizadores que no tienen patrocinadores y cobran a los participantes?

"*Depende del nivel del evento…El tema de los CTF y todo el paquete de hacking, filosóficamente hablando es una iniciativa de software libre, de compartir de entregar,*

antes más que recibir… No estoy en contra de los que cobran, tendrán sus razones, pero lo que quiero llegar, es que no es común…"

- ¿Cuál área de conocimiento en seguridad, consideras más fuerte y retadora según tu experiencia?

"*Es relativo, pero de forma general, se podría ser que entre las áreas de conocimiento más relativamente complejas dependiendo de la persona que lo vea sería criptografía y reversing*"

- ¿Cuál ha sido tu competidor más fuerte?

"*Yo creo que el competidor más fuerte siempre somos nosotros mismos, nosotros con nosotros, que a veces, hay que libéranos de ciertos miedos, de ciertas limitaciones que nos hemos creado… Yendo a la práctica hay demasiada gente buena, que yo recuerde Fernando Quintero y Carlos Fernández, dos compañeros que considero muy buenos*"

¿Ellos son de Colombia? "*Si, de Medellín*"

- ¿Has tenido la oportunidad de conocer equipos o personas fuera de tu círculo social o personal, que se atrevan a afrontar estos retos y cómo lo hacen?

"*Hay mucha gente y equipos que he conocido, que son dignos de admirar por su trabajo individual y en grupo… Particularmente hay unos equipos, por ejemplo, uno en España… lo conozco desde un tiempo, por las publicaciones y los retos en los que ellos participan me parece interesante. Por ejemplo en DEFCON, en EEUU hacen anualmente una competición un CTF, donde participan los mejores equipos a través de una serie de selección, es curioso porque usted puede ver los participantes y uno espera una cantidad de personas diferentes, y cuando ves son adolescentes, por ahí de 16 años, muy jóvenes, también hay gente grande, pero la mayoría son jóvenes y hay obviamente también otra serie de competidores y grupos, incluso una vez armamos un grupo de forma muy rápida era un CTF particular en una charla de DEFCON y nos unimos un amigo de Colombia, otro muchacho de estados unidos que conocimos ahí, y ganamos dentro de esa competición, hay de todo; a lo que quiero llegar es que puedes armar equipos con cualquier tipo de persona y lo interesante es que nos une un solo objetivo, es digamos, muy interesante usted poder compartir en este tipo de ambientes con todas las personas que sea posible, armar equipos con persona de otros países, incluso este tema de los CTF´s tiene tanto, en los EEUU por ejemplo, no sé si en Europa también, pero en EEUU muchas empresas, por ejemplo, Amazon, ESET, estas empresas hacen sus propias competiciones y las usan como mecanismo para atracción o detección de talento, de acuerdo con los resultados del CTF si obtienes tantos puntos te dan un pase para que vayas a una pool pary en la noche en un lugar en las vegas y si tu puntaje definitivamente es muy bueno y tu rendimiento fue muy destacado… Me parece un método supremamente interesante porque las personas que participan no necesariamente tienen cierta cantidad de títulos,*

pero si tienen algo muy importante que necesitan las empresas, son personas que trabajan en equipo capaces de resolver problemas de seguridad, en conclusión, los CTF son una herramienta poderosa para la enseñanza y detectar personas para las empresas"

- ¿Tienes alguna certificación en pentesting?

"Si, tengo Certified Ethical Hacker y en este momento estoy estudiando para OSCP

- ¿Crees que tu perfil profesional creció después de participar en los retos de ciberseguridad?

"*Si, yo creo que la participación en los retos es uno de los elementos que le permite a uno mejorar su rendimiento… definitivamente estar inmerso en este tipo de retos, le entrega a uno muchos elementos para enfrentarse a problemas, que definitivamente vas a tener en muchos lugares."*

- ¿Cuál ha sido el reto de ciberseguridad que más te ha gustado? ¿Porqué?

"Fue hace como unos dos años, en el que participamos varios compañeros en una casa, duramos más de un día, de corrido jugando, fue muy interesante porque estábamos todos reunidos en un mismo lugar, el intercambio de información fue muy interesante se aprendió mucho, se divierte uno mucho, pasa un buen rato… eso es un gana, gana completo en ese tipo de competiciones"

¿Qué nombre tenía esa competición?

"Si no estoy mal, creo que era Cyberex"

- ¿Incluyes el aprendizaje obtenido en los retos, en tu vida laboral?

"Si, absolutamente, hay un conocimiento en particular, pero sobre todo la forma en la que abordas los problemas, es muy usado en el campo laboral"

- ¿Crees que los retos aportan en la formación de los ciberdelincuentes?

"*Es una pregunta difícil, pero empezaría diciendo que el objetivo de los CTF´s no es formar ciberdelincuentes, hay que partir de ese principio, el objetivo simplemente es divertirnos aprendiendo... Yo diría que probablemente algún ciberdelincuente se podrá ver beneficiado de toda esa experticia, y todos los elementos y estructura mental que se obtiene jugando en estos CTF´s, lo podría utilizar de forma maliciosa, eso es bastante difícil de controlar … Es una línea muy delgada, entre la ética y la delincuencia, entonces muy probablemente personas que están involucradas en este tema de ciberseguridad no sabemos cuántos de ellos pasen esa línea de la ética… Por ende, en algún momento podrían estar relacionados con los CTF´s, entonces es probable que pase eso"*

- ¿Cuándo vas a retos que otro tipo de cosas encuentras en estos eventos, además de los propios retos?

"*Viajar a otros países a participar d echarla so CTF´s exclusivamente es una experiencia muy enriquecedora, uno se monta en eso pensando en muchas cosas adicionales, como conocer esa cultura, conocer lugares, compartir con las personas o compañeros, compartir conocimiento, experiencias, hacer networking, conocer personas de otros países, intercambiar ideas, incluso a veces si tienes algo en mente muy probablemente una persona de otro país tiene los elementos, los conocimientos para ayudarte a apalancar esa idea… Los mismos CTF´s que son organizados por empresas les permiten conocer quiénes son los mejores, puedes conversar con ellos, es muy enriquecedora la experiencia*"

4. **Conclusiones**

- La ciberseguridad se ha convertido en un tema de discusión común, pasó de ser un tema pasajero a atraer la atención de todas las personas involucradas con tecnología, tanto profesionales del área como los que se benefician de ella.
- Los retos de ciberseguridad al estilo de CTF, son los más populares y reconocidos a nivel mundial.
- Cuando un organizador cobra a sus participantes deberá tener una razón justificable, puesto que, los retos de ciberseguridad hacen parte de la metodología del software libre, que es la que ha venido promoviendo todos los temas relacionados con hacking, por lo tanto, se debería acoger a esta y contar con patrocinadores.
- A pesar de que los sitios destinados para realizas los retos de ciberseguridad, son vulnerables, el objetivo de los participantes es participar del juego, dedicar el máximo de su esfuerzo a ganar y no se cree que piense en atacar o auditar el sitio malintencionadamente, puesto que perdería el foco de su objetivo.
- Cada reto de ciberseguridad se vive de una manera diferente con un mismo objetivo que es adquirir expertica y conocimiento muy valioso.
- Los CTF´s son una experiencia que todo profesional en ciberseguridad deberá incluir en su portafolio de aprendizaje.
- Todos los participantes tienen diferentes expectativas que en la mayoría de los casos se logra cumplir.
- Después de realizar la primera participación en los CTF´s, ya se querrá seguir participante, entran a ser parte de la vida de las personas que lo hacen.
- Además de diversión, los retos de ciberseguridad son un puente de contacto con empresas reconocidas en la industria que están en busca de talentos.
- Los participantes de grandes eventos de ciberseguridad en muchos de los casos para gran sorpresa, son adolescentes.

- El conocimiento que se adquiere en los retos de ciberseguridad es para toda la vida, se aprenden métodos para la resolución de problemas sin importar el área de conocimiento a la que perteneces.
- El trabajo en equipo además de ser divertido, aporta más conocimiento que el individual, permite intercambiar conocimiento, ideas y llegar a soluciones que quizá parecían imposibles de darse en el momento.
- Los centros educativos pueden adoptar metodologías de enseñanza para los estudiantes basados en retos como CTF´s o ciberejercicios.
- Los role play permiten identificar el estado de defensa que tienen cada uno de los países frente a las amenazas de seguridad.
- Internet se ha convertido en la principal fuente de información y medio de comunicación, ahora con los CTF´s y role play se puede comprobar que, siendo bien utilizado, puede aportar mucho al desarrollo de nuestros países ya sea de forma grupal o individual.
- Entre la ética profesional y la ciberdelincuencia hay una línea muy delgada.
- Para participar en los CTF´s solo necesitas ser apasionado y estar motivado a adquirir nuevos conocimientos.

4.1. **Reflexión**

Realizar las investigaciones para lograr los objetivos propuestos al inicio del TFM se pudo convertir en una ardua tarea, clasificar cada uno de los retos se convierte en un juego de interpretación de conceptos, puesto que prácticamente todos dicen lo mismo con diferentes palabras, no quería ser repetitiva pero tampoco alterar el significado de la redacción de cada uno de estos conceptos y descripciones, aun así, el objetivo inicial se pudo llevar a cabo.

Cuando estaba consultando me sumergía en el mundo de los retos de ciberseguridad, en un comienzo solo identifiqué los que son al estilo CTF y luego en una de las recomendaciones docente me hablaron de los role play, no sabía que existían, comenzando a leer me di cuenta que es un mundo más grande del que parece, que tomándolos en serio, los retos de ciberseguridad pueden crecer y tomar más fuerza. Deberían crear una estrategia de mercado que no los haga ver como un reto, si no, como un juego que además de divertir va a fomentar el conocimiento para llevar a la practica en la defensa de la tecnología frente a ataques y amenazas.

Para finalizar mi reflexión, hablaré un poco de la entrevista, tuve contacto con dos participantes de retos de ciberseguridad, uno de ellos además de participar, creaba retos, no fue posible realizar la entrevista porque su tiempo no lo permitió. El otro participante es Giovanni, un viejo conocido que no sabía hacia parte de este mundo, fue una experiencia muy agradable hablar con él sobre este tema, puesto que se es un gran profesional, un hombre inteligente y que le da aún más credibilidad a lo que es este mundo de la ciberseguridad y sus juegos de aprendizaje, hace que te imagines

la aventura y es casi un contador de historias con el que se tardarían días enteros para conocer cada uno de sus experiencias vividas. Con esta entrevista sigo motivada a seguir conociendo más e incluso teniendo la oportunidad quiero tener mi primer contacto a modo de evento cómo espectador y posteriormente como participante.

4.2. **Análisis crítico**

La metodología para llevar a cabo las investigaciones propuestas fue la correcta, los pasos planeados se siguieron como se habían aplaneado desde el comienzo puesto que uno dependía del otro.
Se inició con investigaciones y aclaración de conceptos, que era la guía para conducir la idea de lo que eran los retos de ciberseguridad, posteriormente la búsqueda de los participantes para realiza las entrevistas, que eran la fuente de alimentación principal del TFM, puesto que, así como la investigación en la Web es fundamental, conocer lo que se vive detrás de todo lo que hay escrito es realmente una aventura.
No se requirió aplicar ningún cambio a la metodología, solo fue necesario resaltar el riesgo levantado en la planificación del trabajo, cuando se identificaba incompatibilidad de tiempo para entrevistar a los participantes.

5. **Glosario**

- **Amazon:** organización, compañía o empresa de nacionalidad estadounidense encargada del comercio electrónico y servicios de cloud computing a diferentes niveles
- **Amenazas:** es cuando se materializa una vulnerabilidad independientemente de si se compromete o no el sistema.
- **Análisis forense**: se define como un conjunto de técnicas de recopilación y exhaustivo peritaje de datos, la cual sin modificación alguna podría ser utilizada para responder en algún tipo de incidente en un marco legal.
- **Ataques o ciberataque:** es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.
- **Blue time:** grupo de personas que se dedican a detectar, analizar, contener todos los ataques.
- **Ciberejercicios:** es una herramienta que permite evaluar el estado de preparación de los participantes frente a crisis de origen cibernético
- **Ciberespionaje:** es el acto o practica de obtener secretos sin el permiso del poseedor de la información.
- **Ciberseguridad:** es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático.

- **Cifrado:** es un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.
- **Concienciar:** es profundizar en el conocimiento de la realidad.
- **Criminales informáticos o ciberdelincuentes:** son personas que realizan actividades delictivas en internet como robar información, acceder a redes privadas, estafas, y todo lo que tiene que ver con los delitos e ilegalidad.
- **Criptografía:** es la ciencia que resguarda documentos y datos que actúa a través del uso de las cifras o códigos para escribir algo secreto en documentos y datos que se aplica a la información que circulan en las redes locales o en internet.
- **CTF (Capture the flag):** son un estilo de competición, generalmente en equipo, que se basa en diversas pruebas. Cada una de ellas nos da una serie de puntos en función de la dificultad o de otros criterios.
- **ESET:** es una compañía de seguridad informática establecida en Bratislava, Eslovaquia.
- **Esteganografía:** trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, de modo que no se perciba su existencia.
- **Gamificación:** es un tipo de aprendizaje que transpone la mecánica de los juegos al ámbito educativo-profesional con el fin de conseguir mejores resultados.
- **Hacking:** es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos
- **Kali Linux:** es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general.
- **Networking:** es una estrategia que consiste en ampliar nuestra red de contactos profesionales con el empleo de redes sociales de tipo profesional.
- **Offensive security:** es un enfoque proactivo y contradictorio para proteger los sistemas informáticos, las redes y las personas de los ataques.
- **Pentesting:** son una práctica para poner a prueba un sistema informático, red o aplicación web para encontrar vulnerabilidades que un atacante podría explotar.
- **Red time:** grupo de personas que se dedican a realizar una serie de pruebas y de ataques.
- **Role Play:** se conoce como técnica de dramatización, simulación o juego de roles.
- **FTP (File Transfer Protocol):** es un protocolo de transferencia de archivos entre sistemas conectados a una red TCP basado en la arquitectura cliente-servidor, de manera que desde un equipo cliente nos podemos conectar a un servidor para descargar archivos desde él o para enviarle nuestros propios archivos
- **Skill (habilidad):** es un tipo de trabajo o actividad que requiere entrenamiento y conocimiento especial-

- **Vulnerabilidad:** es una debilidad del sistema informático que puede ser utilizada para causar un daño.
- **War game (juego de guerra):** es una clase de juego de estrategia en donde, básicamente, dos equipos, por lo general controlados por un jugador cada uno, se enfrentan en un campo de batalla intentando obtener la victoria sobre el rival a través de la utilización de tácticas y estrategias.

(10) (11) (12) (13)

6. **Bibliografía**

(1). Obtenido de http://blondbyte.blogs.upv.es/2017/09/mi-primera-experiencia-en-una-con/
(2). Obtenido de https://ctftime.org/
(3). Obtenido de http://blondbyte.blogs.upv.es/2017/10/introduccion-a-las-competiciones-capture-the-flag-en-ciberseguridad/
(4). Obtenido de https://www.certsi.es/sites/default/files/contenidos/estudios/doc/incibe_taxonomia_ciberejercicios.pdf
(5.). Obtenido de https://www.ccn-cert.cni.es/cursos/atenea.html
(6). Obtenido de http://labs.gf0s.com/
(7). Obtenido de http://captf.com/practice-ctf/
(8). Obtenido de https://www.hacking-lab.com/about/
(9). Obtenido de https://ctf365.com/
(10). Obtenido de https://es.wikipedia.org/wiki/Wikipedia:Portada
(11). Obtenido de https://infseg.com/seguridad/captura-la-bandera-ctf/
(12). Obtenido de https://iiemd.com/gamificacion/que-es-gamificacion
13). Obtenido de https://whatis.techtarget.com/definition/offensive-security

7. **Anexos**

Plan de Trabajo