Universitat Oberta de Catalunya

uoc.edu

El juego de la Ciberseguridad: Securiza2

Autor: Rubén Galiana Rubio
Plan de Estudios: Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Trabajo final de máster – Área de Hacking

Directora del TFM: Angela María García Valdés
Profesor responsable de la asignatura: Víctor García Font

Junio de 2020

Quería agradecer a mis padres y mi hermana el apoyo durante la etapa académica que hoy culmina.
Y a Diana, por estar ahí en todo momento y ayudarme cuando lo he necesitado.

FICHA DEL TRABAJO FINAL

Título del trabajo:	*El juego de la Ciberseguridad: Securiza2*
Nombre del autor:	*Rubén Galiana Rubio*
Nombre del consultor/a:	*Angela María García Valdés*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega:	06/2020
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*Hacking*
Idioma del trabajo:	*Castellano*
Palabras clave	*Juego, ciberseguridad, Securiza2*

Resumen del Trabajo:

La finalidad de este trabajo es realizar un proceso de aprendizaje sobre ciberseguridad a través de un juego de mesa de tipo trivial, donde los jugadores tienen que responder preguntas de ciberseguridad para conseguir el objetivo final de la victoria.

La mecánica del juego consistirá en ir respondiendo correctamente preguntas para conseguir los emblemas de las cinco categorías en las que se divide el juego: defensa, ataque, malware, GRC y cultura. Una vez conseguidos los emblemas en las casillas de los vértices del pentágono que forma el tablero, se tendrá que ir a la casilla central para responder cinco preguntas, una de cada temática. El jugador se proclamará vencedor si responde correctamente cuatro de las cinco preguntas que forman una tarjeta.

La metodología empleada para la realización del trabajo se ha basado, en primer lugar, en investigar las distintas mecánicas empleadas en este tipo de juegos de preguntas. Posteriormente, se han probado distintos juegos del tipo investigado para poder sacar conclusiones y adaptarlo a las mejores mecánicas posibles para que la experiencia de juego sea lo más agradable posible. Por último, se ha añadido un componente adicional, como es la estrategia, pudiendo alterar la dinámica del juego y haciéndolo más imprevisible.

Finalmente, considero que se han conseguido unas buenas dinámicas de juego añadiendo un componente de estrategia que hará que se consiga una buena experiencia de juego a la vez que se realiza un proceso de aprendizaje en el campo de la ciberseguridad de una forma más amena.

Abstract:

The purpose of this work is to carry out a learning process about cybersecurity through a trivial board game, where players have to answer cybersecurity questions to achieve the final goal of victory.

The mechanics of the game will consist of correctly answering questions to obtain the emblems of the five categories the game is divided: defense, attack, malware, GRC and culture. Once the emblems are obtained in the boxes of the vertices of the pentagon that forms the board, you will have to go to the central box to answer five questions, one of each subject. The player will be proclaimed the winner if he answers correctly four of the five questions that form a card.

The methodology used to carry out the work has been based, in first place, on investigating the different mechanics employed in this type of question game. Subsequently, different games of the type investigated have been tested in order to draw conclusions and adapt them to the best possible mechanics to make the gaming experience as enjoyable as possible. Finally, an additional component, strategy, has been added, which can alter the dynamics of the game and make it more unpredictable.

Finally, I believe that good game dynamics have been achieved by adding a strategy component that will make the game experience a good one while making the learning process in the field of cybersecurity more enjoyable.

Índice

Índice de figuras

Capítulo 1. Introducción

1.1. Contexto y justificación del Trabajo

La ciberseguridad se ha convertido en un término muy conocido en los últimos años debido a que la mayoría de las personas pasan gran parte de su día conectadas a Internet, comunicándose a través de medios como el correo electrónico o las redes sociales y realizando sus actividades bancarias y compras online, por lo que los riesgos que se presentan con la digitalización de todos sus datos aumentan considerablemente.

La ciberseguridad es, esencialmente, un nuevo término para la seguridad de la información, la protección de la información vital. Sin embargo, la seguridad de la información ha existido durante décadas, lo que ha provocado que muchos se pregunten qué hay de nuevo en la ciberseguridad. La novedad de la ciberseguridad es que hay información moviéndose más rápido por la red que nunca, por lo que hay que evitar que las personas puedan acceder a información a la que no tienen derecho y puedan usarla con fines adversos. El volumen y la complejidad de la información han aumentado, sin embargo, se sigue manteniendo el concepto básico de protección de la información. Con el aumento del volumen, también existe la posibilidad de causar más daño a más personas. El ciberespacio ha sido militarizado, hay un gran aumento en el hacktivismo, una gran cantidad de ciberdelitos y una dependencia de Internet con la proliferación de los dispositivos.

La mayoría de las personas suelen pensar que la ciberseguridad está principalmente centrada en el malware, los correos electrónicos no deseados, o en simples robos de identidad, por lo que solamente se preocupan por buscar contraseñas más robustas y seguras. Aunque el robo de identidad no es un asunto sin importancia, existen amenazas mucho más serias e importantes en la actualidad. Siendo que Internet no fue diseñado en sus inicios para ser seguro, la tarea de modernizar la seguridad resulta muy compleja.

Debido a la importancia que va adquiriendo la ciberseguridad en la actualidad, cada vez hay más personas que se interesan por esta. A priori, la ciberseguridad puede parecer un campo complicado, debido a la multitud de conceptos que no son nada habituales de escuchar en una conversación usual. Para ayudar a estas personas que se inician en el fascinante pero complejo mundo de la ciberseguridad se ha propuesto complementar este camino a través del aprendizaje basado en juegos. De esta manera, la persona que participe en el juego no solo aprenderá conceptos nuevos sino que también reforzará sus conocimientos con experiencias de aprendizaje activo y le resultará motivador para continuar con su aprendizaje.

1.2. Objetivos del Trabajo

Los principales objetivos de este trabajo de fin de máster son los siguientes:

- Aprendizaje sobre conceptos de ciberseguridad
- Concienciación de las ciberamenazas
- Desarrollar la memoria y la concentración
- Desarrollo de las capacidades intelectuales
- Fomentar el trabajo en equipo
- Impulsar la toma de decisiones
- Realizar un aprendizaje de forma amena y distendida

1.3. Enfoque y método seguido

El enfoque que se le ha dado a este proyecto ha sido la realización de un juego dirigido mayormente a personas que estén empezando en el mundo de la ciberseguridad, a través del cual pueden realizar un proceso de aprendizaje de un modo más ameno, aumentando su motivación e interés por la materia. También puede servir a las personas más experimentadas en la materia a reforzar sus conocimientos y pasar un buen rato en compañía.

Para llevar a cabo este proyecto se investigará a través de diferentes medios sobre los distintos juegos de mesa y sus mecánicas, a la vez que distintos conceptos de la ciberseguridad que resulte interesante incluir en las preguntas del juego. Una vez llevada a cabo dicha investigación, se procederá a diseñar y fabricar el juego de mesa a tamaño real, utilizando distintos métodos de diseño e impresión.

Para materializar esta metodología, en primer lugar, se ha realizado un análisis de los diferentes tipos de juegos de mesa de tipo trivial, prestando especial atención a las mecánicas empleadas por los distintos juegos. Posteriormente, se han probado distintos juegos del tipo investigado para poder sacar conclusiones y adaptarlo a las mejores mecánicas posibles para que la experiencia de juego sea lo más agradable posible. Por último, se ha añadido un componente adicional, como es la estrategia, mediante unas cartas especiales, pudiendo alterar la dinámica del juego y haciéndolo más imprevisible. Con esto, el juego ya no será un simple juego de preguntas, sino que también habrá que pensar en la estrategia correcta para conseguir la victoria ayudando así al desarrollo cognitivo de los jugadores.

1.4. Planificación del Trabajo

Los recursos utilizados para realizar el trabajo han sido: un ordenador, en concreto mi ordenador personal, el software Microsoft Word para la redacción de la memoria, el software Adobe Illustrator para el diseño de algunos componentes del juego y los recursos humanos, en concreto una persona.

Para la elaboración del juego será necesario: la impresión del tablero y las cartas, tanto de preguntas como las especiales, un dado, cinco peones, 25 emblemas, cinco Portaemblemas y un cronómetro.

En la siguiente tabla se muestran las tareas en las que se divide el proyecto, divididas en los hitos parciales de cada entrega. El proyecto se ha planificado para empezar el 19 de febrero de 2020 y se prevé finalizar el 2 de junio de 2020.

Tarea	Duración
Entrega 1 - Plan de trabajo	**10 días**
Problema a resolver	2 días
Objetivos	2 días
Metodología	1 día
Tareas	2 días
Planificación	1 día
Revisión estado del arte	2 días
Entrega 2	**20 días**
Estado del arte	10 días
Definición de la mecánica de juego	5 días
Diseño de tablero y componentes del juego	5 días
Entrega 3	**20 días**
Desarrollo de las preguntas	18 días
Elaboración e impresión del juego	2 días
Entrega 4	**25 días**
Redacción de la memoria	25 días

Ilustración 1: Estimación temporal de tareas

En la siguiente figura se puede observar con mayor claridad las actividades realizadas a lo largo de las semanas.

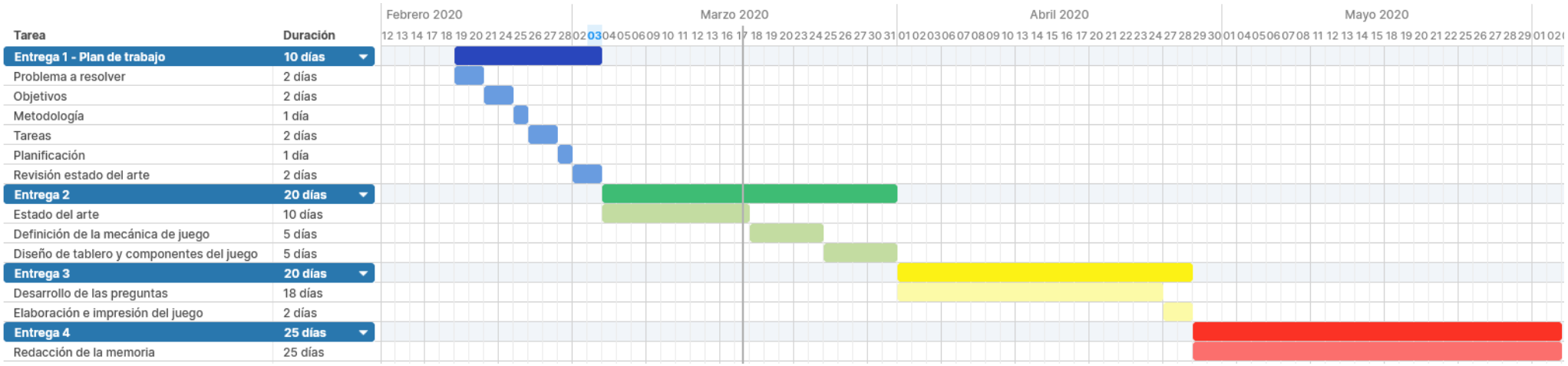

Ilustración 2: Diagrama de Gantt

1.5. Breve descripción de los otros capítulos de la memoria

Este TFM se va a centrar en la elaboración y diseño de un juego de mesa con temática exclusiva de ciberseguridad orientado a aprender y consolidar conocimientos sobre esta.

En el segundo capítulo se desarrollará el estado del arte, es decir, se analizará el aprendizaje basado en juegos como una forma de aprender mediante el entretenimiento a través de dos teorías de aprendizaje: las teorías de comportamiento y las teorías del aprendizaje constructivista.

En el tercer capítulo se explicará el desarrollo del juego que comprende la descripción de la mecánica de juego, así como el diseño del tablero y los dos tipos de tarjetas. También se enumeran los distintos componentes que forman el juego de mesa y, por último, se desarrollarán las preguntas que formarán las tarjetas de preguntas en las que se basa el juego, así como también las distintas cartas especiales, que añadirán un componente de estrategia.

En el cuarto capítulo se tratarán los costes temporales y económicos del proyecto, llevando a cabo una estimación total del coste económico y se analizará la viabilidad de este.

Finalmente, en el quinto capítulo se desarrollarán las conclusiones a las que se ha llegado tras la realización del trabajo. Se analizarán también los problemas surgidos y el planteamientos de mejoras futuras para el proyecto.

Capítulo 2. Estado del Arte

2.1. Introducción

Los juegos son la expresión de la naturaleza lúdica del ser humano. Los juegos también son necesarios y útiles como herramientas para el entretenimiento, la recreación, el aprendizaje y la modificación del comportamiento, ya sea intencional o no. Los juegos proporcionan diversión, participación apasionada, estructura, motivación, gratificación del ego, adrenalina, creatividad, interacción social y emoción, satisfaciendo la necesidad humana de aprendizaje. Hoy en día existe una necesidad cada vez mayor de que los profesores ayuden a los alumnos a participar en el aprendizaje y los mantengan motivados. Para ello, los profesores y los adultos deben comprender la importancia de los juegos en el aprendizaje, así como la forma de utilizar la enseñanza y el aprendizaje basados en los juegos. Los juegos han adquirido recientemente una importancia creciente dentro de la acción formativa, generando la aparición de la teoría de la "epistemología lúdica": su objetivo es identificar las formas de codificar el conocimiento en forma de juegos y cómo dar forma al proceso de adquisición de conocimientos como un proceso de juego.

Existen dos tipos principales de teorías de aprendizaje que guían el uso de los juegos en la educación: las teorías de comportamiento y las teorías del aprendizaje constructivista.

En los juegos basados en las teorías del aprendizaje por comportamiento, el elemento básico del proceso de aprendizaje es una pregunta que el juego dirige al jugador. La respuesta del jugador a esta pregunta es una respuesta que puede ser correcta o incorrecta. Las respuestas correctas se recompensan con una respuesta positiva del juego (por ejemplo, una recompensa o música agradable) que estimula aún más las emociones positivas en el jugador. Una respuesta incorrecta desencadena una respuesta negativa del juego (por ejemplo, una melodía triste o una desventaja).

Los juegos basados en teorías del aprendizaje constructivista se basan en el papel activo del alumno y permiten el logro de niveles taxonómicos más altos de conocimiento. El aprendizaje se basa en problemas, por lo tanto, estos juegos están diseñados como historias reales o ficticias en las que el alumno desempeña un papel, se identifica con lo que está sucediendo en el mundo del juego y resuelve activamente los problemas. El papel del profesor es seleccionar (y producir, si es posible) juegos adecuados y proporcionar orientación y retroalimentación sobre la evolución del alumno durante el juego y los resultados. Estos juegos ayudan a los alumnos a construir modelos mentales apropiados. El uso psicopedagógico de los juegos también genera

cambios en la forma en que el profesor interviene. El profesor desempeña un papel pedagógico más discreto y su impacto es predominantemente formativo [1].

En función de la finalidad del juego y de su construcción, los juegos pueden clasificarse en:

- **Juegos educativos**: con finalidades educativas; practicados de manera no formal e informal, en cualquier lugar y en cualquier momento, con o sin la supervisión de un adulto.
- **Juegos didácticos**: diseñados explícitamente con un propósito de aprendizaje, destinados a enseñar a los alumnos sobre determinados temas, ampliar conceptos, reforzar el desarrollo o ayudar a los alumnos a adquirir una habilidad.

Los tipos de juegos incluyen:

- **Juegos de mesa**: pura estrategia y/o tirar dados.
- **Juegos de cartas**: juegos de estrategia y azar.
- **Videojuegos**: los seres humanos interactúan con una interfaz de usuario para generar una retroalimentación visual en un dispositivo de vídeo.

La estructura básica de un juego didáctico comprende:

- Tema y contenido de acuerdo con la edad de los participantes.
- Objetivo didáctico/finalidad educativa.
- Objetivos operativos/finalidades específicas.
- Tareas didácticas (reconocimiento, nombrar, comparar, etc.).
- Reglas del juego.
- Elementos del juego (competitivo, cooperativo, recompensas, penalizaciones, estímulos).
- Estrategia didáctica (los procedimientos didácticos, los materiales y la organización del juego).
- Las etapas del juego.
- Versiones/complicaciones del juego.

2.2. Metodología: búsqueda, selección y análisis de datos

El propósito de este trabajo es destacar la relevancia de los juegos de mesa para la educación en general y, más específicamente, para la educación de adultos.

La Recomendación del Parlamento Europeo y del Consejo, de 18 de diciembre de 2006, sobre las competencias clave para el aprendizaje

permanente (2006/962/CE) establece, para los graduados de la enseñanza obligatoria, un perfil de formación europeo definido por ocho ámbitos de competencias clave [2]:

- Comunicación en la lengua materna.
- Comunicación en lenguas extranjeras.
- Competencia matemática y competencias básicas en ciencia y tecnología.
- Competencia digital.
- Aprender a aprender.
- Competencias sociales y cívicas.
- Sentido de la iniciativa y el espíritu empresarial.
- Conciencia y expresión cultural.

2.3. Juegos de mesa, resultados del aprendizaje y competencias clave

La documentación sobre el uso de los juegos en la educación menciona como resultados de la educación basada en el juego, las siguientes competencias y habilidades relacionadas con los ocho dominios anteriormente mencionados:

1. Capacidades relacionadas con el proceso de pensamiento:

    a) Pensamiento creativo: capacidad de abordar una cuestión o un problema desde distintos puntos de vista, lo que conduce a una comprensión más profunda y completa de la situación y, al mismo tiempo, ayuda a identificar formas alternativas de abordarla.

    b) Pensamiento analítico y reflexivo: los procesos de análisis y formulación de juicios sobre lo ocurrido.

2. Capacidades relacionadas con los aspectos prácticos/organizativos del aprendizaje:

    a) Competencias organizativas: planificación del trabajo, organización de los recursos, gestión de crisis y solución de problemas, realización del trabajo, medición del progreso, adopción de riesgos calculados.

3. Capacidades relacionadas con la autonomía:

    a) La capacidad de concentrarse durante períodos prolongados y reflexionar críticamente sobre los propósitos y objetivos del aprendizaje.

b) La capacidad de adquirir, procesar y asimilar nuevos conocimientos y aptitudes, así como de buscar y utilizar orientación y apoyo.

c) Competencias de autogestión: estar motivado, actuar con confianza, gestionar y evaluar el propio aprendizaje, demostrar flexibilidad e iniciativa

4. Capacidades relacionadas con los demás:

a) Capacidad de trabajar en colaboración durante el proceso de aprendizaje.

b) Mejora de las aptitudes sociales y las competencias de comunicación.

c) Competencias interpersonales: empatía, creación de consenso, negociación, diplomacia, gestión de conflictos, respetar a los demás, ser un jugador de equipo.

d) Conciencia y expresión culturales.

La creación de competencias sociales en los niños implica el aprendizaje de determinados comportamientos, su adopción y su utilización en situaciones de la vida. Los adultos, que poseen determinadas competencias, pero necesitan mejorarlas, también pueden beneficiarse de los juegos. La educación formal e informal de los niños y los adultos desempeña un papel importante en la configuración de los conocimientos, las aptitudes y las competencias sociales, estas últimas muy deseables en el contexto del actual mercado de trabajo. Los juegos son una alfabetización multimodal por excelencia y brindan la oportunidad de practicar la retórica y las aptitudes de persuasión. Ofrecen problemas que hay que resolver y lecciones que hay que aprender y son actividades que pueden dar lugar a la búsqueda de soluciones a problemas de la vida real.

En el contexto de la necesidad de aprendizaje a lo largo de toda la vida y de la necesidad de aprender juntos, necesidades generadas por un mercado laboral cada vez más versátil y multicultural, los juegos de mesa en la educación de adultos son una solución viable para reunir a los estudiantes y mantenerlos motivados para seguir participando en un proceso de aprendizaje con otros y de otros.

Si bien durante algún tiempo el interés se ha centrado principalmente en la utilización de los videojuegos en la educación, en los últimos años se ha producido un rejuvenecimiento de la atención prestada a los juegos de mesa como resultado de la creciente diversidad de juegos de mesa disponibles en el mercado y de algunos estudios que han puesto de relieve las oportunidades

que ofrece la utilización de los juegos de mesa en la educación (de adultos) que son comparables y similares a las que ofrece la utilización de los videojuegos. Las comunidades de jugadores de juegos de mesa (por ejemplo, Board Game Geek - BGG) alientan a los visitantes a participar en los juegos de mesa "leyendo artículos, haciéndose miembros, vendiendo/comprando juegos y publicando reseñas y comentarios de los juegos en una base de datos existente". Las comunidades de jugadores de juegos de mesa pueden proporcionar una valiosa información sobre cómo analizar el potencial educativo de los juegos de mesa.

Los juegos de mesa son herramientas capaces de proporcionar un desarrollo de habilidades y conocimientos prácticos y directos para personas de todas las edades y en todas las materias. Los juegos bien diseñados crean una atmósfera atractiva, no amenazante pero competitiva y mientras se juega, los estudiantes se centran en el contenido y refuerzan y aplican el aprendizaje.

El tablero y los demás elementos tangibles del juego (cartas, dados, etc.) actúan como metáforas visuales que ayudan a los jugadores a conectar información, convirtiéndose así en vehículos de aprendizaje. La estrategia del juego que incluye preguntas, problemas para resolver y situaciones desafiantes compromete el pensamiento crítico de los estudiantes, la resolución de problemas, la organización de la información y las habilidades prácticas, mejorando el aprendizaje. Los juegos también proporcionan la oportunidad de disminuir el riesgo de que los estudiantes con niveles de conocimiento más bajos se sientan expuestos.

Las preguntas que hacen que el juego funcione comprueban la comprensión y ayudan a identificar las lagunas o errores de aprendizaje. Además, los juegos de mesa son una excelente forma de transformar conceptos abstractos en algo más tangible y, por lo tanto, apoyan la adquisición de nociones que de otro modo serían difíciles de enseñar. Las exigencias de los diversos estilos de aprendizaje pueden abordarse también mediante juegos de mesa.

Los resultados del aprendizaje y las repercusiones de la utilización de juegos de mesa en la educación de adultos pueden sistematizarse de la siguiente manera [3]:

- Aprenden a enfrentarse con éxito a las situaciones cotidianas.
- Intercambian y aprenden a intercambiar información e ideas, y a comunicar pensamientos y sentimientos.
- Crean conciencia y expresión cultural, y competencias interculturales. Comprenden mejor el modo de vida y las mentalidades de otros pueblos si el juego proporciona un enfoque intercultural.

- La enseñanza y el aprendizaje se centran en las necesidades, motivaciones, características y recursos del alumno.
- Los alumnos logran la capacidad de definir objetivos válidos y realistas.
- Aprenden a utilizar los juegos de mesa como medio de comunicación. El alumno desarrolla la capacidad de autoevaluación y la educación basada en el juego aumenta la conciencia del alumno sobre el nivel actual de sus conocimientos.
- Aprenden a identificar, analizar y seleccionar las mejores estrategias para el trabajo / trabajo en equipo / trabajo en grupo, la resolución de problemas, la gestión de conflictos, etc.
- Construyen y desarrollan el pensamiento creativo, analítico y reflexivo, las competencias organizativas, la capacidad de concentrarse durante largos períodos de tiempo, las competencias de autogestión.
- Aprenden a buscar y utilizar la orientación y el apoyo, a trabajar en colaboración.
- Los estudiantes construyen y desarrollan habilidades sociales y competencias de comunicación, y competencias interpersonales.

2.4. Ventajas y desventajas del aprendizaje basado en el juego

Entre las ventajas del aprendizaje basado en juegos, las que considero más relevantes son:

- Promueve una actitud positiva hacia el aprendizaje.
- Desarrolla las habilidades de memoria.
- Conecta a los estudiantes y les ayuda a construir un aprendizaje por sí mismo.
- Involucra a todos los estudiantes de una clase en el aprendizaje activo y los mantiene motivados.
- Apoya el aprendizaje experimental proporcionando un enfoque transdisciplinario de la educación, ya que los estudiantes pueden trabajar en múltiples habilidades relacionadas con varias disciplinas: investigación, resolución de problemas, liderazgo, trabajo en equipo, creatividad, lógica, toma de decisiones, adaptación, habilidades comunicativas y de interacción.

Entre las desventajas cabe destacar:

- Puede consumir mucho tiempo.
- La gestión del tiempo puede ser difícil durante el juego.
- El incumplimiento por parte de los estudiantes del plazo para terminar/completar el juego puede provocar desánimo y baja autoestima.

- El riesgo de que los beneficiarios consideren que la actividad del juego es inconstante, lo que les tentaría a no abordar con responsabilidad y desde las perspectivas del aprendizaje.
- La dificultad de identificar si los estudiantes han aprendido y lo que han aprendido, así como posibles fallos en la evaluación.

Se ha comprobado que el aprendizaje basado en juegos (GBL) promueve una actitud positiva hacia el aprendizaje y el desarrollo de la capacidad de memoria, junto con su potencial para conectar a los alumnos y ayudarles a construir un aprendizaje por sí mismos. El GBL combina la materia con el juego y la capacidad del jugador de retener y aplicar la materia al mundo real de manera equilibrada. Se aborda en términos de método educativo, procedimiento didáctico y organización de la actividad de enseñanza-aprendizaje. Las teorías modernas sobre el aprendizaje efectivo han demostrado que el aprendizaje es más eficaz cuando es activo, experimental, situado, basado en problemas y proporciona una retroalimentación inmediata y los juegos tienen todas estas características.

Los juegos de mesa en equipo ayudan a desarrollar las aptitudes de comunicación y relación: los jugadores trabajan cara a cara para responder a las preguntas o resolver los problemas y se dan cuenta de que el trabajo en equipo los hace mejores y más rápidos para encontrar soluciones y ponerlas en práctica. Los juegos de mesa son una excelente forma de hacer que los jugadores tomen conciencia de los puntos fuertes de la colaboración en los entornos organizativos, esta conciencia puede realmente transformar para mejor las relaciones de trabajo.

Las ventajas y los resultados de aprendizaje del uso de juegos de mesa en la educación, en general y, más específicamente, en la educación de adultos, son lo suficientemente relevantes como para apoyar una mayor investigación sobre este tema y promover actividades de aprendizaje basadas en juegos. En el caso de la educación (para adultos) basada en el juego, el papel del profesor es el de guía y apoyo: el aprendizaje basado en el juego es aprender de la experiencia o aprender haciendo. La tarea del profesor es seleccionar juegos educativos apropiados para el nivel de habilidades y conocimientos generales de los estudiantes que deben desarrollarse [4].

2.5. Conclusión

La documentación sobre el uso de juegos de mesa en la educación es todavía escasa; sin embargo, existe un interés creciente en abordar y estudiar el uso de los juegos de mesa en la educación y la de los adultos en particular,

en el contexto de un mercado laboral versátil, globalizado y multicultural y una mayor necesidad de aprendizaje a lo largo de toda la vida.

La idea más relevante que se promueve mediante el uso de juegos de mesa en la educación de adultos es el hecho de que siempre hay algo nuevo que aprender y siempre hay algo que aprender con y de los demás.

Los juegos serios pueden utilizarse en todos los ámbitos en los que las personas necesitan formación y aprendizaje y en todos los niveles de educación. Los juegos como formas de educación son muy populares en el ejército, en los ámbitos de la seguridad, la protección, el rescate y la atención sanitaria, es decir, en las zonas en las que es difícil formar a las personas en situaciones reales. Últimamente, el número de juegos educativos serios también ha aumentado en los ámbitos de la administración pública, el gobierno, la gestión y otros campos que requieren formas específicas de comunicación, negociación y trabajo en equipo.

La educación basada en juegos proporciona a los alumnos una experiencia, así como la oportunidad de reflexionar sobre esa experiencia y extraer conocimientos, crear nuevas actitudes, aptitudes o formas de pensar basadas en ella. El tipo de aprendizaje interdisciplinario y constructivista que se produce durante la educación basada en juegos ofrece a los estudiantes la oportunidad de cometer errores sin sufrir las consecuencias de la vida real, descubrir su pertinencia personal, comprender las conexiones entre las razones, las acciones, las causas y los efectos, aprender a su propio ritmo, reflexionar sobre su experiencia, asumir el papel de líderes y actuar en consecuencia. Los juegos de mesa ofrecen todas estas oportunidades a los estudiantes y alumnos de todas las edades.

A medida que aumenta el número de juegos diseñados con fines educativos por equipos interdisciplinarios (expertos en didáctica y en las materias seleccionadas, psicología cognitiva, diseñadores gráficos, videógrafos, programadores, publicidad, comercialización), los profesores han comenzado últimamente a participar en el diseño, ensayo y mejora de los juegos educativos, junto con grupos de estudiantes que pueden proporcionar información útil sobre los juegos.

Capítulo 3. Desarrollo del juego

3.1. Mecánica

Securiza2 es un juego de mesa de preguntas y respuestas. Está diseñado para jugar hasta cinco jugadores o equipos. Se podrá jugar tanto individualmente, como en equipo de tantos jugadores se desee.

El tablero de juego tiene forma de pentágono. Los jugadores elegirán un peón y lo colocarán en el centro, donde comenzarán. Empezará a jugar el jugador que más puntuación saque al tirar un dado. En caso de empate, se volverá a lanzar el dado entre los jugadores que hayan empatado, hasta que un jugador saque la puntuación más alta. A continuación, pasará el turno al jugador situado a su derecha. Cuando un jugador requiera responder a una pregunta, será el jugador situado a su izquierda quien deba leérsela.

El objetivo del juego es moverse por las casillas del tablero de juego y obtener los emblemas de las cinco categorías. Las casillas donde se podrán conseguir los emblemas estarán situadas en los vértices del pentágono. Una vez se consigan los cinco emblemas habrá que dirigirse a la casilla central, donde el jugador deberá responder correctamente a cuatro de las cinco preguntas de la tarjeta para proclamarse ganador. Es necesario sacar en el dado el número exacto de espacios para llegar a la casilla central. En caso de no acertar al menos cuatro preguntas, ese jugador perderá el turno.

El jugador podrá moverse tantas casillas del tablero como indique el número del dado en cualquier dirección. Sin embargo, no se podrá invertir la dirección en medio de un movimiento. Hay casillas marcadas con dados en las que, en caso de caer, se deberá volver a tirar.

Cuando el jugador caiga en una casilla normal, deberá responder a una pregunta de la categoría a la que se corresponda el color de la casilla. Si acierta la pregunta volverá a tirar y si falla, perderá el turno. Para ganar los emblemas, se deberá acertar la pregunta de la casilla situada en el vértice del pentágono.

Una vez se lea la pregunta, el jugador tendrá 30 segundos para responder. Se deberá usar el temporizador para poder ver el tiempo que resta. En caso de que se acabe el tiempo, la pregunta se dará por fallada y se perderá el turno.

En caso de caer en la casilla central, el jugador robará una carta especial, que le servirá de ayuda, y posteriormente, volverá a tirar. Solo se podrá tener en la mano una carta de ayuda y será de un solo uso. En caso de caer en la casilla central y ya disponer de una carta de ayuda, el jugador podrá elegir

entre volver a tirar o descartar su carta especial y robar una nueva. En caso de caer en la casilla central y ya disponer de los cinco emblemas, el jugador no robará carta, solo responderá a las preguntas de la tarjeta final.

Si dos o más jugadores ya han conseguido el mismo emblema y uno de ellos cae en la casilla donde se obtiene, deberá retar a otro jugador que esté en posesión de ese emblema, eligiéndolo antes de responder la pregunta. Si acierta la pregunta, el jugador retado perderá el emblema. En caso contrario, el retador será el que lo pierda. En caso de que un jugador caiga en una casilla de emblema y solo ese jugador lo posea, no podrá retar a ningún jugador, y en caso de que falle la pregunta, perderá el emblema que había conseguido.

Categorías de las preguntas:

- Defensa (Azul)
- Ataque (Rojo)
- Malware (Morado)
- GRC (Marrón)
- Cultura (Verde)

3.2. Componentes

- 1 Tablero
- 20 Tarjetas con preguntas
- 16 Cartas especiales
- 1 Cronómetro
- 1 Dado
- 5 Peones
- 25 Emblemas
- 5 Portaemblemas

3.3. Diseño

3.3.1. Tablero

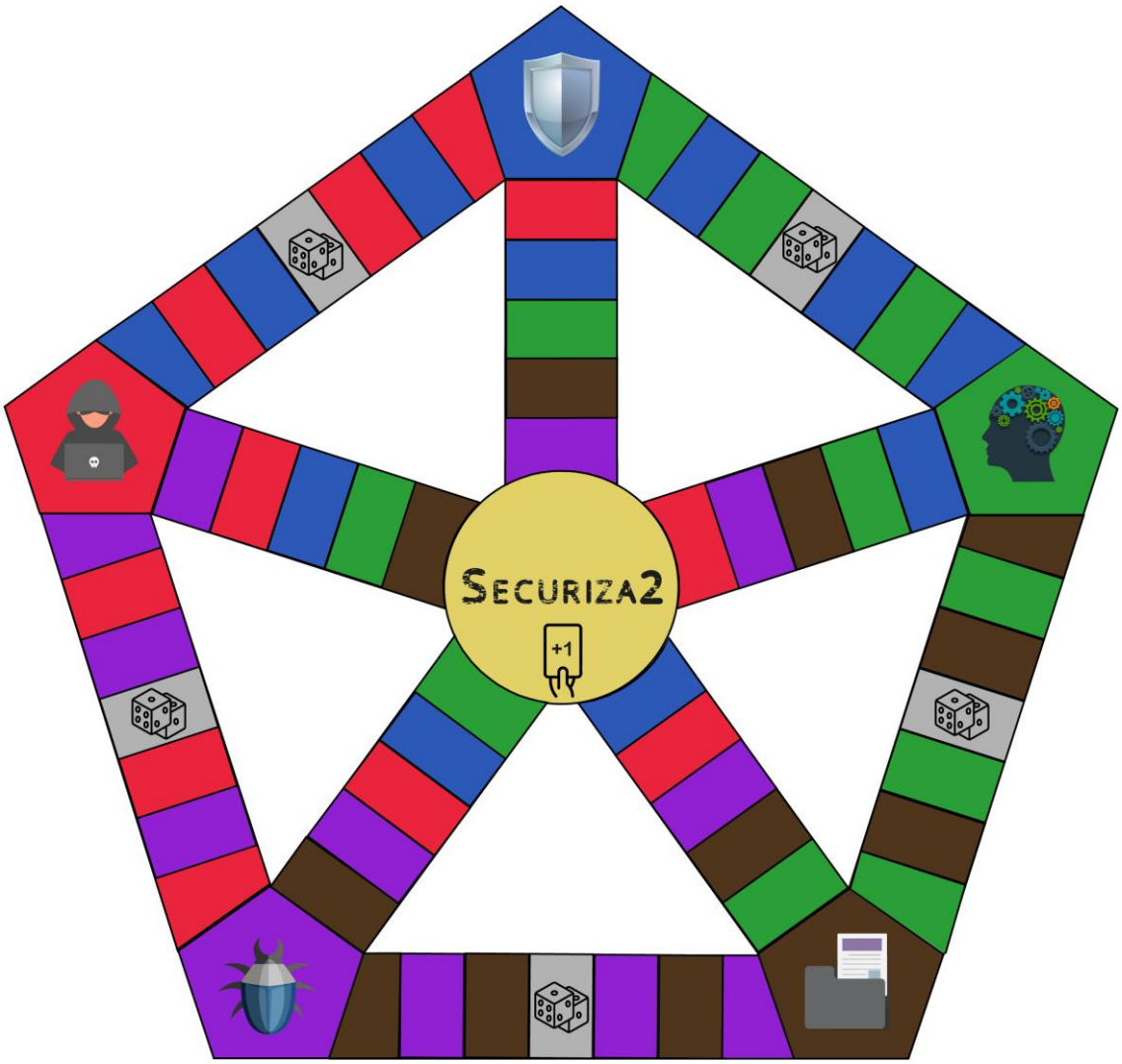

Ilustración 3: Tablero de juego

3.3.2. Tarjetas de preguntas

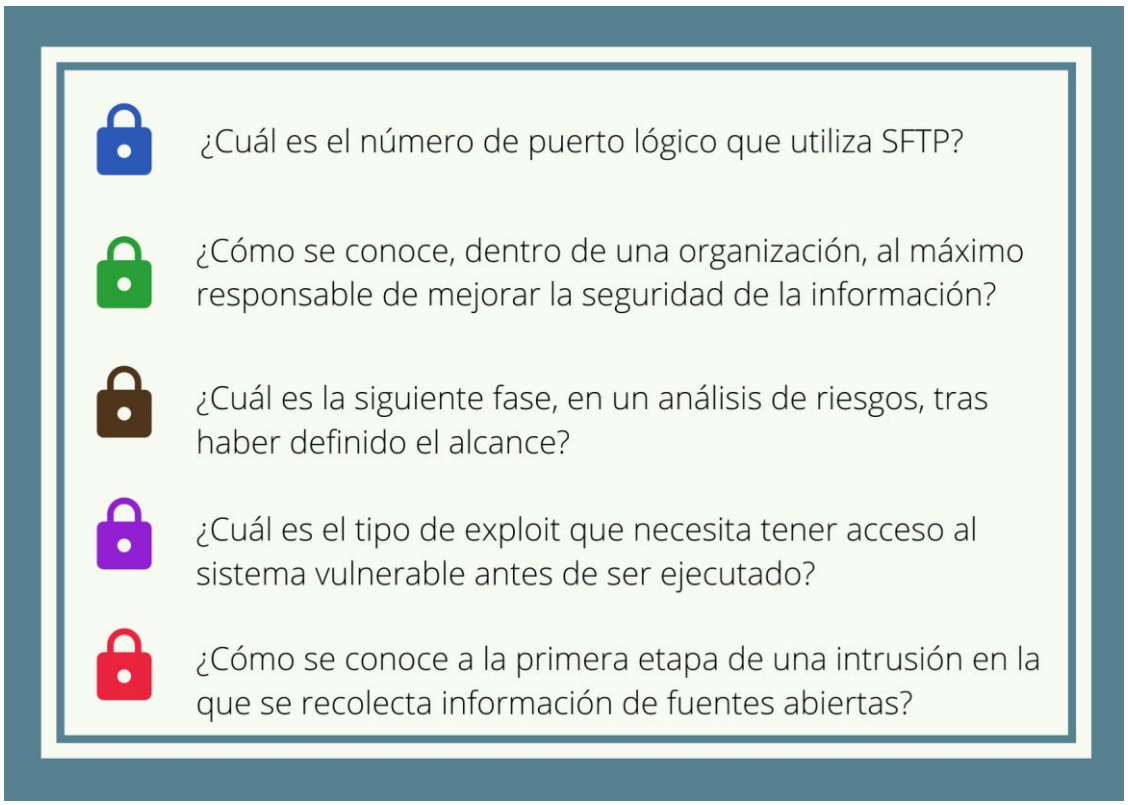

Ilustración 4: Anverso de tarjeta de preguntas

Ilustración 5: Reverso de tarjeta de preguntas

3.3.3. Cartas especiales

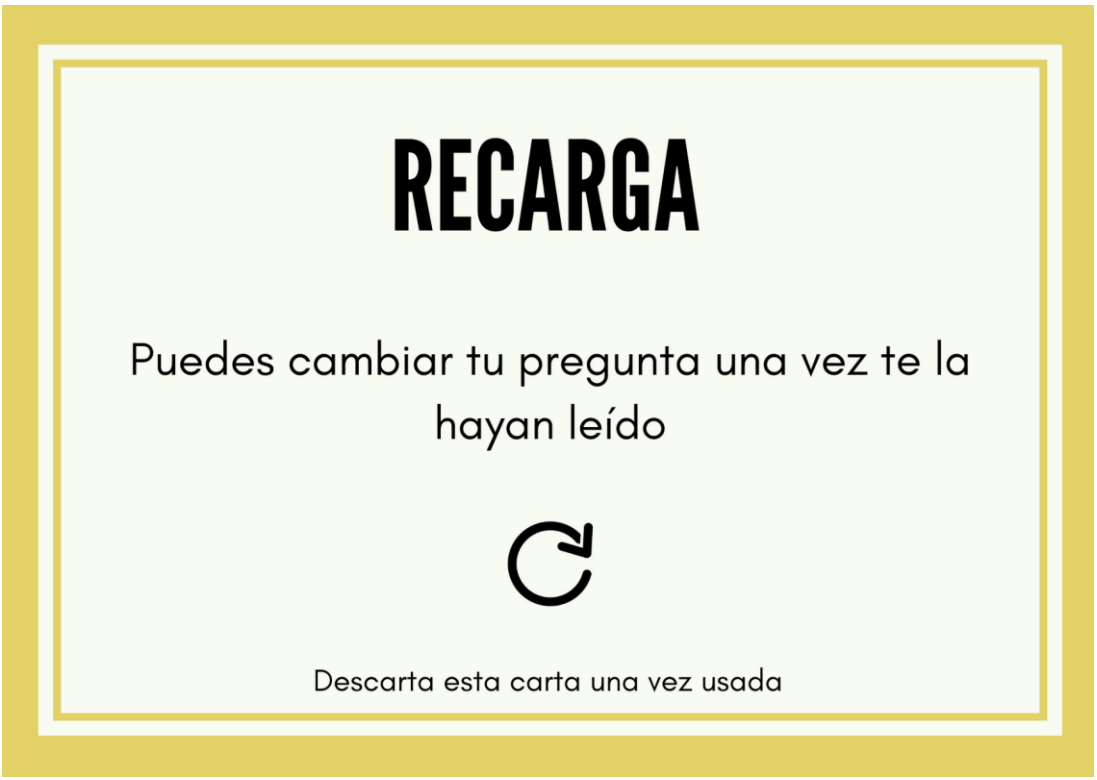

Ilustración 6: Anverso de carta especial

Ilustración 7: Reverso de carta especial

3.4. Desarrollo de las preguntas

3.4.1. Preguntas de Defensa

Pregunta: ¿Cuál es el comando para Windows que muestra el trayecto a una IP o dominio destino mediante el envío de paquetes ICMP echo?

Respuesta: Tracert

Justificación: El comando Tracert se ejecuta en la consola de símbolo de sistema en los sistemas operativos Windows. Gracias a este comando, podremos seguir la pista a los paquetes que vienen desde un host [5].

Pregunta: ¿Cuál es la versión actualizada y más segura del protocolo SSL?

Respuesta: TLS (Transport Layer Security, seguridad de la capa de transporte)

Justificación: El protocolo TLS (Transport Layer Security, seguridad de la capa de transporte) es solo una versión actualizada y más segura de SSL [6].

Pregunta: ¿Cómo se llama el string aleatorio que se añade a la contraseña para que el cifrado sea más seguro y que se almacena en un lugar distinto al de los datos de acceso?

Respuesta: Pepper o pimienta

Justificación: Además de salt también está pepper (“pimienta”). Este valor participa dificultando el ataque de fuerza bruta o de diccionario. También constituye una secuencia aleatoria que, sobre todo si se acompaña de salt, entra en el valor hash junto con la clave. A diferencia del salt, pepper no se almacena junto con los otros datos de acceso en la base de datos, sino separado y en un lugar más seguro [7].

Pregunta: ¿Cuál es el nombre por el que se conoce al sistema que centraliza el almacenamiento y la interpretación de los datos relevantes de seguridad?

Respuesta: SIEM (Security Information and Event Management)

Justificación: Un sistema de gestión de información y eventos de seguridad (en inglés, security information and event management, SIEM) es un sistema que centraliza el almacenamiento y la interpretación de los datos relevante de seguridad. De esta forma, permite un análisis de la situación en múltiples

ubicaciones desde un punto de vista unificado que facilita la detección de tendencias y patrones no habituales [8].

Pregunta: ¿Cuál es el tipo de criptografía que usa un par de claves (pública y privada) para el envío de mensajes?

Respuesta: Criptografía asimétrica

Justificación: La criptografía asimétrica, también llamada criptografía de clave pública o criptografía de dos claves, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que recibirá el mensaje [9].

Pregunta: ¿Cómo se llama el conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos?

Respuesta: IPsec

Justificación: IPsec (abreviatura de Internet Protocol security) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado [10].

Pregunta: ¿Cuál es el número del puerto lógico que utiliza SFTP?

Respuesta: 22

Justificación: Puerto**:**22/tcp Descripción: SSH, scp, SFTP [11].

Pregunta: ¿Cuál es el nombre del sistema de detección de intrusos basado en red (NIDS) desarrollado por Cisco Systems?

Respuesta: Snort

Justificación: Snort es un sistema de detección de intrusos en red, libre y gratuito. Ofrece la capacidad de almacenamiento de bitácoras en archivos de texto y en bases de datos abiertas, como MySQL [12].

Pregunta: ¿Cómo se conoce al proceso de reducción de vulnerabilidades en un sistema mediante medidas como el cerrado de puertos innecesarios o el cambio de claves por defecto?

Respuesta: Hardening o endurecimiento informático

Justificación: Hardening o también llamado endurecimiento informático, es el término que se le da al proceso de reducción de vulnerabilidades en el sistema. Esto se consigue, estableciendo unas medidas de seguridad con el objetivo de estar preparados ante un ataque informático [13].

Pregunta: ¿Cómo se conoce al servidor que ha sido especialmente configurado para la recepción de ataques, con el fin de ofrecer seguridad a la red interna que generalmente provee un solo servicio?

Respuesta: Servidor bastión o pasarela de aplicaciones

Justificación: Un bastion host (servidor bastion o pasarela de aplicaciones) es una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques, generalmente provee un solo servicio (como por ejemplo un servidor proxy) [14].

Pregunta: ¿Cómo se conoce al servidor que se ha configurado para distribuir direcciones no enrutables para todos los dominios, de modo que cada computadora que lo utilice no logre acceder al sitio web real, comúnmente utilizado para neutralizar botnets?

Respuesta: DNS Sinkhole o sumidero de DNS

Justificación: Un sumidero de DNS es un servidor DNS estándar que se ha configurado para distribuir direcciones no enrutables para todos los dominios en el sumidero de DNS, de modo que cada computadora que lo utilice no logre acceder al sitio web real. Cuanto más arriba se encuentre el servidor DNS, más computadoras bloqueará. Algunos de los botnets más grandes se han vuelto inutilizables por los agujeros de dominio de nivel superior (TLD) que abarcan todo Internet [15].

Pregunta: ¿Cuál es la técnica diseñada para detectar código malicioso de forma proactiva sin necesidad de contar con una firma específica?

Respuesta: Heurística

Justificación: La heurística, se trata de una tecnología diseñada para detectar códigos maliciosos de forma proactiva, es decir, sin la necesidad de contar con una firma específica. En esta línea, la solución de seguridad analiza un archivo y compara su comportamiento con ciertos patrones que podrían indicar la presencia de una amenaza. A cada acción que realiza el fichero se le asigna un puntaje, por lo tanto, si ese número es superior a un determinado valor, se clasifica como probable nuevo malware [16].

Pregunta: ¿Cuáles son los cuatro tipos de firmas que se pueden realizar en Suricata?

Respuesta: Pass, Drop, Reject y Alert

Justificación: Todas las firmas tienen diferentes propiedades. Una de ellas es la propiedad Action. Éste determina qué sucederá cuando una firma coincida. Hay cuatro tipos de acción: Pass, Drop, Reject y Alert [17].

Pregunta: ¿Cuál es la palabra clave que hay que poner en una firma de Suricata para realizar la búsqueda de una expresión regular?

Respuesta: pcre

Justificación: La palabra clave pcre (Perl Compatible Regular Expression) busca coincidencias específicas de expresiones regulares [18].

Pregunta: ¿Cuál es la opción del comando tcpdump para que no convierta las direcciones de host, números de puerto, etc. en nombres?

Respuesta: -n

Justificación: -n: No convierte las direcciones (es decir, direcciones de host, números de puerto, etc.) en nombres [19].

Pregunta: ¿En Sysmon, qué número corresponde al ID del evento que se crea al establecer una conexión de red?

Respuesta: 3

Justificación: Evento ID 3: Conexión de red. El evento de conexión de red registra las conexiones TCP/UDP en la máquina. Está desactivado de forma predeterminada. Cada conexión está vinculada a un proceso a través de los campos ProcessId y ProcessGUID. El evento también contiene los nombres de

host de origen y destino, las direcciones IP, los números de puerto y el estado de IPv6 [20].

Pregunta: ¿Cómo se conoce a la información relevante que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento?

Respuesta: IOC o indicador de compromiso

Justificación: Un indicador de compromiso o IOC, del inglés Indicator of Compromise, es toda aquella información relevante que describe cualquier incidente de ciberseguridad, actividad y/o artefacto malicioso, mediante el análisis de sus patrones de comportamiento.1 La intención de un indicador de compromiso es esquematizar la información que se recibe o se extrae durante el análisis de un incidente, de tal manera que pueda reutilizarse por otros investigadores o afectados, para descubrir la misma evidencia en sus sistemas y llegar a determinar si han sido o no comprometidos ya sea desde el punto de vista de monitorización frente a amenazas o por análisis forense [21].

Pregunta: ¿Cuál es la técnica que realiza un número alto de iteraciones internas de la función de hash, usada para que los ataques de fuerza bruta y diccionario sean menos efectivos?

Respuesta: Key Stretching

Justificación: Para hacer que los ataques de fuerza bruta y diccionario sean menos efectivos, podemos hacer que el proceso de hash sea más lento, haciendo que la función de hash incluya un número alto de iteraciones internas. Esta técnica es conocida como Key stretching [22].

Pregunta: ¿En qué está basada la detección que trata de identificar actividades sospechosas comparando el comportamiento de un usuario, proceso o servicio, con el comportamiento de perfil clasificado como normal?

Respuesta: Detección basada en anomalías

Justificación: Detección basada en anomalías: Los procesadores de eventos que basan su detección en un esquema de anomalías tratarán de identificar actividades sospechosas comparando el comportamiento de un usuario, proceso o servicio, con el comportamiento de perfil clasificado como normal [23].

Pregunta: ¿Cómo se conoce al proceso que realiza la interpretación conceptual de múltiples alertas con el objetivo de proporcionar una mejora semántica y de reducir la cantidad global de alarmas en un sistema de detección de intrusos?

Respuesta: Correlación

Justificación: Podemos definir el proceso de correlación de alertas como la interpretación conceptual de múltiples alertas con el objetivo de proporcionar una mejora semántica y de reducir la cantidad global de alarmas en un sistema de detección de intrusos [24].

3.4.2. Preguntas de Ataque

Pregunta: ¿Cuál es el vector de ataque más usado por los ciberdelincuentes? (datos de 2018)

Respuesta: El phishing o spear-phishing

Justificación: Durante 2018, las principales manifestaciones de ciberataques de este tipo fueron los casos de phishing o spear-phishing perpetrados por delincuentes, Estados o actores patrocinados por ellos con el objetivo de desarrollar acciones de espionaje o sabotaje [25].

Pregunta: ¿Cómo se conoce a la primera etapa de una intrusión en la que se recolecta información de fuentes abiertas?

Respuesta: Footprinting

Justificación: Footprinting es la etapa, primera de un test de intrusión la cual se recolecta información Su principal fuente es Internet, lo cual se puede encontrar gran cantidad de información. Después hay que filtrar toda esa información para quedarse con lo más importante [26].

Pregunta: ¿Cómo se conoce a la etapa de una intrusión que consiste en recolectar información directamente del sistema que se va a comprometer?

Respuesta: Fingerprinting

Justificación: Fingerprinting es una etapa que consiste en recolectar información directamente del sistema de una organización, para aprender más sobre su configuración y comportamiento. Esta etapa es aconsejable realizarla en una auditoría autorizada, ya que supuestamente cuyo “atacante” tiene permisos para realizar dicha acción [26].

Pregunta: ¿Cómo se llaman las tablas precalculadas utilizadas generalmente para descifrar hashes de contraseñas?

Respuesta: Tabla arcoíris o rainbow table

Justificación: Una tabla arcoíris (rainbow table) es una tabla precalculada para revertir las funciones hash criptográficas, generalmente usada para descifrar hashes de contraseñas. Las tablas se usan generalmente para recuperar una contraseña (o números de tarjeta de crédito, etc.) de una cierta longitud [27].

Pregunta: ¿Cuál es el tipo de ataque que consiste en forzar a un usuario a ejecutar peticiones no deseadas a una web en la que está autentificado sin que este se dé cuenta?

Respuesta: XSRF o CSRF (Cross-site Request Forgery)

Justificación: Los ataques del tipo Cross-site Request Forgery, o CSRF, consisten en forzar a un usuario a ejecutar peticiones no deseadas a una web en la que están autentificados sin que este se dé cuenta. Este tipo de ataque no busca el robo de datos, si no el que estas peticiones provoquen cambios, ya que el atacante no tiene forma de ver la respuesta a estas peticiones falsas [28].

Pregunta: ¿Cómo se llama la técnica que esconde malware para infectar los dispositivos en los espacios de publicidad de otras páginas web?

Respuesta: Malvertising

Justificación: El nombre de esta práctica viene de las palabras "malicious advertising" (publicidad maliciosa) y lo que hace es esconder malware para infectar nuestros dispositivos en los espacios de publicidad de otras páginas webs [29].

Pregunta: ¿Cómo se llama el tipo de ataque en el que se envían paquetes de datos con una dirección de remitente falsa?

Respuesta: IP spoofing

Justificación: El llamado IP spoofing es una técnica en la que se envían paquetes de datos TCP/IP o UDP/IP con una dirección de remitente falsa. Para inyectar sus propios paquetes en un sistema externo, el atacante utiliza la dirección de un sistema autorizado y de confianza, que de otra manera sería bloqueado por un sistema de filtrado [30].

Pregunta: ¿Cómo se denomina a la actividad orientada a la manipulación de las redes y sistemas de telefonía con el fin del hacking telefónico?

Respuesta: Phreaking

Justificación: El término phreaking deriva del nombre phreaker y puede definirse como el hacking del sistema telefónico, en el sentido que significa la investigación y manipulación creativa de las redes y sistemas de telefonía [31].

Pregunta: ¿Cuál es el número de fases que se siguen normalmente en el proceso del hacking ético?

Respuesta: 5 (Reconocimiento, Escaneo, Intrusión, Persistencia y Limpieza)

Justificación: Las fases del Hacking Ético se pueden dividir en cinco fases distintas. Un hacker ético sigue procedimientos similares a los de un hacker malicioso [32].

Pregunta: ¿Cómo se conoce la práctica fraudulenta que consiste en el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información sensible?

Respuesta: Vishing o Pretexting

Justificación: Vishing o pretexting es una práctica fraudulenta que consiste en el uso de la línea telefónica convencional y de la ingeniería social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad [33] [34].

Pregunta: ¿Cuál es el nombre por el que se conoce al exceso de flujo de datos sobre un montículo que permite un acceso no autorizado a la memoria por parte de un comando o shellcode?

Respuesta: Heap overflow o desbordamiento de montículo

Justificación: En informática, un desbordamiento de montículo (heap overflow/overrun) es un problema aritmético que hace referencia al exceso de flujo de datos sobre un montículo, esto permite un acceso no autorizado a la memoria por parte de un comando o de un programa o script denominado shellcode [35].

Pregunta: ¿Con qué nombre se conoce a uno de los ataques más antiguos que consiste en el envío de un datagrama IP cuyo tamaño total supere el máximo autorizado (65 536 bytes)?

Respuesta: Ping de la muerte

Justificación: El ataque ping de la muerte es uno de los ataques de red más antiguos. El principio de este ataque consiste simplemente en crear un datagrama IP cuyo tamaño total supere el máximo autorizado (65 536 bytes). Cuando un paquete con estas características se envía a un sistema que contiene una pila vulnerable de protocolos TCP/IP, este produce la caída del sistema. Los sistemas más modernos ya no son vulnerables a este tipo de ataque [36].

Pregunta: ¿Cuál es el tipo de ciberataque con el que se intenta redirigir el tráfico web a un sitio falso, explotando vulnerabilidades de software en los servidores DNS o en los equipos de los propios usuarios?

Respuesta: Pharming

Justificación: Pharming es un tipo de ciberataque con el que se intenta redirigir el tráfico web a un sitio falso, explotando vulnerabilidades de software en los sistemas de nombre de dominio, «DNS» por sus siglas en inglés, o en los equipos de los propios usuarios, que permiten a atacantes redirigir un nombre de dominio a otra máquina distinta. [37]

Pregunta: ¿Cuál es el nombre del programa de código abierto que sirve para efectuar un escaneo de puertos escrito originalmente por Gordon Lyon?

Respuesta: Nmap

Justificación: Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas [38].

Pregunta: ¿Cuál es el nombre del ataque usado contra organizaciones en la que el atacante infecta con malware sitios web de terceros muy utilizados por los usuario de la organización de forma que cuando los usuario de la organización acceden a ese sitio web quedan infectados?

Respuesta: Watering hole o ataque de abrevadero

Justificación: El término Ataque de abrevadero, en inglés watering hole attack, es una estrategia de ataque contra organizaciones en la que el atacante infecta

con malware sitios web de terceros muy utilizados por los usuario de la organización. De esta forma cuando los usuario de la organización acceden a ese sitio web quedan infectados. El ataque es altamente efectivo ya que, con la infección de un solo sitio, se puede lograr que miles de víctimas descarguen la amenaza [39].

Pregunta: ¿Cómo se llama el tipo de ataque de denegación de servicio en el que el atacante envía mensajes de ping a una IP de broadcast usando como dirección origen la dirección de la víctima?

Respuesta: Ataque pitufo o smurf

Justificación: En un ataque pitufo o smurf el atacante envía paquetes ICMP echo request (ping) a una IP de broadcast usando como dirección origen la dirección de la víctima, el resto de equipos conectados a la red enviarán un ICMP echo reply a la víctima, si imaginamos que estamos en una red de 100 máquinas, por cada ICMP echo request (ping) que enviemos simulando ser la víctima (spoofing), la víctima recibirá 100 paquetes ICMP echo reply (pong) es decir una inundación de ICMP multiplicada por el total de equipos en la red [40].

Pregunta: ¿Cómo se conoce la técnica utilizada mediante programas de software para extraer información de sitios web?

Respuesta: Web scraping

Justificación: Web scraping es una técnica utilizada mediante programas de software para extraer información de sitios web.1 Usualmente, estos programas simulan la navegación de un humano en la World Wide Web ya sea utilizando el protocolo HTTP manualmente, o incrustando un navegador en una aplicación [41].

Pregunta: ¿Cómo se conoce a la técnica maliciosa en la que el usuario pincha en un enlace oculto pensando que ha pinchado en un enlace legítimo?

Respuesta: Clickjacking

Justificación: Clickjacking es cuando un atacante usa varias capas transparentes u opacas para engañar a un usuario para que haga click en un botón o enlace en otra página cuando intenta hacer click en la página del nivel superior. Por lo tanto, el atacante está "secuestrando" los clicks destinados a

su página y enrutando a otra página, muy probablemente propiedad de otra aplicación, dominio o ambos [42].

Pregunta: ¿Cuál es el nombre por el que se conoce la minería de criptomonedas de forma maliciosa?

Respuesta: Cryptojacking

Justificación: El criptojacking (o minería de criptomonedas maliciosa) se define como el uso no detectado de un dispositivo informático ajeno para extraer monedas digitales. Es la vulneración de un ordenador, smartphone o red de equipos, no para acceder a datos, sino para minar criptomonedas secuestrando recursos de otros [43].

Pregunta: ¿Cuál es el nombre por el que se conoce a la ocultación de información en archivos multimedia?

Respuesta: Esteganografía

Justificación: El término «esteganografía» se utiliza muchas veces para englobar lo que en realidad es un campo más general, que es la ciencia de la «ocultación de información» y que abarca otros campos relacionados, como las marcas de agua, la anonimia o los canales encubiertos [44].

3.4.3. Preguntas de Malware

Pregunta: ¿Cuál es el nombre del primer malware, considerado como el primer arma de la ciberguerra, descubierto en 2010?

Respuesta: Stuxnet

Justificación: En 2010 salía a la luz Stuxnet, un malware que había infectado la central nuclear Natanz, en Irán. Según la investigación de Langner, el propósito de Stuxnet era retrasar el programa nuclear iraní. Stuxnet se puede considerar el primer ciberarma. Es el pionero en este mundo, y señala varios puntos e ideas en los que centrarán sus sucesores en el futuro [45].

Pregunta: ¿Cuál es el nombre por el que se conoce el exploit, supuestamente desarrollado por la NSA, que utilizó el ransomware WannaCry?

Respuesta: EternalBlue

Justificación: EternalBlue, en ocasiones escrito como ETERNALBLUE, es un exploit supuestamente desarrollado por la NSA. Fue filtrado por el grupo de hackers "Shadow Brokers" el 14 de abril de 2017, y fue utilizado en el ataque mundial de ransomware con WannaCry del 12 de mayo de 2017 [46].

Pregunta: ¿Cuál es el nombre por el que se conoce al famoso gusano escrito en VBScript que en mayo de 2000 infectó aproximadamente 50 millones de computadores provocando pérdidas de más de 5.500 millones de dólares?

Respuesta: lLoveYou

Justificación: lLoveYou (o VBS/LoveLetter) es un gusano escrito en VBScript. En mayo de 2000 infectó aproximadamente 50 millones de computadores provocando pérdidas de más de 5.500 millones de dólares [47].

Pregunta: ¿Cómo se conoce al fragmento de software o secuencia de comandos, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo?

Respuesta: Exploit

Justificación: Exploit, en el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de

información para conseguir un comportamiento no deseado del mismo. Su uso principal es como vector para la inyección de una carga útil (payload) que ofrezca al atacante algún tipo de acceso y/o control del equipo comprometido**.** [48].

Pregunta: ¿Cuál es el tipo de exploit que necesita tener acceso al sistema vulnerable antes de ser ejecutado?

Respuesta: Exploit local

Justificación: Exploit local. Si para ejecutar el exploit se necesita tener antes acceso al sistema vulnerable. Por ejemplo el exploit puede aumentar los privilegios del que lo ejecuta. Este tipo de exploits también puede ser utilizado por un atacante remoto que ya tiene acceso a la máquina local mediante un exploit remoto [49].

Pregunta: ¿Cómo se conoce a la capacidad de alterar los componentes de los procesos en memoria que permite que un atacante reemplace las entradas en el IAT o modifique la función API?

Respuesta: Hooking o hookear

Justificación: Hooking o hookear se conoce a la capacidad de alterar los componentes de la memoria del proceso permite que un atacante reemplace las entradas en el IAT o modifique la función API en sí [50].

Pregunta: ¿Cuál es el nombre por el que se conoce al malware que recopila información de un equipo y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario?

Respuesta: Spyware

Justificación: Spyware hace referencia a un malware que recopila información de una computadora y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador [51].

Pregunta: ¿Cómo se conoce a la vulnerabilidad que se descubrió en la implementación del Protocolo de escritorio remoto de Microsoft en 2019, que permite la posibilidad de ejecución remota de código?

Respuesta: BlueKeep

Justificación: BlueKeep es una vulnerabilidad de seguridad que se descubrió en la implementación del Protocolo de escritorio remoto de Microsoft, que permite la posibilidad de ejecución remota de código [52].

Pregunta: ¿Cuál es el término por el que se conoce al amplio rango de programas que son instalados en el PC de un usuario para dar seguimiento o reportar información a un tercero instaladas sin el conocimiento del usuario?

Respuesta: Grayware

Justificación: "Grayware" es un término abarcador aplicado a un amplio rango de programas que son instalados en la computadora de un usuario para dar seguimiento o reportar cierta información a un tercero. Estas aplicaciones son usualmente instaladas y “corren” sin el permiso del usuario [53].

Pregunta: ¿Cómo se conoce al tipo de malware que es capaz de modificar su propio código, pero mantiene su algoritmo original intacto?

Respuesta: Polimórfico

Justificación: En el contexto del malware, un código polimórfico es aquel que usa la técnica del polimorfismo, que consiste en usar un motor polimórfico embebido para cambiar su propio código mientras mantiene su algoritmo original intacto. Cambia solo parte del código, en contraste con el metamorfismo que cambia todo el código, manteniendo otra parte del código igual [54].

Pregunta: ¿Cómo se conoce al tipo de software que se usa para esconder malware y no sea fácilmente detectado por los antivirus?

Respuesta: Crypter

Justificación: Un Crypter es un software que se usa para esconder malware (virus, keyloggers, …) para que no sea fácilmente detectado por los antivirus. Para realizar su función pueden usar técnicas de cifrado y a veces ofuscación. El Crypter toma el archivo ejecutable y obtiene un nuevo archivo ejecutable que al ejecutarse descifra código cifrado que contiene y obtiene el antiguo archivo ejecutable original [55].

Pregunta: ¿Cómo se conoce al programa de ordenador que traduce el lenguaje máquina a lenguaje ensamblador?

Respuesta: Desensamblador

Justificación: Un desensamblador es un programa de computador que traduce el lenguaje de máquina a lenguaje ensamblador, la operación inversa de la que hace el ensamblador. Un desensamblador difiere de un decompilador, en que éste tiene como objetivo un lenguaje de alto nivel en vez de al lenguaje ensamblador [56].

Pregunta: ¿Cuál es la técnica que consiste en la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga?

Respuesta: Cracking

Justificación: El cracking es la modificación del software con la intención de eliminar los métodos de protección de los cuales este disponga: protección de copias, versiones de prueba, números de serie, claves de hardware, verificación de fechas, verificación de CD o publicidad y adware [57].

Pregunta: ¿Cuál es el nombre del primer malware de la historia de tipo gusano, originado en 1971?

Respuesta: Creeper

Justificación: Creeper. Se trata del primer virus de la historia. Nació en 1971 y dejó huella porque infectó los computadores PDP-11, los cuales estaban conectados a red de computadores precursora de Internet, Arpanet. Una de las características de Creeper es que mostraba un mensaje que infectaba el sistema y decía: “Soy el más aterrador (creeper); atrápame si puedes”. Fue creado por Robert Thomas Morris, quien trabajaba para la empresa BBN [58].

Pregunta: ¿Cuál es el nombre del famoso RAT que utiliza plugins modulares utilizado por diversos grupos APT de origen chino?

Respuesta: PlugX

Justificación: PlugX es una herramienta de acceso remoto (RAT) que utiliza plugins modulares. Ha sido utilizado por múltiples grupos de amenazas [59].

Pregunta: ¿Cómo se conoce al tipo de malware que utiliza herramientas y procesos propios del sistema operativo y no droppea ejecutables adicionales en el sistema de la víctima?

Respuesta: Malware fileless o sin archivos

Justificación: Los ataques de fileless malware hacen uso de herramientas y procesos propios del sistema operativo mediante una técnica conocida como “Living off the Land” o “Viviendo de la Tierra”, que le permiten llevar adelante su actividad maliciosa utilizando elementos preinstalados y sin droppear ejecutables adicionales en el sistema de la víctima. Dicho de otra forma, utiliza funcionalidades del sistema operativo en contra del propio usuario. Esto dificulta su detección, ya que el código malicioso se ejecuta a través de procesos legítimos [60].

Pregunta: ¿Cómo se llama el tipo de análisis de malware que se realiza observando el comportamiento del malware mientras se está ejecutando en un sistema?

Respuesta: Análisis dinámico

Justificación: Análisis dinámico de malware: El análisis dinámico o de comportamiento se realiza observando el comportamiento del malware mientras se está ejecutando en un sistema host. Esta forma de análisis se realiza a menudo en un sandbox environment para evitar que el malware infecte realmente a los sistemas de producción; muchas de estas cajas de arena son sistemas virtuales que pueden ser devueltos fácilmente a un estado limpio una vez finalizado el análisis [61].

Pregunta: ¿Cuál es el registro que se refiere al puntero de la pila?

Respuesta: SP (Stack Pointer)

Justificación: SP (Stack Pointer): Se traduce como puntero de pila y es el que se reserva el procesador para uso propio en instrucciones de manipulado de pila. Por lo general, el programador no debe alterar su contenido [62].

Pregunta: ¿Cómo se llama el famoso framework utilizado para reversing y análisis de binarios realizado por el español Sergi Álvarez?

Respuesta: Radare2

Justificación: Radare2 es un marco completo para ingeniería inversa y análisis de binarios; compuesto por un conjunto de pequeñas utilidades que se pueden usar juntas o independientemente de la línea de comando [63].

Pregunta: ¿Cómo se llama el malware de tipo web shell que se aloja en servidores web para proporcionar acceso a una red empresarial utilizado por varios grupos APT de origen chino?

Respuesta: China Chopper

Justificación: China Chopper es un Web Shell alojado en servidores Web para proporcionar acceso a una red empresarial y que no dependa de un sistema infectado que llame a un servidor de control y comando remoto. Ha sido usado por varios grupos de amenazas [64].

3.4.4. Preguntas de GRC (Gobernabilidad, Riesgo y Cumplimiento)

Pregunta: ¿Cuáles son los tres principios que deber respetar la gestión de la información en una organización?

Respuesta: Confidencialidad, integridad y disponibilidad

Justificación: La gestión de la información se fundamenta en tres pilares fundamentales que son, confidencialidad, integridad y disponibilidad. La seguridad de la información aplica barreras y procedimientos que resguardan el acceso a los datos y sólo permite acceder a las personas autorizadas para realizarlo [65].

Pregunta: ¿Cuál es el nombre del procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos ?

Respuesta: Seudonimización

Justificación: Seudonimización es un procedimiento de gestión de datos donde se reemplazan campos de información personal dentro de un registro de datos por uno o más identificadores artificiales o pseudónimos. Un pseudónimo único por cada campo reemplazado, o grupo de campos reemplazados, hace cada registro de datos menos identificable mientras se queda apto para análisis de datos y procesamiento de datos [66].

Pregunta: ¿Cuál es la siguiente fase, en un análisis de riesgos, tras haber definido el alcance?

Respuesta: Identificar los activos

Justificación: Una vez definido el alcance, debemos identificar los activos más importantes que guardan relación con el departamento, proceso, o sistema objeto del estudio. Para mantener un inventario de activos sencillo puede ser suficiente con hacer uso de una hoja de cálculo o tabla [67].

Pregunta: ¿Cómo se conoce la norma que supone la puesta en marcha y aplicación de controles y medidas para gestionar los riesgos generales a los que esté expuesta la continuidad del negocio de una organización?

Respuesta: ISO 22301

Justificación: ISO 22301 es la nueva norma internacional de gestión de continuidad de negocio que, a través del ciclo de mejora continua (PDCA), establece los requisitos para la planificación, el establecimiento, la implantación, la operación, la supervisión, la revisión, la prueba, el mantenimiento y la mejora de un SGCN documentado teniendo en cuenta la gestión de los riesgos globales de cada organización y su capacidad de resiliencia [68].

Pregunta: ¿Cuál es el nombre por el que se conocen las directrices que tienen por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información?

Respuesta: Esquema Nacional de Seguridad

Justificación: La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos estableció el Esquema Nacional de Seguridad que, aprobado mediante Real Decreto 3/2010, de 8 de enero, tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos en su ámbito de aplicación y estará constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información [69].

Pregunta: ¿De qué color es el equipo que se ocupa de establecer las reglas de enfrentamiento, organizar equipos, establecer la estrategia, realizar las evaluaciones de riesgo y supervisar los progresos del Blue, Red y Yellow team?

Respuesta: Blanco o White

Justificación: Los miembros del Equipo Blanco incluyen elementos de Cumplimiento, Gestión, Analistas, Logística y más. Estos son individuos neutrales y omniscientes que establecen las reglas de enfrentamiento, organizan equipos, establecen la estrategia, realizan evaluaciones de riesgo y establecen planes y supervisan los progresos [70].

Pregunta: En 2007 se publicó la primera norma internacional dirigida exclusivamente a la seguridad de riesgos en la cadena de suministro. ¿De qué norma se trata?

Respuesta: ISO 28000

Justificación: La norma ISO 28000 “Especificaciones para los Sistemas de Gestión de la Seguridad para la Cadena de suministro” se lanzó en el 2007. Fue la primera norma internacional dirigida exclusivamente a la seguridad de riesgos en la cadena de suministro. El objetivo de la norma es proporcionar un marco de buenas prácticas para reducir los riesgos para las personas y las cargas en la cadena de suministro [71].

Pregunta: ¿Qué normativa internacional permite el aseguramiento, confidencialidad e integridad de los datos e información?

Respuesta: ISO 27001

Justificación: ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan [72].

Pregunta: ¿Cuál es la entidad designada por España para realizar las actividades de normalización en el país y también participa en la normalización a nivel internacional (normas EN e ISO)?

Respuesta: Asociación Española de Normalización (UNE)

Justificación: La Asociación Española de Normalización (UNE; acrónimo de Una Norma Española) es una entidad privada, multisectorial y sin fines lucrativos, designada por el Ministerio de Economía, Industria y Competitividad como organismo nacional de normalización [73].

Pregunta: ¿Cuál es la metodología para la realización de análisis de riesgos más utilizada en España?

Respuesta: MAGERIT

Justificación: MAGERIT es la metodología de análisis de riesgos más utilizada en España. Su carácter es público y ha sido elaborada por el Centro Criptográfico Nacional, dependiente del Ministerio de Administraciones Públicas [74].

Pregunta: ¿Cuántas medidas de seguridad están recogidas en el Esquema Nacional de Seguridad (ENS)?

Respuesta: 75 medidas

Justificación: De acuerdo con el ENS, la adopción de medidas de seguridad deberá ser proporcional a la naturaleza de la información, el sistema y los servicios a proteger mediante la determinación de la categoría del sistema, atendiendo a los riesgos a los que están expuestos. Así, en el ENS encontramos 75 medidas de seguridad divididas en tres grupos y recogidas en el Anexo II [75].

Pregunta: ¿Qué medidas del Esquema Nacional de Seguridad (ENS) se centran en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad?

Respuesta: Medidas de protección

Justificación: Las medidas de protección, se centrarán en proteger activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad [76].

Pregunta: ¿Qué serie de reglas, normas y protocolos de actuación se encargan de velar por la seguridad informática de la empresa?

Respuesta: Políticas de seguridad

Justificación: Las políticas de seguridad son un conjunto de reglas, normas y protocolos de actuación que se encargan de velar por la seguridad informática de la empresa. Se trata de una especie de plan realizado para combatir todos los riesgos a los que está expuesta la empresa en el mundo digital [77].

Pregunta: ¿En qué año entró en aplicación el Reglamento General de Protección de Datos (RGPD), que dejó obsoleta a la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD)?

Respuesta: 2018

Justificación: El Reglamento General de Protección de Datos (RGPD) es el reglamento europeo relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos. Entró en vigor el 25 de mayo de 2016 y fue de aplicación el 25 de mayo de 2018, dos años durante los cuales las empresas, las organizaciones, los organismos y las instituciones se fueron adaptando para su cumplimiento [78].

Pregunta: ¿Qué fórmula se utiliza para calcular cuantitativamente el riesgo de una iniciativa o proyecto para la mejora de la seguridad de la información?

Respuesta: Riesgo = Probabilidad x Impacto

Justificación: A la hora de calcular el riesgo, si hemos optado por hacer el análisis cuantitativo, calcularemos multiplicando los factores probabilidad e impacto: RIESGO = PROBABILIDAD x IMPACTO. Si por el contrario hemos optado por el análisis cualitativo, haremos uso de una matriz de riesgo [79].

Pregunta: ¿Cómo se conoce a la norma publicada en 2005 que recoge una serie de guías y pautas para el diseño y construcción de CPDs?

Respuesta: Norma TIA 942

Justificación: La norma TIA 942, Telecommunications Infrastructure Standard for Data Centers, es un estándar publicado por la Telecomunications Industry Association (TIA) en abril de 2005, y se se divide en 8 puntos y 9 anexos. El propósito de esta norma es recoger una serie de guías y pautas para el diseño y construcción de CPDs. Cabe destacar que este estándar hace hincapié en todo lo referente a las comunicaciones, como la distribución o el cableado de estas [80].

Pregunta: ¿Qué plan se desarrolla en la fase 3 (respuesta a la contingencia) del plan de continuidad del negocio?

Respuesta: Plan de crisis (o de incidentes)

Justificación: En la fase 3 se documenta el plan de Crisis y los respectivos documentos para la recuperación de los entornos. Este documento es el elemento central en la gestión de la situación de crisis, cuyo objetivo es evitar que tomemos decisiones improvisadas que puedan empeorar la crisis o que, simplemente, no se tomen. Este plan contiene todos los elementos necesarios para la gestión de los momentos iniciales de una crisis [81].

Pregunta: ¿Cómo se conocen los contratos que regulan el arrendamiento de un servicio que implica la instalación completa de un dispositivo en una ubicación física con equipos y softwares compatibles, que permitan a la empresa poder acudir a él en caso de desastre y seguir funcionando en un periodo de 1 a 3 horas?

Respuesta: Contratos hot sites

Justificación: En estos contratos lo que se regula es el arrendamiento de un servicio que implica la instalación completa de un dispositivo en una ubicación física con equipos, procesador de datos, servidores, información real, softwares instalados y compatibles que permitan a la empresa, poder acudir a él en caso de desastre y seguir funcionando en un periodo de 1 a 3 horas. Estos contratos se utilizan para los sistemas centrales más importantes de la empresa, cuyo fallo supondría un estado crítico [82].

Pregunta: ¿Cuál es el plan que va a marcar las prioridades, los responsables y los recursos que se van a emplear para mejorar el nivel de seguridad en el mundo digital de una empresa?

Respuesta: Plan Director de Seguridad

Justificación: Cuando decidimos abordar la ciberseguridad es importante tener una planificación de las actividades a realizar que cuente con el compromiso de la dirección. Este plan va a marcar las prioridades, los responsables y los recursos que se van a emplear para mejorar nuestro nivel seguridad en el mundo digital. A esta planificación la llamaremos Plan Director de Seguridad. Contendrá los proyectos que vamos a abordar tanto técnicos como de contenido legal y organizativos [83].

Pregunta: ¿Cómo se conoce el conjunto de políticas de administración de la información que permite conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información?

Respuesta: Sistema de Gestión de la Seguridad de la Información (SGSI)

Justificación: Podemos definir el SGSI, Sistema de gestión de la seguridad de la información, basado en la norma UNE-ISO/IEC 27001, como una herramienta que nos va a permitir conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en nuestra empresa [84].

3.4.5. Preguntas de Cultura

Pregunta: ¿En qué ciudad española se encuentra la sede oficial del Instituto Nacional de Ciberseguridad (INCIBE)?

Respuesta: León

Justificación: El Instituto Nacional de Ciberseguridad (INCIBE) Tiene su sede oficial en la ciudad de León, en la Avenida José Aguado nº 41, y mantiene una oficina en la Plaza Manuel Gómez Moreno de Madrid [85].

Pregunta: ¿Cuál es la segunda capa del Modelo OSI?

Respuesta: Capa de enlace de datos

Justificación: La capa de enlace de datos es la segunda capa del Modelo OSI y se ocupa del direccionamiento físico, del acceso al medio, de la detección de errores, de la distribución ordenada de tramas y del control del flujo [86].

Pregunta: ¿Cuál es la sexta capa del Modelo OSI?

Respuesta: Capa de presentación

Justificación: La capa de presentación es la capa 6 del Modelo OSI y su objetivo es encargarse de la representación de la información, de manera que, aunque distintos equipos puedan tener diferentes representaciones internas de caracteres, los datos lleguen de manera reconocible [86].

Pregunta: ¿Cuál fue la primera conferencia de hacking de la historia celebrada en 1993?

Respuesta: DEFCON

Justificación: DEFCON es una de las convenciones de hackers más grandes y notables del mundo, que se celebra anualmente en Las Vegas, Nevada. La primera DEFCON tuvo lugar en junio de 1993 [87].

Pregunta: ¿En qué año se llevó a cabo la primera detención en España por hacking?

Respuesta: 1996

Justificación: En enero de 1996, el Grupo de Delitos Informáticos del Cuerpo Nacional de Policía, bajo las órdenes del inspector jefe Carlos García, llevaba a cabo la primera detención en España por "hacking" o penetración en sistemas informáticos. El detenido se apodaba "Mave" y formaba parte del grupo de hackers madrileños Konspiradores Hacker Klub [88].

Pregunta: ¿Cómo se conoce a la actividad que utiliza herramientas digitales ilegales o legalmente ambiguas persiguiendo fines políticos?

Respuesta: Hacktivismo

Justificación: Hacktivismo se entiende normalmente a la utilización no-violenta de herramientas digitales persiguiendo fines políticos; estas herramientas incluyen desfiguraciones de webs, redirecciones, ataques de denegación de servicio, robo de información, parodias de sitios web, sustituciones virtuales, sabotajes virtuales y desarrollo de software [89].

Pregunta: ¿Cómo se conoce a los hackers que actúan ilegalmente con el fin de lograr una mayor seguridad?

Respuesta: Hackers de sombrero gris

Justificación: Un sombrero gris, en la comunidad hacker, hace referencia a un hacker talentoso que actúa ilegalmente, aunque con buenas intenciones. Usualmente no atacan por intereses personales o con malas intenciones, pero están preparados para cometer delitos durante el curso de sus hazañas tecnológicas con el fin de lograr una mayor seguridad [90].

Pregunta: ¿Cómo se conoce a los hackers poco hábiles que usan herramientas desarrolladas por otros para atacar sistemas y redes de computadores?

Respuesta: Script kiddies

Justificación: Un script kiddie es un individuo no calificado que utiliza scripts o programas desarrollados por otros para atacar sistemas y redes de computadoras y desfigurar sitios web. En general, se supone que la mayoría son jóvenes que carecen de la capacidad de escribir programas sofisticados o exploits por su cuenta y que su objetivo es tratar de impresionar a sus amigos u obtener crédito en las comunidades entusiastas de la informática [91].

Pregunta: ¿Cómo se conoce, dentro de una organización, al máximo responsable de mejorar la seguridad de la información?

Respuesta: CISO (chief information security officer)

Justificación: Dentro de una organización, el oficial de seguridad de la información o CISO (chief information security officer) es el responsable máximo en planificar, desarrollar, controlar y gestionar las políticas, procedimientos y acciones con el fin de mejorar la seguridad de la información dentro de sus pilares fundamentales de confidencialidad, integridad y disponibilidad [92].

Pregunta: ¿Cuál es el nombre de la distribución Linux diseñada para preservar la privacidad y el anonimato en la que todas las conexiones salientes están forzadas a salir a través de Tor?

Respuesta: TAILS (The Amnesic Incognito Live System)

Justificación: The Amnesic Incognito Live System o Tails es una distribución Linux diseñada para preservar la privacidad y el anonimato. El sistema está diseñado para ser arrancado como un Live CD o USB sin dejar ningún rastro en el almacenamiento local a menos que se indique explícitamente [93].

Pregunta: ¿Cuál es el término proveniente del inglés que se utiliza para describir la práctica en Internet de investigación y publicación de información privada sobre un individuo o una organización, generalmente con el propósito de intimidar, humillar o amenazar?

Respuesta: Doxing

Justificación: Doxing es un término proveniente del inglés que se utiliza para describir la práctica en Internet de investigación y publicación de información privada o identificante (especialmente información personal) sobre un individuo o una organización, generalmente con el propósito de intimidar, humillar o amenazar.Los métodos empleados para adquirir esta información incluyen búsquedas en bases de datos de acceso público y redes sociales (como Facebook o Twitter), hacking o métodos de ingeniería social [94].

Pregunta: ¿Cómo se conoce al ciberataque en el que se estuvieron robando documentos confidenciales encriptados con el sistema 'Cryptofiler', utilizado por la OTAN y la Unión Europea para sus comunicaciones más sensibles activo desde 2007 y descubierto en 2013?

Respuesta: Octubre Rojo

Justificación: Investigadores rusos detectaron el 14 de enero de 2013 un ciberataque que podría haber estado robando documentos confidenciales encriptados desde 2007 de instituciones gubernamentales como embajadas y de centros de investigación nuclear y compañías estatales de gas y petróleo. El objetivo del ataque es robar documentos encriptados con el sistema 'Cryptofiler', utilizado por la OTAN y la Unión Europea para sus comunicaciones más sensibles. El ciberataque ha sido bautizado como **'**Octubre Rojo**'** y tiene similitudes con 'Flame', otro malware descubierto en 2012 [95].

Pregunta: ¿Cuál fue la respuesta del gobierno de Corea del Norte a la película “La entrevista”, comedia en la que la CIA planea matar a Kim Jong-un?

Respuesta: Ciberataque a Sony Pictures

Justificación: En noviembre de 2014, Sony Pictures sufrió un ataque cibernético después de que un grupo de hackers que se llamaban a sí mismos Guardianes de la Paz obtuvieran acceso a la red de computadoras de la compañía. Corea del Norte negó su responsabilidad, pero describió el ataque como una "acción justa" en respuesta a la película de Sony "La entrevista", una comedia que describe la muerte violenta de Kim Jong-un de Corea del Norte [96].

Pregunta: ¿Cuál es el significado de las siglas PUP?

Respuesta: Potentially Unwanted Program o programa potencialmente no deseado

Justificación: Un programa potencialmente no deseado (PUP, Potentially Unwanted Program en inglés) es, tal y como su propio nombre describe, un programa no deseado. Un usuario puede ser engañado o inducido a descargar este tipo de programa con o sin su consentimiento explícito. Estos programas no deseados son normalmente descargados junto a un programa sí deseado, que sirve como transporte o pantalla para esconder el rastro del PUP [97].

Pregunta: ¿Cuál es la parte de la criptología que se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad?

Respuesta: Criptoanálisis

Justificación: El criptoanálisis es la parte de la criptología que se dedica al estudio de sistemas criptográficos con el fin de encontrar debilidades en los sistemas y romper su seguridad sin el conocimiento de información secreta. En el lenguaje no técnico, se conoce esta práctica como romper o forzar el código, aunque esta expresión tiene un significado específico dentro del argot técnico. A las personas que se dedican al criptoanálisis se llaman criptoanalistas [98].

Pregunta: ¿Cuál es el significado de las siglas TOR?

Respuesta: The Onion Router o el router cebolla

Justificación: El nombre TOR son las siglas de 'The Onion Router', el router Cebolla, y es posiblemente la principal y más conocida Darknet de Internet. El objetivo de este proyecto es el de crear una red de comunicaciones distribuida y superpuesta al Internet convencional. Las Dark Webs que puedes encontrar en la Darknet de TOR se diferencian por tener el dominio .onion [99].

Pregunta: ¿Cómo se conoce al contenido de Internet que no está indexado por los motores de búsqueda convencionales donde reside la mayor parte de la información existente?

Respuesta: Deep web o Internet profunda

Justificación: Internet profunda (del inglés, deep web), es el contenido de internet que no está indexado por los motores de búsqueda convencionales, debido a diversos factores. La principal causa de la existencia de la internet profunda es la imposibilidad de los motores de búsqueda (ejemplo: Google, Yahoo y Bing, y otros) de encontrar o indexar gran parte de la información existente en Internet [100].

Pregunta: ¿Cómo se llama el servicio desarrollado por el CCN-CERT cuyo objetivo es la detección en tiempo real de ataques y amenazas, llevado a cabo a través del análisis del tráfico de red que circula entre las redes de los Organismos de las Administraciones Públicas?

Respuesta: SAT-SARA

Justificación: El Sistema de Alerta Temprana (SAT) de la red SARA (SAT-SARA) es un servicio desarrollado por el CCN-CERT en colaboración con el Ministerio de Hacienda y Administraciones Públicas (Organismo responsable de la red SARA). Su objetivo es la detección en tiempo real de ataques y amenazas, llevado a cabo a través del análisis del tráfico de red que circula

entre las redes de los Organismos de las Administraciones Públicas conectados a la red SARA [101].

Pregunta: ¿Cómo se llama la solución endpoint desarrollada por el CCN cuyo objetivo principal es la detección de malware complejo y movimiento lateral relacionado con APTs?

Respuesta: Claudia

Justificación: Claudia es una solución de endpoint integrada con la herramienta Carmen que permite tener una visión más completa de lo que ocurre dentro de una red, siendo su objetivo principal la detección de malware complejo y movimiento lateral relacionado con APT [102].

Pregunta: ¿Por qué número es conocido el grupo APT Emissary Panda?

Respuesta: APT27

Justificación: Associated Groups: TG-3390, Emissary Panda, BRONZE UNION, APT27, Iron Tiger, LuckyMouse [103].

3.5. Cartas especiales

A continuación se desarrollan las cartas especiales, se introducirán dos de cada tipo, para un total de 16 cartas.

- RECARGA. Puedes cambiar tu pregunta una vez te la hayan leído.

- RECARGA. Cambia la pregunta a tu oponente una vez leída.

- COBERTURA. Suma 1 al resultado de tu tirada.

- COBERTURA. Resta 1 al resultado de la tirada de tu oponente.

- OTRA OPORTUNIDAD. Si fallas una pregunta, puedes volver a tirar. ¡No pierdes turno, aprovéchalo!

- SOLO ANTE EL PELIGRO. Elije al oponente que va a responder la pregunta antes de que la lean. El resto de sus compañeros no podrán ayudarle en la respuesta.

- HORA DEL RETO. Reta a un oponente por un emblema que ya esté en su posesión y elije uno tuyo que el oponente no tenga. Los dos equipos deberán retarse por dicho emblema. Haz una ronda de 5 preguntas (1 tarjeta), quien más preguntas acierte se quedará con el emblema. En caso de empate, no ocurre nada.

- DOBLE OPCIÓN. Restas al equipo adversario 25'' para responder la pregunta.

Capítulo 4. Costes

Tras haber finalizado el desarrollo del juego de mesa Securiza2, y teniendo en cuenta la inversión de tiempo planificada al inicio del proyecto, procedemos a calcular el presupuesto y los recursos necesarios para el mismo.

4.1. Coste temporal

La realización del proyecto comenzó el 19 de febrero de 2020 y ha finalizado el 2 de junio de 2020, teniendo una duración total de 75 días, que entra dentro de lo que se planificó inicialmente.

Lo que sí que ha variado significativamente de la planificación inicial ha sido el reparto de tareas, que debido a compromisos laborales y a la situación provocada por la crisis sanitaria del COVID-19, ha provocado que el desarrollo de las preguntas se llevara a cabo durante la entrega 3 y 4.

Además, y como ya se ha comentado anteriormente, dada la situación creada por la pandemia del COVID-19, ha resultado imposible poder imprimir el juego en la entrega 3, y se llevará a cabo más adelante como se indica en el trabajo futuro.

4.2. Coste económico

Teniendo en cuenta que el proyecto ha sido llevado a cabo por una persona durante 75 días, calcularemos el coste del salario del trabajador en función de la información proporcionada por los Boletines oficiales del Estado.

Según el Régimen General de la Seguridad Social, un Ingeniero Telemático tiene una base mínima mensual de 994,20€ [104].

Se considerará como sueldo la base mínima mensual, ya que vamos a suponer que este TFM es nuestro primer proyecto y carecemos de experiencia laboral. Se estimará el trabajo de tres meses de Ingeniero Telemático, ya que su salario se calcula a mes completo.

$$Coste\ trabajador = \frac{994.20€}{\text{mes}} \times 3\ meses\ = 2982.60€$$

A este coste se añadirá el 28.30% de cotización a la seguridad social [104].

COSTES DEL TRABAJADOR ⟹ **3826.67€**

El único coste de hardware a considerar en este proyecto es el ordenador personal utilizado para el desarrollo completo de este proyecto.

El ordenador fue comprado en el año 2015 por 989.99€. Al ser un ordenador portátil de alta gama, se puede considerar que la vida media de este ronda los 7 años, por lo que, todavía tendremos un rendimiento óptimo por al menos 2 años más.

Calculamos la amortización anual:

$$Amortización\ anual = \frac{precio\ de\ compra}{años\ de\ vida\ media} = \frac{989.99€}{7\ años} = 141.42€/año$$

Teniendo en cuenta que el proyecto durará unos 75 días (2,5 meses), el coste del equipo será:

$$Coste = \frac{141.42€/año}{12\ meses} \times 2.5\ \ meses\ = 29.46€$$

En la siguiente tabla se refleja el coste económico final teniendo en cuenta los recursos que han sido y serán necesarios para el desarrollo del proyecto:

CONCEPTO	COSTE (€)
Costes hardware	29.46
Costes software (Microsoft Word y Licencia Adobe Illustrator)	83.58
Costes del trabajador	3826.67
Costes de impresión tablero y 36 cartas (Tablero cartón pluma 38x38 cm)	25.18
Componentes del juego (dado, peones, emblemas, portaemblemas y cronómetro)	39.16
Total	**4004.05**

Tabla 1: Costes

Por tanto, y como se puede observar, el mayor gasto es el sueldo del trabajador, y el resto de costes son asumibles, por lo que podríamos decir que el proyecto es viable económicamente hablando.

Capítulo 5. Conclusiones

5.1. Conclusiones finales

Como conclusión, el TFM se ha desarrollado satisfactoriamente, dentro de los plazos establecidos inicialmente y pese a las dificultades añadidas por la situación provocada por el COVID-19.

A nivel personal, el desarrollo del trabajo me ha servido para llevar a cabo satisfactoriamente un proyecto de investigación, donde he podido aplicar los conocimientos aprendidos durante el máster en ciberseguridad.

Por otra parte, a nivel profesional, este TFM me servirá para poder poner en práctica los conocimientos aprendidos, y poder jugar con compañeros especializados en ciberseguridad. Sin duda, será una muy buena actividad para poder aprender y reforzar conocimientos mientras pasamos un buen rato.

Finalmente, tras la realización del proyecto he comprendido que actualmente es necesario un juego que trate la ciberseguridad con el fin de poder concienciar a la sociedad sobre lo expuestos que estamos continuamente a peligros digitales.

5.2. Problemas encontrados en el desarrollo del proyecto

Durante la realización del TFM han ido surgiendo algunos problemas:

- Dada la situación provocada por la crisis sanitaria del COVID-19, ha sido imposible imprimir el juego, tarea que estaba prevista para le entrega 3. Una vez se reanude la normalidad, está previsto imprimir el juego y sus cartas, con el fin de poder probarlo.

- Al estar basado en un juego bastante conocido por todos, ha resultado complicado diferenciarlo. Finalmente se ha optado por añadir elementos extra, como las cartas especiales, que le aportan mayor versatilidad al juego.

- La falta de información académica sobre los juegos de mesa aplicados al campo de la ciberseguridad también ha dificultado el desarrollo del capítulo del Estado del Arte.

- En la formulación de las preguntas, también he encontrado dificultades a la hora de encontrar preguntas válidas sobre un tema tan concreto, y que además, encajara bien en las categorías propuestas. Finalmente, con un trabajo de investigación y análisis de documentos, se ha logrado formular todas las preguntas satisfactoriamente.

5.3. Trabajo futuro

Una vez finalizado el proyecto, se proponen varias líneas de trabajo futuro con el fin de mejorar el proyecto:

- Como ya se ha comentado anteriormente, dada la pandemia provocada por el COVID-19, ha resultado imposible poder imprimir el tablero del juego así como las cartas, por lo que está planteado llevarlo a cabo en un futuro.

- Una vez el juego esté impreso, se probará con el fin de detectar cualquier error o desajuste y poder corregirlo.

- Finalmente, se plantea formular más preguntas de cada categoría e ir añadiéndolas progresivamente al juego, con el fin de darle una mayor jugabilidad y versatilidad.

Referencias

[1] Anderson, O., B., Anderson, N., M., Taylor, A., T. (2009). New Territories in Adult Education: Game-Based Learning for Adult Education.

[2] McGonigal, J. (2011). Reality is broken: Why games make us better and how they can change the world. New York, NY: Penguin Books.

[3] Charlier, N., Ott, M., Remmelle, B., Whitton, N. (2012). Not just for children: game-based learning for older adults.

[4] Castell, S. (2011). Ludic Epistemology: What Game-Based Learning Can Teach Curriculum Studies.

[5] Recuperado el 2 de abril del 2020 de: https://www.redeszone.net/tutoriales/internet/que-es-comando-tracert-traceroute/

[6] Recuperado el 2 de abril del 2020 de: https://www.websecurity.digicert.com/es/es/security-topics/what-is-ssl-tls-https

[7] Recuperado el 2 de abril del 2020 de: https://www.ionos.es/digitalguide/servidores/seguridad/rainbow-tables/

[8] Recuperado el 2 de abril del 2020 de: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_informaci%C3%B3n_y_eventos_de_seguridad

[9] Recuperado el 2 de abril del 2020 de: https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica

[10] Recuperado el 2 de abril del 2020 de: https://es.wikipedia.org/wiki/IPsec

[11] Recuperado el 2 de abril del 2020 de: https://es.wikipedia.org/wiki/Anexo:N%C3%BAmeros_de_puertos_de_red

[12] Recuperado el 2 de abril del 2020 de: https://es.wikipedia.org/wiki/Snort

[13] Recuperado el 2 de abril del 2020 de: https://www.ciset.es/publicaciones/blog/746-hardening

[14] Recuperado el 2 de abril del 2020 de: https://es.wikipedia.org/wiki/Bastion_host

[15] Recuperado el 3 de abril del 2020 de: https://es.wikipedia.org/wiki/Sumidero_de_DNS

[16] Recuperado el 3 de abril del 2020 de: https://www.welivesecurity.com/la-es/2013/03/18/heuristica-antivirus-deteccion-proactiva-amenazas/

[17] Recuperado el 3 de abril del 2020 de: https://suricata.readthedocs.io/en/suricata-4.1.4/configuration/suricata-yaml.html

[18] Recuperado el 3 de abril del 2020 de: https://suricata.readthedocs.io/en/suricata-4.1.4/rules/payload-keywords.html#pcre-perl-compatible-regular-expressions

[19] Recuperado el 3 de abril del 2020 de: https://www.tcpdump.org/manpages/tcpdump.1.html

[20] Recuperado el 3 de abril del 2020 de: https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

[21] Recuperado el 3 de abril del 2020 de: https://es.wikipedia.org/wiki/Indicador_de_compromiso

[22] Recuperado el 3 de abril del 2020 de: https://openwebinars.net/blog/almacenar-contrasenas-bases-de-datos/

[23] Recuperado el 3 de abril del 2020 de: https://eprints.ucm.es/16065/1/Sistema_de_deteccion_de_anomalias_de_red_basado_en_procesamiento_de_carga_util.pdf

[24] Recuperado el 3 de abril del 2020 de: https://eprints.ucm.es/16065/1/Sistema_de_deteccion_de_anomalias_de_red_basado_en_procesamiento_de_carga_util.pdf

[25] Recuperado el 3 de abril del 2020 de: https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html

[26] Recuperado el 3 de abril del 2020 de: http://www.ticarte.com/contenido/que-es-footprinting-y-fingerprinting

[27] Recuperado el 6 de abril del 2020 de: https://en.wikipedia.org/wiki/Rainbow_table

[28] Recuperado el 6 de abril del 2020 de: https://blog.evidaliahost.com/cross-site-request-forgery-csrf/

[29] Recuperado el 6 de abril del 2020 de: https://www.osi.es/es/actualidad/blog/2015/05/08/sabes-lo-que-es-el-malvertising-y-como-estar-protegido-frente-el

[30] Recuperado el 6 de abril del 2020 de: https://www.ionos.es/digitalguide/servidores/seguridad/ip-spoofing-fundamentos-y-contramedidas/

[31] Recuperado el 6 de abril del 2020 de: https://hackstory.net/Phreaking

[32] Recuperado el 6 de abril del 2020 de: https://ehack.info/las-fases-del-hacking-etico/

[33] Recuperado el 6 de abril del 2020 de: https://es.wikipedia.org/wiki/Vishing

[34] Recuperado el 6 de abril del 2020 de: https://www.redseguridad.com/actualidad/pretexting-los-ciberdelincuentes-utilizan-el-telefono-para-robar-informacion-confidencial_20130605.html

[35] Recuperado el 6 de abril del 2020 de: https://es.wikipedia.org/wiki/Desbordamiento_de_mont%C3%ADculo

[36] Recuperado el 6 de abril del 2020 de: https://es.wikipedia.org/wiki/Ping_de_la_muerte

[37] Recuperado el 6 de abril del 2020 de: https://es.wikipedia.org/wiki/Pharming

[38] Recuperado el 6 de abril del 2020 de: https://es.wikipedia.org/wiki/Nmap

[39] Recuperado el 8 de abril del 2020 de: https://es.wikipedia.org/wiki/Ataque_de_abrevadero

[40] Recuperado el 8 de abril del 2020 de: https://www.cyberseguridad.net/index.php/197-ataques-de-denegacion-de-servicio-dos-ataques-informaticos-iii

[41] Recuperado el 8 de abril del 2020 de: https://es.wikipedia.org/wiki/Web_scraping

[42] Recuperado el 8 de abril del 2020 de: https://backtrackacademy.com/articulo/que-es-el-clickjacking

[43] Recuperado el 8 de abril del 2020 de: https://www.pandasecurity.com/es/security-info/cryptojacking/

[44] Recuperado el 13 de abril del 2020 de: https://www.incibe-cert.es/blog/esteganografia-y-estegoanalisis-basicos

[45] Recuperado el 13 de abril del 2020 de: https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra

[46] Recuperado el 13 de abril del 2020 de: https://es.wikipedia.org/wiki/EternalBlue

[47] Recuperado el 13 de abril del 2020 de: https://es.wikipedia.org/wiki/ILoveYou

[48] Recuperado el 13 de abril del 2020 de: https://es.wikipedia.org/wiki/Exploit

[49] Recuperado el 13 de abril del 2020 de: https://es.wikipedia.org/wiki/Exploit

[50] Recuperado el 13 de abril del 2020 de: https://subscription.packtpub.com/book/networking_and_servers/9781788392501/8/ch08lvl1sec62/4-hooking-techniques

[51] Recuperado el 13 de abril del 2020 de: https://es.wikipedia.org/wiki/Programa_esp%C3%ADa

[52] Recuperado el 13 de abril del 2020 de: https://en.wikipedia.org/wiki/BlueKeep

[53] Recuperado el 15 de abril del 2020 de: https://desarrolloweb.com/faq/que-es-grayware

[54] Recuperado el 15 de abril del 2020 de: https://es.wikipedia.org/wiki/Polimorfismo_(malware)

[55] Recuperado el 15 de abril del 2020 de: https://es.wikipedia.org/wiki/Crypter

[56] Recuperado el 15 de abril del 2020 de: https://es.wikipedia.org/wiki/Desensamblador

[57] Recuperado el 20 de abril del 2020 de: https://es.wikipedia.org/wiki/Cracking_(software)

[58] Recuperado el 20 de abril del 2020 de: https://www.enter.co/chips-bits/seguridad/los-10-virus-mas-famosos-de-la-historia-disi-2010/

[59] Recuperado el 20 de abril del 2020 de: https://attack.mitre.org/software/S0013/

[60] Recuperado el 20 de abril del 2020 de: https://www.welivesecurity.com/la-es/2019/12/05/fileless-malware-que-es-como-funciona-malware-sin-archivos/

[61] Recuperado el 20 de abril del 2020 de: https://es.wikipedia.org/wiki/An%C3%A1lisis_de_malware

[62] Recuperado el 22 de abril del 2020 de: http://curiosidadestecnologicasycomputacion.blogspot.com/p/registros-de-pila-y-registros-de.html

[63] Recuperado el 2 de abril del 2020 de: https://en.wikipedia.org/wiki/Radare2

[64] Recuperado el 22 de abril del 2020 de: https://attack.mitre.org/software/S0020/

[65] Recuperado el 6 de mayo del 2020 de: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

[66] Recuperado el 6 de mayo del 2020 de: https://es.wikipedia.org/wiki/Seudonimizaci%C3%B3n

[67] Recuperado el 6 de mayo del 2020 de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

[68] Recuperado el 6 de mayo del 2020 de: https://www.aenor.com/certificacion/tecnologias-de-la-informacion/continuidad-negocio

[69] Recuperado el 6 de mayo del 2020 de: https://www.ccn-cert.cni.es/ens.html

[70] Recuperado el 6 de mayo del 2020 de: https://hackernoon.com/introducing-the-infosec-colour-wheel-blending-developers-with-red-and-blue-security-teams-6437c1a07700

[71] Recuperado el 6 de mayo del 2020 de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-28000/

[72] Recuperado el 6 de mayo del 2020 de: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

[73] Recuperado el 6 de mayo del 2020 de: https://es.wikipedia.org/wiki/Asociaci%C3%B3n_Espa%C3%B1ola_de_Normalizaci%C3%B3n

[74] Recuperado el 6 de mayo del 2020 de: https://www.secureit.es/procesos-y-gobierno-it/analisis-y-gestion-de-riesgos/

[75] Recuperado el 6 de mayo del 2020 de: https://dpd.aec.es/el-ens-como-parte-del-rgpd-esquema-nacional-de-seguridad/

[76] Recuperado el 6 de mayo del 2020 de: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1117

[77] Recuperado el 8 de mayo del 2020 de: https://www.emprendepyme.net/politicas-de-seguridad.html

[78] Recuperado el 8 de mayo del 2020 de: https://es.wikipedia.org/wiki/Reglamento_General_de_Protecci%C3%B3n_de_Datos

[79] Recuperado el 8 de mayo del 2020 de: https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

[80] Recuperado el 8 de mayo del 2020 de: https://www.securityartwork.es/2013/04/25/introduccion-al-diseno-y-certificacion-de-cpds-tia-942/

[81] Recuperado el 8 de mayo del 2020 de: https://www.incibe.es/sites/default/files/contenidos/dosieres/metad_plan_de_contingencia_y_continuidad_de_negocio.pdf

[82] Recuperado el 8 de mayo del 2020 de: https://derechoeinternet.wordpress.com/2012/01/24/alternativas-de-

recuperacion-de-desastres-contratos-hotwarmcold-site-contrato-de-instalaciones-duplicadas-sitios-moviles-y-acuerdos-reciprocos/

[83] Recuperado el 8 de mayo del 2020 de: https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad

[84] Recuperado el 11 de mayo del 2020 de: https://www.cic.es/que-es-un-sgsi/

[85] Recuperado el 11 de mayo del 2020 de: https://es.wikipedia.org/wiki/Instituto_Nacional_de_Ciberseguridad

[86] Recuperado el 11 de mayo del 2020 de: https://es.wikipedia.org/wiki/Modelo_OSI

[87] Recuperado el 11 de mayo del 2020 de: https://en.wikipedia.org/wiki/DEF_CON

[88] Recuperado el 11 de mayo del 2020 de: https://www.elmundo.es/tecnologia/2014/02/01/52eca305ca474133388b456d.html

[89] Recuperado el 11 de mayo del 2020 de: https://es.wikipedia.org/wiki/Hacktivismo

[90] Recuperado el 11 de mayo del 2020 de: https://es.wikipedia.org/wiki/Sombrero_gris

[91] Recuperado el 14 de mayo del 2020 de: https://en.wikipedia.org/wiki/Script_kiddie

[92] Recuperado el 14 de mayo del 2020 de: https://es.wikipedia.org/wiki/Oficial_de_seguridad_de_la_informaci%C3%B3n

[93] Recuperado el 14 de mayo del 2020 de: https://es.wikipedia.org/wiki/The_Amnesic_Incognito_Live_System

[94] Recuperado el 14 de mayo del 2020 de: https://es.wikipedia.org/wiki/Doxing

[95] Recuperado el 14 de mayo del 2020 de: http://www.teinteresa.es/tecno/Investigadores-detectan-ciberataque-documentos-secretos_0_847717434.html

[96] Recuperado el 14 de mayo del 2020 de: https://www.dw.com/es/seis-ataques-cibern%C3%A9ticos-que-sacudieron-el-mundo/a-46967214

[97] Recuperado el 15 de mayo del 2020 de: https://blog.360totalsecurity.com/es/programas-pup/

[98] Recuperado el 15 de mayo del 2020 de: https://es.wikipedia.org/wiki/Criptoan%C3%A1lisis

[99] Recuperado el 15 de mayo del 2020 de: https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa

[100] Recuperado el 15 de mayo del 2020 de: https://es.wikipedia.org/wiki/Internet_profunda

[101] Recuperado el 15 de mayo del 2020 de: https://www.ccn-cert.cni.es/gestion-de-incidentes/sistema-de-alerta-temprana-sat/sat-sara.html

[102] Recuperado el 15 de mayo del 2020 de: https://www.ccn-cert.cni.es/soluciones-seguridad/claudia.html

[103] Recuperado el 15 de mayo del 2020 de: https://attack.mitre.org/groups/G0027/

[104] Recuperado el 19 de mayo del 2020 de: http://www.seg-social.es/wps/portal/wss/internet/Trabajadores/CotizacionRecaudacionTrabajadores/36537