ULPGC Universidad de Las Palmas de Gran Canaria | Escuela de Ingeniería Informática

Desarrollo de un simulador de ataques donde practicar amenazas informáticas: implementación de la web, modelo de negocio y análisis de viabilidad

TITULACIÓN: Grado en Ingeniería Informática (plan 40)

AUTOR: Karan Nandpal Sainani

TUTORIZADO POR:
Jorge Marín Rodríguez Díaz

07/2023

Agradecimientos

Para empezar me gustaría agradecer a mi tutor, Jorge Marín Rodríguez Díaz, por su ayuda a la hora de realizar este Trabajo Fin de Grado. También agradecer a mi madre y mi hermana por darme su apoyo incondicional por seguir superándome día tras día en superar esta carrera y cumplir con mis metas personales. También agradecer a mis amigos de la facultad que han estado ahí tanto en los malos y en los buenos momentos de la carrera. Muchas gracias de verdad a todos los que han formado parte de esta etapa tan maravillosa de mi vida.

Resumen

Se trata de una web en donde poder practicar las distintas vulnerabilidades informáticas tanto encontradas en las noticias como las que se pueden encontrar por la red en distintos foros, web especializadas etc. La idea se centra en poder ofrecer al usuario una experiencia estilo a la página **https://www.hackthissite.org/**. De esta manera conseguimos, concienciar el uso correcto de los distintos elementos informáticos en una web para por ejemplo poder evitar un ataque por inyección sql en la base de datos de una empresa X entre otras prácticas fraudulentas. La ciberseguridad es un campo de la informática que esta en constante movimiento y las empresas necesitan proteger su principal activo, que es la información. Además, se planteará una propuesta de un modelo de negocio basado en esta idea y el estudio de viabilidad de la misma.

Abstract

It is a website where you can practice the different computer vulnerabilities both found in the news and those that can be found online in different forums, specialized websites, etc. The idea is focused on being able to offer the user a similar style experience to the page **https://www.hackthissite.org/**. In this way we managed to raise awareness of the correct use of the different computer elements on a website. For example, be able to avoid an attack by sql injection in the database of a company X, among other fraudulent practices. Cybersecurity is a field of computer science that is in constant movement and companies need to protect their most important asset, which is information. In addition, the work also include a proposal for a business model based on this idea and its feasibility study will be proposed.

ÍNDICE GENERAL

Índice de Ilustraciones

Índice de tablas

Índice de gráficos

Capítulo 1: Introducción

Este trabajo fin de grado se centra en el desarrollo de una página web sobre ciberseguridad, con distintos retos para poner a prueba la seguridad de las webs, que sirva para concienciar a todo tipo de público de cara a mantener unas buenas prácticas de uso de estos sistemas. También se plantea una propuesta de un modelo de negocio basado en esta idea y un estudio de viabilidad del mismo.

Además de concienciar a todo tipo de público, lo que se intenta es que se tenga especial precaución cuando ingresamos nuestros datos y dar a conocer cómo se manipulan en la red. La ciberseguridad juega un papel fundamental en todos los ámbitos tecnológicos ya que estamos en la red expuestos ante cualquier acto fraudulento, como la suplantación de identidad o la ingeniería social, entre otras actividades maliciosas (INCIBE, 2019). Asimismo, conseguimos webs seguras que aún así podrán tener fallos de seguridad que mediante los retos implementados veremos. Se ha trabajado con conceptos ligados a las asignaturas de Redes, Análisis de la Seguridad de los Sistemas de Información e Innovación y Creación de Empresas con Base Tecnológica, las cuales se ven en la especialidad de Sistemas de Información correspondiente al plan antiguo del grado en Ingeniería Informática (plan 40, en extinción).

Esta idea nace después de haber realizado unas prácticas de Erasmus en donde una actividad era superar los retos de conocimientos en ciberseguridad de la página web de ejemplo (HackThisSite, 2023) en la que nos estamos apoyando la cual también se referencia al principio de esta memoria, concretamente en el resumen y en el abstract. Al realizar estas prácticas y viendo la importancia de la ciberseguridad a día de hoy y su demanda en el mercado actual, nos ha motivado a indagar más sobre el tema leyendo bibliografía, viendo noticias, web especializadas, distintos foros , etc.

Se tiene como principal objetivo, reforzar todo tipo de sitio web para su correcta puesta en funcionamiento en la red. Aparte de superar los retos, también se dispone de un foro en donde los usuarios puedan discutir y proponer nuevos retos como si fuera una especie de red colaborativa. También se ha implementado una prueba de conocimientos para saber si de verdad se está entendiendo el concepto que se está trabajando en cada reto. Se ha implementado también una sección en donde se puede ver toda la teoría con respecto a estos conceptos trabajados para que se tenga todo en un sitio y el usuario tenga todo a mano en la misma web.

Los ataques informáticos surgen día tras día en nuestro entorno personal, laboral, social, etc. (INCIBE, 2020). Desde mensajes a nuestros móviles diciendo que nos ha llegado un paquete de correos correctamente y nos solicitan confirmación de nuestros datos personales. A primera vista, viendo el link que se nos proporciona se puede determinar que estamos ante un caso de phishing al no corresponder de una URL válida, como vemos en la Ilustración 1.

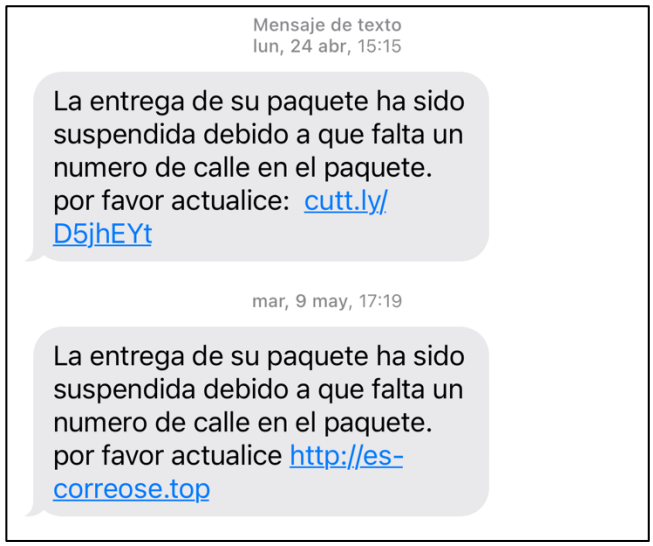

Ilustración 1. Mensaje de phishing

Fuente: Elaboración propia.

También detectar un correcto inicio de sesión en nuestra cuenta, en caso de sospecha recurrir a nuestro proveedor y solicitar un cambio en la contraseña para de esta manera estar seguros de que somos nosotros los que iniciamos sesión en la cuenta. Google por ejemplo, advierte en cada inicio de sesión si de verdad somos nosotros los que iniciamos sesión y en caso de serlo no hace falta que hagamos nada ya que la actividad no es sospechosa, como se puede observar en la Ilustración 2.

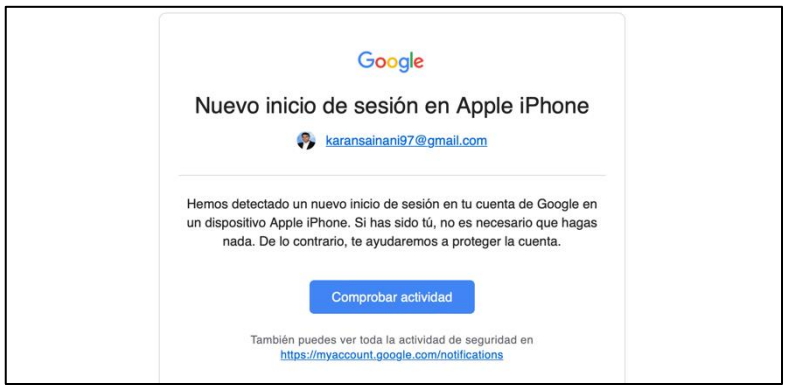

Ilustración 2. Correo de confirmación

Fuente: Elaboración propia.

Respecto a la política de las contraseñas, estas han de ser lo más fuertes posibles para que el atacante no pueda averiguarla, ya sea mediante los métodos tradicionales, por ejemplo por cualquier tipo de ingeniería social como lo es el phishing, un keylogger, que se trata de un tipo de malware cuya idea principal se centra en las pulsaciones de teclado del usuario en cuestión, ya que esta información queda registrada, o a través de la conexión si es que tenemos a un ciberdelincuente conectado a nuestra misma red que intercepte los paquetes que contiene la información de la contraseña, entre otros actos fraudulentos (Infobae, 2022). A continuación veremos una tabla en donde se detalla la importancia de los caracteres que han de ponerse en las contraseñas y el tiempo que tardaría el atacante en descubrirla. Observamos la Ilustración 3.

Número de caracteres	Solo números	Letras minúsculas	Minúsculas y mayúsculas	Números, minúsculas y mayúsculas	Números, minúsculas, mayúsculas y símbolos
4	Instant.	Instant.	Instant.	Instant.	Instant.
5	Instant.	Instant.	Instant.	Instant.	Instant.
6	Instant.	Instant.	Instant.	Instant.	Instant.
7	Instant.	Instant.	2 seg.	7 seg.	31 seg.
8	Instant.	Instant.	2 min.	7 min.	39 min.
9	Instant.	10 seg.	1 hora	7 horas	2 días
10	Instant.	4 min.	3 días	3 semanas	5 meses
11	Instant.	2 horas	5 meses	3 años	34 años
12	2 seg.	2 días	24 años	200 años	3K años
13	19 seg.	2 meses	1K años	12K años	202K años
14	3 min.	4 años	64K años	750K años	16M años
15	32 min.	100 años	3M años	46M años	1BN años
16	5 horas	3K años	173M años	3BN años	92BN años
17	2 días	69 K años	9BN años	179BN años	7TN años
18	3 semanas	2M años	467BN años	11TN años	438TN años

Ilustración 3. Tabla de seguridad contraseñas

Fuente: Infobae (2022)

Es importante también tener en cuenta que se recomienda que las contraseñas han de ser cambiadas cada trimestre como mínimo (Hoswedaje, 2023). No pueden contener ni nombres, ni fechas, ni cualquier tipo de información sensible. Ha de ser auténtica y distinta en todos los aspectos. También en muchos sitios en la red si una contraseña no es usada en al menos 60 días, la cuenta de usuario quedaría desactivada. Pudiéndose activar más tarde al proporcionar las credenciales y las respuestas a las preguntas de seguridad que hayamos establecido en la creación de la cuenta.

Finalmente, añadir que, de cara al mundo laboral, esto se sigue estableciendo en la actualidad y también se ha de matizar en la política de derecho de acceso de las cuentas de un sistema de un trabajo X. El administrador del sistema ha de tener el control absoluto del sistema. Los empleados pueden acceder únicamente a su entorno de trabajo y los jefes de departamentos tienen los mismos privilegios que los empleados pero con la diferencia de que pueden monitorizar todos los accesos para asegurarse de que todo está en orden entre otras actividades privilegiadas.

Capítulo 2: Estado actual y objetivos iniciales

2.1 – Estado actual

Hoy en día la ciberseguridad juega un papel fundamental en nuestra sociedad ya que vivimos en la era de la información. Todas las empresas tecnológicas necesitan expertos con conocimientos en ciberseguridad para proteger su producto y ofrecer seguridad a la hora de comprar dicho producto teniendo la página web con protocolo https entre otras tecnologías aplicables en el proceso de compra (Nunsys, 2023). También tener especial cuidado con qué datos introducimos en las webs, ya que estos probablemente van a pertenecer a la entidad con la que estamos tratando, es decir, debemos de verificar si estamos ante un página web oficial o no.

También debemos asegurar nuestro entorno personal, cuando estamos en casa, por ejemplo, que un atacante puede estar accediendo a nuestra red y nosotros sin estar enterándonos. Para evitar esta actividad sospechosa se debería establecer en la terminal de nuestro ordenador, una lista de direcciones MAC (dirección física de un único dispositivo de red), así tenemos como una especie de invitados que pueden acceder a nuestro wifi. Esto no se suele ver en cafeterías, bares, restaurantes , etcétera, ya que estamos intentando acceder a una red pública y podemos estar en peligro ya que los paquetes con nuestra información viajan por esa red pública y un atacante se puede apropiar de ella fácilmente. Por lo tanto, se recomienda no acceder a redes inseguras como las públicas (Kaspersky, 2023).

Podemos observar respecto a los ciberataques que, estos se producen muchas veces al año. Esta universidad ha recibido varios ataques también como el que sucedió en 2018 (La Provincia, 2018). Se trataba de un ataque DDoS (Ataques de Denegación de Servicios Distribuidos), el cual estaba colapsando la conexión a Internet de la ULPGC, provocando que los servicios universitarios (web, campus virtual, etc.) dejen de funcionar. También las grandes compañías sufren ataques masivos de robo de datos, como el caso de British Airways que los atacantes habían sustraído información sensible (El Confidencial, 2018), como tarjetas de pago, domicilio, nombres, apellidos, y todo lo referente a cuando compramos un billete de avión y los afectados tenían que contactar con los bancos para esclarecer esta situación. Dirigiéndonos ahora a las compañías mas vistas en la prensa y en las noticias, Facebook también sufre este tipo de ataques (Expansión, 2018). Está claro que el hecho de que una de las compañías mas grandes del mundo reciba un ataque

es algo que sorprende bastante. Evidentemente, Facebook ha de reforzar su seguridad en todos los aspectos para conservar a sus usuarios contentos. No obstante, no resulta fácil incluso cuando la compañía tiene como negocio central los datos de sus usuarios, la seguridad absoluta en la red es difícil de conseguir. Se vieron 30 millones de cuentas de usuarios afectadas entre ellas la de propia Mark Zuckerberg inclusive. Al parecer los atacantes se apoderaron de las llaves (tokens) las cuales sirven para guardar la contraseña de un determinado usuario, otorgando al hacker el pleno control de su vida al estar expuesta en este sitio.

Si comparamos ambas noticias, podemos afirmar que es bastante fácil que ocurran estos ataques de nuevo, sobre todo en una red social tan conocida como Facebook, ya que el principal factor de este delito es capturar la mayor masa de información posible sobre sus usuarios. Si a esto le añadimos tanto datos personales como bancarios, que sucedió en el caso de la aerolínea, supone un grave riesgo de perder no solo datos sino dinero también. Cabe destacar en noticias relacionadas que hemos podido observar en diversas fuentes el problema puede surgir de la auditorías que realizan la comprobación correcta de los sistemas de seguridad y no de la compañía en sí, pero digamos que son meras especulaciones que los expertos afirman.

A la hora seleccionar un trabajo, hay que tener estudiada la teoría para que refleje que tenemos cierto dominio en la materia y algunas de las preguntas que suelen hacer los entrevistadores (The Bridge, 2021), son las siguientes:

1) ¿Qué entiende usted por Firewall?

2) ¿Cómo resolviste el peor ataque al que te has enfrentado?

3) ¿Cuáles son las diferencias entre amenazas, vulnerabilidades y riesgos?

4) ¿Cuáles son los ataques más comunes?

Por lo tanto, si queremos adentrarnos en el mundo de la ciberseguridad, tenemos que estar actualizados diariamente para saber distintos tipos de ataques, como se ejecutan, como se resuelven y todo eso conlleva saberse la base de cada uno de ellos y los conceptos básicos. En general, el campo de la informática es muy variante y cada vez aparecen nuevas tecnologías y debemos de ajustarnos al cambio dado a que este suele ser más óptimo y mejor respecto a los que solemos estar habituados a conocer. Tener un perfil proactivo, innovador, creativo, etc., para poder afrontar nuevos problemas. Con respecto a la ciberseguridad en sí, "cacharrear" con la web/aplicación para buscar fallos de seguridad resulta ser un tarea primordial y en su caso, mejorarla para que no vuelva a producirse de nuevo.

2.2 – Objetivos iniciales

Este Trabajo Fin de Grado tiene como objetivos iniciales los siguientes:

- Conseguir el desarrollo de la web en su versión de propuesta mínima viable (PMV), es decir, no nos hemos centrado en desarrollo de la web al máximo sino en de tratar de explicar conceptos de ciberseguridad y de creación de empresas. En la actualidad la web estaría un poco obsoleta dado a que no resulta tan atractiva como las webs actuales.

- Implementación de foros de discusión para proponer nuevos retos, corregirlos, etc. Aquí lo que estamos consiguiendo es que se trate de una red colaborativa estilo Stack Overflow (Stack Overflow, 2023), en donde el usuario puede plantear nuevas soluciones que entre, otras actividades, fortalezcan la web. Para que haya un poco de interacción entre los usuarios.

- Implementación de distintos niveles que requieren cierto dominio de la informática. Inicialmente la web está destinada para aquellas personas que tienen ciertos conocimientos en informática pero, más adelante se programó una sección de teoría en donde se detalla el concepto que se está intentando trabajar en cada reto. Por lo tanto, nuestro segmento de cliente es apto para todo tipo de público, tanto para el quiera iniciarse como el que no tenga conocimientos de nada relacionado con la informática/ciberseguridad. Además, también se incorpora un pequeño cuestionario donde se puede verificar si todo ese conocimiento que hemos adquirido resulta ser aprendido correctamente o no.

- Finalmente se hará un estudio de la viabilidad comercial, operativa y económica del modelo de negocio basado en esta idea. En la viabilidad comercial se expondrá el análisis de la competencia, del cliente/mercado y la propuesta del valor. En la viabilidad operativa analizaremos la posibilidad del despliegue del producto. En la viabilidad económica haremos un análisis del plazo de recuperación, el VAN y la TIR. Todo ello sobre la base de un análisis DAFO y un modelo Canvas.

2.3 Herramientas utilizadas para la implementación de la web

Para la implementación de la web se ha optado por desarrollarla con los lenguajes de programación html, css y javascript. Podemos observar sus logos en la Ilustración 4:

Ilustración 4. Logos de lenguajes de programación utilizados

Fuente: Teorema-rd (2023)

Primeramente hemos maquetado la web, es decir montando su esqueleto, con el lenguaje de programación HTML. Hemos estructurado la web con cuatro pestañas que corresponden con lo siguiente:

- Una primera página de inicio que es la presentación de la web.
- Luego un apartado de formación en donde se han implementado los distintos retos y una prueba de conocimientos tipo test.
- Una sección de un foro, en donde el usuario puede plantear preguntas y recibir respuestas de sus dudas, proponer nuevos retos, corregir los retos existentes, etc. (ver pantallazo en el Anexo II).
- Finalmente, la última página correspondería al formulario de contacto por si el usuario quisiera hacer un comentario o solicitar información general de la web.

A continuación le hemos dado estilo al sitio web empleando CSS. Existe un fichero en el proyecto denominado style.css en donde se han implementado todas las clases que incorporan los ficheros HTML.

Finalmente, hemos empleado JAVASCRIPT para así darle músculos al sitio web. Se ha utilizado este lenguaje para implementar la lógica de cada reto y para que podamos interactuar enviando la solución ya sea mediante un botón, cajetilla, etc., para de esta manera saber si hemos superado el reto con éxito o no.

Todo esto se ha programado con el editor de código fuente Sublime Text, dado a que éste ha sido el editor que el autor utilizó en sus prácticas de Programación IV y tenía soltura en el manejo de este editor. Vemos su logo en la Ilustración 5.

Ilustración 5. Logo de Sublime Text

Fuente: Softonic (2023)

Falta destacar con respecto a la implementación de la web, que esta se pudo haber realizado un poco mejor añadiendo nuevas tecnologías webs, bases de datos, un servidor, etc. Pero, al no disponer de tanto tiempo y recursos para su desarrollo, se ha optado por hacer un producto mínimo viable a efectos de meramente demonstrar los distintos ataques que podamos recibir mediante los retos, como se recoge en la propuesta de TFG.

2.4 - Herramientas utilizadas para el desarrollo del plan de negocio

Para el plan de negocio, nos centraremos en el uso de la metodología Lean-StartUp (Ries, 2011). Esta forma de crear negocios, se basa en crear modelo de forma

ágil con el uso de pocas herramientas y sencillas que permitan visualizar como funciona el producto/servicio ofertado.

Se ha empezado por el Business Model Canvas (Osterwalder y Pigneur, 2013), como parte fundamental de la metodología Lean-StartUp, para ver, de forma resumida y esquemática, el negocio. El lienzo nos da la posibilidad de exponer, gráficamente, cuál es nuestro modelo de negocio, estructurado en nueve partes. Estas nueve secciones comprenden las siguientes cuatro áreas principales: clientes, oferta, infraestructura y evaluación de beneficios. Entre sus características principales encontramos las siguientes:

- Ofrece una representación simple del *business*.
- Fomenta un enfoque integral y sistémico.
- Impulsa la toma de decisiones estratégicas y la innovación.

Las secciones dentro del Business Model Canvas son las siguientes y se debe rellenar en este orden para que haya coherencia en lo que estamos intentando modelar a través de este lienzo:

1) Propuesta de valor: ¿Qué necesitaría tu segmento de clientes? ¿De qué forma resolverás sus dolencias?

2) Segmentos de clientes: ¿Cuáles son nuestros clientes más relevantes? ¿A quién le estamos generando valor?

3) Canales: ¿Qué canales desean nuestros clientes? ¿Cómo estamos llegando a ellos?

4) Relación con el cliente: ¿Qué tipo de vínculo mantendrás con tu clientela?

5) Vías de ingresos: ¿Cuál será la manera en la que tu negocio genere ingresos y se financie?

6) Recursos clave: ¿Requieres de algún recurso clave para tu negocio?

7) Actividades clave: ¿Qué tareas son primordiales para que tu modelo funcione?

8) Asociados clave: ¿Quiénes serán los particulares u organizaciones relevantes de tu negocio?

9) Estructura de costes: ¿Cuál son tus gastos? ¿Cuáles son los más relevantes?

Podemos observar a continuación un ejemplo de Business Model Canvas en la Ilustración 6:

Ilustración 6. Ejemplo de Canvas

Fuente: Crehana (2023)

Con respecto a la otra herramienta utilizada para el plan de negocio, hemos empleado el análisis DAFO (Humphrey, 2005). Sus siglas corresponden a Debilidades, Amenazas, Fortalezas y Oportunidades. Se trata de un modelo que describe la realidad, tanto interna como externa, de un producto, marca o empresa para facilitar la toma de decisiones y definición de estrategias.

Las secciones del análisis DAFO son las siguientes:

- Fortalezas: Aquí se describe lo mejor que tiene nuestro negocio respecto a otros. Se trata de diferenciar nuestro producto diciendo qué podemos ofrecer que otros no hagan. Es un análisis formado de características positivas internas.

- Debilidades: Se describen los aspectos en donde el negocio "flaquea", ya bien sea por los recursos empleados estén obsoletos o no, por ejemplo. Otro ejemplo sería no ir por la solución más óptima, sino tratar de realizarla con los métodos tradicionales que se suelen utilizar, es decir, no innovar en dichos procesos inicialmente y plantear estrategias para mitigar esta debilidad en el futuro. Esta parte del DAFO tiene características internas negativas del negocio.

- Oportunidades: Son factores que favorecen el desarrollo del negocio o establecen la posibilidad de impulsar mejoras, de forma externa. Por ejemplo, la situación económica del país o el marco legal.

- Amenazas: Sería todo nuestro entorno externo negativo que actúa sobre nuestro negocio. Se trata de aquellos factores que puedan poner en peligro la viabilidad de nuestro negocio.

Podemos observar a continuación un ejemplo de Análisis DAFO en la Ilustración 7:

Ilustración 7. Ejemplo de Análisis DAFO

Fuente: Infoautonomos (2023)

2.4.1 - Viabilidad comercial, operativa y económica

Desde un punto de vista teórico, la viabilidad comercial se puede definir como el estudio de la posibilidad de implantación en el mercado de un producto o servicio, con un determinado nivel de éxito (Rodríguez-Ariza, 2017). Dicha determinación vendrá dada por la existencia de clientes que demanden nuestro producto o servicio, así como que existan pocos competidores en el mercado, o que se cuente con una propuesta de valor diferenciadora. También comprende el estudio de las ventas, dado que debemos ser capaces de, desde el estudio obtenido del mercado, determinan una previsión la cantidad de productos vendidos o servicios ofrecidos.

En cuanto a la viabilidad operativa, de acuerdo con Rodríguez-Ariza (2017), también denominada técnica o tecnológica, recoge si un proyecto es posible de realizar, desde el punto de vista de las características técnicas del momento de implantación del producto o servicio. Incluye limitaciones físicas, procesos de fabricación, recursos humanos, incluso aspectos legales que puedan impedir la implantación de nuestro producto o servicio. Un ejemplo recaería en el realizar viajes espaciales para particulares, cuestión que podría realizarse en un futuro, pero no en el momento actual.

Finalmente, y no por ello menos importante respecto a su orden, la viabilidad económico-financiera, recoge si el proyecto es rentable en el largo plazo, obteniéndose beneficios, así como una corriente de tesorería donde los cobros, en el largo plazo, superen a los pagos, manteniendo una inversión inicial, tanto propia como ajena, que soporte las pérdidas de implantación del proyecto en el mercado, y su crecimiento. Según la Cámara de Comercio de Oviedo (2020), esto nos permitiría tener una visión de la estrategia a implantar, con el objetivo de obtener financiación e inversores. De los indicadores más utilizados para estimar el plazo de recuperación de la inversión están el VAR (Valor Actual Neto) y la TIR (Tasa Interna de Retorno), que básicamente descuentan los flujos netos de caja futuros al momento inicial, donde ocurre la inversión.

Capítulo 3: Competencias específicas y aportaciones del trabajo

3.1 – Competencias específicas

CII02. Capacidad para planificar, concebir, desplegar y dirigir proyectos, servicios y sistemas informáticos en todos los ámbitos, liderando su puesta en marcha y su mejora continua y valorando su impacto económico y social.

Con este trabajo fin de grado se puede observar que, la implementación de la web se ha realizado de manera planificada desde el principio hasta el final con su despliegue del producto mínimo viable. Ha habido diversos errores cuando se estaba implementado y estos han sido corregidos. También se ha estudiado su impacto económico y social al tratar de desarrollar el plan de negocio correspondiente al proyecto web que estamos realizando. Más adelante en el capítulo 4 del desarrollo se verán todos los avances realizados.

CII07. Conocimiento, diseño y utilización de forma eficiente los tipos y estructuras de datos más adecuados a la resolución de un problema.

En cuanto al uso eficiente de tipos y estructuras de datos, cabe mencionar el uso de almacenamiento local de Javascript y la notación de objetos en Javascript (JSON) en la implementación del prototipo del foro. Dicha mención se debe a que hemos utilizado dichas estructuras dado al coste económico y tecnológico cara un producto mínimo viable (no es necesario el despliegue de un servidor ni un sistema de gestión de base de datos).

CII08. Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.

Los lenguajes de programación utilizados han sido HTML, CSS y Javascript debido a que son los utilizados en la capa del cliente siempre (front-end). Asímismo el

paradigma del programación utilizado ha sido la programación secuencial no orientada a objetos, con las bondades del asincronismo de Javascript.

Dichos lenguajes y paradigmas han sido utilizados debido a la poca complejidad de un producto mínimo viable, intentándolo hacer lo más genérico, y sencillo de desarrollar, sin hacer uso de ningún framework.

CII011. Conocimiento y aplicación de las características, funcionalidades y estructura de los Sistemas Distribuidos, las Redes de Computadores e Internet y diseñar e implementar aplicaciones basadas en ellas.

En cuanto al uso de las redes de internet se hace uso en uno de los retos se usa parte del modelo OSI en el análisis de los paquetes de red. De esta forma hemos evidenciado el uso del protocolo HTTPS frente a HTTP por su seguridad.

CII016. Conocimiento y aplicación de los principios, metodologías y ciclos de vida de la ingeniería de software.

En cuanto a la ingeniería del software hemos tenido especialmente en cuenta el ciclo de vida del software. La aplicación web implementada se encuentra en un fase de prototipo debido a que es una propuesta del programa futuro. En el caso de llevarse acabo el desarrollo completo de la aplicación, se plantearía una metodología y unos principios de ingeniería del software adaptados al producto, mercado y el equipo de desarrollo.

CII017. Capacidad para diseñar y evaluar interfaces persona computador que garanticen la accesibilidad y usabilidad a los sistemas, servicios y aplicaciones informáticas.

En el prototipo realizado hemos implementado una interfaz de usuario web de uso sencillo y común en las aplicaciones webs para que sea fácil la muestra de la funcionalidad del software.

SIO4. Capacidad para comprender y aplicar los principios y prácticas de las organizaciones, de forma que puedan ejercer como enlace entre las comunidades técnica y de gestión de una organización y participar activamente en la formación de los usuarios.

En lo respectivo a la capacidad mencionada hacemos especial alusión a la formación de los usuarios en las organizaciones. En concreto, algo que esta muy

patente hoy en día es el tema de la ciberseguridad en las empresas, por lo que este trabajo de fin de grado pretende dar una herramienta para que las organizaciones instruyan a sus empleados en materias relacionadas con la seguridad de información.

3.2 – Aportaciones al entorno socio-económico y técnico

Este trabajo fin de grado ofrece a la sociedad una herramienta sencilla, que evidencie los riesgos de la ciberseguridad en los sistemas de información. A través de los retos se explica tanto a particulares como empresas la problemática de la brechas de seguridad en ciertos sistemas que comprometen los datos.

Desde el punto vista económico, se pretende también demostrar la pérdida monetaria del uso inadecuado de los sistemas, sin tener en cuenta la parte de seguridad, llevando tanto a particulares como organizaciones a pérdidas monetarias importantes (Cybersecurity News, 2023). Asimismo, hemos desarrollado una herramienta que derivada de su plan de negocio no tendría un gran impacto económico en su desarrollo y generaría mayor impacto económico en sus usuarios comentados previamente.

Respecto al aspecto técnico y social hemos acercado un aspecto como es el de la ciberseguridad a un plano más simple para usuarios no expertos a través del uso de retos que se pueden seguir fácilmente y formando en lo relativo a esta cuestión a través de una prueba de conocimientos. Adicionalmente, hemos también creado un foro al que se pueden unir usuarios y expertos para llevar el aspecto técnico a la sociedad sin conocimiento en la materia.

Capítulo 4: Desarrollo

4.1 – Desarrollo informático

En la realización de este TFG se ha seguido la metodología software incremental, puesto a que se ha ido construyendo el producto final de manera progresiva.

Se ha empezado por montar la estructura básica de la web con sus respectivas pestañas, concretamente las de inicio, formación, foro y contacto. Con respecto a la de inicio, hemos incorporado información básica de presentación del autor.

Luego, en la de formación, es donde está todo el jugo de la página web y en esta se han implementado los retos y un prueba de conocimientos tipo test. Cada reto es independiente y no tiene que ver nada con el anterior o posterior. Específicamente hay seis retos en los cuales se tratan conceptos de ciberseguridad que pone a prueba a los usuarios para ver si son capaces de resolver este tipo de cuestiones. Con respecto a su implementación, podemos observar en los ficheros que se ha seguido una estructura similar en todos ellos haciendo uso de los lenguajes de programación mencionados (HTML,CSS y JAVASCRIPT). Para cada reto, después de superarlo se redirige a una página de felicitación por superar el reto trabajado, esta página es la misma para cada uno de los retos.

También se ha programado una pestaña de contacto fácil de entender, en caso de que se requiera contacto con el creador o solicitar información general entre otras acciones que pueden realizar los usuarios (esto es meramente visual, no se puede enviar el formulario de contacto puesto a que no hay una base de datos detrás de la página web). Finalmente se implementado un foro de discusión para que los usuarios tengan un lugar para interactuar. Este foro almacena el contenido del mismo haciendo uso de localStorage el cual nos permite almacenar los datos de manera local en el navegador que utiliza el usuario para utilizar la web.

A continuación vamos a destacar lo más importante del software desarrollado, que sería el apartado de Formación (ver en Anexo I, el código de los retos):

1) Empezando por el primer reto, este se resuelve de manera muy sencilla y básicamente consiste en averiguar la contraseña que se pide y además se da una pista y es que ha de conocerse bien el lenguaje de programación HTML (Mozilla, 2020). He ahí el dato que determinará la contraseña a buscar. Observamos la Ilustración 8:

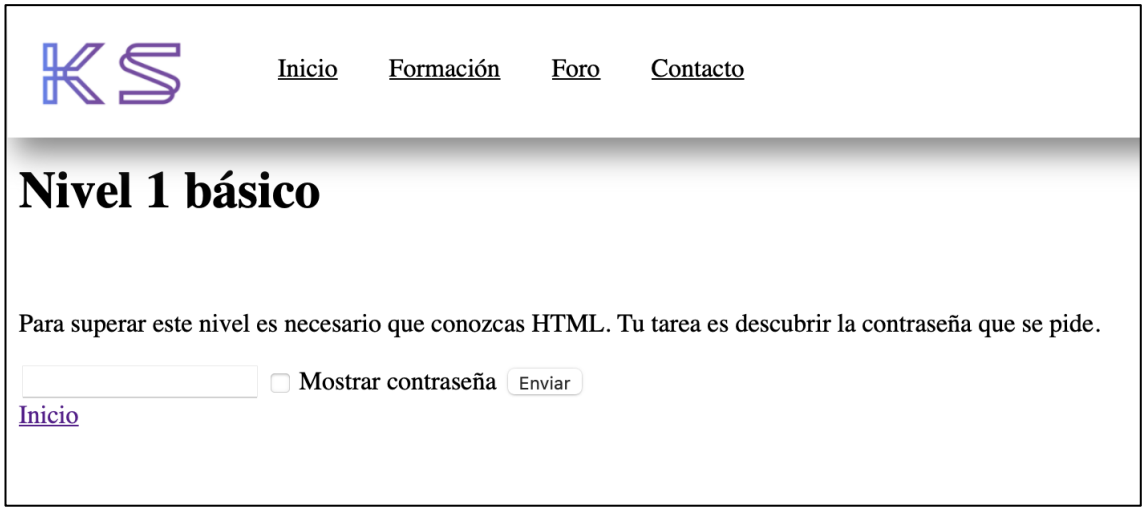

Ilustración 8. Captura del sitio web creado

Fuente: Elaboración propia

Vemos el código HTML de la página y efectivamente hay una contraseña puesta como comentario justo en el body del fichero. Vemos la Ilustración 9:

Ilustración 9. Captura del código HTML implementado

Fuente: Elaboración propia

2) Luego hemos implementado el reto 2, que consiste en codificar y decodificar un mensaje que se da como enunciado. Aquí el usuario tiene que hacer uso de la consola del navegador y no utilizar otros métodos para resolver este ejercicio.

Codificar transforma unos datos en otros, de forma que no sean legibles de la manera original, sin la pérdida de información. Decodificar en el proceso contrario (Esero, 2022).

Observamos la Ilustración 10:

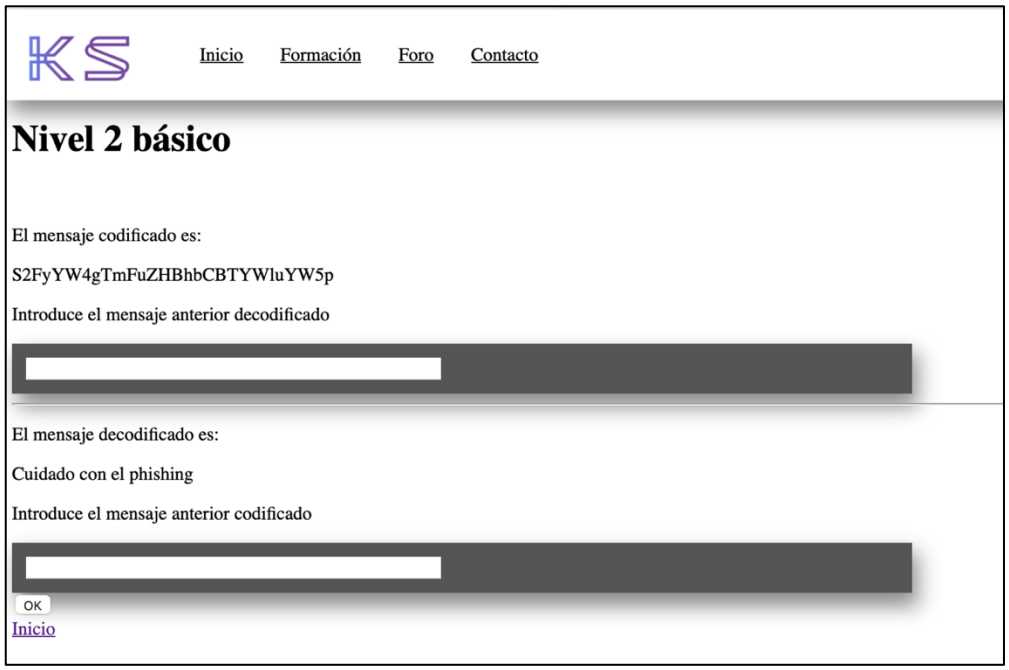

Ilustración 10. Captura del sitio web creado

Fuente: Elaboración propia

Una vez que estemos en la consola del navegador web, hemos de introducir lo siguiente para el primer caso que es decodificar, haciendo uso de la función atob, que decodifica una cadena de datos que ha sido codificada utilizando la codificación en base-64 (Mozilla, 2023) tal y como se ve en la Ilustración 11.

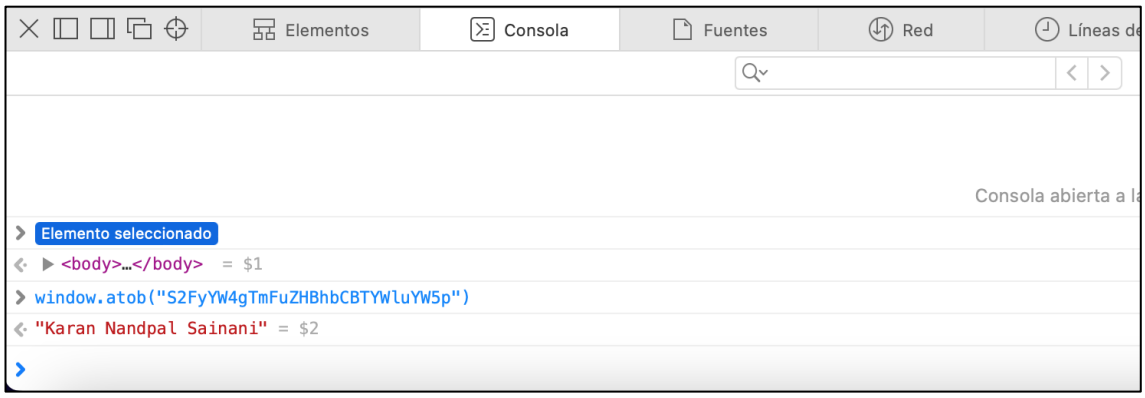

Ilustración 11. Captura de la consola

Fuente: Elaboración propia

Así podemos ver el mensaje codificado, que en este caso su decodificación correspondería a "Karan Nandpal Sainani". Lo ingresamos en la cajetilla y seguimos con el otro apartado.

En el siguiente apartado tenemos que hacer el proceso inverso de lo que hemos hecho anteriormente. En este caso se trata de codificar y usaremos la función btoa (Mozilla, 2022), que vemos en la Ilustración 12:

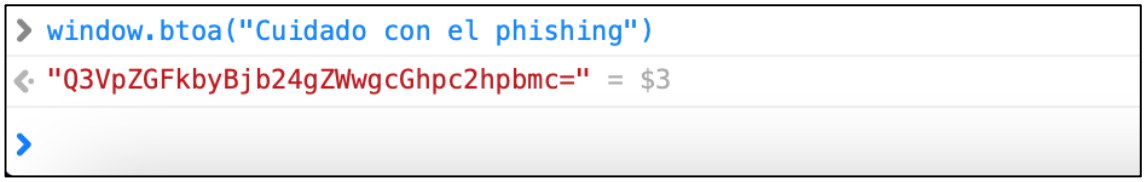

Ilustración 12. Captura de la consola

Fuente: Elaboración propia

La aplicamos y del mismo modo nos sale el mensaje codificado. Estos 2 retos corresponderían a un nivel de principiante, ahora en el siguiente reto a explicar se sube al nivel intermedio.

3) A continuación procederemos a explicar el tercer reto implementado. En este reto es imprescindible conocer el protocolo de red HTTP (Cloudflare, 2023), en cuanto lo que viene siendo su uso y sus diferencias frente al protocolo HTTPS. La tarea es descubrir el usuario y contraseña que se piden, según vemos la Ilustración 13.

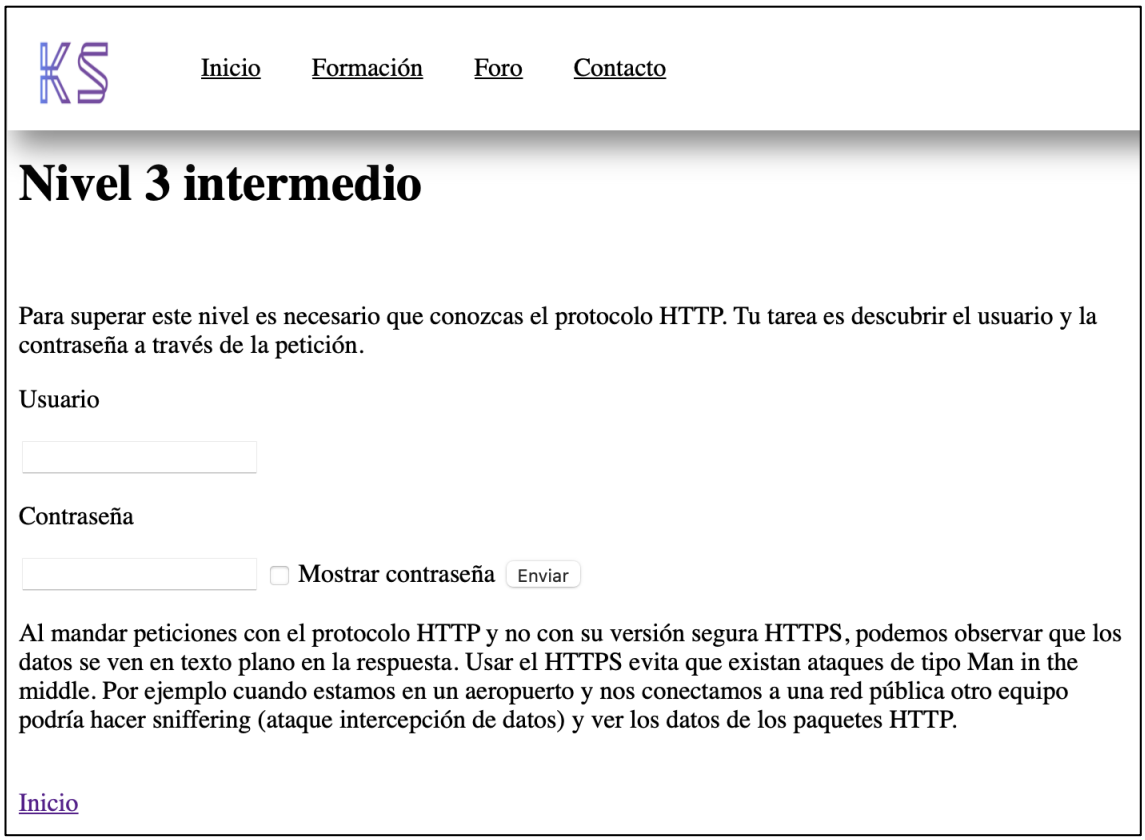

Ilustración 13. Captura del sitio web creado

Fuente: Elaboración propia

Primeramente introduciremos unos datos aleatorios cualesquiera para hacer el login, como intentando adivinar el usuario y contraseña que se nos pide. Luego nos dirigimos al apartado de red de nuestro navegador para ver el paquete que se ha enviado, tal y como se observa en la Ilustración 14:

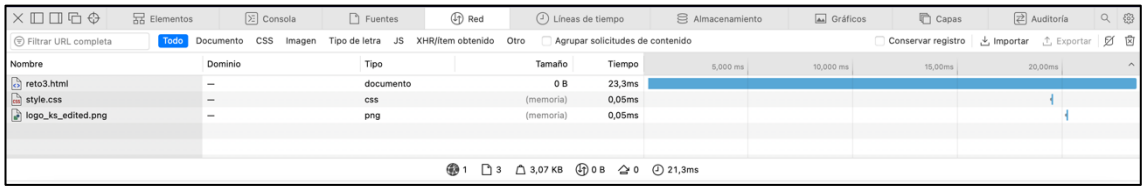

Ilustración 14. Captura del apartado de red

Fuente: Elaboración propia

Aquí podemos ver que se ha enviado correctamente el paquete de red con los datos facilitados, observando la Ilustración 15.

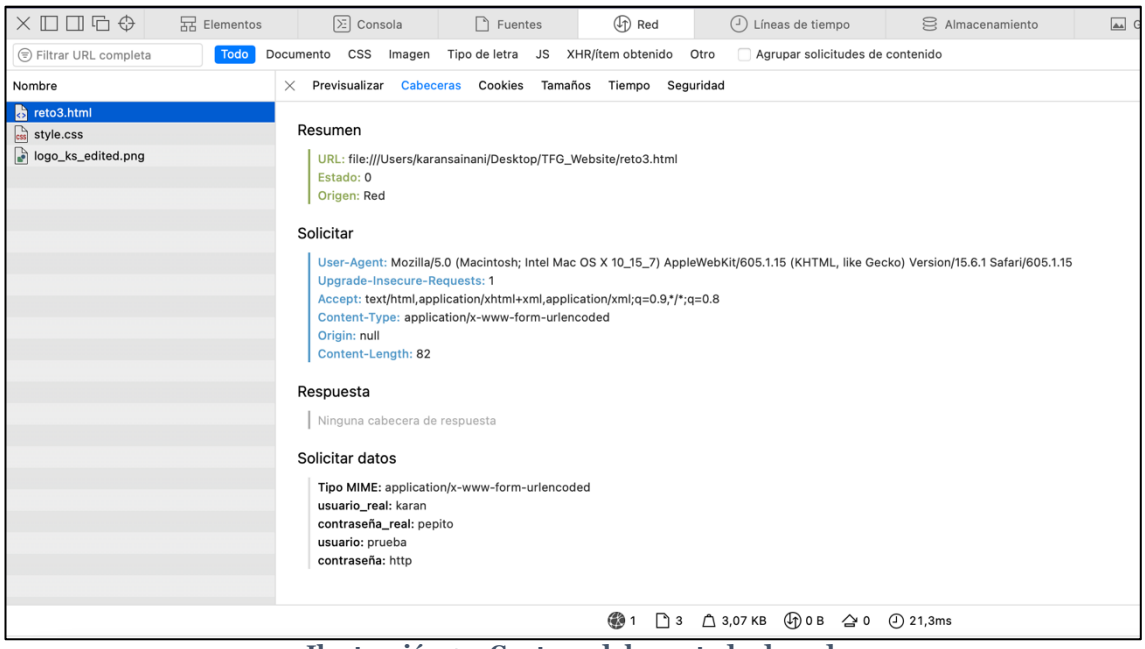

Ilustración 15. Captura del apartado de red

Fuente: Elaboración propia

Ahora si nos dirigimos al apartado de Cabeceras, podemos observar en la sección de "Solicitar datos" el usuario y contraseña que deberíamos de poner en la cajetilla para superar este reto. Tal y como se explica el enunciado de este ejercicio, esta práctica es muy importante dado que podríamos estar expuestos a un ataque de tipo *Man-in-the-Middle* (WeLiveSecurity, 2021). Esto es muy común a la hora de conectarnos a una red pública, ya sea una cafetería, aeropuerto, etc., puesto que otro equipo podría hacer *sniffering* que se trata de un ataque de intercepción de datos (EC-Council, 2023) y ver los datos de los paquetes HTTP.

4) El cuarto reto implementado trata sobre los algoritmos hash. Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija (Torres, 2011). En la siguiente Ilustración 16 podemos observar como se comporta dicha función.

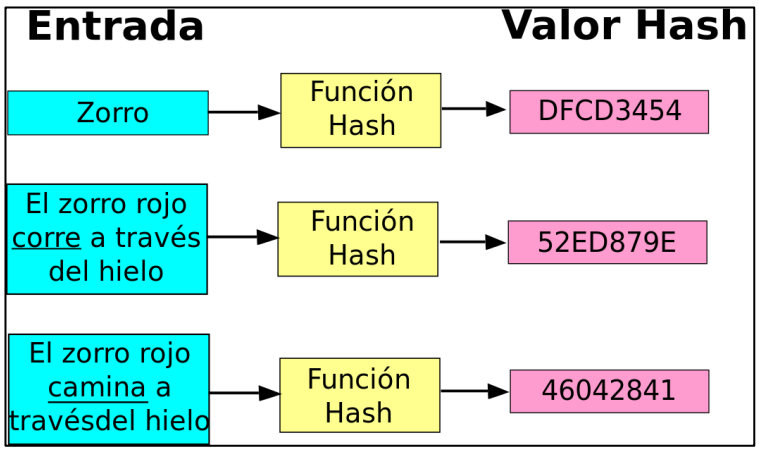

Ilustración 16. Esquema de la función hash

Fuente: Torres (2011)

El enunciado del ejercicio es el siguiente, vemos la Ilustración 17:

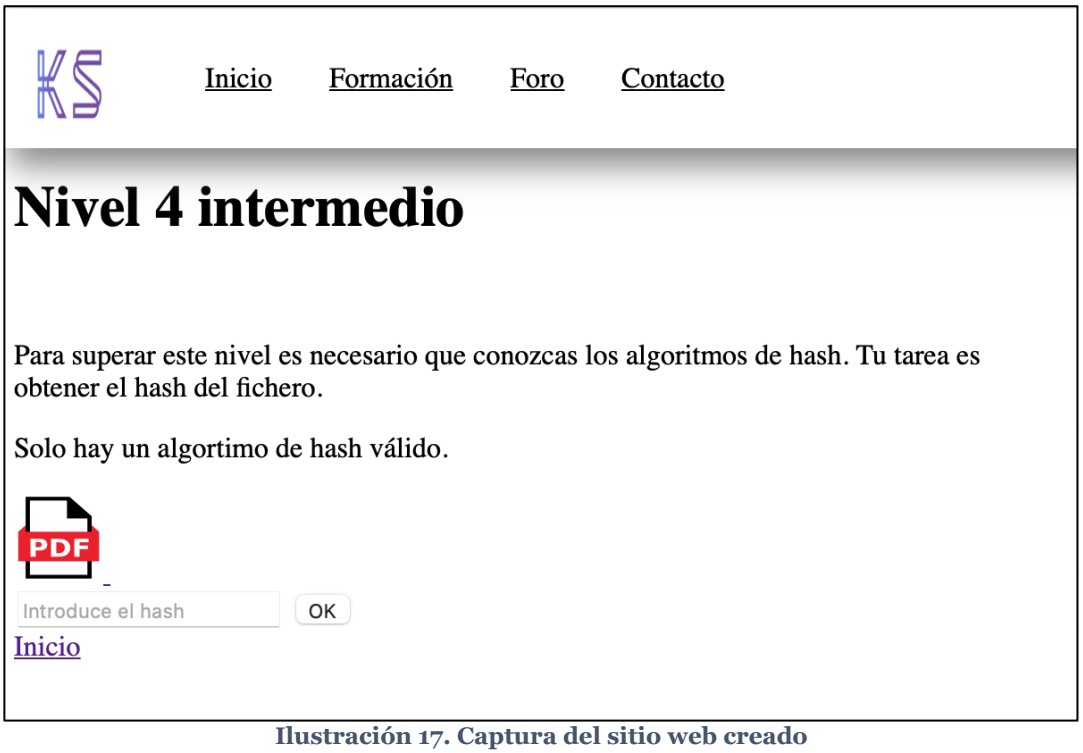

Ilustración 17. Captura del sitio web creado

Fuente: Elaboración propia

El usuario debe ir probando hasta dar con el algoritmo correcto. La solución es aplicar un algoritmo SHA-256 que es el más utilizado frecuentemente a día de hoy (Educative, 2023). Nos dirigimos a la terminal y aplicamos dicho algoritmo, como podemos ver en la Ilustración 18.

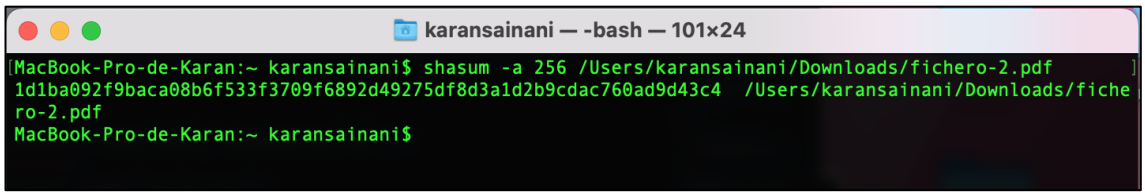

Ilustración 18. Obteniendo el hash de un documento

Fuente: Elaboración propia

Se obtiene el hash del documento facilitado en el enunciado. Entonces lo copiamos y lo ponemos en la cajetilla del enunciado y habremos superado este reto.

5) En cuanto al quinto reto creado, este trata sobre las inyecciones SQL (OWASP, 2023) sin hacer uso de base de datos, es puramente demostrativo. La sentencias SQL que debemos introducir se explican en el enunciado de este reto que mostramos en la Ilustración 19.

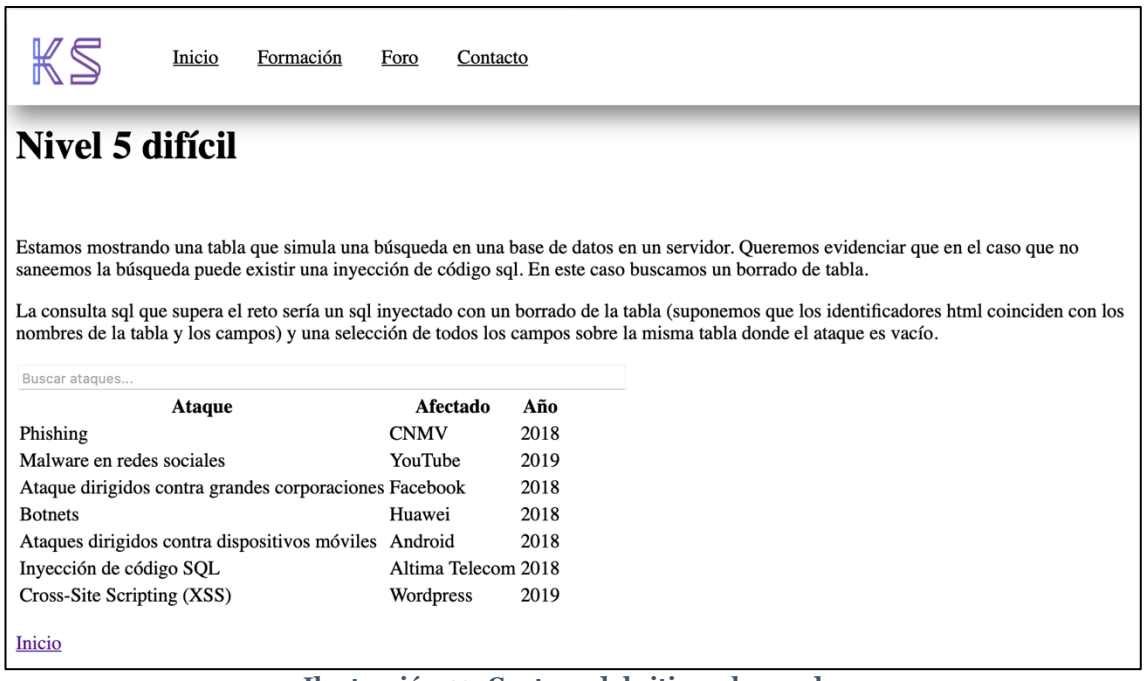

Ilustración 19. Captura del sitio web creado

Fuente: Elaboración propia

¿Qué es una inyección SQL?

La inyección SQL es una forma de introducción de código malicioso, que utiliza una vulnerabilidad informática presente en un programa, en el nivel de validación de las entradas, para realizar acciones sobre una base de datos.

Ahora siguiendo con el reto, hemos de introducir las siguientes sentencias SQL con su inyección correspondiente. Una de ellas podría ser la siguiente:

1) Phishing'; delete from tabla; select * from tabla where ataque = '

Aquí lo que estamos diciendo es que, eliminamos todos los registros de la tabla denominada "tabla" y luego se añade una orden más para corregir un error de sintaxis que lo producirá una comilla simple sobrante. Estamos suponiendo las siguientes premisas:

- A efectos demostrativos, suponemos que la tabla de la base de datos se llama "tabla".

- Suponemos que el campo que contiene el nombre de los ataques puestos en la tabla se denomina "ataque".

- Suponemos que la sentencia de consulta de datos, teniendo en cuenta las premisas anteriores, es la siguiente:

2) select * from tabla where ataque like 'filtro';
Nota: La variable "filtro" incluiría el ataque a buscar en la tabla.

Partiendo de estas premisas y suponiendo que la entrada de datos no esta validada, se podría incluir una sentencia correcta en sintaxis SQL sustituyendo la variable "filtro", como podría ser la siguiente:

3) delete from tabla;

Dicha sentencia borraría totalmente los datos de la tabla en el servidor. Dado a que no podemos inyectar esta sentencia en el servidor directamente, sustituyendo la variable "filtro", debemos hacer uso de otras sentencias auxiliares, para generar una sentencia válida. Dicha sentencia auxiliar se muestra a continuación:

4) select * from tabla where ataque = ' ';

Adicionalmente, dado que se debe generar una sentencia válida, la unión entre la sentencia disponible en el servidor para hacer el filtrado, la sentencia a inyectar y la

sentencia auxiliar no pueden tener errores de sintaxis. Por tanto, la sentencia ejecutada en el servidor es la siguiente:

5) select * from tabla where ataque like '*Phishing'; delete from tabla; select * from tabla where ataque = ' ';

La parte de la sentencia subrayada en amarillo coincide justamente con la primera sentencia SQL que aparece durante la explicación de este reto, que es la que se introduce en tabla del reto en cuestión. De esta forma se superaría el reto inyectando una sentencia de borrado en la base de datos utilizando el filtro disponible con posible entrada de sentencias SQL no validada.

6) El sexto y último reto trata sobre obtener mediante fuerza bruta (Kaspersky, 2023) una contraseña que se nos pide. Para eso el usuario ha de generar un script que automatice todas las posibles combinaciones numéricas. Nosotros, con fines demostrativos, supondremos que la extensión es entre 5-6 números. La contraseña a encontrar cuenta con 6 números.

Su enunciado, como vemos en la Ilustración 20, es el siguiente:

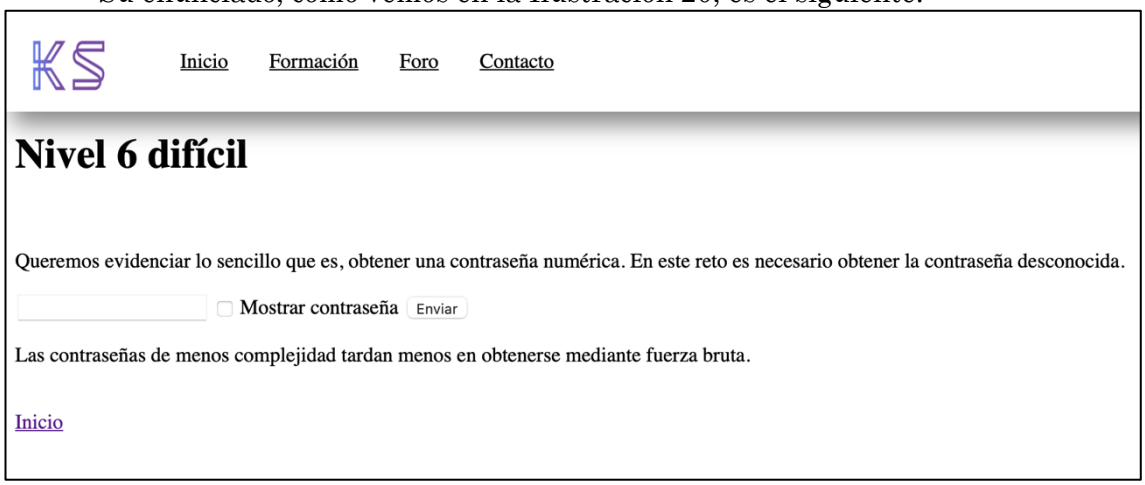

Ilustración 20. Captura del sitio web creado

Fuente: Elaboración propia

¿Qué es un ataque por fuerza bruta?

Probar todas las posibles combinaciones hasta encontrar aquella que permite el acceso.

El script que he generado para que se haga la prueba con todas las posibles combinaciones, sería el que se puede observar en la Ilustración 21:

fuerzaBruta.js

```
function fuerzaBruta () {
    password_inicial=9999;
    password_final=999999;

    for(password_actual=password_inicial; password_actual <= password_final; password_actual++) {
        if (contra == "terminado")
            break;

        console.log(password_actual);
        document.getElementById("password").value = password_actual;
        document.getElementById("ok").click();
    }
}

fuerzaBruta();
```

Ilustración 21. Captura del script desarrollado para el reto 6

Fuente: Elaboración propia

El código itera entre "password_inicial" y "password_final" de forma incremental de 1 en 1, de tal forma que prueba todas las posibles combinaciones entre esos 2 números. Esto lo hemos programado dentro de una función denominada "fuerzaBruta()".

Luego, introducimos el script desarrollado en la consola del navegador. Se nos generarán todas las posibles combinaciones hasta dar con la correcta, que hemos programado en el fichero "reto6.html". Veamos las combinaciones al ejecutar el script en la Ilustración 22.

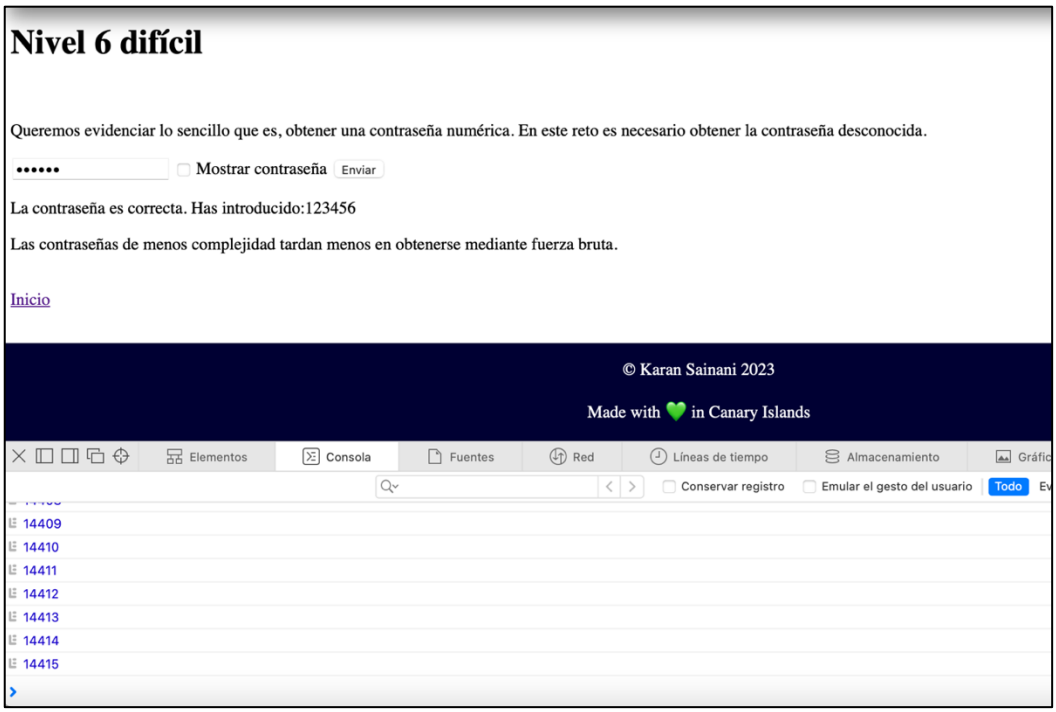

Ilustración 22. Ejecución del script del reto 6

Fuente: Elaboración propia

4.2 – Desarrollo del plan de empresa

En este apartado nos centraremos a realizar en análisis de plan de empresa de nuestro negocio en particular, haciendo uso de las herramientas ya mencionadas previamente. En primer lugar, presentaremos el Canvas, como resumen de nuestra idea de negocio, posteriormente el DAFO, para en análisis interno y externo de la empresa, y el estudio de las tres viabilidades, la comercial, la operativa y la económica.

4.2.1 – Desarrollo del *Business Model Canvas*

Se incluye en el Anexo de la memoria, el lienzo del modelo de negocio desarrollado para esta aplicación web.

I. Propuesta de Valor

En cuanto a nuestra propuesta de valor, hemos analizado nuestros competidores para ver en que nos diferenciamos. Dichas cuestiones son las siguientes:

1) Propuesta de Valor de los RETOS

1.1) Retos sencillos que conciencien la ciberseguridad: No hemos encontrado un servicio similar, en español, que ofrezca, retos de ciberseguridad para concienciar a la población. Asimismo, no hemos visto que los retos disponibles en lengua inglesa, sean retos sencillos y clasificados por dificultad. Esto es valorado por los potenciales clientes en la encuesta.

1.2) Variedad de ejemplos dentro de la ciberseguridad: Nosotros ofrecemos ejemplos sencillos (contextualización del reto) relacionados con las diferentes problemáticas de la ciberseguridad, vinculados con los retos.

2) Propuesta de Valor del FORO-EXPERTO

2.1) Contacto directo con el experto en ciberseguridad: Nuestra aplicación ofrece el contacto directo con un experto en ciberseguridad a través de un foro, que resuelve cualquier duda a los usuarios en materias de seguridad informática, con un horario

establecido. Esto se trata de una propuesta de valor innovadora, dado que, ningún competidor analizado cuenta con dicho experto.

2.2) Feedback de los usuarios a través del foro: En el foro, otros usuarios pueden ver las respuestas a otras preguntas, siempre y cuando sean públicas, cuestión que les puede ayudar antes de la consulta del experto.

II. Segmento de Clientes

- ***Particulares que quieren iniciarse en el mundo de la ciberseguridad:*** Estos clientes serían uno de los primeros targets del servicio ofrecido, pues se desea que las personas físicas puedan aprender sobre ciberseguridad, sus riesgos, a nivel usuario, así como también tener la posibilidad de consultas de sus problemáticas de seguridad informática en su día a día.

- ***Informáticos que no sean expertos en ciberseguridad:*** Este segmento sería similar al anterior, pero con mayores conocimientos en el ámbito técnico. Podrían ser capaces de resolver retos de mayor complejidad e introducirse en el mundo de la seguridad informática, pudiendo expandir sus conocimientos.

- ***Empresas que quieran dar nociones a sus empleados:*** En este contexto entraría la seguridad de las organizaciones, siendo los empelados los que recibirían formación para aplicarlo en el día a día de la informática de la empresa, de forma similar a los particulares.

III. Canales

- ***Anuncios de publicidad:*** Para captar a los clientes potenciales se usarán anuncios publicitarios, mayormente con Google Adwords y otros medios como redes sociales, que están muy vigentes en la actualidad.

- ***Página web:*** La web, además de ser la plataforma de retos y el foro, principalmente, contará con un espacio de captación de usuarios, no disponible en el producto mínimo viable, en donde se podrá contratar el servicio de los retos y el foro con el experto, de una forma atractiva y sencilla para el cliente.

- ***Empresas e instituciones académicas:*** Nos serviremos las universidades y empresas interesadas, pero no asociadas, que deseen difundir nuestros servicios con el bien que se realiza a la comunidad, desde el punto de vista de dar conocimiento sobre seguridad informática y también el contacto con un experto en horario lectivo.

IV. Relación con los clientes

- ***Formulario de la web:*** Existirá un pequeño formulario de contacto donde el cliente potencial o el ya cliente podrá contactar con el administrador de la web, de tal forma que pueda solucionar sus dudas técnicas u económicas sobre el producto, por ejemplo.

- ***Redes sociales:*** Se notificará a los seguidores la creación de nuevos retos y consultas destacadas realizadas en el foro, así como campañas publicitarias para captar nuevos clientes.

- ***E-mail y teléfono:*** Como alternativa complementaria al formulario, se dispondrá de estos medios también para que sea el usuario o potencial usuario el que decida el medio por el que comunicarse con la empresa.

V. Vías de Ingreso

- ***Subvenciones a la creación de empresas innovadoras:*** Organismos públicos locales pueden ofrecer subvenciones para empresas jóvenes, que nos permitan obtener primeras vías de ingreso para los primeros años de existencia de la empresa, como puede ser las SPEGC.

- ***Servicios para las empresas:*** A las empresas, por el servicio del experto y formación a través de retos a los empleados, se les cobra una cuota por mes y empleado por el uso de los servicios.

- ***Crowdfunding:*** Expondremos en webs que ofrezcan esta forma de financiación con el fin de hacer preventa de suscripciones a nuestro servicio, con el fin de financiar la puesta en marcha de la aplicación web.

VI. Recursos clave

- ***Foro:*** Esta herramienta es clave como interacción con el experto en ciberseguridad, siendo la propuesta diferenciadora principal de la plataforma frente a los competidores. Dicho recurso debe funcionar de forma ágil con los usuarios, que deberán recibir respuestas acordes a sus preguntas, de forma rápida y veraz.

- ***Retos:*** Los retos que sean ofrecidos a los usuarios deben ser de utilidad para ellos, y de aprendizaje, con el fin que dichos usuarios aprendan más en la temática de ciberseguridad y cómo protegerse ante posibles ataques informáticos.

- ***Experto en ciberseguridad:*** Es otro de los recursos clave, dado que sin él no existiría el foro. Es importante distinguir entre este y el foro, dado que debe tener una plataforma con la que trabajar, pero en sí mismo debe estar en continua formación y actualización sobre temas de ciberseguridad, y estar disponible para las consultas de los usuarios, y ser muy buen comunicador, así como un excelente técnico en su área.

VII. Actividades clave

- ***Actualización sobre la ciberseguridad:*** Mantener la plataforma a la vanguardia de la seguridad informática, de tal forma que contenga el estado del arte de la aplicación de las problemáticas de la ciberseguridad más actuales.

- ***Propuesta de nuevos retos:*** La organización estará en continuo proceso de generación de nuevas ideas y retos que implantar en la plataforma, que sea útiles para los clientes y relejen las problemáticas de ciberseguridad más frecuentes.

- ***Evaluación de conceptos trabajados en los retos:*** Paralelamente, se trabajará en evaluar y dar conocimiento sobre el trasfondo de los retos, con el fin de determinar si los usuarios han adquirido los conocimientos que se pretenden obtener de ellos.

VIII. Asociados clave

- ***Alianzas con empresas dedicadas al mundo de la ciberseguridad:*** Nos podremos asociar con empresas que no sean competidoras directas de nuestro servicio, pero sí que puedan ser sponsors u ofrecer, de forma complementaria a sus productos y servicios, también el nuestro, ofreciéndose una relación B2B en la que ganan ambas partes y sentidos.

- ***Relaciones con instituciones académicas:*** Principalmente, las universidades pueden ofrecer a sus alumnos y partes interesadas dentro de la vida académica nuestros servicios, con el fin de formar a la comunidad universitaria, además de empresas que puedan estar relacionadas con el ámbito universitario, como puede ser en la rama investigadora.

- ***Relaciones con otras empresas en el sector:*** Nos referimos a las empresas no tan vinculadas a la ciberseguridad, pero sí al ámbito informático, que pueden ofrecer nuestros servicios de forma complementaria.

- ***Alianzas con entidades relacionadas con la informática:*** Estas entidades serían organizaciones relacionadas con la informática, como puede ser colegios profesionales de ingenieros en informática, por ejemplo, donde podrían dar publicidad de nuestros servicios y nosotros darles publicidad y una mayor difusión, o incluso ofrecer charlas de ciberseguridad, en función de los acuerdos a los que se llegue.

IX. Estructura de costes

- ***Publicidad:*** Nuestra inversión se centra en la obtención de clientes, a través de los canales de difusión, siendo nuestro principal gasto las campañas en redes sociales y, en el futuro, algún gasto por ser sponsor en algún evento o con empresa afín/asociada.

- ***Pago al experto en ciberseguridad:*** El experto en principio será el dueño de la empresa, pero entendemos que su retribución debe ser un gasto para la empresa, aunque con cargo a beneficios.

- ***Pago del hosting:*** Es necesario alojar la aplicación web en algún hosting, que deberá ser pagado de forma mensual u anual, en función del tráfico.

Inicialmente se irán a modelos de hosting más clásicos y, posteriormente, si se logra un volumen elevado de usuarios, se puede migrar a servicios como Amazon WS y MicroSoft Azure.

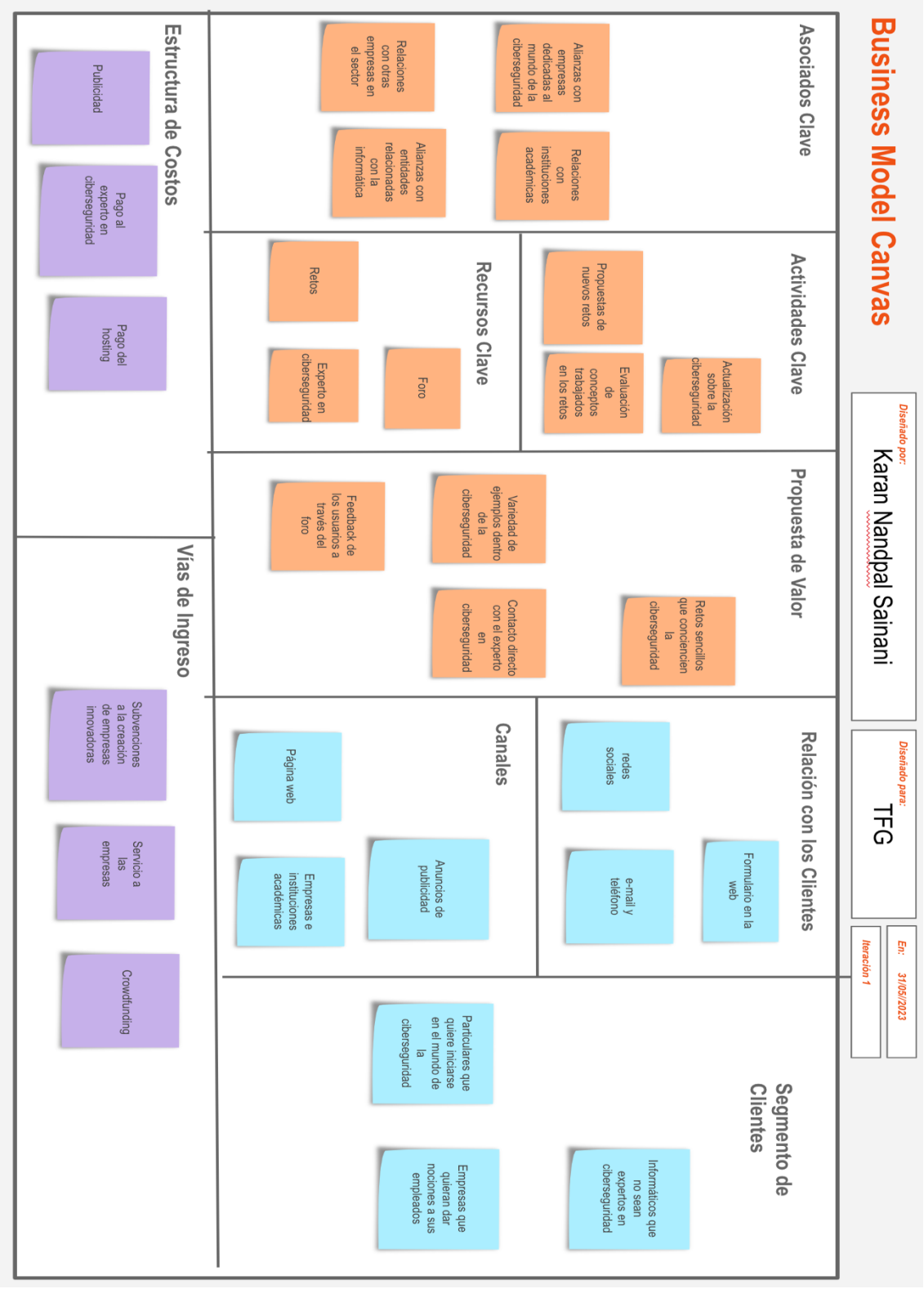

Ilustración 23. Business Model Canvas desarrollado

Fuente: Elaboración propia

4.2.2 – Desarrollo del Análisis DAFO

Tabla 1. Análisis DAFO

Debilidades	**A**menazas
• No disponemos de experiencia en el mercado (empresa joven). • No contamos con usuarios en la actualidad. • No poseemos de alianzas comerciales. • No tenemos financiación para el terminar el desarrollo del producto.	• Muchos ingenieros se están formando en ciberseguridad dado a su alta demanda. • Actualmente contamos con un entorno con incertidumbre económica con posibilidad de crisis (la gente no dispone de renta para gastar en servicios que no son estrictamente necesarios). • Existen otros recursos para formar en ciberseguridad.

Fortalezas	**O**portunidades
• Contamos con un experto en ciberseguridad. • Contamos de una red colaborativa de desarrollo propio. • Disponemos de retos sencillos de entender. • Formulamos un cuestionario de conocimientos bastante completo.	• La sociedad no cuenta con conocimientos en seguridad informática. • No existen competidores que cuenten con foros colaborativos. • Cada día existen mas ataques informáticos a empresas y particulares.

Fuente: Elaboración propia

Conclusión del DAFO desarrollado:

De las cuestiones comentadas en el DAFO, podemos extraer que se trata de un sector en auge (aquel relacionado con la seguridad informática), cuestión que nos favorece tanto desde el punto de vista positivo (hay mayor cantidad de ataques y más interés por parte de los usuarios, así como desconocimiento por parte de estos), como desde el punto de vista negativo (hay más competidores y expertos en la temática).

En cuanto a las debilidades, que muchas de ellas se irán mitigando a medida que comience la implantación del negocio, se realizará contacto posterior para crear alianzas estratégicas con socios clave, como son las universidades, donde incluimos las ULPGC, así como entes públicos que ayudan a empresas, como puede ser la SPEGC, que están muy probablemente preocupados por la seguridad de sus usuarios (PYMEs).

Asimismo, con la realización de la encuesta, hemos encontrado potenciales usuarios de la aplicación, que de ser implantada realmente, podrían hacer uso de ella, y estarían dispuestos a pagar por ella (según los datos reportados en la encuesta realizada).

4.2.3 – Estudio de la Viabilidad Comercial

1. Análisis de la competencia

Para ver si contamos con competidores del producto que se presenta en este TFG, hemos realizado un análisis de la competencia, con el fin de estudiar similitudes y diferencias entre otras empresas y organismos del sector. Dicho análisis se ha realizado teniendo en cuenta dos tipologías de competidores: directos, siendo aquellos cuyas actividades son muy similares a las nuestras, e indirectos, cuyas actividades están relacionadas con las nuestras pero con una propuesta de valor totalmente diferente.

1.1 Identificación de competidores directos

1) Hackthissite (https://www.hackthissite.org)

Actividades claves:

- Desafíos de piratería ética relacionados con: Aplicaciones, programación, JAVASCRIPT, forense, esteganografía.
- CTF (Capture The Flag), juegos para aprender seguridad informática.
- Comunidad viva y dedicada a aprender y compartir conocimientos.
- Muchos proyectos activos en desarrollo.
- IRC (Internet Relay Chat, es un Sistema de chat mundial que requiere una conexión a Internet y un cliente IRC, que envía y recibe mensajes a través del servidor IRC).
- Discord, foros no expertos.

Idioma:
- Inglés

Precio:
- 0€, todos sus servicios son gratuitos.

Tráfico de la web:
- Visitas mensuales: 157.900.

2) Hellboundhackers (https://hbh.sh/home)

Actividades claves:
- Desafíos de piratería relacionados con: Aplicaciones, JAVASCRIPT, ingeniería inversa, enrutamiento, penetration-testing, desencriptar, esteganografía, tracking, ingeniería social, php patching.
- Blog, foro no expertos.
- Banco de código.
- Artículos.
- Sección de noticias tecnológicas.

Idioma:
- Inglés

Precio:
- 0€, todos sus servicios son gratuitos.

Tráfico de la web:
- No disponible

3) Hackertest (http://www.hackertest.net)

Actividades clave:
- Desafíos de seguridad informática relacionados con: JAVASCRIPT, PHP, HTML, pensamiento gráfico.

- Ofrece 20 desafíos que se van desbloqueando a medida que vamos pasando de desafío.

Idioma:
- Inglés

Precio:
- 0€, todos sus servicios son gratuitos.

Tráfico de la web:
- Visitas mensuales: 6.600.

4) Tryhackme (https://tryhackme.com)

Actividades clave:
- Lecciones y desafíos de ciberseguridad relacionados con: Red teaming, offensive pentesting, fundamentos de la web, ciberdefensa, atacando y defendiendo AWS.
- Comunidad grande de estudiantes de ciberseguridad.
- Apartado de competición de hacking (los usuarios pueden competir entre ellos uniéndose a salas para tal efecto).
- Blog.
- Apartado tanto para la educación como para las empresas.
- Sección de noticias.

Idioma:
- Inglés

Precio:
- 0€, todos sus servicios son gratuitos.

Tráfico de la web:
- Visitas mensuales: 3.100.000.

5) Hackthebox (https://www.hackthebox.com)

Actividades clave:

- Laboratorio virtuales de hacking.

- Guerra de hacking multijugadores.
- Capture The Flag.
- Cursos de ciberseguridad.
- Portal de información para trabajos relacionados con la ciberseguridad.
- Blog, foro no experto.
- Comunidad grande de usuarios (tanto empresas como particulares).
- Glosario.

Idioma:
- Inglés

Precio:
- 0€, para lo básico de la web que ayuda a incrementar tu nivel de hacking.
- 12€/mes, para todas las características y servicios de la web.
- 115€/anual, con un 20% de descuento para lo mismo que lo anterior.

Tráfico de la web:
- Visitas mensuales: 47.436.

1.2 Identificación de competidores indirectos.

1) Incibe (https://www.incibe.es)

Actividades clave:
- Trabaja para afianzar la confianza digital, elevar la ciberseguridad y contribuir al mercado digital para el uso seguro del ciberespacio en España.
- Servicios de respuestas y atención a incidentes.
- Herramientas y recursos: simuladores de ataques, guías de seguridad y listas de verificación.
- Formación y captación.
- Programas de apoyo a empresas.

Idioma:
- Español

Precio:
- Hay recursos gratuitos y para otros servicios hay que solicitar presupuesto.

Tráfico de la web:

- Visitas mensuales: 460.700.

2) Ciberseguridad (https://ciberseguridad.com)

Actividades clave:
- Noticias de ciberseguridad, ciberataques, vulnerabilidades informáticas.
- Consejos y guías.
- Servicios y soluciones.
- Formación.
- Ayuda a la empresas.
- Información de empleo en Ciberseguridad.
- Tendencias en Ciberseguridad.

Idioma:
- Español.

Precio:
- Depende del servicio solicitado.

Tráfico de la web:
- Visitas mensuales: 380.138.

3) Kaspersky (https://www.kaspersky.es)

Actividades clave:
- Productos y soluciones.
- Descargas y pruebas gratuitas.
- Información sobre amenazas y noticias de seguridad.
- Recursos educativos.
- Soporte técnico.
- Compra y renovación de productos.

Idioma:
- Español.

Precio:
- Dependiendo del producto y las soluciones a aplicar.

Tráfico de la web:

- Visitas mensuales:1.167.000.

Tras enumerar los competidores que hemos detectado tanto de forma directa como indirecta, hemos realizado la siguiente comparativa entre competidores con el fin de analizar las diferentes actividades que ofrecen cada uno de ellos.

Ilustración 24. Comparativa de competidores

Fuente: Elaboración propia

De todos los competidores, concluimos lo siguiente, separados en dos bloques:

- En cuanto a los competidores directos, sus actividades clave en cuanto a retos son similares a los nuestros, sin tener en cuenta la dificultad, dado que el servicio ofrecido por nosotros es menos complejo de entender y acceder, e intenta ser más amigable al usuario. Asimismo, dichos competidores son de habla inglesa, por lo que podríamos considerar una estrategia de océano azul el hecho

de implantar estas soluciones en España y países latinoamericanos. Finalmente, ninguno de ellos cuenta con un experto en materia de ciberseguridad, aunque sí con el foro, propuesta que nos da un carácter diferenciador clave, percibido por el cliente, según lo que hemos podido sondear en la encuesta.

- En lo que respecta a los competidores indirectos, sus actividades clave son muy dispares a la que nosotros ofrecemos, siendo mayormente formación. Es también muy útil para los usuarios, visto desde el tráfico que estas webs generan y en español, pero no deja de ser cierto que, si los usuarios de habla castellana dispusiesen de retos como los de habla inglesa, podrían mejorar sus habilidades en materia de seguridad informática. Asimismo, hay servicios que se facturan al usuario, como en los competidores directos, por lo que es un posible nicho de generación de ingresos el uso de retos, con la combinación del experto en esta materia.

1.3 Clasificación de características

Las características más importantes a tener en cuenta en este mercado, después de analizar a la competencia y sin importar el orden, son:

- Variedad de desafíos de hacking/piratería/ciberseguridad y lecciones formativas.

- Precio y poseer una comunidad en la que poder interactuar con el creador y otros usuarios.

- Sección de noticias de ciberseguridad y ofertas de empleo relacionadas con este campo.

2. Análisis de los clientes

Acorde a la metodología seguida, denominada Lean-StarUp, hemos realizado el análisis de los clientes en los siguientes subapartados, respondiendo a diversas preguntas y características.

¿Quién es nuestro cliente? ¿Qué perfiles o figuras aparecen en nuestro proceso de venta?

Nuestro cliente objetivo, va dirigido a un gran espectro de población. El perfil más habitual es gente joven o adulta con ganas de aprender conocimientos relacionados con el mundo de la ciberseguridad, sus ventajas, aplicabilidad e importancia en la actualidad, entre otras cuestiones.

Según el INE(2022), y teniendo solo en cuenta el número de usuarios de nuestro país, en el año 2022 en España, el 94,5% de la población, de 16 a 74 años, ha utilizado Internet en los últimos tres meses, 0,6 puntos más que en 2021. Esto supone un total de 33,5 millones de usuarios, siendo este nuestro mercado potencial.

Analizar a qué tipo de mercado se enfoca nuestro producto.

Nuestro mercado geográfico es de habla hispana, como puede ser España o países de Latinoamérica. En cuanto al mercado demográfico, el producto se dirige a particulares y empresas. También hacia el mercado psicográfico a gente no experta en ciberseguridad.

Analizar qué consecuencias puede tener lo anterior sobre las decisiones empresariales iniciales y sobre las expectativas que podemos tener.

Las consecuencias que podemos tener es que algunos de los mercados no tengan interés, por ejemplo los particulares. Esto se resolverá a partir del análisis de las expectativas confirmadas a través de la encuesta.

Mapa de Empatía:

En base a lo desarrollado hasta ahora, vamos a concluir con un mapa de empatía para conocer aún más a nuestro cliente:

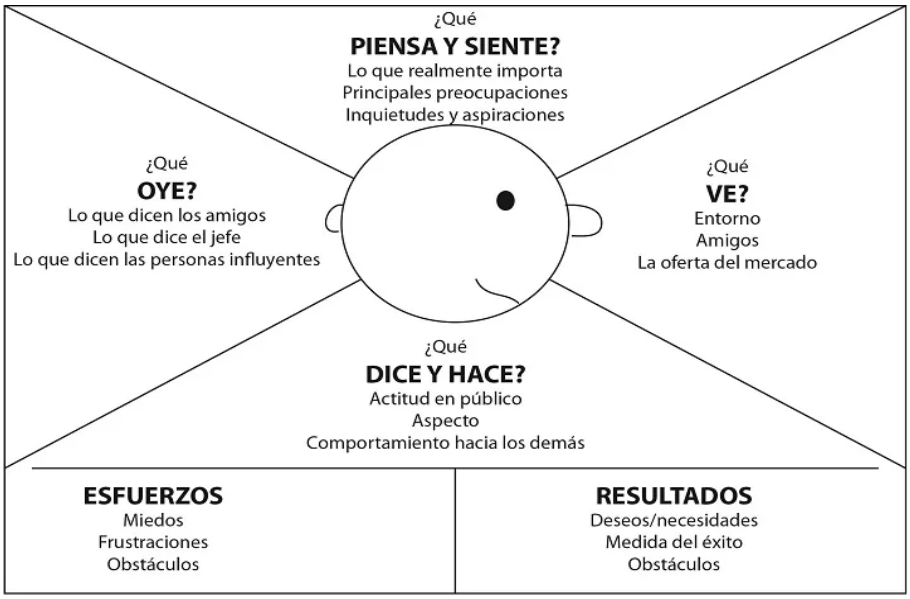

Ilustración 25. Mapa de Empatía

Fuente: López (2016)

Para desarrollar esto, vamos a establecer que el cliente es Jorge un hombre de 25 años que vive solo y esta estudiando y trabajando para pagarse los estudios universitarios.

1) ¿Qué piensa y siente?

- Jorge es una persona que le gusta hacer todas sus operaciones en la red con precaución.

- Leer sobre seguridad informática es una de sus preocupaciones puesto a que tiene la gran mayoría de cosas que usa diariamente por medio de servicios tecnológicos.

- Le preocupa sufrir un ataque y verse comprometido.

2) ¿Qué ve?

- Jorge se fija en sus compañeros de clase como interactúan con sus trabajos entregados, como los salvaguardan, tener el sistema operativo actualizado, etc.

- La oferta del mercado para estudiantes es amplia, en todo tipo de servicios, excepto en ofertas de empleos ya que, se requiere un cierto mínimo de conocimientos en ciberseguridad.

3) ¿Qué oye?

- Jorge oye quejarse a las personas de que han sufrido alguna vez un ataque informático, el más usual, el phishing en mensajes de texto, de que han recibido un paquete y necesitan que confirmen sus datos (cuando en realidad no habían solicitado ningún paquete).

- Escucha a otros que no se preocupan por su seguridad en la red y no le gusta.

4) ¿Qué dice y hace?

- Mantiene sus redes sociales privadas.

- Hace una copia de seguridad cada año de todos sus documentos.

- Quiere aprender más sobre la ciberseguridad.

5) ¿Qué esfuerzos, miedos, frustraciones y obstáculos encuentra?

- No le resulta fácil aprender sobre ciberseguridad puesto a la falta de base en programación.

- Le frustra sufrir un ataque y no enterarse.

- No tiene suficiente dinero para pagarse un sitio web en donde practicar.

6) ¿Qué le motiva (deseos, necesidades, medida del éxito, obstáculos superados)?

- Le motiva seguir estudiando/formándose en este campo debido a su alta preocupación en el mercado laboral a día de hoy.

- Toma como reto personal dedicarse a este campo debido a que le cuestan desde pequeño las matemáticas y en este campo se utilizan bastante.

- Le gusta superar sus límites y se marca retos con frecuencia.

Para profundizar un poco más en el conocimiento de nuestro potencial cliente, hemos realizado una encuesta, con una muestra de 82 personas. A partir de sus resultados, podemos confirmar que el segmento de clientes que hemos elegido es el que tiene la necesidad de nuestro producto y que no ha sido capaz de resolver con otro competidor. A continuación se muestran los resultados obtenidos:

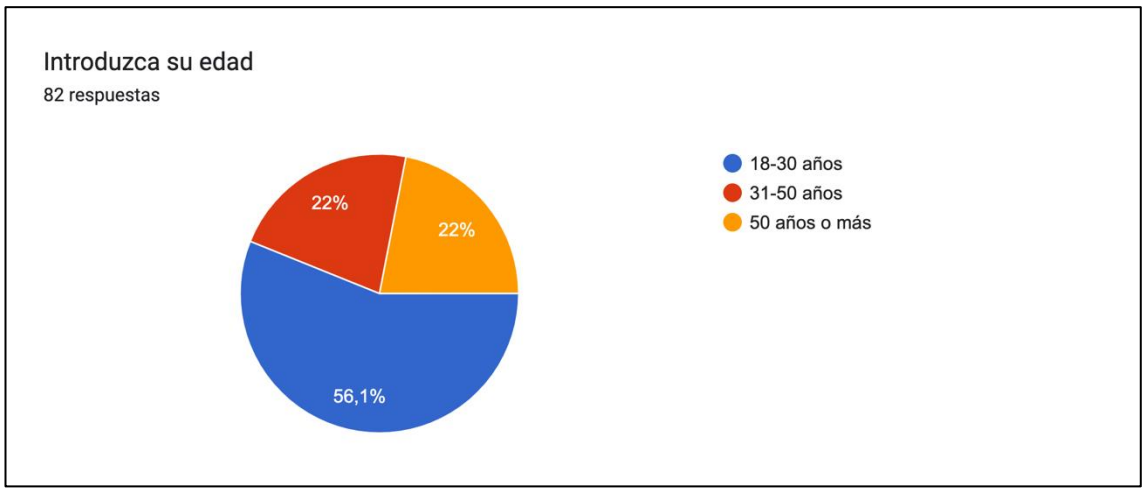

Gráfico 1. Respuestas a la pregunta 1 de la encuesta

Fuente: Elaboración propia.

En los datos recabados, hemos obtenido una muestra balanceada entre jóvenes (menores de 30 años) y adultos de mediana edad.

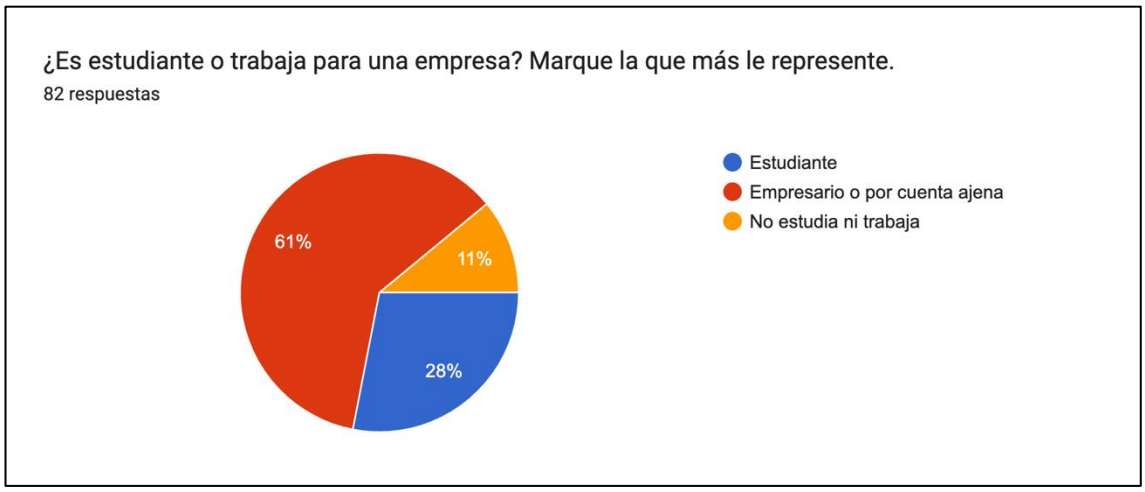

Gráfico 2. Respuestas a la pregunta 2 de la encuesta

Fuente: Elaboración propia.

Asimismo, la mayor parte de la participación ha sido de gente que trabaja por cuenta ajena o es empresario. Presuponemos que dicho colectivo, estará mas concienciado con el tema de la ciberseguridad y desearía aprender sobre ello y estaría dispuesto a pagar por ello.

Gráfico 3. Respuestas a la pregunta 3 de la encuesta

Fuente: Elaboración propia.

Podemos observar, que la mayor parte de los encuestados no renuevan su contraseña habitualmente, teniendo en cuenta posteriormente que los encuestados están preocupados por la ciberseguridad.

¿Cada cuánto suele actualizar el sistema operativo de su ordenador/móvil/tablet?

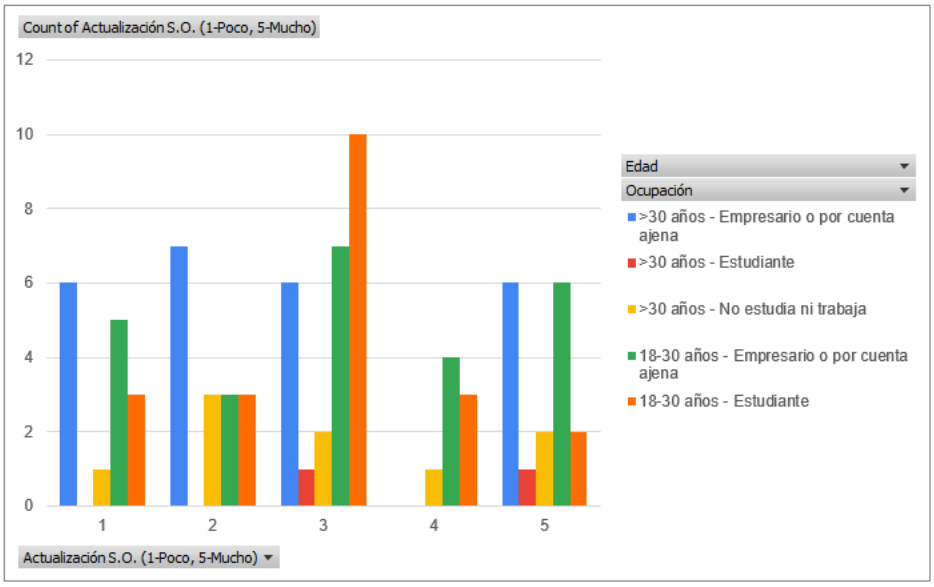

Gráfico 4. Respuestas a la pregunta 4 de la encuesta

Fuente: Elaboración propia.

Hemos segmentado el gráfico anterior en los diferentes perfiles con los que contamos en la encuesta, para ver si existen diferencias significativas en la actualización del sistema operativo por grupo de edad u ocupación. Podríamos decir que son bastante homogéneos, habiendo disparidades entre los usuarios, únicamente destacando el grupo de estudiantes jóvenes que considera que no lo actualiza ni poco ni mucho, por lo que presuponemos que lo hacen en la medida que estiman necesario o el sistema les avisa.

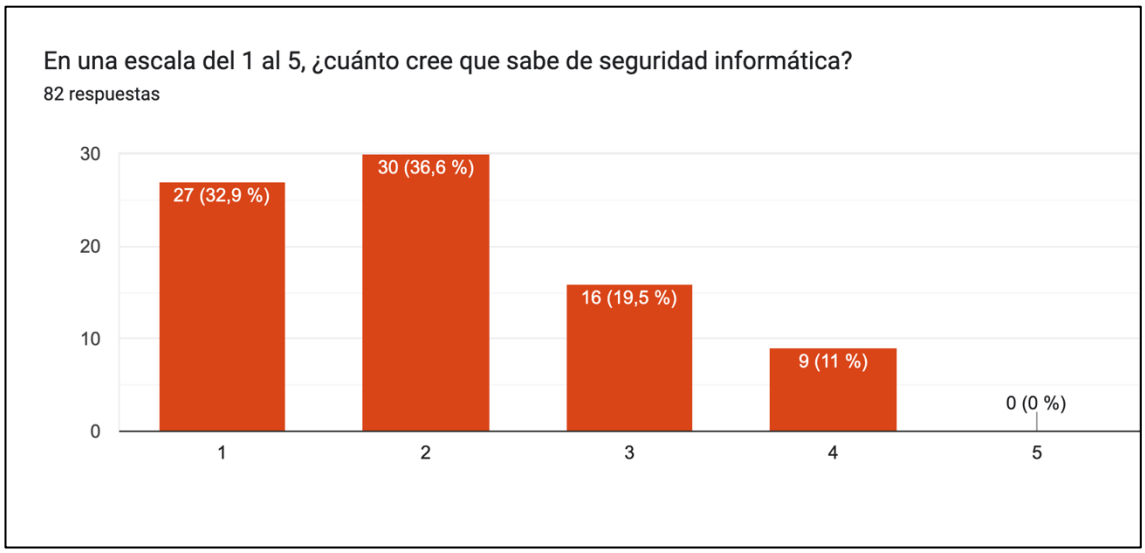

Gráfico 5. Respuestas a la pregunta 5 de la encuesta

Fuente: Elaboración propia.

De los datos obtenidos, se puede concluir que los encuestados no cuentan con un amplio conocimiento en seguridad informática.

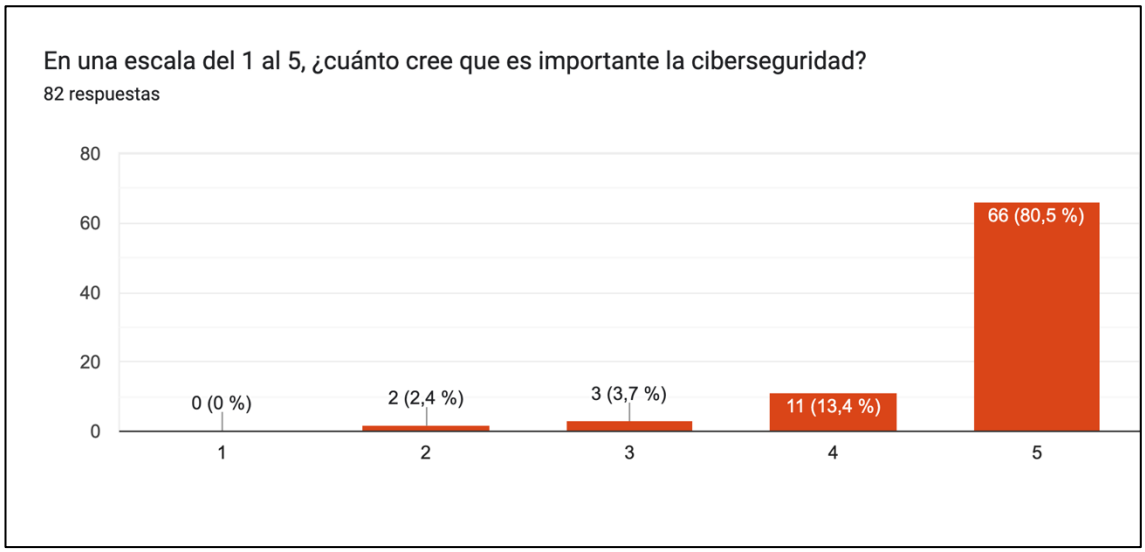

Gráfico 6. Respuestas a la pregunta 6 de la encuesta

Fuente: Elaboración propia.

Sin embargo, como ya adelantábamos previamente, todos están de acuerdo en que la ciberseguridad es muy importante.

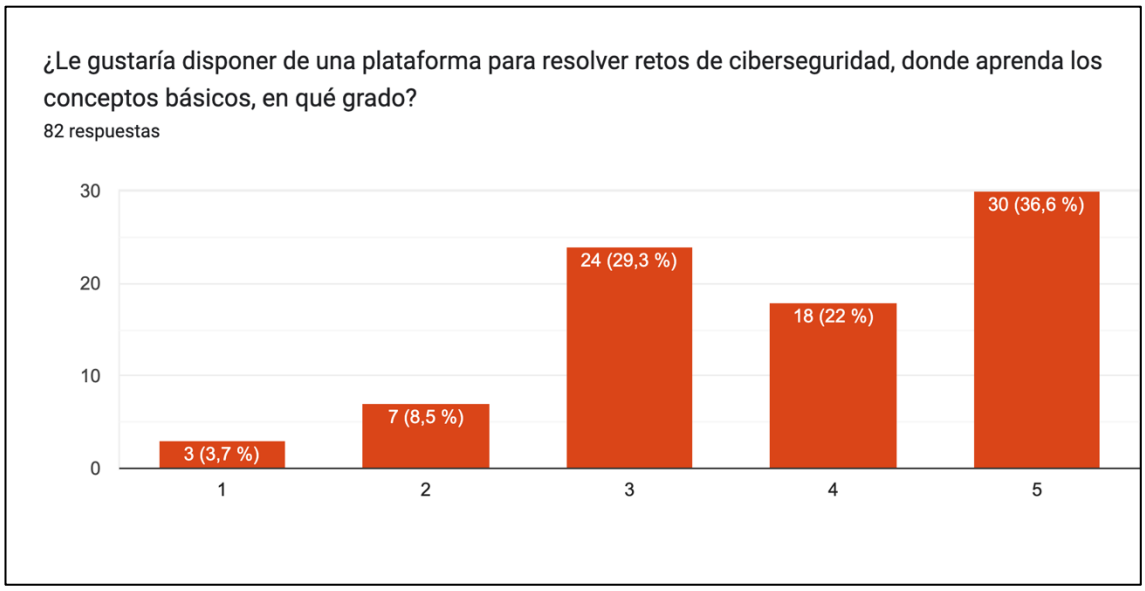

Gráfico 7. Respuestas a la pregunta 7 de la encuesta

Fuente: Elaboración propia.

La muestra cree en un amplio espectro que una plataforma para resolver retos de ciberseguridad, le sería útil.

Gráfico 8. Respuestas a la pregunta 8 de la encuesta

Fuente: Elaboración propia.

Asimismo, son más los que creen que un foro con expertos, les sería de mayor utilidad.

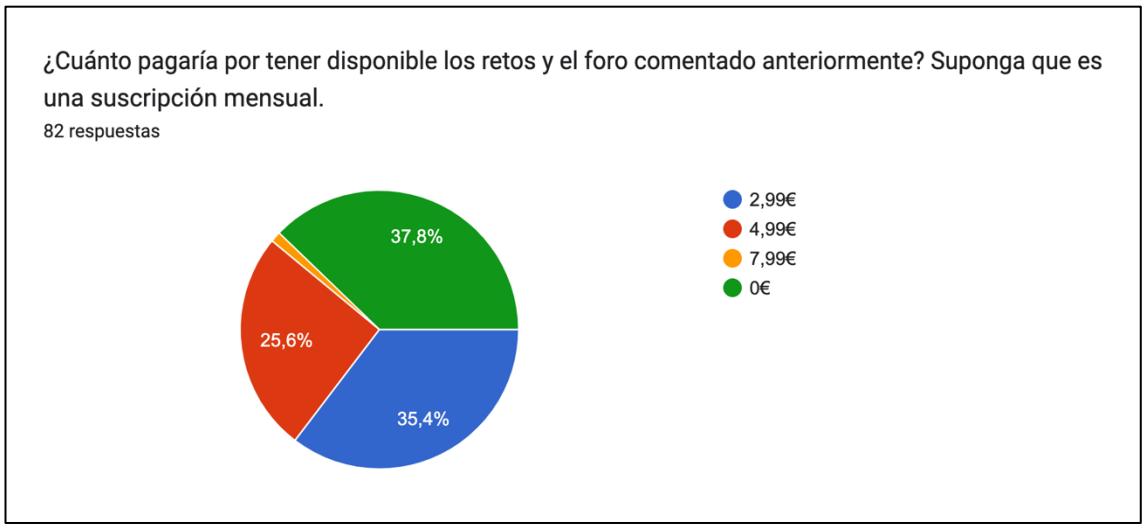

Gráfico 9. Respuestas a la pregunta 9 de la encuesta

Fuente: Elaboración propia.

Podemos concluir a nivel de ingresos, que entorno a un 60% de la muestra, estaría dispuesto a pagar 2,99€, por una plataforma como la que nosotros ofrecemos.

De las conclusiones parciales realizadas en cada gráfico, podemos concluir que los usuarios, en términos generales, están preocupados por la seguridad informática, no tienen mucho conocimiento sobre esta, tanto a nivel práctico (por las preguntas realizadas) así como por concienciación. Por ello, dichos usuarios han marcado que ven atractivos los retos y el foro con el experto, siendo esto último lo más atractivo, y más de la mitad estaría dispuesto a pagar, como mínimo, tres euros mensuales por su acceso, cuestión que nos da indicios para la tarea de establecimiento de precios y el estudio de la viabilidad económica.

4.2.4 – Estudio de la viabilidad operativa

En este apartado, realizaremos un análisis de la viabilidad operativa, técnica o también denominada tecnológica, con el fin de determinar si es posible su despliegue en el mercado y que los usuarios hagan uso del producto. Como resulta evidente, a lo largo de esta memoria, hemos desarrollado el producto mínimo viable, por lo que

podemos afirmar que es técnicamente posible programar la aplicación con las funcionalidades que hemos descrito. En cuanto a su despliegue, dicha aplicación se podría implantar en un hosting web sin ninguna dificultad, sin necesidad de uso de grandes servidores (sin uso de Amazon AWS o MS Azure, por ejemplo), teniéndose en cuenta esta cuestión en los costos de mantenimiento de la web. En un futuro, en función del número de usuarios o tráfico de la web, podríamos plantearnos la migración a alguno de los servicios web de hosting mencionados anteriormente. Por tanto, concluimos que la aplicación es viable para un puesta en marcha en el mercado.

4.2.5 – Estudio de la viabilidad económica

Para el estudio de la viabilidad económica, realizaremos el cálculo del VAN y del TIR, determinando antes los flujos netos de caja para dichos cálculos. Supongamos que, para este proyecto, es necesario un mobiliario por 2.000 euros, que corresponde al mobiliario de la oficina dentro de casa, ya que el proyecto es en remoto, 30.000 euros, que es el coste de la activación del intangible de la aplicación informática (el equivalente de un año de sueldo de un programador informático), 6.750 euros en equipos para procesos de información (ordenador, entre otros), y se incluyen unos 3.000 euros en gastos de constitución y puesta en marcha del negocio (gestión del autónomo y gastos de gestoría iniciales). El total de la inversión ascendería a 41.750, según podemos ver en la Tabla 2 a continuación. De estos importes, suponemos como autofinanciación los 30.000 euros, puesto que somos nosotros los que llevaremos el desarrollo, y 7.000 euros serán puestos de nuestra liquidez personal, financiándose 4.750 euros.

Tabla 2. Detalle de inversión inicial

INVERSIÓN INICIAL	2023
INVERSIONES INTANGIBLES	30.000,0
Aplicaciones informáticas	30.000,0
INVERSIONES MATERIALES	8.750,0
Mobiliario	2.000,0
Equipos procesos información	6.750,0
PROVISIÓN DE FONDOS	3.000,0
Gastos de constitución y puesta en marcha	3.000,0
TOTAL	41.750,0

Fuente: Elaboración propia.

En cuanto a los flujos de efectivo propiamente dichos, hemos determinado el fujo de ingresos teniendo en cuenta la encuesta hecha previamente, y los mercados geográficos a los que nos dirigiremos durante los cinco primeros años. En primer lugar, hemos tomado como referencia, como mercado potencial, el número de usuarios de las plataformas INCIBE y ciberseguridad.com, siendo una media de 420 mil usuarios (estimamos que los usuarios que usan ambas plataformas son los mismos). En España, acorde la estadística del INE en 2022, 33,5 millones de españoles usan internet, por lo que un 1,25% de los usuarios que usan internet en España usan INCIBE y ciberseguridad.com. Si extrapolamos esto a las personas que usan internet en Gran Canaria (Gobierno de Canarias, 2022), que son 827.664 personas, nos da un mercado potencial de 10.377 personas que activamente visitan webs sobre ciberseguridad en Gran Canaria. Teniendo en cuenta que se han encuestado a 82 personas, y que de estos el 60% pagaría, al menos, 2,99 euros por el producto, los usuarios captados en un mes ascienden a unos 49 clientes que, si fuésemos capaces de obtener esos clientes mensualmente, acabaríamos el año con 590 usuarios el primer año, que representan el 9% del mercado potencial grancanario en temas de seguridad informática.

En cuanto al segundo año, partimos de un planteamiento de expansión a todas Canarias (2.261 mil habitantes en 2023 según DatosMacro (2023b), siendo el porcentaje de usuarios de internet el 97%, de acuerdo con EuropaPress(2023a), lo que ascendería a 2.194 miles de usuarios. Partiendo del supuesto anterior, donde captamos en torno a un 60% de las personas que llegamos a encuestar, también teniendo en cuenta el esfuerzo realizado en publicidad con marketing digital, que comentaremos más adelante, podemos estimar que, en el segundo año, se podría llegar a 2.155 usuarios entre lo que se captó en Gran Canaria el primer año, y en el total de Canarias en este segundo año. En el tercer año, se hace una expansión a Andalucía, teniendo en cuenta que los habitantes de dicha región son 8.538 mil (Datos Macro, 2023a) y que el 84,7% usan internet (EuropaPress, 2023b), podemos constatar que 7.232 miles de usuarios usan internet que, por transitividad de la hipótesis realizada con Canarias, podríamos tener 7.314 usuarios, teniendo en cuenta los que ya hemos adquirido en Canarias y estamos adquiriendo, por el efecto del marketing digital. Para toda España, pariendo de los datos que ya teníamos (33,5 millones de españoles que usan internet y el uso de INCIBE y ciberseguridad.com), podemos estimar que para el cuarto año podríamos tener 31.211 usuarios. Para el quinto año, suponemos un incremento del 10% respecto al cuarto año, por lo que tendríamos 34.332 usuarios. En la Tabla 3 mostramos un resumen de los usuarios que se obtienen cada año.

Tabla 3. Usuarios a final de cada año.

	PRIMER	SEGUNDO	TERCERO	CUARTO	QUINTO
USUARIOS AL FINAL DEL AÑO	590	2.155	7.314	31.211	34.332

Fuente: Elaboración propia.

Los ingresos, suponiendo que se ingresan aproximadamente 3 euros por cada mes, sería según lo expuesto en la Tabla 4:

Tabla 4. Ingresos al final de cada año.

	PRIMER	SEGUNDO	TERCERO	CUARTO	QUINTO
INGRESOS	21.254	77.591	263.309	1.123.589	1.235.947

Fuente: Elaboración propia.

En cuanto a los gastos o costes de la aplicación, hemos identificado 3 costes principales:

- Coste del hosting. Hemos verificado a través de Amazon AWS y Microsoft Azure, en un servidor tipo EC2, el coste por cada 500 usuarios y año (suponiendo que por cada 500 usuarios hay 10 concurrentes para que no afecte al rendimiento de la plataforma). Teniendo en cuenta el coste de Azure por 12 meses e incluyendo el de Amazon, realizando una media aritmética simple entre los dos precios obtenemos 578,16 euros al año.

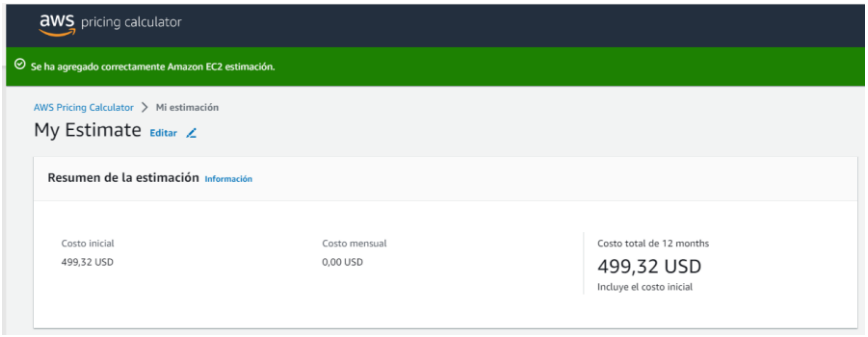

Ilustración 26. Coste estimado en AWS por 500 usuarios por año

Fuente: Amazon (2023).

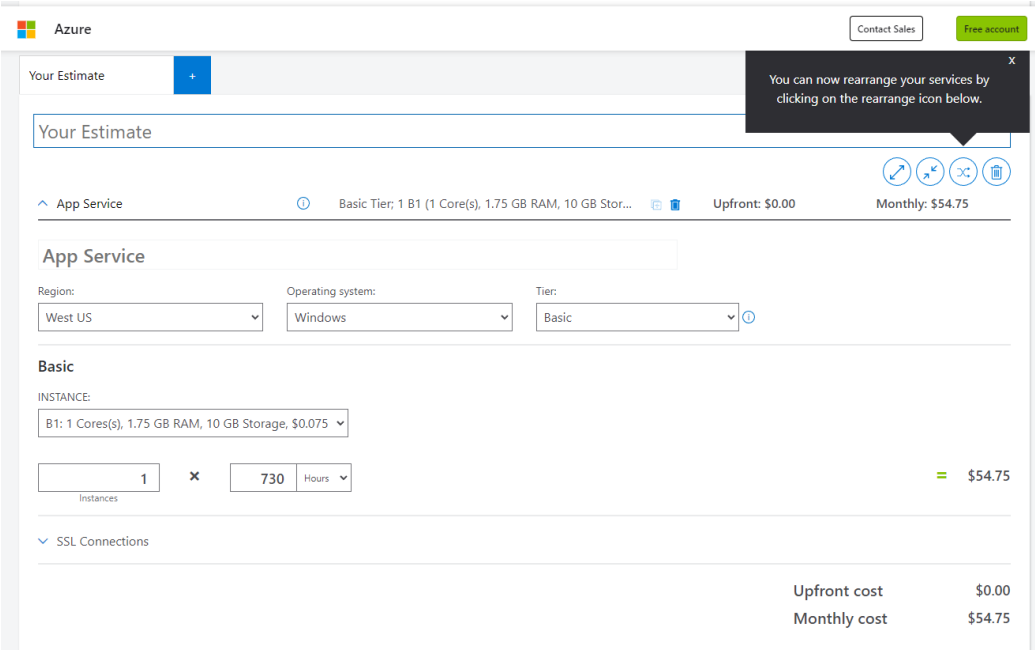

Ilustración 27. Coste estimado de Azure por 500 usuarios por año.

Fuente: Microsoft (2023)

- Coste de marketing digital en Google Adwords. Según Xplora (2020), el coste de Google Adwords para una web básica (suponemos una web básica con un tráfico inferior a 5 mil usuarios al mes) sería de 75 euros al mes, 9000 euros al año; de una web media (entre 5 y 10 mil usuarios), sería de 400 euros al mes, 4800 al año; y de una web compleja, de más de 10 mil usuarios al mes, sería de 900 euros al mes, 10.800 euros al año.

- Coste de marketing digital en Instagram. De acuerdo con Jevnet (2022), el coste de una campaña en una región pequeña, como puede ser Canarias, estaría en torno a 3 euros por cada mil impresiones al mes, 36 euros al año por cada mil impresiones, 6,5 euros para fuera de Canarias, sin incluir todo el territorio español (78 euros al año por cada mil impresiones) y para toda España 10 euros por mes y por mil impresiones (120 euros al año).

Por tanto, los costos, teniendo en cuenta el volumen de usuarios que obtenemos cada año, sería el expuesto en la Tabla 5.

Tabla 5. Total de costos de la aplicación en cada año.

	PRIMER	SEGUNDO	TERCERO	CUARTO	QUINTO
GOOGLE ADWORDS	900	900	4.800	10.800	10.800
INSTAGRAM	21.254	38.796	114.101	749.059	411.982
HOSTING	683	2.492	8.457	36.090	39.699
COSTE TOTAL POR AÑO	**22.837**	**42.188**	**127.358**	**795.949**	**462.481**

Fuente: Elaboración propia.

De ambos, podemos obtener los flujos netos de caja, teniendo en cuenta la devolución del préstamo y la inversión total realizada (véase Tabla 6).

Tabla 6. Determinación de los flujos netos de caja, con la información expuesta anteriormente.

Año	2023	2024	2025	2026	2027	2028
Ingresos		21.254	77.591	263.309	1.123.589	1.235.947
Gastos		22.837	42.188	127.358	795.949	462.481
Beneficios		-1.583	35.403	135.951	327.640	773.466
Amortización		8.350	8.350	8.350	8.350	8.350
Inversión	41.750					
Préstamos	4.750					
Devolución prestamos			-1.128	-1.128	-1.128	-1.128
Flujo neto de caja	-37.000	6.767	42.626	143.173	334.862	780.689
FNC acumulado	-37.000	-30.233	12.393	155.566	490.429	1.271.117

Fuente: Elaboración propia.

Con los datos expuestos anteriormente, podríamos calcular el VAN y la TIR. En cuanto al cálculo del VAN, Valor Actual Neto, consiste en actualizar los cobros y pagos futuros (suponemos que todos los ingresos y costes se pagan en el año) al momento actual, teniendo en cuenta la inversión. Estos flujos se descuentan a un tipo de interés k (véase Ecuación 1). Este importe nos permite tomar decisiones:

- Si el VAN es mayor que cero, el proyecto generará beneficios.

- Si es cero, es indiferente.

- Si es menor que cero, generará perdidas.

Ecuación 1. Formula del cálculo del VAN.

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{(1+k)^t} = -I_0 + \frac{F_1}{(1+k)} + \frac{F_2}{(1+k)^2} + \cdots + \frac{F_n}{(1+k)^n}$$

Fuente: Economipedia (2020b)

Donde:

- Ft son los flujos de dinero en cada periodo.
- I_0 es la inversión realiza en el momento inicial (t = 0).
- n es el número de periodos de tiempo.
- k es el tipo de descuento o tipo de interés exigido a la inversión.

De acuerdo con los flujos de efectivo planteados previamente, nuestro cálculo del VAN sería el dispuesto en la Ecuación 2 (suponiendo una tasa de descuento de un 5%):

Ecuación 2. Cálculo del VAN de nuestro proyecto

$$VAN = -37.000 + \frac{6.767}{(1{,}05)} + \frac{42.626}{(1{,}05)^2} + \frac{143.173}{(1{,}05)^3} + \frac{334.862}{(1{,}05)^4} + \frac{780.689}{(1{,}05)^5} = 968.684\ euros$$

Fuente: Elaboración propia.

Por tanto, podemos constatar que el proyecto generará beneficios en el futuro. En lo que respecta al cálculo de la TIR, esta está íntimamente relacionada con el VAN, puesto es que el tipo de descuento que hace que el VAN sea cero. En función del valor de al TIR, podemos estimar si el negocio es económicamente viable o no (ver Ecuación 3):

- Si TIR>k, entonces el negocio es rentable.

- Si TIR=k nos da indiferencia a realizar el negocio.

- Si TIR<k, entonces el negocio no es rentable, daría pérdidas.

Ecuación 3. Cálculo teórico de la TIR.

$$VAN = -I_0 + \sum_{t=1}^{n} \frac{F_t}{(1+TIR)^t} = -I_0 + \frac{F_1}{(1+TIR)} + \frac{F_2}{(1+TIR)^2} + \cdots + \frac{F_n}{(1+TIR)^n} = 0$$

Fuente: Economipedia (2020a)

Aplicado a nuestra casuística, sería la información dispuesta en la Ecuación 4.

Ecuación 4. Cálculo de la TIR aplicado a nuestro proyecto

$$VAN = -37.000 + \frac{6.767}{(1+TIR)} + \frac{42.626}{(1+TIR)^2} + \frac{143.173}{(1+TIR)^3} + \frac{334.862}{(1+TIR)^4} + \frac{780.689}{(1+TIR)^5} = 0$$

Fuente: Elaboración propia.

De esta expresión, realizando un cálculo a través de una función de una hoja de cálculo, obtendríamos que la TIR es 146%, mucho mayor que nuestra tasa de descuento del 5%. Finalmente, en cuanto al plazo de recuperación de la inversión, este sería de 1 año y 10 meses (1,8 años), que sería el tiempo que tardaríamos en cubrir la inversión inicial (41.750 euros) con los flujos netos de caja obtenidos.

Capítulo 5: Conclusiones y trabajo futuro

5.1 – Conclusiones del Trabajo Fin de Grado

Para abordar el plan de empresa y el Producto Mínimo Viable (PMV), realizado en este Trabajo Fin de Grado, hemos necesitado estudiar la importancia de la ciberseguridad en los distintos entornos. Ha sido una oportunidad excelente para aprender más sobre ciberseguridad y sobre las diferentes técnicas de ataque más usadas, incluso existiendo alguna que no conocía previamente. Nos permite estar actualizados siempre en temas de seguridad, puesto que algún día pudiéramos sufrir algunos de estos ataques. Conocer los métodos que estos "ciberdelincuentes" emplean, sirven como ejemplo de concienciación de cara a mantener un código siempre seguro ya que, en la mayoría de casos, son vulnerabilidades en la implementación que los atacantes descubren. En aplicación a lo aprendido, hemos implementado los ataques de menor a mayor complejidad, viendo así, reto por reto, la codificación y decodificación de un mensaje, la diferencias principales de los protocolos de red HTTP frente HTTPS, la importancia de los algoritmos hash, un ejemplo de inyección SQL (sin hacer uso de ninguna base datos, puesto a que no tenemos back-end en la aplicación web desarrollada) y, finalmente, un ataque por fuerza bruta para la obtención de una contraseña numérica.

Es cierto que son pocas las personas que se informan diariamente de estos fenómenos, pero hemos aprendido que resulta ser labor imprescindible para personas dedicadas al sector de la informática, puesto a la masiva información que está presente en las redes y cada vez se tienden a subir más cosas personales, dejando así la duda de que puedan ser atacadas algún día. Es importante matizar las técnicas que han sido empleadas por los diferentes atacantes dada su diversidad, originalidad y eficiencia, todo ello unido a una concienciación absoluta en materias de ciberseguridad. A pesar de estar informados en todo momento y subiendo los parámetros de seguridad de nuestro sistema, siempre podemos ser víctimas indirectas de un ataque como lo es el caso de los ataques por inyección SQL, los cuales acceden a las bases de datos que contiene información que le proporcionamos a las empresas.

En cuanto al Producto Mínimo Viable, hemos podido aprender a desarrollar una aplicación web simple, incluyendo las dificultades de implementación de los retos en ciberseguridad. En este hemos podido aplicar distintas tecnologías para realizar un producto presentable y acorde a los estándares web actuales.

Finalmente, en lo relativo al plan de empresa, hemos diseñado un modelo de negocio acorde al producto que queremos vender en nuestro mercado. En él hemos aplicado diversas herramientas disponibles en el modelo Lean-StartUp como es el Business Model Canvas. Asimismo, hemos analizado el mercado desde diferentes ópticas a través del análisis de viabilidades, habiéndose cumpliendo los objetivos iniciales del Trabajo Fin de Grado.

5.2 – Trabajo futuro

En este Trabajo Fin de Grado, nos hemos marcado una serie de objetivos que se han cumplido. En resumidas cuentas, se ha tratado de la creación de un Producto Mínimo Viable y de un plan de negocio. En este marco, hemos programado una aplicación web sencilla que muestra las funcionalidades de los retos y el foro, y un modelo de negocio simple que se ajuste a esta realidad, con el fin de demostrar la viabilidad de la implementación del producto en el mercado.

Derivado de nuestro interés en seguir desarrollando el producto, determinamos un trabajo futuro que se podría continuar desarrollando para vender la aplicación web definitiva. Hemos valorado las siguientes dos líneas de trabajo futuras:

1) Mejorar el Producto Mínimo Viable. El objetivo que perseguimos es lanzar el producto en el mercado, implementando el back-end del producto incluyendo más retos y mejorando el foro.

2) Seguir "pivotando" el modelo de negocio. A través de las reseñas de los fututos clientes y mayor análisis del mercado, creando una *landing page* para ver el comportamiento del potencial cliente. Con esto podremos afinar la viabilidad económica y la comercial para el futuro lanzamiento del producto.

Al realizarse estas dos líneas, podría haber mayor confianza y algunos clientes potenciales donde poner el producto en fase de prueba. Con ello, podríamos cerciorarnos que el producto funcionaría en el mercado y crearnos posibles escenarios de implantación del producto.

Capítulo 6: Bibliografía

Amazon (2023). Estimación del coste de un servidor Amazon AWS. Recuperado el 11 de julio de 2023 de https://calculator.aws/#/

Cámara de Comercio de Oviedo (2020). ¿Cómo determinar la viabilidad económica de un proyecto empresarial? Aspectos clave. Recuperado el 26 de mayo de 2023 de https://www.mba-asturias.com/empresas/viabilidad-economica-proyecto-empresarial/

Cloudflare. (2023). ¿Qué es HTTP? Recuperado el 3 de junio de 2023 de https://www.cloudflare.com/es-es/learning/ddos/glossary/hypertext-transfer-protocol-http/

Crehana (2023). Ejemplos de modelo canvas. Recuperado el 21 de mayo de 2023 a partir de https://www.crehana.com/blog/negocios/ejemplos-de-modelo-/

Cybersecurity News. (2023). El 69% de las organizaciones españolas experimentaron al menos una violación de datos en 2022. Recuperado el 22 de mayo de 2023, de https://cybersecuritynews.es/el-69-de-las-organizaciones-espanolas-experimentaron-al-menos-una-violacion-de-datos-en-2022/

DatosMacro (2023a). Población de toda Andalucía. Recuperado el 11 de julio de 2023 de https://datosmacro.expansion.com/ccaa/andalucia

DatosMacro (2023b). Población de toda Canarias. Recuperado el 11 de julio de 2023 de https://datosmacro.expansion.com/ccaa/canarias

EC-Council. (2023). What are Sniffing Attacks? Recuperado el 3 de junio de 2023 de https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-are-sniffing-attacks/

Economipedia (2020a). Tasa interna de retorno (TIR). Recuperado el 11 de julio de 2023 de https://economipedia.com/definiciones/tasa-interna-de-retorno-tir.html

Economipedia (2020b). Valor actual neto (VAN). Recuperado el 11 de julio de 2023 de https://economipedia.com/definiciones/valor-actual-neto.html

Educative. (2023). How is SHA-256 used in blockchain and why? Recuperado el 5 de junio de 2023 de https://www.educative.io/answers/how-is-sha-256-used-in-blockchain-and-why

El Confidencial. (2018). British Airways sufrió el robo de datos personales y de tarjetas de crédito de 380.000 clientes. Recuperado el 20 de mayo de 2023 de https://www.elconfidencial.com/empresas/2018-09-06/british-airways-robo-de-datos-iag_1612552/

EuropaPress (2023a). Casi el 97% de las viviendas de Canarias tienen acceso a internet. Recuperado el 11 de julio de 2023 de https://www.europapress.es/islas-canarias/noticia-casi-97-viviendas-canarias-tienen-acceso-internet-20230514150049.html

EuropaPress (2023b). El número de personas que usa Internet a diario se sitúa en un 84,7% según el Barometro Audiovisual de Andalucía. Recuperado el 11 de julio de 2023 de https://www.europapress.es/esandalucia/malaga/noticia-numero-personas-usa-internet-diario-situa-847-barometro-audiovisual-andalucia-20230321135251.html

Expansión. (2018). La ciberseguridad se convierte en prioridad para las empresas. Recuperado el 24 de mayo de 2023 de https://www.expansion.com/economia-digital/companias/2018/10/12/5bc0ef4546163f07218b45f0.html

Gobierno de Canarias (2022). Conocimiento publica la encuesta sobre equipamiento y uso de las TICs en los hogares canarios. Recuperado el 11 de julio de 2023 de https://www3.gobiernodecanarias.org/noticias/conocimiento-publica-la-encuesta-sobre-equipamiento-y-uso-de-tic-en-los-hogares-canarios/

HackThisSite (2023). HackThisSite. Recuperado el 2 de mayo de 2023 de https://www.hackthissite.org/

Hoswedaje. (2023). ¿Cada cuánto tiempo es conveniente cambiar las contraseñas? Recuperado el 14 de mayo de 2023 de https://www.hoswedaje.com/seguridad/cada-cuanto-tiempo-es-conveniente-cambiar-las-contrasenas/

Humphrey, A. (2005) SWOT Analysis for Management Consulting. SRI Alumni Newsletter. SRI International, United States.

INCIBE. (2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. Recuperado el 12 de mayo de 2023 de https://www.incibe.es/empresas/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

INCIBE. (2020). Evitando riesgos de ciberseguridad en el puesto de trabajo. Recuperado el 12 de mayo de 2023 de

https://www.incibe.es/empresas/blog/evitando-riesgos-ciberseguridad-el-puesto-trabajo

INE (2022). Población que usa Internet (en los últimos tres meses). Tipo de actividades realizadas por Internet. Recuperado el 8 de junio de 2023 de https://www.ine.es/ss/Satellite?L=es_ES&c=INESeccion_C&cid=1259925528782&p=1254735110672&pagename=ProductosYServicios%2FPYSLayout#:~:text=En%20el%20a%C3%B1o%202022%20en,33%2C5%20millones%20de%20usuarios.

Infoautonomos (2023). Análisis DAFO. Recuperado el 21 de mayo de 2023 a partir de https://www.infoautonomos.com/plan-de-negocio/analisis-dafo/

Infobae (2022). Infografía cuanto tiempo demora un hacker en descubrir tu contraseña. Recuperado el 3 de mayo de 2023 a partir de https://www.infobae.com/america/tecno/2022/05/06/infografia-cuanto-tiempo-demora-un-hacker-en-descubrir-tu-contrasena/

Jevnet (2022). Precio de la publicidad en Instragram. Recuperado el 11 de julio de 2023 de https://www.jevnet.es/precio-publicidad-instagram/

Kaspersky. (2023). Brute Force Attack. Recuperado el 7 de junio de 2023 de https://www.kaspersky.com/resource-center/definitions/brute-force-attack/

Kaspersky. (2023). Public Wi-Fi Risks: The Dangers of Using Free Wi-Fi. Recuperado el 21 de mayo de 2023 de https://www.kaspersky.es/resource-center/preemptive-safety/public-wifi-risks

La Provincia. (2018). ULPGC blinda su web ante un ataque de 'purga'. Recuperado el 20 de mayo de 2023 de https://www.laprovincia.es/sociedad/2018/10/09/ulpgc-blinda-ataque-web-purga-9444555.html

López, H. (2016). El Mapa de Empatía: Diseño de modelos de negocio a través del cliente. Recuperado el 12 de junio de 2023 de https://hugolopezc.com/mapa-de-empatia-herramienta-emprendedores/

Microsoft (2023). Estimación del coste de un servicio de Microsoft Azure. Recuperado el 11 de julio de 2023 de https://azure.microsoft.com/es-es/pricing/calculator/

Mozilla. (2020). Documentación Web de MDN. Recuperado el 1 de junio de 2023 de https://developer.mozilla.org/es/docs/Web/HTML

Mozilla. (2022). Cadenas binarias. Recuperado el 1 de junio de 2023 de https://developer.mozilla.org/es/docs/Web/API/btoa

Mozilla. (2023). Función WindowsBase64.atob(). Recuperado el 1 de junio de

2023 de https://developer.mozilla.org/es/docs/Web/API/atob
Nunsys. (2023). La importancia de la ciberseguridad en el eCommerce. Recuperado el 16 de mayo de 2023 de https://www.nunsys.com/la-importancia-de-la-ciberseguridad-en-el-ecommerce/

Osterwalder, A.; Pigneur, Y. (2013). Business Model Generation. Hoboken, NJ: Wiley.

OWASP. (2023). SQL Injection. Recuperado el 6 de junio de 2023 de https://owasp.org/www-community/attacks/SQL_Injection

Ries, E. (2011). The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses. Crown Business.

Rodríguez-Ariza, L. (2017). Viabilidad de proyectos. Universidad de Granada. Recuperado el 26 de mayo de 2023 de https://ugremprendedora.ugr.es/viabilidad-de-proyectos/

Softonic (2023). Sublime Text para Mac. Recuperado el 3 de mayo de 2023 a partir de https://sublime-text.softonic.com/mac

Stack overflow. (2023). Recuperado el 24 de mayo de https://stackoverflow.com/

Teorema-rd (2023). Course 2048oc programming in html5 with javascript and css3. Recuperado el 3 de mayo de 2023 a partir de https://teorema-rd.com/curso/course-20480c-programming-in-html5-with-javascript-and-css3

The Bridge. (2021). 10 preguntas para una entrevista de trabajo en ciberseguridad. Recuperado el 22 de mayo de 2023 de https://www.thebridge.tech/blog/10-preguntas-entrevista-de-trabajo-ciberseguridad

Torres, J. (2011). Búsqueda hash. Recuperado el 1 de junio de 2023 a partir de http://jitorres.blogspot.com/2011/11/busqueda-hash.html

Xplora (2020). Coste Google Adwords. Recuperado el 11 de julio de 2023 de https://www.xplora.eu/precio-google-ads/

Capítulo 7: Anexo

I. Anexo código de los retos y el cuestionario desarrollado.

reto1.html

```html
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Reto 1 </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script>
            function comprobarPassword() {

                if (document.getElementById("password").value == "aprobar") {
                    location.href="retoSuperado.html";
                } else {
                    alert("Contraseña incorrecta");
                }

            }

            function showPassword() {
                var x = document.getElementById("password");
                if (x.type == "password") {
                    x.type = "text";
                } else {
                    x.type = "password";
                }
            }
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>
            </ul>

        </nav>
        </header>

        <h1> Nivel 1 básico </h1>

        <br>
        <p> Para superar este nivel es necesario que conozcas HTML. Tu tarea es descubrir la contraseña que se pide. </p>
        <input type="password" name="contraseña" id="password">
        <input type="checkbox" onclick="showPassword()"> Mostrar contraseña
        <button onclick="comprobarPassword()"> Enviar </button>

        <!-- La contraseña es: aprobar -->

        <div class="footer">

            <p>© Karan Sainani 2023</p>
            <p> Made with &#128154 in Canary Islands </p>
        </div>


    </body>

    <br>
    <a href="index.html">Inicio</a>

</html>
```

reto2.html

```html
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Reto 2 </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script src="retos.js">
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>
            </ul>

        </nav>
        </header>

        <h1> Nivel 2 básico </h1>

        <br>


        <p>El mensaje codificado es:</p>
        <p id="mensaje_codificado"> S2FyYW4gTmFuZHBhbCBTYWluYW5p</p>

        <p> Introduce el mensaje anterior decodificado </p>
        <div class="tool">
            <input id="entrada1" type="text" size="50"/>
            <!--<button type="submit" onclick="encriptar()">Encriptar</button> -->
        </div>

        <hr>

        <p>El mensaje decodificado es:</p>
        <p> Cuidado con el phishing</p>

        <p> Introduce el mensaje anterior codificado </p>
        <div class="tool">
            <input id="entrada2" type="text" size="50"/>

        </div>

        <button type="submit" onclick="codificar_descodificar()">OK</button>

         <div class="footer">

             <p>© Karan Sainani 2023</p>
             <p> Made with &#128154 in Canary Islands </p>
         </div>


    </body>

    <br>
    <a href="index.html">Inicio</a>

</html>
```

retos.js

```
var resultado1;
var resultado2;


function codificar_descodificar(elemento){
  var texto1 = document.getElementById("entrada1").value;
  var texto2 = document.getElementById("entrada2").value;

  if ( texto1 == "Karan Nandpal Sainani"  && texto2 =="Q3VpZGFkbyBjb24gZWwgcGhpc2hpbmc=") {
    location.href = "retoSuperado.html";
  } else {
    alert("Error, inténtalo de nuevo");
  }
}
```

reto3.html

```
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Reto 3 </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script>
            function comprobarUserPassword() {

                if (document.getElementById("password").value == document.getElementById("password_real").value && document.getElementById("user_real").value == document.
                    getElementById("user").value) {
                    console.log("Aquí");
                    location.href="retoSuperado.html";
                } else {
                    alert(" Usuario y/o contraseña incorrecta");
                    document.getElementById("formulario").submit();
                }

            }

            function showPassword() {
                var x = document.getElementById("password");
                if (x.type == "password") {
                    x.type = "text";
                } else {
                    x.type = "password";
                }
            }
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>
            </ul>

        </nav>
        </header>

        <h1> Nivel 3 intermedio </h1>

        <br>
        <p> Para superar este nivel es necesario que conozcas el protocolo HTTP. Tu tarea es descubrir el usuario y la contraseña a través de la petición. </p>
        <form action="reto3.html" method="post" id="formulario">
            <input type="hidden" name="usuario_real" id="user_real" value="karan">
            <input type="hidden" name="contraseña_real" id="password_real" value="pepito">
            <p> Usuario </p>
            <input type="text" name="usuario" id="user">
            <p> Contraseña </p>
            <input type="password" name="contraseña" id="password">
            <input type="checkbox" onclick="showPassword()"> Mostrar contraseña
            <input type="button"   onclick="comprobarUserPassword()" value="Enviar">
        </form>

        <p> Al mandar peticiones con el protocolo HTTP y no con su versión segura HTTPS, podemos observar que los datos se ven en texto plano en la respuesta. Usar el HTTPS
        evita que existan ataques de tipo Man in the middle. Por ejemplo cuando estamos en un aeropuerto y nos conectamos a una red pública otro equipo podría hacer sniffering
        (ataque intercepción de datos) y ver los datos de los paquetes HTTP. </p>

        <div class="footer">

            <p>© Karan Sainani 2023</p>
            <p> Made with &#128154 in Canary Islands </p>
        </div>


    </body>

    <br>
    <a href="index.html">Inicio</a>

</html>
```

reto4.html

```html
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Reto 4 </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script>
            function comprobarHash() {

                if (document.getElementById("hash").value == "1d1ba092f9baca08b6f533f3709f6892d49275df8d3a1d2b9cdac760ad9d43c4") {
                    location.href="retoSuperado.html";
                } else {
                    alert("Hash incorrecto");
                }

            }
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>
            </ul>

        </nav>
        </header>

        <h1> Nivel 4 intermedio </h1>

        <br>
        <p> Para superar este nivel es necesario que conozcas los algoritmos de hash. Tu tarea es obtener el hash del fichero. </p>

        <p> Solo hay un algortimo de hash válido. </p>

        <a href="fichero.pdf" download>
        <img src="icon_pdf.png" width="50" height="50">
        </a>
        <br>
        <input type="text" placeholder="Introduce el hash" id="hash">
        <button id="Ok" onclick="comprobarHash()"> OK </button>

        <!-- Terminal: shasum -a 256 /Users/karansainani/Desktop/TFT01-v17\ KNS_firmado_OK2.pdf  -->

        <div class="footer">

            <p>© Karan Sainani 2023</p>
            <p> Made with &#128154 in Canary Islands </p>
        </div>


    </body>

    <br>
    <a href="index.html">Inicio</a>

</html>
```

reto5.html

```html
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Reto 5 </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script>
            function buscar() {
    // Declare variables
    var input, filter, ul, li, a, i, txtValue;

    input = document.getElementById('busqueda');
    filter = input.value.toUpperCase();
    tabla = document.getElementById("tabla");
    tr = tabla.getElementsByTagName('tr');

    for (i = 1; i < tr.length; i++) {
        td = tr[i].getElementsByTagName('td');
        texto = ""
        for (j = 0; j < td.length; j++) {
            texto = texto + " " + td[j].innerText || td[j].textContent;
        }
        console.log(filter.toLowerCase());
        if (texto.toUpperCase().indexOf(filter) > -1) {
            tr[i].style.display = "";
        } else if (filter.toLowerCase().indexOf('\'; delete from tabla; select * from tabla where ataque = \'') > -1) {
            console.log("hola");
            tabla.innerHTML = "<p>La tabla se ha borrado con éxito</p>";

            setTimeout(function(){
                location.href = "retoSuperado.html";
            }, 3000);

        } else {
            tr[i].style.display = "none";
        }
    }
}
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>
            </ul>

        </nav>
        </header>

        <h1> Nivel 5 difícil </h1>

        <br>
        <p> Estamos mostrando una tabla que simula una búsqueda en una base de datos en un servidor. Queremos evidenciar que en el caso que no saneemos la búsqueda puede existir una inyección de código sql. En este caso buscamos un borrado de tabla. </p>

        <p> La consulta sql que supera el reto sería un sql inyectado con un borrado de la tabla (suponemos que los identificadores html coinciden con los nombres de la tabla y los campos) y una selección de todos los campos sobre la misma tabla donde el ataque es vacío. </p>

        <!-- Phishing'; delete from tabla; select * from tabla where ataque = ' -->
        <!-- -->

        <!--  select * from tabla where Contact like '$variable'-->
        <!-- select * from tabla where Contact like 'Maria'; delete from tabla; select * from tabla where ataque = ''-->


        <!-- Maria'; delete from deudas; select * from deudas where dinero= ' -->

        <!-- Eliminar todos los registros de la tabla tabla y luego se añade una orden mas para corregir un error de sintaxis que lo produciría una comilla simple sobrante -->

        <!-- Introducimos la primera comilla simple para concatenar en la string del código('$variable') nuestras consultas de ataque, el motivo de introducir la segunda comilla (al final de  nuestra sql) es porque necesitamos cerrar la comilla simple que se queda al final de la consulta original ('$variable') -->


        <!-- Necesito cerrar  -->


        <input type="text" id="busqueda" onkeyup="buscar()" placeholder="Buscar ataques..." size="70">
        <table id="tabla">
            <tr>
            <th>Ataque</th>
            <th>Afectado</th>
            <th>Año</th>
            </tr>
            <tr>
            <td>Phishing</td>
            <td>CNMV</td>
            <td>2018</td>
            </tr>
            <tr>
            <td>Malware en redes sociales</td>
            <td>YouTube</td>
            <td>2019</td>
            </tr>
            <td>Ataque dirigidos contra grandes corporaciones</td>
            <td>Facebook</td>
            <td>2018</td>
            </tr>
            <td>Botnets</td>
            <td>Huawei</td>
            <td>2018</td>
            </tr>
            <tr>
            <td>Ataques dirigidos contra dispositivos móviles</td>
            <td>Android</td>
```

```
            <td>2018</td>
            </tr>
            <tr>
            <td>Inyección de código SQL</td>
            <td>Altima Telecom</td>
            <td>2018</td>
            </tr>
            <tr>
            <td>Cross-Site Scripting (XSS)</td>
            <td>Wordpress</td>
            <td>2019</td>
            </tr>
        </table>


        <div class="footer">

            <p>© Karan Sainani 2023</p>
            <p> Made with &#128154 in Canary Islands </p>
        </div>


    </body>

    <br>
    <a href="index.html">Inicio</a>

</html>
```

reto6.html

```
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Reto 6 </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script>
            contra = "";
            function comprobarPassword() {
                let mensaje=document.getElementById("mensaje");
                let password_correct="123456";
                if (document.getElementById("password").value == password_correct) {
                    contra = "terminado";
                    mensaje.innerHTML="La contraseña es correcta. Has introducido:" + password_correct;
                    setTimeout(function(){
                        location.href = "retoSuperado.html";
                    }, 3000);
                } else {
                    let password_user=document.getElementById("password").value;
                    mensaje.innerHTML="La contraseña es incorrecta. Has introducido:" + password_user;

                }

            }

            function showPassword() {
                var x = document.getElementById("password");
                if (x.type == "password") {
                    x.type = "text";
                } else {
                    x.type = "password";
                }
            }
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>
            </ul>

        </nav>
        </header>

        <h1> Nivel 6 difícil </h1>

        <br>
        <p> Queremos evidenciar lo sencillo que es, obtener una contraseña numérica. En este reto es necesario obtener la contraseña desconocida. </p>
        <input type="password" name="contraseña" id="password">
        <input type="checkbox" onclick="showPassword()"> Mostrar contraseña
        <button id="ok" onclick="comprobarPassword()"> Enviar </button>
        <p id="mensaje"></p>
        <p> Las contraseñas de menos complejidad tardan menos en obtenerse mediante fuerza bruta. </p>

        <div class="footer">

            <p>© Karan Sainani 2023</p>
            <p> Made with &#128154 in Canary Islands </p>
        </div>


    </body>

    <br>
    <a href="index.html">Inicio</a>

</html>
```

cuestionario_OK.html

```
<!DOCTYPE html>
<html lang="es">
    <head>
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
        <title> Karan Sainani - Cuestionario </title>
        <link rel="stylesheet" type="text/css" href="style.css">
        <script>
        alert("Bienvenido a la Autoevaluación correspondiente al primer mes \n\nSeleccione las respuestas que crea correctas, teniendo en "+
      "\ncuenta las siguientes consideraciones \n\n1. Los aciertos tienen un valor de 0,625 puntos"+
      " \n\n2. Las respuestas no contestadas ni suman ni restan puntos.")

        function Borrar() {
            document.querySelectorAll('input').forEach(function(input){
            if (input.type == 'radio')
                input.checked = false;
            });
        }


        function Nivel () {
            var resp = new Array;
            var score = 0;

            resp[0] = document.getElementById('preg1_a').checked;
            resp[1] = document.getElementById('preg2_c').checked;
            resp[2] = document.getElementById('preg3_a').checked;
            resp[3] = document.getElementById('preg4_a').checked;
            resp[4] = document.getElementById('preg5_b').checked;
            resp[5] = document.getElementById('preg6_a').checked;
            resp[6] = document.getElementById('preg7_b').checked;
            resp[7] = document.getElementById('preg8_b').checked;
            resp[8] = document.getElementById('preg9_a').checked;
            resp[9] = document.getElementById('preg10_c').checked;
            resp[10] = document.getElementById('preg11_b').checked;
            resp[11] = document.getElementById('preg12_a').checked;
            resp[12] = document.getElementById('preg13_a').checked;
            resp[13] = document.getElementById('preg14_c').checked;
            resp[14] = document.getElementById('preg15_c').checked;
            resp[15] = document.getElementById('preg16_c').checked;

            for (let i=0;i<resp.length;i++)
                if (resp[i])
                  score++;

            score = score/16*10;

        if (score >= 9 && score <= 10) {
                alert(score + "/10 " + "Muy bien, prueba a superarlo");
                }
        if (score >= 7 && score < 8) {
                alert(score + "/10 " + "Bien, pero puedes hacerlo mejor");
                }
        if (score >= 5 && score < 6) {
                alert(score + "/10 " + "Aprobado por los pelos. No te fíes");
                }
        if (score >= 3 && score < 4) {
                alert(score + "/10 " + "Insuficiente. Has de estudiar más");
                }
       if (score < 2) {
                alert("Su puntuación es: "+ score
                +"\nLa puntuación máxima que podía obtener es 10"
                +"\nTiene que reviazar nuevamente sus lecciones"
                +"\nSu porcentaje de aciertos es menos del 10%");
            }
        }
        </script>
    </head>

    <body>

        <header>
        <nav id="nav">
            <img src="logo_ks_edited.png" class="img_logo">

            <ul>
                <li><a data-page="about" href="form.html">Contacto</a></li>
                <li><a href="foro.html">Foro</a></li>
                <li><a data-page="formacion" href="formacion.html">Formación</a></li>
                <li><a data-page="home" href="index.html">Inicio</a></li>

            </ul>

        </nav>
        </header>

        <br>
        <div class="pregresp">
        <div class="pregunta">1. ¿Qué es la función hash?<br/>
        </div>
        <div class="respuestas">
        <input id="preg1_a" type="radio" name="preg1" value="a" /> a. Es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de
        caracteres con una longitud fija <br />
        <input id="preg1_b" type="radio" name="preg1" value="b" /> b. Es un programa que sirve para ocultar detalles de los documentos <br />
        <input id="preg1_c" type="radio" name="preg1" value="c" /> c. Se trata de una librería que sirve para cifrar cualquier bloque arbitrario de datos<br />
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">2. ¿Qué protocolo de red crees que es más seguro?<br/>
        </div>
        <div class="respuestas">
        <input id="preg2_a" type="radio" name="preg2" value="a"/> a. HTTP<br/>
        <input id="preg2_b" type="radio" name="preg2" value="b"/> b. Ninguno<br/>
        <input id="preg2_c" type="radio" name="preg2" value="c"/> c. HTTPS<br/>
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">3. ¿Qué es una Inyección SQL?<br/>
        </div>
```

```
        <div class="respuestas">
        <input id="preg3_a" type="radio" name="preg3" value="a"/> a. Es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar operaciones sobre una base de datos<br/>
        <input id="preg3_b" type="radio" name="preg3" value="b"/> b. Código malicioso que se inyecta en la capa del cliente sobre una aplicación<br/>
        <input id="preg3_c" type="radio" name="preg3" value="c"/> c. Ninguna es correcta<br/>
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">4. ¿Es importante tener el WPS del router desactivado?<br/>
        </div>
        <div class="respuestas">
        <input id="preg4_a" type="radio" name="preg4" value="a"/> a. Sí, debido a que cualquiera puede acceder a nuestro WiFi si lo tenenmos activado<br/>
        <input id="preg4_b" type="radio" name="preg4" value="b"/> b. No, es indiferente<br />
        <input id="preg4_c" type="radio" name="preg4" value="c"/> c. Solo en algunas ocasiones<br/>
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">5. ¿En que consiste un ataque de fuerza bruta?<br/>
        </div>
        <div class="respuestas">
        <input id="preg5_a" type="radio" name="preg5" value="a"/> a. Forzar al ordenador, abriendo y cerrando procesos en el sistema<br/>
        <input id="preg5_b" type="radio" name="preg5" value="b"/> b. Probar todas las posibles combinaciones hasta encontrar aquella que permite el acceso <br/>
        <input id="preg5_c" type="radio" name="preg5" value="c"/> c. Probar todas las posibles combinaciones posibles hasta que el ordenador se caliente<br/>
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">6. ¿Son seguras las redes públicas?<br/>
        </div>
        <div class="respuestas">
        <input id="preg6_a" type="radio" name="preg6" value="a"/> a. Bajo ningún concepto<br/>
        <input id="preg6_b" type="radio" name="preg6" value="b" /> b. Sí<br/>
        <input id="preg6_c" type="radio" name="preg6" value="c" /> c. Depende del establecimiento<br/>
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">7. Cuando introducimos nuestros datos, por ejemplo para hacer un login, ¿Qué es lo que "viaja" por la red?<br/>
        </div>
        <div class="respuestas">
        <input id="preg7_a" type="radio" name="preg7" value="a"/> a. Las credenciales llegan al administrador y éste decide si dar paso o no<br/>
        <input id="preg7_b" type="radio" name="preg7" value="b"/> b. Paquetes de red, que contienen dicha información<br/>
        <input id="preg7_c" type="radio" name="preg7" value="c"/> c. No "viaja" nada en la red<br/>
        </div>
        </div>

        <br>
        <div class="pregresp">
        <div class="pregunta">8. ¿Qué es un script? <br/>
        </div>
        <div class="respuestas">
        <input id="preg8_a" type="radio" name="preg8" value="a"/> a. Un guión con comandos sólo para desahibilitar webs<br/>
        <input id="preg8_b" type="radio" name="preg8" value="b"/> b. Secuencia de comandos que se utiliza para manipular, personalizar y automatizar las instalaciones de un sistema existente<br/>
        <input id="preg8_c" type="radio" name="preg8" value="c"/> c. Secuencia de programas ejecutándose en segundo plano<br/>
        </div>
        </div>

        <!-- Pregunta 9 -->
        <br>
        <div class="pregresp">
        <div class="pregunta">9. ¿Qué es la autenticación de 2 factores?<br/>
        </div>
        <div class="respuestas">
        <input id="preg9_a" type="radio"  name="preg9" value="a"/> a. La Autenticación de Dos Factores es una herramienta que ofrecen varios proveedores se servicio en línea, que cumple la función de agregar una capa de seguridad adicional al proceso de inicio de sesión de tus cuentas de Internet<br/>
        <input id="preg9_b" type="radio" name="preg9" value="b"/> b. Se trata de iniciar sesión 2 veces <br/>
        <input id="preg9_c" type="radio" name="preg9" value="c"/> c. Ninguna de la anteriores<br/>
        </div>
        </div>

        <!-- Pregunta 10 -->
        <br>
        <div class="pregresp">
        <div class="pregunta">10. ¿Qué pasa si no actualizo el sistema operativo?<br/>
        </div>
        <div class="respuestas">
        <input id="preg10_a" type="radio" name="preg10" value="a"/> a. Iría mas lento el ordenador y consumiría más recursos <br/>
        <input id="preg10_b" type="radio" name="preg10" value="b"/> b. No pasa nada<br/>
        <input id="preg10_c" type="radio" name="preg10" value="c"/> c. Si no actualizas el sistema operativo de tu ordenador queda expuesta a fallas y vulnerabilidades de seguridad que facilitan el robo de información personal y la invasión de privacidad.<br/>
        </div>
        </div>


        <!-- Pregunta 11 -->
        <br>
        <div class="pregresp">
        <div class="pregunta">11. ¿Qué es un firewall?<br/>
        </div>
        <div class="respuestas">
        <input id="preg11_a" type="radio" name="preg11" value="a"/> a. Protege la red Wi-Fi solamente <br/>
        <input id="preg11_b" type="radio" name="preg11" value="b"/> b. Un firewall es un dispositivo de seguridad de la red que monitoriza el tráfico entrante y saliente y decide si debe permitir o bloquear un tráfico específico en función de un conjunto de restricciones de seguridad ya definidas<br/>
        <input id="preg11_c" type="radio" name="preg11" value="c"/> c. Es una barrera que hay en el sistema para parar procesos<br/>
        </div>
        </div>


        <!-- Pregunta 12 -->
        <br>
        <div class="pregresp">
        <div class="pregunta">12. ¿Qué es la ingeniería social?<br/>
        </div>
        <div class="respuestas">
        <input id="preg12_a" type="radio" name="preg12" value="a"/> a. Manipula a las personas para que compartan información que no deberían compartir, descarguen software
```

```
        que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delicuentes o bien cometan otro errores que comprometan sus activos o seguridad
        personal o empresarial<br/>
219     <input id="preg12_b" type="radio" name="preg12" value="b"/> b. Un tipo de ingeniería que afecta a lo social<br/>
220     <input id="preg12_c" type="radio" name="preg12" value="c"/> c. Una rama de la ingeniería que se encarga de explicar los razonamientos sociales<br/>
221     </div>
222     </div>
223
224
225     <!-- Pregunta 13 -->
226     <br>
227     <div class="pregresp">
228     <div class="pregunta">13. ¿Qué es el cifrado extremo a extremo?<br/>
229     </div>
230     <div class="respuestas">
231     <input id="preg13_a" type="radio" name="preg13" value="a"/> a. Para el caso de WhatsApp cuando chateas con otra persona a través de WhatsApp Messenger. Este cifrado
        garantiza que solo tú y la persona con quien te comuniques puedan leer o escuchar lo que se envía, y que nadie más, ni siquiera WhatsApp, pueda hacerlo<br/>
232     <input id="preg13_b" type="radio" name="preg13" value="b"/> b. Cifra el número de móvil para que solo tus amigos te puedan ver<br/>
233     <input id="preg13_c" type="radio" name="preg13" value="c"/> c. Ninguna de las anteriores<br/>
234     </div>
235     </div>
236
237
238     <!-- Pregunta 14 -->
239     <br>
240     <div class="pregresp">
241     <div class="pregunta">14. ¿Qué es el phishing por correo electrónico?<br/>
242     </div>
243     <div class="respuestas">
244     <input id="preg14_a" type="radio" name="preg14" value="a"/> a. Un ajuste en nuestro servicio de correo electrónico<br/>
245     <input id="preg14_b" type="radio" name="preg14" value="b"/> b. Una forma de enviar correos más seguros<br/>
246     <input id="preg14_c" type="radio" name="preg14" value="c"/> c. El phishing por correo electrónico es una forma común de ataque cibernético en la cual los delincuentes
        envían correos electrónicos falsificados que parecen provenir de una fuente legítima, como una institución financiera, una empresa reconocida o un servicio en línea
        popular<br/>
247     </div>
248     </div>
249
250
251     <!-- Pregunta 15 -->
252     <br>
253     <div class="pregresp">
254     <div class="pregunta">15. ¿Qué es el malware?<br/>
255     </div>
256     <div class="respuestas">
257     <input id="preg15_a" type="radio" name="preg15" value="a"/> a. Una configuración estándar que tienen todos los ordenadores actuales<br/>
258     <input id="preg15_b" type="radio" name="preg15" value="b"/> b. Un software que solamente monitoriza el sistema<br/>
259     <input id="preg15_c" type="radio" name="preg15" value="c"/> c. El malware, hace referencia a cualquier tipo de software maligno que trata de afecta a un ordenador,
        móvil u otro dispositivo electrónico, es un software hostil, intrusivo o molesto<br/>
260     </div>
261     </div>
262
263
264
265     <!-- Pregunta 16 -->
266     <br>
267     <div class="pregresp">
268     <div class="pregunta">16. ¿Cuál de los siguientes no es un algoritmo de cifrado?<br/>
269     </div>
270     <div class="respuestas">
271     <input id="preg16_a" type="radio" name="preg16" value="a"/> a. Triple DES<br/>
272     <input id="preg16_b" type="radio" name="preg16" value="b"/> b. AES-256<br/>
273     <input id="preg16_c" type="radio" name="preg16" value="c"/> c. SHA-256<br/>
274     </div>
275     </div>
276
277
278
279
280
281
282
283     <input name=Resulta onClick=Nivel() type=button value=Resultados>
284     <input type="reset" onclick=Borrar() value="Borrar resultados" name="reset">
285     <a href="index.html"> Inicio </a>
286     <br>
287     <br>
288     <br>
289     <br>
290     <br>
291     <br>
292     <div class="footer">
293
294         <p>© Karan Sainani 2023</p>
295         <p> Made with &#128154 in Canary Islands </p>
296     </div>
297
298 </body>
299 <br>
300
301
302 </html>
```

II. Anexo del foro.

Karan: Bienvenidos a mi página web. Aquí podrás practicar tus conocimientos en ciberseguridad.

Patricia: ¡Hola! Quería Información sobre la página web.

Juan: Yo también quería información.