uc3m | Universidad Carlos III de Madrid

Grado Universitario en Ingeniería Telemática
2017-2018

Trabajo Fin de Grado

"Cybersecurity Sorting Hat: Ampliación de funcionalidades de análisis y desarrollo de interfaz de usuario avanzada 2"

Javier Sanz López

Tutora

Ana Isabel González-Tablas Ferreres

Madrid, 2018

RESUMEN

El propósito del documento presentado a continuación consiste en presentar a los lectores las características del proyecto Cybersecurity Sorting Hat. Este proyecto consiste en una aplicación web, cuya funcionalidad principal es la de definir un perfil concreto del usuario dentro del área de la ciberseguridad. Los principales usuarios potenciales de esta aplicación son los alumnos del Máster de Ciberseguridad de la Carlos III, aunque se contempla la posibilidad de que en un futuro esta aplicación sea de utilidad para otro tipo de usuarios.

En el sector de la ciberseguridad, se considera la clasificación de los profesionales que desempeñan su trabajo en este campo bajo unos marcos muy concretos una necesidad primordial. Debido a esto, se crearon diferentes marcos, los cuales definen y nombran cada uno de los roles o perfiles que se pueden encontrar en un proyecto que esté relacionado con la ciberseguridad.

El siguiente Trabajo de Fin de Grado consiste en la prolongación, mejora e inclusión de nuevas funcionalidades sobre el Trabajo de Fin de Máster realizado por un antiguo alumno de la Universidad Carlos III de Madrid. El desarrollo de este Trabajo de Fin de Grado se ha realizado respetando la funcionalidad de la aplicación sobre la que está basado, a la vez que añadiendo funcionalidades, algunas más básicas y otras más avanzadas, de las que el proyecto inicial carecía.

El siguiente documento analiza el proceso necesario para el correcto progreso de este proyecto, en términos de planificación, documentación, planteamiento y el desarrollo de las funcionalidades incorporadas en la aplicación, junto a la relevancia que dichas mejoras producen en una aplicación de estas características.

PALABRAS CLAVE

- TFG: Trabajo Fin de Grado.
- TFM: Trabajo Fin de Máster.
- NICE: National Initiative for Cybersecurity Education.
- NIST: National Institute of Standards and Technology.
- NCWF: NICE Cybersecurity Workforce Framework.
- TKSAs: Knowledges, Skills, Abilities and Tasks.
- IISP: Institute of Information Security Professionals.
- PHP: Hypertext Preprocessor.
- MVC: Modelo-Vista-Controlador.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ACLARACIONES PREVIAS SOBRE EL TRABAJO

Como requisito previo a la exposición del proyecto desarrollado, es conveniente exponer los antecedentes de este. Este TFG se corresponde a la continuación y ampliación del TFM de Javier Vila, un alumno del Máster de Ciberseguridad de la Universidad Carlos III de Madrid, el cual lo presentó bajo el título de: "Cyber Range Systems: A Cybersecurity Sorting Hat".

La aplicación web desarrollada en este proyecto es de gran tamaño y con amplia variedad de funcionalidades, lo cual provoca que el trabajo no pueda ser terminado en su totalidad en un solo TFM. Por lo tanto, en este Trabajo de Fin de Grado se trabaja para dotar a la aplicación original de las funcionalidades que restan para poder ser considerada como una aplicación web completa. Dado el gran número de funcionalidades que el cliente deseaba añadir a la aplicación original ha sido posible realizar un trabajo de forma paralela a otra compañera de la facultad, Sandra Sánchez Esperante.

Cada alumno ha sido encargado del desarrollo y creación de distintas funcionalidades y partes de la aplicación, pero el núcleo y la temática es compartida, y esto provoca una complementariedad que se puede ver en ambos TFGs.

El proyecto de mi compañera se presentó en junio de 2018, pero por circunstancias personales, la parte que se me ha encargado será presentada en la siguiente convocatoria.

1. INTRODUCCIÓN

Este capítulo contiene una introducción del proyecto y detalla cuales han sido los motivos para la elección de este. Asimismo, se exponen las principales funcionalidades y características de la aplicación. En el último capítulo de este punto, se realiza una breve descripción de la estructura que sigue el presente documento.

1.1. Motivaciones para la realización del trabajo.

Actualmente, vivimos en una sociedad que tiene una necesidad vital de estar conectada. Esta necesidad ha sido impulsada, de forma principal, por la facilidad al acceso de internet gracias a los llamados "teléfonos móviles inteligentes" o "smartphones". Hace unos años, la única manera de disfrutar de las posibilidades que nos ofrecía internet era a través de un ordenador, pero ahora, gracias a nuestros dispositivos móviles, tenemos acceso a internet desde cualquier lugar a unas velocidades que se creían imposibles hace tan sólo unos años.

Los estudios indican que el tráfico de IP aumenta con un ritmo anual medio de un 24%, pudiendo llegar a los 3,3 Zettabytes (2^{70} bytes) en 2021 [1], y que el mismo año existirán 12 miles de millones de dispositivos capaces de realizar conexiones móviles a internet [2].

Debido al exponencial crecimiento de las conexiones a internet, se ha producido también un enorme aumento de los ataques informáticos. Los denominados ciberataques son maniobras que atacan a usuarios particulares de internet o empresas, para intentar causar algún tipo de robo de información sensible o de malfuncionamiento. En España, en 2017 se produjeron 120.000 ciberataques [3] de distinta importancia, lo que supone un aumento del 140%. Algunos de los más conocidos a nivel mundial fueron el virus WannaCry o las filtraciones de Shadow Brokers [4].

Estos preocupantes datos han provocado que el sector de la ciberseguridad se convierta en vital, tanto como para particulares que desean sentirse protegidos en Internet, como para compañías, las cuales desean proteger la información sensible de la que disponen, de ataques maliciosos.

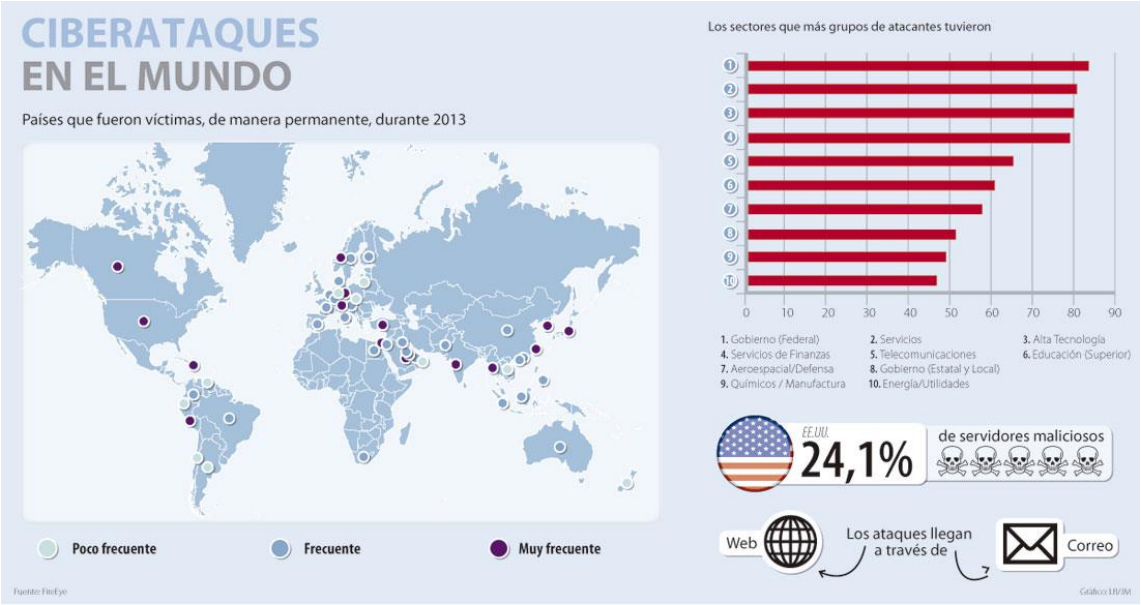


Figura 1.1: Mapa de los ciberataques en el mundo, y por sectores. [5]

La gran mayoría de las empresas no dispone de recursos suficientes para garantizar esta seguridad, y por lo tanto el incremento en la inversión en ciberseguridad se ha disparado en los últimos años. Según los últimos datos, las empresas de nuestro país destinan un 22% de media de su presupuesto en la ciberseguridad. [6]

A la vista de estos datos, se puede deducir que la educación de los profesionales o futuros profesionales del sector cobra una enorme importancia. Las empresas del sector precisan de personal experto en una materia en concreto, por lo que determinar el perfil más adecuado para los profesionales o estudiantes cobra una mayor trascendencia, sobre todo con el fin de aumentar su empleabilidad en las empresas del sector.

Con el objetivo de facilitar esta tarea se crea la organización propuesta por NICE Cybersecurity Workforce Framework (NCWF), la cual será usada en el proyecto. Esta clasificación se compone de 7 categorías, las cuales incluyen 33 áreas de especialización y 52 perfiles distintos, definidos por los conocimientos y habilidades necesarias para el correcto desempeño de las funciones requeridas por dicho perfil.

El proyecto descrito en este documento se apoya en estos recursos para construir un portal web funcional para encontrar perfiles de ciberseguridad adecuados para el usuario.

Cabe destacar el término “funcional” ya que el objetivo principal del mismo consiste en convertir al proyecto base, el cual tenía grandes deficiencias, en un portal web que pueda ser de utilidad para los usuarios que precisen de una herramienta de estas características. Se le ha dotado de nuevas funcionalidades de las que carecía y se han añadido tablas y nuevas vistas para dotarlo de una usabilidad de la que carecía.

1.2. Objetivos del proyecto.

La finalidad de este Trabajo de Fin de Grado es la de ayudar a los profesionales o futuros profesionales del sector de la ciberseguridad a encontrar el perfil que más se adecúa a sus conocimientos y habilidades personales, y a su vez, a identificar los aspectos a mejorar con el objetivo de fomentar la empleabilidad de dichos profesionales.

Con el objetivo de cumplir la funcionalidad para la que está pensada la aplicación, se deben de cumplir los siguientes requisitos:

- Creación de bases de datos de usuarios, con protección de las contraseñas mediante encriptación, con el objetivo de proteger la información de posibles ataques de inyección SQL.

- Inclusión de un middleware encargado de coordinar la comunicación entre las vistas y la base de datos.

- Autenticación de los usuarios de forma segura, utilizando los recursos del middleware para gestionar las funciones de mantenimiento de sesión de forma segura.

- Creación de nuevas vistas que correspondan con las funcionalidades añadidas al proyecto original (Perfil de usuario, edición de dicho perfil y adición de certificaciones en la base de datos).

- Creación de modelos que se correspondan con los objetos con los que vamos a tratar en la aplicación (Usuarios, Certificaciones, Roles de Trabajo…).

- Utilización de los recursos proporcionados por el TFG desarrollado en paralelo a este por Sandra Sánchez Esperante, y búsqueda de la cohesión entre los dos proyectos para el resultado final.

- Adaptación de las funcionalidades desarrolladas en el proyecto inicial desarrollado por Javier Vila en la plataforma mejorada, la cual se desarrolla en este TFG y el de la compañera Sandra Sánchez, con el fin de crear una plataforma web funcional.

1.3. Estructura del documento.

El propósito del siguiente apartado es exponer brevemente, las partes en las que se divide el presente documento.

- Introducción y objetivos: En este capítulo se describe la situación del mercado empresarial actual, en el que la seguridad en internet ha cobrado una importancia vital, y por tanto las empresas invierten cada vez más en profesionales de esta área. Asimismo, se explica cuál es el papel de la aplicación aquí propuesta en el mercado y de qué forma puede ser útil para las empresas o los profesionales del sector.

- Estado de la cuestión: Este capítulo tiene como objetivo principal explorar los detalles técnicos. Esto se consigue a través de la comparación de la aplicación desarrollada para este TFG con otras aplicaciones de características similares que podemos encontrar en otros países. Por otra parte, se detallan las razones por las cuales se ha elegido el marco del NICE Cybersecurity Workforce Framework, y los perfiles de ciberseguridad que este define.

- Diseño y desarrollo software: Los siguientes capítulos son los encargados de explicar detalladamente la arquitectura y el diseño de la solución técnica propuesta para este proyecto. Indica las modificaciones que han sido incluidas sobre el proyecto original y la manera de llevarlas a cabo desde un punto de vista técnico.

- Planificación y presupuesto: Este capítulo es de gran importancia ya que detalla la gestión tanto del tiempo como de los recursos disponibles para el proyecto. En él encontramos la planificación detallada que se ha seguido para la realización de este proyecto y también una estimación aproximada del presupuesto del proyecto.

- Marco regulador: Consiste en un análisis de la legislación vigente en Europa y en España que esté relacionada con la materia de la que trata el proyecto y pueda afectarlo en mayor o menor medida.

- Conclusiones: Este capítulo resume las conclusiones a las que se llega una vez terminado el proyecto. Se analiza si se han cumplido los objetivos marcados al comienzo de la planificación del mismo y se estudian posibles líneas futuras de modificación y ampliación del proyecto.

2. ESTADO DE LA CUESTIÓN

2.1. Situación actual.

Debido al intenso auge de la ciberseguridad, la búsqueda de perfiles concretos dentro del sector se convierte en una tarea imprescindible. Es por ello que existen varias aplicaciones que realizan operaciones de carácter similar a la desarrollada en este proyecto, aunque cada una de ellas posee unas características distintas.

En los siguientes apartados se expondrán las características propias de cada una de estas aplicaciones, y las diferencias que existen entre ellas y con la desarrollada en este Trabajo de Fin de Grado.

2.1.1. National Initiative for Cybersecurity Careers and Studies (NICCS)

El NICCS [7] es un portal gubernamental de los Estados Unidos, en concreto del departamento de Seguridad Nacional (Homeland Security). Es considerado como el portal referente en el estudio de la ciberseguridad.

Está orientado a empleados del Gobierno, estudiantes, educadores o profesionales del área de ciberseguridad en dicho país. Su objetivo principal es el de proveer a los perfiles descritos anteriormente con las herramientas adecuadas para adquirir los conocimientos necesarios en ciberseguridad para crecer en sus carreras profesionales, y para eliminar las grandes diferencias de conocimiento que aparecen en los diferentes perfiles.

Para lograr este objetivo, NICCS ofrece varias aplicaciones que detallamos en los puntos siguientes, todas ellas basadas en el marco NICE Workforce, el mismo que ha sido utilizado para el desarrollo de este proyecto.

DHS PushButtonPD™ Tool: [8] Es una herramienta de gratuita y de uso fácil, en la forma de una hoja de Excel. Su principal cometido es el de ayudar a directivos, managers o representantes de RRHH para definir vacantes para posiciones y para ayudar a los candidatos a decidir si están o no cualificados para un puesto.

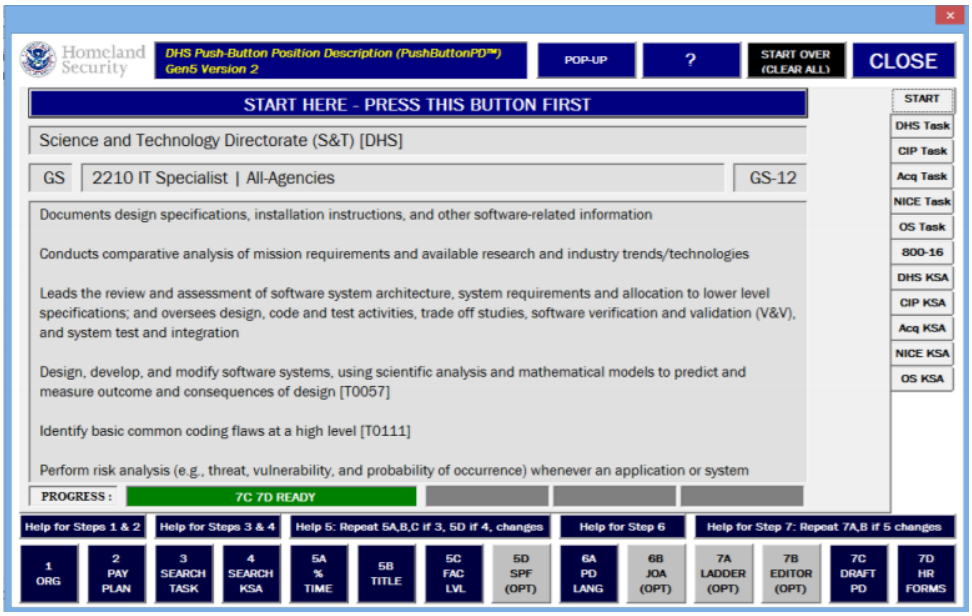


Figura 2.1: DHS PushButtonPd™ Tool [9]

Mapping Tool: [10] Esta herramienta permite a los managers y encargados de recursos humanos encontrar información acerca de los perfiles de ciberseguridad para decidir qué relación tienen sus equipos de trabajo con el marco establecido por el NCWF.

2.1.2 Institute of Information Security Professionals (IISP)

Este organismo sin ánimo de lucro y afincado en Londres fue creado en el año 2006 por profesionales del área de la ciberseguridad.

En su portal web podemos encontrar una aplicación que realiza una función similar a la desarrollada en este proyecto, pero con ciertas diferencias. La aplicación contenida en este portal no sigue el marco definido por el NCFW, ya que tiene uno propio llamado IISP Skills Framework [11].

La web ofrece otros servicios adicionales, como la oferta de puestos de trabajo en el área de la ciberseguridad. Cabe destacar, por último, que es necesario contar con una membresía para acceder a la funcionalidad completa de la aplicación.

2.1.3 Cyberseek.org

Este portal tiene el objetivo de proveer de información útil sobre la oferta y la demanda de trabajos en el área de ciberseguridad, con el objetivo de disminuir la brecha de aptitudes que existe actualmente en la sociedad americana, en la cual la demanda de puestos de trabajo supera en gran medida a la oferta de trabajadores disponibles que cuenten con los conocimientos necesarios para desempeñar dichas funciones [12].

La aplicación cuenta con dos herramientas principales, las cuales explicamos a continuación.

Mapa Interactivo: Esta sección ofrece un gran número de estadísticas sobre ofertas de trabajo de ciberseguridad, ordenadas en un mapa que divide dichas estadísticas por estados. Se puede recorrer el mapa y descubrir los datos de cada estado.

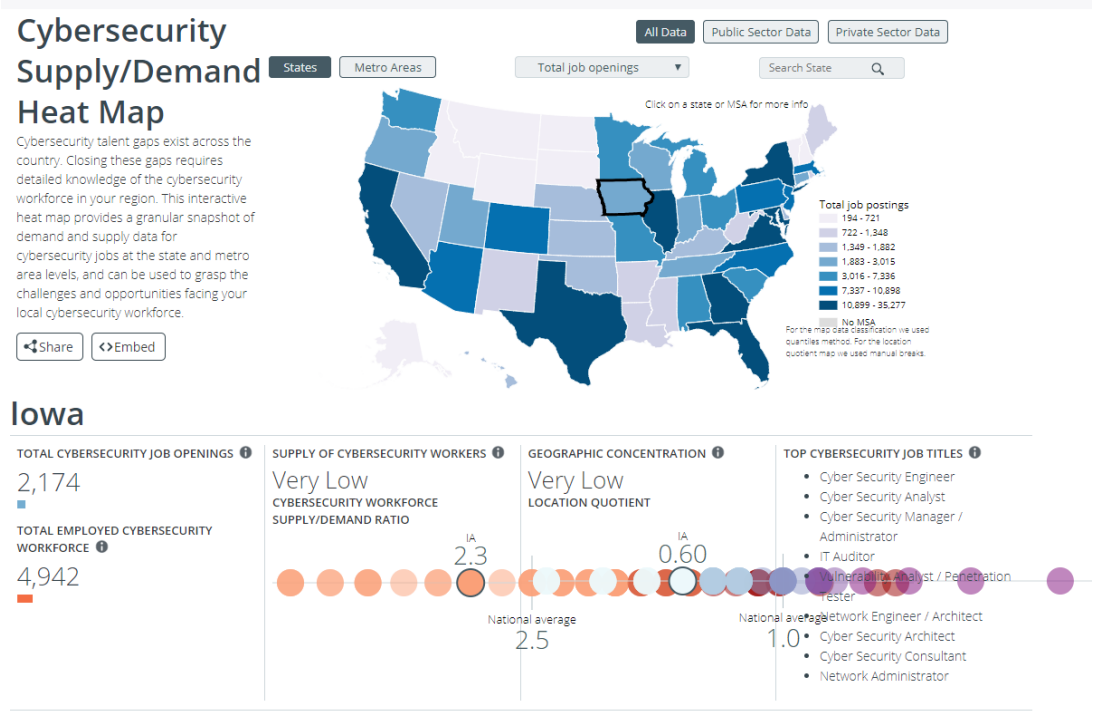


Figura 2.2: Mapa Interactivo [13]

Trayectoria Profesional: Dado que hay tantas oportunidades para los trabajadores para empezar o avanzar en sus carreras en la ciberseguridad, esta aplicación ofrece un camino profesional interactivo que muestra puestos de trabajo, de una forma similar a la del NCWF, y muestra oportunidades de transición comunes entre ellos, además de información detallada acerca de salarios, credenciales y habilidades necesarias asociadas a cada rol.

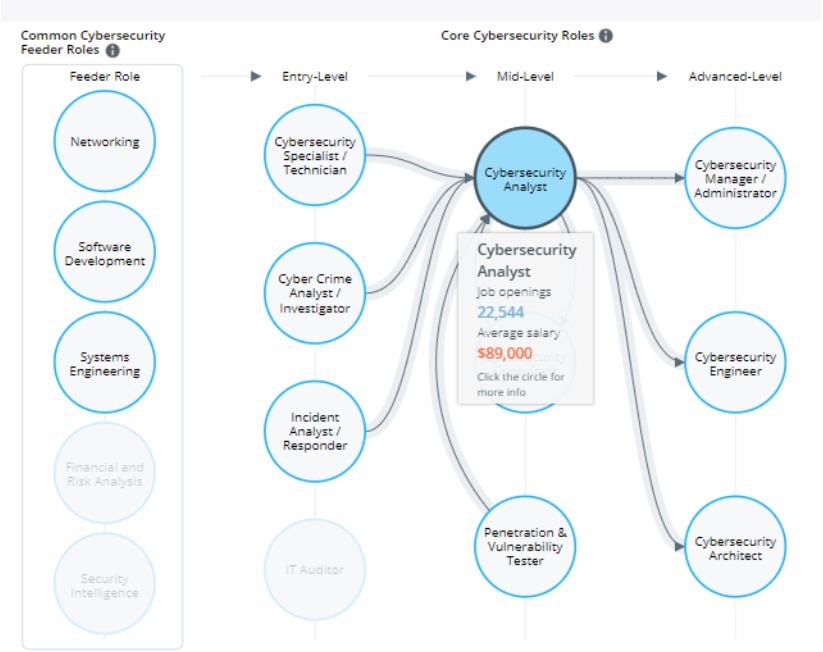


Figura 2.3: Trayectoria Profesional [14]

2.2. Marco actual.

En la siguiente sección se definen los marcos existentes en la actualidad y algunos planes de futuro, comparándolos entre ellos. Asimismo, se indican las razones por las que el marco escogido para nuestro proyecto ha sido el denominado como NCWF.

2.2.1. NICE Cybersecurity Workforce Framework (NCWF)

El marco NCWF es un recurso nacional que categoriza y describe trabajos de ciberseguridad [15]. Es en el que están basados la mayoría de las herramientas descritas anteriormente.

Este marco describe la ordenación que describe a los trabajos y trabajadores del área de ciberseguridad, sin importar dónde o para quien se realice el trabajo. El marco se puede aplicar en todos los sectores: público, privado y académico.

El marco NICE se compone de los siguientes componentes:

- 7 Categorías – Agrupaciones de funciones comunes de ciberseguridad
- 33 Áreas de especialidad – Distintas áreas de trabajo de ciberseguridad
- 52 Roles de trabajo – Agrupaciones más detalladas de trabajo. Se componen de: Tareas (Tasks), Habilidades (Skills), Habilidades (Abilities) y Conocimientos (Knowledges).

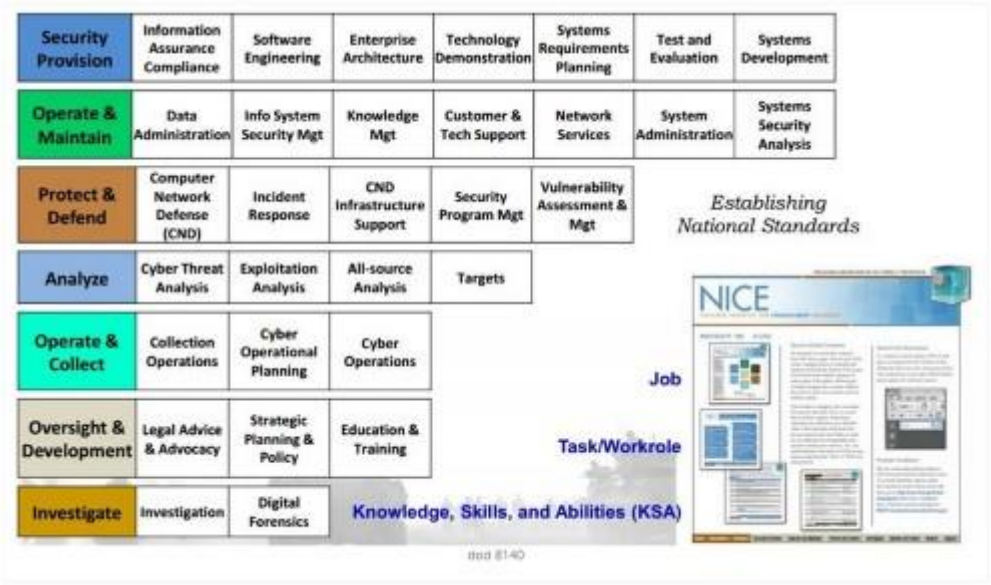


Figura 2.4. Categorías y Áreas de especialidad del NICE Cybersecurity Workforce Framework [15]

El documento que define este marco expone todos los componentes de los que se forma, además de las relaciones que existen entre cada uno de ellos de forma detallada. A continuación, se presentan ejemplos de tablas para los cuatro tipos de componentes para poder apreciar las características y relaciones de cada una de ellas. Se han traducido al castellano para facilitar la lectura de estas.

TABLA 2.1- TABLA DE ÁREA DE ESPECIALIDAD DEL NCWF

Categorías	**Área de especialidad**	**Descripción de Área de especialidad**
Recoger y operar (CO)	Operación de recolección (CL)	Ejecuta la colección usando estrategias apropiadas dentro de las prioridades establecidas durante el proceso de administración.
	Planificación Operacional Cibernética (PL)	Realiza funciones conjuntas de focalización y planificación. Reúne información y desarrolla planes operacionales y de apoyo de órdenes. Dirige planes a nivel estratégico y operacional para todo el rango de información y operaciones.
	Operaciones Cibernéticas (OP)	Realiza actividades para reunir pruebas de entidades criminales, para mitigar amenazas posibles o a tiempo real. Además de protección anti-espionaje o sabotaje internacional.

Además, recoge tablas más detalladas en las que se puede ver con más claridad las relaciones existentes entre las categorías y los roles de trabajo que podemos encontrar en dichas categorías. A continuación, se muestra parte de la tabla para la categoría de la tabla anterior:

TABLA 2.2. ROLES DE TRABAJO DEL NWFC [15]

Categorías	**Áreas de especialidad**	**Grupos de trabajo**	**NCWF ID**	**Descripción de grupo de trabajo**
Collect and Operate (CO)	Operaciones Cibernéticas (OP)	Ciber Operador	CO-OP-001	Maneja la recogida y procesamiento de sistemas para localizar o explotar objetivos. Realiza navegación de red y análisis táctico forense.
	Operación de recolección (CL)	Mánager de recopilación	CO-CL-001	Identifica autoridades de recogida y entornos. Determina las capacidades de los activos disponibles, identifica nuevas capacidades de la colección, y construye nuevos planes de diseminación.
		Manager de requerimientos de recopilación	CO-CL-002	Evalúa grupos de operaciones y desarrolla estrategias de requerimientos basadas en los efectos. Desarrolla, procesa, valida y coordina el envío de requerimientos.

Dichos componentes serán los utilizados en nuestra aplicación para formar un perfil de ciberseguridad del usuario. Estos roles de trabajo se componen de una gran variedad de TKSA's. La siguiente tabla recoge de forma muy detallada todos los TKSA's para un determinado grupo de trabajo, incluido en la categoría definida en tablas anteriores.

TABLA 2.3. NCWF WORKROLES DESCRIPTION [15]

ID Grupo de trabajo	CO-CL-001
Categoría	**Recoger y operar (CO)**
Área de especialidad	Operación de recolección (CL)
Nombre del grupo de trabajo	Mánager de recopilación (311)
Descripción del grupo de trabajo	Identifica autoridades de recogida y entornos. Determina las capacidades de los activos disponibles, identifica nuevas capacidades de la colección, y construye nuevos planes de diseminación.
Tasks	T0562, T0564, T0568, T0573, T0578, T0604, T0605, T0625, T0626, T0631, T0632, T0634, T0645, T0646, T0647, T0649, T0651, T0657, T0662, T0674, T0681, T0683, T0698, T0702, T0714, T0716, T0721, T0723, T0725, T0734, T0737, T0750, T0753, T0755, T0757, T0773, T0779, T0806, T0809, T0810, T0811, T0812, T0814, T0820, T0821, T0827
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0431, K0449, K0417, K0579, K0596, K0369, K0444, K0471, K0392, K0395, K0440, K0445, K0516, K0560, K0427, K0446, K0561, K0565, K0405, K0480, K0610, K0612, K0353, K0361, K0364, K0366, K0380, K0382, K0383, K0386, K0387, K0390, K0401, K0404, K0412, K0419, K0425, K0435, K0448, K0453, K0454, K0467, K0474, K0475, K0477, K0482, K0492, K0495, K0496, K0498, K0503, K0505, K0513, K0521, K0522, K0526, K0527, K0552, K0553, K0554, K0558, K0562, K0563, K0569, K0570, K0580, K0581, K0583, K0584, K0587, K0588, K0601, K0605, K0613
Skills	S0238, S0304, S0305, S0311, S0313, S0316, S0317, S0324, S0325, S0327, S0328, S0330, S0332, S0334, S0335, S0336, S0339, S0342, S0344, S0347, S0351, S0352
Abilities	A0069, A0070, A0076, A0078, A0079

2.2.2. IISP Skills Framework

El marco de destrezas del IISP define las capacidades que deberían poseer los expertos en el campo de la Seguridad y Garantía de la información en internet, para un correcto desempeño de sus funciones en el trabajo. Se desarrolló a través de la colaboración entre organizaciones de los sectores público y privado y líderes académicos mundiales en materia de seguridad.

Define las destrezas y las capacidades que se esperan de los profesionales de la ciberseguridad en la práctica, y no es solamente una evaluación de sus conocimientos. No todos los roles requieren experiencia precisa en todas las áreas de competencia [16].

2.2.3. European Cybersecurity Act

La Unión Europea pretende mejorar su capacidad de adaptación a través de la creación de un marco de certificaciones para productos, servicios y procesos de tecnologías de la información y comunicación a nivel europeo. Esta propuesta será encargada a ENISA (European Union Agency for Network and Information Security), la cual pasará a ser la agencia permanente de ciberseguridad de la unión [17].

El borrador de la regulación esboza un mecanismo para la implantación de unas certificaciones de ciberseguridad europeas, que se pueden entregar a productos, procesos o servicios IT específicos. La novedad es que estos certificados tendrán validez en todo el territorio comunitario, lo que provoca que los usuarios tengan más facilidades para desarrollar sus proyectos fuera de sus fronteras. Se podrán conseguir de forma voluntaria en cualquier país miembro de la unión.

A continuación, se muestra un gráfico de la estructura de aprobación de los cursos por los organismos reguladores de la unión. Las certificaciones aún no tienen un esqueleto definido, debido a que se trata de un proyecto activo hoy en día.

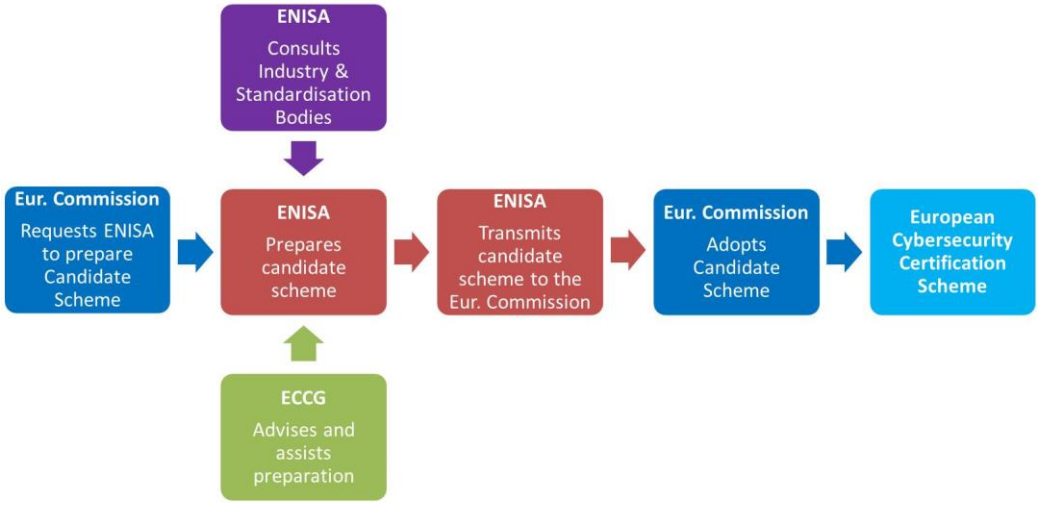


Figura 2.5. Estructura de la gestión europea del futuro marco de certificaciones de ciberseguridad [17]

2.3. Diseño de soluciones.

Como se ha podido ver en los apartados anteriores, existen varias aplicaciones que realizan funciones similares, pero la mayoría de ellas están pensadas para usuarios muy concretos, y no para estudiantes del área de ciberseguridad.

Esta aplicación será de gran valor para diferentes perfiles, ya que puede ser de utilidad para estudiantes, trabajadores y empresas del área de la ciberseguridad. Además, la decisión de elegir el marco NCWF como el utilizado en la aplicación fomenta que el radio de posibles usuarios se amplíe, al ser el marco más común y más utilizado mundialmente en el sector. El usuario al que está destinada la aplicación desarrollada en este proyecto se centra sobre todo en alumnos del Master de Ciberseguridad de la Universidad Carlos III, aunque es posible que se extienda a estudiantes de carreras similares en otras universidades.

3. DISEÑO TÉCNICO Y ANÁLISIS

En el siguiente capítulo se realiza un análisis de la solución técnica elegida para desarrollar este proyecto. Acto seguido, se expondrán los requisitos de software, y los casos de uso que contiene la aplicación.

Como se explica en capítulos anteriores de este documento, el objetivo de esta aplicación es ayudar a estudiantes de ciberseguridad a encontrar el perfil que más se adecúa a sus características. Un perfil corresponde a cada una de las posiciones que se espera que existan en un equipo dedicado a la ciberseguridad.

Cada perfil lleva asociados unas habilidades, destrezas y conocimientos, los llamados TKSAs, que serán explicados con mayor detalle en siguientes capítulos de este documento. Para la correcta realización de las funciones asociadas a un perfil, es necesario que el trabajador disponga de esas habilidades, destrezas y conocimientos.

Para conocer los perfiles más adecuados para el usuario y el porcentaje de dominio que tienen en una categoría más amplia en el campo de la ciberseguridad, los usuarios deben cumplimentar el test presente en esta aplicación. Deben seleccionar los TKSAs con los que cuentan, y la aplicación calculará los resultados convenientes.

Por ello, gracias a la aplicación desarrollada en este proyecto, estos profesionales o futuros profesionales del campo de la ciberseguridad pueden encontrar qué perfil es el más adecuado a sus características y en qué porcentaje, para determinar que otras TKSAs deben mejorar para llegar a un completo dominio de las funciones necesarias para el desempeño del trabajo descrito en dicho perfil. Esto puede serles de gran utilidad para el desarrollo de su futuro laboral, ya que la mayoría de ellos estarán en fases iniciales dado que son estudiantes del máster.

3.1. Arquitectura de la aplicación

Para explicar la arquitectura sobre la que se forma la aplicación se ha recurrido a una división por capas. La siguiente figura, la cual nos muestra la arquitectura seguida por la aplicación, está basada en el modelo de arquitectura de software de tres capas, ya que es el más utilizado actualmente, y la que explica de forma más completa y sencilla la arquitectura de la aplicación [18].

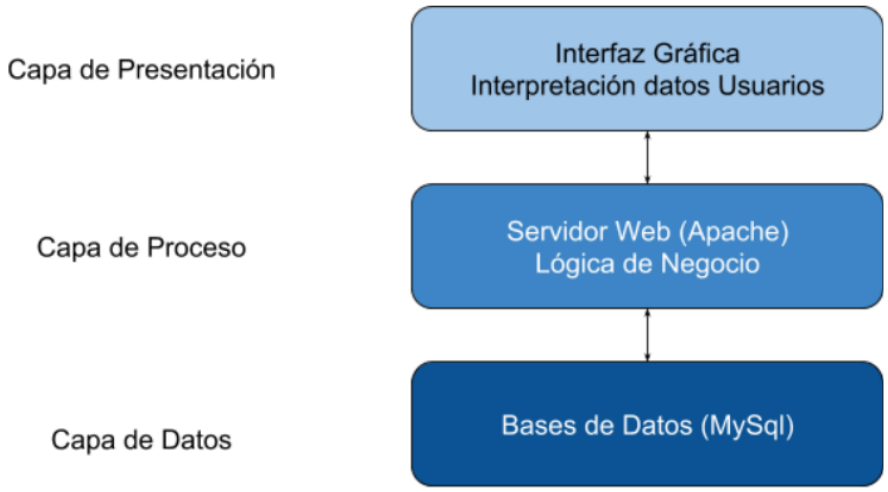


Figura 3.1. Arquitectura de la aplicación web.

Describiremos las tres capas de la más profunda, la capa de datos, a la más superficial, la capa de presentación.

La capa de datos es el lugar donde se encuentran almacenados los datos necesarios para el funcionamiento de la aplicación. Además de almacenar esos datos, se encarga también de recuperarlos y de mantenerlos de forma segura. Es fundamental que esta capa funcione de forma perfecta, ya que son datos críticos para el correcto funcionamiento de la aplicación. En este proyecto se compone de una base de datos en lenguaje SQL, usando el programa MySQL. Se ha elegido este lenguaje de base de datos por su sencillez y por ser el más común.

La capa de proceso o de negocio es en la cual reside toda la lógica de la aplicación. Recoge las peticiones de usuario, realiza las operaciones necesarias, solicitando y recogiendo los datos provenientes de la capa de datos si es necesario, y devuelve esa información al usuario. Este proyecto sigue el patrón de arquitectura Modelo-Vista-Controlador, lo que facilita en gran medida futuros cambios y actualizaciones de la aplicación. En próximos apartados de este documento se explican las funcionalidades presentes en la aplicación y el framework utilizado para la implantación del modelo MVC.

La capa de presentación es aquella que el usuario puede ver y con la que puede interactuar. Recoge la información enviada por el usuario y la envía al servidor. Reciben la información que se genera desde la capa de proceso y la muestran al usuario. Además, generan la presentación y la visualización de la que dispondrá el usuario. En este proyecto, la capa de presentación está compuesta por las diferentes vistas que podemos encontrar para cada funcionalidad que el portal permite realizar al usuario.

De forma global, este sistema abarca las tres partes fundamentales de la arquitectura. Su progreso se abordó en tres fases. La primera, sobre la que se han realizado las modificaciones y desarrollada por Javier Vila, tenía un gran peso en la capa de datos, y bastante poco repartido entre las dos restantes.

El proyecto descrito en este documento se centra en gran medida en la capa de proceso, ya que se implementa un framework para añadir gran cantidad de funcionalidades, y en menor medida, en las capas de datos y presentación con la creación de nuevas bases de datos y vistas necesarias para el funcionamiento de las nuevas funcionalidades añadidas al proyecto base. La mayoría de los cambios en la capa de presentación se recogen en otro Trabajo de Fin de Grado desarrollado por la alumna Sandra Sánchez Esperante.

Con la unión de estos proyectos se pretende construir un proyecto común, consistente en una gran plataforma web totalmente funcional. El proyecto descrito en el Trabajo de Fin de Máster del alumno Javier Vila [19] sentó las bases de este proyecto. En él se desarrollaba la funcionalidad de test, la principal de la aplicación. Por otro lado, carecía del resto de funcionalidades necesarias para una plataforma web de calidad.

La primera mejora al proyecto inicial fue recogida en el TFG de la alumna Sandra Sánchez Esperante [20]. En dicho trabajo se crea una interfaz de usuario intuitiva y fácil de utilizar para cualquier usuario de la aplicación. Se mejora la interfaz de la funcionalidad de test y se crean nuevas vistas correspondientes a un gran número de funcionalidades que serán incluidas en la aplicación por el proyecto expuesto en este documento.

Por último, el TFG descrito en este documento pretende conectar los dos anteriores, resultando en una plataforma web que pueda ser de utilidad a los usuarios, y la creación de nuevas funcionalidades que suplirán las carencias de la plataforma inicial. Se han desarrollado las funcionalidades de: Registro, inicio de sesión, perfil de usuario y gestión de certificaciones. Se han creado también las tablas necesarias para el funcionamiento de la aplicación en la base de datos. Por último, se ha diseñado una iconografía para la aplicación con el objetivo de que pueda ser diferenciada de otras aplicaciones existentes en el mercado.

3.2. Especificación de requisitos de software.

La Especificación de Requisitos de Software o ERS es una especificación completa del funcionamiento del sistema que se va a desarrollar. Incluye un conjunto de casos de uso que describe todas las interacciones que tendrán los usuarios con el software, y los requisitos funcionales y no funcionales. [21]

3.2.1. Requisitos funcionales.

Se definen como requisitos funcionales aquellos que se corresponden con los casos de uso.

TABLA 3.1. RF01 Registro de usuarios.

Identificador	RF01
Nombre	Registro de usuarios.
Descripción	En la pantalla de inicio, el usuario podrá registrarse rellenando el formulario adecuado que aparece en dicha página. Una vez rellenos los datos, serán almacenados en la base de datos y podrán ser usados para el inicio de sesión.
Requisitos previos	Ninguno.

TABLA 3.2. RF02 Inicio de sesión de usuarios.

Identificador	RF02
Nombre	Autenticación de usuarios.
Descripción	En la pantalla de inicio, el usuario podrá iniciar sesión rellenando el formulario adecuado que aparece en dicha página. Una vez rellenos los datos, se enviarán a la base de datos que comprobará que las credenciales son correctas. Si lo son, se iniciará sesión en la aplicación.
Requisitos previos	Ninguno.

TABLA 3.3. RF03 Cierre de sesión.

Identificador	RF03
Nombre	Cierre de sesión.
Descripción	En todo momento será visible en la barra de navegación superior una opción que active la funcionalidad de cierre de sesión. El usuario perderá el token de sesión y se volverá a la pantalla de inicio.
Requisitos previos	RF02.

TABLA 3.4. RF04 Cumplimiento del test.

Identificador	RF04
Nombre	Cumplimiento del test.
Descripción	Una vez accedido a la opción del test, el usuario deberá rellenar el formulario presente, marcando todos los checkbox de los TKSAs con los que cuente.
Requisitos previos	RF02

TABLA 3.5. RF05 Realización de test.

Identificador	RF05
Nombre	Realización de test.
Descripción	Cuando el usuario accione el botón GO, se procederá a añadir todos los TKSAs marcados a una lista, preparada para su cálculo, pero antes se muestra dicha lista para que el usuario determine su corrección.
Requisitos previos	RF02, RF04

TABLA 3.6. RF06 Cálculo de resultados del test.

Identificador	RF06
Nombre	Modificación de test.
Descripción	Una vez comprobado la corrección de los datos, se realizará el algoritmo de cálculo de roles de trabajo más adecuados y categorías. Los resultados correctos se mostrarán en pantalla en dos tablas distintas.
Requisitos previos	RF02, RF04, RF05

TABLA 3.7. RF07 Añadir Certificación.

Identificador	RF07
Nombre	Añadir Certificación.
Descripción	En todo momento será visible en la barra de navegación superior una opción que permita al usuario añadir una certificación. Será redirigido a una pantalla en la que introduce los datos de la nueva certificación, y pulsando un botón manda esa información a la base de datos.
Requisitos previos	RF02.

TABLA 3.8. RF08 Perfil de Usuario.

Identificador	RF08
Nombre	Acceso a la página del perfil de usuario.
Descripción	En todo momento será visible en la barra de navegación superior una opción que permita al usuario acceder a su perfil de usuario, con su información y las certificaciones que posee.
Requisitos previos	RF02.

TABLA 3.9. RF09 Editar Perfil.

Identificador	RF09
Nombre	Editar Datos del Perfil de Usuario.
Descripción	El sistema proporciona varios campos, en los que el usuario debe introducir los nuevos datos sobre su perfil que desee cambiar: nombre de usuario, contraseña o rol de usuario.
Requisitos previos	RF08.

TABLA 3.10. RF10 Añadir Certificación Usuario.

Identificador	RF10
Nombre	Añadir Certificación al perfil del Usuario.
Descripción	El sistema proporciona la posibilidad al usuario de seleccionar las certificaciones que posee. Se enlaza en la base de datos la certificación, junto con el perfil que define, al usuario, y se mostrará en su perfil desde ese momento.
Requisitos previos	RF07 y RF08.

TABLA 3.11. RF11 Borrar Certificación Usuario.

Identificador	RF11
Nombre	Borrar Certificación del perfil de Usuario.
Descripción	El sistema proporciona la posibilidad de borrar certificaciones de las que posee el usuario. En un select se selecciona la certificación a borrar y se pulsa un botón, que transmite la información a la base de datos, la cual desenlazará dicha certificación del usuario y no aparecerá más en su perfil.
Requisitos previos	RF07, RF08 y RF10.

TABLA 3.12. RF12 Consulta de dashboard.

Identificador	RF12
Nombre	Consulta de dashboard.
Descripción	En todo momento será visible en la barra de navegación superior una opción que acceda al perfil del dashboard. El sistema mostrará de forma gráfica la información obtenida de los test del usuario.
Requisitos previos	RF02, RF04, RF05

3.2.2. Requisitos no funcionales.

Los requisitos no funcionales representan aquellos que pueden usarse para definir la operación de un sistema, pero sin entrar en sus detalles específicos.

TABLA 3.13. RNF01 Conexión a internet.

Identificador	RNF01
Nombre	Conexión a internet.
Descripción	Para acceder a la aplicación y mantenerse en ella será imprescindible el acceso a una conexión a internet en todo momento.
Requisitos previos	Ninguno

TABLA 3.14. RNF02 Protección de información.

Identificador	RNF02
Nombre	Protección de información.
Descripción	La protección de los datos de usuario se protege contra ataques maliciosos. Contraseñas encriptadas para la confidencialidad.
Requisitos previos	Ninguno

TABLA 3.15. RNF03 Compatibilidad entre navegadores.

Identificador	RNF03
Nombre	Compatibilidad entre navegadores.
Descripción	El desarrollo se realizará para que la aplicación sea funcional en cualquier navegador de los presentes en el mercado actual.
Requisitos previos	Ninguno

3.3. Casos de uso.

Un caso de uso es una secuencia de transacciones que realiza un sistema en respuesta a un evento comenzado por un actor sobre él. [22]

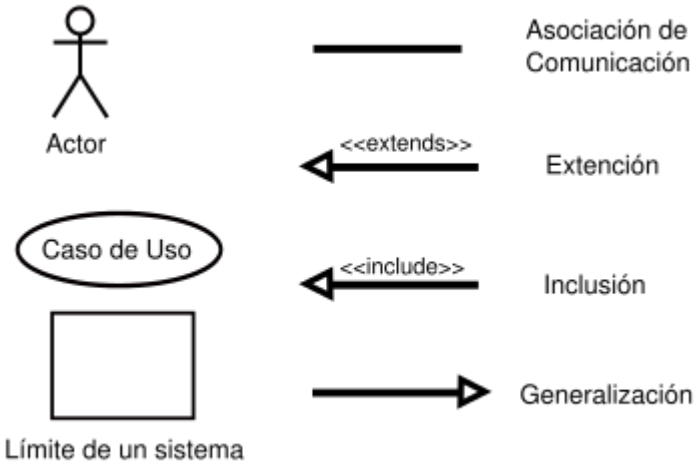
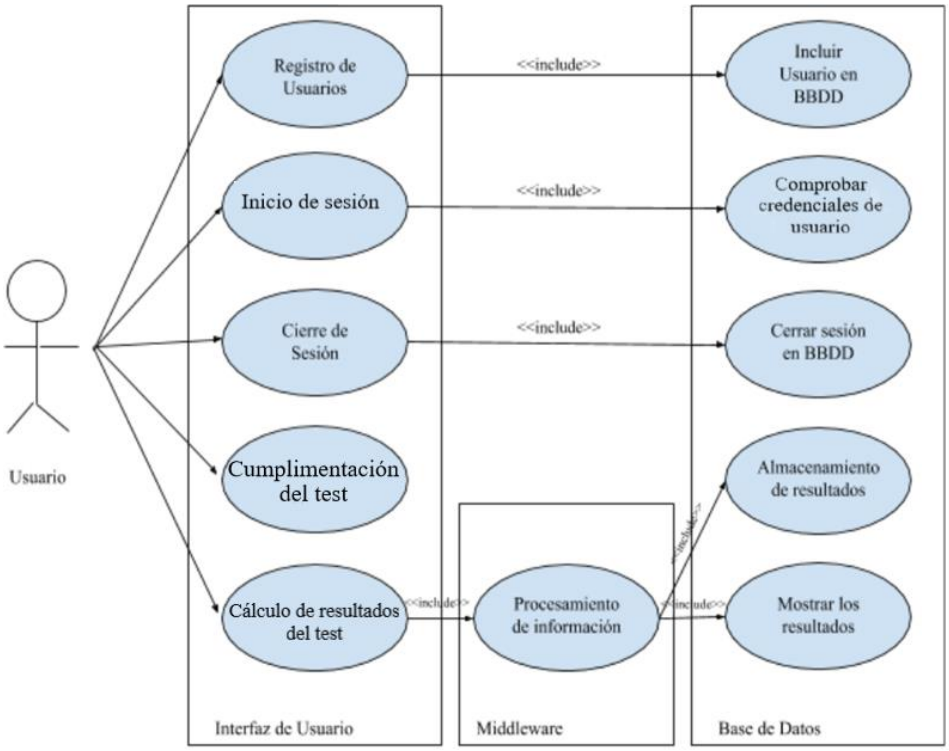


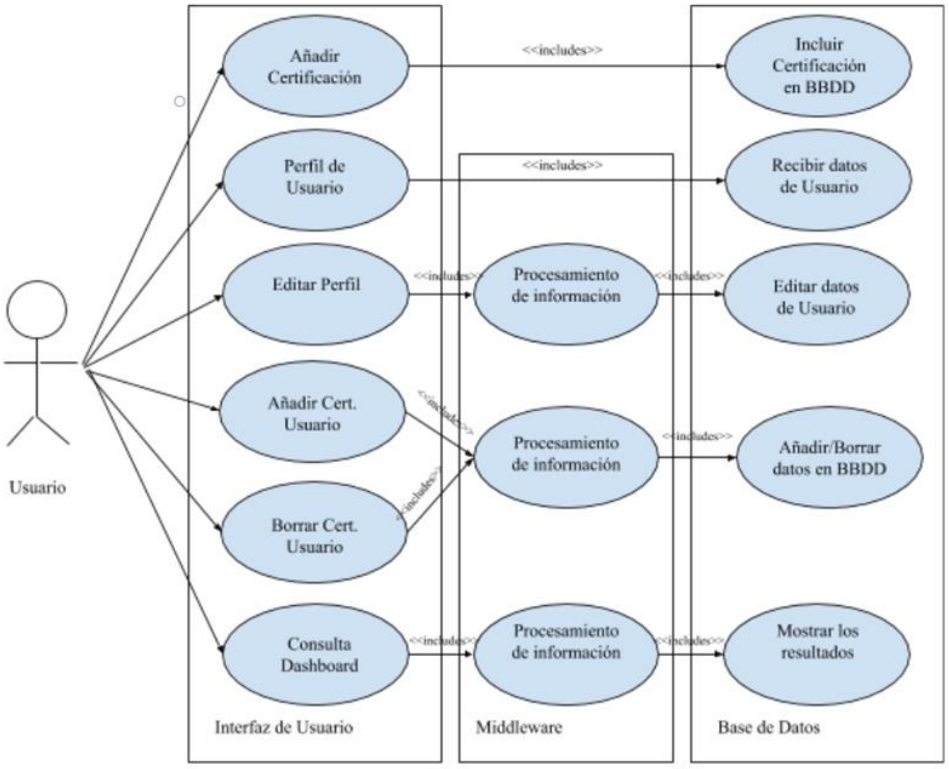
Figura 3.2. Notación de caso de uso [22]

Partiremos de los requisitos funcionales explicados en el apartado anterior para desarrollar los casos de uso que se encuentran en nuestra aplicación.

Cada globo azul representa una acción que se debe de realizar para llevar a cabo la funcionalidad necesaria para el cumplimiento de cada caso de uso. Algunas de ellas pueden ser ejecutadas directamente a petición del usuario, y otras serán activadas por otras partes del software. Cada caso de uso se compone del camino completo que se debe seguir a través de las instrucciones marcadas en dichos globos, para la realización de una acción completa.

A continuación, se muestra el diagrama de los casos de uso presentes en la aplicación en dos partes para facilitar su entendimiento.





Figuras 3.3. y 3.4. Diagramas de casos de uso 1 y 2

4. DESARROLLO SOFTWARE

4.1. Diseño de la aplicación.

El paso previo al desarrollo de la aplicación consiste en planificar el diseño de la nueva aplicación.

El portal en el que está basado este proyecto tenía un diseño muy básico, usando PHP sin ningún tipo de Framework, y con HTML y CSS para las vistas, y cierto JavaScript para realizar los métodos del test.

Tras un análisis previo de las funcionalidades que se planeaba añadir a la aplicación, se vio de forma clara la necesidad de incorporar un Framework PHP, el cual ayudara a la realización de dichas tareas, a través del uso de APIs, y para tratar de mejorar la comunicación con la base de datos.

Para ello, después de realizar una comparación entre diferentes Frameworks existentes en el mercado, se decidió a usar Laravel debido a las ventajas que ofrece con otras opciones.

En cuanto a la metodología de trabajo, se decidió hacer uso de la metodología ágil, dadas las características del proyecto, y la necesidad de adaptarse a todos los pequeños cambios y modificaciones que se tengan que realizar.

4.1.1. Laravel

Laravel es un framework de código abierto para desarrollar aplicaciones y servicios web sobre PHP en sus versiones 5 y 7. Este framework trata de crear código elegante de forma sencilla y permitiendo multitud de funcionalidades a través de la utilización de otros frameworks y dependencias externas. [23]

Este framework sigue el patrón MVC de una forma muy sencilla, lo que facilita futuras modificaciones de la aplicación. Añade controladores que permiten organizar el código sin tener que añadir todo el código PHP en las vistas.

Otras ventajas que podemos encontrar en Laravel y que lo hacen el framework indicado para la realización del proyecto son:

- **Eloquent:** Transforma las consultas SQL a un sistema MVC, que las hace mucho más sencillas de manejar, además de evitar los ataques de inyección SQL. [24]

- **Autenticación:** Laravel incluye un sistema de autenticación avanzado, el cual encripta datos sensibles a la hora de incluirlos en la base de datos. Además, añade un campo "token" en la base de datos de usuarios, lo cual permite manejar el inicio y cierre de sesión correctamente. Todas estas funcionalidades tienen como finalidad proteger a la aplicación de posibles ataques, como por ejemplo a los "Cross-site Scripting".

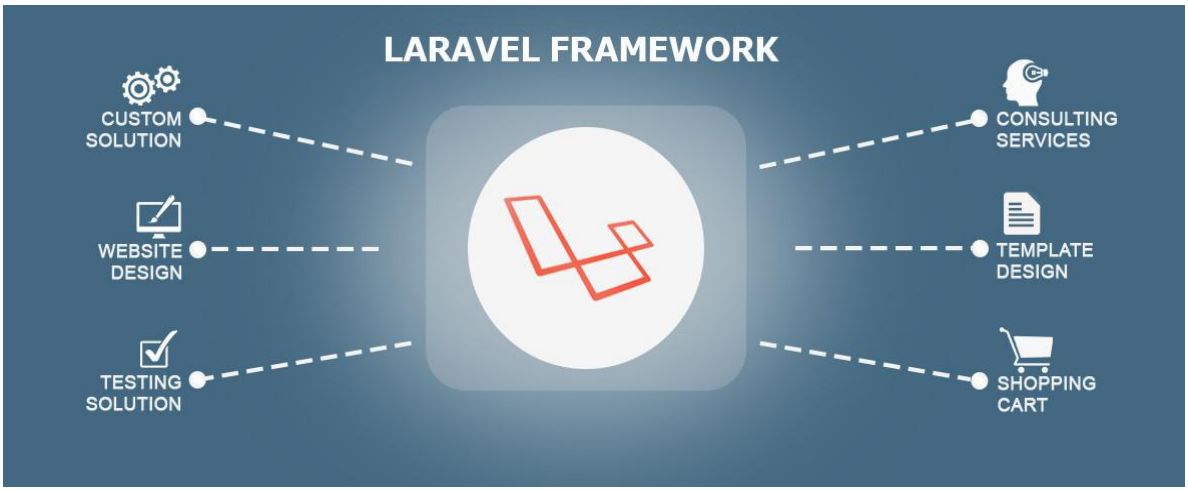


Figura 4.1. Descripción del Framework de Laravel [25]

4.1.2 Otros Frameworks

Laravel no es el único framework existente en el mercado, ya que existen varias aplicaciones alternativas muy apreciadas por los programadores que normalmente construyen sus aplicaciones en PHP.

El primero que se debe mencionar es Symfony2. Este framework se considera ideal para proyectos de grandes magnitudes, debido a que cuenta con un gran número de componentes de gran reutilización. Cuenta con licencia de código libre del MIT y con una gran comunidad de usuarios los cuales aportan nuevos componentes o ideas de código continuamente, lo que fomenta el continuo crecimiento de Symfony2.

El segundo framework a destacar es Codeigniter. Ha sido el referente de la programación en PHP durante muchos años, aunque actualmente ha quedado relegado al tercer puesto en cuanto a importancia. Este framework destaca sobre todo por su ligereza y rapidez, siendo una muy buena opción de iniciación en el desarrollo de aplicaciones en PHP para desarrolladores con no demasiada experiencia.

Los dos frameworks expuestos anteriormente son muy buenas opciones para el desarrollo de aplicaciones PHP, lo que lleva a la pregunta ¿Por qué elegir Laravel por encima de sus competidores? La respuesta se encuentra en su extrema facilidad de aprender y de usar. Además, cuenta con plantillas propias, las denominadas Blade, y con el servidor HomeStead, lo que nos ahorrará la instalación de un servidor web o PHP en nuestra máquina local. [26]

4.1.3. Metodología Ágil

"Agile" es un conjunto de metodologías para el desarrollo de proyectos que precisan de rapidez y flexibilidad para adaptarse a condiciones cambiantes en un mercado o sector, e intenta aprovechar dichos cambios para conseguir una ventaja competitiva. [27]

Este tipo de metodologías se están imponiendo claramente en los últimos años a las metodologías tradicionales en proyectos de tecnología, entre otras debido a las siguientes razones [28]:

- Las metodologías Agile son flexibles, rápidas, consistentes y responsivas.
- Se centran en gran medida en las personas y están orientadas a la comunicación.
- Están testadas en un ambiente dinámico y han resultado muy flexibles en la adaptación a los cambios que se producen en el entorno de trabajo.
- Los métodos Agile incluyen inspecciones regulares, lo cual fomenta las cualidades de liderazgo para estimular el trabajo en equipo.
- Los métodos Agile siguen las mejores prácticas que ayudan a conseguir un código de alta calidad de forma rápida y sencilla.

Por todas estas razones, se ha decidido usar una metodología Agile para el desarrollo de este proyecto. En concreto se ha elegido Scrum, una de las más utilizadas a nivel mundial y que se caracteriza por adoptar una estrategia de desarrollo incremental, en lugar de la planificación y ejecución completa del producto. [29]

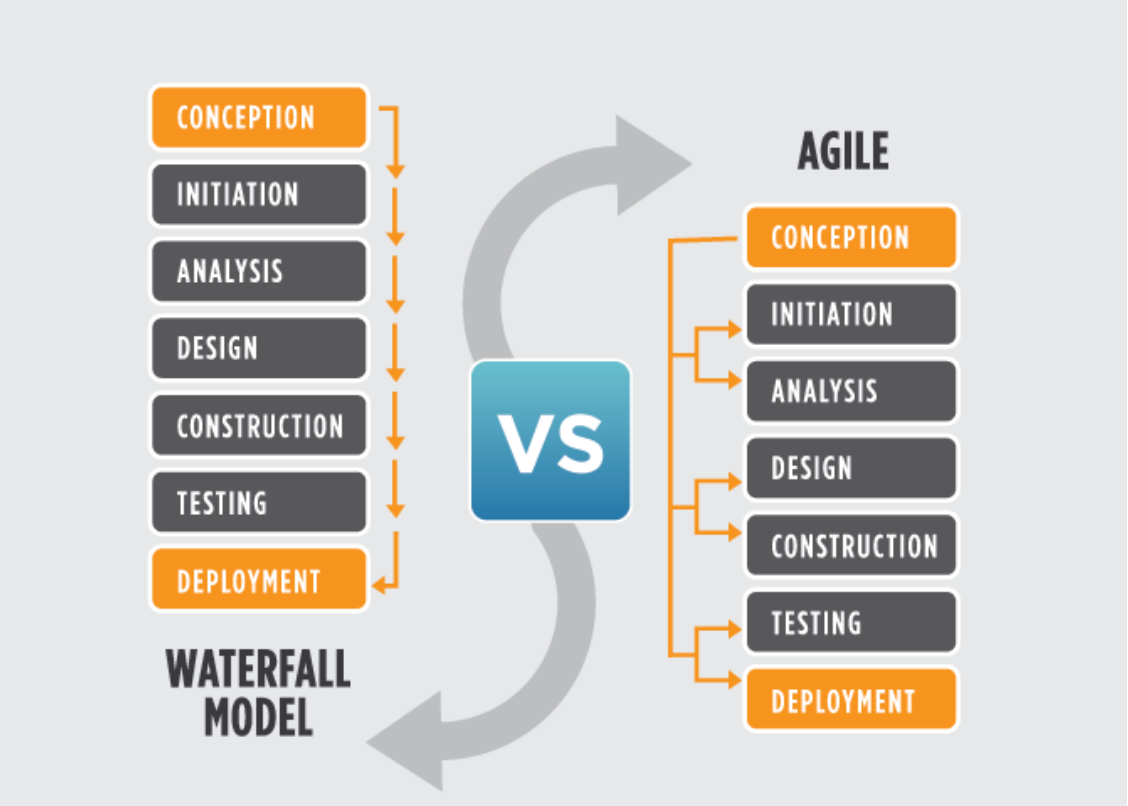


Figura 4.2. Comparación entre metodología en cascada y ágil [28]

4.2 Diagramas de flujo

A continuación, se representan los diagramas de flujo de las principales funcionalidades que ofrece la aplicación. Algunas de ellas se incluían en el proyecto original y han sido modificadas, y otras han sido desarrolladas por completo en este proyecto. Este capítulo tiene como objetivo crear una imagen general de las funcionalidades existentes en el proyecto base, y las modificaciones y desarrollos se explicarán con mayor detalle en el capítulo 4.3.

4.2.1 Registro de usuarios

La siguiente figura representa la funcionalidad del registro de usuarios. Es una funcionalidad imprescindible ya que no se puede acceder al portal sin realizar este paso previamente. En la página de inicio, el usuario debe introducir los datos del nuevo usuario y pulsar el botón de Register. Esto enviará los datos a la base de datos, la cual los almacenará si son correctos. Esta funcionalidad no estaba incluida en el proyecto de Javier Vilas, pero es de vital importancia para el funcionamiento de la aplicación.

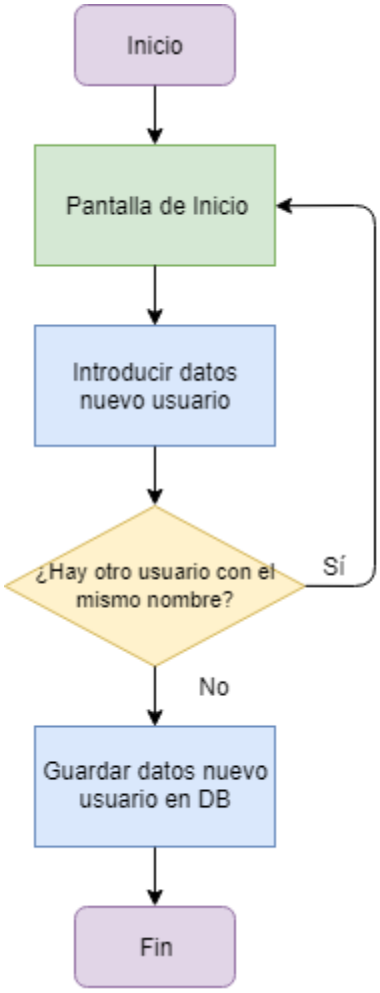


Figura 4.3. Diagrama de flujo del Registro de usuarios

4.2.2 Inicio de sesión

Una vez registrado el usuario, volveremos a la página de inicio. Allí debemos introducir los datos del usuario creado anteriormente. El sistema comprobará que los datos introducidos por el usuario coinciden con aquellos almacenados en la base de datos y, si existe una coincidencia, entrará al menú principal de la aplicación registrado con dicho usuario.

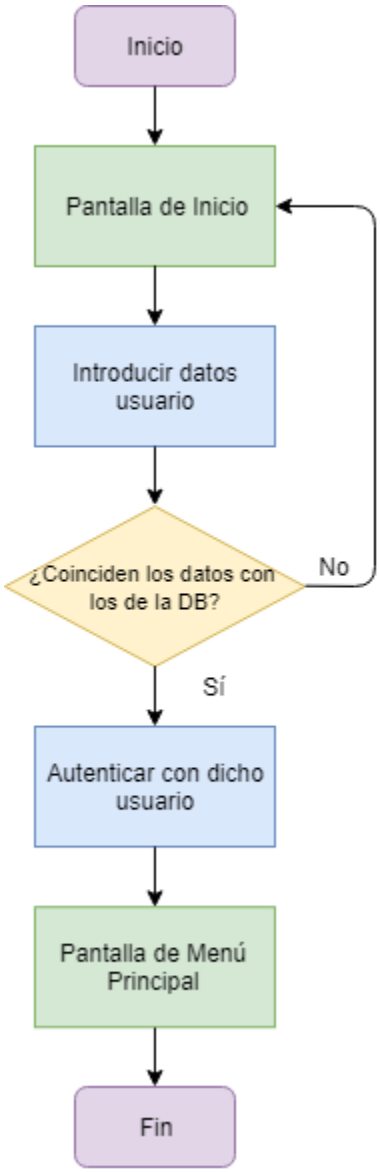


Figura 4.4. Diagrama de flujo de inicio de sesión

4.2.3 Realización del Test

La funcionalidad principal de la aplicación es la realización del test para conocer el perfil de ciberseguridad más recomendado para el usuario. Actualmente, cada vez que se realiza un nuevo test se borran los datos antiguos sobre los 10 roles más adecuados y similitud con las categorías de ese usuario, aunque los TKSAs seleccionados se mantienen. Se realiza así para evitar sobrecargas en la base de datos. Esta funcionalidad sigue el diagrama de flujo mostrado a continuación.

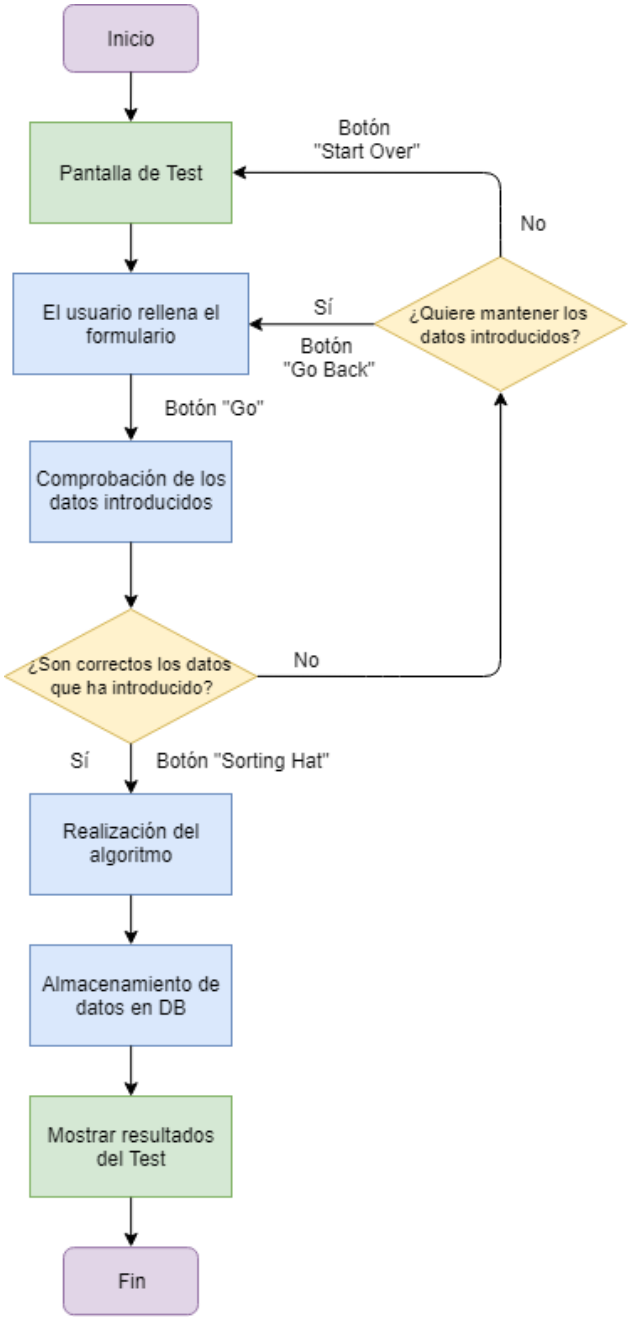


Figura 4.5. Diagrama de flujo de realizar test

4.3. Modificaciones del modelo previo.

En este apartado se explican de forma detallada los cambios que se han desarrollado sobre el proyecto inicial. Se realizará la división por funcionalidades para facilitar la comprensión de los cambios al lector. La mayoría de las interfaces gráficas de la aplicación han sido desarrolladas en el proyecto de la compañera Sandra Sánchez Esperante, por lo que sólo se incluirá este apartado cuando las mismas hayan sido desarrolladas en este proyecto.

4.3.1 Registro de Usuarios

El proyecto inicial carecía de cualquier tipo de identificación de usuario, por lo que se llegó a la conclusión de que el desarrollo de esta funcionalidad tenía una prioridad muy alta. En los siguientes apartados se explican los cambios desarrollados en este proyecto.

- **Bases de Datos**

El proyecto original carecía de una base de datos de usuarios, por lo que el primer paso en el desarrollo fue la creación de esta en nuestra base de datos global. Su composición es la siguiente.

#	Nombre	Tipo
1	**id**	int(11)
2	**email**	varchar(45)
3	**username**	varchar(45)
4	**password**	varchar(255)
5	**user_role**	enum('student', 'enterprise', 'admin')
6	**created_at**	date
7	**updated_at**	date
8	**remember_token**	varchar(100)

Figura 4.6 Estructura de la base de datos de usuarios

Los campos principales son username, email y password, los cuales corresponden a los datos introducidos por el usuario en la página de inicio. La información almacenada en el campo “password” debe ser confidencial y protegida ante posibles ataques externos. Para ello se utiliza el método “bcrypt” de Laravel, el cual protege la información del campo, y conoce además el hash para desencriptarla a la hora de iniciar sesión.

- **Funcionalidad**

Una vez introducidos los datos de nombre de usuario, contraseña, email y el rol, cuando se clica en el botón inferior los datos son enviados al controlador de usuario (UserController). Este recoge la información del formulario y crea un nuevo objeto de User, el cual es enviado a la base de datos para que sea añadido. Laravel ofrece la opción de incluir restricciones a la hora de enviar el formulario, lo que facilita en gran medida la comprobación de que el nombre de usuario sea único, o que la contraseña tenga una longitud mínima establecida entre otras funciones.

A continuación, se muestra un diagrama de la funcionalidad explicada anteriormente.

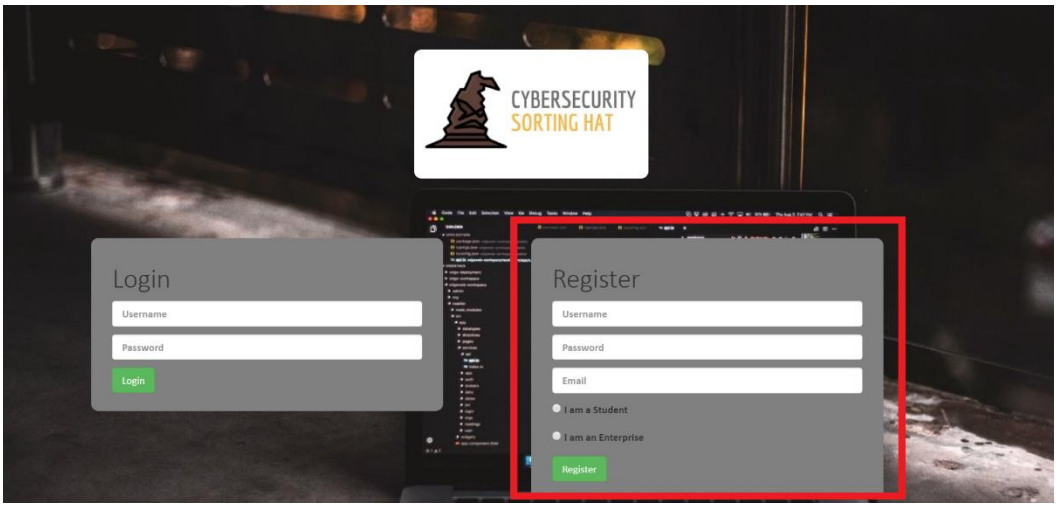


Figura 4.7 Función de Registro en la vista de inicio

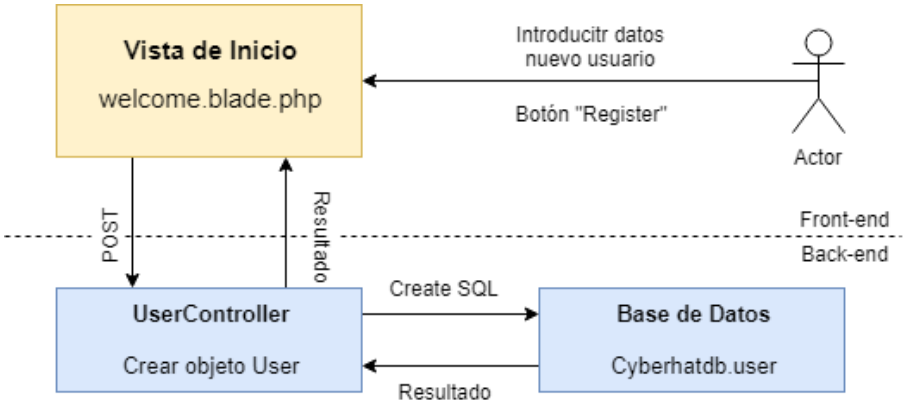


Figura 4.8 Diagrama de la funcionalidad de Registro

4.3.2 Inicio y Cierre de sesión

Una vez implementada la funcionalidad de registro de usuarios, se decidió implementar la funcionalidad para que esos usuarios pudieran acceder a la plataforma utilizando las credenciales introducidas anteriormente en la base de datos.

- **Bases de Datos**

Para el desarrollo de esta funcionalidad, se comprueba la información contra la base de datos “User”, la cual se explica con detalle en el apartado 4.3.1.

- **Funcionalidad**

Existen múltiples formas de comprobar la existencia de los datos introducidos por el usuario en la base de datos, pero las soluciones ofrecidas por PHP en su forma más básica carecían de varios factores claves a la hora de navegar por la totalidad de la aplicación.

Por otra parte, Laravel nos soluciona este problema a través de su configuración “Auth” la cualnos permite comprobar los datos de usuarios de forma sencilla, maneja la comprobación de la contraseña encriptada en la base de datos, e incluye un token de sesión que se mantiene durante el tiempo que el usuario esté autenticado en la plataforma.

También incluye una opción para el cierre de sesión, que retira el token al usuario, evitando problemas de coordinación al tener sesiones abiertas en dos pestañas o ventanas.

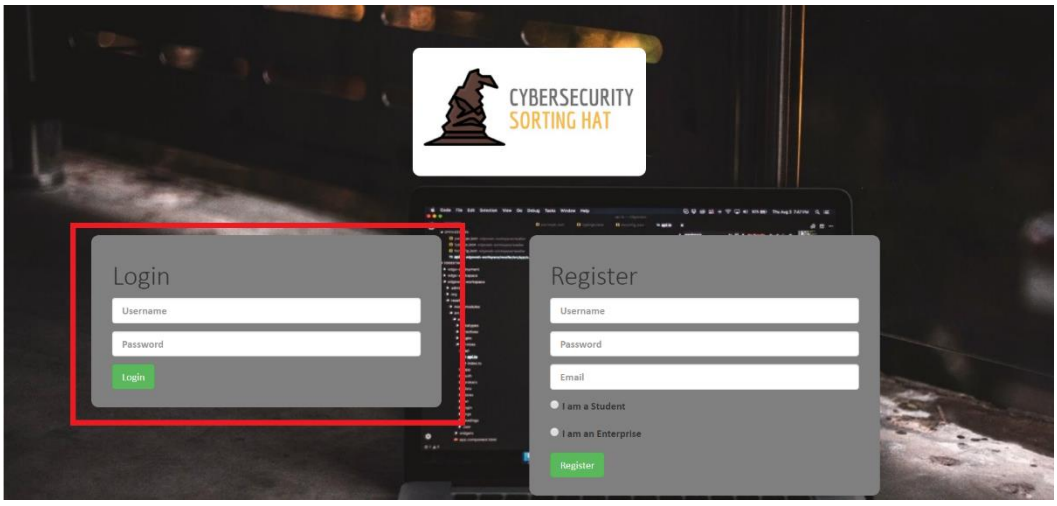


Figura 4.9 Función de Inicio de Sesión en la vista de inicio

Figura 4.10 Función de Cierre de Sesión en la vista del menú principal

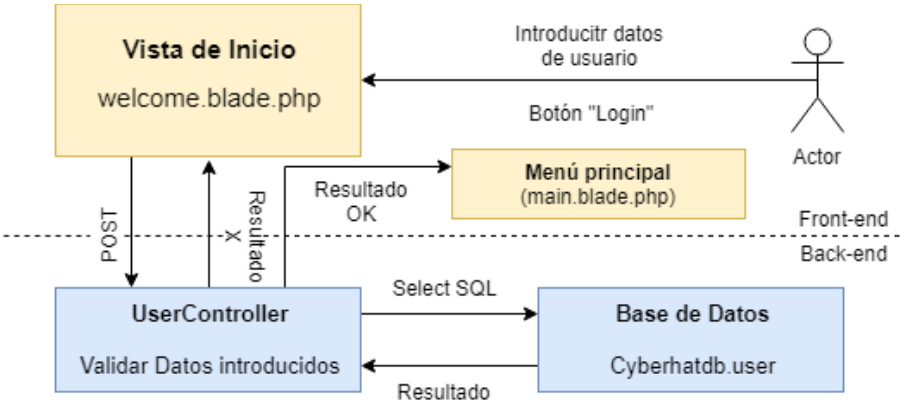


Figura 4.11 Diagrama de la funcionalidad de Inicio de Sesión

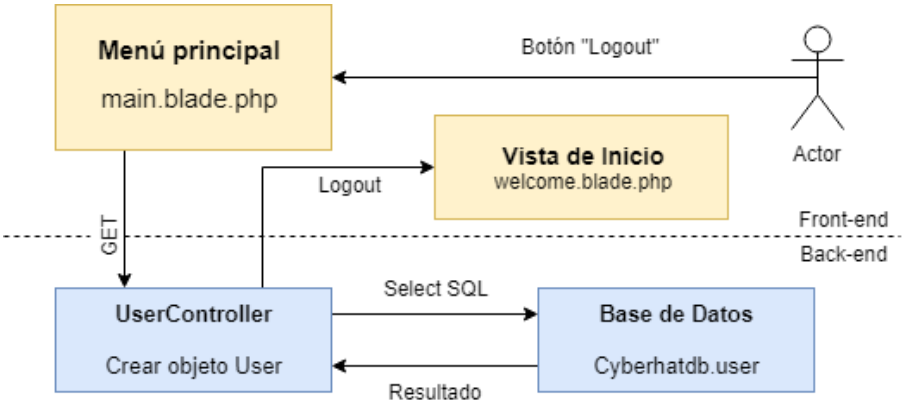


Figura 4.12 Diagrama de la funcionalidad de Cierre de Sesión

4.3.3 Añadir Certificación

A la hora de elaborar un perfil de usuario de ciberseguridad detallado, es importante conocer las certificaciones que el mismo posee. Cada certificación tiene un perfil tipo asociado, por lo que puede servir de guía sobre qué TKSAs debería marcar el usuario. Por el momento, las certificaciones se añaden de forma informativa.

- **Bases de Datos**

Para la creación de esta funcionalidad ha sido necesario añadir dos nuevas tablas a nuestra base de datos cyberhatdb. La primera ha sido nombrada como "certification". Su estructura es la siguiente:

#	Nombre	Tipo
1	**id** 🔑	int(11)
2	**certification_title**	varchar(255)
3	**profile_id** 🔗	int(11)
4	**certifier**	varchar(100)
5	**certifier_link**	varchar(255)
6	**country**	varchar(100)
7	**created_at**	date
8	**updated_at**	date

Figura 4.13 Estructura de la tabla certification

En ella se almacenan los datos de las certificaciones añadidas por el usuario, con toda la información relacionada con la misma: título, perfil relacionado, entidad que otorga esta certificación y su país de emisión. Esta información puede ser revisada por el usuario administrador para comprobar su veracidad.

- **Vistas**

En el proyecto inicial, no existía la funcionalidad de añadir una certificación, y por lo tanto ha sido necesario la creación de una nueva vista para la realización de la misma. Se accede a ella a través del menú principal, después de seleccionar la opción "Add Certification" de la barra superior. Al realizar esta acción nos encontraremos con la página siguiente:

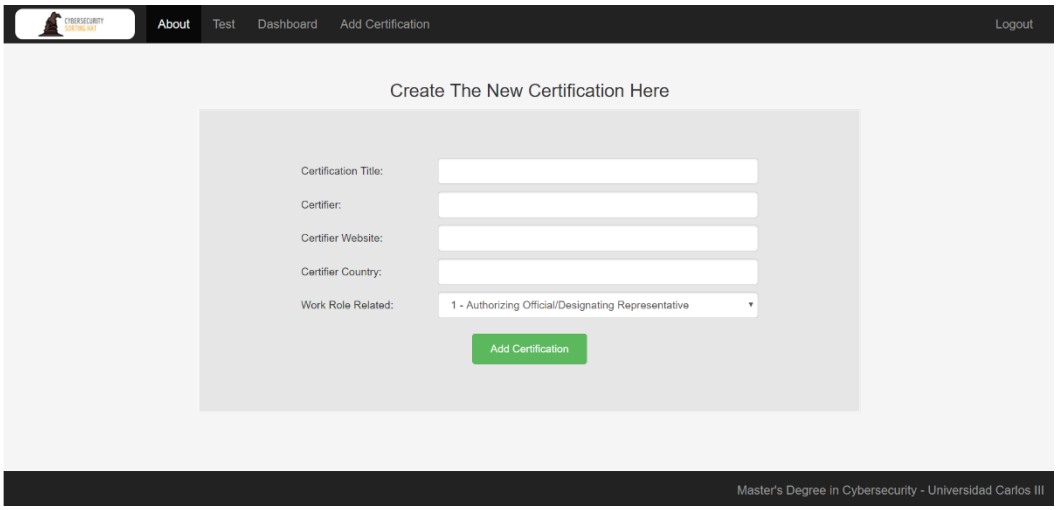


Figura 4.14 Vista de Añadir Certificación

La interfaz está creada de forma sencilla, para que resulte intuitiva para cualquier tipo de usuario. Consiste en unos campos en los que el usuario introducirá la información necesaria sobre la certificación y un botón, el cual enviará la información introducida al back-end cuando es seleccionado.

- **Funcionalidad**

En lo relacionado con la funcionalidad en sí, esta funcionalidad se desarrolla de una manera muy sencilla. El primer paso consiste en que el usuario rellene la información necesaria en los campos que podemos apreciar en la imagen de la vista en el apartado anterior. Una vez rellenos, se procederá a hacer clic en el botón verde de la parte inferior de la pantalla. Esto enviará los datos al controlador, en este caso CertificationController, el cual creará una nueva instancia del objeto Certification usando los modelos de Laravel y, si no está ya incluido en la base de datos, lo añadirá usando la sentencia CREATE de SQL.

En la siguiente figura se puede apreciar un diagrama del intercambio de información que se produce al realizar esta funcionalidad.

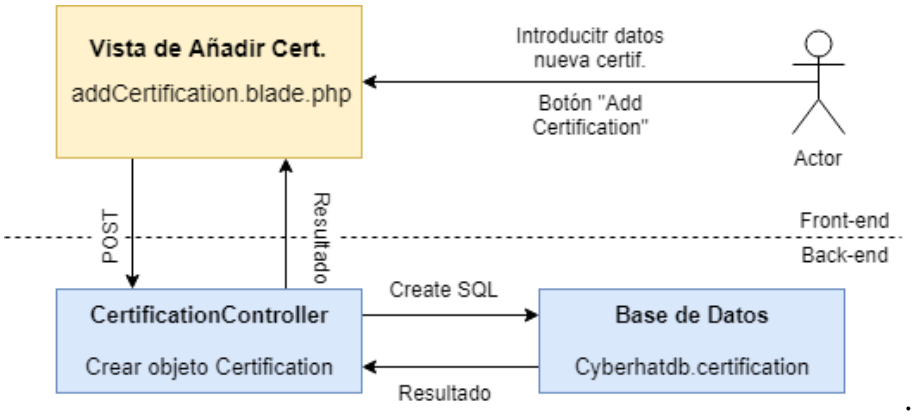


Figura 4.15 Diagrama de la funcionalidad de Añadir Certificación

4.3.4 Perfil de Usuario

Una de las funcionalidades principales de una aplicación que se coordina por la existencia de usuarios reside en la capacidad de acceder a una página de perfil de los mismos, en la cual se expondrá toda la información detallada acerca de dicho usuario.

- **Bases de Datos**

Para el desarrollo de esta funcionalidad se ha requerido de la información contenida en las tablas “user” y “certification”, ya que en ellas se puede encontrar la información necesaria para cumplimentar el perfil de usuario.

Por otra parte, se estimó necesaria para el desarrollo de la funcionalidad la creación de una tabla que uniera las dos anteriores, para indicar qué usuarios han adquirido qué certificaciones, para su posterior publicación en la página de perfil de usuario. Para ello se creó la tabla “user_has_certifications”, cuya sencilla estructura se puede ver en la siguiente figura.

#	Nombre	Tipo
1	user_id	int(11)
2	certification_id	int(11)
3	created_at	date
4	updated_at	date

Figura 4.16 Tabla user_has_certification

La tabla consta de dos claves principales, las cuales se corresponden con el id de un usuario y el id de una certificación. De esta forma podemos conectar ambas tablas para habilitar la posibilidad de ver las certificaciones con las que cuenta un usuario.

- **Vista**

Para el desarrollo de esta funcionalidad se ha creado una vista estructurada de forma muy sencilla e intuitiva y en la cual se muestra la información recabada de las bases de datos explicadas anteriormente. Para acceder a ella se debe clicar en la opción “About” en la barra de navegación superior de la aplicación.

Una vez realizada esta acción, se redirigirá al usuario a la siguiente vista:

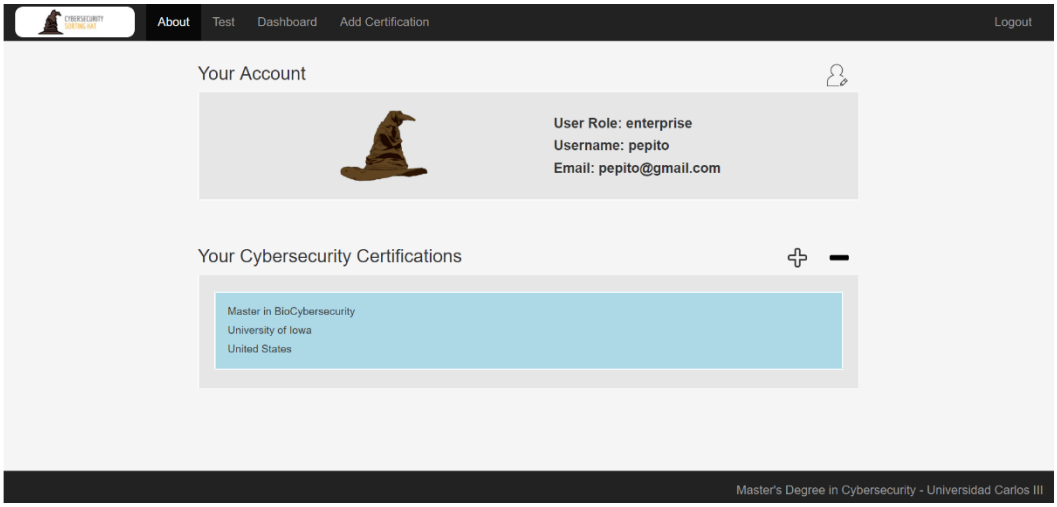


Figura 4.17 Vista de Perfil de Usuario

En ella se pueden ver dos secciones totalmente diferenciadas. La primera corresponde a los datos del usuario en sí, los cuales eligió a la hora de registrarse. Se puede ver el nombre de usuario, el rol de usuario y el mail.

La segunda se compone de una lista en la que se muestran los datos correspondientes a las certificaciones que dicho usuario posee. De cada una de las certificaciones se muestran: el título de esta, el organismo oficial que la otorga y el país en el que se encuentra dicho organismo.

- **Funcionalidad**

Esta página tiene una función de carácter informativo, por lo que solo dispone de dos funcionalidades extra. Existe la posibilidad de editar estos datos del usuario, simplemente haciendo clic en el símbolo de la parte superior derecha del recuadro superior, el cual se encuadra en verde en la siguiente imagen. Esta funcionalidad se explicará en más detalle en secciones posteriores de este documento.

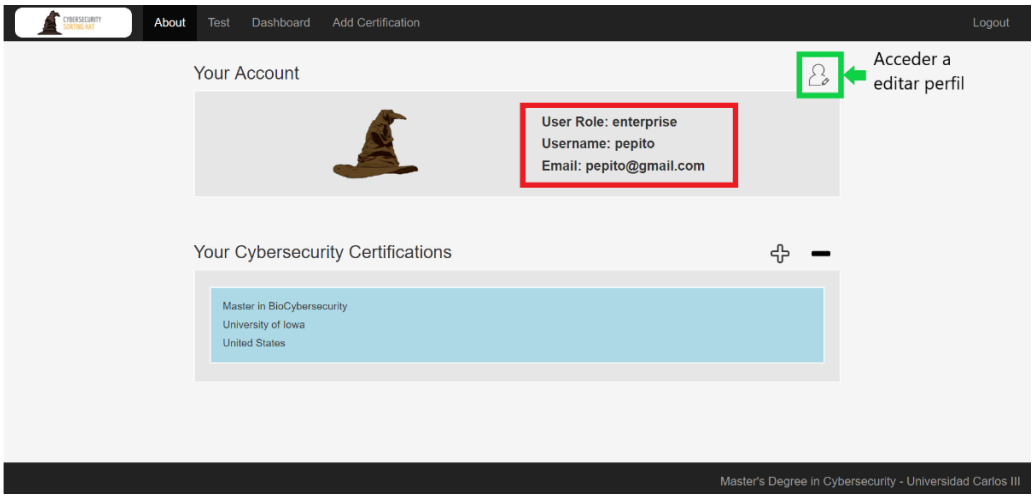


Figura 4.18 Datos de usuario y Edición de Perfil en Vista de Perfil de Usuario

En la esquina superior derecha del recuadro inferior podemos encontrar dos opciones, las cuales nos dan la posibilidad de añadir o borrar certificaciones para el usuario seleccionado. Estas dos funcionalidades serán explicadas más adelante y podemos encontrarlas encuadradas en verde en la siguiente imagen.

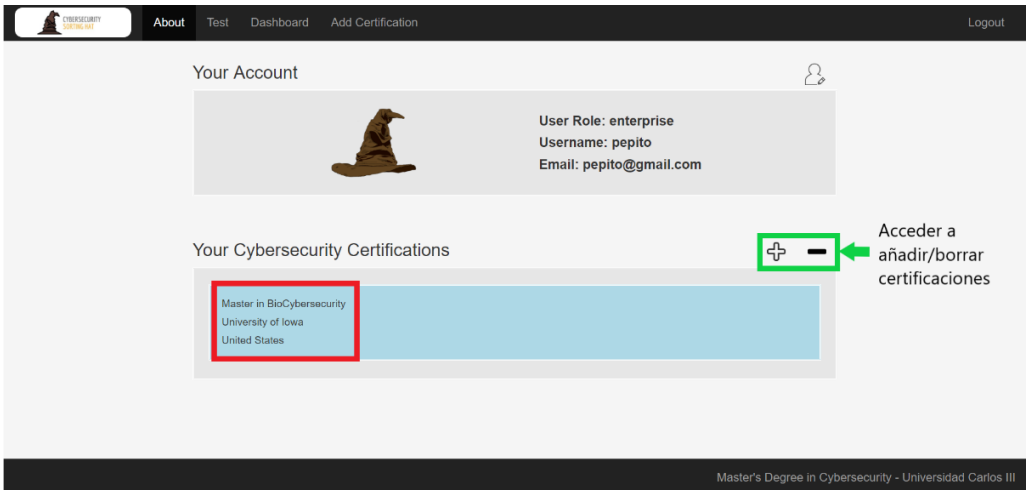


Figura 4.19 Certificaciones y Añadir/Borrar Certif. en Vista de Perfil de Usuario

4.3.5. Editar datos de usuario

En cualquier aplicación, es conveniente incluir una opción para editar los datos del usuario, ya que es necesario adaptarse a los cambios que puedan aparecer en los mismos, sin tener que recurrir a la creación de un nuevo usuario.

- **Bases de Datos**

De la misma forma que la funcionalidad anterior, esta se relaciona con la tabla “user” de la base de datos, ya que se requiere de una modificación de la información almacenada en dicha tabla para la actualización de los datos del usuario.

- **Vistas**

Para la implementación de la siguiente funcionalidad, ha sido necesaria la creación de una nueva vista en la que el usuario pudiera introducir los datos que desea modificar en su perfil. A continuación, podemos ver una captura de dicha vista dentro de la aplicación.

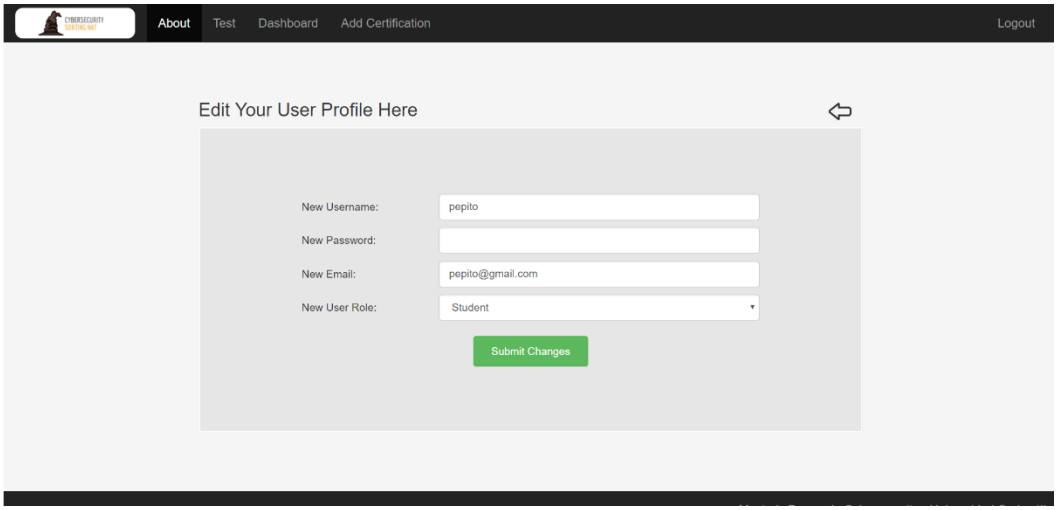


Figura 4.20 Vista de Edición de Perfil de Usuario

Como se puede observar, esta página está compuesta por un form, el cual contiene cuatro recuadros, correspondientes con los datos de los que se compone un usuario actualmente y un botón encargado de enviar la información al backend. Los campos tienen como valor por defecto los datos con los que cuenta el usuario en ese momento.

Asimismo, en la parte superior del recuadro, se puede observar un botón en forma de flecha, el cual nos permite volver a la vista anterior.

- **Funcionalidad**

La funcionalidad de esta página está desarrollada de forma intuitiva como el resto de la aplicación, para que resulte sencilla de usar para cualquier tipo de usuario.

Para realizar la modificación de sus datos, el usuario debe rellenar los campos que desee cambiar con la nueva información. Una vez realizado esto, deberá hacer clic en el botón de la parte inferior para que los nuevos datos sean transmitidos al controlador correspondiente, y este actualice la información contenida en la tabla de la base de datos. Los datos que no hayan sido modificados mantendrán el valor que tenían previamente.

Podemos ver una descripción del intercambio de datos que se produce en esta funcionalidad en el siguiente diagrama:

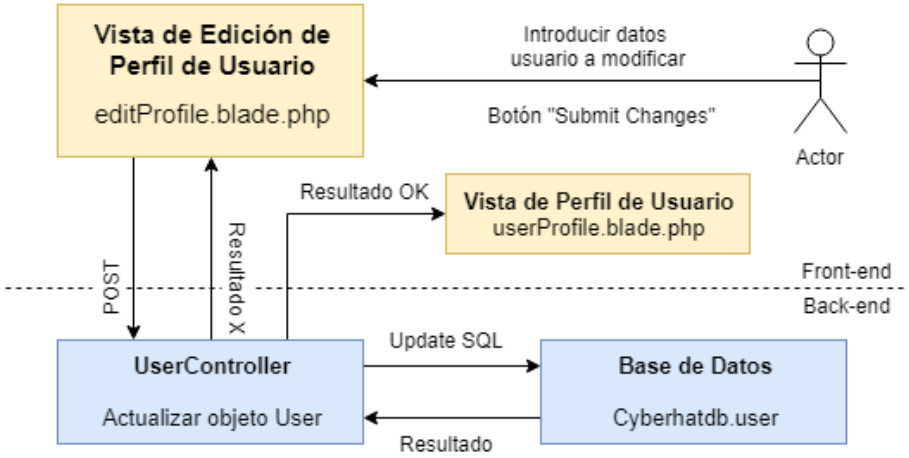


Figura 4.21 Diagrama de la funcionalidad de Editar Perfil de Usuario

4.3.6. Añadir/Borrar Certificación de Usuario

Dado que la aplicación nos ofrece una opción en la que se pueden añadir certificaciones oficiales a la base de datos, es necesario crear de la misma forma una opción que conecte dichas certificaciones con los usuarios presentes en el portal.

Por lo tanto, se crearon estas dos opciones, a las cuales se puede llegar a través del perfil de usuario, de la manera explicada en dicha sección de este documento.

- **Bases de datos**

De la misma manera que la funcionalidad de mostrar el perfil de usuario, estas dos se relacionan directamente con la tabla “user_has_certification”, y de forma indirecta con las tablas “user” y “certification” de la base de datos, ya que se requiere de una modificación de la información almacenada en la primera para conseguir la unión de datos entre las otras dos.

- **Vistas**

Para poder realizar esta funcionalidad, ha sido necesaria la creación de dos vistas, las cuales son muy similares, y que se pueden ver en las siguientes imágenes.

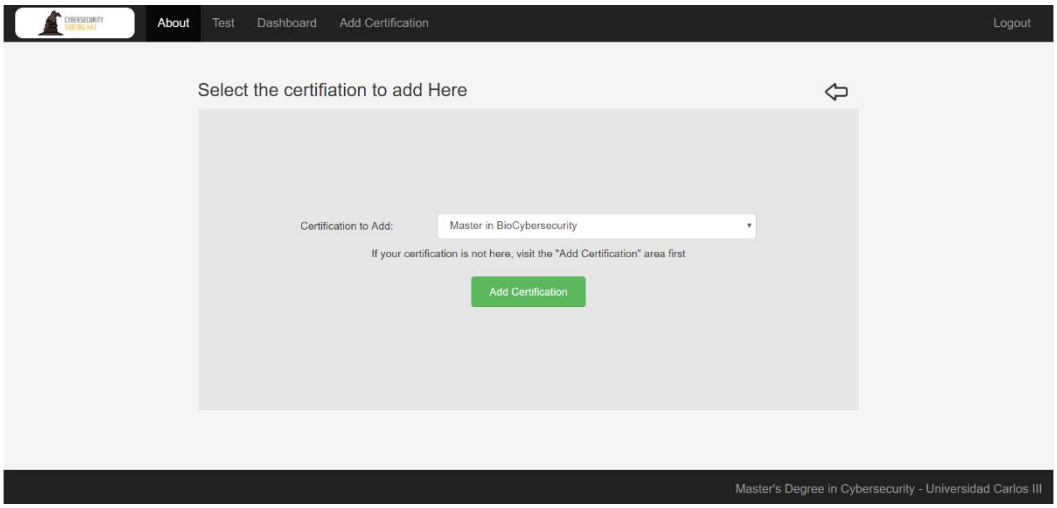


Figura 4.22 Vista de Añadir Certificación de Usuario

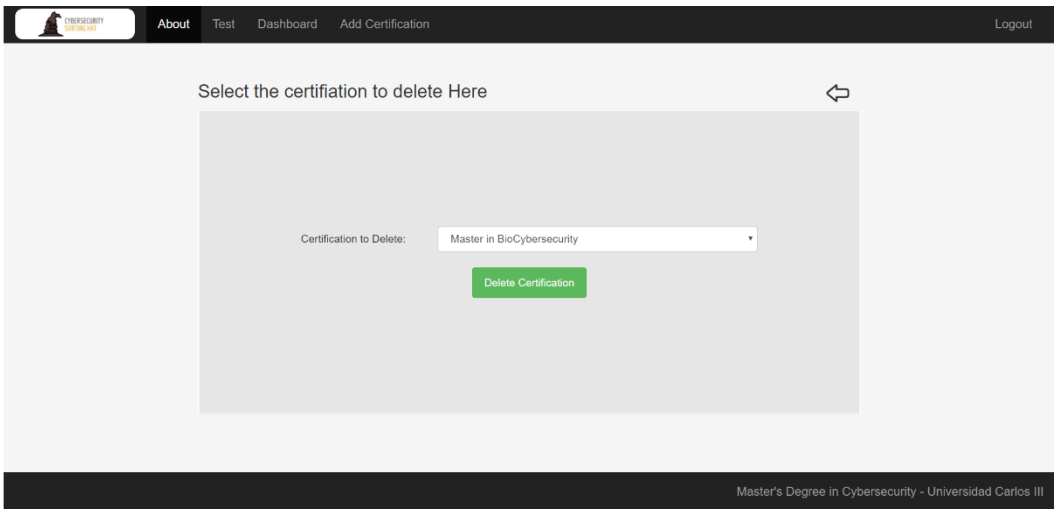


Figura 4.23 Vista de Borrar Certificación de Usuario

Ambas se componen de un campo selector en el que aparecen todas las opciones disponibles y de un botón que envía la información al backend.

- **Funcionalidad**

El funcionamiento de ambas opciones es muy sencillo. En cuanto a la opción de añadir una certificación, el usuario debe seleccionar una de las certificaciones almacenadas en la base de datos y de las que no dispone en su perfil y después pulsar en el botón inferior para añadir la vinculación entre los dos objetos. El diagrama que se observa a continuación explica esta funcionalidad.

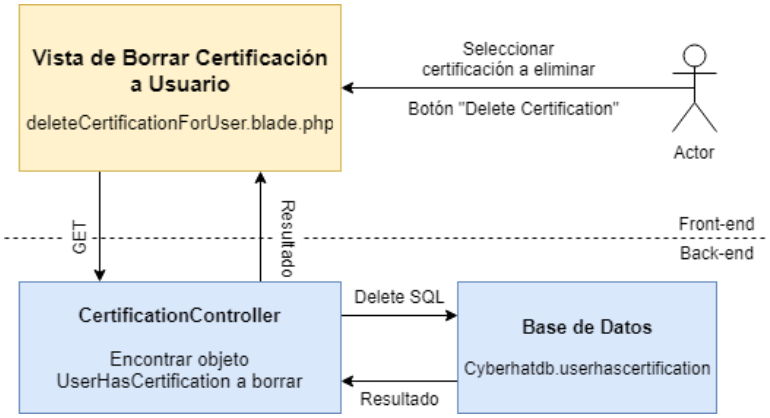


Figura 4.24 Diagrama de la funcionalidad de Añadir Certificación de Usuario

En cuanto a la función de borrar certificación, el usuario debe elegir entre una de las certificaciones que tiene enlazadas a su perfil y acto seguido pulsar el botón, lo cual deshará dicho enlace en la tabla. Se puede apreciar el intercambio de información presente en esta funcionalidad en la siguiente figura.

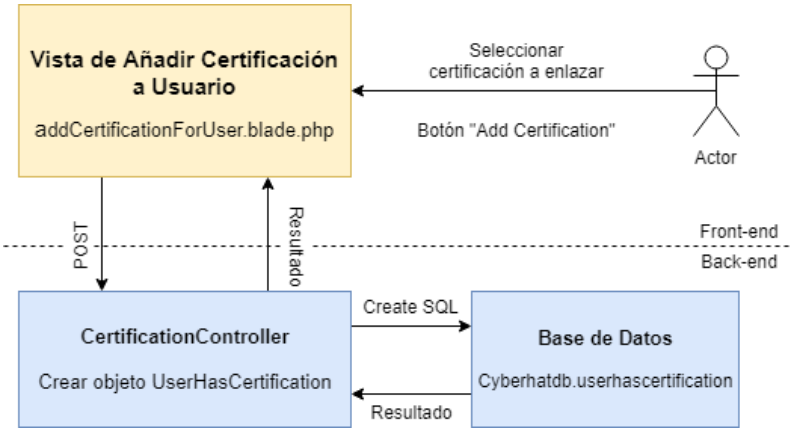


Figura 4.25 Diagrama de la funcionalidad de Borrar Certificación de Usuario

4.3.7. Test

La funcionalidad de test es sobre la que se desarrolla el resto de la aplicación. Nos permite encontrar los perfiles de ciberseguridad que más se adecúan a nuestras habilidades, destrezas y conocimientos. Esta funcionalidad era la única desarrollada completamente en la versión previa, por lo que en este proyecto sólo ha sido necesario adaptarlo a las necesidades de la nueva aplicación mejorada.

Se realiza utilizando los frameworks explicados en capítulos previos de este documento (NCWF) utilizando la fórmula de los TKSAs.

- **Bases de Datos**

En la primera versión, los datos resultantes del test sobre los roles de trabajo de ciberseguridad más adecuados se mostraban en pantalla una vez se realizaban los pasos necesarios para conseguir los resultados, pero no existía un enlace entre el usuario y los perfiles con su porcentaje.

En la nueva versión esto se convierte en una necesidad por la existencia de la funcionalidad de dashboard, la cual se explicará en el siguiente capítulo de este documento. Por ello se han creado dos nuevas tablas en la base de datos que vinculan al usuario con los perfiles y categorías más adecuados para ellos.

La primera se denomina “user_has_workrole” y en ella se enlazan los usuarios con los id de los distintos roles de trabajo que el test ha determinado más adecuados, y el porcentaje de similitud.

#	Nombre	Tipo
1	**workrole_id**	int(11)
2	**percentage**	float
3	**user_id**	int(11)

Figura 4.26 Estructura de la tabla user_has_workrole

La segunda es la tabla “user_has_category” y relaciona el porcentaje de similitud que se puede encontrar entre el usuario y las siete categorías existentes en nuestro test de perfiles de ciberseguridad.

#	Nombre	Tipo
1	user_id	int(11)
2	category_id	int(11)
3	percentage	float

Figura 4.27 Estructura de la tabla user_has_category

- **Funcionalidad**

La opción del test se realiza siguiendo tres pasos distintos. El primer paso corresponde en marcar todas las casillas de los TKSAs de las diferentes categorías que el usuario posee. Una vez realizada esta acción, se procederá a hacer clic en el botón “GO”, el cual se puede observar en la parte derecha de la pantalla.

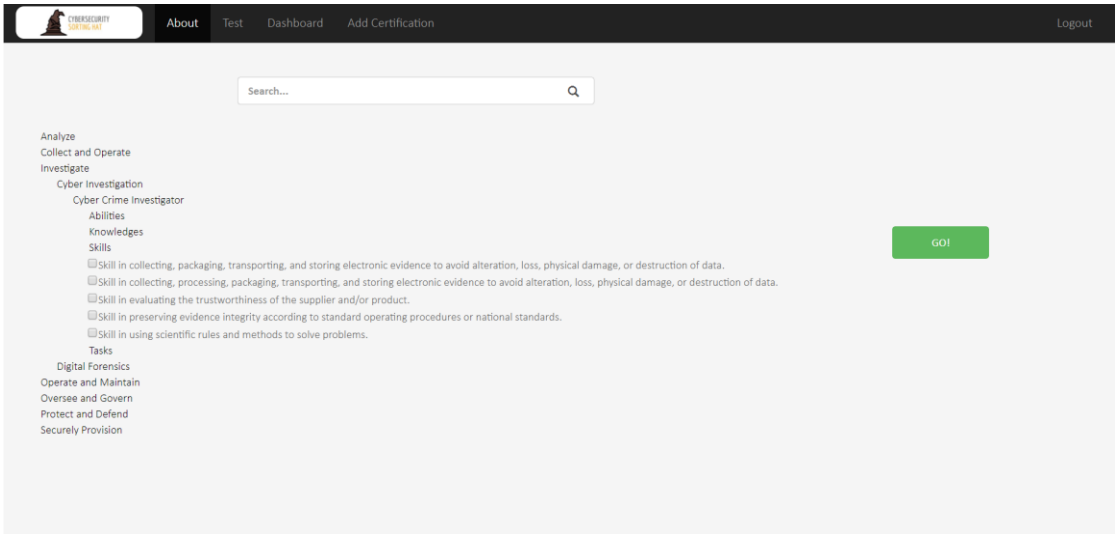


Figura 4.28 Primera pantalla del test

Esta acción nos llevará a la siguiente pantalla. Los TKSAs seleccionados se almacenarán en la base de datos y en esta pantalla podremos ver un resumen de los mismos para poder revisarlos antes de realizar el test final.

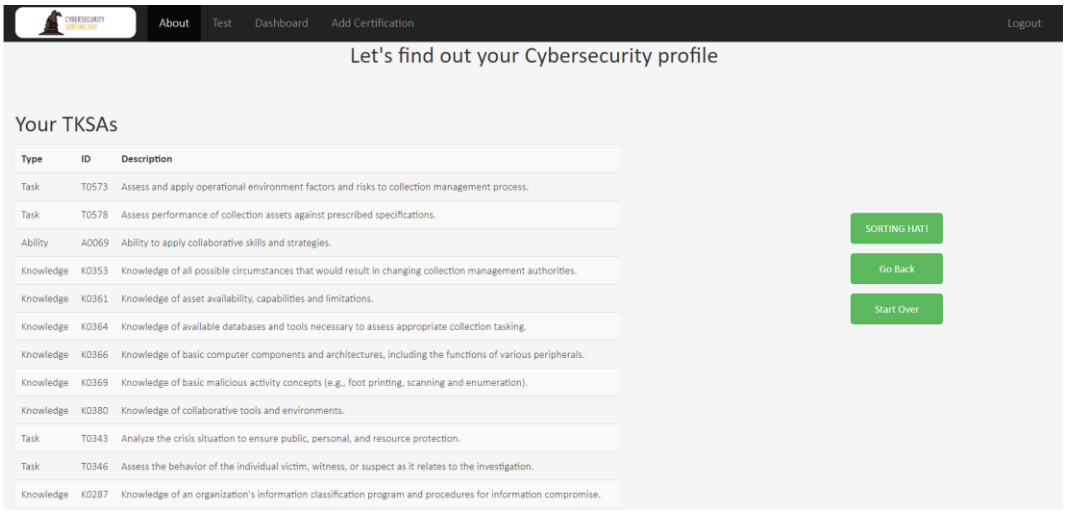


Figura 4.29 Segunda pantalla del test

Una vez comprobado que los TKSAs seleccionados son correctos, se procederá a pulsar el botón “SORTING HAT” de la sección derecha de la pantalla, el cual procederá a realizar el algoritmo de test. La tercera pantalla corresponde a los resultados del test, en la que podremos visualizar las tablas con los diez roles de trabajo más adecuados a las características del usuario junto a sus porcentajes, y al porcentaje de adecuación de las habilidades del usuario con las siete categorías principales.

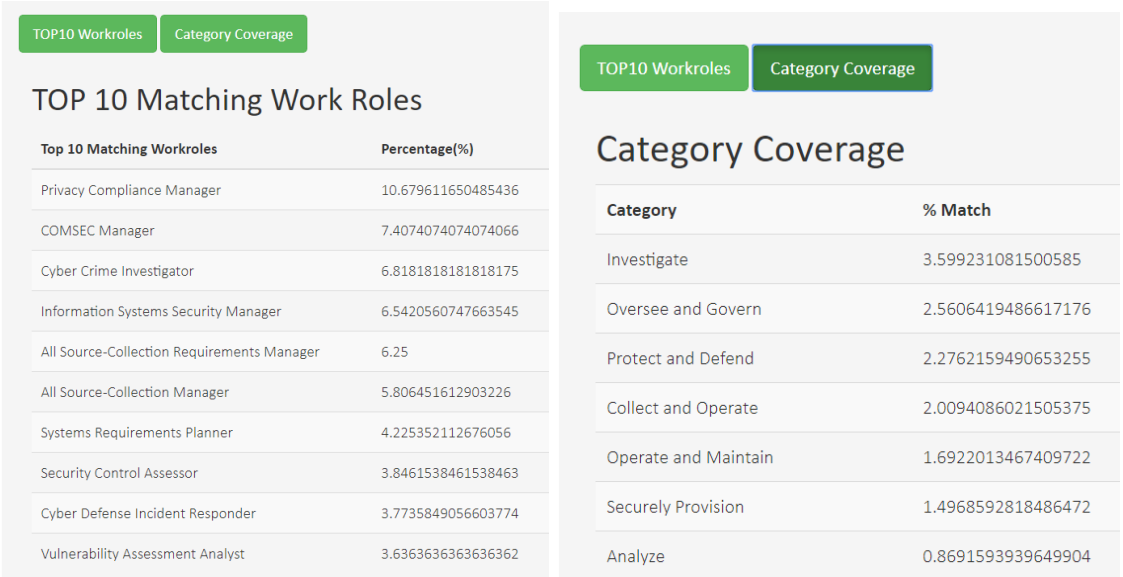


Figura 4.30 Detalles de tablas de resultados de test

El algoritmo para el cálculo de los porcentajes se puede observar en la siguiente figura.

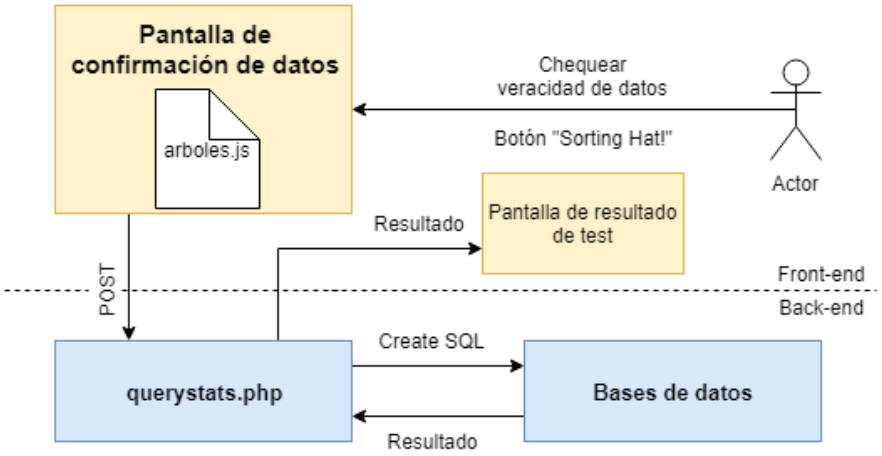


Figura 4.31 Diagrama de funcionalidad de test

En la última página, la cual muestra los resultados del test, podemos encontrar un botón para guardar los datos y salir. Esto guardará los resultados en las tablas mencionadas anteriormente y volver a la página inicial del test.

4.3.8. Dashboard

En la barra de navegación superior podemos encontrar la opción “Dashboard”. En esta sección podremos encontrar una representación gráfica de los resultados obtenidos en el test, tanto por el usuario actual, como un usuario medio.

Actualmente, sólo la sección de resultados del usuario y la división de roles de usuario están operativos, por lo que los resultados reflejados en esta sección son forzados por el desarrollador, y la implantación de un usuario medio se tendrá en cuenta como objetivo en futuras ampliaciones de la aplicación.

- **Bases de Datos**

En esta funcionalidad, no ha sido necesaria la creación de tablas adicionales, ya que los datos necesarios están almacenados en las tablas “user_has_workrole” y “user_has_category”, las cuales han sido explicadas en detalle en la sección anterior relacionada con la funcionalidad de la realización del test.

- **Funcionalidad**

Esta página se divide en cuatro partes diferenciadas. En las tres primeras, podemos encontrar dos gráficas circulares, la primera correspondiente a los datos del usuario que ha iniciado sesión en la aplicación y la segunda representa el mismo tipo de figura, pero relacionada con el usuario medio. La última representa la población de usuarios divididos en sus respectivos roles.

Figura 4.32 Gráfica de Roles de trabajo en el Dashboard

Las dos primeras gráficas que podemos encontrar corresponden a los diez roles de trabajo más adecuados para el usuario actual y medio. La información se recibe desde las tablas de la base de datos y se adecúa para su correcta visualización en la página.

De la misma forma se recibe la información de las categorías, pero en este caso al tener siete datos fijos, se procede a mostrar los datos almacenados en forma de gráfica de barras, para dotarlo de un aspecto más visual.

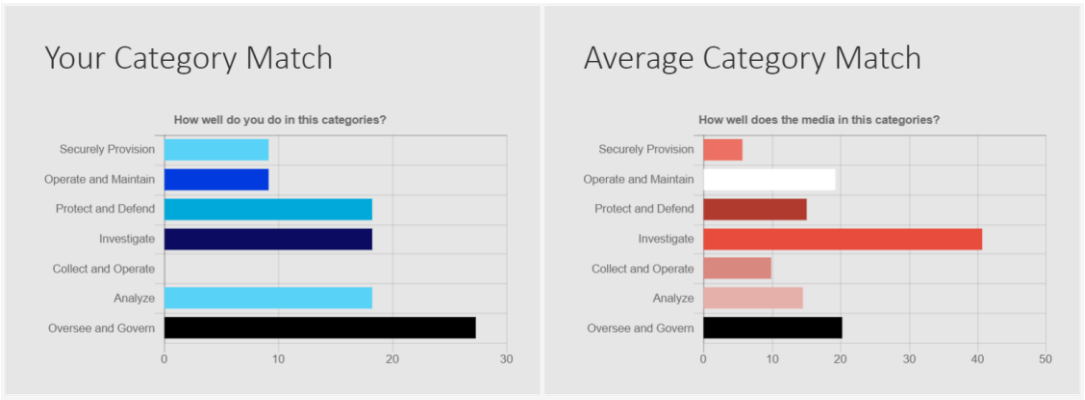


Figura 4.33 Gráfica de Categorías en el Dashboard

A continuación, encontramos otra gráfica circular en la que se pueden visualizar los porcentajes de similitud de las áreas de especialidad con las habilidades y destrezas del usuario. Las áreas de especialidad corresponden a una división intermedia entre roles de trabajo y categorías. Esto provoca que un área de especialidad pueda contener uno o más roles de trabajo.

Figura 4.34 Gráfica de Áreas de Especialidad en el Dashboard

Por último, podemos encontrar una gráfica de donut, en la cual se hace un estudio de los roles de usuario presentes en la aplicación y su posterior cálculo de porcentaje para adaptarlo a la gráfica.

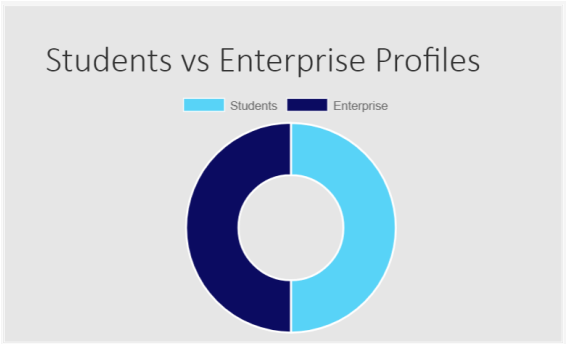


Figura 4.35 Gráfica de Comparación de Roles en el Dashboard

4.4. Entorno y herramientas de desarrollo

Para el desarrollo de la aplicación han sido necesarias varias herramientas para su correcto desarrollo y testeo. Uno de los pilares imprescindibles es un servidor web y el escogido para la aplicación es un servidor Apache, ya que es de código abierto, está presente en todas las plataformas y es el más extendido en la actualidad. [30]

La base de datos se desarrolla en el lenguaje SQL, y se utiliza un servidor MySQL para su administración. El criterio seguido es el mismo que para el servidor web, ya que es un software de código abierto, con gran aceptación en el mercado y con gran sencillez que permite futuros desarrollos sobre la base de datos actual.

Ambos se engloban en el software XAMPP, el cual ha sido el utilizado para el desarrollo de esta aplicación. XAMPP es un servidor independiente de plataforma de código libre. Te permite instalar de forma sencilla Apache en tu propio ordenador, sin importar tu sistema operativo. Su uso es gratuito e incluye además servidores de bases de datos como MySQL con su respectivo gestor phpMyAdmin. Incorpora también el intérprete de PHP, el intérprete de Perl, servidores de FTP como ProFTPD o FileZilla FTP Serve, etc. entre muchas opciones más. [31]

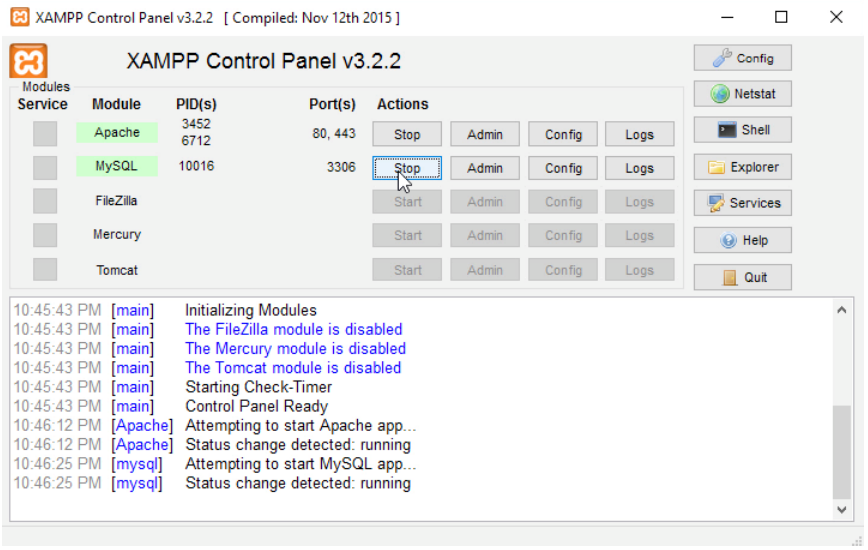


Figura 4.36 Panel de Control de Xampp

Para el desarrollo del código se ha utilizado el programa Microsoft Visual Studio Code. Visual Studio Code es un editor de código gratuito el cual incluye herramientas para realizar funciones de debug, gestión de repositorios Git y plug-ins para facilitar el desarrollo del código. [32]

4.5. Seguridad en la aplicación

La seguridad en internet se ha presentado durante todo este documento como una necesidad primordial en cualquier tipo de aplicación web y la búsqueda de esta es el objetivo de la aplicación desarrollada. Por lo tanto, se debe dotar a nuestra aplicación de los mismos mecanismos de seguridad que se esperan de una aplicación de gran calidad.

El OWASP es un organismo sin ánimo de lucro con base en Estados Unidos y creado en 2001, cuyo objetivo es el de permitir a las organizaciones concebir, desarrollar, adquirir, operar y mantener aplicaciones en las que se pueda confiar. [33]

Este organismo publica cada año un documento en el que se especifican los 10 riesgos más críticos que pueden presentar las aplicaciones web. El último que ha salido a la luz es el de 2017, el cual se refleja en la siguiente tabla:

OWASP Top 10 - 2017
A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE) [NEW]
A5:2017-Broken Access Control [Merged]
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization [NEW, Community]
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Figura 4.37 Top 10 de vulnerabilidades del OWASP [34]

En los siguientes apartados se exponen brevemente las vulnerabilidades con más posibilidades de ocurrir en la aplicación, y las medidas que se han tomado para asegurar la aplicación ante ellas.

4.5.1. Inyección

El término "Inyección SQL" hace referencia a un ataque contra un sitio o aplicación web en el que se añade código de lenguaje de consulta estructurado (SQL) a un campo de entrada de un formulario web con el objetivo de acceder a una cuenta o modificar los datos. [35]

Estos ataques son muy comunes en páginas con registro e inicio de sesión con usuarios como la nuestra, por lo que debemos implementar recursos para protegerla.

La solución que se ha planteado para esta posible vulnerabilidad reside en dos factores. El primero es ocultar la información enviada en el form usando una petición “POST” de HTTP. Adicionalmente, se utilizan los recursos que nos otorga Laravel para la autenticación, pudiendo almacenar en la base de datos versiones encriptadas de la contraseña en vez de tener la información a la vista, por lo que, aunque el atacante pudiera conseguir esa información, no le sería de ninguna utilidad.

4.5.2. Cross-Site Scripting

El XSS o Cross-Site Scripting es un tipo de vulnerabilidad informática típico de las aplicaciones web, que permite a una tercera persona inyectar código malicioso de Javascript u otro lenguaje similar en las páginas web visitadas por el usuario. Se usa para extraer información delicada de la página web, como los nombres de usuario y sus contraseñas en el caso de nuestro portal. [36]

Para evitar este tipo de ataques, se implementa una comprobación de los datos introducidos en cualquier tipo de form existente en la aplicación, usando el comando “require” de Laravel. Por esto, los campos deben cumplir una serie de características para que sean validados por la aplicación y sean transmitidos al siguiente nivel. Si no los cumplen, se producirá una excepción.

4.5.3. Gestión de autenticación y de sesión

Las funcionalidades relacionadas con el mantenimiento de sesiones son críticas en aplicaciones como la expuesta en este documento y frecuentemente no se protegen de forma necesaria. Esto permite a posibles atacantes tener acceso a información sensible, como claves o tokens de sesión, o incluso para intentar asumir las identidades de otros usuarios a través de los datos robados.

Para proteger la aplicación contra este tipo de posibles ataques, el método de gestión de Laravel incluye un token encriptado, el cual se utiliza para mantener la sesión del usuario mientras este esté conectado. Si se intenta atacar esta información, el resultado obtenido no podrá ser utilizado contra los usuarios de la aplicación debido a que la clave para desencriptar el token está almacenada en los módulos de la aplicación Laravel.

4.6. Evaluación de Software

Uno de los requisitos más importantes en el desarrollo software es la calidad del mismo, por lo que, una vez realizado el desarrollo completo de la aplicación, conviene comprobar que el portal desarrollado cumple con los pilares básicos de calidad de software.

- **Funcionalidad:** Para que cumpliera este requisito, la aplicación debe realizar el trabajo deseado. En este caso, la aplicación lo cumple, ya que la funcionalidad principal, la de test, realiza su trabajo de forma correcta. Asimismo, el resto de las funcionalidades presentes en la aplicación también desempeñan su función correctamente.

- **Eficiencia:** Este requisito refleja si la aplicación responde con una velocidad apropiada. En la aplicación desarrollada en este proyecto, ninguna tarea requiere de tiempo excesivo para realización. El tiempo medio de carga de una página web oscila entre los 4,2 y los 4,5 segundos, y ninguna de nuestras funcionalidades supera en gran medida estos tiempos. Por estas razones, se puede concluir que la aplicación cumple con los estándares de eficiencia requeridos.

- **Usabilidad:** Este requisito está relacionado con la satisfacción del usuario a la hora de visitar el portal. Un examen más exhaustivo de este requisito se puede observar en el siguiente capítulo, relacionado con las pruebas de experiencia de usuario, pero en general, todos los usuarios de prueba que tuvieron acceso al portal manifestaron su satisfacción y comodidad a la hora de navegar por las distintas partes de la aplicación.

- **Mantenibilidad:** Para el cumplimiento de este requisito, la aplicación debe de ser mantenible con un bajo coste. El código de la presente aplicación está escrito de forma sencilla y concisa, por lo que cualquier tipo de mantenimiento o expansión de la aplicación debe ser sencilla para el desarrollador encargado de la tarea.

Después de comprobar los anteriores requisitos de calidad de software, se puede llegar a la conclusión de que la aplicación cumple con los estándares de calidad necesarios para un desarrollo software.

5. PRUEBAS DE EXPERIENCIA DE USUARIO

Una vez completado el desarrollo de la aplicación, se procedió a comenzar con las pruebas de experiencia de usuario. El objetivo de estas era testear la aceptación que tendría la aplicación en un grupo de posibles usuarios.

Para realizar este experimento, se escogieron cuatro personas con perfiles diferenciados, pero que desarrollan o planean desarrollar su carrera profesional en el área de las telecomunicaciones y la informática. Entre los elegidos encontramos tres estudiantes de distintos grados de la rama de ingeniería de telecomunicaciones y un desarrollador web con varios años de experiencia en el sector.

Al tratarse de una aplicación completa y totalmente funcional, se pidió a los usuarios que probaran todas las funcionalidades existentes y que grabaran este proceso y las sensaciones que tenían en el transcurso de la prueba. Al finalizar la prueba se les entregó un cuestionario con varias preguntas para conocer su experiencia con la aplicación. Los resultados de este cuestionario se pueden encontrar en el Anexo B de este documento.

Para realizar la grabación de pantalla se utilizó el software ScreenCastify para Google Chrome. Este programa es una extensión del navegador, el cual permite grabar la pantalla y el micrófono de forma sencilla y gratuita [37].

Se probarán todas las funcionalidades presentes en la aplicación y que se cumplen los requisitos fijados al comienzo del proyecto a través de las siguientes pruebas:

- Registrar un usuario en la aplicación e iniciar sesión en el portal con él.
- Acceso a la página de perfil del usuario y edición de alguna de sus credenciales.
- Creación de una certificación y enlazado de la misma con el perfil de usuario.
- Cumplimentación del test y comprobación de resultados obtenidos en este.
- Chequeo de las estadísticas del usuario en la pantalla de dashboard.

Tras analizar las pruebas y las respuestas a los cuestionarios otorgados a los usuarios posteriormente, se llegó a las siguientes conclusiones:

- El 100% de los usuarios consiguió registrar un perfil de usuario e iniciar sesión con el mismo sin ningún tipo de problema.

- El 75% de los usuarios entrevistados piensa que los enlaces de la barra de navegación superior son suficientemente descriptivos. Asimismo, un 50% declaró que echó en falta más funcionalidades en el perfil de usuario.

- Todos los entrevistados fueron capaces de realizar el test sin ningún tipo de problema, aunque uno de los cuatro entrevistados declaró no comprender los resultados reflejados en el Dashboard. Es necesario aclarar que para la realización del test se les otorgó una breve explicación acerca del funcionamiento del mismo y de los TKSAs.

- Un 50% de los usuarios que realizaron la prueba cree que debería incluirse más imaginería de la universidad en la aplicación, con el objetivo de que sea se vea de forma clara el organismo para el que fue creada.

Para concluir este capítulo, es necesario apuntar que, adicionalmente a todas las pruebas y cuestionarios realizados, la gran mayoría de los usuarios que testearon la aplicación apuntaron que se sentían cómodos con ella en el transcurso de la prueba, y las notas que otorgaron al portal reflejan que la sensación que tuvieron fue satisfactoria.

6. PLANIFICACIÓN Y PRESUPUESTO

En este capítulo se hará un análisis de la planificación que se ha llevado a cabo para este proyecto, tanto temporal como de costes.

6.1. Planificación temporal

El proyecto se ha desarrollado a lo largo de cinco meses, con un parón de un mes entre mediados de marzo y mediados de abril por razones de salud, por lo que la planificación inicial tuvo que ser adaptada a la nueva situación. Antes de comenzar el desarrollo del proyecto, se llevó a cabo una planificación con el objetivo de coordinar a todas las partes incluidas en este proyecto.

Esta planificación se siguió durante todo el desarrollo del proyecto, y se puede observar en el diagrama de Gantt contenido en la siguiente página. En él se incluyen las tareas realizadas por cada desarrollador, en diferentes colores, además de la distribución en el tiempo de cada una de las tareas necesarias para el desarrollo de la aplicación.

TABLA 6.1. PLANIFICACIÓN TEMPORAL DEL PROYECTO

6.2. Presupuesto del proyecto

Al tratarse de un proyecto software, no se ha necesitado de capital externo para el comienzo del proyecto. Los costes asociados se derivarán del tiempo empleado por los desarrolladores en el progreso del proyecto.

El desarrollador encargado de llevar a cabo este proyecto es un estudiante de último curso de la Universidad Carlos III de Madrid, por lo que se le considera un desarrollador Junior, debido a que no tiene gran experiencia de trabajo en el sector. Este hecho representa un gran ahorro de costes, ya que una persona de estas características tiene los conocimientos necesarios para el desarrollo de una aplicación como la presentada en este proyecto, con un coste menor.

Para determinar el coste que supondría el sueldo de un programador con dichas características nos ayudamos de la calculadora salarial de la empresa británica de recursos humanos Hays. [38]

Según los resultados ofrecidos por la calculadora, en la Comunidad de Madrid, el sueldo anual de un desarrollador de PHP con una experiencia de 0 a 2 años oscila entre los 25.000 y los 29.000€. Se decidió seleccionar como posible sueldo la opción superior, dado que el desarrollador de este proyecto también realiza ciertas tareas de gestión de experiencia de usuario. Este cálculo resulta en un total de 13,94€/hora [39].

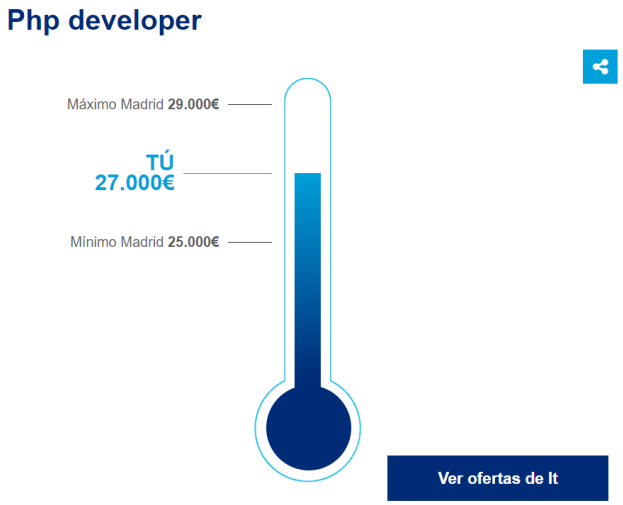


Figura 6.1 Calculadora de sueldo anual desarrollador PHP [38]

Por otra parte, hemos de calcular también el sueldo asociado al tutor del proyecto. El sueldo medio de un profesor titular de universidad en España está alrededor de los 54.000€ anuales [40], lo que resulta en unos 25,96€/hora [39].

Con estos datos, se ha realizado una estimación de horas de trabajo por cada tarea y el coste de cada una de estas, que se puede ver reflejado en la siguiente tabla. Las seis primeras tareas se engloban en el grupo de preparación, las cuatro siguientes comprenden el área de desarrollo y las cuatro últimas componen el grupo de la memoria y revisión.

TABLA 6.2. TABLA DE COSTES DEL PROYECTO

Tarea	Horas	Sueldo/Hora	€/Tarea
Especificación De Requisitos	6	25,96 €	155,76 €
Lectura de Documentación	20	13,94 €	278,80 €
Formación	40	13,94 €	557,60 €
Estudio del Proyecto Base	15	13,94 €	209,10 €
Planificación de soluciones	8	13,94 €	111,52 €
Decisión de soluciones	5	25,96 €	129,80 €
Diseño	30	13,94 €	418,20 €
Desarrollo de código	160	13,94 €	2.230,40 €
Pruebas	35	13,94 €	487,90 €
Comprobación funcionamiento	5	25,96 €	129,80 €
Escritura de la memoria	110	13,94 €	1.533,40 €
Corrección de la memoria	15	25,96 €	389,40 €
Revisión final del proyecto	5	13,94 €	69,70 €
Total Proyecto			6.701,38 €

Trabajador encargado de la tarea
Ana Isabel González-Tablas Ferreras
Javier Sanz López

Los resultados arrojados por la tabla anterior son claros, la mayor parte del tiempo se emplea en el desarrollo del código de la aplicación. Estas tareas representan un total de 230 horas, lo cual se traduce en el 50,66% del tiempo empleado en el total de la aplicación.

La realización de tareas relacionadas con la memoria y planificación emplean una cantidad de tiempo bastante similar. Las primeras ocupan un total de 130 horas, lo que se traduce en un 28,63%, y las segundas se desarrollan a lo largo de 94 horas, otorgándoles un 20,70% del tiempo total empleado en este proyecto.

7. MARCO REGULATORIO

Como hemos descrito a lo largo de todo este documento, la ciberseguridad es uno de los temas que ha cobrado mayor importancia en los últimos años en el área tecnológica. Internet y todas las tecnologías que han aparecido y crecido junto a ella han provocado la aparición de nuevas amenazas contra la seguridad nacional que ni siquiera se podían haber imaginado. En los primeros años de existencia de internet, los países carecían de legislación acerca del tema, pero con el tiempo creció la necesidad de regular la ciberseguridad, y la normativa se ha tenido que adaptar a las necesidades de protección en el mundo virtual que demandan los ciudadanos y las empresas. [41]

En este capítulo, se expondrá la regulación existente en la actualidad en materia de ciberseguridad presente a nivel estatal y europeo.

7.1. Directiva Europea NIS

Como parte de la estrategia de ciberseguridad de la UE, la Comisión Europea propuso la Directiva sobre seguridad de las redes y de la información o NIS. Es la primera pieza de la legislación sobre ciberseguridad a escala de la UE. El objetivo es mejorar la ciberseguridad en toda la UE.

La directiva se adoptó en 2016 y posteriormente todos los Estados miembros de la UE han comenzado a adaptar la legislación nacional a las directrices comunitarias. La UE da a los países de la UE cierto grado de flexibilidad para tener en cuenta las circunstancias nacionales, por ejemplo, para reutilizar las estructuras organizativas existentes o para alinearse con la legislación nacional existente.

La Comisión Europea mantiene un mapa que muestra el estado de la transposición de la Directiva NIS en todos los Estados miembros de la UE. [42]

7.2 Ley Orgánica de Protección de Datos

En noviembre de 2017 fue aprobada por el Consejo de Ministros la nueva Ley de Protección de Datos (LOPD) que comenzará a aplicarse el próximo 25 de mayo de 2018. Esta ley viene a sustituir a la LOPD vigente y en ella encontramos una serie de cambios que afectan a la mayoría de las empresas de nuestro país. Por eso es importante conocer las principales novedades.

En el nuevo texto, se elimina el concepto de consentimiento tácito y se refuerza convirtiéndose en una acción más positiva y expresa. Además, aparece la figura del Delegado de Protección de Datos. El principio de transparencia también se recoge en la nueva ley. Se refiere a que los usuarios deberán ser informados del tratamiento de los datos, siempre que les afecte, de forma clara y concisa. Por último, cabe destacar que promueve la existencia de mecanismos de autorregulación en el sector público y privado. [43]

Figura 7.1 Novedades en la Regulación General de Protección de Datos [44]

7.3. Ley de Conservación de Datos

El objetivo de esta Ley consiste en la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los organismos competentes siempre que sea necesario previa autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal.

Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. [45]

8. CONCLUSIONES

En este capítulo se analizan las conclusiones obtenidas una vez finalizado el desarrollo del proyecto, tanto personales como de cumplimiento de objetivos. Además, se exploran futuras vías de desarrollo de la aplicación.

8.1. Cumplimiento de Objetivos Iniciales

Al comienzo del desarrollo de este proyecto, se marcaron unos objetivos iniciales. En este apartado, se analiza el nivel de cumplimiento de estos en la aplicación final.

- **Objetivo Inicial:** Creación de bases de datos de usuarios con protección intensiva de las mismas.

- **Evaluación Final:** Utilizando los recursos que nos proporciona el framework Laravel, los datos de usuario se protegen utilizando cifrado para las contraseñas. Gracias a ello, se previenen los ataques de inyección SQL.

- **Objetivo Inicial:** Inclusión de middleware que fomentara la coordinación front-end/back-end.

- **Evaluación Final:** Se ha cumplido este objetivo, al implementar funciones de enrutamiento a través de los sistemas proporcionados por el framework PHP.

- **Objetivo Inicial:** Autenticación de usuarios de forma segura y gestión de sesiones.

- **Evaluación Final:** La gestión del mantenimiento de sesiones se realiza de forma segura. El método Auth de Laravel permite autenticar el usuario a través de la desencriptación de la contraseña y la sesión se mantiene a través de un token.

- **Objetivo Inicial:** Creación de vistas para nuevas funcionalidades, de las que carece la aplicación.

- **Evaluación Final:** Se han creado nuevas vistas para las funcionalidades de: añadir certificación, perfil de usuario, edición de este y adición/borrado de certificaciones de un usuario.

- **Objetivo Inicial:** Creación de modelos de objetos presentes en la aplicación (usuarios, certificaciones…).

- **Evaluación Final:** Se han creado modelos para todos los objetos creados a partir de las tablas de la base de datos (usuarios, certificaciones, sus enlaces…) con el objetivo de facilitar su gestión.

- **Objetivo Inicial:** Utilización de los recursos del TFG de Sandra Sánchez y búsqueda de cohesión con los elementos de nuevo desarrollo.

- **Evaluación Final:** Las vistas creadas por Sandra Sánchez han sido utilizadas en este proyecto, y las que han sido creadas han seguido las pautas establecidas por dicho TFG.

- **Objetivo Inicial:** Adaptación del proyecto inicial, creado por Javier Vilas, dentro de la nueva plataforma.

- **Evaluación Final:** La funcionalidad de test desarrollada en el trabajo de fin de Master del alumno Javier Vilas ha sido respetada en todo momento en la aplicación final, añadiendo nuevas funcionalidades para adecuarlo a la nueva plataforma.

8.2. Conclusiones personales

El proceso de elección de un trabajo de Fin de Grado se extendió durante varios meses, ya que buscaba algo que pudiera ser de valor añadido para otras personas y que, además, supusiera un reto para mí como ingeniero y desarrollador.

En el transcurso de mis estudios del Grado de Ingeniería Telemática en la Universidad Carlos III de Madrid, he ido adquiriendo un gran interés tanto por la programación como por la ciberseguridad y decidí que mi deseo era desarrollar mi carrera profesional en estas dos áreas de especialización.

Por lo tanto, cuando la tutora de este proyecto me presentó la idea me resultó muy llamativa, ya que aunaba los dos factores que más me atraían. Por una parte, podía desarrollar mis capacidades como programador ya que el lenguaje PHP no se imparte en el Grado de Ingeniería Telemática y, además, aprender sobre perfiles de trabajo de ciberseguridad.

En este momento, una vez finalizado el desarrollo del proyecto, puedo afirmar que los objetivos marcados en el párrafo anterior se han cumplido, lo que me supone una gran satisfacción personal. El desarrollo de la aplicación completa me ha ayudado a adquirir nuevos conocimientos en el desarrollo de aplicaciones PHP, lo cual será de utilidad a lo largo de mi carrera profesional. Asimismo, he podido ampliar mis conocimientos en el campo de la ciberseguridad, uno de los más punteros en la actualidad.

Por último, cabe destacar que la aplicación va a ser de utilidad para otros alumnos de la universidad en la que he desarrollado mis estudios. El hecho de que otros alumnos puedan beneficiarse de la aplicación desarrollada en este proyecto para su futura carrera profesional me llena de orgullo, y me hace sentir que he podido devolver algo valioso a la institución que me permitió desarrollar mis estudios y lanzar mi carrera profesional.

8.3. Futuras líneas de trabajo

Las aplicaciones web están en constante mejora y, por lo tanto, en el transcurso del desarrollo de la presentada en este proyecto, se han definido futuras posibles mejoras que pueden ser implementadas.

- Ampliación del perfil de usuario: imagen de usuario, nuevos datos, subida de currículo a la plataforma…

- Sistema de conexión entre las certificaciones y el test: Las certificaciones corresponden a un perfil determinado, y deberían marcarse automáticamente en el test los TKSAs asociados a dicho perfil.

- Función de recuperación de contraseña: Implementación de una opción en la página de inicio de recuperación de contraseña en caso de que el usuario la haya olvidado. Además, se debe implementar la seguridad asociada a esta opción.

- Creación de la versión en castellano del portal: La app debería de estar disponible en varios idiomas, al menos inglés y castellano.

- Descarga de informes, histórico del usuario y corrección de la barra de búsqueda de TKSAs en el Test

ANEXO A: PRUEBAS DE EXPERIENCIA DE USUARIO

TABLA A.1. USUARIO G.F.S [46]

Cuestión	Respuesta
Nombre del usuario de prueba	G.F.S
¿Cuál es su ocupación profesional?	Estudiante de Ingeniería Telemática en la Universidad Carlos III.
¿Es suficiente la información que se ofrece en pantalla para saber a qué institución corresponde el sitio?	Hay cierta información, como por ejemplo en la barra inferior, pero no es suficiente.
¿Encontró alguna dificultad a la hora de registrar un usuario en la aplicación e iniciar sesión con él? En caso afirmativo, ¿Podría indicarnos cuál/es?	No, he conseguido hacer las dos cosas sin problema.
En general, ¿los nombres de los enlaces son suficientemente descriptivos acerca de las páginas a las que llevan? En particular, ¿hubo alguno que lo confundió?	En mi opinión todos son bastante claros acerca de a que página redirigen.
¿Cree que el perfil de usuario tiene las características adecuadas? ¿Añadiría alguna funcionalidad adicional?	El perfil de usuario es suficiente, aunque podría tener ciertas mejoras, como una imagen de perfil.
¿Ha experimentado algún tipo de dificultad a la hora de realizar la funcionalidad de test?	No, la realización del test es sencilla.
¿Entendió adecuadamente los datos reflejados en la pantalla de Dashboard?	Sí, los datos se reflejan de forma clara en el dashboard.
Para concluir, ¿Qué nota general de 1 a 10 le otorgaría a la aplicación Cybersecurity Sorting Hat?	8

TABLA A.2. USUARIO J.S.L [46]

Cuestión	Respuesta
Nombre del usuario de prueba	J.S.L
¿Cuál es su ocupación profesional?	Estudiante de Ingeniería de Tecnologías de Telecomunicaciones en la Universidad Carlos III.
¿Es suficiente la información que se ofrece en pantalla para saber a qué institución corresponde el sitio?	Sí, es suficiente, ya que está presente en la parte inferior en todas las pantallas.
¿Encontró alguna dificultad a la hora de registrar un usuario en la aplicación e iniciar sesión con él? En caso afirmativo, ¿Podría indicarnos cuál/es?	No he encontrado ninguna dificultad, me ha resultado un proceso muy sencillo y funciona correctamente.
En general, ¿los nombres de los enlaces son suficientemente descriptivos acerca de las páginas a las que llevan? En particular, ¿hubo alguno que lo confundió?	Sí, el nombre de los enlaces te deja muy claro a qué opción vas a acceder si clicas en ellos.
¿Cree que el perfil de usuario tiene las características adecuadas? ¿Añadiría alguna funcionalidad adicional?	El perfil de usuario tiene las características suficientes. Cualquier adición sería solo decorativa.
¿Ha experimentado algún tipo de dificultad a la hora de realizar la funcionalidad de test?	No, todo el proceso del test me ha resultado sencillo e intuitivo.
¿Entendió adecuadamente los datos reflejados en la pantalla de Dashboard?	Sí, las gráficas son una manera muy visual de mostrar los datos obtenidos en el test.
Para concluir, ¿Qué nota general de 1 a 10 le otorgaría a la aplicación Cybersecurity Sorting Hat?	8.5

TABLA A.3. USUARIO R.L.M [46]

Cuestión	Respuesta
Nombre del usuario de prueba	R.L.M
¿Cuál es su ocupación profesional?	Desarrollador de aplicaciones web en empresa de consultoría.
¿Es suficiente la información que se ofrece en pantalla para saber a qué institución corresponde el sitio?	Hay cierta mención, pero no es suficiente, se necesita mucha más información en todas las pantallas
¿Encontró alguna dificultad a la hora de registrar un usuario en la aplicación e iniciar sesión con él? En caso afirmativo, ¿Podría indicarnos cuál/es?	No. Realicé el proceso con facilidad
En general, ¿los nombres de los enlaces son suficientemente descriptivos acerca de las páginas a las que llevan? En particular, ¿hubo alguno que lo confundió?	Algunos son descriptivos, pero quizá falte algo más de concreción en otros. Especialmente la opción dashboard.
¿Cree que el perfil de usuario tiene las características adecuadas? ¿Añadiría alguna funcionalidad adicional?	El perfil de usuario tiene las características básicas, pero requiere de varias más para poder dotarlo de cierta calidad.
¿Ha experimentado algún tipo de dificultad a la hora de realizar la funcionalidad de test?	No. He realizado el test con normalidad.
¿Entendió adecuadamente los datos reflejados en la pantalla de Dashboard?	Si. Los datos se entienden de forma adecuada en las gráficas.
Para concluir, ¿Qué nota general de 1 a 10 le otorgaría a la aplicación Cybersecurity Sorting Hat?	7.5

FIGURA A.4. USUARIO O.S.G [46]

Cuestión	Respuesta
Nombre del usuario de prueba	O.S.G
¿Cuál es su ocupación profesional?	Estudiante de Ingeniería de Sistemas de Telecomunicaciones en la Universidad Carlos III.
¿Es suficiente la información que se ofrece en pantalla para saber a qué institución corresponde el sitio?	Sí, es suficiente con lo que contiene la aplicación.
¿Encontró alguna dificultad a la hora de registrar un usuario en la aplicación e iniciar sesión con él? En caso afirmativo, ¿Podría indicarnos cuál/es?	No. Los dos procesos he podido hacerlos sin ninguna dificultad.
En general, ¿los nombres de los enlaces son suficientemente descriptivos acerca de las páginas a las que llevan? En particular, ¿hubo alguno que lo confundió?	Todos los enlaces de la barra de navegación superior son descriptivos, dan a entender perfectamente que opción representan.
¿Cree que el perfil de usuario tiene las características adecuadas? ¿Añadiría alguna funcionalidad adicional?	A mi parecer el perfil de usuario cuenta con las funcionalidades suficientes, por lo que no sería necesario añadir ninguna más.
¿Ha experimentado algún tipo de dificultad a la hora de realizar la funcionalidad de test?	No, el proceso de test se realizó sin dificultades.
¿Entendió adecuadamente los datos reflejados en la pantalla de Dashboard?	Encontré ciertas dificultades para entender los datos del dashboard, quizá sería útil implementar algo de información adicional para el usuario.
Para concluir, ¿Qué nota general de 1 a 10 le otorgaría a la aplicación Cybersecurity Sorting Hat?	9

ANEXO B: MANUAL DE INSTRUCCIONES DE USO

Para el despliegue de la aplicación, se han de seguir unos sencillos pasos que se detallan en este capítulo. Todo el despliegue está explicado usando el programa XAMPP, ya que se trata del utilizado durante todo el desarrollo del proyecto. Para usar programas similares, se debe consultar su documentación.

Antes de proceder al despliegue, es importante reseñar que se debe copiar la carpeta que contiene el código de la aplicación llamada “SortingHat” dentro de la carpeta “htdocs”, la cual se encuentra en el directorio de XAMPP.

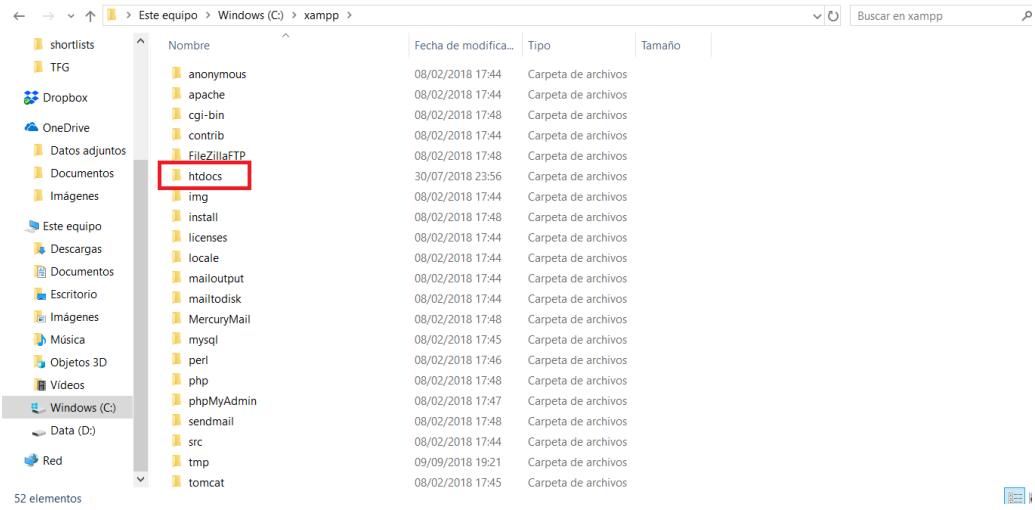


Figura B.1. Localización de la carpeta htdocs en el directorio de XAMPP

1. Desplegar el servidor Apache y las bases de datos

El primer paso que debemos seguir es encender el servidor web y el de SQL que contendrá las bases de datos necesarias para la aplicación.

Para ello, abrimos el programa XAMPP. En su pantalla principal nos encontraremos diferentes opciones de servidores que podemos iniciar. Para el funcionamiento de nuestra aplicación sólo son necesarios los dos primeros: el servidor Apache y MySQL. Por lo tanto, seleccionamos la opción “Start” en ambos, y la pantalla debería de verse como la siguiente imagen:

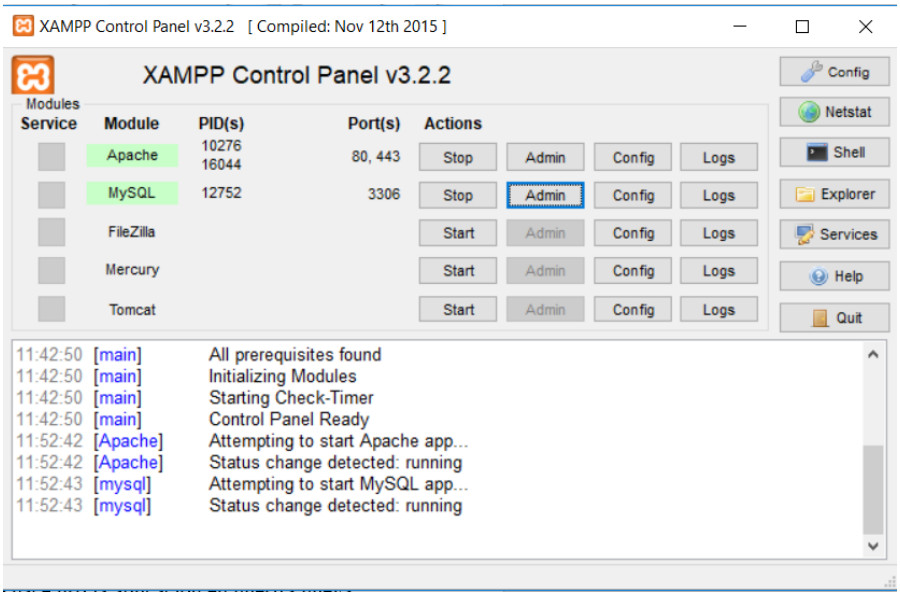


Figura B.2. Servidores desplegados en XAMPP

2. Cargar la base de datos

Una vez realizado el paso anterior, hemos de cargar la base de datos sobre la que funciona la aplicación en el gestor de MySQL. Por lo tanto, hemos de seleccionar la opción "Admin" para MySQL en la pantalla de XAMPP. Esto abrirá una pestaña del navegador predeterminado, en el que se puede ver el administrador de SQL.

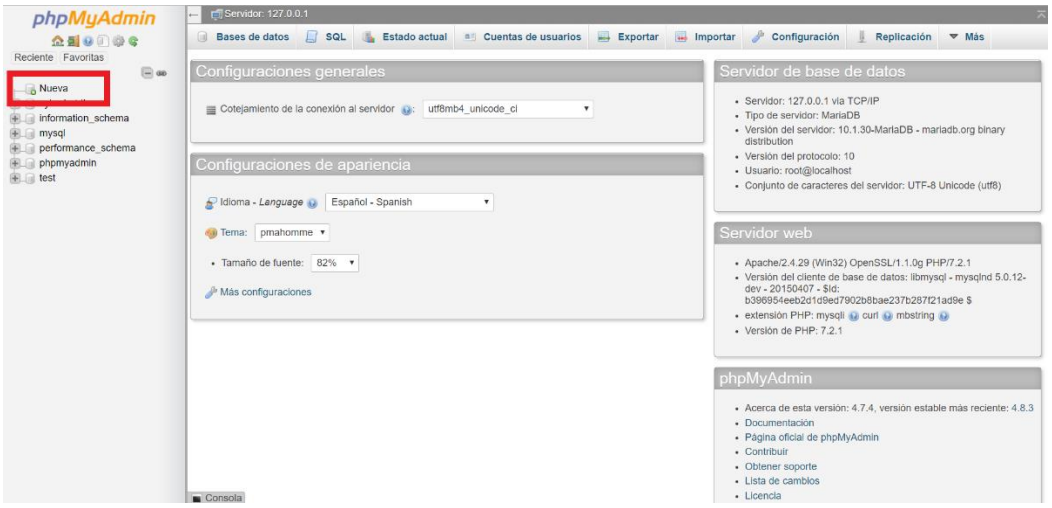


Figura B.3 Página principal de PHPMyAdmin

Dentro de esta página, debemos de elegir la opción “Nueva” de la parte izquierda de la vista. Esto nos redirigirá a otra página, en la cual podemos elegir el nombre de la nueva base de datos. Es importante que la nombremos “cyberhatdb”, ya que de otra forma la aplicación no la reconocería. Una vez realizado este paso nuestra nueva base de datos debería aparecer en la lista.

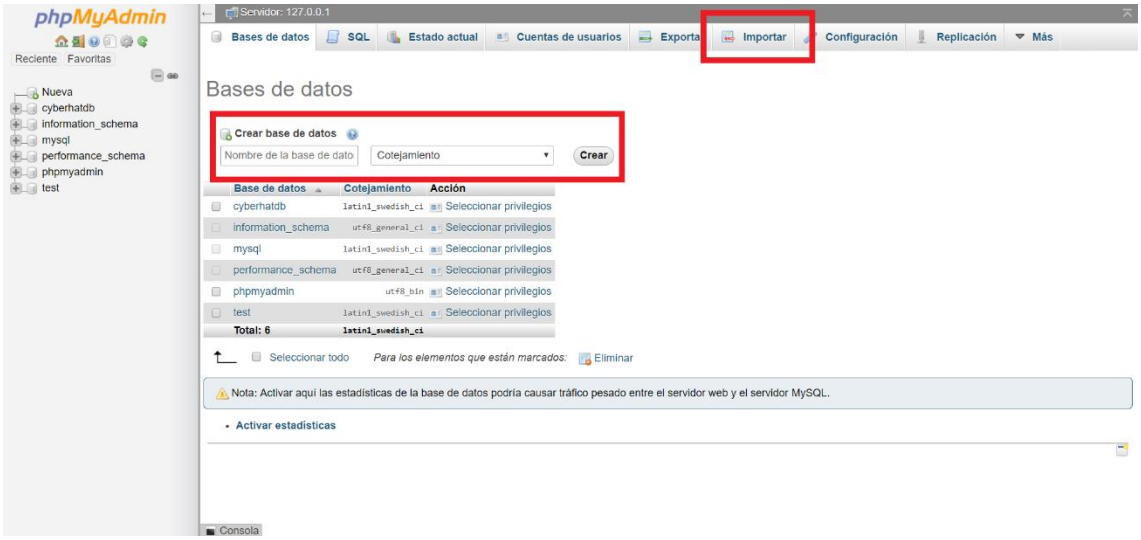


Figura B.4. Página de añadir base de datos en PHPMyAdmin

Por último, debemos cargar las tablas de las que hace uso la aplicación en nuestra nueva base de datos. Para ello debemos seleccionar la opción “Importar” de las presentes en la barra superior. Esta acción nos redirigirá a la siguiente página.

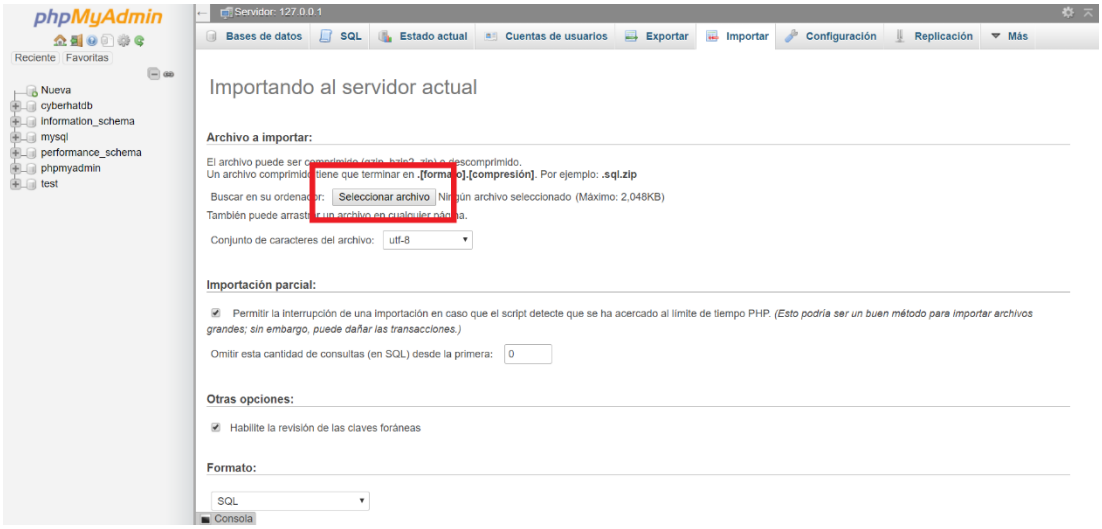


Figura B.5. Pantalla de importar tablas en PHPMyAdmin

Hacemos clic en la opción “Seleccionar Archivo” y elegimos el archivo “cyberhatdb.sql” presente en la carpeta principal del proyecto. Esto cargará las tablas a la nueva base de datos, la cual tendría este aspecto una vez realizado este paso.

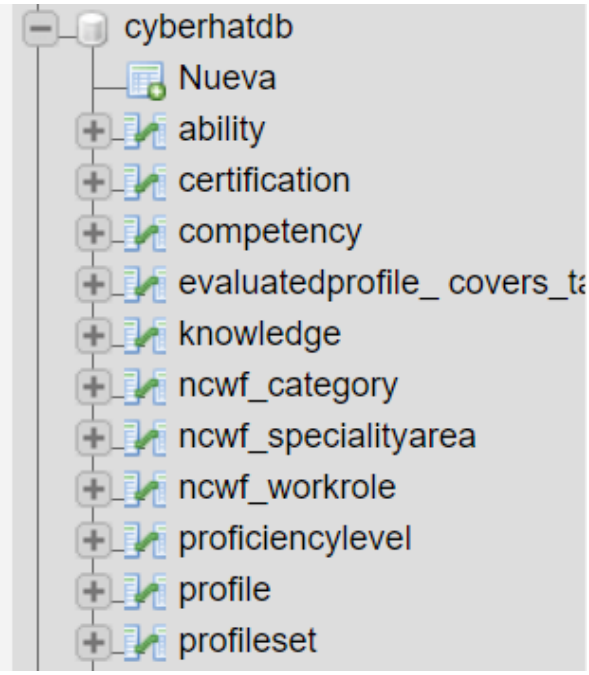


Figura B.6. Detalle de las tablas en la base de datos

Como podemos ver en la imagen anterior, las tablas han sido cargadas, por lo que podemos proceder al siguiente paso.

3. Abrir la aplicación en el navegador

Por último, debemos abrir la aplicación en el navegador. Para ello, debemos introducir la siguiente dirección en el navegador: localhost/sortingHat/public/

Esto nos dirigirá a la pantalla de inicio de la aplicación.

ANEXO C: VERSIÓN EN INGLÉS

ABSTRACT

The purpose of the document presented below is to present the following readers the characteristics of the Cybersecurity Sorting Hat project. This consists of a web application; whose main functionality is to define a profile of the user within the area of cybersecurity. The main users of this application are the students of the Master's in Cybersecurity of the University Carlos III of Madrid, although it is feasible that this application will be useful for other types of users in the future. that in the future this application will be useful for other types of users.

In the cybersecurity sector, the classification of professionals who work in this field under very specific frameworks is considered as a primordial necessity. Therefore, different frameworks were created to define and designate each of the roles or profiles that can be found in a project that is related to cybersecurity.

The following TFG consists of the prolongation, improvement and inclusion of new functionalities on the TFM carried out by a previous student of the University Carlos III of Madrid. The development of this End of Degree Work has been accomplished by respecting the functionality of the application on which it is based and more so adding functionalities with some being more basic and others more complex, something in which the initial project lacked.

The following document analyzes the procedure necessary for the correct development of this project, in terms of planning, documentation, and the implementation of the functionalities incorporated in the application. These different aspects come together with the relevance that these improvements produce in an application consisting of these characteristics.

PREVIOUS NOTES ABOUT THE WORK

As a prerequisite to the presentation of the developed project, it is essential to explain the background of it. This TFG corresponds to the continuation and extension of the TFM of Javier Vila, a student of the Master of Cybersecurity of the University Carlos III de Madrid, which was presented under the title: "Cyber Range Systems: A Cybersecurity Sorting Hat".

This is an extensive web application with a wide variety of features, therefore the work cannot be completed in its totality in a single TFM. Thus, in this End of Degree Project, work is being carried out to provide the original application of the remaining functionalities in order to be considered as a complete web application. Given the large number of functionalities that the client wanted to add to the original application, it has been possible to work in parallel to another faculty colleague, Sandra Sanchez Esperante.

Each student has overseen the development and creation of different functionalities and parts of the application, but the core of the application and the subject matter is shared, resulting in an interdependency that can be seen in both TFGs.

My colleague's project was presented in June 2018, but due to personal circumstances the part that I have been asked to do will be presented in the following convocation.

1. INTRODUCTION

This chapter will begin with a brief introduction to the project and followed by the detailed reasons and motives that have led to its creation. It also sets out the main objectives and functionalities to be developed. Finally, this chapter will be completed with the detailed structure in which the project follows.

1.1. Work Motivation.

Today, we live in a society that has a vital need to be connected. This need has been driven, primarily, by the ease of access to the internet, with credit to the so-called "intelligent mobile phones" or "smartphones".

The studies indicate that IP traffic increases at an average annual rate of 24%, being able to reach 3,3 Zettabytes (2 70 bytes) in 2021 [1], and that in the same year there will be 12 billion devices capable of making mobile internet connections [2].

Due to the exponential growth of Internet connections, there has also been a huge increase in computer attacks. The alleged cyber-attacks are maneuvers that attack individual Internet users or companies, thus trying to cause theft of sensitive information or malfunctioning.

These worrying statistics have caused the cybersecurity sector to become crucial for individuals who want to feel protected on the Internet, as well as for companies who want to protect their sensitive information from any malicious attacks.

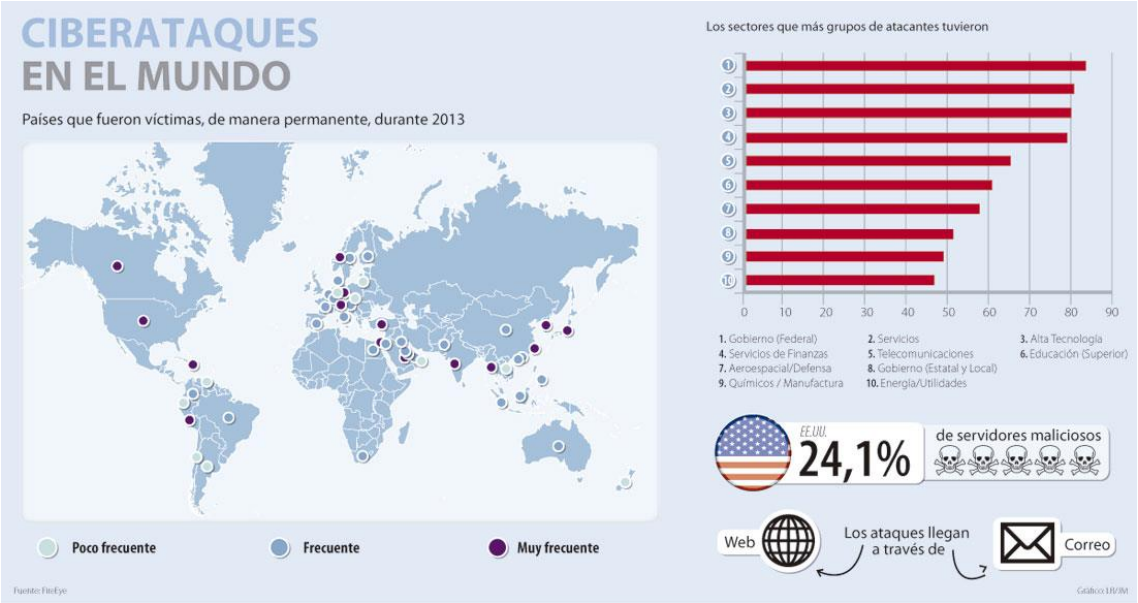


Figure 1.1: Map of cyberattacks in the world, and by sector. [5]

According to the latest data, the companies in our country allocate 22%, on average, of its budget on cybersecurity. [6]

From this data, it can be inferred that the education of professionals, or future professionals, in the sector gains enormous importance. To facilitate this task, the organization, proposed by NICE, was created. It is the Cybersecurity Workforce Framework (NCWF), which will be referred to in the project. It is composed of 7 categories, which include 33 areas of specialization and 52 different profiles, defined by the TKSAs needed for the job and the accurate performance of the jobs required.

The project described in this document relies on these resources to construct a functional web portal to find suitable cybersecurity profiles for the user. The term "functional" should be highlighted, as the main objective consists of turning the base project, which had great deficiencies, into a web site. This website can be useful for users who need a tool of these characteristics. It has been equipped with new functionalities, tables and views have been added to make using it increasingly accessible.

1.2. Goals

The purpose of this End-of-Grade Project is to help professionals or future professionals in the cybersecurity industry to find the profile that is most suitable for them based on their personal knowledge and skills, and in turn, to identify the aspects to improve with the objective of increasing the employment of such professionals.

With the aim of fulfilling the functionality for which the application is intended, it must satisfy the following requirements:

- Creation of user databases, with password protection by encryption, with the purpose of protecting the information from possible SQL injection attacks.

- Inclusion of a middleware in charge of coordinating the communication between the views and the database.

- Authentication of users in a safe way, using the resources of the middleware to manage the session maintenance functions in a way that is secure.

- Creation of new views corresponding to the functionalities added to the original Project (User profile, editing of that profile and addition of certifications in the database).

- Creation of models that correspond to the objects with which we are going to treat in the application (Users, Certifications, Work Roles...).

- Use of the resources provided by the TFG developed in parallel to this one by Sandra Sánchez Esperante, and the search for cohesion between the two projects for the resultant one.

- Adaptation of the functionalities developed in the initial Project developed by Javier Vila in the improved platform, which is developed in this TFG and that of the colleague Sandra Sánchez, with the objective of creating a functional web application.

1.3. Structure of the document.

This section describes the points to be dealt with in this document and the order in which they will appear.

- Introduction and objectives: This chapter describes the market situation, where companies are investing more in cybersecurity professionals. It also explains how this application can be useful for companies or professionals in this field.

- State of the art: The main purpose of this chapter is to explore the technical details of the web portal. The characteristics of the framework defined by the NICE Cybersecurity Workforce Framework are also defined.

- Software design and development: The following chapters are in charge of explaining in detail the architecture and design of the technical solution proposal for this project..

- Planning and Budgeting: This chapter is key as it details the management of both time and resources available for the project.

- Regulatory framework: Consists of an analysis of the legislation existant in Europe and in Spain related to the subject matter of the project that can affect it.

- Conclusions: This chapter summarizes the conclusions that are reached once the project is finished. It is analysed whether the objectives set at the end of the project have been reached and possible future lines of action in modification and extension of the project are studied.

2. STATE OF THE ART (SUMMARY)

Due to the strong rise of cybersecurity, the search for specific profiles within the field becomes an essential task. That is why there are several applications that perform operations of a similar nature to the one developed in this project, although each of them has different characteristics.

The NICCS is an online portal of the Government of the United States, in particular the department of Homeland Security. It is considered the reference portal in the study of cybersecurity.

It is held at state level and its main objective is to provide government employees, students, educators, or professionals in the cybersecurity field with the right tools to acquire the required cybersecurity knowledge to advance in their professional careers.

To achieve this goal, NICCS offers several applications based on the NICE Workforce framework, which has been used for the development of this Project. The NCWF framework categorizes and describes work by cybersecurity. This is what most of the tools described in the next paragraph are based on.

This framework provides the ordering that describes the jobs and workers in the area of cybersecurity, no matter where or for whom the work is done. It consists of the following components:

- 7 Categories - Groupings of common cybersecurity functions
- 33 Specialty Areas - Different Cybersecurity Work Areas
- 52 Working Roles - More detailed working groupings. They are composed of: Tasks, Skills, Skills and Knowledges.

Two of the tools based on this framework are:

- PushButton, which consists of an Excel sheet, whose main task is to help managers or HR representatives to define job vacancies.
- Mapping Tool: This tool allows managers and resource managers to research for information about cybersecurity profiles in order to decide how their teams relate to the framework.

The second most important body is the IISP or Institute of Information Security Professionals. This non-profit organization based in London was created in 2006 by professionals in the area of cybersecurity.

The applications contained in its portal do not follow the framework defined by the NCFW, as it has its own called IISP Skills Framework. This Framework defines the skills and capabilities expected of cybersecurity professionals in practice, and is not just an assessment of their knowledge.

We can also find other tools in different websites, such as Cyberseek.org, which offers us very useful applications such as its interactive map with job offers in the field of cybersecurity, or the career path tool, which shows the logical relationships between the different work profiles within the field.

It also details the European Union's proposal to create a framework of job profiles in the field of cybersecurity at European level.

3. SYSTEM ARCHITECTURE AND DESIGN (SUMMARY)

In this section we perform a technical analysis of the technical solution chosen in order to develop this project along with the software requirements and use cases contained in the platform.

A profile corresponds to each of the positions that are expected to be part of a cybersecurity team. Each profile has associated skills, abilities and knowledge, the so-called TKSAs, which will be explained in more detail in subsequent chapters of this document. For the correct performance of the functions associated with a profile, it is essential that the worker has TKSAs. This application can be very helpful in the development of their future professional career in the field of cybersecurity.

The application is distributed in three layers in the way it is shown in the following image:

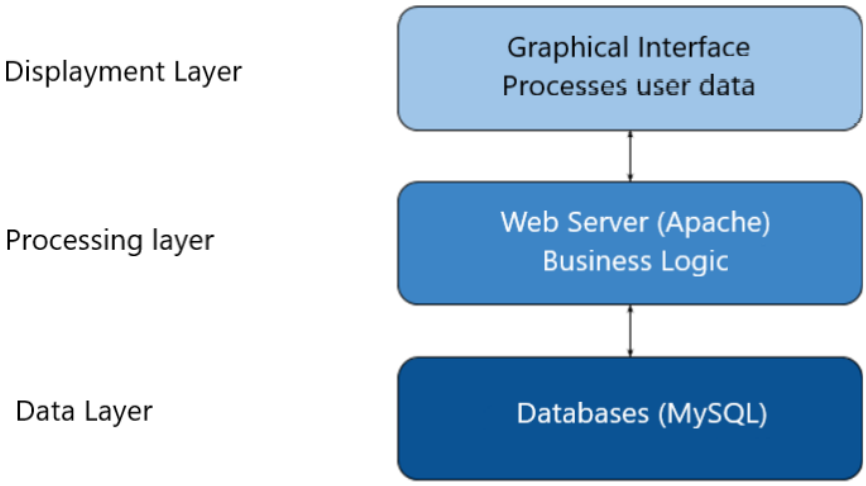


Figure 3.1. Web application architecture.

The Software Requirements Specification or ERS is a complete specification of the operation of the system to be developed. Functional and non-functional requirements are covered in this section.

- **Functional requirements:** User register, User login, User logout, Test fulfillment, Test results, Test results computation, Add certification, User Profile, Edit User Profile, Add Certification from User, Delete Certification from User and Dashboard.

- **Non-functional requirements:** Internet Connection, Data Protection and Compatibility between web browsers.

The use cases are the descriptions of the activities that must be performed to complete a certain process. They are the sequence of interactions that take place between a system and its actors. An image of them can be found in the Spanish version of the document.

4. SOFTWARE DEVELOPEMENT (SUMMARY)

The portal on which this project is based had a very basic design, using PHP without any Framework, together with some HTML and CSS for the views, and a little JavaScript to perform the test methods.

After a previous analysis of the functionalities that were planned to be added to the application, it was clearly perceived the need to incorporate a PHP Framework. An analysis was made of the available and most popular PHP frameworks in the market, with the aim of finding the one that best suits the specifications of the project. The chosen one was Laravel due to the easy learning curve that it has and also the inmense amount of libraries available.

It has been decided to use an Agile methodology for the development of this project. In particular, Scrum has been chosen, which is characterized by the adoption of an incremental development strategy, instead of a waterfall strategy. It has been proven that Agile methodologies are the most adequate for most software projects.

The application in which this Project is based only contained one main functionality, the test one, with just one screen in which the ítems contained would hide or appear depending on the buttons the user pressed. In this new versión, the application includes multiple additional functionalities. When we first enter the website, the view that we come across is the welcome page. In this page we can find two different functionalities: Register and Login.

To register an user, we have to fill in the necessary data for its creation, then hit the register button. That Will perform the tasks needed to store the user object to the table in the database if the introduced data is correct. To log in, we will hace to introduce the data of an existing user in the form and hit the Login button. If there is a match, the user will be redirected to the main page of the app.

In the main page we can access to the rest of the functionalities through the upper navigation bar. First we have the “Add Certification” option. This page gives the user the option to add an oficial cybersecurity certification to the database by filling a simple form.

The user profile page shows all the available information about the user. The upper section displays the user main information, and the lower part shows the certifications that the user has obtained. You can find links to additional functionalities, such as editing the user data and adding or deleting certifications from the user profile.

The other two available functionalities are the test and the dashboard. The test was the one implemented in the old Project, and it has maintained its structure, but adapting it to the new platform. Once you finish, they will be stored in the database, linked with the user, and also shown in the screen. The dashboard page will retrieve those user stored data from the test, and display them in various graphics.

The chosen web server for the application is an Apache server and a MySQL server is used for the database, since they are open source, is present in all platforms and is the most extended at the moment. Both are included in the XAMPP software, which is an open source platform-independent server.

To develop the code, Microsoft Visual Studio Code has been used. It is a free code editor which includes tools for debugging functions, Git repository management and plug-ins to facilitate the code development.

The application has been provided with security for the most probable vulnerabilities that can occur to a platform of this kind, such as SQL inyection attacks, cross-site scripting attacks, or session management attacks.

To finish, in this chapter the software is evaluated to check that it fulfills the minimum quality requirements. After a check on each one of them, it is seen that the application described in this Project meets this quality standards.

5. USER EXPERIENCE TESTING

Once the developement process of the application was finished, the user experience tests started. Four people with different backgrounds but all related to the computer or communications field were chosen. They were given a series of instructions to perform in the application, while being recorded. Additionally, they were handed in a questionnaire with some questions about their experience with the application. This questionnaires are presented in the Annex A of this document.

The results show that most of the users think that the application is easy to use, with some exceptions, and that there are some áreas that need some improvement, like the user profile or the need for more imaginery of the institution in charge of the application.

6. PLANNING AND BUDGET (SUMMARY)

The project has been developed over a period of five months, with a one-month hiatus between mid-March and mid-April for health reasons, so the schedule had to be adapted. Planning was carried out with the aim of coordinating all parts involved in this project. This planning is reflected in the Gantt diagram in the Spanish version of this document.

As this is a software project, no external capital was needed for the commencement of the project. The associated costs will be generated by the time spent by the developers in the progress of the Project.

The person in charge of completing this project is a Junior developer, which results in big cost reductions. In the corresponding section of the Spanish version of the document, a table with the costs associated with each phase of the development of the project can be found.

7. LEGAL FRAMEWORK (SUMMARY)

In this chapter, we will explain the current regulations regarding cybersecurity at state and European level.

The NIS European Directive was proposed to establish a community framework related to cybersecurity. It must be adapted and included to every states's legislation, with some flexibility to reutilize state facilities or regulations.

The new Organic Data Protection Law written by the spanish government will start to be applied May 25th 2018. It includes a series of changes to the previous regulations in order to adapt them to the actual situation. The concept of tacit consent is eliminated and it is reinforced by becoming a more positive and express action. In addition, the figure of the Data Protection Delegate is created.

To sum up, we can find the spanish Data Protection Law. The objective of this Law is to regulate the obligation of operators to keep data generated or processed in the context of electronic communications as well as the obligation of the transfer of such data to the competent bodies whenever necessary.

8. CONCLUSIONS

This chapter discusses the conclusions reached at the end of project development, both personal and related to objectives fulfillment. In addition, future ways of developing implementation are also explored.

8.1. Meeting Initial Objectives

At the beginning of the development of this project, initial objectives were set. This section analyses the level of fulfillment of these in the final version.

- Initial Objective: Creation of user databases with intensive protection.
- Final Evualuation: Using the resources provided by the framework (Laravel), user data is protected using encrypted passwords. As a result, SQL injection attacks are prevented.

- Initial Objective: Inclusion of middleware that promotes front-end/back-end coordination.

- Final Assessment: This objective has been achieved by implementing the routing functions through the systems provided by Laravel.

- Initial Objective: Secure user authentication and session management.

- Final Evualuation: Session maintenance management is done in a safe way. Laravel's Auth method allows you to authenticate the user through thedecryption of the password and the session is maintained through a token.

- Initial Objective: Implementation of views for new functionalities, which the application lacked.

- Final Evaluation: New views have been created for the following functionalities: add certification, user profile, edition of this one and addition/deletion of certifications of a user.

- Initial Objective: Creation of models of objects present in the application (users, certifications...).

- Final Evualuation: Templates have been created for all objects created from the database tables (users, certifications, their links...) with the objective of facilitating its management.

- Initial objective: Use of the resources of the TFG of Sandra Sánchez and search for cohesion with the elements of new development.

- Final Evualuation: The views created by Sandra Sánchez have been used in the project, and those that have been created have followed the guidelines established by that TFG.

- Initial objective: Adaptation of the initial project, created by Javier Vilas within the new platform.

- Final Evualuation: The test functionality developed in the TFM work created by Student's Master Javier Vilas has been respected at all times in the application adding new functionalities to adapt it to the new platform.

8.2. Personal Conclusions

The process of choosing a Final Degree job took several months, because I was looking for something that could be of added value to other people and that, was also a challenge for me as an engineer and programmer.

In the course of my studies of the Degree of Telematic Engineering at the University Carlos III of Madrid, I have developed a great interest both in programming as well as in the field of cybersecurity and decided that my desire was to pursue my professional career in something related to these two areas of specialization.

Therefore, when the tutor of this project introduced me to the idea, I found it very interesting, because it brought together the two things that attracted me the most. On the one hand, I could develop my skills as a programmer since the PHP language is not taught in the Degree in Telematic Engineering and, in addition, learn about work profiles in the field of cybersecurity.

At this moment, once the development of the project is finished, I can affirm that the objectives established in the previous paragraph have been met, which is a great achievement for me. The development of the complete application has helped me to acquire new knowledge in the development of PHP applications, which will be useful for my professional career. I have also been able to broaden my knowledge in the field of cybersecurity, one of the most cutting-edge at present.

Finally, it should be noted that the application is going to be useful for other students of the university where I have developed my studies. The fact that other students can benefit from the application developed in this project for their future career makes me feel that I have been able to give back something valuable to the institution that allowed me to develop my studies and launch my professional career.

8.3.Future work lines

Web applications are in constant improvement and, therefore, in the process of development of the one presented in this project, possible future improvements have been defined which can be implemented.

- Expansion of the user profile: user image, new data, upload of CV to the platform...
- Connection system between the certifications and the test: The certifications correspond to a certain profile, and the TKSAs associated with that profile should be marked automatically in the test.
- Password recovery function: Implementation of an option in the welcome page for password recovery startup in case the user has forgotten it. In addition, the security associated with this option must be implemented.
- Implementation of the spanish versión of the website: The website should have versions in various languages, at least english and spanish.
- Documents Download, History of the user and correction of the TKSA search bar in the test function.

BIBLIOGRAFÍA

[1] El tráfico IP en España se triplicará antes de 2021, 08-08-2017 [En línea] Disponible en: http://www.fibratel.com/blog/3000/

[2] Mobile on the fast track to 2021, 07-02-2017 [En línea] Disponible en: https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1819184

[3] España bate su record de ciberataques: 120.000 incidentes en 2017, 12-01-2018 [En línea] Disponible en: https://www.abc.es/tecnologia/informatica/abci-espana-bate-record-ciberataques-120000-incidentes-2017-201801111645_noticia.html

[4] Los mayores ciberataques de 2017 hasta la fecha, 11-07-2017 [En línea] Disponible en: https://www.pandasecurity.com/spain/mediacenter/noticias/ciberataques-hasta-la-fecha/

[5] Del total de las empresas colombianas, el 98% son víctimas de ataques informáticos, 10-03-2014 [En línea] Disponible en: https://www.larepublica.co/alta-gerencia/del-total-de-empresas-las-colombianas-98-son-victimas-de-ataques-informaticos-2103995

[6] Las empresas españolas destinan a ciberseguridad el 22% de su presupuesto de TI, que cae con respecto a 2016, 05-12-2017 [En línea] Disponible en: http://www.europapress.es/portaltic/ciberseguridad/noticia-empresas-espanolas-destinan-ciberseguridad-22-presupuesto-ti-cae-respecto-2016-20171205125550.html

[7] About NICCS, 21-06-2017 [En línea] Disponible en: https://niccs.us-cert.gov/about-niccs

[8] PushButtonPD™, 29-03-2018 [En línea] Disponible en: https://niccs.us-cert.gov/workforce-development/dhs-pushbuttonpd-tool

[9] PushButtonPD™ Generation 5, 01-09-2018 [En línea] Disponible en: https://niccs.us-cert.gov/sites/default/files/documents/pdf/dhs_pushbuttonpd_gen5v2_tool_brochure_20180109.pdf?trackDocs=dhs_pushbuttonpd_gen5v2_tool_brochure_20180109.pdf

[10] Mapping Tool, 02-03-2018 [En línea] Disponible en: https://niccs.us-cert.gov/workforce-development/intro-mapping-tool

[11] IISP: Our Mission [En línea] Disponible en: https://www.iisp.org/imis15/iisp/About_Us/Our_Mission/iispv2/About_us/Our_Mission .aspx?hkey=9a43cc5c-8b71-4770-bfa9-d60e5c7b3ba9

[12] About Cyberseek.org, [En línea] Disponible en: https://www.cyberseek.org/index.html#about

[13] Cybersecurity Supply/Demand Heat Map, [En línea] Disponible en: https://www.cyberseek.org/heatmap.html

[14] Cybersecurity Career Pathway, [En línea] Disponible en: https://www.cyberseek.org/pathway.html

[15] National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST, 08-2017 [En línea] Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

[16] IISP Knowledge Framework - Version 1 [En línea] Disponible en: https://www.iisp.org/imis15/iisp/About_Us/Our_Frameworks/Our_Knowledge_Framew ork/iisp/About_Us/Our_Knowledge_Framework.aspx?hkey=6e8644f9-fc2f-4f53-9784b0fb2dba5e8b

[17] EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position, 08-06-18 [En línea] Disponible en: https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Content%20Preview%20of%20Offshore%20Profile.pdf?ver=201707-19-070239-550

[18] Arquitectura de las aplicaciones web, [En línea] Disponible en: https://programacionwebisc.wordpress.com/2-1-arquitectura-de-las-aplicaciones-web/

[19] TFM: Cyber Range Systems: A Cibersecurity Sorting Hat, Javier Vila López, 27/09/2017.

[20] TFG: Cybersecurity Sorting Hat: Ampliación de funcionalidades de análisis y desarrollo de interfaz de usuario avanzada 1, Sandra Sánchez Esperante, 2018.

[21] Especificación de requisitos de Software (ERS), Wikipedia, [En línea] Disponible en: https://es.wikipedia.org/wiki/Especificaci%C3%B3n_de_requisitos_de_software

[22] Definición de casos de uso, sistemas.com, [En línea] Disponible en: https://sistemas.com/casos-de-uso.php

[23] Laravel, Wikipedia, 02-08-2018 [En línea] Disponible en: https://es.wikipedia.org/wiki/Laravel

[24] ¿Qué es Laravel?, Ventajas del desarrollo a medida para tus proyectos, Synergy, 31-01-2018 [En línea] Disponible en: https://www.synergyweb.es/blog/laravel-desarrollo-medida.html

[25] 10 Significant benefits of Laravel Framework, LinkedIn, 18-12-2017 [En línea] Disponible en: https://www.linkedin.com/pulse/10-significant-benefits-laravel-framework-ved-raj

[26] Los 10 Framework PHP que solicitan las empresas, OpenWebinars, 28-09-2015 [En línea] Disponible en: https://openwebinars.net/blog/los-10-mejores-frameworks-php-que-solicitan-las-empresas/

[27] Metodología 'Agile'. La Revolución De Las Formas De Trabajo, BBVA NOTICIAS 25-05-2018, [En línea] Disponible en: https://www.bbva.com/es/metodologia-agile-la-revolucion-las-formas-trabajo/

[28] Why does Agile Developement Metodology proves to be a better choice for your Project, 360Logica [En línea] Disponible en: https://www.360logica.com/blog/why-agile-development-methodology-proves-to-be-a-better-choice-for-your-project/

[29] Scrum (Desarrollo de Software), Wikipedia, 30-07-2018 [En línea] Disponible en: https://es.wikipedia.org/wiki/Scrum_(desarrollo_de_software)

[30] Servidor HTTP Apache, Wikipedia [En línea] Disponible en: https://es.wikipedia.org/wiki/Servidor_HTTP_Apache

[31] ¿Qué es XAMPP y para que se utiliza?, 13-11-2011 [En línea] Disponible en: https://mantenimientosdeunapc.blogspot.com/2011/11/que-es-xampp-y-para-que-sirve.html

[32] Visual Studio Code, Wikipedia [En línea] Disponible en: https://en.wikipedia.org/wiki/Visual_Studio_Code

[33] About the Open Web Application Security Project, OWASP, 08-07-2018 [En línea] Disponible en: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

[34] OWASP Top 10 2017, OWASP, [En línea] Disponible en: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

[35] Qué es una inyección SQL y cómo defenderse contra ella, Avast Software, [En línea] Disponible en: https://www.avast.com/es-es/c-sql-injection

[36] Cross-Site Scripting, Wikipedia, [En línea] Disponible en: https://es.wikipedia.org/wiki/Cross-site_scripting

[37] About ScreenCastify, ScreenCastify [En línea] Disponible en: https://www.screencastify.com/products/screen-recorder/

[38] Calculadora salarial, Hays [En línea] Disponible en: https://guiasalarial.hays.es/trabajador/calculadora-salarial

[39] Convertir salario anual a salario por hora, [En línea] Disponible en: https://convertir-sueldo-hora-ano.appspot.com

[40] ¿Cuál es el salario de un profesor en España?, Superprof, 13-09-2017 [En línea] Disponible en: https://www.superprof.es/blog/sueldo-de-un-profesor-en-espana

[41] ¿Qué leyes regulan la ciberseguridad en la Unión Europea y en España?, Signaturit, 26-04-2017 [En línea] Disponible en: https://blog.signaturit.com/es/que-leyes-regulan-la-ciberseguridad-en-la-union-europea-y-en-espana

[42] NIS Directive, ENISA, [En línea] Disponible en: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii/nis-directive

[43] La nueva LOPD, Abogacía Española, 29-01-2018 [En línea] Disponible en: https://www.abogacia.es/2018/01/29/la-nueva-lopd/

[44] El Gobierno dota de mayor eficiencia a la Ley de Conservación de Datos, El Diario, 13-05-2014 [En línea] Disponible en: https://www.eldiario.es/turing/vigilancia_y_privacidad/ley-conservacion-datos_0_259674834.html

[45] Modelo de test de usuario, Universidad de Chile [En línea] Disponible en: http://web.uchile.cl/DctosIntranet/05UsabilidadExperienciaUsuario/HerramientasTesteo/ModeloTestUsuario.docx.pdf