UNIVERSIDAD COMPLUTENSE
MADRID

Facultad de Informática

Universidad Complutense de Madrid

Curso 2016-2017

HERRAMIENTA DE APRENDIZAJE ONLINE EN CIBERSEGURIDAD Y HACKTIVISMO EN REDES ADAPTADO A NIVEL DE USUARIO

Trabajo de fin de grado del Grado en Ingeniería Informática

AUTOR: JESÚS DEL OLMO CABRERA
DIRIGIDO POR: MARCOS SÁNCHEZ-ÉLEZ MARTÍN

12 DE JUNIO DE 2017

Contenido

Resumen

Este proyecto tiene como finalidad el desarrollo de una herramienta de aprendizaje en el campo de la ciberseguridad y hacktivismo, adaptándose al nivel de conocimiento o necesidad de los usuarios, y creando perfiles específicos con distintos privilegios y accesos a contenidos.

A medida que pasan los años la sociedad se sumerge más y más en el mundo digital. De esta manera, muchos de los actos cotidianos que la gente ejercía de manera convencional y/o analógica en este momento se realizan de forma digital, ya sea a través de internet o de dispositivos móviles. Esto ha dado lugar a que la mayoría de los usuarios que se ven obligados a usar esta tecnología lo hagan con muy poca información de base, sin conocer el riesgo al que se exponen, y priorizando la velocidad antes que la seguridad. Además, muchas veces la información que se puede encontrar navegando en la red no está adaptada al perfil de usuario que la requiere.

Para nuestra herramienta, se ha elegido como plataforma de aprendizaje un entorno web en lugar de una aplicación móvil. El entorno seleccionado permite incluir las funcionalidades de aprendizaje necesarias para poder instruir adecuadamente a todos aquellos que busquen o necesiten alcanzar un conocimiento más profundo sobre ciberseguridad, o para los que se están iniciando en estos momentos. Además, un entorno web permite un mejor uso por parte de las personas de edad más avanzada, siendo estas uno de los perfiles de usuarios a los que está dirigida la web.

Así mismo, la herramienta permite a los usuarios más expertos hacer apunte de errores, subir contenido nuevo para la mejora de la web, así como escalar privilegios y convertirse en moderadores de la misma y administrar los contenidos a posteriori.

También se ha desarrollado un apartado muy interesante denominado “perfiles” destinado a aquellos *perfiles profesionales* que pueden demandar necesidades más específicas de ciberseguridad con contenido dedicado específico. Los perfiles que mostramos en estos momentos son el de *periodista,* con contenido que le permita proteger su información, *empresarios,* dedicado a contenido para proteger su empresa y por último *figuras públicas,* donde haremos un énfasis en la privacidad de su vida privada en las redes sociales, donde multitud de ellos han visto vulnerada su intimidad.

Palabras clave: Ciberseguridad, aprendizaje, perfiles, profesionales, redes, arquitectura computadores, web, tutoriales.

Abstract

This project's purpose is developing a learning tool about hacktivism and cybersecurity's field. It will be adapted to several knowledge levels per user's capacities, creating specific profiles with different privileges and access to content.

As the years go by, Society is diving more and more into the digital world, as a result, day to day acts that people used to do in the traditional way, are performed in a digital way nowadays, using internet or smartphones. As a result, most of the users feel obliged to use this technology with a poor base of information, without knowing the risk that they are exposed, prioritizing speed before security. Besides, many times the information we can find in the internet is not adapted to the user's profile required

As a learning platform, it has been chosen a website instead a smartphone's app. The chosen environment let include the learning's functionalities needed to teach appropriately everyone who is looking or needing to reach a deep knowledge about cybersecurity or for those who are starting now. We have to remark that a website is better to the elder 'skills which is one of the user's profiles that the website is created for.

Likewise, the tool let the most expert users point fails, upload new content to improve the website and the possibility to scale privileges and become a web's moderator, being able to manage the content.

Also, it has been developed a very interesting section called "profiles" focused on those professional's profiles which have a more specific demand in the cybersecurity environment, with specific content. The profiles that the website is showing now are journalist, which dedicate content to protect their information; businessmen, with content to protect their Company; and finally, public figures, where an emphasis will be done at the protection of their private's life at social networks, where many of them have seen his privacy violated several times.

Keywords: Cybersecurity, learning, profiles, professions, nets, computer architecture, web, tutorials.

1 INTRODUCCIÓN

Hoy en día la ciberseguridad juega un papel muy importante en nuestra sociedad debido al gran desarrollo y crecimiento de las nuevas tecnologías y al uso que la gente le da en su vida. Las familias acostumbran a pedir comida a domicilio comprándola por internet, muchas otras personas se lanzan a la compra de ropa y demás productos de forma online, utilizamos aplicaciones para conocer gente… A la hora de llevar a cabo este tipo de acciones tenemos que proporcionar nuestros datos personales, fiándonos de que queden en la web donde estamos haciendo gestiones y no lleguen a terceros.

Por norma general no se suele revisar la política de cookies de los sitios webs que se visitan, al considerarse tedioso e inútil para nuestro objetivo (que es en realidad tener acceso a dicha web), pero muchas veces conviene que se le eche un vistazo para saber *"qué hacen esas cookies"* o incluso "*quien más se beneficia*" de la información que proporcionan las personas que acceden a la web.

La gente no comprueba el origen de los correos que reciben y se basan únicamente en el contenido que estos contienen sin ser conscientes de que, si acceden a las condiciones, pueden poner en riesgo su seguridad en la red.

Tampoco se suele tener en cuenta a la hora de navegar por la red detalles tan simples como las URL's de los sitios que se visitan, pudiendo comprobar con un solo vistazo si la web es segura y conocer su fiabilidad.

Conviene resaltar un par de ejemplos muy significativos que se han dado en nuestra sociedad en estos últimos meses y que han tenido bastante repercusión: Elecciones de los EEUU, Hillary Clinton se posiciona con ventaja sobre el candidato republicano Donald Trump y pocos días del final de la campaña por la presidencia, se anuncia que se vuelve a reabrir el caso por el servidor personal de emails que Clinton tenía cuando era secretaria de estado y por el cual fue acusada y al final el mismo caso quedó archivado en el año 2015.

Hace pocos días el director del FBI anunció que asesores de la campaña electoral de Trump y hackers rusos se vieron envueltos en el espionaje de la candidata a la presidencia. Todo por emplear un servidor casero más susceptible al ataque de los hackers [(1)].

Otro ejemplo de violación de la privacidad: Nos remontamos al año 2013, año en el que el ex técnico de la CIA y de la NSA Edward Snowden se pone en contacto con uno de los periódicos más prestigiosos de los EEUU "The Guardian" para revelar que el gobierno estadounidense presidido por Obama, podía acceder a los servidores de prestigiosas empresas como Facebook, Google, Microsoft, Apple… para recabar toda la información de sus usuarios, alegando que llevaron a cabo esta acción en base a la "seguridad nacional" [(2)].

Además, existen colectivos donde la formación en ciberseguridad es todavía más necesaria como puede son periodistas, abogados o activistas pro derechos humanos.

En el entorno periodístico existe una necesidad real de proteger la información, las comunicaciones y los equipos tecnológicos con los que los periodistas trabajan diariamente [(3)]. Aquellos que realizan su labor en una empresa o corporación, pueden verse más protegidos ante las amenazas con base a la ciberseguridad, pues trabajan junto a un grupo profesional dedicado a proteger redes y ordenadores, evitando así cualquier tipo de ataque. El problema reside en que no todos los periodistas se mueven en el mismo ámbito laboral, muchos trabajan de forma autónoma y se encuentran indefensos ante la falta de información, herramientas y preparación para proteger sus activos, necesitando ayuda en este ámbito.

Los despachos de abogados albergan una ingente cantidad de información de gran valor, no solo para el bufete en sí, también es muy importante para el cliente y la competencia. El secreto profesional es un pilar fundamental dentro de su campo laboral, que si en algún momento se quebranta puede llegar a suponer penas considerables, como puede ser la inhabilitación, multas o presión, todo recogido en el artículo 199.2 del Código Penal [(4)].

A día de hoy la información y documentación que se maneja en los despachos es en su gran mayoría digital, en forma de correo electrónico, bases de datos, información de la nube… Por ello, es primordial trabajar con el software adecuado y revisar periódicamente las actualizaciones que se hacen del sistema para corregir las debilidades que se vayan encontrando y evitar amenazas como la ocurrida con el virus de tipo ransomware llamado "*WannaCry*" el 12 de mayo de 2017 [(5)].

No obstante, hay personas, organizaciones e instituciones que deben sentirse más concernidas por el ejercicio de esta tarea. A continuación, se entresacan las más significativas [(6)]:

- Padres. Se incluyen también tutores y otros responsables de la educación en el entorno familiar. Son actores esenciales para la creación de conciencia de ciberseguridad, ya que bajo su tutela se producirán los primeros contactos de los menores con las tecnologías de la información y telecomunicaciones. Deberán integrar adecuadamente la educación en este campo con el resto de la educación familiar, para conseguir la adaptación a este medio.
- Docentes. Miembros del sistema de enseñanza, que son también actores esenciales. Prolongan la acción de los padres en la escuela y ayudan a crear el grado de ciberconciencia mediante la transmisión de conocimientos sobre el ciberespacio. En ciertos casos sustituyen a los padres que, por su situación socioeconómica, no pueden ejercer sus tareas en este campo.
- Voluntarios. Personas con sensibilidad social que aportan sus conocimientos y experiencia, empleando su tiempo en tareas relacionadas con la creación de conciencia de ciberseguridad.
- Asociaciones. Tienen un papel similar al de las instituciones, pero su pervivencia es más azarosa. Mientras que están activas, pueden ser un refuerzo importante de otros actores, sobre todo en lugares con pocos recursos tecnológicos.

Todo lo mencionado anteriormente son ejemplos para resaltar la importancia de la concienciación y formación en ciberseguridad.

1.1 OBJETIVOS

En este apartado se tratarán los distintos aspectos que se plantean tratar empleando nuestra herramienta web.
Desde el punto de vista del usuario estos son los objetivos que se pretenden alcanzar:

1. Educar a las personas que accedan a la web en ciberseguridad y Hacktivismo.
    - Podrán adquirir conocimientos basados en nuestros distintos módulos de aprendizaje.

2. Proporcionar un entorno en el que el usuario pueda poner a prueba los conocimientos adquiridos haciendo los test de evaluación.
    - Cuando el usuario entre en nuestra web encontrará un examen inicial para medir su nivel de conocimientos actual.
    - Habrá un examen por cada módulo de aprendizaje.

3. Prestar una ayuda personalizada a los distintos sectores profesionales incluidos en la web.
    - Existirán tres apartados para apoyar en lo necesario al sector periodístico, empresarial y figuras públicas.

4. Premiar a los usuarios en base a los resultados obtenidos, otorgándole más privilegios en la web, de forma que pueda llegar convertirse en moderador de la misma.

Como objetivos de carácter general se resaltan los siguientes:

1. Acceder a información y herramientas asociadas con la ciberseguridad de una manera sencilla y actualizada.
2. Tener una herramienta que pueda estar en constante crecimiento y modificación.
3. Tener una herramienta que sirva para fomentar la autodefensa digital.

1.2 MÉTODO DE TRABAJO

En este apartado se tratará el proceso de desarrollo que se ha llevado a cabo para elaborar el proyecto.

Existen diversos modelos de desarrollo, pero se ha elegido destacar los dos siguientes [7] (Figura 1):

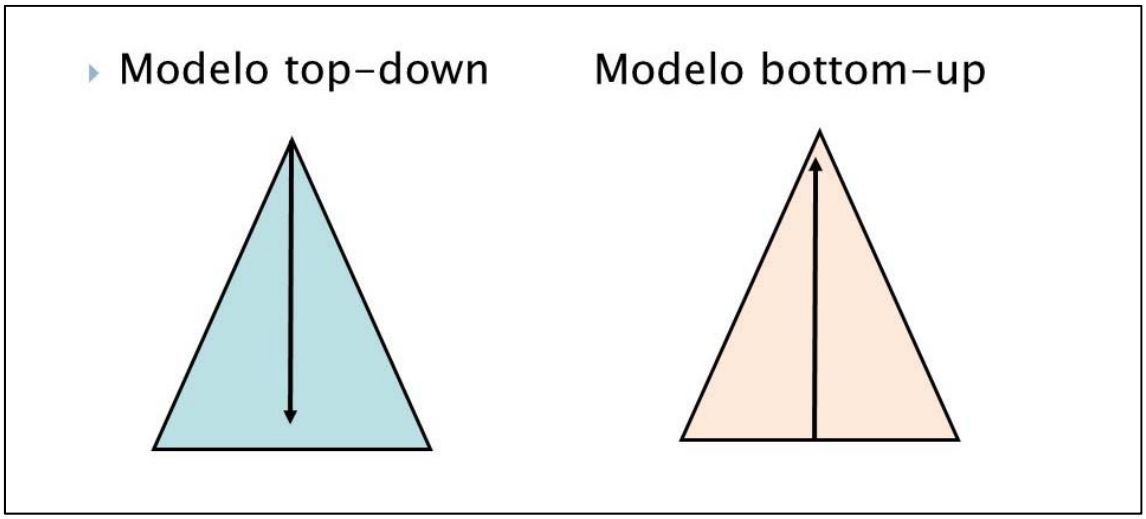


Figura 1: Modelo top-down y Modelo bottom-up.

- Modelo Top-Down: Este modelo se enfoca en la planificación y conocimiento completo del sistema que se va a desarrollar. Se necesita alcanzar un nivel de detalle bastante profundo en el sistema para empezar con la codificación en si misma o haber finalizado una de las partes de éste. En contrapartida, el hecho de desarrollar el proyecto con esta metodología hace que se retrasen las pruebas funcionales del sistema hasta que el diseño esté en gran parte completo.

- Modelo Bottom-Up: Este modelo de desarrollo se centra en la programación y las pruebas prematuras, que se llevan a cabo en cuanto la primera parte o módulo del sistema esté completo. El riesgo que se asume al aplicar este modelo es el hecho de que los módulos no casen entre si una vez se hayan finalizado y se empleé más tiempo del previsto en integrar cada una de las partes.

En este proyecto se han combinado ambos modelos de desarrollo, dado que ha habido momentos en los que se priorizó otorgar al mismo una visión más global de cada una de las partes y en otros casos prevaleció el enfoque individual de cada módulo.

El esquema de desarrollo es el siguiente:

1. Planificar el cuerpo de la web que se va a implementar
    a. Este apartado consiste en pensar cada uno de los apartados de los cuales se compondrá la herramienta web y que plantilla utilizar para otorgar de un estilo a la misma.

2. Implementar las secciones
    a. Consiste en completar cada uno de los apartados que aparecerán en la web, entendiendo como completar definir el estilo, el contenido que mostrará, los permisos necesarios para poder acceder a la sección (en función del rol del usuario).

3. Comprobar funcionalidad
    a. Una vez la herramienta está operativa, realizar las pertinentes pruebas para probar que todo funciona como estaba planificado desde el principio. Pruebas realizadas:
        i. Login y registro por parte de usuario registrado y sin registrar.
        ii. Acceso a las secciones públicas y privadas de la herramienta.
        iii. Poder visualizar los contenidos didácticos e imágenes.

4. Pruebas con usuarios
    a. Se han realizado las pruebas necesarias para comprobar la funcionalidad de los usuarios dentro de la herramienta en función del rol que se les ha otorgado. Pueden llevar a cabo:
        i. Acceder al contenido público de la herramienta. Ejemplo: (Perfiles profesionales).
        ii. Acceder y realizar los cursos propuestos. Ejemplo: (Módulo 1, examen).
        iii. Subir contenido nuevo a la página, (esto solo puede hacerlo un usuario con permisos de moderador o administrador).
        iv. Administrar los ajustes generales de la web (esto solo puede hacerlo el administrador).

5. Obtención de certificado SSL
    a. Para garantizar la seguridad de los usuarios de la web, se utilizó un certificado de seguridad SSL (Secure Socket Layer) para que la información entre el usuario y el servidor esté siempre cifrada.

2 CIBERSEGURIDAD

La ciberseguridad es la Seguridad de la Información como la protección de la confidencialidad, integridad y la disponibilidad de la misma. Como confidencial se entiende que es la propiedad con la que se pretende que la información no se encuentre a disposición de cualquier persona o pueda ser divulgada. La integridad puede ser definida como la propiedad de conservar la exactitud y la complejidad de los activos de información. Mientras que por disponibilidad entendemos que es la propiedad de ser accesibles y utilizables ante cualquier persona que los solicite en cualquier momento dado [(8)].

Aquellas personas que realizan labores en el campo de la ciberseguridad sustentan su trabajo en la denominación CIA, y no es el organismo de seguridad americano, se trata de los conceptos mencionados en el párrafo anterior *confidentiality*, *integrity* y *availability.* Un ejemplo de cada concepto empleando como escenario de este un banco:

- Confidencialidad: Ingresar dinero en el banco sin que nadie más, aparte de ti mismo, sepa la cantidad que has ingresado.
- Integridad: Poder retirar siempre el dinero que hayas ingresado, nunca más ni menos, dado que indicaría que el banco ha perdido tu dinero o te ha dado dinero de más.
- Disponibilidad: Siempre que la persona desee sacar dinero debe de tener el servicio disponible, sin que este se vea interrumpido ante cualquier acontecimiento que ocurra.

2.1 ANTECEDENTES DE LA CIBERSEGURIDAD

La ciberseguridad es un aspecto de vital importancia para los usuarios, ya que les permite usar sus sistemas de manera confidencial y segura, evitando ser el objetivo de ataques informáticos de distintos tipos.

Al comenzar narrar los inicios de la ciberseguridad, debemos resaltar y definir en qué consiste la ***criptología***, ciencia que estudia los distintos modos de codificar y descodificar mensajes para que únicamente emisor y receptor puedan leer su contenido [(9)].

De esta forma podemos encontrar sus orígenes en el antiguo Egipto, donde observamos cómo sus famosos jeroglíficos guardaban un significado oculto. más adelante en el tiempo nos topamos con el cifrado de sustitución, máquina enigma (empleada durante la Segunda Guerra Mundial) [(10)].

Todas estas técnicas se basan, como se ha definido anteriormente, en el cifrado de información. De este modo, sólo los individuos indicados que vieran el mensaje podrían interpretarlo. Queda analizar como ***transmitir*** esa información, como facilitar la forma en la cual la gente pudiera comunicarse entre sí y pudieran hacerlo de la forma más rápida posible independientemente de la distancia. En este punto "nace" internet.

2.2 ÁMBITO

La ciberseguridad abarca distintos ámbitos de la sociedad estando muy presente y cada día más, en la vida de las personas. Estos son los más destacados:

- Educacional: Es importante que la gente esté bien formada para que siempre pueda proteger sus propios intereses y no le priven de su derecho a la libertad.
- Laboral: Se debe de promover dentro de la empresa entre los empleados, no solo los directivos, una concienciación de empleo de estándares básicos de ciberseguridad para que no se produzcan pérdidas en de la empresa.

- Familiar: Dentro del núcleo familiar, los padres deben de proteger a sus hijos en la red como quien les pone límites cuando están fuera de casa por el hecho del riesgo al que están expuestos. Internet no se libra del peligro, y por el simple hecho de que estén en casa no quiere decir que estén a salvo, por lo que los padres deben de tener los conocimientos suficientes para poder proteger la privacidad de sus hijos. Es más, puede darse el caso de que sean los hijos quienes eduquen a los padres.
- Gubernamental: Este es un pilar fundamental ya que su objetivo consiste en proteger a los ciudadanos que utilicen los sistemas de información y telecomunicaciones. Para ello se ha desarrollado un marco normativo y el impulso de una estructura que aúne las distintas constituciones y agentes responsables y conocedores de la materia [(11)].

2.3 CIBERSEGURIDAD EN LA ACTUALIDAD

Según el INCIBE en su informe del 19/09/2016: El sector de la ciberseguridad constituye uno de los ámbitos tecnológicos de mayor proyección nacional e internacional para la industria, además de convertirse en un sector con enormes expectativas de empleo. El aumento de ciberataques, y la proliferación de nuevas amenazas con un grado de sofisticación elevado y creciente, conducen a la necesidad de incorporar profesionales expertos en ciberseguridad para cubrir puestos de trabajo especializados en distintos tipos de organizaciones [(12)].

La información es uno de los pilares más valiosos de cualquier empresa y uno de los perfiles que se están buscando en el mundo laboral es el de *responsable de Seguridad de la Información (**CISO** "Chief Information Security Officer" en inglés).* Su cometido consiste en proteger a la compañía y la información de ataques cibernéticos. Debe de tener conocimientos legales, teniendo como referencia el ISO 27001, estándar internacional para la seguridad de la información, y la LOPD, Ley Orgánica de Protección de Datos. Y sobre todo estar preparado antes el nuevo Reglamento General de Protección de Datos (GDPR) establecido por la Unión Europea, que se aplicará por encima de la LOPD a partir de mayo de 2018.

Deben disponer también de los certificados internacionales en el ámbito de la seguridad como la Certificación de Auditor de Sistemas de Información (CISA, por sus siglas en inglés), la Certificación en Riesgos y Control de Sistemas de Información (CRISC) o la Certificación en Gestión de Seguridad de la Información (CISM), entre otras.

De sus funciones he destacado:

- Los Responsables de Seguridad de la Información están al cargo de las siguientes funciones:
- Detección y análisis de los puntos débiles de la compañía en materia de ciberseguridad y protección informática.
- Desarrollo, ejecución y supervisión de las estrategias de seguridad de la información.
- Gestión, manejo y vigilancia del control de acceso a la información de la compañía.
- Control del cumplimiento regulatorio y normativo del negocio.
- Estar informado de las novedades del sector y mantener una constante actualización de conocimientos para dar una respuesta flexible y ágil a cualquier incidente cibernético que afecte a la empresa.
- Garantizar la máxima protección y privacidad de los datos e informaciones corporativa.
- Fijación y control presupuestario del departamento.

Es importante mencionar, para incentivar a los futuros candidatos al puesto, que el salario se asemeja al de los directores de IT del mercado, llegando incluso en algunos casos a superarlo. El salario puede variar en función de su formación, bagaje profesional o certificaciones, aunque también se valora mucho la experiencia dentro de la propia compañía y el conocimiento de sus procesos [25].

3 MOTIVACIÓN

A continuación, se exponen distintos puntos que han servido de motivación para el desarrollo del proyecto:

- Existencia creciente de preocupación por la ciberseguridad y aparición de iniciativas dispersas y de muy diferente índole.
    - Necesidad de encontrar una metodología que permita educar a todo tipo de personas en dicho tema y dirigirlas a los recursos más adecuados para ellas. Proporcionarles un método pedagógico *step-by-step* que les permita avanzar en su interés/capacidad para mejorar su seguridad
    - El poder ofrecer un espacio donde la gente aprenda y pueda expresar sus dudas junto el resto de personas que se hayan inscrito y puedan ayudarse las unas a las otras. Es importante que cumplan que vayan aprendiendo los conceptos desde lo más básico para que asienten las bases de lo que les espera en el futuro, dado que este campo crece cada día más y aun ritmo vertiginoso.
- Deficiencias en la educación sobre ciberseguridad.
    - En muchos casos se da la situación en el que los mismos educadores no están preparados para impartir esta materia, ya sea porque no precisan de los conocimientos necesarios o por el hecho de la falta de experiencia en el terreno.
- No se trata de un problema exclusivo de las élites.
    - Los mismos ciudadanos de a pie son víctimas potenciales de los ciberataques, por lo que es importante que cualquier persona que lo desee pueda utilizar esta herramienta y protegerse de cara a futuros ataques cibernéticos.
- Importancia de la ciberseguridad para toda la población en general y para algunos colectivos en particular, con mención a la geografía, legislación del lugar y actividad del colectivo.
    - Quiero destacar un informe en el cual se tratan los siguientes temas: Vigilancia digital, Privacidad contra la vigilancia; Ciberseguridad, sociedad

civil y vulnerabilidad en la era de las comunicaciones… Todo esto se puede encontrar en el Informe de 57 países sobre "Communications surveillance in the digital age" [(13)].

Del análisis de las motivaciones que han llevado al desarrollo de este trabajo se ha decidido que una herramienta de aprendizaje web es la mejor metodología a seguir para que más población participe activamente en su propia ciberseguridad…

Además, como queremos que sea una herramienta que pueda mejorarse de forma activa por parte de los usuarios necesitamos definir los distintos roles que van a existir en la herramienta, los permisos que poseen y la repercusión que debe alcanzar el usuario en la web para poder aspirar a un rol con más privilegios.

Los roles que existen en la web son los siguientes:

- **Administrador:** Se encarga como bien dice el nombre de administrar la configuración de la herramienta web.
- **Autor:** Tiene la capacidad de subir contenido a la web y crear así sus propios cursos y exámenes.
- **Suscriptor:** Es aquel usuario que decide suscribirse a los módulos de aprendizaje que se ofrecen en la web. Podrán convertirse en autores si participan de forma activa y positiva en la web.
- **Usuario eventual:** Solo dispone de la consulta de los apartados que no requieren suscripción, como puede ser el de "Perfiles Profesionales".

Un usuario cuando accede por primera vez a la web y se inscribe en alguno de los módulos ofertados, pasa a ser un *suscriptor*, pudiendo únicamente comentar y dar su opinión acerca de los contenidos que ha ido observando en la web.

Para que el usuario tuviera algo más de protagonismo en la herramienta, los *autores* de la web podrán dotar de más privilegios a aquellos suscriptores que hayan colaborado de manera activa aportando conocimiento, soporte y retroalimentación para ayudar a mejorar el funcionamiento de la herramienta.

De esta forma un usuario podría convertirse en *autor* y llegar a desarrollar y subir a la web su propio contenido y optimizar los ya existentes. Hay que reseñar que un autor podrá modificar contenidos de todos los módulos, a no ser que el administrador le reste espacio de maniobra en la herramienta, pero a priori podrá editar todos los módulos de aprendizaje.

El número de *autores* que puede haber en la web es ilimitado, dependerá de la decisión del *administrador* el otorgar privilegios a más usuarios. No hay un criterio estricto para pasar de suscriptor a autor, estará en la mano del administrador o administradores, ya que también podría haber más de uno si el administrador original quisiera repartir la carga de trabajo que conlleva la herramienta.

Aunque en este proyecto sólo desarrollamos la herramienta, la idea que subyace es que del uso de ésta por parte de diferentes colectivos se cree una comunidad que participe en la mejora de los contenidos de la herramienta mediante alguno de los roles anteriormente descritos.

4 TECNOLOGÍA EMPLEADA

A continuación, se va a especificar las herramientas, aplicaciones y/o tecnología empleadas para desarrollar el proyecto.

4.1 SERVIDOR WEB SEGURO

Para que la conexión del usuario con la herramienta web sea segura (fiable y confidencial) se ha implementado un servidor web seguro empleando el protocolo de seguridad SSL (Secure Sockets Layer), de forma que la comunicación entre el servidor y el usuario esté encriptada. Esto es necesario llevarlo a cabo para que los datos que se envían y reciben durante las transferencias de información estén protegidos, de modo que, si un hacker se hace con alguno de los paquetes de la transacción, le sea imposible (o muy difícil al menos) interpretar su contenido.

Es necesario comentar con más detalle el origen y uso del protocolo SSL.

Este protocolo tiene a grandes rasgos dos objetivos, *cifrar* la información entre el cliente y el servidor y la *identificación*, que consiste en garantizar que la máquina o servidor con el que estás comunicándote es con quien de verdad deseas establecer dicha comunicación.

- Cifrado: Se define el proceso en 4 pasos
    1. Los ordenadores entre los que se produce la comunicación se ponen de acuerdo en cómo cifrar la comunicación, empleando RSA, AES…
    2. Servidor envía un certificado al ordenador cliente, con una clave pública y el periodo de validez del certificado.
    3. Ahora desde el ordenador cliente empieza el cifrado de la información, se envían tres mensajes para lograrlo
        - Ambos ordenadores calculan el código secreto que van a usar.
        - El cliente le solicita al servidor que empiece a cifrar.
        - Ha terminado de cifrar el mensaje.
    4. El servidor recibe la petición del cliente y cifra los mensajes, de forma que ningún “man in the middle” pueda interpretar los mensajes que se están intercambiando.
- Identificación: Se define en 4 pasos

    1. La compañía solicita un certificado de autenticidad, para lo que la empresa deberá de brindar la siguiente información:
        - Servidor web.
        - Nombre de la compañía.
        - Donde se encuentra la compañía.

        - La autoridad certificadora verificará la autenticidad de la compañía.
    2. La autoridad certificadora crea un certificado para la compañía que contiene la siguiente información:
        - Número de serie.
        - Identificador del algoritmo.
        - Fecha de validez.
        - Clave pública del sujeto.
        - Identificador de la compañía.
        - Firma del algoritmo.
    3. El certificado se instala en el servidor de la web
        - Configurar el servidor web para utilizar el certificado.
    4. El buscador reconoce tu web como segura.

Para nuestra web se ha utilizado "*Let's Encrypt*" [(14)], una entidad certificadora que ofrece certificados SSL abiertos, libres y gratuitos. Ahora cuando los usuarios accedan a la web, en la URL les aparecerá "https://" al comienzo, indicando que la conexión es segura. Pasos a seguir:

- Acceder al panel de configuración del sitio e instalar Let's Encrypt.
- Actualizar las URL's de tu página, pasando de http a https
    - Accediendo a ajustes de la página y cambiando la dirección del sitio y de Wordpress.

4.2 HTML Y CSS

La herramienta de aprendizaje se ha desarrollado usando principalmente el lenguaje HTML, que permite crear la estructura de la web mediante etiquetas.

Ofrece una gran versatilidad, estructura lógica y es fácil de interpretar por humanos y máquinas. La estructura está formada por un árbol donde encontramos la raíz y a partir de ésta el resto de etiquetas se insertan de manera lógica. Todo realizado en un simple fichero de texto para el cual solo se necesita un editor como el bloc de notas que nos ofrece cualquier sistema operativo [(15)].

Un aspecto que merece la pena destacar es el hecho de que la información aparece dividida en bloques:

- **Cabecera (*Head*):** Información técnica.
    - Información contextual de la página: Metadatos que nos proporcionan información que no queda lo suficientemente clara en el contenido.
    - Referencia a otros ficheros: Todos los recursos que necesite la página aparecerán en este apartado, como por ejemplo CSS o JavaScript, etc…
    - Scripts y estilos: Pueden definirse en un documento externo independiente o aparecer en la cabecera.
- **Cuerpo (*Body*):** El resto de información o contenido.
    - Videos, enlaces, imágenes…

Para darle un estilo propio a la web se emplea lo que se conoce como hojas de estilos o CSS (*Cascading Style Sheet*) [(16)]. Algunas de sus características son:

- Definición de distancia entre distintos elementos del documento.
- Añadir elementos en el documento con mayor precisión.
- Definir la visibilidad de todos los elementos mostrados en el documento.
- Ofrece una gran flexibilidad a la hora de desarrollar el estilo de la web.
- Permite la combinación con lenguajes distintos.

A continuación, se destacan una serie de términos básicos de CSS sobre los que hay que profundizar.

4.2.1 WORDPRESS

Es un CMS (Content ManagementSystem) que permite crear y mantener los aspectos fundamentales de una web [(17)]. Desarrollado en PHP (Hypertext Preprocessor) para entornos que usen MySQL y Apache y es software libre.

CARACTERÍSTICAS PRINCIPALES:

- Sistema de publicación web basado en entradas ordenadas por fecha; clasificadas en una o más categorías o taxonomías.
- Su diseño visual se basa en el sistema de plantillas elegido, que puede tener distintas opciones de modificación dependiendo del autor de ésta.

- Bloques con funciones específicas.
- Plugins que permiten añadir funcionalidad extra a la web.

A continuación, se van a especificar los dos aspectos en torno a los que gira la herramienta web.

4.2.2 DIVI

DIVI es un tema que permite al usuario configurar de forma modular el diseño y estilo de su plantilla en Wordpress (Figura 2).

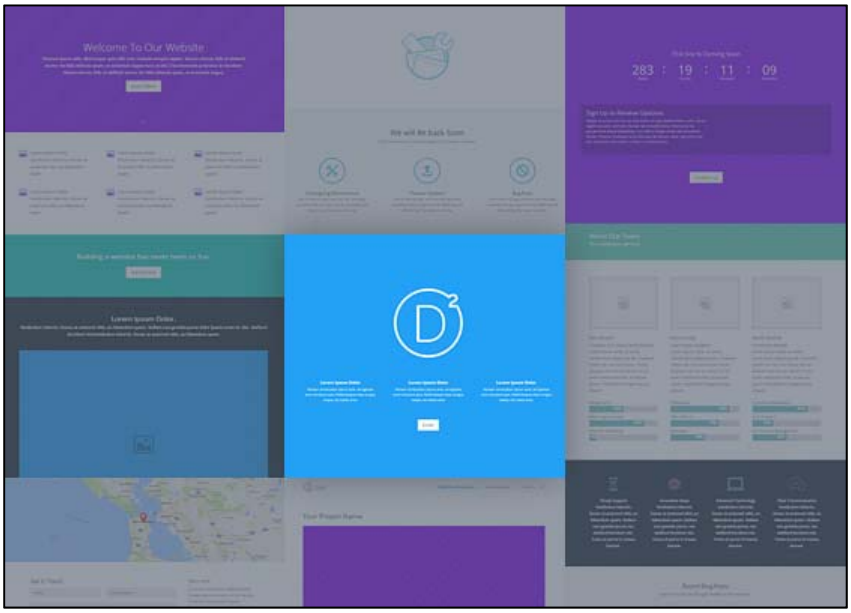


Figura 2: DIVI.

4.3 LEARNPRESS

Es un plugin que de Wordpress (Figura 3) que ofrece al usuario la posibilidad de convertir su web en un entorno de enseñanza adaptable a las necesidades del usuario.

Figura 3: LearnPress.

Las funciones que ofrece este plugin son:

- Creación de módulos/cursos de enseñanza:
    1. Dentro de la pestaña de Learnpress acceder a “Cursos”.
    2. Haz clic en el botón “Añadir nuevo”.
    3. Introducir los datos pertinentes:
        - Título del curso.
        - Breve introducción/explicación del mismo junto con una foto o video.
        - Añadir las lecciones que quieres que formen parte del curso.
- Creación de lecciones para los alumnos:
    1. Dentro de la pestaña de Learnpress acceder a “Lecciones”.
    2. Haz clic en el botón “Añadir nuevo”.
    3. Introducir los datos pertinentes:
        - Título de la lección.
        - Breve introducción/explicación de la misma junto con una foto o video.
        - Opción para limitar el tiempo de la lección.
- Creación de preguntas para utilizar en los exámenes:
    1. Dentro de la pestaña de Learnpress acceder a “Preguntas”.
    2. En el banco de preguntas hacer click en “Añadir nuevo”.
    3. Introducir los datos pertinentes:
        - Título de la pregunta.
        - Breve introducción/explicación de la misma junto con una foto o video.
        - Tipo de respuesta:
            - Verdadero o falso.
            - Opción múltiple.
        - Explicación de la pregunta.
        - Opción para dar pistas.

- Creación de exámenes para evaluar a los alumnos:
    1. Dentro de la pestaña de Learnpress acceder a “Exámenes”.
    2. Haz clic en el botón “Nuevo examen”.
    3. Introducir los datos pertinentes:
        - Título del examen.
        - Breve introducción/explicación de la misma junto con una foto o video.
        - Campo donde añadir las preguntas.
        - Opción para mostrar/ocultar la pregunta.
        - Duración.
        - Grado de aprobación del examen.
        - Campo para decidir si se puede rehacer el examen.
        - Verificación de respuesta.
        - Opción para dar pista.

4.4 SQL

Es un lenguaje empleado en la gestión de bases de datos relacionales [18]. El uso de este lenguaje nos permite efectuar consultas, de forma sencilla, de la información que almacena la base de datos, así como hacer cambios en ellas.

De sus características principales cabría destacar:

- Definición de datos:
    - Opciones para desarrollar eliminar y modificar esquemas de relación.
- Modificación de datos:
    - Opciones para realizar consultas y modificar las tuplas resultantes.
- Integridad:
    - Ofrece restricciones de integridad.
- Control de transacciones:
    - Se puede especificar el comienzo y fin de una transacción.
- Definición de vistas: Se incluyen comandos que permiten definir vistas.

- SQL incorporado y dinámico: Capacidad para incorporar instrucciones de SQL en lenguajes como Java, C++, PHP…
- Autorización: Se incluyen comandos para especificar el acceso a las relaciones y vistas de la base de datos.

4.4.1 Tablas creadas

Vamos a comentar las tablas creadas durante la instalación de WP, así como la relación entre ellas:

- wp_commentmeta: Cada comentario contiene información denominada meta data y se almacena en wp_commentmeta (Figura 4).

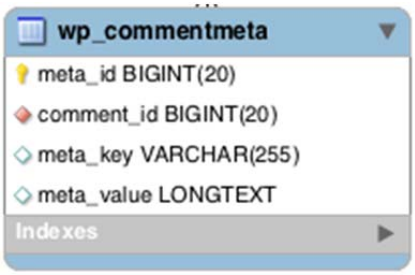


Figura 4: wp_commentmeta.

- wp_comments: Los comentarios dentro de WordPress se almacenan en la tabla wp_comments (Figura 5).

Figura 5: wp_comments.

- wp_links: Contiene información relacionada con los enlaces introducidos en la función de enlaces de WordPress (Figura 6).

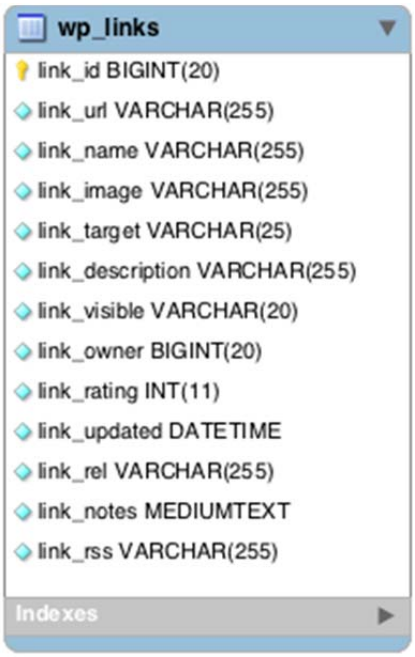


Figura 6: wp_links.

- wp_options: Las opciones definidas en el panel Administración> Configuración se almacenan en la tabla wp_options (Figura 7).

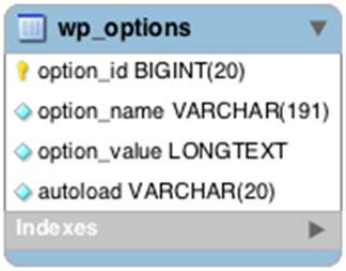


Figura 7: wp_options.

- wp_postmeta: Cada post contiene información denominada metadatos y se almacena en wp_postmeta (Figura 8).

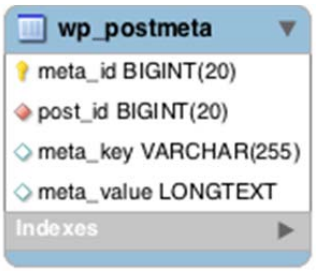


Figura 8: wp_postmeta.

- wp_posts: El núcleo de los datos de WordPress son los posts. Se almacena en la tabla wp_posts. También las páginas y los elementos del menú de navegación se almacenan en esta tabla (Figura 9).

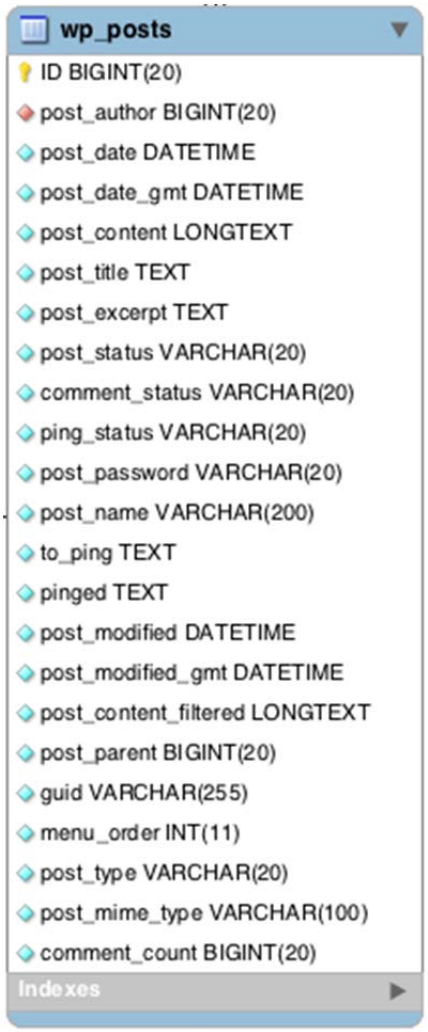


Figura 9: wp_posts.

- wp_terms: Las categorías de las dos publicaciones y los enlaces y las etiquetas de las publicaciones se encuentran en la tabla wp_terms (Figura 10).

Figura 10: wp_terms.

- wp_term_relationships: Los posts se asocian con categorías y etiquetas de la tabla wp_terms y esta asociación se mantiene en la tabla wp_term_relationships. La asociación de enlaces a sus respectivas categorías también se mantiene en esta tabla (Figura 11).

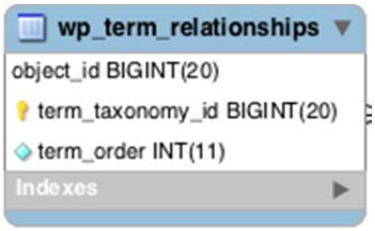


Figura 11: wp_term_relationships.

- wp_term_taxonomy: Esta tabla describe la taxonomía (categoría, vínculo o etiqueta) de las entradas de la tabla wp_terms (Figura 12).

Figura 12: wp_ term_taxonomy.

- wp_usermeta: Cada usuario ofrece información denominada metadatos y se almacena en wp_usermeta (Figura 13).

Figura 13: wp_ usermeta.

- wp_users: La lista de usuarios se mantiene en la tabla wp_users (Figura 14).

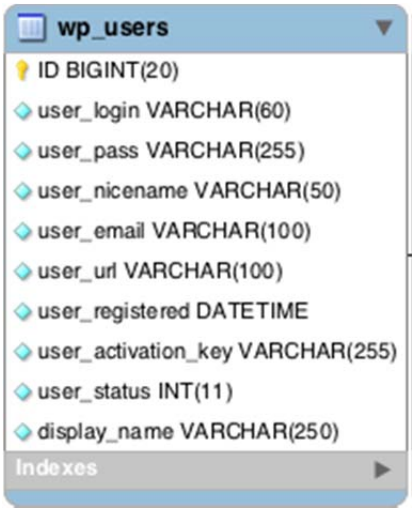


Figura 14: wp_ users.

4.4.2 DIAGRAMA UML DE LA BASE DE DATOS

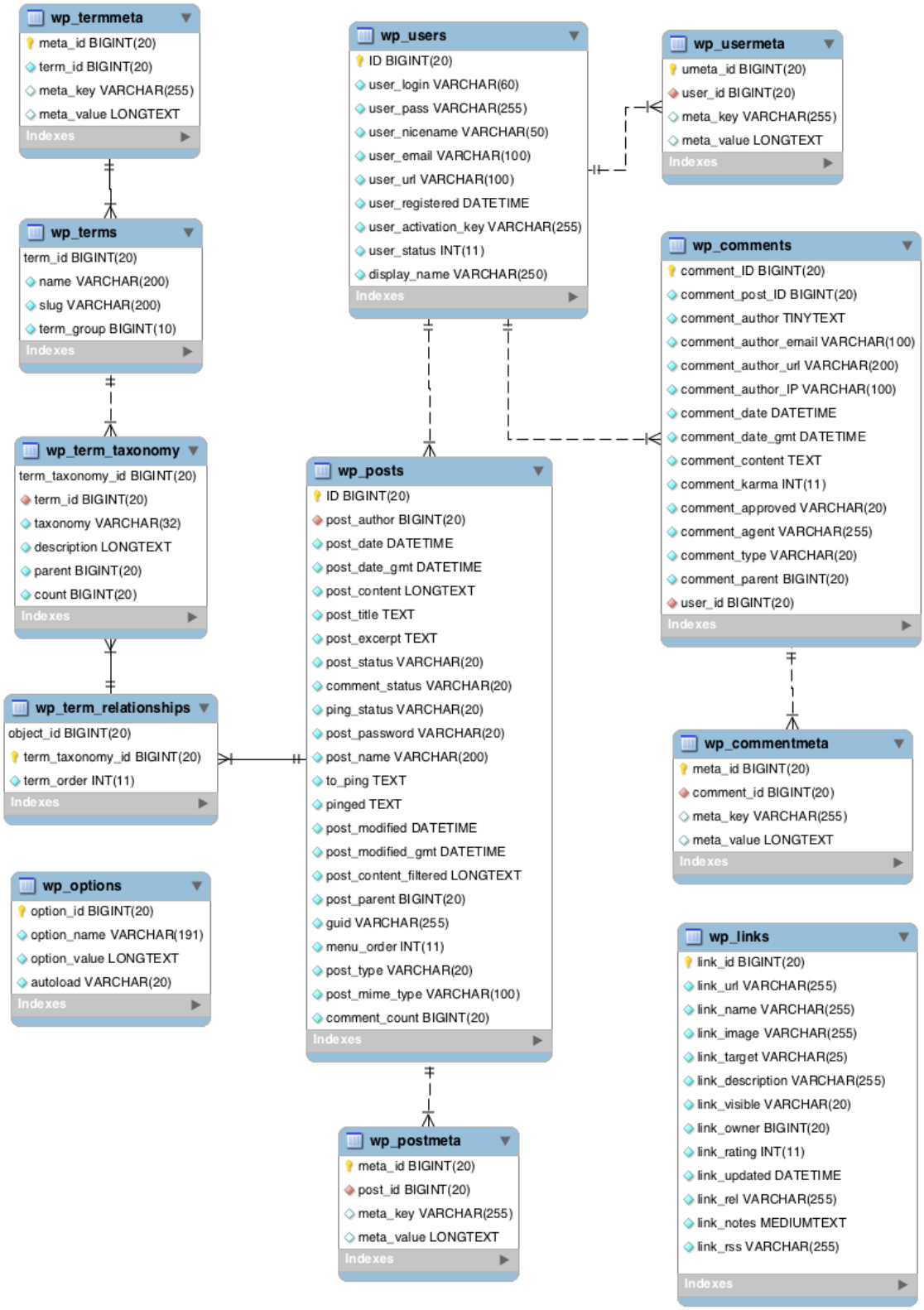


Figura 15: Diagrama UML.

4.5 PHP

Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.
Lo que distingue a PHP de algo del lado del cliente como Javascript es que el código es ejecutado en el servidor, generando HTML y enviándolo al cliente. El cliente recibirá el resultado de ejecutar el script, aunque no se sabrá el código subyacente que era
Lo mejor de utilizar PHP es su extrema simplicidad para el principiante, pero a su vez ofrece muchas características avanzadas para los programadores profesionales [19].

Características a destacar:

- Permiten efectuar consultas con el fin de recuperar, de forma sencilla, información de bases de datos, así como hacer cambios en ellas.
- Tiene la posibilidad de utilizar programación por procedimientos o programación orientada a objetos (POO), o una mezcla de ambas.
- Con PHP no se está limitado a generar HTML. Entre las capacidades de PHP se incluyen la creación de imágenes, ficheros PDF, texto XHTML, e incluso películas Flash.
- Soporte para un amplio abanico de bases de datos.
    - MySQL, PDO, ODBC, CURL…
- Procesamiento de texto.
- Capacidad para ampliar su funcionalidad utilizando módulos.
- Manejo de excepciones.

5 ESTRUCTURA DE LA WEB

En este apartado de la memoria se presentará la estructura de la herramienta diseñada.

5.1 DIAGRAMA DE LA ESTRUCTURA DE LA WEB

Esta es la estructura de la web, analizando cada una de las páginas desde que accedes al dominio https://ciberseguridad.jacynycz.es (Figura 16).

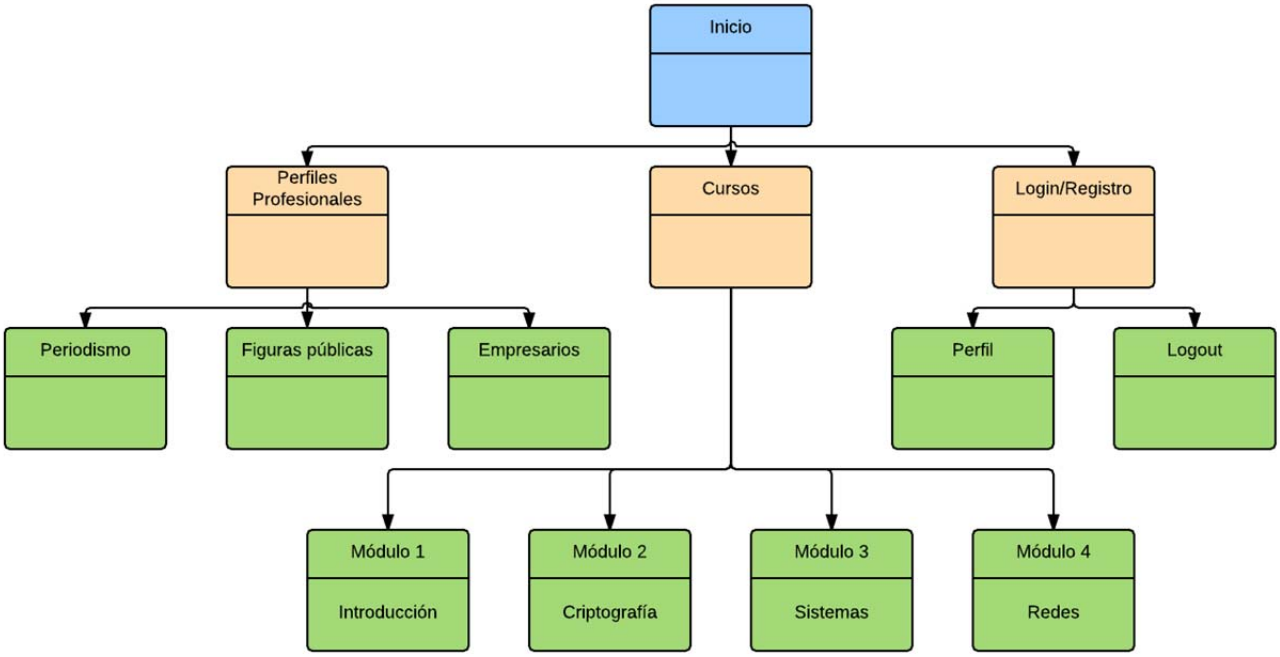


Figura 16: Estructura web.

5.2 INICIO

A la hora de acceder a la web, se presenta la información básica de las funciones que desempeña la herramienta. Se muestran también los distintos apartados desarrollados en el menú superior (Figura 17).

Figura 17: Inicio de la web.

En el *body* inferior se muestra las tres características más relevantes de la página (Figura 18).

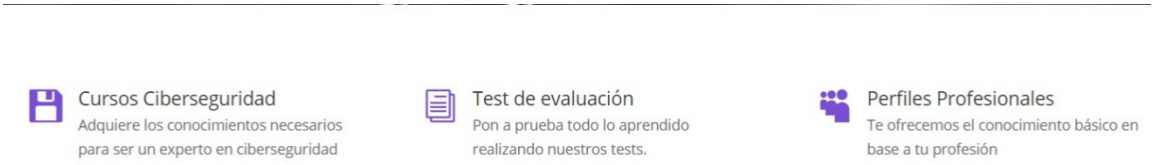


Figura 18: Body inferior.

5.3 CURSOS

En esta sección los usuarios podrán encontrar toda la teoría necesaria para empezar a formarse en ciberseguridad y Hacktivismo. Se han escogido en principio cuatro módulos de aprendizaje centrados en distintos temas que se han considerado básicos para iniciarse en la materia.

5.3.1 Módulo 1: Introducción

En este módulo se pretende concienciar al usuario de la importancia de la seguridad y se le brindan una serie de conceptos muy básicos para empezar su aprendizaje en la materia.

Se divide en dos lecciones, la primera haciendo énfasis en definiciones de términos elementales para poder avanzar en la materia de ciberseguridad, como puede ser *"diferencias entre un hacker y un cracker"* o los pasos a seguir para atacar un objetivo o defenderse de un ataque, etc...

La segunda parte del módulo se centra en los orígenes de internet, explicando cómo se formó ARPANET, la creación del protocolo TCP...

5.3.2 Módulo 2: Criptografía

En este módulo se estudian los conceptos de la criptografía aplicados a la ciberseguridad.

Los puntos que se estudian son:

- Objetivos
- Conceptos básicos
- Técnicas clásicas (Ejemplos)
    - Sustitución
    - Desplazamiento
- Técnicas más avanzadas (Ejemplos)
    - DES
    - RSA
    - PKI

5.3.3 Módulo 3: Sistemas

En este módulo se abordará el funcionamiento de un sistema desde el punto de vista del sistema operativo Linux.

Elementos que se analizan:

- Usuarios y grupos
- Archivos
- Programas

Se considerarán los activos anteriores de forma que se puedan defender ante un ataque dirigido.

También se analizarán distintas amenazas para nuestros sistemas, como pueden ser troyanos, gusanos, virus, …. Y la manera de poder contrarrestarlos.

5.3.4 Módulo 4: Redes

En este módulo se empieza definiendo el protocolo TCP/IP, cuál es su objetivo, etc.

Se define el modelo OSI con respecto el protocolo TCP/IP con sus respectivas capas y las vulnerabilidades que puede haber en cada una de ellas. (Figura 19)

Figura 19: Modelo OSI vs Protocolo TCP/IP.

5.4 PERFILES PROFESIONALES

La idea de este apartado es habilitar una sección donde los usuarios acudan buscando conocimiento y/o herramientas con un enfoque concreto basado en el campo en el que están especializados. Un ejemplo referente podría ser el *perfil periodístico*, donde los usuarios encontrarían consejos o manuales para encriptar sus comunicaciones a la hora de comunicarse con sus confidentes. En este caso cabe mencionar un episodio real que tuvo lugar en el año 2013, cuando Glenn Greenwald, periodista del *The Guardian*, publicó las revelaciones sobre el programa de vigilancia PRISM y otros programas de la NSA gracias a la información proporcionada por Edward Snowden. Todo esto se produjo cuando Glenn Greenwald comenzó a utilizar GPG para cifrar sus correos, de otra forma Edward Snowden jamás habría compartido su información (2).

Otro perfil que se ha decidido añadir es el de *figuras públicas,* inspirado en la necesidad que se ha podido observar en la sociedad cuando un famoso ha sido hackeado y ha visto como su intimidad queda al descubierto. Por poner un caso más concreto, últimamente se ha dañado la imagen de muchas actrices al hackear sus smartphones, accediendo en muchos casos a sus cuentas personales, descargar de esta forma fotos íntimas de alto contenido erótico que suben a la red más adelante [(20)].

5.5 EXAMEN DE EVALUACIÓN

Cuando el usuario se inscriba en el primer módulo, después de completar los temas de introducción y orígenes, tendrá que hacer un examen tipo test para poder evaluar sus conocimientos en ciberseguridad, de forma que se pueda discernir el grado de conocimiento actual del usuario en ese momento.

Si el alumno aprobara el examen se le notificaría al moderador que lo puso para poder darle así permiso para poder llevar a cabo el siguiente módulo de aprendizaje. En el perfil del usuario aparece una barra de progreso del curso, el cual aparecerá completado cuando termine las lecciones y apruebe los exámenes que lo compongan.

En caso de suspenderlo no podría seguir avanzando, pero se cuenta con la opción, en función de lo que decida el moderador, de repetir el examen hasta que el usuario lo apruebe.

Las preguntas elegidas para comprobar dicho nivel son las siguientes:

1. ¿En qué consiste la ciberseguridad?
    - El uso de herramientas de espionaje a favor de la sociedad
    - La defensa del ciberespacio
    - Prevenir a toda costa que la gente sepa hackear
    - Infiltrarse en las redes de grupos terroristas

(Con esta primera cuestión se busca conocer si el usuario tiene claro el concepto de ciberseguridad).

2. De los siguientes hechos que vamos a mostrar, indica aquel que se corresponde con un ejemplo de hacktivismo:
    - Una banda organizada roba a los clientes de un banco a través de internet
    - Unos estudiantes irrumpen en la web de su profesor de universidad y cuelgan fotos obscenas
    - Una organización trata de revelar información confidencial de una empresa que se lucra injustamente de sus clientes
    - Unos delincuentes usurpan la identidad de empresarios para hacerse con su negocio

(En este caso se quiere saber si el usuario sabe lo que es el hacktivismo a base de los

3. ¿Cuál es la diferencia entre un virus, un gusano y un troyano?
    - Un virus se replica a sí mismo, un gusano hace lo mismo adhiriéndose a un archivo y un troyano no se puede replicar
    - Un virus se replica a si mismo adhiriéndose a un archivo, un gusano no puede replicarse y un troyano sí que se replica
    - Un virus se replica a si mismo adhiriéndose a un archivo, un gusano se replica sin necesidad de ningún archivo y el troyano no puede replicarse

(En esta pregunta se busca conocer el grado de conocimiento del usuario en relación con los programas dañinos que puedan afectar al sistema, haciéndole elegir la definición correcta para lo que es un virus, un gusano y un troyano).

4. ¿Qué web de las que se muestran a continuación encripta la comunicación entre los usuarios y la web?
    - http://www.ases.com
    - https://www.bbvamola.es
    - ftp://download.miproyecto.com
    - http://ciberseguridad.es

(En esta pregunta se pretende conocer el grado de conocimiento en la rama de seguridad web, a la hora de fijarse en el link de la página seleccionada).

5. ¿De los sistemas mostrados a continuación, cuál se utilizar para prevenir un ataque?
    - IDS
    - IPS

(Con esta pregunta el objetivo consiste en elegir, por parte del usuario, la mejor herramienta o sistema a la hora de prevenir un ataque).

6. ¿Qué tipo de herramienta podemos emplear para permanecer anónimos en la red?
    - VPN
    - WPA
    - WEP
    - CSMA-CD

(A la hora de mantener nuestro anonimato al navegar por internet es necesario conocer qué tipo de herramientas nos proporcionan este tipo de protección).

Las preguntas que se realizan a continuación se van a centrar en las redes, que es un aspecto fundamental de la ciberseguridad.

7. ¿Cuál es el propósito del proceso del "routing"?
    - Dividir el mensaje en paquetes para acortar el mismo
    - Seleccionar el camino óptimo para dirigir el trafico de datos a la red deseada
    - Enviar datos a todos los destinatarios de un red de forma directa
    - Convertir un URL a una dirección IP

(El routing es un aspecto básico dentro de la conexión a internet, por lo que se exige que el usuario domine esté ámbito)

8. ¿Cuál es el propósito de autenticación del usuario en una red?
    - Conseguir los datos del usuario para su futuro uso
    - Determinar qué tipo de recursos se le van a proporcionar el usuario
    - Mantener el registro de las acciones del usuario
    - Exigir al usuario que pruebe su identidad

(La autenticación es MUY importante a la hora de navegar por internet)

9. ¿Qué protocolo de red se emplea para asignar automáticamente una dirección IP a un ordenador en una red?
    - FTP
    - DHCP
    - SMTP
    - CSMA

(Esta es una pregunta algo más “avanzada” pero se considera relevante en el ámbito global de la ciberseguridad)

10. ¿Qué capa del modelo OSI se encarga del routing?
    - Transporte
    - Red
    - Aplicación
    - Física

(Que el usuario tenga conocimiento del modelo OSI es imprescindible para su inicio en el aprendizaje en ciberseguridad, dado que en este modelo se sustenta la arquitectura de redes).

6 PROYECCIÓN DE FUTURO

En este apartado se propondrán las mejoras que podrán mejorar la funcionalidad y/o contenidos de la herramienta web.

- Se añadirán dos secciones más:
    - Tutoriales y manuales: Sección donde los usuarios aprenderán a utilizar determinados programas para satisfacer sus necesidades respecto al tipo de problema que les haya surgido. En concreto los contenidos o conocimientos que se impartirán a priori serán los siguientes:
        - **Como montar un servidor web seguro:** Cuando los usuarios se conectan a la web, es necesario añadir una capa más de seguridad mediante protocolos de seguridad, como puede ser el SSL, para cifrar el contenido de las comunicaciones del usuario con la web, garantizando de esta forma la fiabilidad y confidencialidad durante las transacciones [(21)].
        - **Privacidad en los servicios web:** En la era de la comunicación, las personas hacen público en su día a día cantidad ingente de información en las redes sociales que creen que solo sus contactos pueden ver. Es necesario concienciar a los usuarios de estas redes de que revisen la política de privacidad y enseñarles a administrar sus perfiles para que sean capaces de añadir más capas de seguridad por ellos mismos [(22)].
        - **Usar de forma correcta y segura tu Smartphone:** Los teléfonos móviles que se usaban antaño, únicamente empleados para llamar y enviar mensajes de texto, han sido sustituidos por los Smartphones, debido a su amplia gama de funciones y versatilidad que hacen la vida del usuario más sencilla. El poder conectarse a internet para acceder a las redes sociales es la característica más utilizada y es necesario ofrecer una serie de consejos en ciberseguridad para que el usuario esté siempre a salvo de cualquier tipo de ataque, y use su terminal de manera responsable [(23)].

        - **Deep y dark web:** Son todas aquellas páginas que no están indexadas por los motores de búsqueda tradicionales, como google, bing… y por lo tanto no puedes acceder a ellas públicamente. Toda a la información de la Deep web abarca el 90% del contenido de la red y es interesante que el usuario sepa desenvolverse en ella [24].
    - Herramientas y programas: Este apartado es necesario que exista para complementar al anterior. Que aprendan a usar un programa gracias al manual, pero no lo puedan obtener se antoja absurdo, pues en esta sección los usuarios tendrán la oportunidad de descargar las herramientas que necesiten.
- Se ampliará el apartado de Perfiles Profesionales:
    - Esta sección abarca únicamente el ámbito profesional, como bien indica el título, pero la idea es que se traten otro tipo de perfiles para llegar a más usuarios que necesiten esta formación.
        - Perfil basado en la edad
        - Perfil basado en Conocimientos
- Mejora del seguimiento del usuario
    - En el punto en el que se encuentra la herramienta los usuarios son independientes a la hora de realizar los cursos de aprendizaje, el moderador o administrador que ha creado el curso impone unos temas y unos exámenes que el usuario debe aprobar para finalizar el curso de forma satisfactoria, pero no puede ver el transcurrir del usuario mientras los lleva a cabo. Una mejora del seguimiento del usuario podría ser útil en ciertos casos para implementar el rol "*profesor alumno*" y así el moderador podría guiar a los usuarios que el considerase en función de cómo están llevando el módulo.

7 APÉNDICE

7.1 MANUAL DE USO

En este apartado se mostrará un manual de la herramienta web en base al rol que el usuario tenga asignado. Los roles que se pueden encontrar de menor a mayor privilegio son suscriptor, autor y administrador. Importante señalar que las funciones que pueden llevar a cabo los suscriptores pueden realizarlas también los autores, y las que estos lleven a cabo también podrán ser desempeñadas por los administradores.

7.1.1 SUSCRIPTOR

- Antes de poder obtener un rol en la página debes registrarte en "https://ciberseguridad.jacynycz.es" (Figura 20), y así lograr acceder al contenido exclusivo.

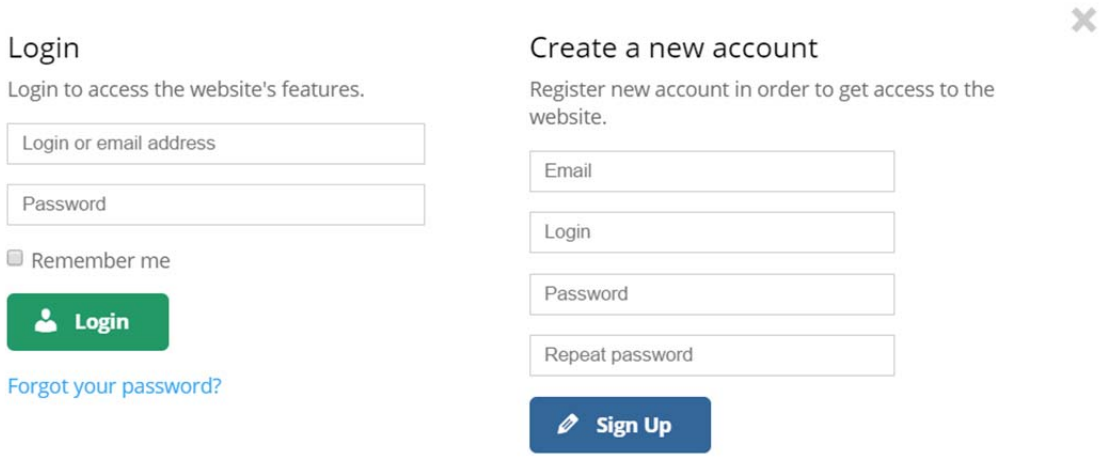


Figura 20: Login/Registro.

- A continuación, se accederá a la página principal de la web, donde en el menú superior derecho podrás encontrar las siguientes secciones (Figura 21):

Figura 21: Menú principal.

- Entrando en “Perfiles Profesionales” podemos ver el contenido dedicado al sector periodístico, empresarial y figuras públicas. Pongamos como ejemplo el periodístico. (Figura 22).

Figura 22: Perfil periodístico.

- Una vez dentro podremos ver los consejos que se ofrecen a los profesionales de este sector (Figura 23):

Emplear una contraseña segura:

1. Usar una contraseña que sea distinta del resto de tus cuentas
2. Usar una contraseña compuesta por números, letras y símbolos
3. No utilices información personal ni palabras comunes para crearla
4. Emplea un administrador de contraseñas para que esté a buen recaudo

Usa PGP en tus emails

PGP es un programa de criptografía de llave pública. Se emplea para proteger la privacidad en las comunicaciones. Es una herramienta imprescindible para los periodistas si pretenden intercambiar información con una fuente cuyo deseo es permanecer en el anonimato. Funciona usando un par de claves, una pública(para que nuestros contactos puedan enviarnos información) y una privada(para descifrar los correos recibidos y firmas los enviados, para asegurar que fueron enviados por ti) Modo de uso:

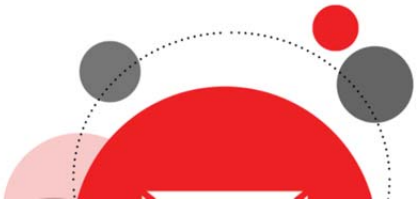


Figura 23: Perfil periodístico consejos.

- A continuación, conviene analizar la sección “Cursos” donde los suscriptores podrán inscribirse a los mismos para poder realizarlos (Figuras 24 y 25).

Figura 24: Cursos.

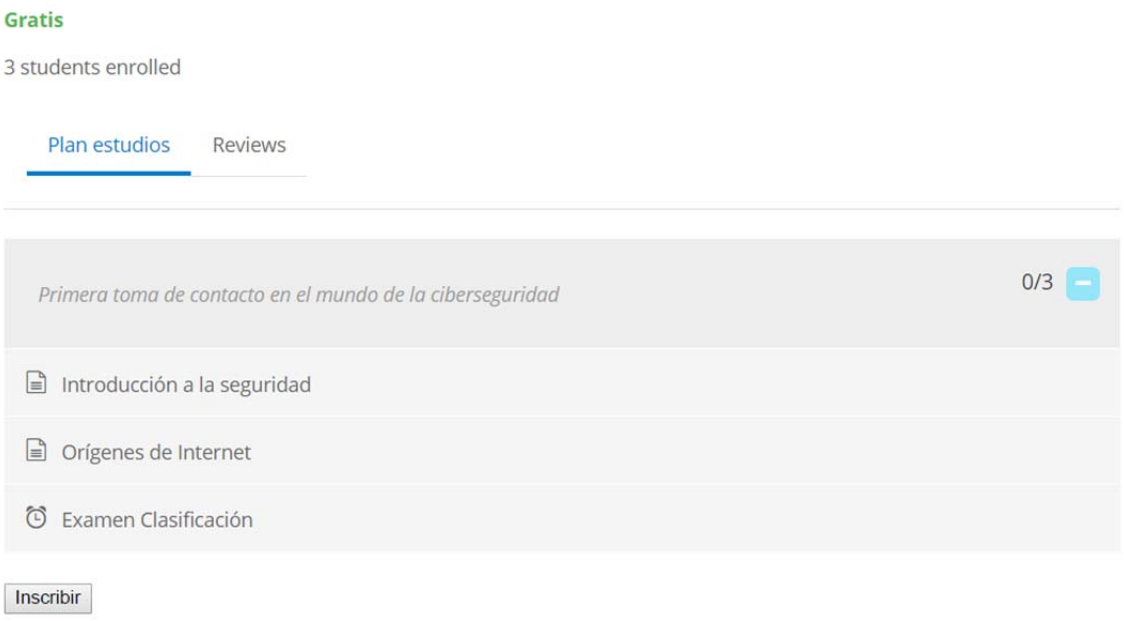


Figura 25: Inscribirse Cursos.

- Una vez el usuario se ha inscrito en el curso, podrá estudiar los contenidos que se les proporcionan y realizar el examen de evaluación (Figuras 26, 27 y 28).

Figura 26: Contenido Curso.

Figura 27: Examen Curso.

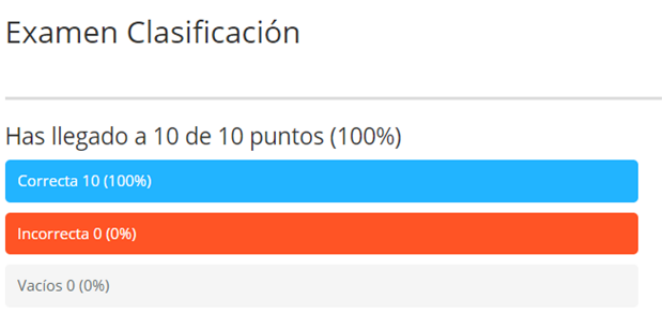


Figura 28: Examen Completo.

- Por último, el usuario podrá consultar y modificar su perfil dentro de la herramienta (Figuras 29 y 30):

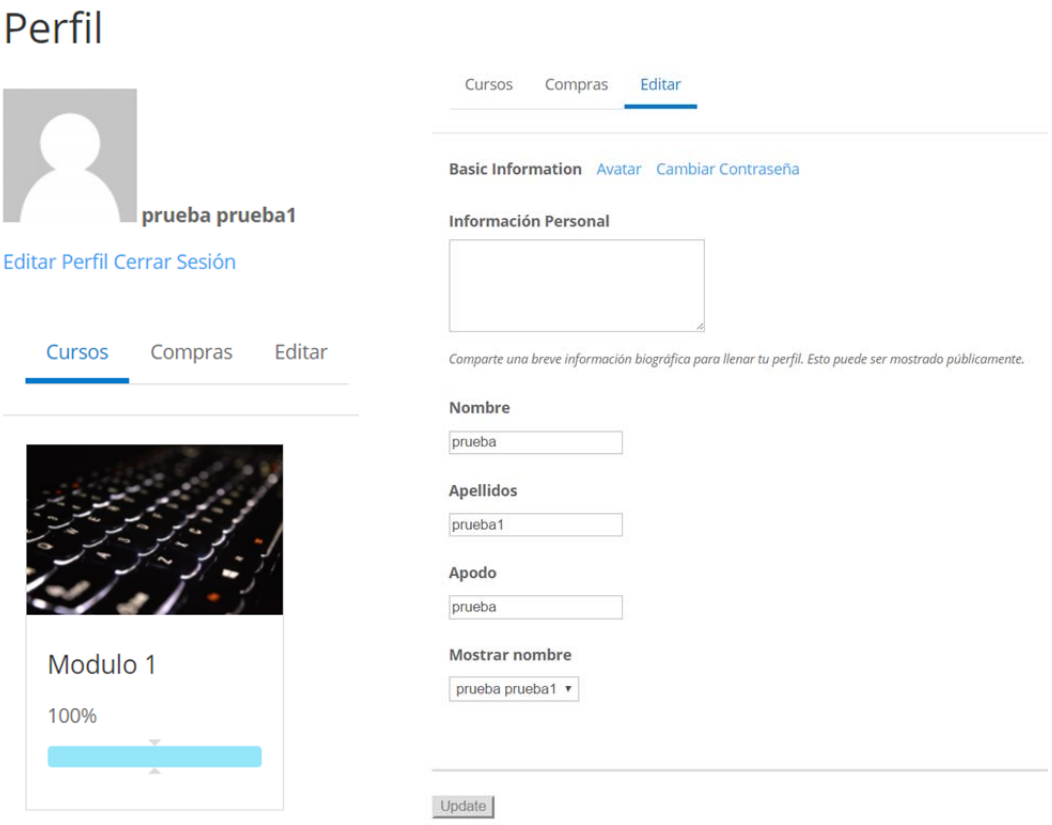


Figura 29 y 30: Acceso y edición Perfil.

7.1.2 AUTOR

EL autor es un rol que se sitúa por encima del rol de suscriptor, y tiene privilegios de edición en la herramienta. Tiene un menú, en el panel lateral izquierdo de la página, para realizar todos estos cambios (Figura 31).

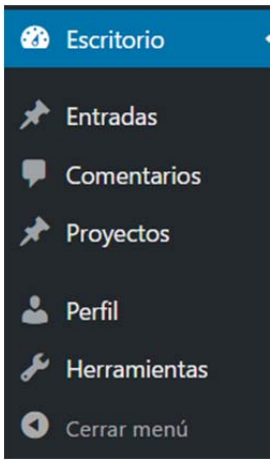


Figura 31: Menú autor.

- Pueden añadir entradas y gestionar comentarios en los módulos (Figuras 32 y 33):

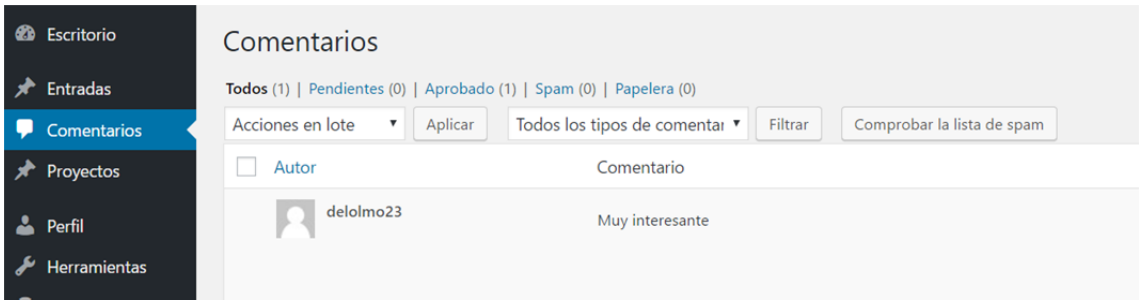


Figura 32: Comentarios.

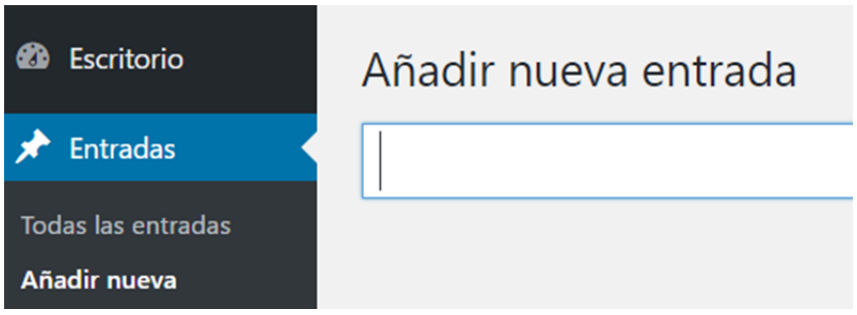
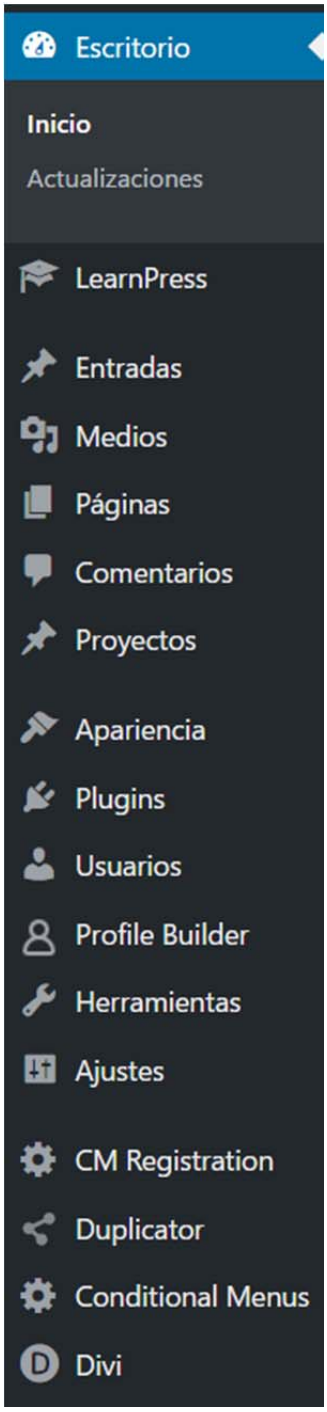


Figura 33: Entradas.

7.1.3 ADMINISTRADOR

Este es el rol de la herramienta con mayores privilegios y el que mayor funcionalidad tiene. Su menú está cargado de distintos apartados (Figura 34):



- LearnPress: Plugin de enseñanza que se ha utilizado en la herramienta.

- Entradas: Son los distintos Post que pueden publicarse en la web.

- Medios: Opción para subir contenido multimedia a la web (Fotos, videos, música...).

- Páginas: Apartado para crear y modificar las páginas de la web.

- Comentarios: Opción para administrar los comentarios que se han publicado en las páginas.

- Proyectos: Te permite crear y administrar distintos proyectos.

- Apariencia: Te permite cambiar el estilo de la pagina, modificando desde la interfaz que te habilita Wordpress o desde el CSS de la plantilla elegida.

- Plugins: Módulos que añaden funcionalidad extra a la web de forma automática, sin tener que programar.

- Usuarios: Permite añadir/eliminar usuarios y editar los permisos y roles que poseen.

- Divi: Plugin que se ha elegido para dotar del estilo deseado a la herramienta web y donde puedes editar el mismo.

Figura 34: Entradas.

- Una de las características más importantes del administrador radica en la capacidad de crear cursos (Figura 35):

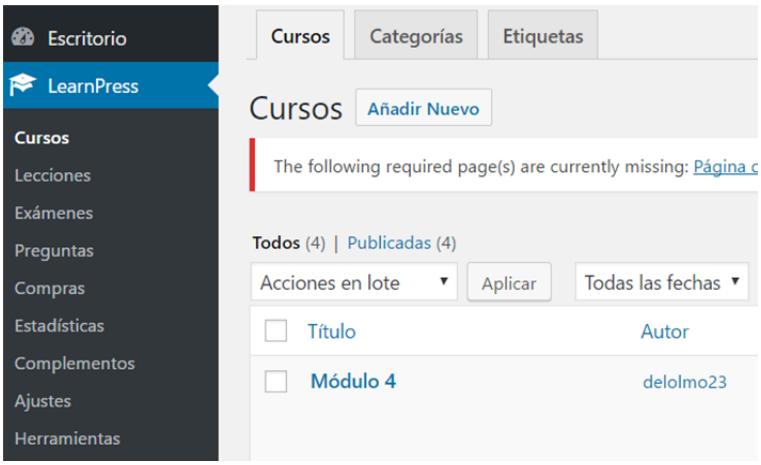


Figura 35: Crear curso.

- Una vez creado el curso debes introducir las lecciones que deseas que se imparta en éste (Figura 36).

Figura 36: Agregar lecciones al curso.

- Por último, editamos las opciones del curso a nuestro gusto (Figura 37).

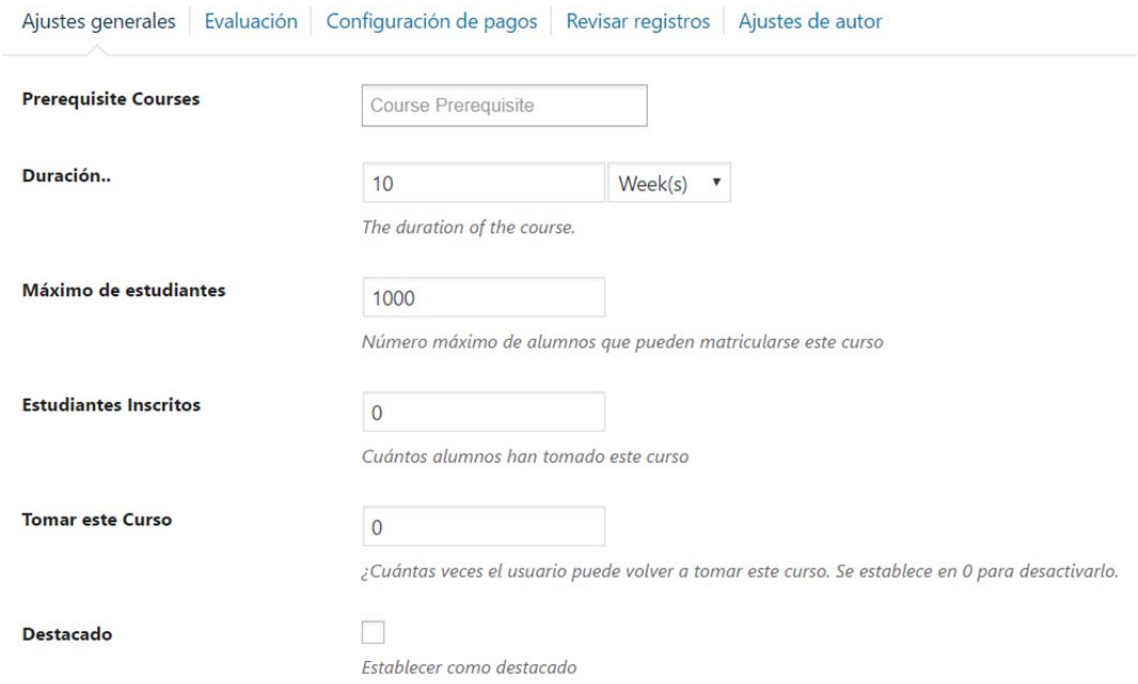


Figura 37: Editar opciones del curso.

- Como hemos visto en el apartado anterior, los cursos necesitan tener lecciones ya creadas para que los cursos tengan contenido que mostrar (Figura 38).

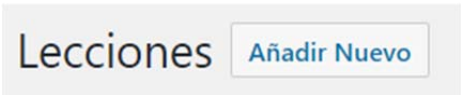


Figura 38: Añadir lección.

- A continuación, se debe editar la lección en si misma (Figura 39).

Figura 39: Editar lección.

- El siguiente punto que hay que tratar es la elaboración de exámenes (Figura 40).

Figura 40: Crear examen.

- Añadir las preguntas pertinentes que quieres que aparezcan (Figura 41).

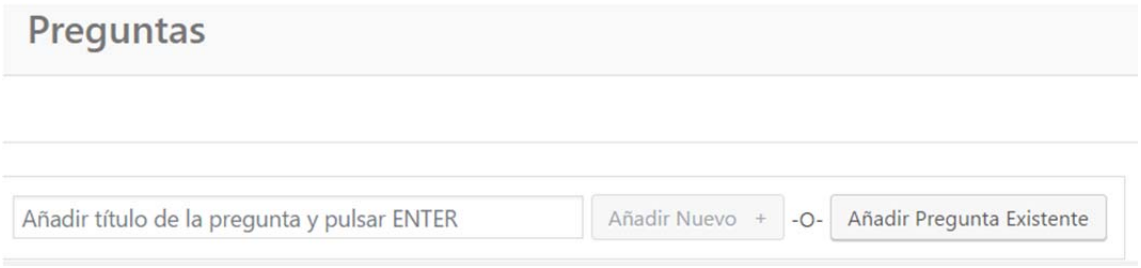
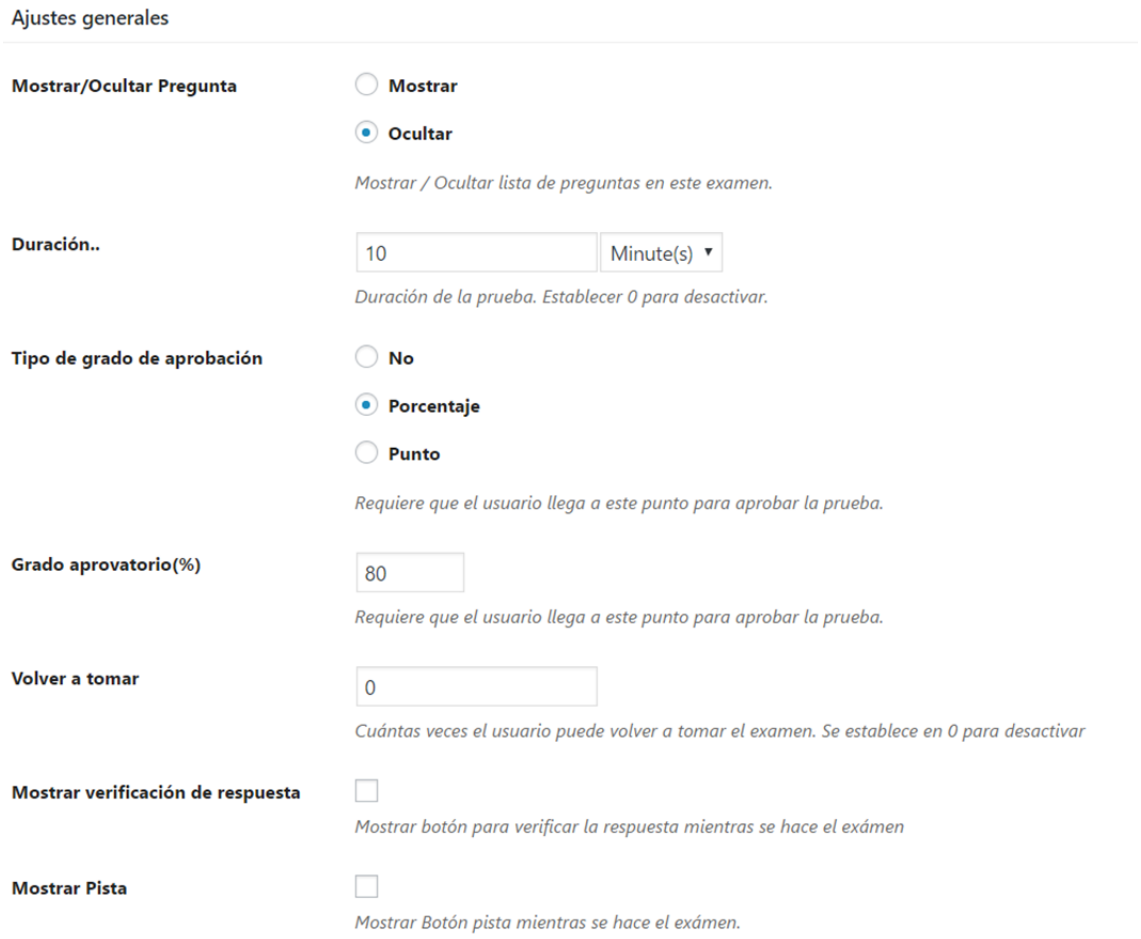


Figura 41: Añadir preguntas al examen.

- Para finalizar, se deben rellenar los campos correspondientes a la edición del examen (Figura 42).



- El último apartado que vamos a tratar es el de crear las preguntas de los exámenes (Figura 43).

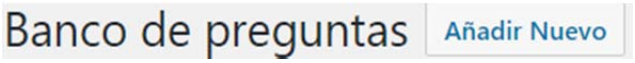


Figura 43: Crear preguntas.

- Las preguntas pueden ser de tipos variados, el que vamos a mostrar es Verdadero o Falso (Figura 44).

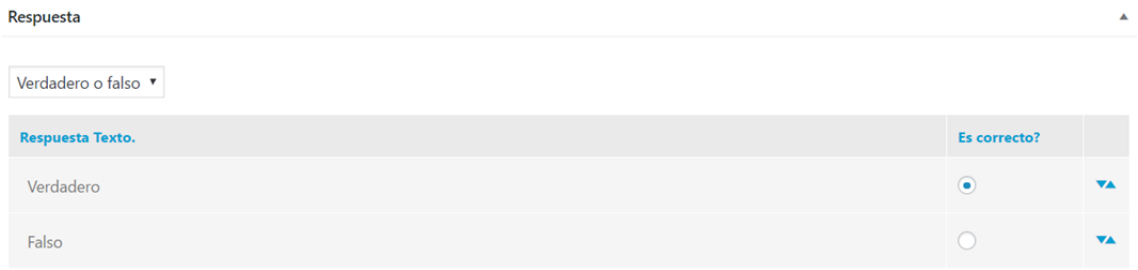


Figura 44: Tipo preguntas.

- Ya, por último, modificar los ajustes de las preguntas (Figura 45).

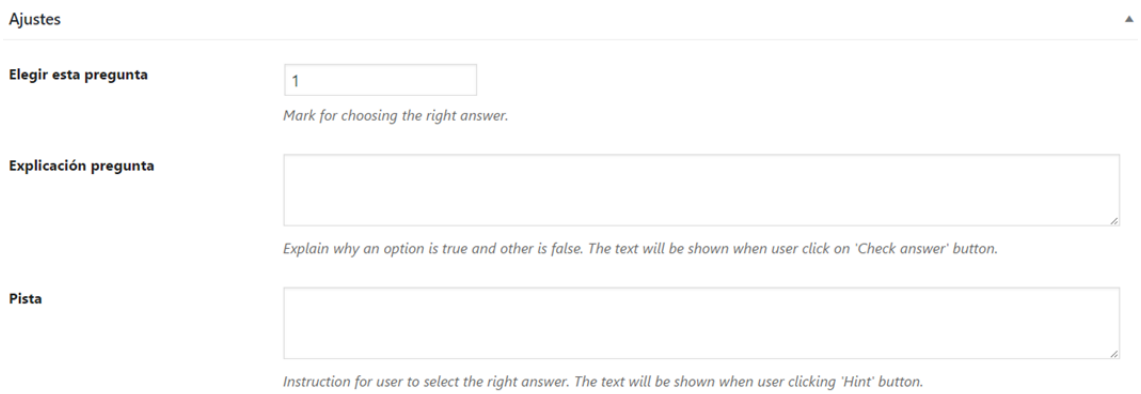


Figura 45: Ajustes preguntas.

- El administrador, como hemos comentado anteriormente tiene la capacidad de asignar roles a los distintos usuarios y a estos roles asignarles una serie de permisos (Figura 46).

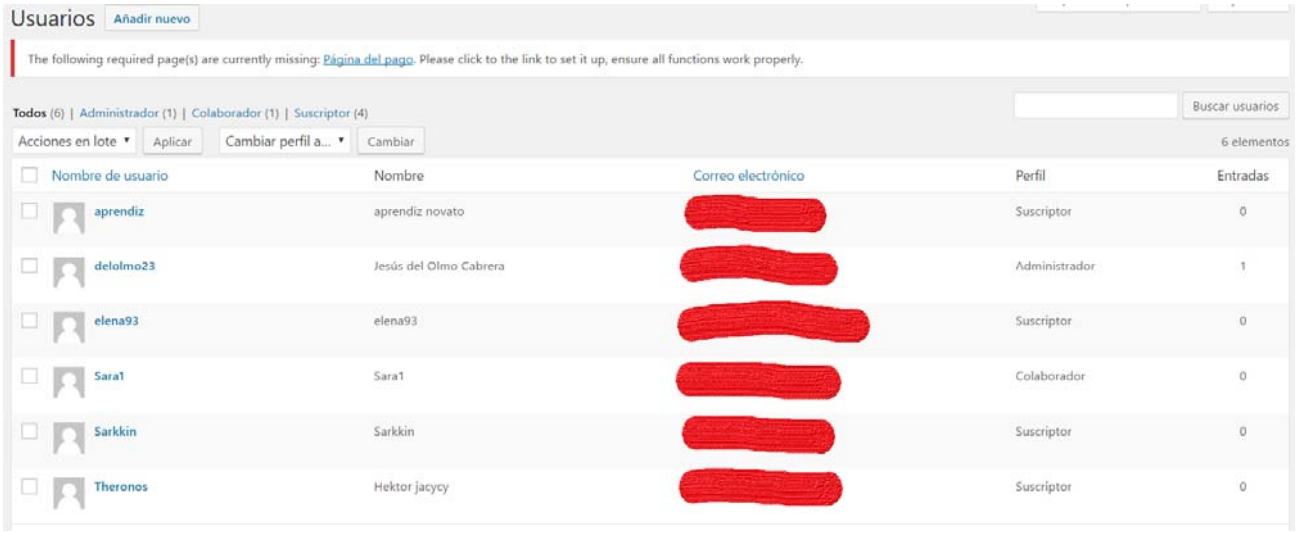


Figura 46: Roles.

- Para añadir/eliminar permisos de los roles de los usuarios hay que acceder al archivo “wp-includes/capabilities.php”. Estas son las funciones que vamos a usar:
    - get_role(): Obtiene los permisos que posee el perfil (Figura 47).

```
$privilegios_autor = get_role('administrator');
```

Figura 47: get_role.

    - add_cap(): Añade permisos al perfil (Figura 48).

```
$rol->add_cap($privilegio);
```

Figura 48: get_cap.

    - remove_cap(): Elimina los permisos del perfil (Figura 49).

```
$perfil = get_role('editor');
$perfil->add_cap('delete_users');
```

Figura 49: remove_cap.

8 CONCLUSIONES

Es un hecho que la tecnología forma parte de la vida de todas las personas en la sociedad actual, por lo que es importante saber defenderse para evitar daños futuros.

Con este proyecto la principal finalidad se basó en educar a las personas en la autodefensa digital, proporcionando una plataforma donde puedan formarse y poner a prueba todo lo aprendido.

Dicha plataforma se ha llevado a cabo gracias al desarrollo de una primera versión de la herramienta de seguridad, que proporciona al usuario una estructura de aprendizaje basada en su conocimiento previo, pudiendo formarle de forma más adecuada.

Otro de los objetivos que se han alcanzado ha sido el poder elaborar un apartado dedicado a los perfiles profesionales, de periodismo y empresarial más concretamente, para satisfacer todas las necesidades tecnológicas de su mundo laboral.

También se ha logrado, gracias al foro que incluye la herramienta y la capacidad de retroalimentación que tiene, crear una comunidad en la que los usuarios participen y colaboren entre ellos.

No se ha podido lograr el juntar a un grupo heterogéneo de gente para que testearan la herramienta desarrollada.

Gracias al desarrollo de este proyecto he logrado aprender y cultivarme dentro del mundo de la ciberseguridad y de todos los conocimientos adquiridos quiero destacar:

- Desarrollo de un servidor seguro.
- Las necesidades tecnológicas de varios sectores de la sociedad.
- Utilización de varias herramientas de auditorías de seguridad.
- Uso del plugin Learnpress.

Ya para terminar, quiero hacer una reseña del trabajo futuro que se puede llevar a cabo a partir de este proyecto, mejorando la herramienta en los siguientes aspectos:

- Añadir distintas secciones que amplíen la funcionalidad de la herramienta, como puede ser el apartado de tutoriales.
- Ampliar los perfiles profesionales, de forma que abarquen otros ámbitos, como puede ser edad, experiencia…

9 BIBLIOGRAFÍA

(1) La Vanguardia. Clinton culpa de su derrota al FBI y los hackers rusos. [Internet]. 2017 [citado el 24 de mayo 2017]. Disponible en: http://www.lavanguardia.com/internacional/20170503/422235722502/clinton-elecciones-eeuu-fbi-hackers-rusos.html

(2) El País. Snowden dice que quiso denunciar el control de EE UU a sus ciudadanos. [Internet]. 2013 [citado el 24 de mayo 2017]. Disponible en: http://internacional.elpais.com/internacional/2013/06/09/actualidad/1370806341_432561.html.

(3) Ciberseguridad para periodistas [Internet]. Fesp.org. 2015 [citado el 24 May 2017]. Disponible en: http://www.fesp.org/index.php/noticias/item/5987-ciberseguridad-para-periodistas

(4) Agra P. Ciberseguridad en Despachos de Abogados [Internet]. El documentalista audiovisual. 2017 [citado el 24 de mayo 2017]. Disponible en: https://eldocumentalistaudiovisual.com/2017/02/08/ciberseguridad-en-despachos-de-abogados/

(5) Pérez I. WannaCry: 6 datos que debes saber sobre el ciberataque global [Internet]. CriptoNoticias. 2017 [citado el 24 de mayo 2017]. Disponible en: https://criptonoticias.com/colecciones/wannacry-6-datos-debes-saber-ciberataque-global/#axzz4i1VCT3JT

(6) "Conciencia ciudadana de ciberseguridad" or José Manuel Roldán Tudela. Monografías 137 Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa: un reto prioritario.

(7) Top-down y bottom-up [Internet]. Es.wikipedia.org. 2014 [citado el 24 de mayo2017]. Disponible en: https://es.wikipedia.org/wiki/Top-down_y_bottom-up

(8) Los despachos de abogados ante los ataques cibernéticos [Internet]. Legaltoday.com. 2014 [citado el 24 de mayo 2017]. Disponible en: http://www.legaltoday.com/practica-juridica/penal/nuevas_tecnologias/los-despachos-de-abogados-ante-los-ataques-ciberneticos

(9) ¿Qué es la criptología? [Internet]. Ciencia. 2014 [citado el 24 de mayo 2017]. Disponible en: http://kerchak.com/que-es-la-criptologia/

(10) G. Bejerano P. Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial. Eldiarioes [Internet]. 2017 [citado el 25 de mayo 2017]. Disponible en: http://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html

(11) Estrategia de ciberseguridad nacional [Internet]. 1st ed. Madrid: Departamento de seguridad nacional; 2017 [citado el 26 de mayo 2017]. Disponible en: http://www.lamoncloa.gob.es

(12) Cómo hacer frente a los 5 incidentes de ciberseguridad más comunes (2/2) [Internet]. INCIBE. 2017 [citado el 25 de mayo 2017]. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/hacer-frente-los-5-incidentes-ciberseguridad-mas-comunes-22

(13) Finlay A. Communications surveillance in the digital age. 1st ed. [S.l.]: APC [u.a.]; 2014.

(14) How to Add Free SSL in WordPress with Let's Encrypt [Internet]. BEGINNER'S GUIDE FOR WORDPRESS. 2016 [citedo el 29 de mayo 2017]. Disponible en: http://www.wpbeginner.com/wp-tutorials/how-to-add-free-ssl-in-wordpress-with-lets-encrypt/

(15) Luján Mora S. Programación en Internet: clientes web. 1st ed. Alicante: Editorial Club Universitario; 2001.

(16) Introducción a CSS [Internet]. Librosweb.es. 2005 [citado el 25 de mayo 2017]. Disponible en http://librosweb.es/libro/css/

(17) Sala J. Qué es WordPress - características principales [Internet]. Webempresa.com. 2017 [citado el 25 de mayo 2017]. Disponible en: https://www.webempresa.com/wordpress/que-es-wordpress.html

(18) SQL [Internet]. Es.wikipedia.org. 2017 [citado el 25 de mayo 2017]. Disponible en: https://es.wikipedia.org/wiki/SQL#Referencias

(19) PHP: ¿Qué es PHP? - Manual [Internet]. Php.net. 2001 [citado el 25 de mayo 2017]. Disponible en: http://php.net/manual/es/intro-whatis.php

(20) Porcel M. Filtradas fotos íntimas de Emma Watson y Amanda Seyfried. huffingtonpost [Internet]. 2017 [citado el 25 de mayo 2017]. Disponible en: http://www.huffingtonpost.es/2017/03/15/filtradas-fotos-intimas-de-emma-watson-y-amanda-seyfried_a_21895829/

(21) Crear Servidor Web Apache seguro en Ubuntu [Internet]. EnREDesao. 2017 [citado el 30 de mayo 2017]. Disponible en: https://enredesao.wordpress.com/tutoriales-servicios-de-red/servidor-web/crear-servidor-apache-seguro-en-ubuntu/

(22) Labrador D, Pidal A, Román M. Trabajo: Privacidad en servicios web - FdIwiki ELP [Internet]. Wikis.fdi.ucm.es. 2017 [[citado el 30 de mayo 2017]. Disponible en: http://wikis.fdi.ucm.es/ELP/Trabajo:_Privacidad_en_servicios_web

(23) Castañeda M, Coronado A, Laina M, Rodríguez L. Trabajo: Usar el móvil de manera segura - FdIwiki ELP [Internet]. Wikis.fdi.ucm.es. 2017 [[citado el 30 de mayo 2017].

Disponible en: http://wikis.fdi.ucm.es/ELP/Trabajo:Usar_el_m%C3%B3vil_de_manera_segura

(24) FM Y. Qué es la Dark Web, en qué se diferencia de la Deep Web y cómo puedes navegar por ella [Internet]. Xataka.com. 2017 [citado el 30 de mayo 2017]. Disponible en: https://www.xataka.com/basics/que-es-la-dark-web-en-que-se-diferencia-de-la-deep-web-y-como-puedes-navegar-por-ella