UNIVERSIDAD POLITÉCNICA DE MADRID

Escuela Técnica Superior de

Ingeniería y Sistemas de Telecomunicación

PROYECTO FIN DE GRADO

IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN PLATAFORMA MÉDICA PARA ENTORNO DE VIDEOJUEGOS TERAPÉUTICOS

ALBA AGUILAR LÓPEZ

Julio 2019

ESCUELA TÉCNICA SUPERIOR DE INGENIERÍA Y SISTEMAS DE TELECOMUNICACIÓN

PROYECTO FIN DE GRADO

TÍTULO: IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD EN PLATAFORMA MÉDICA PARA ENTORNO DE VIDEOJUEGOS TERAPÉUTICOS

AUTOR: ALBA AGUILAR LÓPEZ

TITULACIÓN: GRADO EN INGENIERÍA TELEMÁTICA

TUTOR: MARTINA ECKERT

DEPARTAMENTO: TEORÍA DE LA SEÑAL Y COMUNICACIONES

VºBº MIEMBROS del Tribunal Calificador:

PRESIDENTE: MARTA SÁNCHEZ

TUTOR: MARTINA ECKERT

SECRETARIO: MARIA LUISA MARTÍN RUIZ

Fecha de lectura:

Calificación:

El secretario,

AGRADECIMIENTOS

Quiero agradecer este trabajo a mi familia por estar en las buenas y en las malas, pero siempre ahí.

A mi tutora Martina por estar en todo momento, por su confianza y su sinceridad.

A Jesús por apoyarme en cada paso, por sus consejos, su paciencia y por estar siempre a mi lado.

RESUMEN

En el grupo de investigación GAMMA (Grupo de Aplicaciones Multimedia y Acústica), que pertenece al centro de investigación CITSEM (Centro de Investigación en Tecnologías Software y Sistemas Multimedia para la Sostenibilidad), la Dra. Martina Eckert lleva a cabo una investigación sobre el desarrollo de juegos interactivos para que personas con discapacidad motora, principalmente niños y adolescentes, puedan utilizarlos para llevar a cabo la rehabilitación de una manera más dinámica, divertida y amena.

Hasta ahora se han creado diferentes videojuegos de ordenador cuyo manejo es a través de la cámara Kinect de Xbox, de Microsoft. Todos ellos son configurables a distancia vía la plataforma web *Blexer-med*, la cual también permite realizar un seguimiento de la evolución de los usuarios durante su rehabilitación utilizando dichos videojuegos. Para ello, se almacenan los resultados de todos los pacientes en una base de datos, y el terapeuta los puede consultar y ajustar la dificultad de los ejercicios de rehabilitación a las necesidades del paciente.

A medida que se realizan pruebas de la plataforma, se observa la necesidad de crear una segunda versión mejorada de ella. Además, dada la sensibilidad de los datos que se tienen que procesar, va a ser necesario que la plataforma web cumpla las especificaciones reguladas sobre la protección de datos, así como los requisitos especificados para una plataforma web.

Por todo ello, en este Proyecto Fin de Grado, por un lado, se han llevado a cabo una serie de modificaciones para darle seguridad a la plataforma. Para ello, se ha realizado un análisis de las vulnerabilidades que afectan a al sistema que nos atañe y que solución se puede implementar para solventarlas. Por otro lado, se implementa una segunda versión de la plataforma web, que incluye un diseño renovado, la corrección de algunos errores y la inclusión de alguna funcionalidad nueva.

Con todo ello, se consigue una versión actualizada de la plataforma, llamada *Blexer-med 2.0*, que cumple con los requisitos necesarios para poder obtener datos de prueba de los videojuegos serios que serán añadidos a ella de aquí en adelante. Es una web segura para el usuario, que se ajusta a las reglas de la legislación española y europea. Además, cuenta con una interfaz y unas funcionalidades que permiten al especialista utilizarla sin ningún tipo de complejidad.

Abstract

In the GAMMA research group, which belongs to the CITSEM research center, Dr Martina Eckert is devoted to the development of interactive games to allow people with motor disabilities, mainly children and teenagers, accomplish their rehabilitation processes in a more dynamic and pleasant way.

Different videogames, which are handled through the Xbox Kinect camera have already been implemented. All are connected to a database and can be configured at a distance by a therapist via the web platform *Blexer-med*. The therapist is also able to follow the evolution of the users during their rehabilitation through this platform and access the database that stores all patient's results. The configuration via the platform allows the specialist to adapt the rehabilitation exercises to the specific user's needs.

During tests, the need to create an enhanced version of the platform arose. Also, it has to be taken into account that sensitive patient's data is processed, and that therefore the platform must meet all requirements about data protection.

For all this, in the present Final Degree Project, some modifications have been made in order to increase the security of the platform. On one hand, a wide analysis about possible vulnerabilities of the web platform has been performed, and solutions have been proposed to avoid them. On the other hand, the web platform has been updated, to improve some design aspects and functionalities.

As a result, an updated version of the platform, called *Blexer-med 2.0* has been achieved, which meets all requirements needed to obtain test data with the serious games that will be created added in the future. It is a secure web for the users, which completely fulfills all the Spanish and the European legislation. Furthermore, the web platform has a professional design, in addition to an interface and functionalities that allow the specialist to use it easily.

Tabla de Contenidos

Indice de Figuras

Indice de Tablas

Acrónimos

AES	*Advanced Encryption Standard*
AJAX	*Asynchronous JavaScript*
ARP	*Address Resolution Protocol*
Blexer	*Blender Exergames*
CITSEM	*Centro de Investigación en Tecnologías Software y Sistemas Multimedia para la Sostenibilidad*
DNS	*Domain Name System*
GAMMA	*Grupo de Aplicaciones Multimedia y Acústica*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IEC	*International Electrotechnical Commission*
IP	*Internet Protocol*
ISO	*International Organization for Standardization*
ITU	*International Telecommunication Union*
LOPD	*Ley Orgánica de Protección de Datos*
LSSI	*Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*
MAC	*Media Access Control*
MD5	*Message Digest Algorithm 5*
ONTSI	*Observatorio Nacional de las Telecomunicaciones y de la Sociedad de Información*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
PBKDF2	*Password Based Key Derivation Finction 2*

RGPD	*Reglamento General de Protección de Datos*
RIP	*Routing Information Protocol*
RLOPD	*Reglamento de desarrollo de la Ley Orgánica de Protección de Datos*
SHA	*Secure Hash Algorithm*
SQL	*Structured Query Language*
SSH	*Secure SHell*
SSL	*Secure Sockets Layer*
TCP	*Transmission Control Protocol*
TIC	*Tecnologías de la Información y la Comunicación*
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
VLAN	*Virtual Local Area Network*
WAN	*Wide Area Network*.

1. Introducción y Objetivos

1.1. Introducción

Durante los últimos años, la tecnología ha experimentado un rápido desarrollo, convirtiéndose en un elemento necesario, y a veces indispensable para las personas, que nos proporciona herramientas y mecanismo para facilitar actividades de nuestro día a día.

En el grupo de investigación GAMMA, que pertenece al centro de investigación CITSEM, la Dra. Martina Eckert dirige una línea investigación cuyo principal objetivo es desarrollar herramientas que logren que personas con discapacidad motora, en su mayoría niños y adolescentes, puedan realizar sus ejercicios de rehabilitación de una manera sencilla y divertida, utilizando para ello videojuegos de ordenador junto con la cámara Kinect de Xbox de Microsoft.

Durante los últimos años, en el marco del proyecto *Blexer (Blender Exergames)* [1], se han implementado multitud de tecnologías para llevar a cabo este objetivo. Como primer paso, se elaboraron diferentes videojuegos atractivos y dinámicos para los usuarios, utilizando el software de animación y motor de juegos *Blender*. Más tarde, apareció la necesidad de disponer de una base de datos para almacenar los resultados obtenidos de las partidas de cada paciente. Por otra parte, también fue necesario crear una interfaz gráfica intuitiva a través de la que el especialista pudiera consultar dichos resultados, y además, personalizar la rehabilitación a las necesidades de cada paciente.

Por lo tanto, se creó la plataforma *Blexer-med* [2], que permite a los terapeutas, de una manera sencilla, llevar un seguimiento detallado de la rehabilitación de cada uno de sus pacientes y adecuar los ejercicios del juego a sus necesidades específicas. Así, el especialista puede modificar parámetros como es el tiempo que el usuario tiene que dedicar a ese ejercicio, el número de repeticiones, etc. Además, puede consultar y controlar los resultados obtenidos tras la realización de esos ejercicios, pudiendo así llevar un control más detallado de la evolución de cada usuario.

Actualmente, se está creando una nueva versión del sistema, que se basa en tecnologías más avanzadas, como la segunda versión de la cámara Kinect y el motor de juegos Unity, que permite la creación de juegos más atractivos y potentes.

La actividad que nos atañe en este proyecto es el manejo de información. A medida que pasa el tiempo los volúmenes de datos que es necesario manejar es inmenso, y por ello

apareció la necesidad de crear una herramienta que permitiera su almacenaje y control, perdiendo de esta forma el control físico de la información.

Como resultado de todo lo anterior, surge la necesidad de implementar medidas de seguridad informática que protejan los datos manejados, tanto para impedir el ataque de un organismo no autorizado, como para prevenir la posible pérdida dada por mal uso de la herramienta o fallo propio de ella. Además de lo anterior, también se pretende actualizar y renovar la plataforma web.

1.2. Objetivos

Con este proyecto se pretende dar un fuerte empujón a la investigación de la Doctora Eckert, dotando a la plataforma de las medidas de seguridad necesarias y mejorando el diseño y la funcionalidad para hacerla operativa.

Se puede concluir que los objetivos principales se dividen en dos grandes grupos. El primero, es dotar al sistema *Blexer-med* [2] de las medidas de seguridad necesarias para poder ser utilizada sin restricciones. La información que se maneja debe estar protegida de cualquier ataque o usuario no autorizado, y, además, es imprescindible que cumpla una serie de requisitos para poder ser operativa según la Ley Orgánica de Protección de Datos [3] y la LSSI (*Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*) [4]. En primer lugar, se realizará un análisis del sistema categorizándolo por capas; en cada una de ellas se identifican las vulnerabilidades y su posible resolución. Posteriormente, se llevará a cabo la implementación del resultado del análisis.

Funcionalidades a implementar o actualizar:

- Realizar una copia de seguridad de la base de datos de forma automática cada cierto periodo de tiempo.
- Reforzar la formación de contraseñas y asegurar su almacenamiento y transmisión.
- Recoger los datos en el formato adecuado.
- Reforzar la seguridad de los datos enviados a través de la red.
- Modificar los métodos en estado obsoleto por otros más actuales.

El segundo objetivo es actualizar la interfaz de usuario de la plataforma web. Para ello se plantean una serie de objetivos:

- Hacer el diseño más atractivo.
- Renombrar parámetros que no son intuitivos.

- Modificar los campos de comentarios para permitir escritura libre sin restricciones de símbolos.
- Corrección de errores de formato y diseño en tablas.
- Cierre de sesión por inactividad del usuario.
- Bloqueo del botón "**atrás**" del navegador para evitar volver a introducir las credenciales.

2. Antecedentes

El marco tecnológico en el que se engloba este Proyecto de Fin de Grado es el campo orientado a la salud, actualmente denominado eSalud *(eHealth* en inglés).

eSalud es una palabra que apareció ante la generalización de las TIC (*Tecnología de la Información y la comunicación*) en nuestra sociedad. Según un informe de ONTSI (*Observatorio Nacional de las Telecomunicaciones y de la Sociedad de Información*) sobre el desarrollo de la Sociedad de la Información en España [5], eSalud es "*la aplicación de las Tecnologías de la Información y de la Comunicación en el amplio rango de aspectos que afecten al cuidado de la salud, desde el diagnostico hasta el seguimiento de los pacientes, pasando por la gestión de las organizaciones implicadas en estas actividades*".

Por otra parte, según el portal de salud publicado de la Unión Europea [6], el término *eHealth* es aquel que define un conjunto de herramientas basadas en las tecnologías de la información y la comunicación que se emplean en tareas de prevención, diagnóstico, tratamiento, seguimiento, así como en la gestión de la salud y del modo de vida. En la Figura 1 se representan algunas aplicaciones que tiene la eSalud en la actualidad.

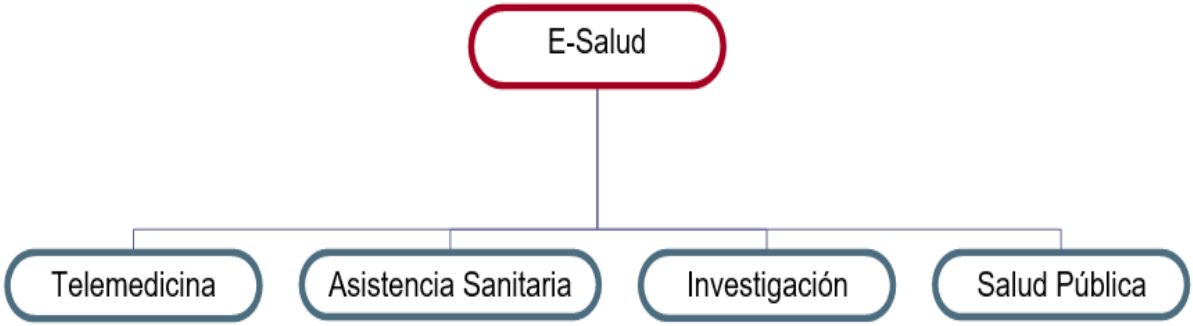

Figura 1. Esquema de las aplicaciones principales de la eSalud

Este proyecto forma parte del proyecto *Blexer*, en el que se están desarrollando una serie de juegos atractivos dirigidos a personas que no pueden realizar los movimientos que se requieren en aplicaciones similares en el mercado. De esta manera, esta plataforma permite a los usuarios utilizar videojuegos no solo como entretenimiento, sino como una herramienta para llevar a cabo su rehabilitación de una manera más divertida y amena. Actualmente existe un juego completo llamado *Phiby's Adventures*, que se utiliza para practicar diferentes movimientos de brazo y tronco, como, por ejemplo, remar o escalar. En la Figura 2 se pueden ver escenas de los ejercicios.

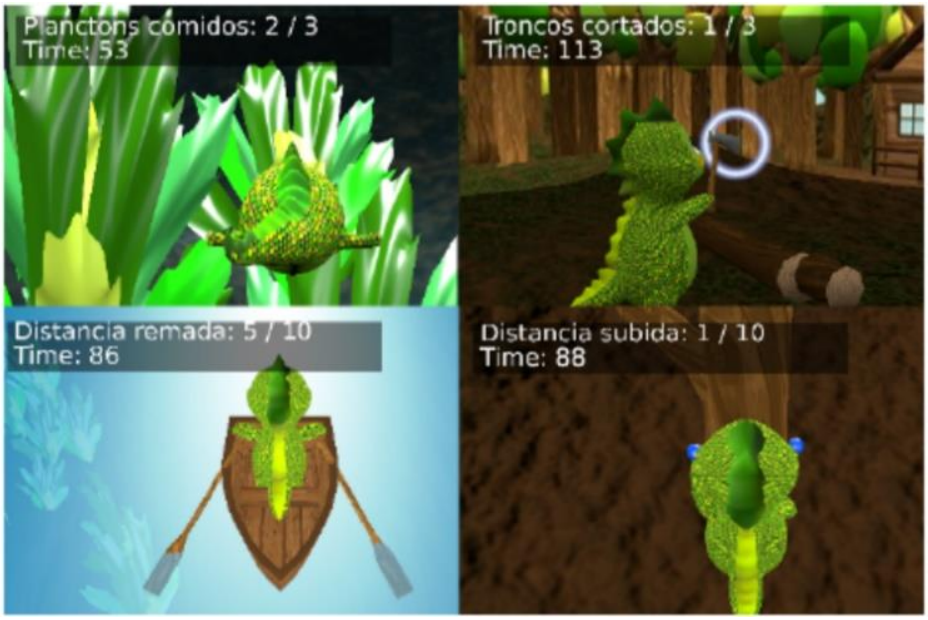

Figura 2 Juego *Phiby's Adventures*. [1]

Visto el gran potencial del proyecto, se fue más allá, y se implementó una plataforma web, por Mónica Jiménez Ramos en su Trabajo Fin de Grado, llamada *Blexer-med* [2] .

Figura 3. Página de la plataforma web *Blexer-med* [2]

Blexer-med surge de la necesidad de una base de datos que almacene resultados y permita llevar un seguimiento de la rehabilitación de los usuarios, así como de una herramienta que posibilite a un especialista adaptar el videojuego a las necesidades de cada uno de sus

pacientes. Un aspecto para destacar es la ausencia de la necesidad de que el paciente se desplace para llevar a cabo su rehabilitación pudiendo utilizar el juego en su propia casa. Además, el terapeuta podrá monitorizar los resultados y actualizar los ejercicios de manera remota.

Para cumplir este cometido, en primer lugar, se crea una plataforma web amigable, basada en un Web Service implementado en Java. La herramienta permite gestionar los juegos que están creados en ese momento, pudiendo añadir nuevos en un futuro. Estos juegos se adaptan a las necesidades de cada paciente mediante la configuración de parámetros como pueden ser el tiempo de realización del ejercicio, el número de veces que se debe realizar en ese tiempo, etc.

También existen tres roles en función del tipo de usuario: Administrador, Centro Médico y Médico. Cada rol tiene sus propias funciones y permisos para otorgarle a la plataforma mayor robustez al manejar datos personales de pacientes. La plataforma web, además, utiliza una base de datos SQL (*Structured Query Language)*, donde se almacenan todos los resultados de los juegos, así como los datos de los usuarios de *Blexer-med*.

Por otro parte, el middleware *Chiro* desarrollado por Ignacio Gómez-Martinho durante su Trabajo Fin de Grado [7], el cual conecta los múltiples dispositivos con los videojuegos, se modifica con el objetivo de que se descarguen las configuraciones de los ejercicios realizadas por los especialistas en el videojuego de cada paciente cuando se comienza una partida, y al finalizar dicha partida se envíen los resultados a la plataforma web. En la Figura 4 se puede observar el diagrama de conexiones como combinación de todos los elementos que forman parte del proyecto de Mónica Jiménez Ramos.

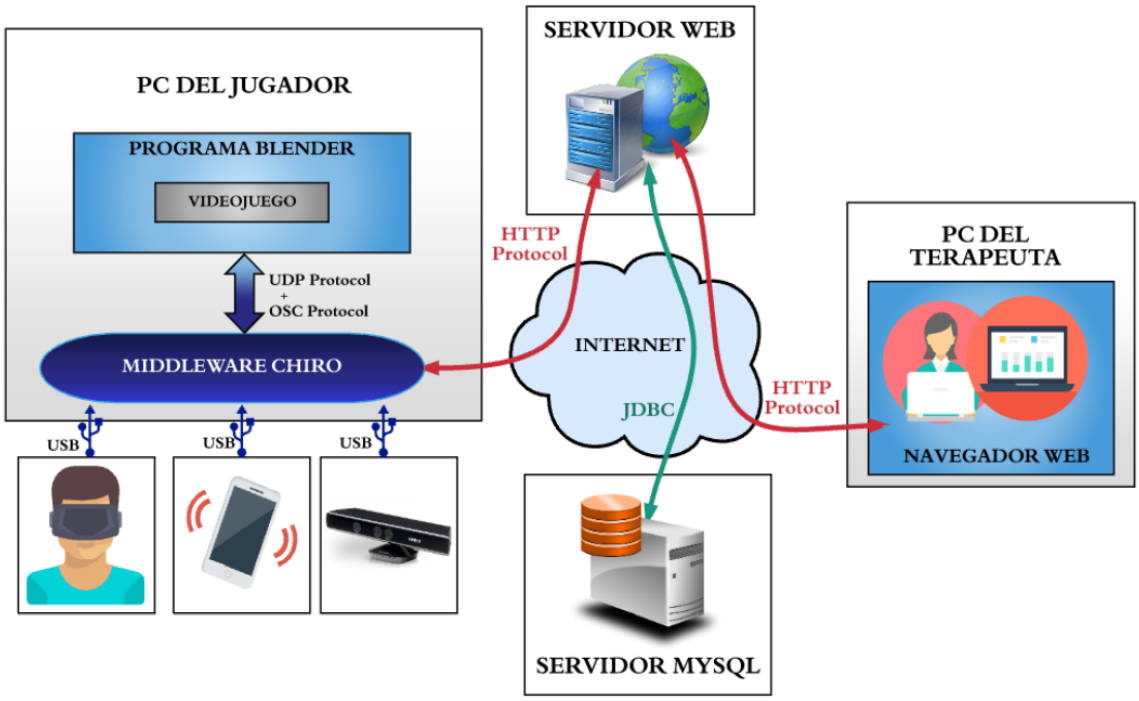

Figura 4 Diagrama de conexiones del proyecto de Mónica Jiménez Ramos. [2]

Este proyecto continúa el trabajo de Mónica Jiménez Ramos, creando una segunda versión para añadir o mejorar aspectos, que tras una serie de pruebas de la funcionalidad de la web, se han visto necesarios. En este proyecto se manejan datos personales médicos, en la mayoría de los casos de pacientes menores de edad, y por ello, es imprescindible contar con las medidas de seguridad suficientes para garantizar la protección de los datos y de la web ante ataques de terceros no autorizados. Además, según las leyes en vigor, la plataforma debe cumplir una serie de requisitos para poder ser operativa.

Con relación a los proyectos similares a *Blexer-med*, actualmente en el mercado existen numerosos casos donde se utilizan videojuegos como herramienta para la implementación de tratamientos rehabilitadores integrales, no solo para tratamientos físicos, sino también para psicológicos y sociales.

REHABILITY [8] es una empresa que permite al paciente realizar sus ejercicios de rehabilitación ya sea desde el centro médico o de manera remota, siempre contando con supervisión médica constante. La supervisión se realiza mediante un software que permite establecer y ajustar parámetros personalizados, además de recopilar y analizar los datos obtenidos a distancia. Funciona en dispositivos móviles, tabletas y PC. Los ejercicios se realizan en ambientes familiares para garantizar la motivación del paciente. Esta herramienta tiene además una versión adaptada para la rehabilitación de niños y otra para la de los ancianos.

NIRVANA [9] es un dispositivo médico basado en realidad virtual creado por la empresa *BTS Bioengineering*, similar a la Kinect de Xbox, diseñado para ayudar a la rehabilitación motora en personas con trastornos neuromotores. Se puede ver una representación de Nirvana en la Figura 5. Utiliza estimulaciones neuro-sensoriales y permite realizar ejercicios de rehabilitación en cualquier parte del cuerpo.

Figura 5. Dispositivo médico Nirvana

En este sistema el paciente no necesita usar ningún tipo de sensor, mando, visores o guantes para realizar el ejercicio. Los ejercicios son monitorizados en tiempo real para poder adaptarse a las necesidades de cada paciente. Por otro lado, el sistema facilita al paciente informes sencillos y claros sobre su progreso.

El sistema funciona de tal manera que proyecta escenarios en la pared o en el suelo, y el paciente interactúa con los elementos que encuentra en la proyección, de tal manera que el sistema detecta los movimientos que realiza el usuario y en función de ello modifica la escena proporcionando una respuesta visual.

El centro *LESCER* llevó a cabo un estudio sobre la utilización de los videojuegos como herramienta de rehabilitación neuropsicológica en pacientes con daño cerebral adquirido [10]. El estudio explica que los videojuegos ofrecen al paciente actividades cercanas a la vida real, en un entorno motivador y protegido, facilitando su participación en la rehabilitación. Por otro lado, indica la necesidad de que un profesional paute al paciente en el modo de realizar la tarea. Finalmente, concluye afirmando que los videojuegos pueden ser utilizados para alcanzar los objetivos de la terapia, que son aprender o reentrenar habilidades.

Dos empresas, *SINPROMI. S. L.* e *ITER. S.A*, han desarrollado una plataforma para la rehabilitación física y entrenamiento cognitivo llamada *ADVANTED* [11]. Esta aplicación permite al paciente resolver ejercicios utilizando el movimiento corporal. Estos ejercicios son diseñados previamente por personal cualificado, como pueden ser terapeutas o educadores.

Como en el proyecto *Blexer*, *ADVANTED* utiliza la cámara Kinect de Microsoft como herramienta para recoger los movimientos del usuario, además los juegos o entrenamientos pueden ser configurados de manera sencilla para adaptarlo a la necesidad del usuario. La principal ventaja de esta herramienta es que los ejercicios que posee son altamente configurables, es decir, los ejercicios no están completamente integrados o definidos en la plataforma, sino que se permite implementarlos mediante un programa de configuración de forma sencilla. En la Figura 6 se puede ver un ejemplo de configuración de *ADVANTED*.

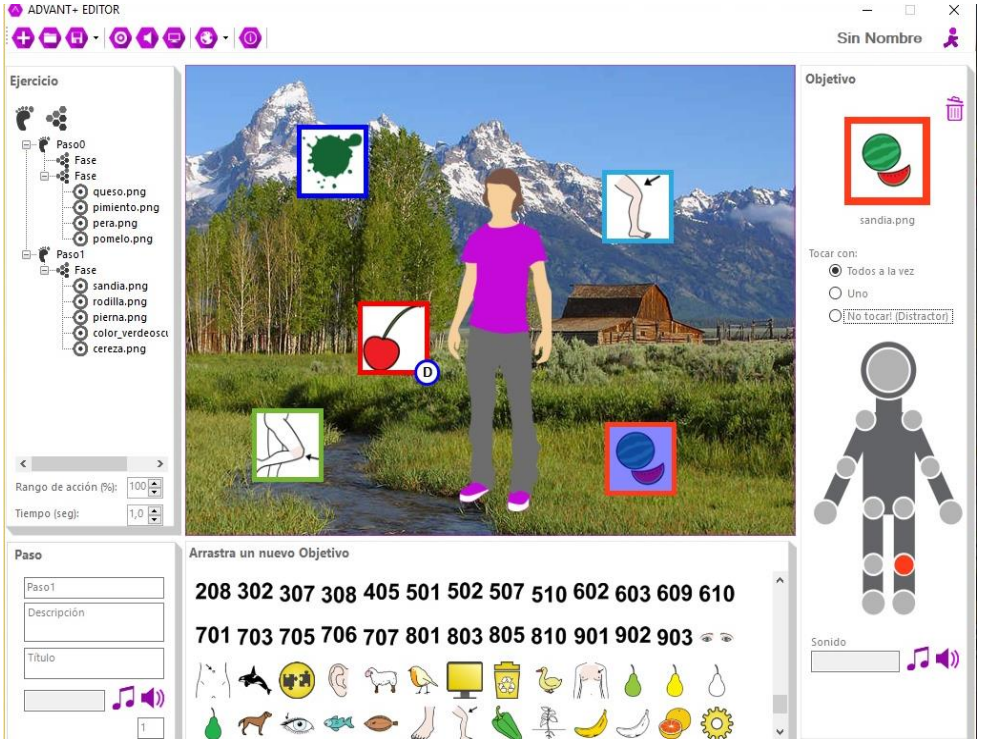

Figura 6 Ventana de configuración de *ADVANTED* [11]

3. Estudio de la seguridad

Es importante en este trabajo el conocimiento y la correcta manipulación de todos los datos, dada la relevancia especial por el contexto en el que se están tratando. Para ello, se realiza un análisis sobre las pautas y prácticas para el tratamiento seguro de la información que establece la legislación europea y española ante este tema, además de un reconocimiento de todas aquellas vulnerabilidades de los sistemas o los problemas derivados de procesar la información en ellos contenida.

Para llevar a cabo este objetivo, el primer paso es identificar lo que debe ser protegido y en qué grado hay que hacerlo. Por ese motivo, se lleva a cabo el Sistema de Gestión de la Seguridad de la Información (SGSI) [12], el cual está formado por cuatro pasos que se deben aplicar: PDCA (*PLAN-DO-CHECK-ACT*), es decir, Planear, Hacer, Verificar, Actuar.

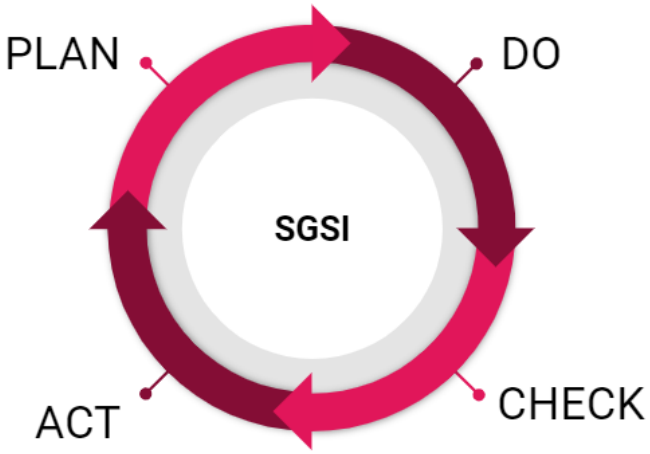

Figura 7. Sistema de gestión de la seguridad de la Información

a. **Planificar:** Se identifican los elementos que requieren ser protegidos, se lleva a cabo un análisis de riesgos y se establecen las posibles soluciones en caso de ocurrir alguno de ellos.

b. **Hacer**: se implementan las medidas de seguridad necesarias partiendo de las decisiones tomadas en el anterior punto.

c. **Verificar:** se revisa que las medidas de seguridad implementadas cumplen su función correctamente

d. **Actuar:** consiste en la ejecución de las tareas de mantenimiento necesarias, así como en la proposición de mejoras.

Posteriormente se llevará a cabo un análisis sobre la normativa que es necesario tener en cuenta para obtener un sistema completamente seguro.

3.1. Legislación y Normativas

3.1.1. Normativas de regulación de la seguridad informática

Las normas ISO (*International Organization for Standardization)* son normas o estándares de seguridad establecidos por la Organización Internacional para la Estandarización (*ISO*) y la IEC (*International Electrotechnical Commission*) que se encargan de establecer estándares y guías relacionadas con sistemas de gestión, y aplicables a cualquier tipo de organización internacional, con el propósito de facilitar el comercio, el intercambio de información y contribuir a la transferencia de tecnologías [13].

En este trabajo especialmente se hará hincapié en la familia de normas ISO/IEC 27000, las cuales hacen referencia a la gestión de la seguridad. Contienen las mejores prácticas recomendadas en seguridad informática para desarrollar, implementar y mantener la seguridad de la información. Solo se mencionan aquellas normas que son vinculantes con el carácter del trabajo, tomando como base la información de [14].

- **ISO/IEC 27002:** es un código de buenas prácticas para la gestión de la seguridad, que contiene principalmente:
    - Recomendaciones sobre qué medidas tomar para asegurar los sistemas de información
    - Descripciones sobre aspectos a analizar para garantizar la seguridad de la información
- **ISO/IEC 27005:** Normativa sobre la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y técnicas de evaluación de riesgos de seguridad en la información.
- **ISO/IEC 27799:2008:** Normativa para implementar la seguridad de la información en la industria de la salud. Se aplica a la información de salud en todos los aspectos relacionados con la toma, el almacenamiento y la transmisión de los datos. De esta manera, se asegura la confidencialidad, integridad y disponibilidad de ellos.

3.1.2. Normativas de regulación de cifrado de datos

Las normativas españolas y europeas permiten cualquier mecanismo de cifrado que garantice que la información no sea inteligible ni manipulada por terceros. En este caso, sólo se describen aquellas que están relacionadas e influyen en el sistema que atañe al proyecto.

Ley Orgánica de Protección de Datos y Reglamento de desarrollo de la Ley Orgánica de Protección de Datos [3]

La nueva normativa sobre protección de datos indica que se debe analizar el riesgo al que están sometidos los datos que se tratan; a partir de ello, y para cada caso, se deben implementar las medidas adecuadas para su protección.

Según esta ley, las empresas o entidades que deben cifrar los datos son aquellas que, después del análisis de riesgo, necesitan implantar medidas de nivel alto, es decir:

- Las que tratan datos sensibles o especialmente protegidos, como pueden ser datos bancarios, datos médicos, etc.
- Las que contengan datos para fines policiales sin consentimiento de la persona afectada.
- Si tratan datos derivados de actos de violencia de género.

Estos datos, además, siempre deberán ser cifrados según el reglamento RLOPD (*Reglamento de desarrollo de la Ley Orgánica de Protección de Datos*):

- Cuando se transmitan a través de redes públicas o inalámbricas.
- Cuando los dispositivos portátiles se encuentren fuera de las instalaciones.

Reglamento General de Protección de Datos de la Unión Europea (RGPD) [15]

En este caso, no solo se deben cifrar los datos sensibles, sino que se deben cifrar los datos en función del riesgo que el afectado pueda recibir en caso de que se descubrieran por otra persona o empresa no autorizada.

- **Cifrado Obligatorio:** Es obligatorio cifrar los datos de carácter personal en los siguientes casos:
    - Cuando lo imponga el Estado, siendo en nuestro caso lo que indique la LOPD (*Ley Orgánica de Protección de Datos*) para datos de nivel alto:
        - Origen étnico o racial
        - Opiniones políticas
        - Convicciones religiosas o filosóficas
        - Afiliación sindical
        - Datos de salud y vidas sexual
    - Cuando se esté adherido a un código de conducta.
    - Cuando la evaluación de impacto en la protección de datos lo ha recomendado.
    - Cuando sea necesario suprimir o reducir un riesgo.

- **Cifrado voluntario:** Para el resto de las situaciones no es obligatorio cifrar los datos que se manejan, pero se recomienda hacerlo aunque no sea necesario. El cifrado es un mecanismo que permite mitigar los riesgos del tratamiento de datos de carácter personal para así mantener la seguridad. Por otro lado, según indica el reglamento, las empresas que tengan implementado un sistema de cifrado y sufran un ataque que afecte a los datos personales, no están obligadas a informar de ello a los afectados, ya que al estar protegida la información no hay peligro para los derechos del usuario. En caso contrario, es decir, cuando la empresa o entidad no disponga del sistema de cifrado de los datos personales, estará obligada a informar a todos los usuarios cuya información personal se haya visto afectada por el ataque.

Ley de Autonomía del Paciente [16]

Todos aquellos datos tratados por profesionales de la salud deben ser cifrados debido a:

- Artículo 7.1, que dictamina que "*Toda persona tiene derecho a que se respete el carácter confidencial de los datos referente a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la ley*".
- Los datos relacionados con la salud son de nivel alto.

3.2. Problemática de Seguridad: Amenazas y Ataques

Por las redes telemáticas circula mucha información sensible que es necesario proteger. Una amenaza es, como se indica en [17], "*una violación potencial de la seguridad, que existe cuando hay una entidad, circunstancia, capacidad, acción o evento que podría causar daño*". Existen dos tipos de amenazas:

- **Accidentales**: son aquellos que aparecen de forma no premeditada
  - Ejemplos: Fallo en los sistemas, mal uso de las herramientas, etc.
  - Medidas de seguridad: revisión periódica de los equipos, actualización y realización de pruebas de los programas informáticos con frecuencia, correcto mantenimiento de las instalaciones, alta formación del personal, etc.
- **Intencionales:** participación maliciosa de una entidad o sujeto que pretende hacer un uso indebido de la red. A este tipo de amenazas se les denomina ataques. Existen dos tipos de ataque:
  - **Activo**: Es aquel que provoca la alteración del comportamiento normal de un recurso o servicio, por ejemplo, la información es cambiada, desaparece, los datos no se envían al destinatario correcto, etc.
  - **Pasivo**: Es aquel que no provoca ninguna alteración del funcionamiento del sistema, se limitan a registrar el uso de los recursos y/o a acceder a la

información guardada. Por ejemplo, cuando se hace una copia de datos sensibles por un sujeto no autorizado.

3.2.1. Ataques típicos en redes telemáticas

Antes de realizar un estudio de las vulnerabilidades de nuestro sistema es importante conocer algunos de los tipos de ataques más relevantes para nuestro proyecto, contra las redes informáticas, así como las posibles consecuencias [18].

- **Reconocimiento de sistemas:** su principal objetivo es robar información sobre un determinado sistema informático. Realiza esta tarea escaneando sus puertos, de modo que así el atacante podrá conocer qué servicios están activos o la versión de los sistemas operativos y las aplicaciones.
- **Detección de vulnerabilidades:** como su propio nombre indica, este ataque consiste en detectar las posibles vulnerabilidades de un sistema informático para posteriormente desarrollar una herramienta, conocida como *exploit*, que permita explotarlas fácilmente.
- **Robo y modificación de información mediante interceptación de mensajes: e**l atacante controla la comunicación de forma transparente, es decir, sin que los participantes de la comunicación se percaten de que se está robando información o modificando los mensajes de la comunicación.
- **Análisis del tráfico:** este ataque consiste en observar los datos y la información que se transmite a través de redes sin modificarlos. Las herramientas que permiten llevar a cabo este objetivo se conocen como *sniffers*.
    - **Suplantación de identidad:** también conocido como *spoofing*, consiste en que un atacante se hace pasar por una entidad distinta a través de la falsificación de los datos de la comunicación. En función de la tecnología utilizada existe una clasificación para los ataques de *spoofing*.
        - **IP (***Internet Protocol* **) Spoofing** si el atacante falsifica la dirección IP origen de un paquete TCP (*Transmission Control Protocol*)/IP.
        - **ARP** (*Address Resolution Protocol)* **Spoofing** si se falsifica la tabla ARP que construye las tramas de solicitud y respuesta, es decir, modifica la tabla con el objetivo de que los paquetes se envíen a un host atacante en lugar de hacerlo al destino correcto.
        - **DNS** (*Domain Name System)* **Spoofing** cuando se falsifica la relación entre el nombre de dominio y una IP, ante una consulta de resolución de nombres.
        - **Web Spoofing** cuando se enruta una conexión a través de una página falsa con otra página para obtener información del atacado.

- **Inyección de código SQL** se produce cuando se inserta código SQL malicioso dentro del código SQL programado con el objetivo de alterar el funcionamiento normal del programa.

3.3. Estudio de medidas de seguridad para sistemas informáticos

Como se ha visto en el punto 3.2. los ataques se producen a causa de las vulnerabilidades de nuestro sistema, por lo tanto, en primer lugar, será necesario conocer las amenazas de un sistema, para así poder definir los mecanismos de seguridad adecuados para evitar o minimizar las consecuencias de los ataques. Por ello, en este punto se va a utilizar el modelo OSI (*Open Systems Interconnection*) para conocer los posibles ataques de cada capa del sistema, y así poder implantar las medidas de seguridad más adecuadas en cada una.

3.3.1 Servicios de seguridad necesarios en servidores web

La seguridad de la información tiene como objetivo aplicar procedimientos para proteger los datos que se manejan. La información es un bien muy importante y por tanto se debe gestionar de forma eficaz el almacenamiento, procesamiento y transmisión. Según la recomendación X.800 del ITU-T (*International Telecommunication Union*-T) [19] se definen los siguientes servicios de seguridad [20] para llevar a cabo esta tarea:

1. **Confidencialidad**

La confidencialidad es la seguridad frente a la divulgación a terceros no autorizados, es decir, es la capacidad de un mensaje de mantener oculto su contenido de forma que, si una tercera persona no autorizada intercepta el mensaje, no pueda interpretar su contenido.

Un mecanismo utilizado que garantice este aspecto es la Criptografía, encargándose de cifrar los datos para que resulten incomprensibles a aquellos usuarios que no dispongan de los permisos necesarios, y, por tanto, los mecanismos para descifrar el mensaje.

Como se observa en el ejemplo de la Figura 8, Alice le manda a Bob un mensaje encriptado con la clave pública de Bob, la cual Alice conoce. Bob podrá desencriptar el mensaje con su clave privada, la cual es la única clave que permite hacerlo.

Figura 8. Envio de mensaje con confidencialidad.

En el caso de que una tercera persona obtenga el mensaje no podrá ver su contenido, ya que está encriptado y no dispone de la clave privada que hace pareja con la clave pública que se utilizó para encriptar el mensaje.

2. Integridad

La integridad es la seguridad ante la modificación no autorizada durante el tratamiento o almacenamiento de la información, es decir, tiene como objetivo identificar que un mensaje no ha sido modificado por una tercera persona.

Como se observa en el ejemplo de la Figura 9, Alice le manda a Bob un mensaje y el valor *hash* del mensaje. Bob, al recibir el mensaje, calcula su valor *hash*. Si el valor calculado y el que se le envía coinciden es que no ha habido modificaciones en el mensaje.

Figura 9. Envió de mensaje con Integridad

3. Disponibilidad

La disponibilidad es la seguridad de facilitar el acceso a la información a quien esté autorizado y seguridad contra denegación a accesos autorizados. Es necesario implementar medidas de seguridad que protejan la información y que, en caso de que sea dañada, se pueda recuperar en su totalidad, por ejemplo, por medio de la realización de copias de seguridad.

4. Autenticidad

Seguridad frente a la identidad emisora de la información, es decir, este servicio garantiza que una entidad es quien dice ser. Como se observa en el ejemplo de la Figura 10, Alice le manda a Bob un mensaje encriptado con su clave privada y con la clave pública de Bob, conocida por Alice. Bob puede desencriptar el mensaje con su clave privada, que es la única clave que puede desencriptarlo. Bob sabe que el mensaje ha sido enviado por Alice, porque ella lo ha encriptado con su clave privada y para desencriptarlo Bob ha tenido que usar la correspondiente clave publica, que él conoce que es de Alice.

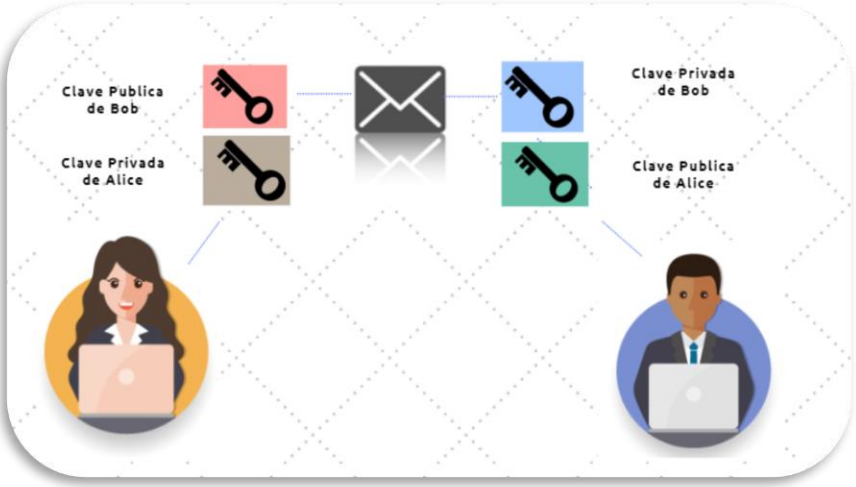

Figura 10 Envío de mensaje con Autenticidad

5. No repudio:

Evita que el emisor y receptor puedan negar su participación en una comunicación.

6. Anonimato.

Trata de mantener oculta la identidad de la persona que realiza una operación telemática. Por ejemplo: encuestas, dinero electrónico, votaciones electrónicas, etc.

3.3.2. Modelo OSI

El modelo OSI fue desarrollado en 1983 por la Organización Internacional de Estándares (ISO). Desde entonces ha sido utilizado como el esquema principal para la comprensión y análisis del funcionamiento de las redes. La mayor parte de los protocolos de comunicación en la actualidad utilizan su estructura, debido a que es una arquitectura estandarizada que permite la comunicación a distintos tipos de hardware y software. Está formada por 7 capas, permitiendo dividir la comunicación en partes más pequeñas y sencillas, además de impedir que los cambios de una capa afecten al resto de capas.

El modelo OSI se creó desde una perspectiva teórica, y por ese motivo, hoy en día se utiliza una estructura más practica como es el esquema TCP/IP, que consiste en un conjunto de protocolos utilizados de manera simultánea para permitir el correcto funcionamiento de la red. En la Figura 11 se puede ver una comparativa entre la arquitectura de OSI y TCP/IP.

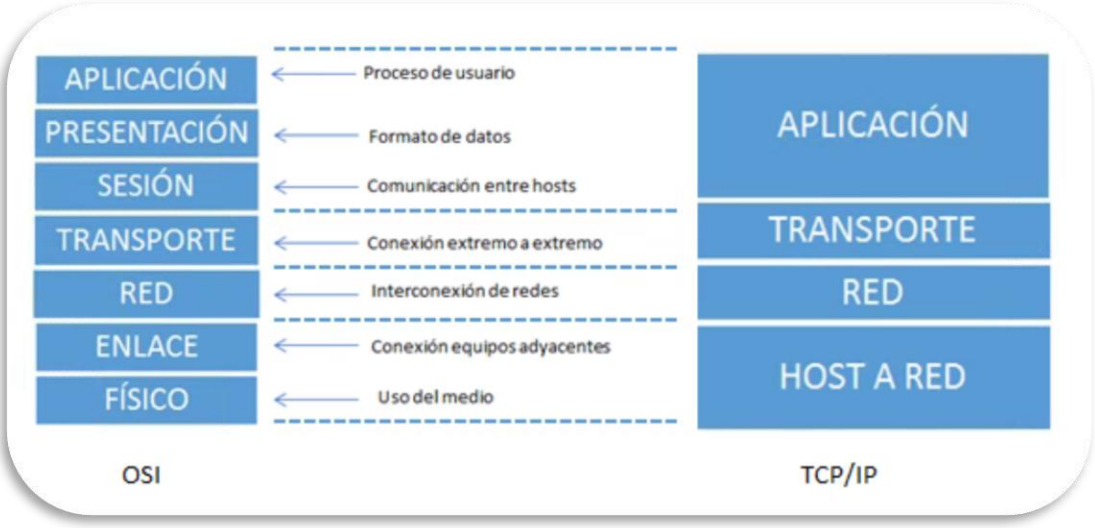

Figura 11. Comparación del modelo OSI con el modelo TCP/IP

Las tareas de las capas principales de la estructura de red son:

- **Capa Física:** establece cómo se transmite el flujo de datos a través de un medio físico (modulación, codificación de canal, etc).
- **Capa de Enlace: s**e encarga del direccionamiento a nivel de trama. Es el nexo entre la capa de red y la capa física.
- **Capa de Red:** se encarga del encaminamiento de paquetes a través de redes.
- **Capa de Transporte:** recoge los datos que vienen de la aplicación y los fracciona en segmentos para posteriormente enviarlos a la capa de red. Los protocolos habitualmente utilizados son TCP y UDP (*User Datagram Procol)*, los cuales establecen

un vínculo entre el origen y el destino. La diferencia entre ambos radica en que TCP es fiable y orientado a conexión, y por tanto más adecuado para aplicaciones que requieran fiabilidad y pocos errores, mientras que UDP no lo es, proporcionando únicamente una multiplexación por puerto a cada dirección IP, siendo así más adecuado para aplicaciones con requisitos estrictos de retardo.

- **Capa de Aplicación:** se ocupa del manejo de la sesión y aplicaciones concretas que se ejecutan en el equipo.

Por tanto, además de utilizarse para el desarrollo de protocolos de telecomunicación, se utilizará en este caso como base para entender cómo aplicar estrategias de seguridad en una estructura por capas.

Será imprescindible que las capas inferiores funcionen correctamente y estén libres de ataques para que el resto de las capas realice su tarea exitosamente. De esta manera se van a analizar las vulnerabilidades y los posibles ataques que se pueden producir en cada capa y así poder implementar medidas de seguridad para reforzar o evitar posibles amenazas.

3.3.3. Análisis de las vulnerabilidades y ataques en la estructura de Red

Se ha realizado un análisis de cada una de las capas que forman la estructura comentada anteriormente. Para ello se ha descrito la tarea que realiza cada capa, y posteriormente las vulnerabilidades que podemos encontrar y los ataques que harían efecto en ellas, tomando [17] y [21] como referencia. Por último, se han determinado las medidas de seguridad necesarias para neutralizar cada uno de los problemas.

En primer lugar, se mencionarán las vulnerabilidades comunes a todas las capas y después se realizará un análisis más detallado particularizando para cada una de ellas.

3.3.3.1. Vulnerabilidades y ataques generales

Una vulnerabilidad describe las debilidades y los métodos que se usan para provocar ataques a las políticas de seguridad, tal y como se ha explicado en el apartado 3.2.1. Los ataques pueden ser debidos a diversas razones, como puede ser fraude, extorsión, robo de información confidencial, acceso no autorizado, anulación de un servicio o muchas veces simplemente un desafío personal.

Los ataques pueden provenir de dos fuentes principales:

- Internos: usuarios autenticados o que tienen acceso al recurso.
- Externos: usuarios que acceden remotamente al sistema.

3.3.3.2. Vulnerabilidades y ataques por capas

Capa Física

Los ataques de la capa física son cualquier daño o modificación sin autorización de los dispositivos físicos pertenecientes a la red, por ejemplo, corte o desconexión del cable de red, interferencia de algún dispositivo que impida el funcionamiento de la red, e incluso hasta un incendio.

El ataque a los sistemas físicos de la red de comunicaciones ocasiona un gran impacto en la comunicación, muchas veces mayor que en el caso de que se dañaran el resto de las capas, ya que todas las capas se sustentan en la física. Por lo tanto, es necesario impedir que terceros no autorizados ingresen a las instalaciones donde permanecen los dispositivos físicos, y para ello es necesario un control de acceso donde se encuentre la red desplegada. Por otro lado, es necesaria una copia de seguridad actualizada de los datos como respaldo ante los ataques o fallo de los servicios.

Capa de Enlace

Esta capa se encarga de la transferencia de datos de un nodo a otro de la red. Para ello prepara los datos mediante una señal de inicio y de final de cada paquete, para posteriormente enviarlos a través de la capa física. Es importante destacar que en esta capa se encuentran las direcciones MAC (*Media Access Control*) las definiciones de las VLAN (*Virtual Local Area Network*), además de los protocolos para la red WAN (*Wide Area Network*.).

Por lo tanto, las principales vulnerabilidades son la facilidad de falsificación de las direcciones MAC y la localización de redes inalámbricas. Las medidas de seguridad para estos casos serían la realización de un filtrado de direcciones MAC y el cifrado en conexiones inalámbricas.

Capa de Red

En esta capa se encuentra definido el diseño de la red lógica, se encarga de garantizar que la información que envía el emisor llegue al receptor, es decir, del encaminamiento de paquetes entre redes, utilizando para ello direcciones IP, y siendo el *router* el elemento que centraliza el manejo del tráfico.

Por lo tanto, las vulnerabilidades de esta capa son el control no autorizado, además de los mecanismos de seguridad que no incluyan los protocolos de encaminamiento como RIP (*Routing Information Protocol*) u OSPF (*Open Shortest Path First*). Las medidas de seguridad que son necesarias implementar en esta capa son contraseñas fuertes y la configuración correcta de los protocolos de administración de la red a través de conexiones cifradas.

Capa de Transporte

La capa de transporte es la encargada de obtener los datos de la aplicación y fragmentarlos en segmentos para posteriormente enviarlos a la capa de red. Las principales vulnerabilidades de seguridad en este nivel son las relacionadas con el cifrado de los datos que se envían de un extremo a otro. Es importante en este caso la autenticación del origen y del destino para evitar posibles manipulaciones de datos que atente sobre la integridad del mensaje transmitido, además de la evasión de ataques de inyección. Los mecanismos de seguridad en esta capa serán la utilización de protocolos de capa 4 de comunicación segura, como pueden ser SSL (*Secure Sockets Layer*), TLS (*Transport Layer Security*) o SSH (*Secure SHell*), los cuales permiten la protección de los datos mediante su cifrado.

Capa de Aplicación

La capa de aplicación se encarga del manejo de la sesión y las aplicaciones que se ejecutan en el equipo. Esta capa permite la utilización de múltiples protocolos a condición de las necesidades del usuario. Por ello, una de las principales vulnerabilidades es la mala configuración del protocolo seleccionado, ya que pueden provocar un punto de acceso a la red. En esta capa el mecanismo de seguridad por excelencia es la instalación de un firewall de alto nivel permitiendo un alto control del tráfico de red.

4. Implementación de las medidas de seguridad

Después del análisis realizado en el apartado 3, teniendo en cuenta todos los factores que intervienen:

- Análisis de seguridad de todas las capas que forman parte de la arquitectura de un sistema, y las medidas de seguridad necesarias para solventar cada una de ellas.
- Las medidas para que una plataforma web cumpla los requisitos necesarios para ser un sistema operativo según la LOPD y la LSSI.
- La recomendación ITU-T X800 que determina los requisitos que se tienen que cumplir para que la información se almacene, procese y transmita segura.

Se resumen en la Tabla 1 las medidas que el sistema debe tener para poder ser completamente seguro.

Tabla 1 Soluciones por capas análisis de vulnerabilidades

Capa	Medidas de Seguridad
Física	• Crear copia de seguridad de todos los datos almacenados en la base de datos. • Desarrollo de código para que la copia de seguridad se realice de manera automática, cada cierto tiempo estipulado por el administrador. • Para que las copias de seguridad no ocupen demasiada memoria se eliminarán aquellas copias obsoletas, con fecha anterior a la determinada por el administrador.
Red	• Reforzar contraseñas para adecuarla a la normativa de seguridad informática. • Los campos de los formularios sigan su estructura correspondiente, es decir, que el correo sea del tipo correo@dominio.es, o que el teléfono solo esté formado por números.
Transporte	• Reforzar el método de consulta Ajax (*Asynchronous JavaScript*) para que la información viaje segura. • Necesidad de autenticarse para poder acceder a la plataforma donde se pueden consultar los datos personales.
Aplicación	• Instalación de firewall de alto nivel. • Actualizar las versiones de los softwares utilizados en el sistema.

4.1. Actualización de software

En primer lugar, se actualizan las versiones de los diferentes tipos de software utilizados para la creación de la plataforma. Las ventajas que da realizar este proceso son según [22] las siguientes:

- Acelerar el rendimiento del servicio.
- Ejecutar correcciones de errores. Habrá menos posibilidades de que aparezcan errores y virus en el servidor.
- Mejorar las características de los sistemas.
- Mayor adaptabilidad frente al uso con otros sistemas.
- Mayor seguridad.

Las actualizaciones que se han llevado a cabo son las que se exponen en la Tabla 2.

Tabla 2 Actualización de las versiones de software del sistema

Sistema	Versión Anterior	Versión Nueva
Servidor base de datos MySQL	mysql-5.7.24-winx64	mysql-8.0.13-winx64
Servidor Tomcat	Tomcat v7.0.72 Server	Tomcat v9.0 Server
Eclipse	Eclipse Indigo (2011)	Eclipse Neon (2017)
JRE	JRE 7.79-winx64	JRE 8.1 – winx 64

4.2. Realización de copias de seguridad de la base de datos regulares

Una base de datos es un conjunto de datos pertenecientes a un mismo contexto donde se guarda información fundamental para un posterior uso de ella. Un aspecto muy importante para tener en cuenta es realizar copias de seguridad de forma regular, no solo de los datos que contiene sino también de su estructura. Las webs, al fin y al cabo, son aplicaciones, y no están exentas de necesitar copias de seguridad, puesto que es posible que puedan ser atacadas por usuarios externos o tener algún fallo físico de los servidores donde están alojadas, produciendo que nuestros usuarios no puedan disponer del servicio.

Las copias de seguridad, por tanto, son el mecanismo más acertado para respaldar la información de la web. Se pueden realizar mediante un administrador de servidores o programadas para realizarse de forma automática. De esta manera, todos los datos se almacenan al instante, de acuerdo con la fecha y hora que se especifique en el código programado. Además, esta información puede ser utilizada de forma inmediata en caso de ser necesaria.

La plataforma cuenta con una base de datos MySQL alojada en el servidor del centro de investigación CITSEM y es administrada por el gestor de bases de datos *phpMyAdmin*. **Este gestor sólo permite realizar copias de seguridad manualmente**, para lo que es necesario entrar en la aplicación y realizar una serie de pasos para llegar a crearla. Pero, para no tener que acordarse y ahorrar tiempo, interesa disponer de un proceso automático que genere una copia de seguridad de la base de datos cada cierto periodo de tiempo, que en este caso se ha

acordado que sea una vez por semana. Para solucionarlo, se va a utilizar un comando que proporciona MySQL, el cual permite crear, en la carpeta que se establezca, un archivo que contendrá la copia de seguridad de la base de datos que se le indique. Para este trabajo se realizará una copia de la base de datos completa. Este archivo tiene la extensión *.sql* y su nombre contendrá la fecha en la que se realizó la copia para tener un control de los ficheros.

Para que este comando sea ejecutado automáticamente a una hora y día concreto, ha sido necesario crear mediante *Cron*, un *script* programado en *Batch*. *Cron* [23] es un administrador de procesos informáticos que ejecuta tareas en intervalos de tiempo regulares (cada segundo, cada hora, cada semana, cada mes, etc.). Opera en segundo plano, es decir, el proceso se lleva a cabo en prioridad baja, utiliza menos recursos y permite el aumento de la velocidad de procesado o la ejecución de más procesos simultáneamente. Por otro lado, *Batch* es un lenguaje de programación que usa un sistema de procesado por lotes de forma secuencial. Se utiliza para automatizar tareas desde la consola de Windows.

Otra consideración a tener en cuenta en este apartado es que se accede a la base de datos con un usuario y contraseña, las cuales deben ir añadidas **en claro** en el código que realiza la copia de seguridad, cosa que no se debe permitir. Para darle más seguridad al proceso y que un usuario no autorizado pueda obtener las credenciales de la base de datos, se utiliza una herramienta que proporciona MySQL llamada *mysql_config_editor*. Esta herramienta cifra las credenciales del usuario y la contraseña con un alias de host para utilizarlos en vez de las propias credenciales. El alias se almacena en un archivo de configuración en el directorio de inicio. Es importante recordar que esta acción sólo se deberá realizar **una vez** en la consola de comandos.

Una vez realizado la encriptación, se programa un archivo con extensión *.bat* que se encargará de ejecutar la copia de seguridad como se muestra en la Figura 12.

backup.bat

```
::Creamos la fecha actual
echo off
set fecha=%date:~0,2%-%date:~3,2%-%date:~6,4%
set fecha=%fecha:/=%


cd C:\Programa\mysql-5.7.24-winx64\bin
mysqldump --login-path=myhostalias blexermed > C:\Users\albaa\Documents\PFG\Software\backup\prueba_%fecha%.sql
```

Figura 12. Archivo ejecutable que crea la copia de seguridad de la base de datos

Una vez ejecutado se obtiene un fichero de extensión *.sql*, donde se encuentran almacenados los datos y la estructura de la base de datos, como se muestra en la Figura 13.

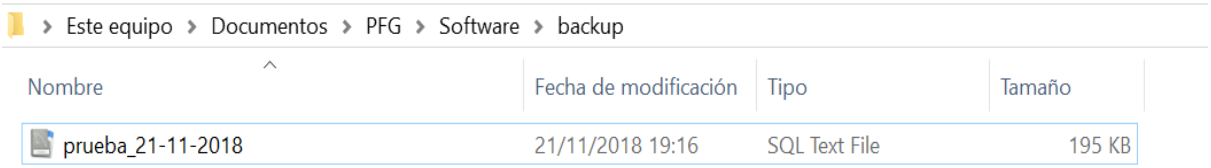

Figura 13. Comprobación de la ejecución de la copia de seguridad

El siguiente paso será automatizar la creación de copias de seguridad para que se realicen cada periodo personalizable. Para ello, se hace uso de una herramienta que proporciona Windows llamada "**Programador de Tareas"**.

El "**Programador de Tareas"** es una herramienta que proporciona una amplia variedad de posibilidades. En este caso permite, no solo ejecutar diferentes tareas en tiempos determinados, sino programar acciones sin estar presente.

En primer lugar, se busca en el inicio del ordenador "programador de tareas". Como se observa en la Figura 14 el programador de tareas se divide en tres columnas:

- En el panel de la izquierda aparece un listado de carpetas donde se organizan las tareas programadas.
- En el panel del medio se encuentra el resumen del programador de tareas, donde se encuentran todas las tareas que están activas en ese momento.
- En el panel de la derecha están los accesos directos a acciones frecuentes.

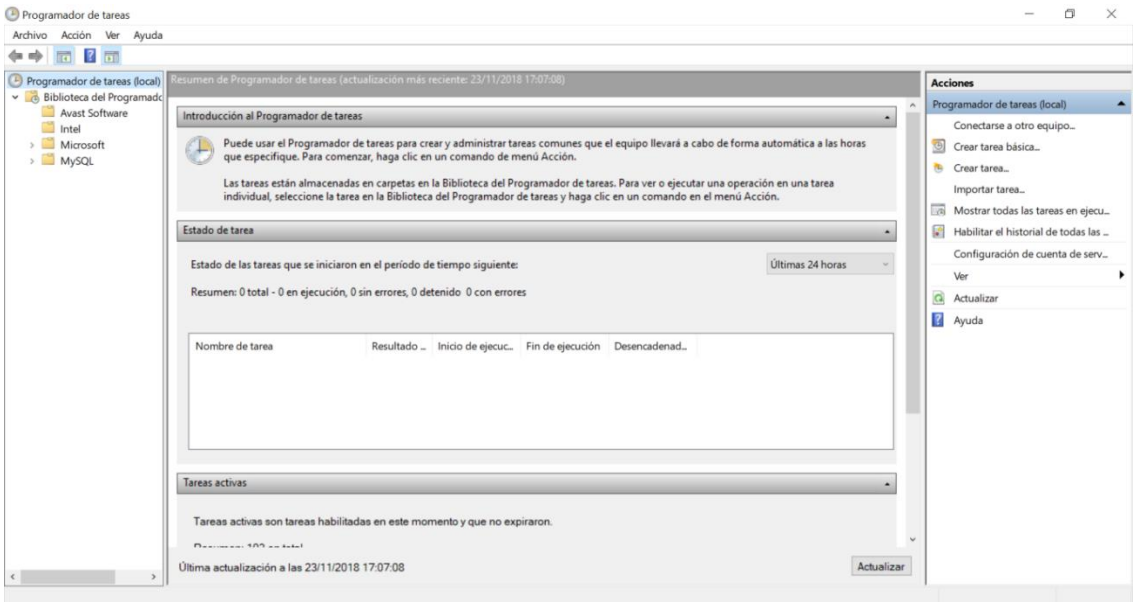

Figura 14 Página principal del programador de tareas.

Se busca la tarea que se desea modificar, en este caso "**Backups base de datos**". Si se quiere modificar algún dato de configuración habrá que pulsar dos veces sobre la tarea.

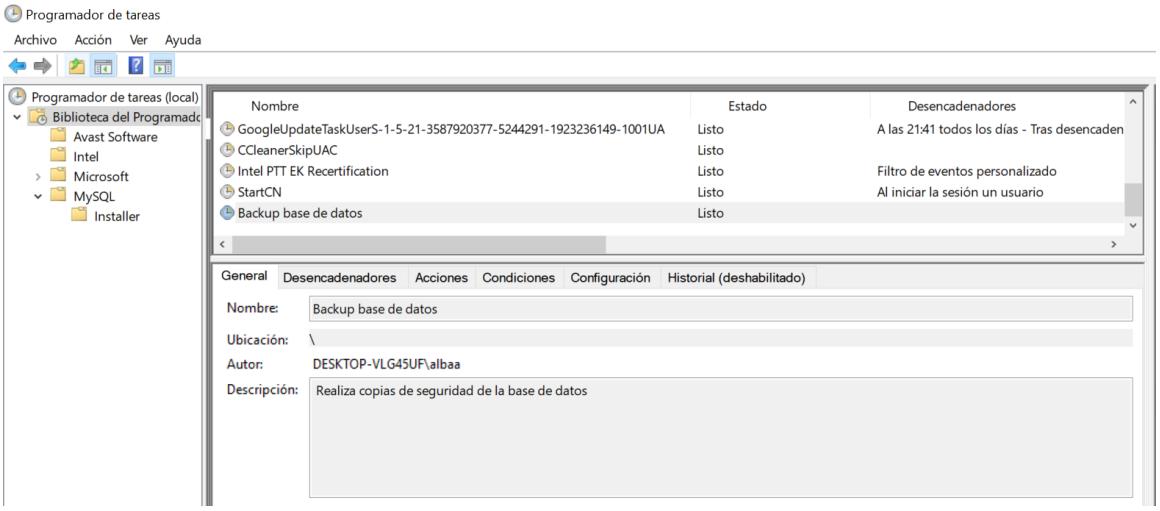

Figura 15 Tarea programada para realizar copia de seguridad

En la primera pestaña, "**General**", se indica el nombre que tendrá la tarea y una pequeña descripción para saber qué acción realiza. Por último, hay que seleccionar "**Ejecutar tanto si el usuario inicio sesión como si no**" para que se realice la tarea ante cualquier situación y, también en el desplegable de la parte inferior indicar que el sistema operativo para el que se configura la tarea es Windows 10. La configuración correcta de la tarea se muestra en la Figura 16.

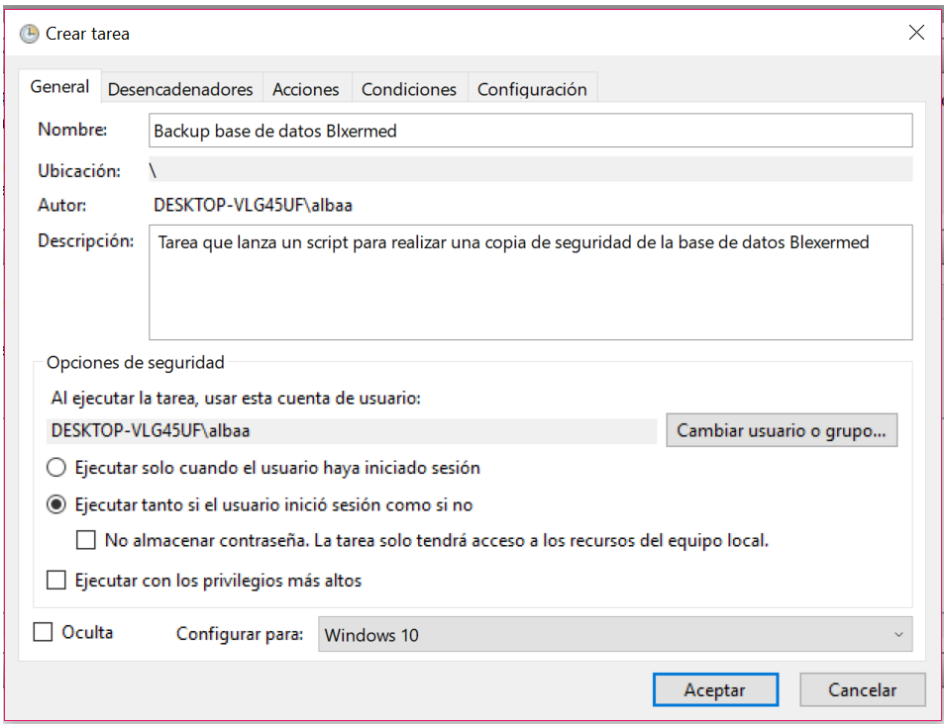

Figura 16. Configuración de la pestaña "General"

En la siguiente pestaña, "**Desencadenadores**", se pulsa el botón "**Nuevo**", apareciendo la pestaña de la Figura 17 . En esta pestaña se indica la fecha en la que se desea que la tarea comience y cada cuanto debe ejecutarse.

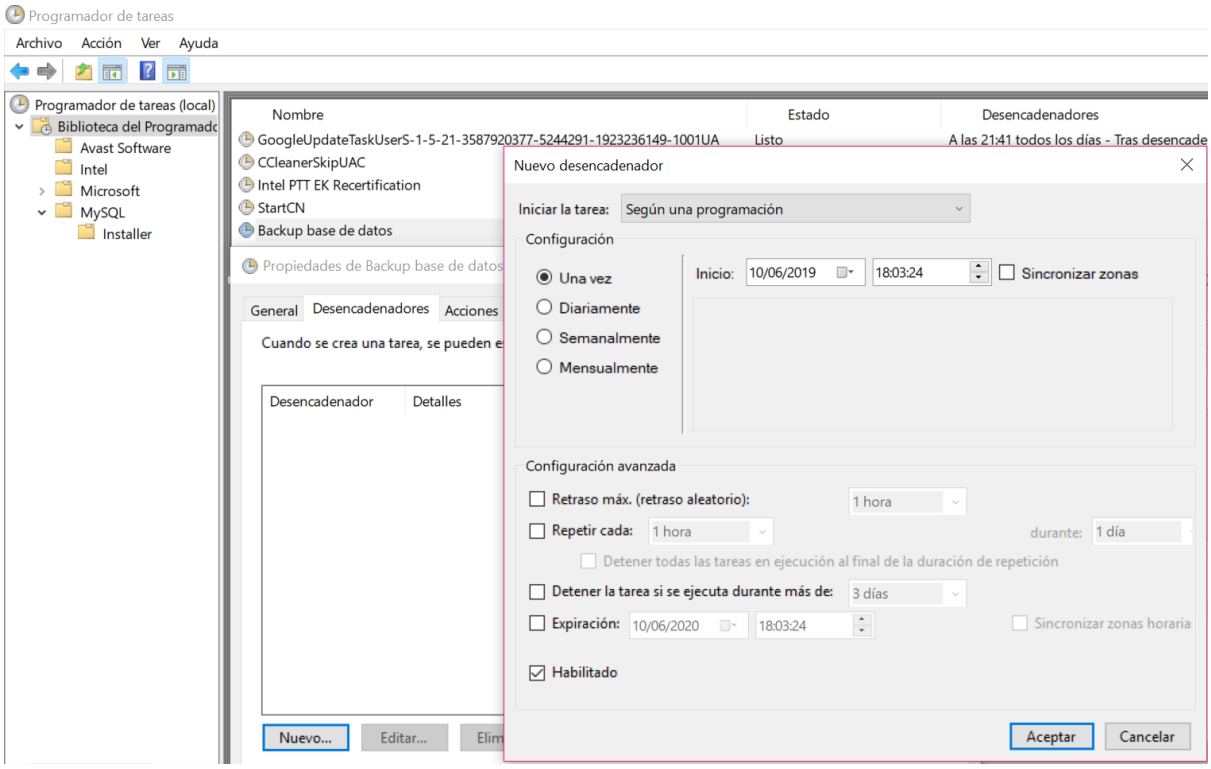

Figura 17 Pestaña "Desencadenante, configuración periodo de tiempo de la ejecución de la tarea

En la pestaña "**Acciones**", se selecciona la tarea que debe ejecutarse, en este caso el script que mencionamos en el apartado 4.2, encargado de realizar una copia de seguridad de la base de datos de *Blexer-med*.

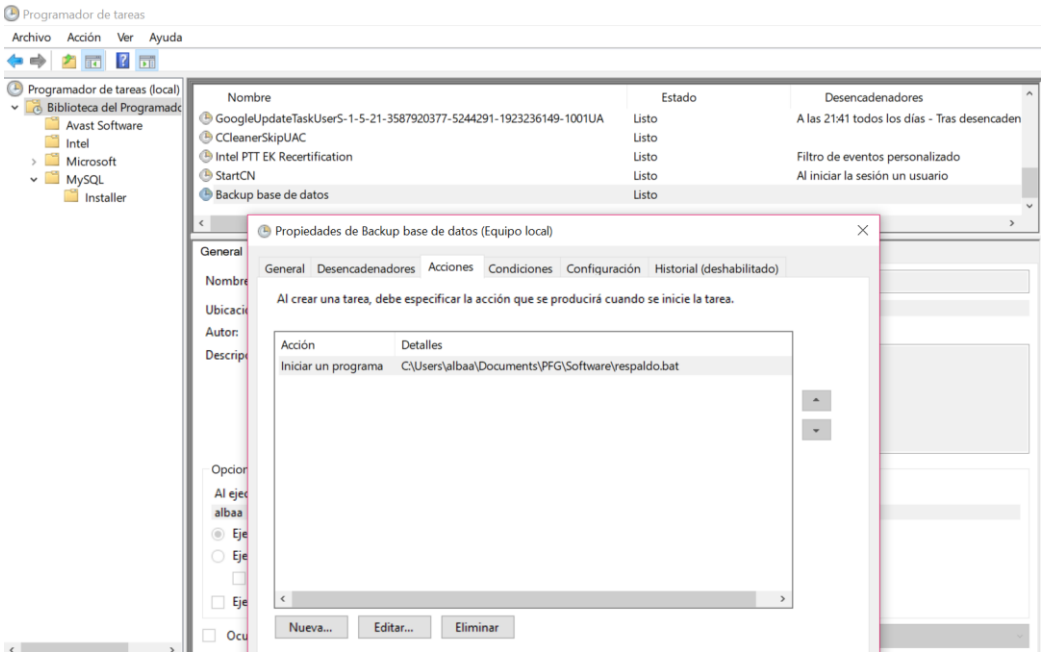

Figura 18 Pestaña "Acciones" y selección del elemento a ejecutarse

La siguiente pestaña, "**Condición**", mostrada en la Figura 19 permite establecer las causas que inician, o no, las tareas.

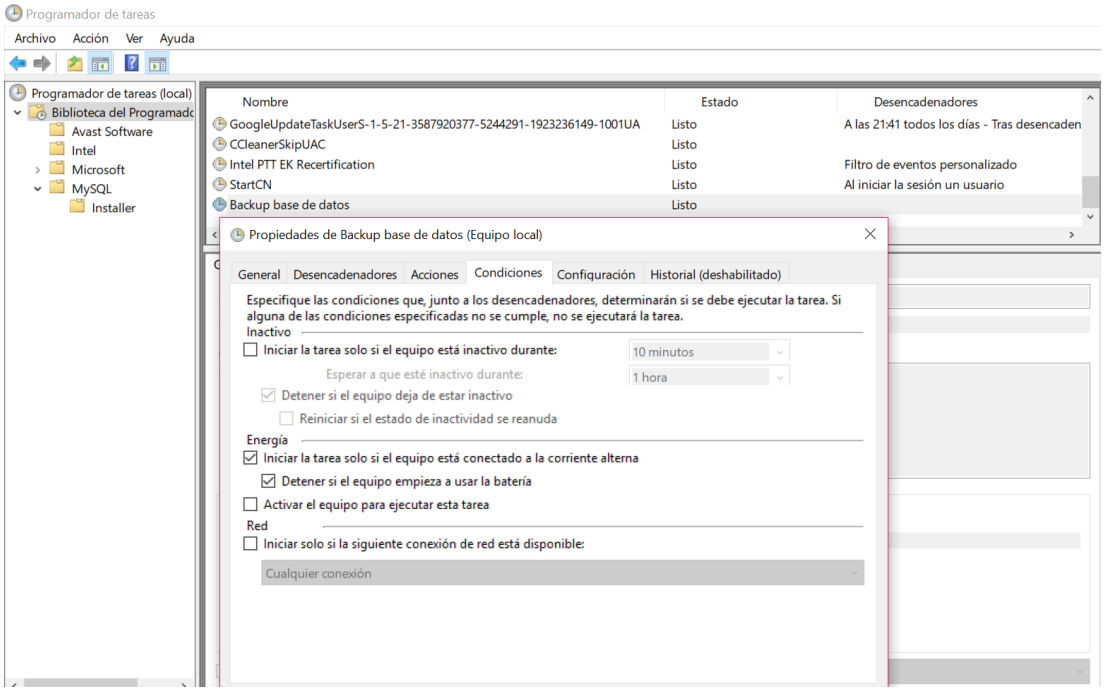

Figura 19 Pestaña Condición, se establece que condiciones inician la tarea

La última pestaña es "**Configuración**" mostrada en la Figura 20. En esta pestaña existen una seria de campos de configuración para personalizar el tratamiento de la tarea, ya sea cómo

proceder si la tarea no se puede ejecutar, si se espera un periodo de tiempo para volverla a lanzar y cuánto tiempo se espera, etc.

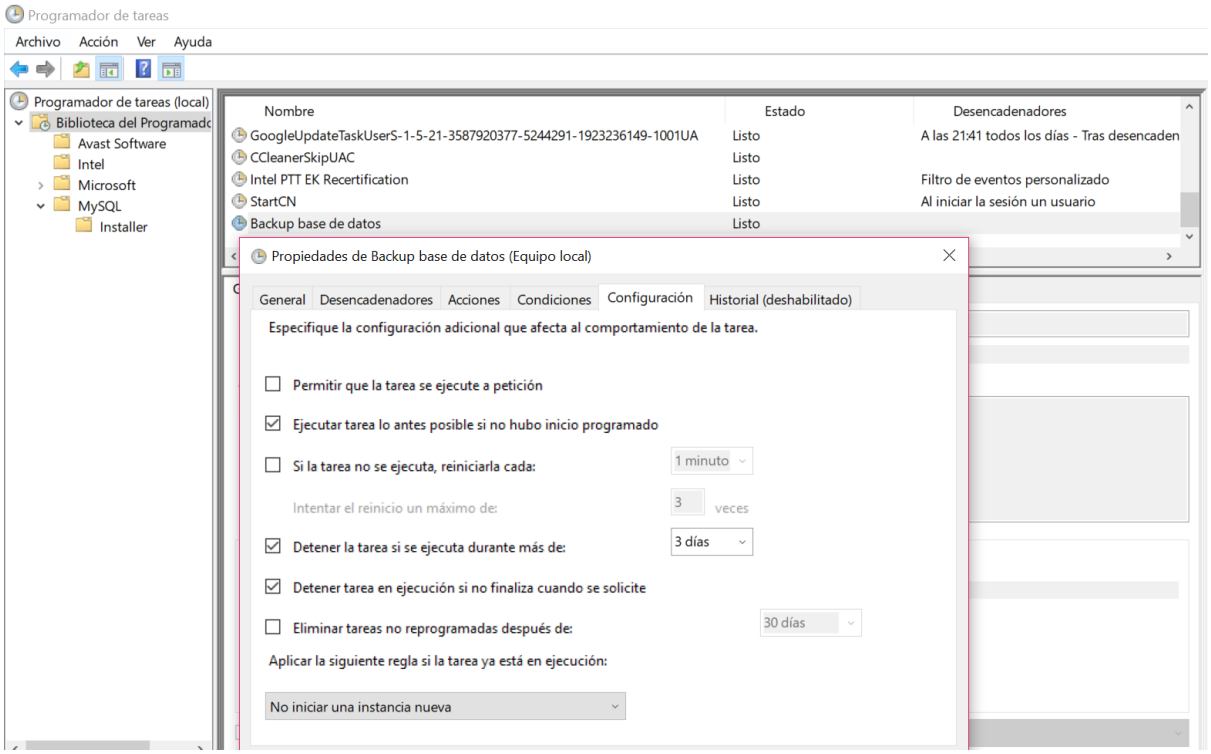

Figura 20 Pestaña de configuración para personalizar la ejecución de la tarea

Una vez programada la tarea de realizar una copia de seguridad una vez a la semana, aparece un nuevo inconveniente: el espacio que se necesitaría para almacenar todas las copias de seguridad. Para solucionar este problema, se programa un código en *Batch* que elimina todas las copias de seguridad con fecha anterior a 60 días de la fecha actual, mostrado en la Figura 21.

limpiarBackup.bat

```
:: Elimina archivos de mas de 60 dias de antiguedad de la carpeta especificada
@echo off
Forfiles /p "C:\Users\albaa\Downloads\prueba" /s /m *.* -d -60 /c "cmd /c del /q @path"
```

Figura 21 Programa que borra copias de seguridad anterior a 60 días de la fecha actual

Se programa esta tarea para que se ejecute automáticamente utilizando el procedimiento del programador de tareas.

4.3. Seguridad en formación, almacenamiento y transmisión de contraseñas

Las contraseñas son elementos a los que muchas veces no se les da la importancia que requieren, pero si se generan y controlan de una manera acertada y eficiente, permiten evitar intrusismo o suplantación de identidad digital, además de *spam* u otros problemas de acceso a los datos por parte de terceros.

Según el estándar ISO/IEC 27002 las contraseñas deben seguir una serie de pautas para poder considerarse seguras:

- Longitud mínima 8 caracteres
- Longitud máxima 16 caracteres
- Contener al menos una mayúscula
- Contener al menos un número entero

En el programa se usan reglas *JQuery* para comprobar los diferentes campos de los formularios, pero en este caso no existe ninguna regla que permita comprobar que un valor introducido cumple con las reglas anteriormente descritas. Por eso, será necesario crear una regla personalizada, para posteriormente comprobar si se cumple el formato, y en caso de que no sea así, el sistema muestre un mensaje al usuario y no le permita continuar con el registro.

Para controlar que la contraseña que se introduce cumple con los requisitos mencionados, se ha creado una función personalizada, donde se comprueba una expresión regular, para posteriormente añadirla a la regla.

Una expresión regular es una secuencia de caracteres que forman un patrón de búsqueda. En este caso, como se observa en la Figura 22, la variable "**patron**" está inicializada con una expresión regular que permite comprobar si la contraseña tiene entre 8 y 16 dígitos y si contiene al menos una mayúscula, una minúscula y un número.

```
//Regla personalizada para que la contraseña contenga 8 digitos minimo, un numero y una mayuscula
$.validator.addMethod("pass",function(value,element){
    var patron = /^(?=.*\d)(?=.*[a-z])(?=.*[A-Z]).{8,16}$/;
    return patron.test(value);
 }, "Passwords are 8-16 characters with uppercase letters, lowercase letters and at least
     one number.");
```

Figura 22 Código para que la contraseña tenga entre 8 y 16 dígitos, un número y una mayúscula

Si se analiza el código, se impone que en la contraseña:

- Exista al menos algún dígito (?:.*\d)
- Exista al menos una mayúsculas (?:.*[A-Z])
- Exista al menos una minúsculas (?:.*[a-z])

- Con el cuantificador {8,16} se indica que la contraseña debe tener una longitud mínima de 8 y máximo 16

Posteriormente, se añade la regla creada al resto de código para comprobar si la contraseña cumple con las especificaciones. Cuando el usuario introduzca una contraseña que no cumpla las reglas anteriormente descritas, el sistema le avisara con un mensaje tal y como se muestra en la Figura 23.

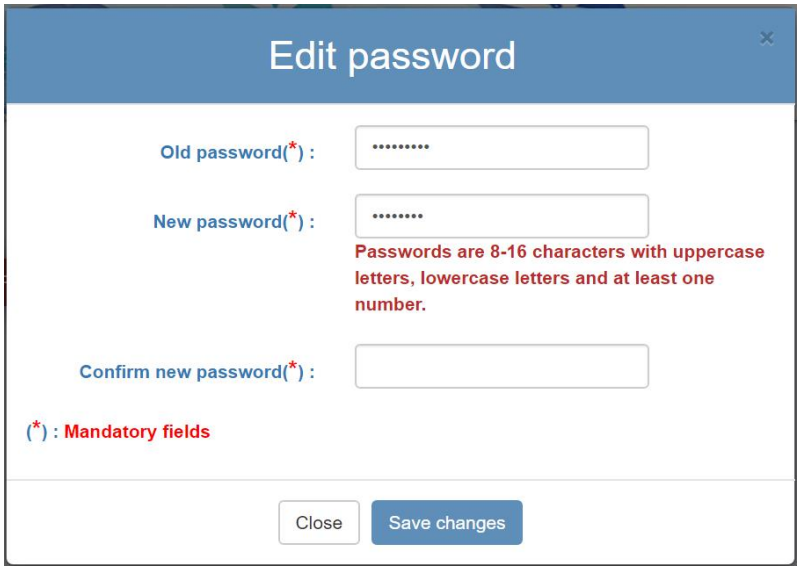

Figura 23 Mensaje que se muestra cuando no se introduce una contraseña valida

Una vez que se ha validado la correcta formación de las contraseñas, es necesario fortalecer el modo en el que se almacenan en la base de datos y se envían a través de la red. El método más seguro es mediante encriptación, en este caso utilizando la función *hash*.

Un *hash* es una secuencia cifrada de caracteres, que se obtiene al aplicar algoritmos sobre la contraseña dada por el usuario. Cada vez que el usuario introduce la contraseña en la plataforma se genera el *hash*, el cual se compara con el almacenado en la base de datos, y en caso de que coincidan significará que la contraseña es correcta. El *hash* se almacena en la base de datos cuando la contraseña se crea por primera vez o se modifica la existente [17].

Existen varias funciones *hash*, pero las que se adaptan a las contraseñas deben cumplir cinco propiedades principales:

1. El mismo mensaje procesado por la misma función *hash* debe dar siempre la misma cadena.
2. No se puede generar el mensaje a partir de su *hash*.
3. Un cambio en el mensaje debe dar una cadena diferente, aunque se use la misma función *hash*.

4. Dos mensajes diferentes nunca pueden producir el mismo *hash*.
5. El algoritmo debe ser lento, ya que uno rápido ayudaría a los ataques de fuerza bruta, es decir, aquellos que se basan en probar todas las combinaciones posibles hasta encontrar la correcta.

Existen varias funciones *hash* que cumplen estas propiedades. Se valoran alguna de las más usadas para determinar cuál es la más adecuada al trabajo [24].

Algoritmo MD5 (*Message Digest Algorithm 5*)

MD5 realiza un procesamiento por bloques de 512 bits para generar números de 128 bits. Aunque MD5 es un algoritmo muy utilizado, no es seguro ya que es susceptible a ataques de fuerza bruta debido a que su algoritmo es rápido. Además, no es resistente a las colisiones, es decir, diferentes contraseñas pueden producir el mismo *hash*. Por tanto, como no cumple dos de las reglas para ser una función *hash* robusta se ha descartado.

Algoritmo SHA (*Secure Hash Algorithm*)

SHA es muy similar a MD5 pero genera números de 160 bits. Sin embargo, como en MD5, aunque en menor medida, puede generar el mismo *hash* para dos contraseñas diferentes. Por ello también se descarta.

Algoritmo PBKDF2 (*Password Based Key Derivation Finction 2*)

Este algoritmo tiene como objetivo hacer que la función *hash* sea lo suficientemente lenta como para impedir ataques, pero lo suficiente rápida para no causar un retraso notable para el usuario. Para llevar a cabo su objetivo toma un factor de trabajo que determina que tan lenta será la función *hash*, de manera que, si el ordenador se vuelve más rápido o más lento, el factor de trabajo se modifica para adaptarse. Por tanto, se implementa este algoritmo para funciones *hash* para encriptar las contraseñas que se guardan en la base de datos y viajan a través de la red. Una vez implementado las contraseñas se ven encriptadas como muestra la Figura 24.

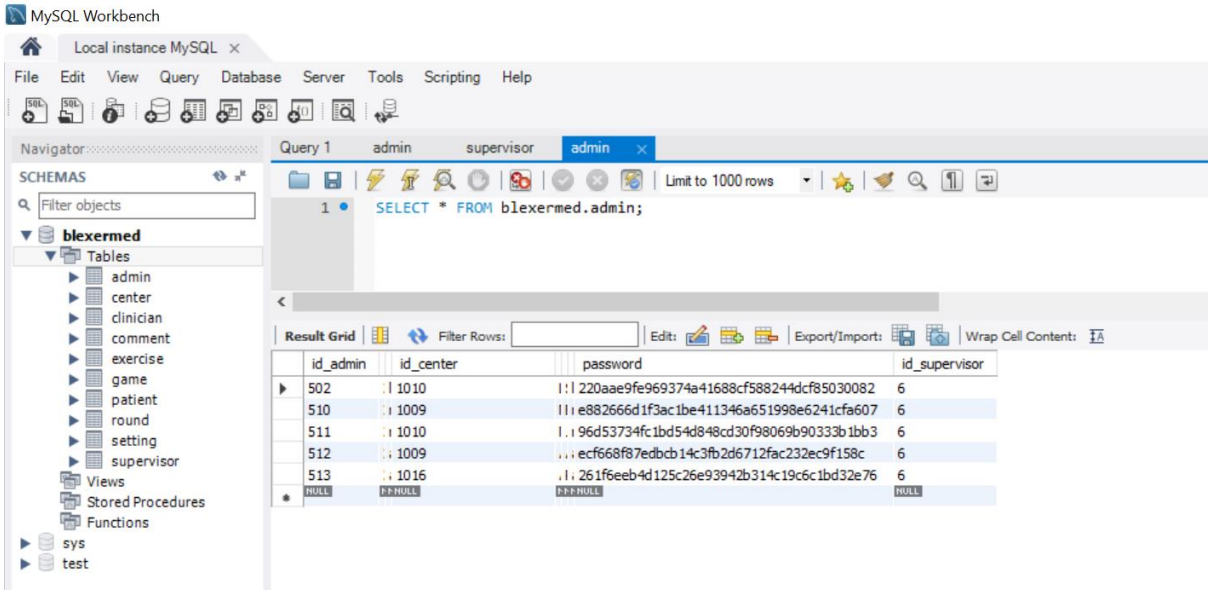

Figura 24 Función hash en contraseñas en la base de datos

4.4. Seguridad de transmisión de información

Una de las principales consideraciones cuando se crea una plataforma web es la seguridad de los datos e información que se envían. No proporcionar a un sistema una buena seguridad puede provocar problemas que van desde la sobrecarga en un servidor, hasta la manipulación de la información alojada en la base de datos o en los paquetes que viajan por la red.

Es importante establecer las medidas de seguridad necesarias para evitar los riesgos de los servicios de seguridad mencionados en el apartado 3.3.1. Para ello se deben controlar dos factores predominantemente. El primero es el control de acceso, es decir, un usuario tiene restringido el acceso a unas páginas o contenido determinado. En este caso, esta tarea se lleva a cabo mediante la separación en roles de la plataforma web, además de la necesidad de unas credenciales para entrar en cada rol. El segundo factor es dotar a los mensajes que se transmiten con un mecanismo de seguridad. Para ello se proponen tres métodos:

1. **Protocolo HTTPS (*Hypertext Transfer Protocol Secure*)**

Una metodología para que la transmisión de paquetes sea segura es utilizar un protocolo HTTPS. Actualmente se utiliza el protocolo HTTP (*Hypertext Transfer Protocol*) para la transmisión de datos entre cliente y servidor.

HTTP es un protocolo de comunicaciones que asegura que la transferencia de información se va a hacer correctamente mediante el esquema petición-respuesta entre un cliente y un servidor. Por otro lado, HTTPS, es la manera más segura de acceder a los contenidos de

internet, debido a que cualquier dato o información que se introduzca en el navegador será cifrada.

No se ha implementado este método porque **supone un coste anual** por su utilización, debido a que es necesario tener un certificado.

2. **Cifrado de los datos de la base de datos**

El segundo método es cifrar los datos de la base de datos, de tal forma que cuando se quiera transmitir información ya este cifrada de antemano.

MySQL está previsto de un algoritmo llamado AES (*Advanced Encryption Standard*) que permite cifrar la información que se encuentra en la base de datos. AES es un algoritmo de cifrado simétrico, es decir, requiere de una contraseña para descifrar la información. En este algoritmo se permite la utilización de claves de un tamaño máximo de 256 bits, por lo cual se considera uno de los protocolos más seguros.

Una vez revisado y comprendido el código que se realizó para la cumplimentación de la página se ha visto que las consultas y el envío de información a la base de datos se hace mediante el método Ajax de *JQuery*. Dicho método no contempla una opción para enviar la información cifrada, y, por ello, se ha descartado este método.

Se puede ver en el Anexo 5. Manual de usuario para encriptar datos de la base de datos con la herramienta MySQL un manual de usuario de como cifrar la información de la base de datos.

3. **Añadir complementos que otorguen seguridad al método *Ajax***

Para establecer una fuerte seguridad en la transmisión de la información que se envía desde el cliente al servidor y viceversa, se ha analizado la metodología creada para hacer las consultas. En este caso, como se comentaba antes, se ha visto que se utiliza el método *Ajax* de *JQuery* para hacer las consultas al servidor. *Ajax* es una tecnología de desarrollo web que permite al usuario intercambiar información entre el servidor y el cliente, con lo que se consigue que la web sea dinámica, ágil y rápida.

En primer lugar, cualquier sitio web debe enviar la información de su contenido usando el método POST, ya que este método hace que los datos viajen ocultos hacía el destino. Si en contraposición se utilizase el método GET, toda la información sería visualizada en la barra de direcciones.

Actualmente se utiliza el método GET para la petición y solicitud de la información. Mediante el programa *Wireshark*, en la Figura 25 se puede ver como la contraseña aparece en la barra de direcciones cuando se utiliza el método GET.

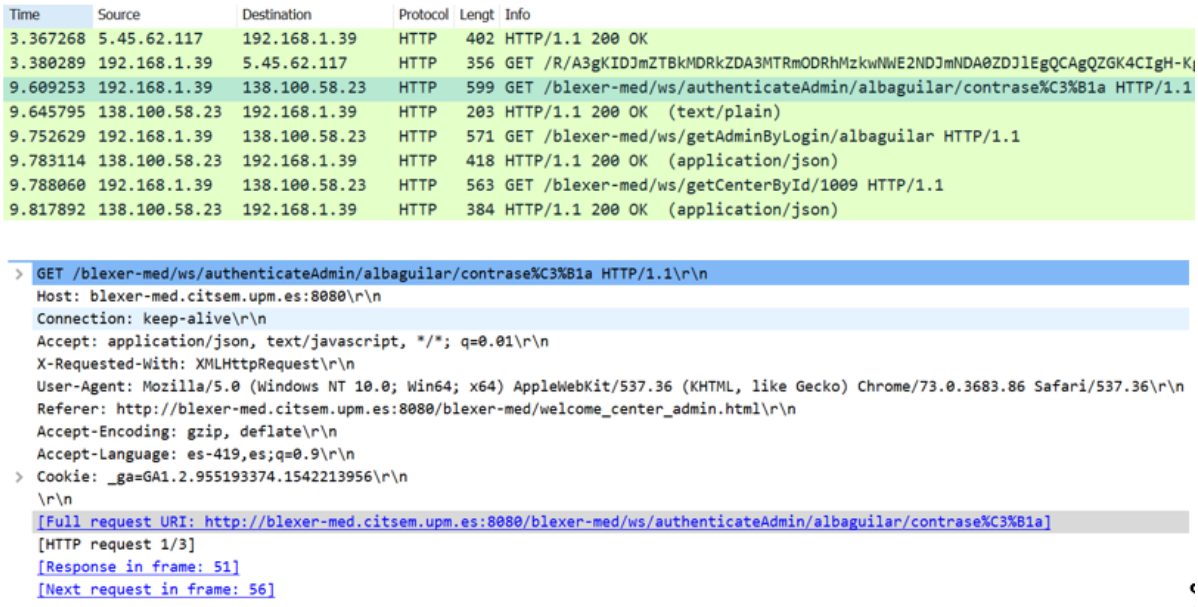

Figura 25 Captura del Wireshark de la autenticación del médico.

Se modifica el método de petición y envío de información para que funcione con el método POST, en lugar de GET. En este caso, si se visualiza la captura de *Wireshark* en la Figura 26 se puede ver el tráfico cuando un usuario se autentica. En este caso, la contraseña ya no se muestra como parámetro de la barra de direcciones.

Figura 26 Captura Wireshark utilizando el método POST

En segundo lugar, es importante validar los campos requeridos en un formulario, es decir, los campos completados deben tener un formato y extensión apropiados, dificultando así los posibles ataques.

En este caso se ha utilizado una librería para *JavaScript* que permite fácilmente validar cualquier campo de un formulario. Se han añadido varias validaciones:

1. El formato del email debe tener un patrón name@dominio.es.
2. Se comprueba que solo se hayan añadido números en los campos como, por ejemplo, código postal o número de teléfono.

3. Se comprueba que al modificar la contraseña sean iguales la nueva añadida y la de validación.

Si el usuario no introduce un valor válido, se le mostrara un mensaje de error como el que aparece en la Figura 27 para el caso de un patrón de email no válido:

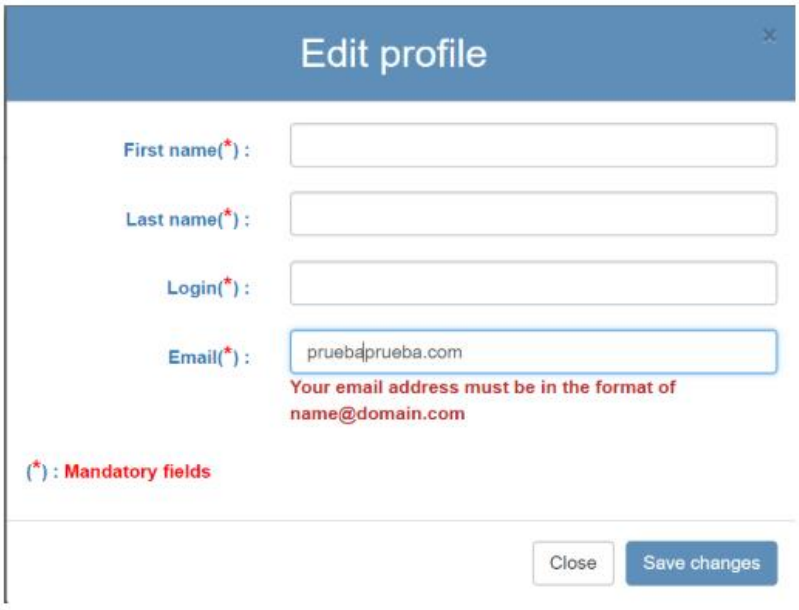

Figura 27 Mensaje de error si no se introduce un formato de email valido

Al igual que en el resto de los casos, como se puede ver en la Figura 28, si el usuario no introduce solo números, se le mostrará un mensaje de error.

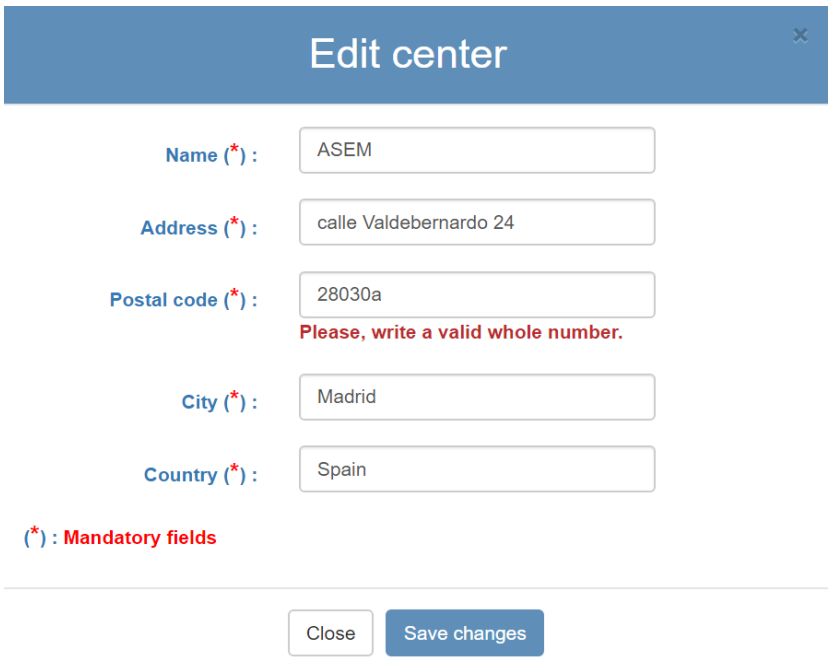

Figura 28 Mensaje de error si no se han introducido solo números

Y por último, cuando un usuario modifica su contraseña, en el caso de que no haya introducido en el campo "N**ew password**" y en el "**Confirm new password"** el mismo valor, se mostrará un mensaje de error como el de la Figura 29.

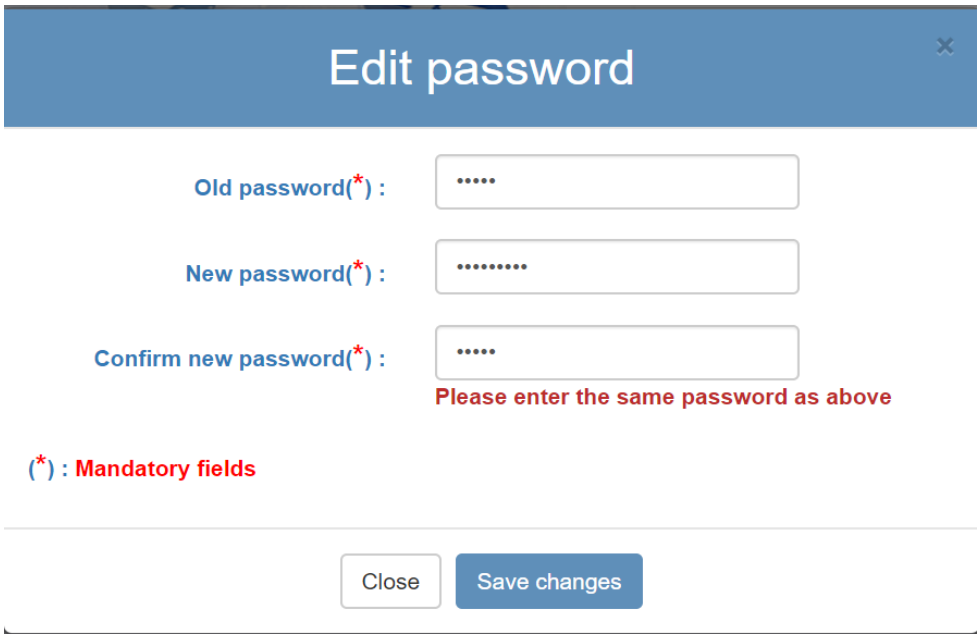

Figura 29 Mensaje de error si no se introduce mismo valor al modificar la contraseña

5. Diseño de la Web

En este apartado se desarrollan las modificaciones que se aplican al diseño y funcionalidades de la página web. En los objetivos se establece, en primer lugar, la necesidad de modificar el diseño para que sea más atractivo ante los usuarios. Posteriormente, tras las pruebas realizadas de la primera versión de la plataforma web, se han observado una serie de mejoras necesarias para la correcta funcionalidad de la herramienta como se ha visto en los objetivos.

5.1. Modificación del diseño de la página web

Cada color provoca unas sensaciones determinadas en las personas, por lo que influye en cómo se comportan los usuarios. Acertar con la elección y cantidad de colores que se utiliza en la página es fundamental para que esta refleje la filosofía que se quiere transmitir. La psicología del color, por tanto, ayuda a fortalecer el uso de una página web. Muchos estudios [25] han demostrado que muchas de las decisiones que se toman a la hora de interactuar con aplicaciones telemáticas están fuertemente influenciadas por el color.

El proyecto está dirigido a personal cualificado que realiza un seguimiento sobre la rehabilitación motora de mayoritariamente niños, por ello, se elige una gama de colores azules y grises para las páginas principales de la web. El gris se asocia con formalidad y profesionalidad y el azul con salud, calma, seriedad y eficacia. Además, cada página tiene un fondo de pantalla acorde con el tipo de usuario: Super Administrador, Administrador de Centro o Médico.

En la Figura 30 se muestra la visualización de la página principal del Super Administrador en la primera versión de la plataforma web y en la Figura 31 de la segunda versión. En la Figura 32 y Figura 33 se muestran las comparativas de la página del Centro Médico y en la Figura 34 y Figura 35 las de la página del Médico. En estas imágenes se compara la visualización de la primera versión de la web en comparativa con el diseño de la segunda versión. Como se observa, se ha añadido un fondo personalizado para el rol con la gama de colores especificada. Por otro lado, se ha modificado la visualización del formulario de autenticación, dividiéndolo en dos partes. En la parte izquierda se muestra el rol al que estamos accediendo, el icono de la plataforma y las opciones de los otros roles. En la parte de la derecha, el formulario para entrar a la web y los iconos de las entidades colaboradoras. De esta manera se consigue una primera impresión de profesionalidad, así como una plataforma más intuitiva de utilizar donde cada rol se diferencia notablemente.

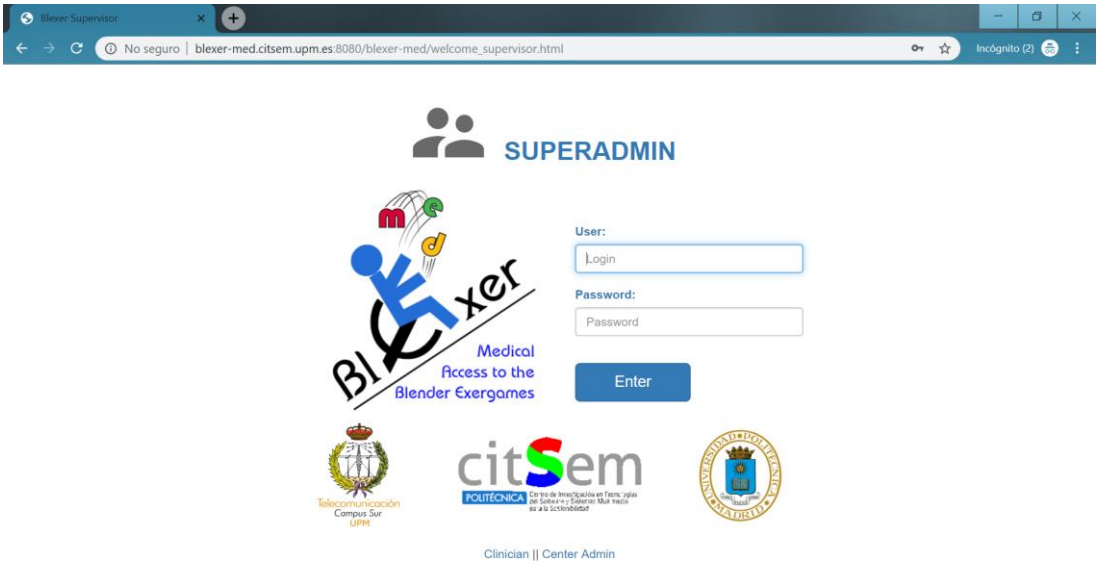

Figura 30 Página de autenticación del Super Administrador V1

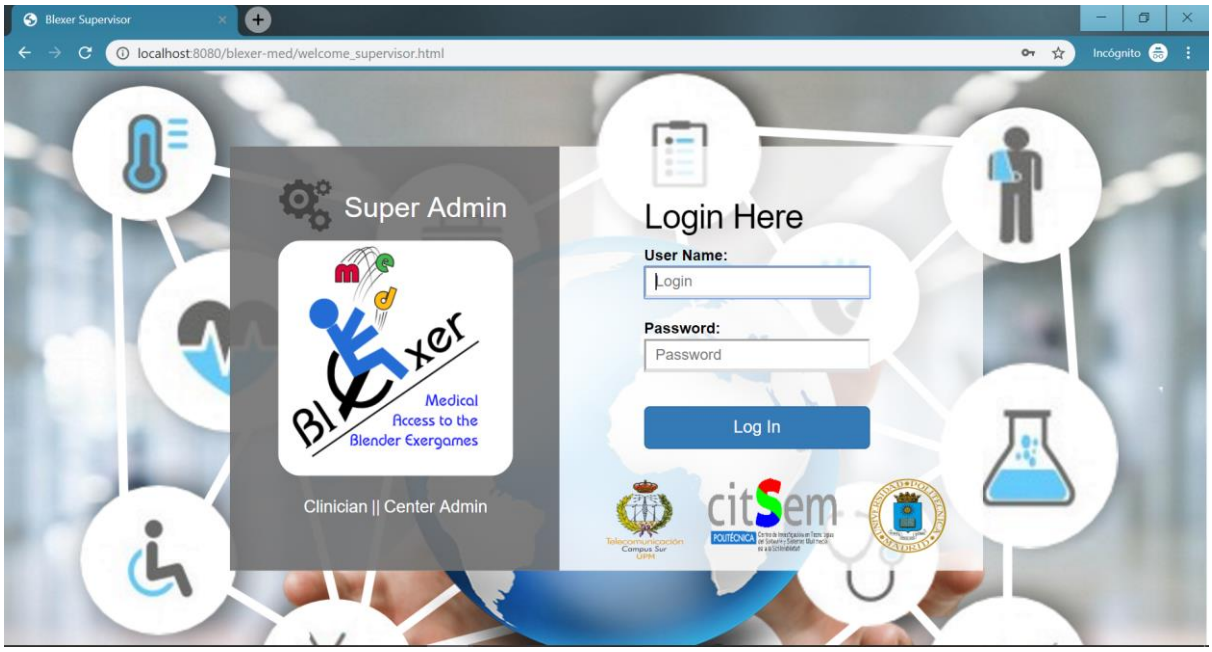

Figura 31. Página de autenticación del Super Administrador V2

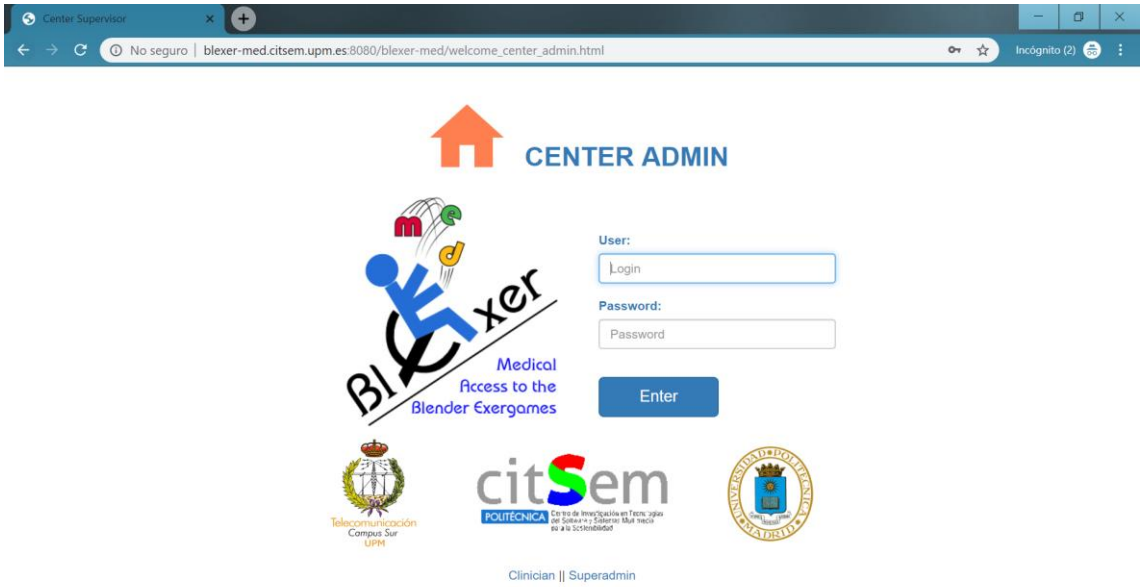

Figura 32 Página de autenticación del Centro Médico V1

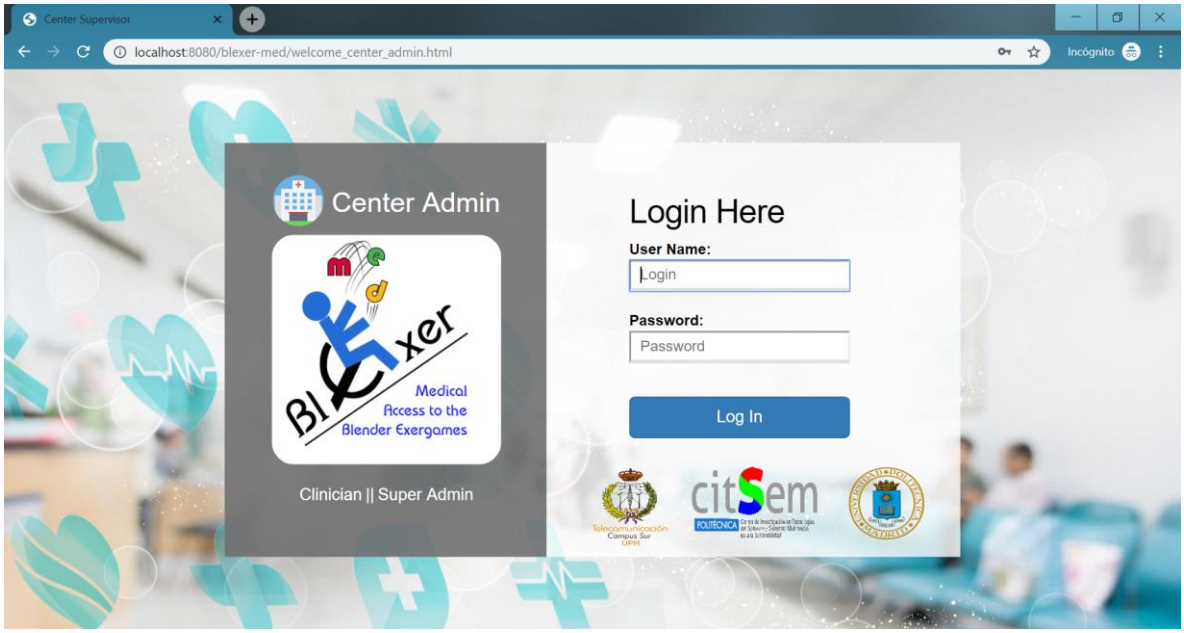

Figura 33 Página de autenticación del Centro Médico V2

Figura 34 Página de autenticación del Médico V1

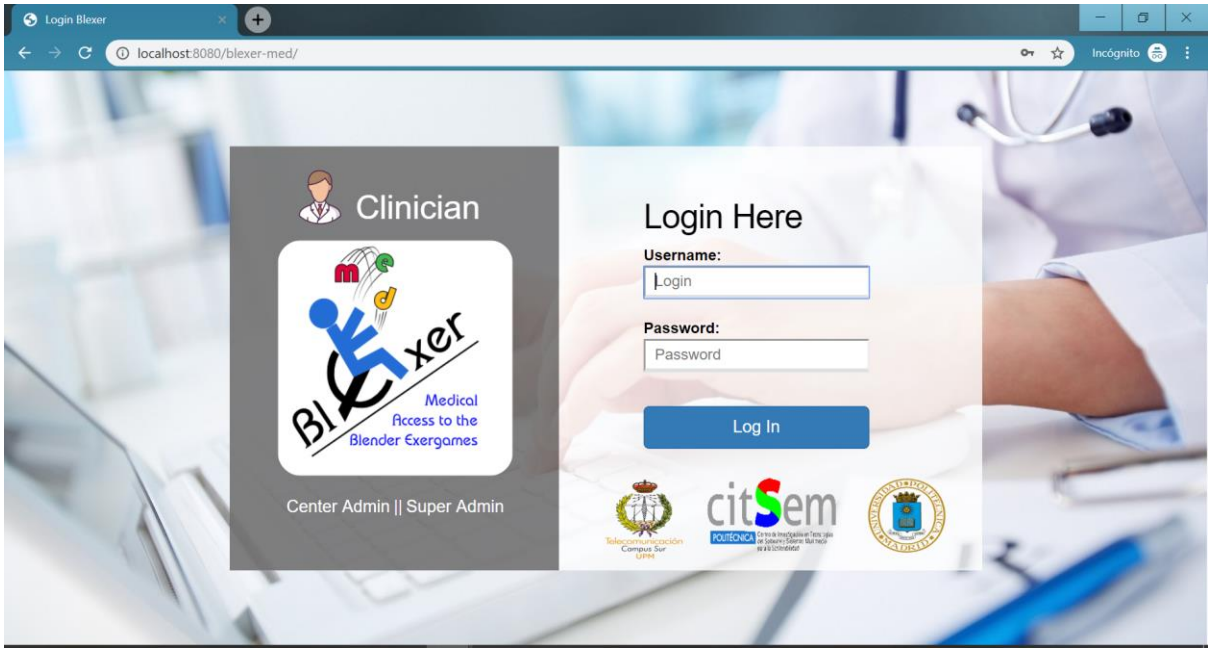

Figura 35 Página de autenticación del Medico V2

Para el resto de las páginas internas de cada rol, se ha seguido con la gama de colores grises y azules, alternándola con colores más llamativos para diferenciar las funcionalidades de la plataforma. En la Figura 36 y Figura 37 se puede ver una comparativa del aspecto de la primera y segunda versión.

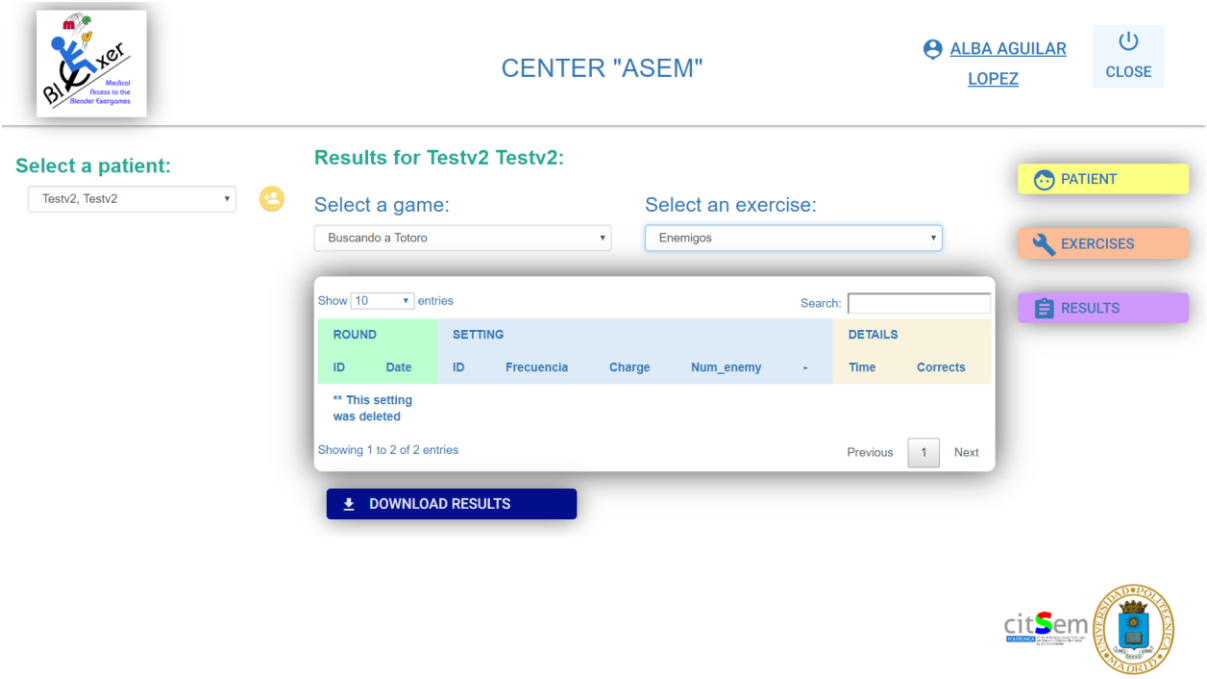

Figura 36 Página interna V1

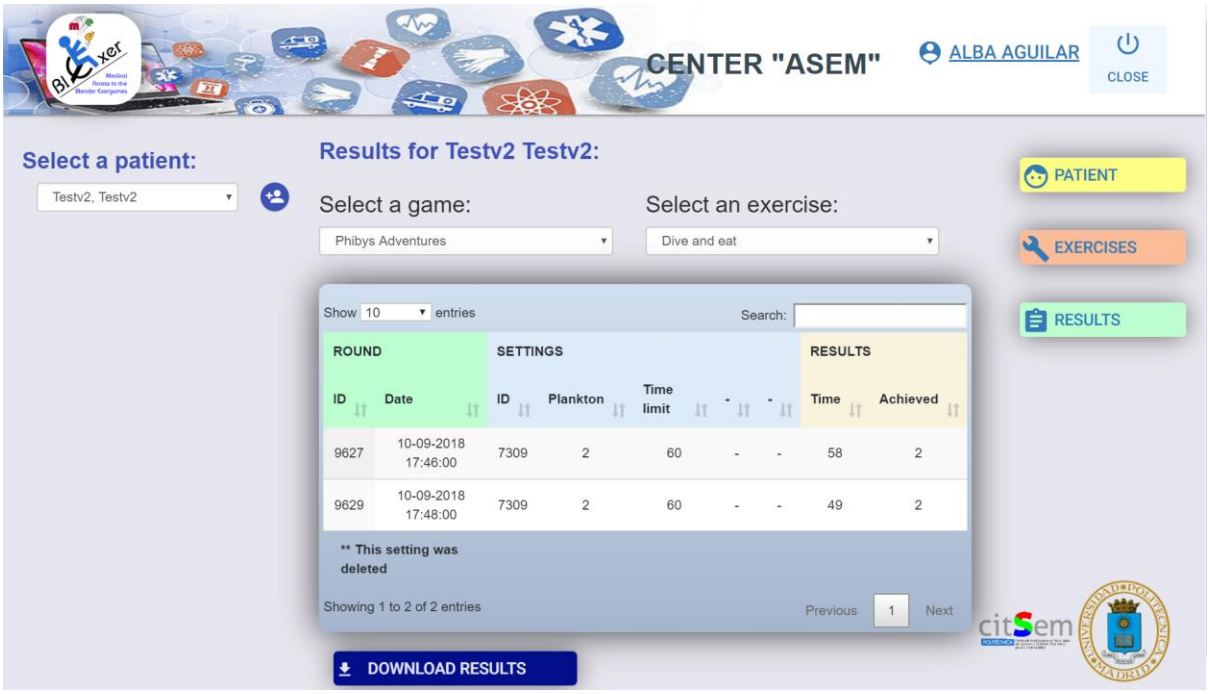

Figura 37 Página interna V2

5.2. Mejora de funcionalidades de la plataforma web

Después de realizar numerosas pruebas con diferentes usuarios, de todas las funcionalidades que ofrece la plataforma web, se vio la necesidad de cambiar algunas de ellas para mejorar la usabilidad y hacer la web más operativa.

5.2.1. Solucionar la ordenación de tabla

Se ha solucionado la ordenación de los datos de las tablas por orden ascendente o descendente según la distinción seleccionada, ya que este aspecto no funcionaba correctamente en la versión anterior. En la Figura 38 se observa una tabla ordenada por el ID.

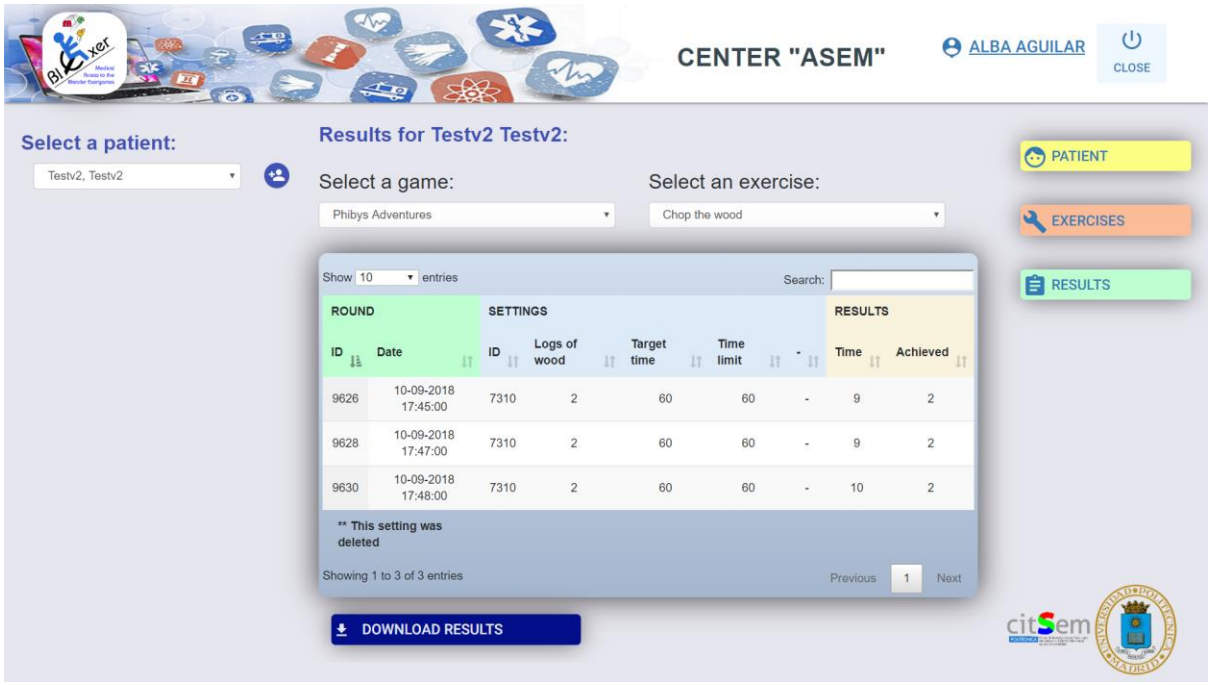

Figura 38 Tabla de datos ordenada por ID

5.2.2. Estructuración de las tablas para que se adapten a los datos

Otro de los cambios ha sido modificar la estructuración de las tablas para que se dimensionen en función de los datos a mostrar. En la Figura 39 y la Figura 40 se puede ver un ejemplo de la primera versión, donde los datos sobrepasan las dimensiones de la tabla y como se visualiza después de su modificación.

Figura 39 Tabla de datos V1

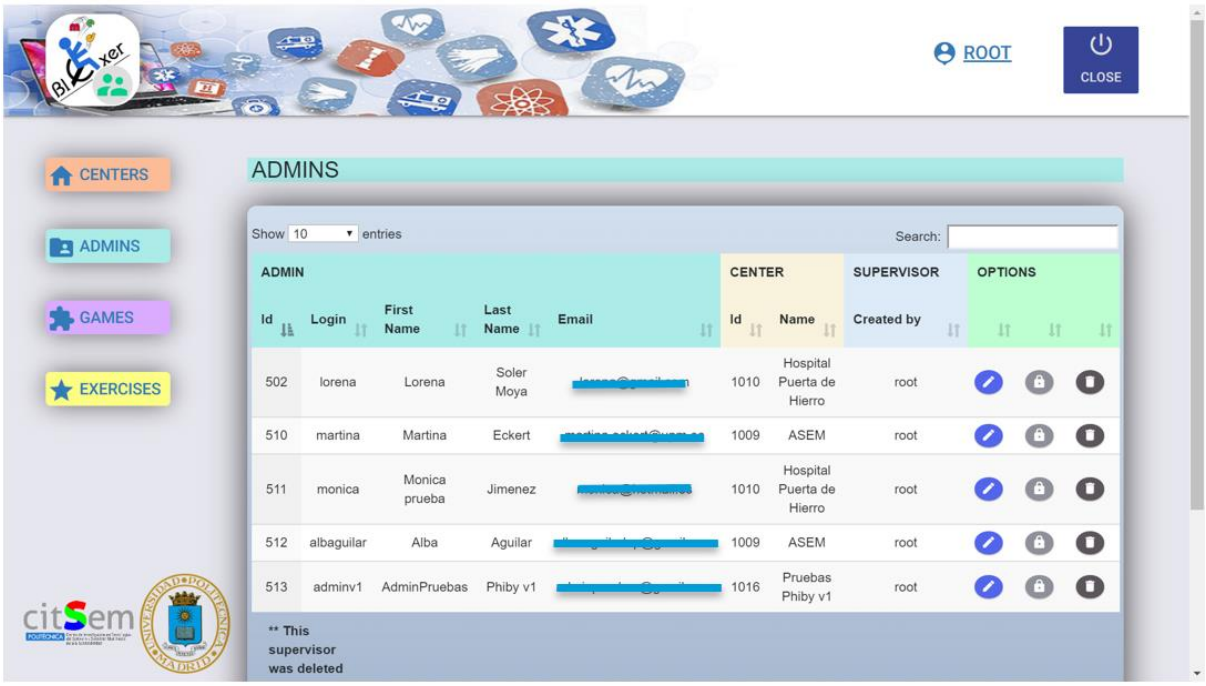

Figura 40 Tabla de datos V2

5.2.3. Cierre de sesión por inactividad

Cerrar sesión de la cuenta activa una vez finalizado su utilización es una tarea que a veces se pasa por alto, pero que es de suma importancia para que ningún usuario sin autorización pueda tener acceso a ella. Por ello, dada la importancia de la seguridad de los datos manejados y la suplantación de identidad, algo muy recomendable es poder cerrar sesión de la cuenta tras un periodo de inactividad de manera automática. Para ese fín, se ha desarrollado en la plataforma un mecanismo que cierra la sesión de todos los usuarios tras un periodo de 10

minutos de inactividad, redirigiendo a la página de autenticación del rol en el que se encontraba el usuario.

Se ha utilizado el comando "**setTimeout ()"** [26]**,** el cual permite realizar una acción en un tiempo determinado. Este método es soportado por la mayoría de los navegadores del mercado. La estructura del método es la mostrada en la Tabla 3.

Tabla 3 Estructura metodo "**setTimeout"**

setTimeout(function, milliseconds, param1, param2,…)	
Function	Acción que va a ser ejecutada
milliseconds	Opcional. Numero de milisegundos que se espera antes de realizar la función
Param	Opcional. Parámetros adicionales para pasarle a la función

Como se puede observar en la Figura 41, tres minutos antes de que la sesión se cierre por inactividad, salta un mensaje de aviso. Sino se realiza ninguna acción, pasado ese tiempo, la sesión se cierra.

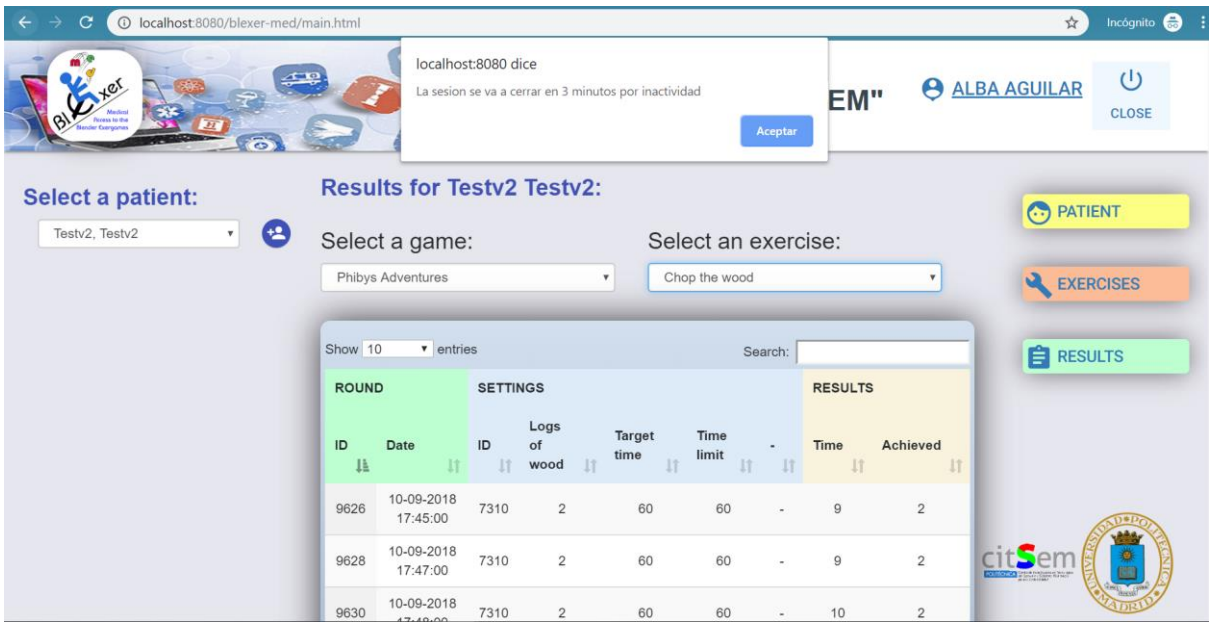

Figura 41 Mensaje de aviso por inactividad

5.2.4. Bloqueo del botón "**atrás**" del navegador

En la primera versión de la página, cada vez que se usaba el botón "**atrás**" del navegador, se cerraba sesión y se tenía que volver a introducir las credenciales. Esto es debido a que las páginas de los roles son una única página **html** en donde los elementos se van cargando, por tanto, aunque se realizaran acciones en la página, cuando se quería ir para atrás, el navegador detecta que la anterior es la página de autenticación.

Para evitar que esto ocurra se ha creado un código que detecta que se ha pulsado el botón "**atrás**" y anula que se redirija a la página de autenticación. El código utiliza una función de *Windows* que devuelve el historial de la última página donde ha estado el usuario, una vez se pulsa el botón "**atrás"**, la página se redirige a la última almacenada en el historial.

El método utilizado es "**window.history.back();"** [26]**,** el cual no recibe ningún parámetro ni devuelve ningún valor. Además, es compatible con la mayoría de los navegadores del mercado.

5.2.5. Otros

Por otro lado, se ha realizado pequeñas modificaciones para remplazar nombre de parámetros de las diferentes tablas de datos y resultados. Así como, modificar el área de texto donde los usuarios de la plataforma pueden escribir comentarios sobre los pacientes, para que no tenga longitud mínima, ni restricciones de caracteres.

5.3. Despliegue del código de la plataforma web en el servidor

En primer lugar, se abre el programa *Filezilla* para conectarse con el servidor, se rellena el formulario que aparece en la parte superior de la ventana, como se muestra en la Figura 42, y se pulsa sobre "**Conexión rápida".**

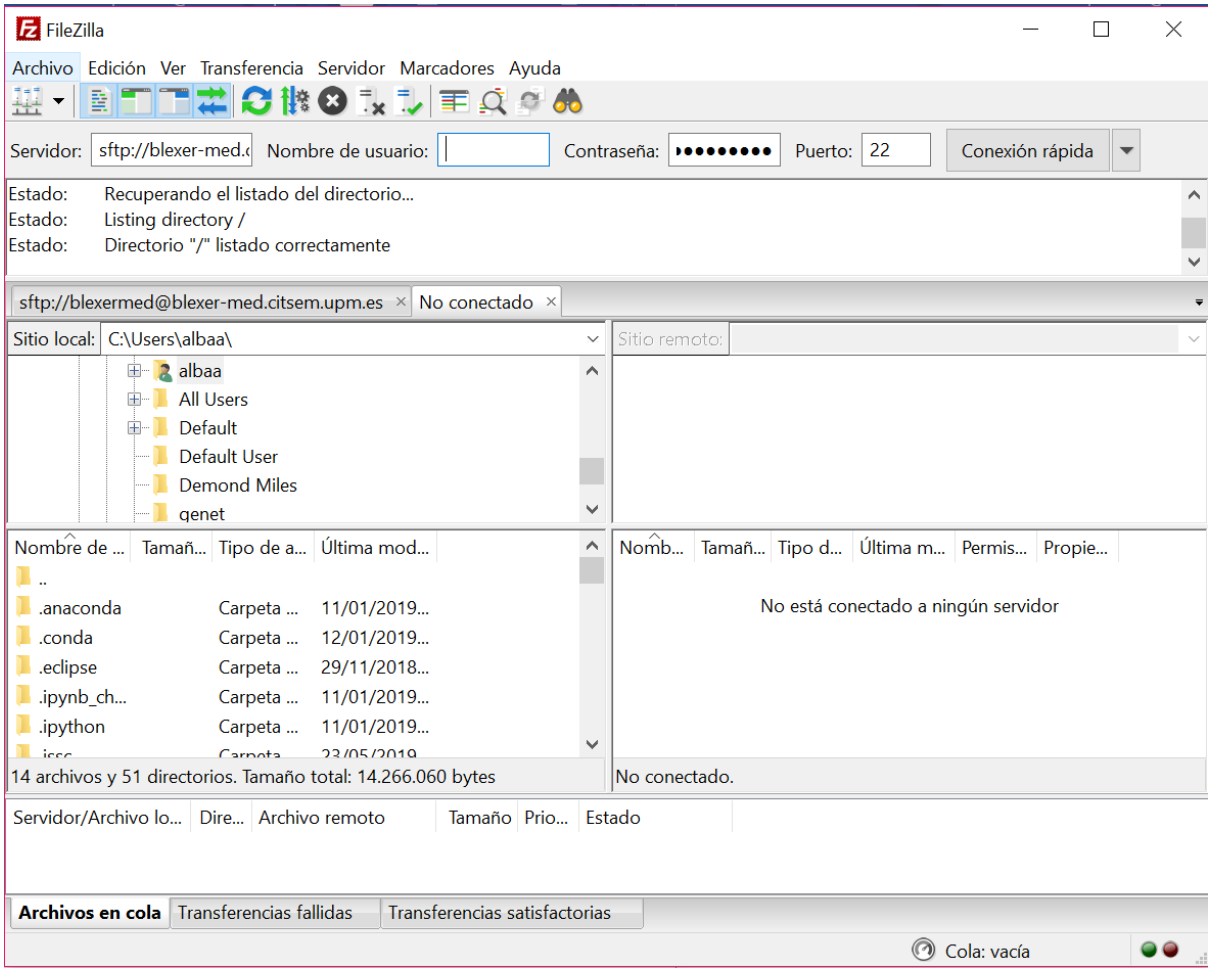

Figura 42 Conexión con Servidor usando Filezilla

Una vez se ha conectado al servidor aparecerán los directorios disponibles, como se observa a la derecha en la Figura 43. En este caso los ficheros de la web se colocan en la carpeta **"tomcat".**

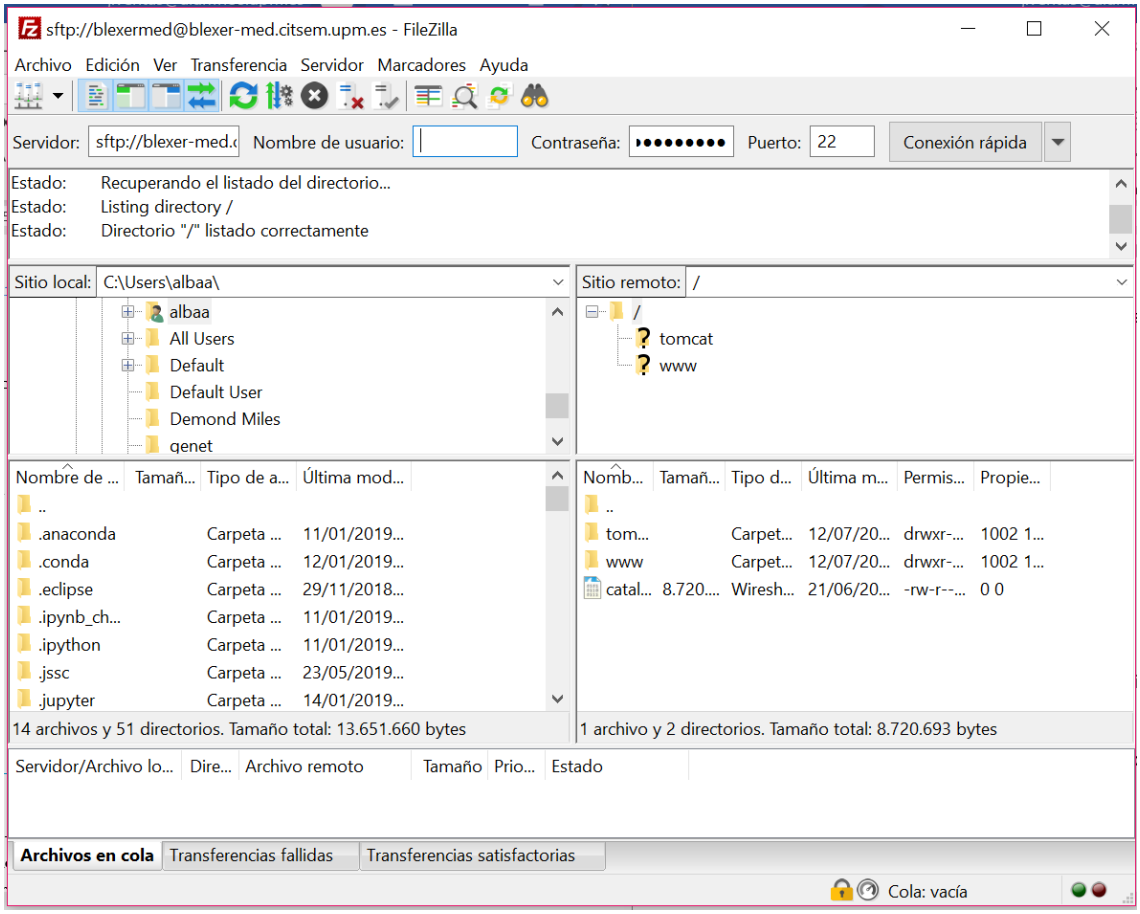

Figura 43 Servidor conectado

Si al añadir los ficheros el programa da algún error, este será registrado en el fichero "**catalina.out**", que se encuentra en la carpeta raíz.

Para obtener los ficheros que son necesarios añadir al servidor, en primer lugar, se abre el proyecto eclipse donde se ha desarrollado el programa de la web. Posteriormente, sobre el nombre del proyecto, se pulsa botón derecho, luego "**Export"** y por último "**WAR File**", como se muestra en la Figura 44.

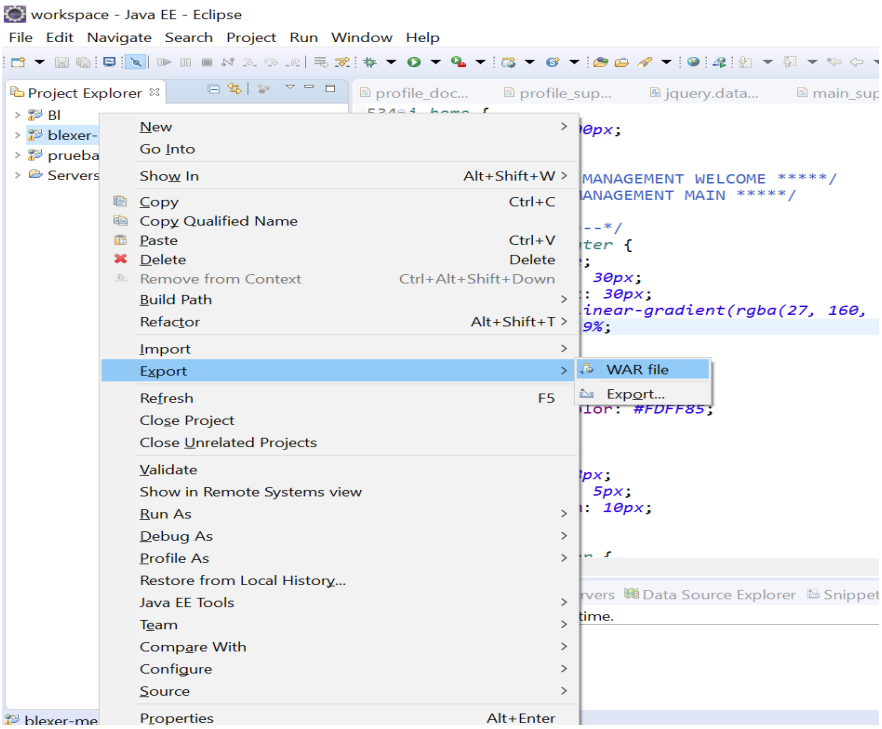

Figura 44 Crear fichero WAR del proyecto en Eclipse

En la pestaña que aparece, Figura 45, se selecciona la carpeta donde se quiere descargar fichero *.war* con los archivos que se suben al servidor y se marca la casilla "**Export source files".** Por último, se pulsa **"Finish".**

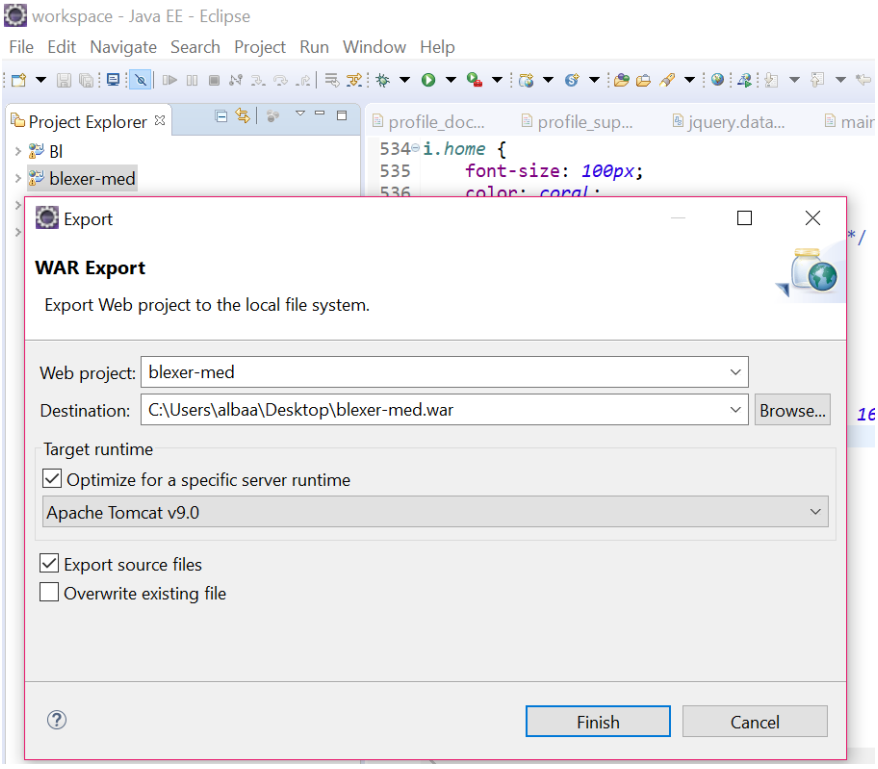

Figura 45 Pestaña WAR Export

El siguiente paso será descomprimir el fichero generado con extensión *.war* en una carpeta con el nombre que se quiere que se muestre en la url, es decir, si la carpeta se llama prueba, la ruta de la web será: http://blexer-med.citsem.upm.es:8080/prueba/. Por último, se arrastra la carpeta creada descomprimida al directorio "**tomcat"** de Filezilla, obteniendo un resultado como en el mostrado en la Figura 46.

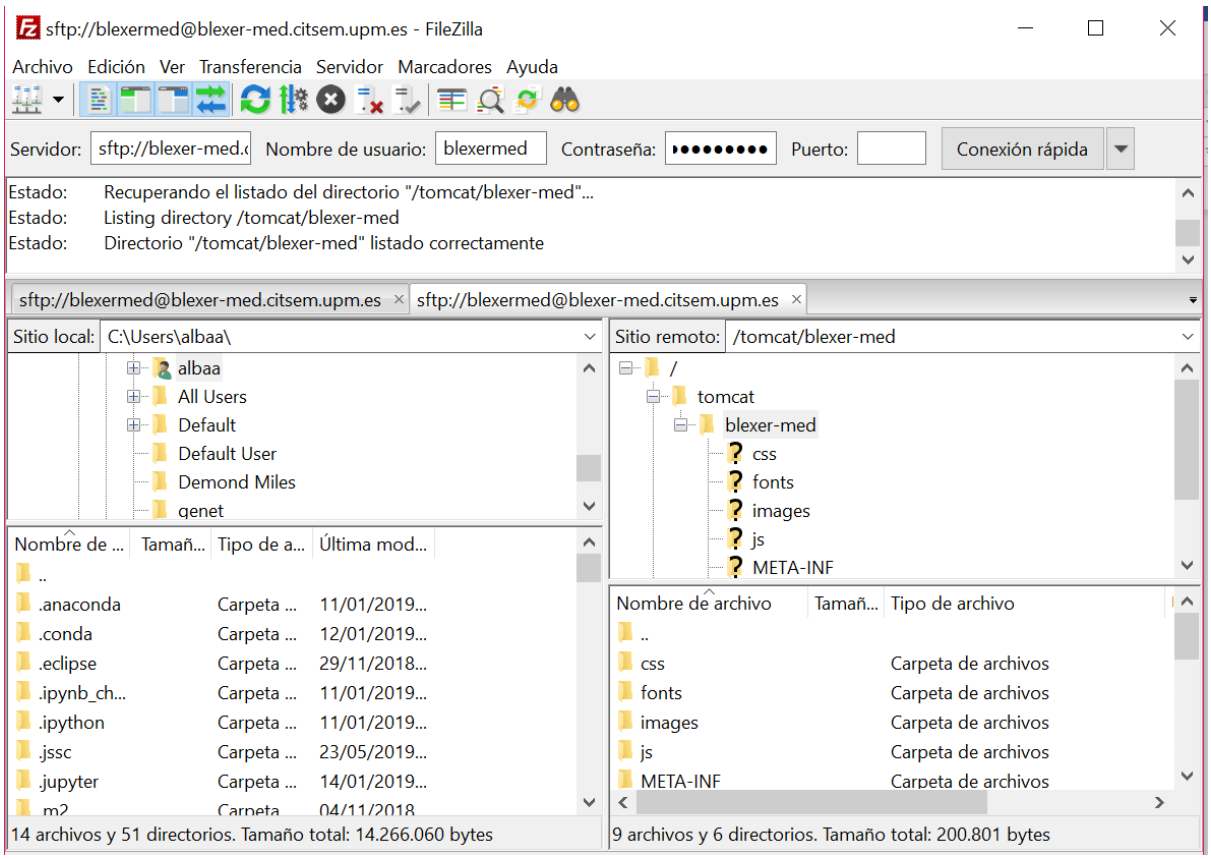

Figura 46 Subida código al Servidor.

6. Conclusiones

El principal objetivo de este Proyecto Fin de Grado es implementar las medidas de seguridad necesarias para solventar las vulnerabilidades y los posibles ataques que pudieran afectar a la plataforma. Además, modificar la web de tal forma de que sea intuitiva y más atractiva para el usuario, así como mejorar las funcionalidades para que tengan una completa usabilidad.

El primer objetivo se ha cumplido, en primer lugar, debido al estudio de todas las leyes y normas que atañen al trabajo, extrayendo de ellas las partes necesarias para hacer el sistema funcional en el ámbito legal, y en segundo lugar gracias a un análisis de las vulnerabilidades del sistema por capas donde se han determinado exactamente las medidas de seguridad necesarias cubriendo todos los posibles flancos de la plataforma. Todo ello ha permitido implementar una serie de medidas de seguridad personalizadas al proyecto de forma que tenga la capacidad para ser operativo y estar protegido de la intrusión de cualquier ataque o usuario no deseado.

En este caso ha sido principalmente la creación de un programa que realiza copias de seguridad de la base de datos, donde se puede personalizar cada cuanto tiempo se desea realizar la copia. Además, se puede seleccionar la fecha de antigüedad de los ficheros que se quieren eliminar para que no se exceda la capacidad de memoria del almacenamiento de archivos. Por otro lado, se ha fortalecido la transmisión de paquetes para que cualquier usuario externo sin autenticación no pueda conocer las claves de acceso a la plataforma ni la información que se transmite. Por último, haciendo uso de la LSSI, se han configurado las contraseñas para que tengan el patrón establecido como seguro, además de reforzar el método de encriptación para que se almacene en la base de datos y se transmita por la web cumpliendo los servicios de seguridad necesarios (confidencialidad, integridad, etc.).

El segundo objetivo se refiere a la mejora del diseño y las funcionalidades de la plataforma web. Se ha modificado la presentación para que sea más profesional e intuitiva para el usuario, así como se han mejorado algunos elementos que no funcionaban correctamente tras realizar las pruebas de la primera versión de la web.

En resumen, en este Proyecto de Fin de Grado, se han implementado las medidas de seguridad necesarias para que este protegida ente cualquier tipo de ataque, la información manejada se procese, almacene y transmita de forma eficiente y segura además de que cumpla con los requisitos estipulados por las leyes a la que hace referencia.

7. Líneas futuras de trabajo

Una vez desarrollado el proyecto se proponen trabajos futuros para continuar con la línea de la investigación en donde está marcado este trabajo fin de grado.

En primer lugar, referente a la seguridad de la plataforma, se recomienda de comprar un certificado de seguridad para implementar HTTPS en vez de HTTP si el proyecto tiene una mayor usabilidad. También será necesario que en el middleware se implementen medidas de seguridad para la transmisión de paquetes hacia la base de datos.

En segundo lugar, referente a las funcionalidades de la plataforma web, se requiere incluir nuevas formas de ajuste de parámetros que se adapten al entorno de videojuegos que se está implementando actualmente. Estos juegos tienen más libertad de juego que el primer prototipo mencionado y se busca una estructura genérica de parámetros que sea flexible para llevar a cabo diferentes configuraciones. Además, interesa mostrar mediante graficas la evolución de los pacientes comprendida en un rango de fechas, y mejorar el fichero Excel de resultados de las pruebas seleccionado por el usuario.

Por otro lado, sería necesario que el paciente pueda modificar su contraseña o recuperarla en caso de olvido.

En la web del rol del médico, sería interesante que el especialista pueda buscar al paciente a través del nombre o apellido, en vez de seleccionarlo de un desplegable. Si en un futuro existe un gran listado de usuarios, el desplegable dificulta la manera de encontrar al paciente requerido.

Además, un buen avance de la plataforma seria que el paciente pudiera comunicarse con el especialista mediante un chat dentro de la plataforma web. Esta funcionalidad permitiría que el paciente pudiera resolver las dudas que le surjan, comunicarle al médico si desea ejercitar otra parte del cuerpo y/o estar al tanto de su progreso en la rehabilitación.

Referencias

[1] M. Eckert, I. Gómez-Martinho, C. Esteban, Y. Peláez, M. Jiménez, M. L. Martín Ruiz, M. Manzano, A. Aglio, V. Osma, J. Meneses y L. Salgado, «The Blexer system – Adaptive full play therapeutic exergames with web-based supervision for people with motor dysfunctionalities,» *EAI Endorsed Transcations on Serius Games*, vol. 5, nº 16, septiembre 2018.

[2] M. Jiménez Ramos, *Plataforma médica para el entorno de videojuego terapéutico "Blexer"*, Madrid: ETSIST, 2017.

[3] *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos*, 2018.

[4] «Ley 34/2002, de 11 de julio de Servicios de la Sociedad de la Información y del Comercio Electrónico».

[5] ONTSI, «ontsi.red.es,» [En línea]. Available: https://www.ontsi.red.es/ontsi/sites/ontsi/files/informe_ciudadanos_esanidad.pdf. [Último acceso: Marzo 2019].

[6] European Union, «Summary minutes 14th Meeting of the eHealth Network 13 November 2018,» Noviembre 2018. [En línea]. Available: https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20181113_mi_en.pdf. [Último acceso: Marzo 2019].

[7] I. G. M. González, Desarrollo e implementación de middleware entre Blender, Kinect y otros dispositivos, Proyecto Fin de Grado, Universidad Politécnica de Madrid, Julio 2016.

[8] REHABILITY, «Web de REHABILITY,» [En línea]. Available: http://www.rehability.me/#activeageing. [Último acceso: Marzo 2019].

[9] BTS Bioengineering, «web de NIRVANA,» [En línea]. Available: https://www.btsbioengineering.com/es/products/nirvana/. [Último acceso: Marzo 2019].

[10] B. López, A. Guzmán, B. Mangas, A. Nagore y A. Reyero, «Experiencia sobre el uso de videojuegos en la rehabilitación neuropsicológica de pacientes con daño cerebral adquirido,» Madrid, 2012.

[11] V. González, «Jugando con ADVANT: ADVANTed Therapeutics. Plataforma para la rehabilitación física y el entretenimiento cognitivo,» Madrid, 2012.

[12] ISO27000, «Sistema de Gestión de la Seguridad de la Información (SGSI),» [En línea]. Available: http://www.iso27000.es/download/doc_sgsi_all.pdf. [Último acceso: Febrero 2019].

[13] C. N. Murphy y J. Yates, The International Organization for Standarization (ISO): Global governance through voluntary consensus, New York: Routledge, 2009.

[14] F. J. Valencia Duque y M. Orozco Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000,» *Revista Ibérica de Sistemas e Tecnologias de Informaçao,* nº 22, pp. 73-88, 2017.

[15] M. Recio Gayo, «Los nuevos y los renovados Derechos en Protección de Datos en el RGPD, así como sus limitaciones.,» *Actualidad civil,* nº 5, p. 2, 2018.

[16] C. García Ortega, V. Cózar Murillo y J. Almenara Barrios, «La autonomía del paciente y los derechos en materia de información y documentación clínica en el contexto de la Ley 41/2002,» *Revista española de salud pública,* nº 78.4, pp. 469-479, 2004.

[17] M. L. Martín Ruiz, *Apuntes de Seguridad en Redes y Servicios.*

[18] Á. Gómez Vieites, «Tipos de Ataques e Intrusos en las Redes Informáticas,» [En línea]. Available: https://www.edisa.com/wp-content/uploads/2014/08/Ponencia_-_Tipos_de_ataques_y_de_intrusos_en_las_redes_informaticas.pdf. [Último acceso: Marzo 2019].

[19] Comité consultivo internacional telegráfico y telefónico, «Redes de comunicaciones de datos: Interconexion de sistemas abiertos (ISA), seguridad, estructura y aplicaciones.,» Unión internacional de telecomunicaciones, Ginebra, 1991.

[20] Centro Criptológico Nacional, «Esquema nacional de seguridad. Valoración de los sistemas.,» Ministerio de Defensa, Madrid, 2011.

[21] J. S. Rivera, C. Augusto Mejía y J. Ramírez, «Vulnerabilities, types of attack and ways to mitigate it on OSI layer model applied to the data networks of organizations.,» 2012.

[22] INTECO-CERT, «Actualizaciones de Software,» Mayo 2011. [En línea]. Available: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_actualizaciones_software.pdf. [Último acceso: Abril 2019].

[23] S. González, «Manual Básico de Cron,» *Durán,* vol. 13, nº 13, p. 2014, 13 05 2012.

[24] Y. Miranda, «Algoritmos HASH y vulnerabilidades a ataques,» 2009.

[25] M. S. C. Diez, «El poder del color,» León, 2012.

[26] W3CSS, «W3Schools,» [En línea]. Available: https://www.w3schools.com/. [Último acceso: 23 Mayo 2019].

[27] COIT, «Mapa del titulado de Ingeniería de Telecomunicación,» 2017. [En línea]. Available: https://www.coit.es/informes/informe-socioprofesional-coitaeit-mapa-del-titulado-de-ingenieria-de-telecomunicacion/mapa. [Último acceso: Junio 2019].

Anexos

Anexo 1. Manual de usuario para crear una copia de seguridad de la base de datos de forma manual

El primer paso es abrir la consola de comandos y acceder al directorio donde se encuentra almacenado el servidor de la base de datos de MySQL, lo cual se muestra en la Figura 47.

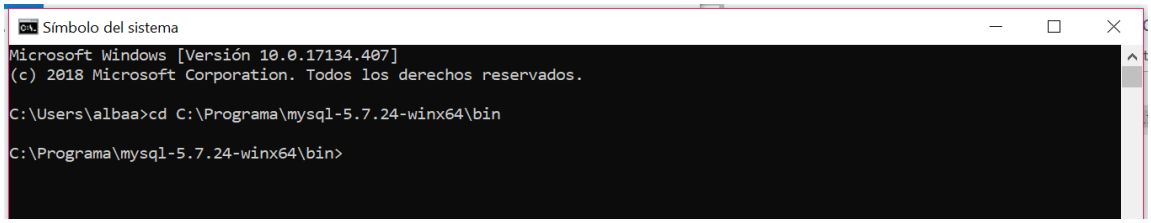

Figura 47. Localización del servidor de la base de datos

Se comprueba que la base de datos se encuentra en el servidor de MySQL y que contiene la información necesaria. Para ello, primero se entra en el servidor ejecutando el comando resaltado en azul en la Figura 48.

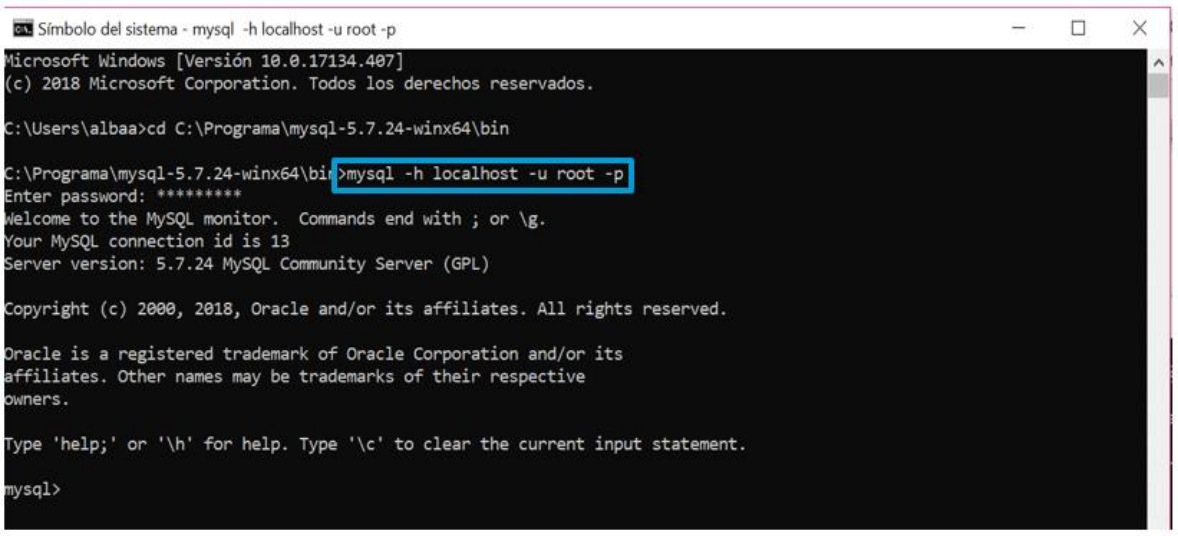

Figura 48. Comando para entrar en el servidor

Posteriormente, se comprueba que la base de datos se encuentra en el registro y que contiene los datos pertinentes. Este paso se ha realizado según se muestra en la Figura 49 ejecutando el comando resaltado en azul.

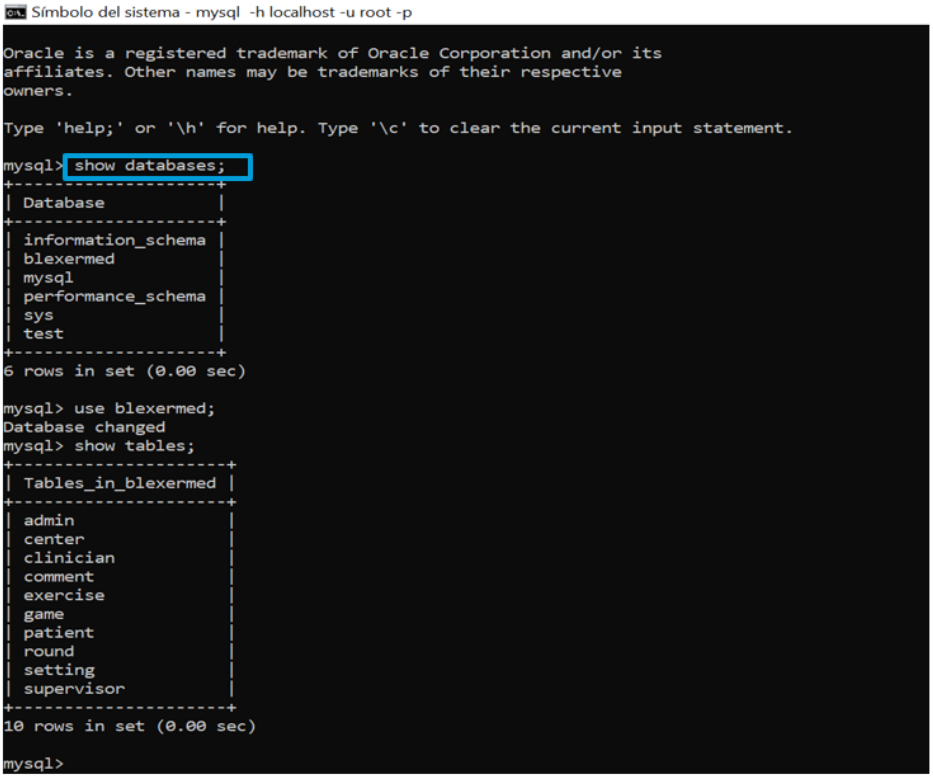

Figura 49. Visualización de la base de datos creada y sus datos correspondientes

Para crear una copia de seguridad de la base de datos, se utiliza un comando que proporciona MySQL, el cual permite crear, en la carpeta que se establezca, un archivo que contendrá la copia de seguridad de la base de datos que se le indique. Este archivo tiene extensión *.sql* y su nombre contendrá la fecha en la que se realizó la copia para tener un control de los ficheros. El comando sería el que se muestra en la Figura 50.

```
mysqldump -h [nuestro.servidor.com_o_IP] -u [usuario] -p[password] [base_de_datos] > ruta/archivo_backup.sql
```

Figura 50. Comando creación copia de seguridad

Se ejecuta el comando proporcionado por MySQL como se observa en la Figura 51. Los parámetros utilizados son:

- Servidor: localhost
- Usuario: root
- Base de datos: blexermed

```
C:\Programa\mysql-5.7.24-winx64\bin>mysqldump -h localhost -u root -p blexermed > C:\Users\albaa\Documents\PFG\Software\buckup\copiaSeguridad.sql
Enter password: *********

C:\Programa\mysql-5.7.24-winx64\bin>
```

Figura 51. Creación copia de seguridad

Como se ve en la Figura 52, se ha creado la copia de seguridad de la base de datos correctamente en la carpeta indicada.

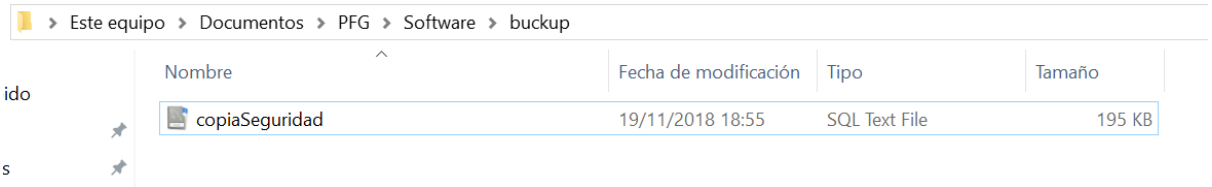

Figura 52 Comprobación de la creación de la copia de seguridad de la base de datos

Una vez obtenida la copia de seguridad, será posible importarla en cualquier momento, haciendo uso del comando que se muestra en la Figura 53

```
C:\Programa\mysql-5.7.24-winx64\bin>mysql -h localhost -u root -p blexermed < C:\Users\albaa\Documents\PFG\Programas\localhost.sql
Enter password: *********
```

Figura 53 Comando para restaurar una copia de seguridad

Anexo 2. Manual de usuario para crear una copia de seguridad de la base de datos de forma automática

En primer lugar, se utiliza una herramienta que proporciona MySQL llamada *mysql_config_editor*, la cual cifra las credenciales del usuario y la contraseña con un alias de host para utilizarlos en vez de las credenciales. Este alias se almacena en un archivo de configuración en el directorio de inicio.

Así, el primer paso será crearse un alias host con las credenciales del usuario y la contraseña como se muestra en la Figura 54.

```
C:\Programa\mysql-5.7.24-winx64\bin>mysql_config_editor set --login-path=myhostalias --user=root --password
Enter password: *********
```

Figura 54. Comando para la creación de usuario y contraseña de forma oculta

Es importante recordar que esta acción sólo se deberá realizar una vez en la consola de comandos. En la Figura 55, se modificará el comando, el cual contiene las credenciales en claro por el alias.

```
mysqldump -u root -p --password=miContraseña blexermed > C:\Users\albaa\Documents\PFG\Software\backup\prueba_%fecha%.sql
```

```
mysqldump --login-path=myhostalias blexermed > C:\Users\albaa\Documents\PFG\Software\backup\prueba_%fecha%.sql
```

Figura 55. Modificación de usuario y contraseña por el alias creado

Una vez realizado esto, se programa un archivo con extensión *.bat* que se encargará de ejecutar la copia de seguridad. Será el que se muestra en la Figura 56.

backup.bat

```
::Creamos la fecha actual
echo off
set fecha=%date:~0,2%-%date:~3,2%-%date:~6,4%
set fecha=%fecha:/=%


cd C:\Programa\mysql-5.7.24-winx64\bin
mysqldump --login-path=myhostalias blexermed > C:\Users\albaa\Documents\PFG\Software\backup\prueba_%fecha%.sql
```

Figura 56. Archivo ejecutable que crea la copia de seguridad de la base de datos

Una vez ejecutado se obtiene lo que se puede ver en la Figura 57.

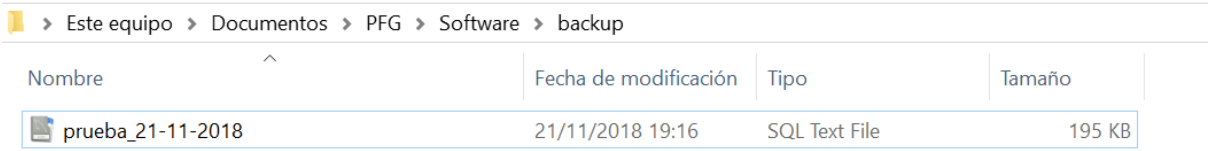

Figura 57. Comprobación de la ejecución del ejecutable

Anexo 3. Manual de usuario para la configuración de la copia de seguridad de la base de datos

Para modificar el directorio donde se almacenan las copias de seguridad de la base de datos, será necesario, en primer lugar, abrir el ejecutable con un programa de edición de texto como pueden ser *Sublime text* o *Wordpad*.

Posteriormente, como se muestra en la Figura 58, habrá que modificar la última línea, después del símbolo ">" y escribir la ruta del nuevo directorio donde se guardarán los ficheros. A continuación, se escribirá el nombre del fichero, en este caso "prueba" seguido de "_%fecha%.sql", donde se mostrará seguido del nombre del fichero la fecha en la que se ha realizado la copia de seguridad y la extensión del fichero. Es muy importante que después del nombre del fichero se ponga la extensión *.sql*.

```
::Creamos la fecha actual
echo off
set fecha=%date:~0,2%-%date:~3,2%-%date:~6,4%
set fecha=%fecha:/=%


cd C:\Programa\mysql-5.7.24-winx64\bin
mysqldump --login-path=myhostalias blexermed > C:\Users\albaa\Documents\PFG\Software\backup\prueba_%fecha%.sql
```

Figura 58 Código del ejecutable para realizar la copia de seguridad de la base de datos.

Anexo 4. Manual de usuario para la configuración de eliminación de copias de seguridad antiguas

En el ejecutable donde está desarrollado cuando se borra una copia de seguridad, está configurado de tal forma que se especifica el número total de días que una copia de seguridad debe ser almacenada.

```
:: Elimina archivos de mas de 60 dias de antiguedad de la carpeta especificada
@echo off
Forfiles /p "C:\Users\albaa\Documents\PFG\Software\backup\" /s /m *.* -d -60 /c "cmd /c del /q @path"
```

Figura 59 Ejecutable para el borrado de copias de seguridad de la base de datos antiguas

En este caso, se ha configurado para 60 días. Si se quisiera ampliar o reducir el número de días, habría que modificar el texto que se visualiza en morado y escribir la cantidad (en días) que se desee.

Anexo 5. Manual de usuario para encriptar datos de la base de datos con la herramienta MySQL

MySQL está previsto de un algoritmo llamado AES que permite cifrar la información que se encuentra en la base de datos. En primer lugar, se va a comprobar la configuración por defecto que tiene el algoritmo; para ello es necesario consultar la variable **block_encryption_mode,** como se ve en la Figura 60.

```
mysql> SELECT @@session.block_encryption_mode;
+---------------------------------+
| @@session.block_encryption_mode |
+---------------------------------+
| aes-128-ecb                     |
+---------------------------------+
1 row in set (0.00 sec)
```

Figura 60 Consulta de la configuración por defecto del algoritmo AES

Para comprobar lo que ocurre en el caso de que se cifre un texto con una contraseña se utilizará el comando **AES_ENCRYPT** como se muestra en la Figura 61, en el cual la función recibe dos parámetros: el primero contiene el texto a cifrar y el segundo la contraseña con la que se quiere cifrar.

```
mysql> SELECT HEX(AES_ENCRYPT('Informacion', 'passwordSegura'));
+-----------------------------------------------------+
| HEX(AES_ENCRYPT('Informacion', 'passwordSegura')) |
+-----------------------------------------------------+
| 4062734278A314418B6AC1900551F2D7                    |
+-----------------------------------------------------+
1 row in set (0.00 sec)
```

Figura 61 Uso del comando AES_ENCRYPT

Como se observa en la Figura 62, el algoritmo AES tiene configurado por defecto una clave de tamaño de 128 bits, para que el cifrado sea completamente seguro se va a modificar la configuración para que sea de 256 bits como se indicaba anteriormente.

```
mysql> SET @@session.block_encryption_mode = 'aes-256-ecb';
Query OK, 0 rows affected (0.00 sec)

mysql> SELECT @@session.block_encryption_mode;
+---------------------------------+
| @@session.block_encryption_mode |
+---------------------------------+
| aes-256-ecb                     |
+---------------------------------+
1 row in set (0.00 sec)
```

Figura 62 Modificación tamaño de clave a 256 bits

Como se puede apreciar en la Figura 63 se ha modificado la configuración a 256 bits, por tanto, si volvemos a utilizar la función anterior, se observará que devuelve un valor diferente y más robusto

```
mysql> SELECT HEX(AES_ENCRYPT('Informacion', 'passwordSegura'));
+-------------------------------------------------+
| HEX(AES_ENCRYPT('Informacion', 'passwordSegura')) |
+-------------------------------------------------+
| B18464A9F19465BFA2E59F2476E7C095                |
+-------------------------------------------------+
1 row in set (0.00 sec)
```

Figura 63 Comprobación de la clave de 256 bits

Para comprobar que los datos fueron cifrados correctamente se hará uso de las funciones inversas **AES_DESCRYPT y UNHEX**. El resultado de esta acción se muestra en la Figura 64.

- **AES DESCRYPT**: recibe el dato devuelto por la función anterior y la password
- **UNHEX**: recibe como único parámetro el valor en hexadecimal.

```
mysql> SELECT AES_DECRYPT(UNHEX('B18464A9F19465BFA2E59F2476E7C095'), 'passwordSegura');
+-------------------------------------------------------------------------+
| AES_DECRYPT(UNHEX('B18464A9F19465BFA2E59F2476E7C095'), 'passwordSegura') |
+-------------------------------------------------------------------------+
| Informacion                                                             |
+-------------------------------------------------------------------------+
1 row in set (0.00 sec)
```

Figura 64 Descifrado de los datos

Anexo 6. Presupuesto

Finalmente, en esta sección se estima el coste necesario para llevar a cabo este Proyecto Fin de Grado.

Considerando un salario bruto anual para un ingeniero de telecomunicaciones junior, tomando [27] como referencia, de 23.553€. Suponiendo que en un año hay 251 días hábiles, con 8 horas de trabajo al día, por tanto, si se han realizado 432 horas de trabajo:

$$\frac{432}{251 * 8} 23553 = 5067{,}18\ €$$

Como se muestra en la Tabla 4, los costes del proyecto son los costes de la mano de obra, el equipo, en este caso un portátil, material de oficina y otros costes (luz, electricidad, etc). Como los costes del material de oficina y otros costes son difíciles de determinar se ha realizado una estimación aproximada.

Tabla 4 Costes del proyecto

Concepto	**Coste (€)**
Equipo:	900
Materiales de oficina	150
Otros costes (luz, electricidad, etc)	450
Costes mano de obra	5067,18
Costes Totales	6567,18