UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ESCOLA POLITECNICA SUPERIOR DE GANDIA

Grado en Ing. Sist. de Telecom., Sonido e Imagen

"Aplicación en la nube para la gestión integral de exploraciones neuropsicológicas"

TRABAJO FINAL DE GRADO

Autor/a:
Marta Botella Campos

Tutor/a:

Felipe Vico Bondía

GANDIA, 2019

Resumen

El objetivo de este proyecto es diseñar un programa informatizado de exploración neuropsicológica que sustituya a las valoraciones en papel y optimice los tiempos de exploración, corrección y elaboración de informes.

Esta aplicación informática ha sido diseñada con la colaboración de 7 profesionales médicos del Hospital Dr. Peset y será implantado por primera vez en este centro en diciembre de 2019.

El objetivo último es tener una herramienta informática unificada que facilite la interacción entre los diferentes profesionales de la neuropsicología y crear una base de datos neuropsicológicos a nivel nacional, para facilitar el diagnóstico precoz y favorecer otras vías de investigación.

Palabras clave

Aplicación, Nube, Neuropsicología, Java, MySQL.

Abstract

The aim of this project is to design a computerized program of neuropsychological explorations to replace paper assessments and optimize exploration, correction and reporting times.

This computer application has been designed with the collaboration of 7 medical professionals from Dr. Peset Hospital and will be set up for the first time in this center in December 2019.

The ultimate goal is to create a unified computer tool that facilitates the interaction between the different neuropsychological professionals, and create a neuropsychological database at a national level, to facilitate early diagnosis and favor other research paths.

Keywords

Application, Cloud, Neuropsychology, Java, MySQL.

Contenido

Tabla de Figuras

1. Introducción

1.1. Motivación

El envejecimiento es el conjunto de cambios bioquímicos, morfológicos, psicológicos, funcionales y sociales que aparecen en los individuos como efecto de la acción del tiempo[1].

Podemos distinguir distintos tipos de envejecimiento[1]:

- **Envejecimiento funcional:** los cambios sufridos por los individuos permiten una buena adaptación al medio tanto física como psíquicamente.
- **Envejecimiento óptimo:** ocurre en las mejores condiciones posibles e implica pocas o ninguna pérdida, y una baja probabilidad de sufrir enfermedades.
- **Envejecimiento patológico:** los cambios se producen como consecuencia de una enfermedad o malos hábitos, dificultando o impidiendo la acción al medio.

Dentro del conjunto de enfermedades patológicas que conllevan un deterioro de las facultades físicas e intelectuales de un individuo, encontramos las demencias como principal causa de dependencia en personas mayores de 65 años.

La Organización Mundial de la Salud (OMS) define la demencia como un síndrome que provoca una degeneración cognitiva progresiva que conlleva un deterioro de la memoria, el intelecto, el comportamiento y la capacidad para realizar actividades cotidianas. En la actualidad, este síndrome afecta a unos 50 millones de personas a nivel mundial[3]. Sin embargo, el marcado crecimiento de la población mayor de 65 años como consecuencia del aumento de la esperanza y calidad de vida[1] indica que la tasa de dependencia de la población mayor de 64 años alcanzará el 60 % en los próximos 30 años[2] (ver Figura 1).

Aunque la demencia es causada por diversas enfermedades y lesiones que afectan al cerebro[3], se calcula que el 60-70% de los casos se deben a la enfermedad de Alzheimer, seguida por los accidentes cerebrovasculares, la demencia por cuerpos Lewy (causada por la acumulación de proteínas en las células nerviosas) y la demencia frontotemporal (debido a la degeneración del lóbulo frontal). Si bien no existe ningún tratamiento para curar la demencia ni revertir su evolución, un diagnóstico precoz puede contribuir a mejorar la salud física, la cognición, la actividad diaria y el bienestar de los afectados, además de proporcionar apoyo e información a sus cuidadores y familiares[3].

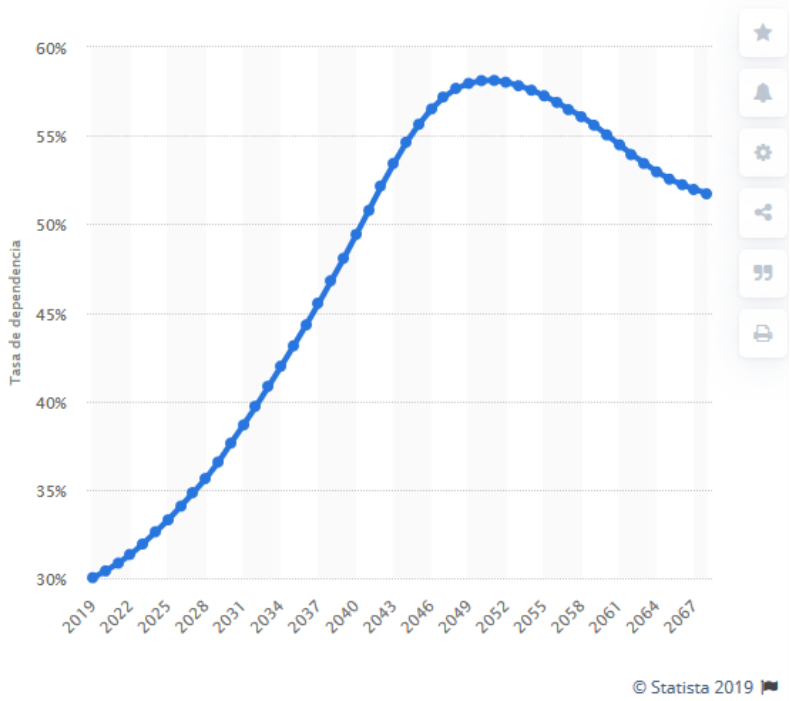


Figura 1: Tasa de dependencia de la población mayor de 64 años en España de 2019-2068[2].

En el año 2015, se estimó que el impacto económico de este síndrome equivalía al 1'1% del producto interior bruto (PIB) mundial. Debido a las tasas de crecimiento esperadas para los próximos 30 años, la OMS ha establecido la evaluación de la demencia como prioritaria, de modo que puedan ponerse en marcha iniciativas que cubran las necesidades de estos enfermos y contribuyan a reducir el riesgo de deterioro cognitivo de los mismos antes del año 2025[3].

1.2. Digitalización en Sanidad Pública

La Fundación Tecnología y Salud define la *salud digital* como el conjunto de Tecnologías de la Información y la Comunicación (TIC) que se emplean en sanidad para prevenir, diagnosticar, tratar y gestionar la información en el entorno sanitario, para mejorar así su eficiencia y ahorrar costes[4]. Aunque el Sistema Nacional de Salud se caracteriza por su alta calidad, lo cierto es que, en muchas Comunidades Autónomas, se sigue llevando a cabo un registro en soporte papel que acarrea dificultades tanto de almacenamiento como de gestión y acceso a los datos. Por este motivo, el Ministerio de Sanidad ha destacado la importancia de potenciar y controlar los datos sanitarios de las historias clínicas y las recetas electrónicas de forma digital[5]. Además, en febrero de 2019, el Comité Europeo de la Regiones dictaminó que los estados miembros de la Unión Europea deben cooperar para adaptar la transformación digital de la sanidad, mejorando así su eficiencia y favoreciendo la investigación[8].

En la actualidad, no existe una red estatal que permita el acceso a los historiales clínicos de los ciudadanos, sino que cada Comunidad Autónoma gestiona los datos de los pacientes tratados de forma independiente. En la Comunidad Valenciana, la aplicación informática implantada por la Agencia Valenciana de Salud (AVS) se denomina *Orión Clinic*, y fue implantado por primera vez en el Hospital Dr. Peset en el año 2009[6]. Este programa es un sistema generalista en el que participaron más de 200 profesionales de la salud, con el propósito de construir un sistema de información clínico-asistencial para los centros hospitalarios que permitiese mejorar la atención al paciente y ayudase en la actividad clínica, incrementando así la eficiencia del proceso asistencial. Aunque *Orión Clinic* cubre todas las áreas de atención desde la Admisión hasta la hospitalización domiciliaria (pasando por las Consultas externas, las Urgencias y los Servicios de Prevención y Seguridad)[7], también presenta carencias específicas de los distintos sectores de la actividad sanitaria.

En el caso que nos atañe, los profesionales médicos especialistas en Neuropsicología deben estudiar los efectos que las lesiones o un funcionamiento anómalo del sistema nervioso central tienen sobre los procesos cognitivos, psicológicos, funcionales y emocionales. Para ello, a menudo se precisa el uso de marcadores que permitan detectar los cambios patológicos de la enfermedad de forma no invasiva. En el caso de la cognición, este marcador tiene la ventaja de ser no invasivo y no provocar efectos secundarios. También resulta ser un marcador muy económico, ya que el único coste es el tiempo de valoración neuropsicológica (90 minutos de exploración neuropsicológica con el paciente) y el tiempo de corrección de los test (30 minutos de corrección y elaboración del informe)[9].

Sin embargo, marcadores de este tipo están siendo infrautilizados debido al coste sanitario que supone, puesto que el tiempo que requiere un profesional especializado en la valoración de cada paciente es comparativamente mayor al del estudio de otros marcadores. Actualmente, el Hospital Dr. Peset no dispone de un contrato hospitalario para realizar valoraciones neuropsicológicas en la práctica clínica habitual; sino que se realizan mediante un convenio de colaboración con la Universidad de Valencia (UV) [9].

1.3. Polisabio: Proyecto Geinen

Polisabio es un programa de colaboración entre la Universidad Politécnica de Valencia (UPV) y la Fundación para el Fomento de la Investigación Sanitaria y Biomédica de la Comunidad Valenciana (Fisabio) cuyo objetivo es crear participaciones activas y

colaboraciones entre ambas instituciones, que den lugar a proyectos de investigación científico-técnicos.

El objetivo de este proyecto es diseñar un programa informatizado de exploración neuropsicológica que sustituya a las valoraciones en papel y optimice los tiempos de exploración, corrección y elaboración de informes, que será implantado por primera vez en el Hospital Dr. Peset en diciembre de 2019.

Esta aplicación informática ha sido diseñada con la colaboración de 7 profesionales médicos de este centro:

- **Antonio del Olmo:** Jefe de Sección de Neurología.
- **Helena Vico Bondía:** Psicóloga y Neuróloga investigadora.
- **Pilar Lacalle Alba:** Profesora asociada de la UV y Neuropsicóloga.
- **Sara Villalba Agustín:** Profesora de la Universidad Católica de Valencia (UCV) y Neuropsicóloga.
- **Alba Montesdeoca Rozalén:** Coordinadora de ensayos clínicos y Neuropsicóloga.
- **Marcos Galán Morán:** Neuropsicólogo.
- **Alba Romero Peiró:** Neuropsicóloga.

Con la implantación de este programa, se espera reducir la duración de las sesiones de exploración neuropsicológica, obtener una corrección inmediata de los test realizados y proporcionar una elaboración parcial del informe, el cual quedará pendiente de interpretación de los resultados y la elaboración del diagnóstico neuropsicológico. Estas medidas disminuirán el tiempo de trabajo del neuropsicólogo y aumentarán la disponibilidad para valorar más pacientes: teniendo en cuenta que el profesional que realiza exploraciones neuropsicológicas tiene capacidad para valorar 3 pacientes al día y que se prevé un ahorro del 33% de dicho tiempo, la instauración de esta aplicación ampliará la valoración de 3 a 4 pacientes al día y en el Hospital de 9 a 12 pacientes por semana, por lo que los beneficios anuales serían de 2094 € por neurólogo o psicólogo[9]. Además, se generará una base de datos que facilitará el análisis y estudio de marcadores neuropsicológicos de riesgo de la enfermedad de Alzheimer y otras enfermedades neurodegenerativas.

En España se estima un coste medio anual por paciente y año de 14.956 € en los pacientes que están en fases leves, 25.562 € en que están con demencia moderada y 41.669 € en los que están en fases de demencia avanzada[9]. Por tanto, la posibilidad de realizar exploraciones

neuropsicológicas a un mayor número de pacientes contribuirá a realizar más diagnósticos en fases precoces, que permitan el inicio temprano de los tratamientos establecidos así como la posibilidad de participar en ensayos clínicos con fármacos potencialmente modificadores de la enfermedad, con la consecuente reducción de costes sociosanitarios. Asimismo, este proyecto permitirá mejorar la calidad asistencial, dado que se podrá realizar exploración neuropsicológica a un 33% más de pacientes, lo que contribuirá a realizar más diagnósticos precoces, y disminuirá la ansiedad provocada por la incertidumbre diagnóstica y permitirá al paciente organizar sus asuntos y manifestar sus voluntades anticipadas.

Plan de trabajo y cronograma

El plan de trabajo establecido para este proyecto es el siguiente[9] (ver Figura 2):

1. Desarrollo de las especificaciones concretas y funcionalidades que debe contener el software a desarrollar (1 semana).
2. Repaso por parte del personal de apoyo de las partes del lenguaje de programación que serán necesarias para el desarrollo del software. Programación avanzada orientada a objetos, interfaces gráficas y bases de datos (2 semanas).
3. Desarrollo del software preliminar. Dicho software debe tener todas las funcionalidades requeridas salvo el hecho de que funcionará en una sola máquina y sin comunicación con otras máquinas. Método de sprint en 15 días: cada 15 días se producirá una reunión entre los investigadores del grupo y el personal de apoyo donde se evaluará si las diferentes partes del software están siendo desarrolladas correctamente y como se especificó y pulir detalles en caso de ser necesario. Esta fase consta de 2 subfases (10 semanas en total, 5 semanas cada parte):
    - Desarrollo de la estructura de datos necesaria para soportar las diferentes funcionalidades.
    - Desarrollo del interfaz gráfico de usuario necesario. En esta fase preliminar del software, la información de los pacientes se almacenará en un sistema de archivos de forma local en la máquina donde se esté ejecutando el programa.
4. Puesta a punto mediante la experimentación práctica del software usado en consulta con pacientes reales. En dicha fase los test neuropsicológicos se pasarán empleando el software y tomando notas de manera manual como hasta ahora (2 semanas).

5. Desarrollo de la versión final del software que funcione con una base de datos unificada para todas las máquinas en las que se esté ejecutando. En esta versión del software, la información quedará almacenada en una base de datos en un servidor del hospital (6 semanas).
6. Desarrollo de medidas de seguridad de acceso a la base de datos para personal autorizado empleando el mismo sistema de autenticación que al arrancar Windows (1 semana).
7. Puesta a punto mediante la experimentación práctica del software usado en consulta con pacientes reales. En esta parte se comprobará el funcionamiento y correcta sincronización del software cuando es empleado por diferentes usuarios simultáneamente (2 semanas).

Entregables

A los 15 días del inicio del proyecto, se entregó un dosier con todas las especificaciones del software. Tras finalizar la semana 15 se elaboró una versión preliminar del manual para la utilización del software realizado y tras finalizar la semana 24 se entregó un informe completo donde se reportaron todos los resultados obtenidos así como las incidencias acontecidas.

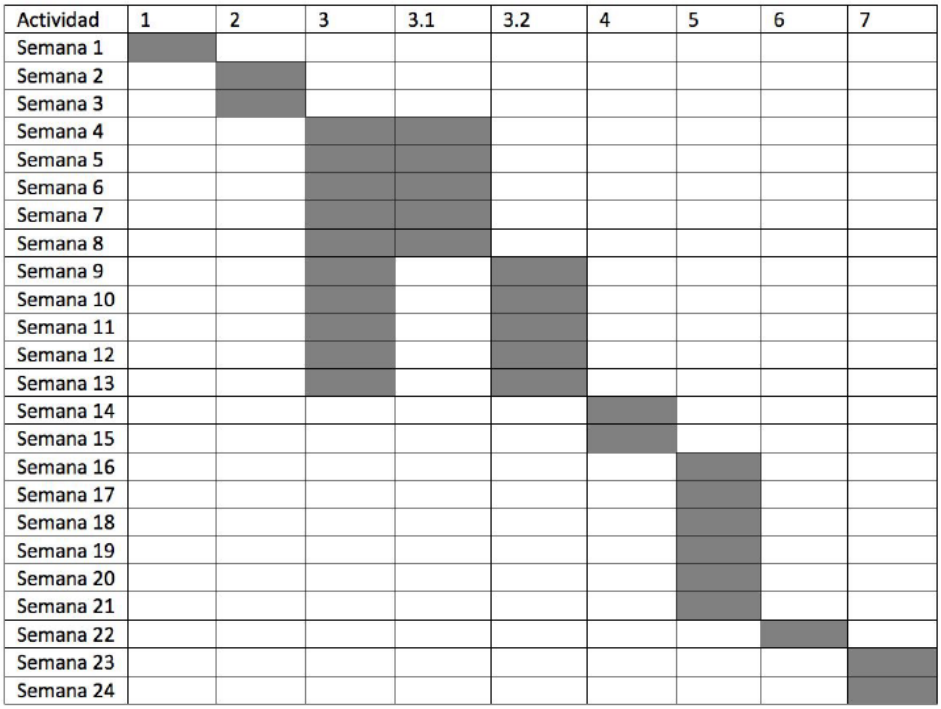


Figura 2: Cronograma del proyecto.

2. Sistema informático integrado para la exploración neuropsicológica

Como dijimos anteriormente, el objetivo de este proyecto es diseñar un programa que sustituya las valoraciones en formato papel y optimice los tiempos de exploración, corrección y elaboración de informes; además de crear una base de datos de marcadores neuropsicológicos de riesgo de las enfermedades neurodegenerativas, para extraer estadísticas de población y facilitar un diagnóstico precoz.

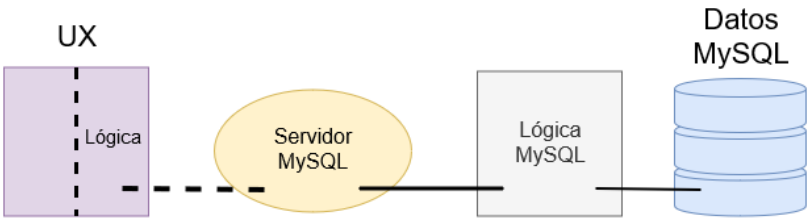


Figura 3: Diseño lógico del Proyecto Geinen.

Para ello, creamos un servidor MySQL que contendrá la base de datos y cuya lógica de acceso viene determinada por el sistema de gestión de base de datos de Oracle Corporation (ver Figura 3). La interacción con el servidor se lleva a cabo a través de la interfaz gráfica, la cual a su vez hace uso de la clase `Logica.java` para insertar y extraer datos. Por su parte, la lógica de funcionamiento del programa hace uso de la clase `ConexionMySQL.java` para conectarse al servidor y devolver la información, o los códigos de respuesta asociados a las acciones realizadas. De esta forma, conseguimos tunelizar la lógica del sistema de gestión MySQL para devolverla al usuario con un formato adecuado para su correcta interpretación: información solicitada o errores de conexión, por ejemplo.

En los subsiguientes apartados repasaremos los distintos elementos que componen esta aplicación, los cuales son:

- Tecnologías utilizadas
- Servidor
- Bases de datos
- Seguridad y encriptación
- Arquitectura de software
- Interfaz de usuario

2.1. Tecnologías utilizadas

En el libro *Piensa en Java*, Bruce Eckel asevera que: "*La programación está relacionada con gestionar la complejidad: la complejidad del problema que se quiere solucionar, que yace sobre la complejidad de la máquina en que se soluciona*"[10].

Con esta idea en mente, decidimos basar la programación de esta aplicación en el lenguaje de programación Java. Al ser un lenguaje de programación orientado a objeto se simplifica enormemente la tarea pero, además, al tratarse de una aplicación cliente-servidor Java nos provee de una serie de mecanismos para implementar la conexión desde el lado del cliente y manipular también la conexión desde el lado del servidor. La gestión de la base de datos se llevó a cabo con MySQL puesto que, además de ser una solución de código abierto, nos proporciona las herramientas necesarias para crear un servidor en el que almacenar nuestra base de datos. Como es costumbre, las peticiones de acceso a la base de datos se hicieron mediante comandos SQL. Los scripts para generar los ejecutables para instalar la aplicación fueron generados con *Inno Setup Compiler*, mientras que la creación de los ejecutables se llevó a cabo con el programa *Launch4j* (ver ANEXO I).

En los subsiguientes apartados veremos los aspectos técnicos y de seguridad del servidor, la base de datos y la aplicación.

2.2. Servidor MySQL

Para poder acceder a la base de datos, necesitaremos un servidor que la contenga. En este proyecto elegimos *MySQL Community Server* por su facilidad de instalación y configuración en el entorno Windows, que es el sistema operativo más común utilizado en Sanidad Pública. Aunque en esta sección mostraremos los resultados en este entorno, la aplicación se instalará también en Mac OS. Para facilitar la instalación en ambos entornos, deberemos llevar a cabo una configuración estándar del servidor que permita el acceso desde ambas plataformas (ver ANEXO II). Por su parte, la base de datos se gestionará haciendo uso de *MySQL Workbench* puesto que este entorno de desarrollo proporciona una interfaz intuitiva y manejable desde la que llevar a cabo las configuraciones de la base de datos necesarias para cumplir con los requerimientos técnicos del programa.

2.2.1. Usuarios y privilegios

Una vez instalado el servidor y creada la base de datos (ver ANEXO II y ANEXO III), en la sección *Users and Privileges* de la pestaña *Administration* (ver Figura 4), encontraremos el usuario *root* que creamos durante la instalación y los roles administrativos de que dispone.

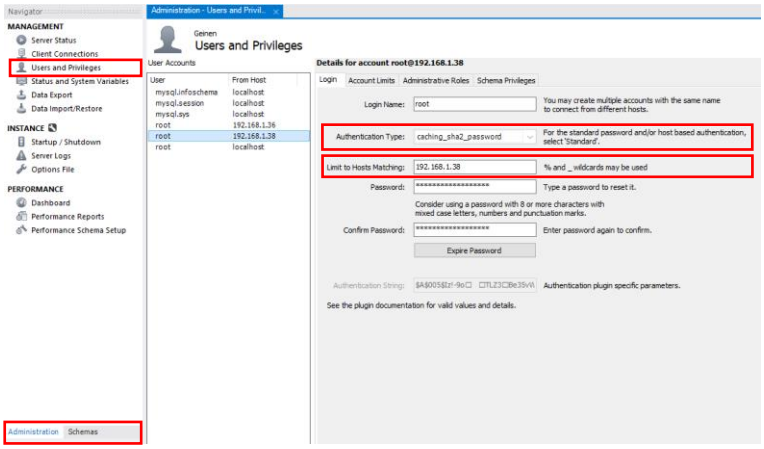


Figura 4: Conexión al servidor – Usuarios y privilegios.

En la imagen podemos ver que creamos un usuario *root* que puede acceder también desde las IPs 192.168.1.38 y 192.168.1.36. Como puede observarse, esto implica que cada nueva conexión de este usuario requeriría dar de alta un nuevo usuario con su IP. Para evitar esto, creamos un usuario *root* que pueda acceder desde cualquier IP tecleando en el campo *Limit to Hosts Matching* la tecla %. De este modo, cuando un usuario se conecte por VPN[11] (Virtual Private Network) o de forma remota desde cualquier computadora dentro de nuestra LAN[12] (Local Area Network), podrá acceder a la base de datos sin problemas.

Recordemos que una LAN es una red de dispositivos interconectados dentro de un área geográfica pequeña como lo es una casa, un edificio o un grupo de edificios. Las redes de área local se caracterizan por tener una velocidad de transferencia alta sin necesidad de realizar conexiones directas entre dispositivos (ver Figura 5). Esto implica que, para conectarnos desde fuera de esta red, necesitaremos establecer un túnel con una conexión VPN que nos permita llevar a cabo conexiones cifradas punto-a-punto con el servidor.

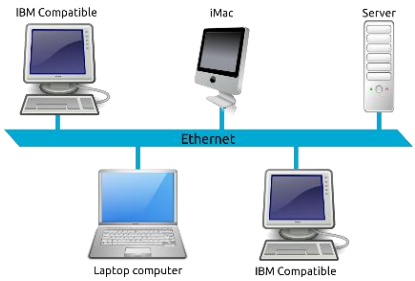


Figura 5: Red de área local[54].

2.3. Base de datos MySQL

MySQL es considerada como una de las bases de datos de código abierto más populares del mundo[13], tan sólo superada por Oracle, que es quién la desarrolla. Además, es posible utilizar la versión Enterprise para aquellas empresas que deseen utilizar la versión comercial de este sistema de gestión, por lo que empresas como Google o Facebook la utilizan[14]. Al finalizar el proyecto, se obtuvo una base de datos con 51 tablas. La mayor parte de las tablas son muy parecidas entre sí, de modo que evitaremos repasarlas todas. Sin embargo, hay ciertas características de configuración que merecen ser mencionadas.

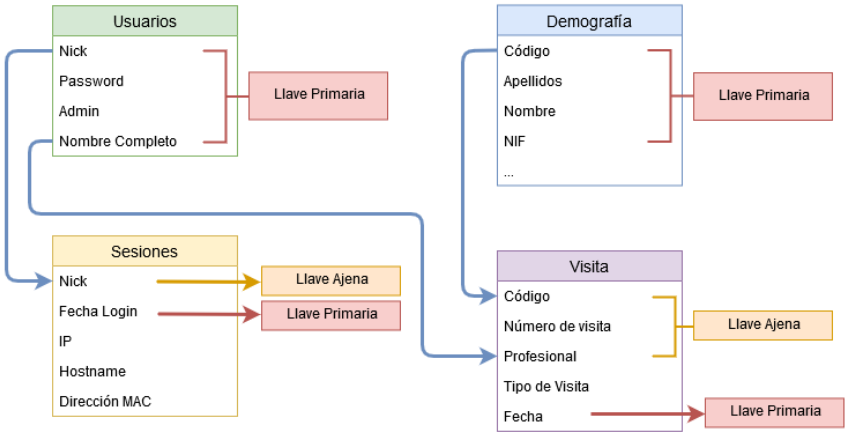


Figura 6: Esquema relacional de las tablas creadas.

En la Figura 6, podemos ver un ejemplo de la relación establecida entre las tablas creadas. Si bien todas tienen claves primarias (campos únicos dentro de esas tablas), la mayor parte de ellas tiene claves ajenas que hacen referencia a otras tablas, de forma que la relación cruzada entre ambas queda asegurada. La presencia de claves ajenas provee de cierta consistencia a los datos introducidos, dado que éstos deberán existir previamente en las tablas a las que pertenecen.

Es posible crear una tabla en MySQL sin claves primarias pero, en ese caso, las tablas pasarán a ser no editables – es decir, los datos introducidos no podrán ser modificados ni eliminados; por lo que en el futuro, se procederá a eliminar las llaves primarias para evitar una posible alteración indeseada. En el ANEXO III podemos ver el proceso de creación de la base de datos y sus correspondientes tablas en *MySQL Workbench*.

2.4. Seguridad y encriptación

La privacidad del paciente y la seguridad de la información médica electrónica[15] son aspectos fundamentales para el Sistema Nacional de Salud. Dicha seguridad y privacidad están protegidas por una serie de leyes y directivas estatales y comunitarias, como son: el Reglamento General de Protección de Datos[16] a nivel Europeo, la Ley Orgánica de Protección de Datos[17], el Real Decreto-ley 5/2018[18] o la Ley 41/2002[19], reguladora de la autonomía del paciente. Dada la sensibilidad de los datos manejados, aunque el Comité Ético del Hospital Universitario Dr. Peset ha dado permiso para realizar este proyecto, el cumplimiento de la normativa será un aspecto crítico a la hora de dar el visto bueno. Para garantizar todos los aspectos relacionados con la seguridad, hemos dotado al proyecto de los siguientes elementos:

- Registro de sesiones y de comandos.
- Funciones criptográficas hash: SHA-2.
- Conexión segura SSL.
- Cifrado RSA.
- Certificados de infraestructura de clave pública, x509.

En los subsiguientes apartados repasaremos todos estos aspectos.

2.4.1. Registro de sesiones y de comandos

El nuevo Reglamento Europeo de Protección de Datos otorga una mayor responsabilidad a aquellos que tratan datos personales y modifica el concepto de protección de datos actual haciendo hincapié en la trasparencia, la proactividad y la trazabilidad[20]. La información a recopilar en la trazabilidad de un producto depende del producto mismo. Sin embargo, el concepto de trazabilidad, en términos generales, consiste en mantener un registro de las distintas etapas de un producto. De esta manera, podemos hablar de trazabilidad ascendente y descendente[21]. La trazabilidad ascendente consiste en seguir los pasos de un producto desde el inicio, en nuestro caso, el inicio de sesión; mientras que la trazabilidad descendente consiste en seguir el rastro hasta el origen.

La forma en que se decidió implementar la trazabilidad en nuestro programa fue mantener un registro de sesiones y de los comandos utilizados en cada sesión. Para ello, siempre que un usuario introduzca su nombre de usuario y contraseña para entrar en el programa, se registrará de forma automática el nombre de usuario, la fecha y hora del inicio de sesión, la IP desde la que se ha realizado la conexión al servidor, el nombre del host desde el que se inició sesión y

la MAC del dispositivo electrónico utilizado (ver Figura 7). Esta tarea se llevará a cabo sin intervención del usuario, por lo que es independiente del mismo.

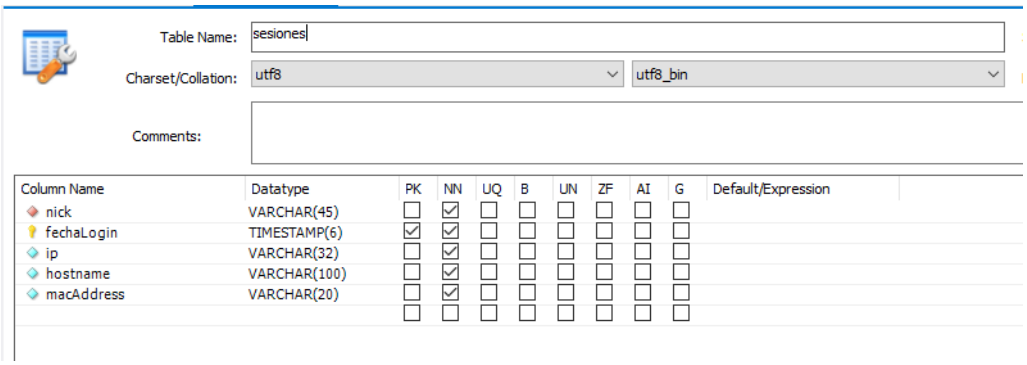


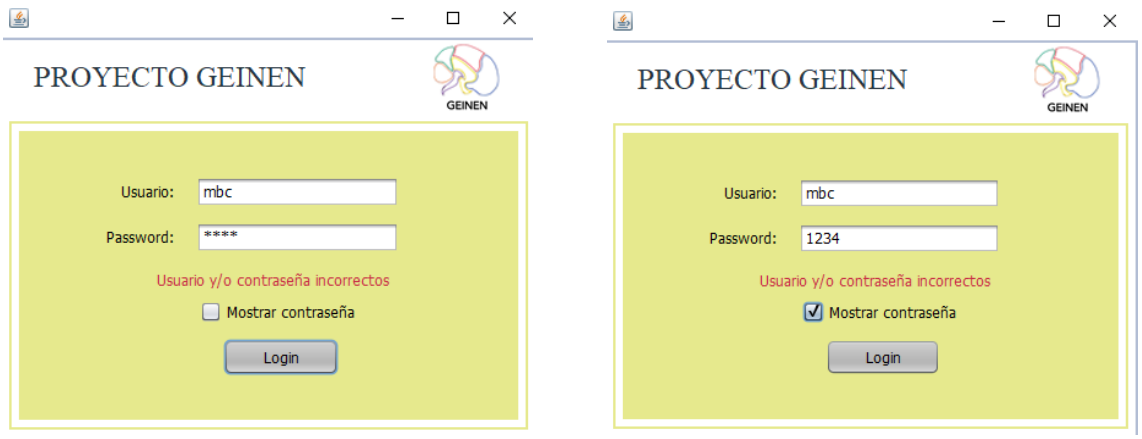
Figura 7: Tabla de registro de sesiones.

La información registrada en esta tabla puede ser de gran importancia en caso de detectarse un acceso indebido al servidor. De ser así, al conocer el nombre del host y la MAC desde los que se produjo el acceso, sería posible averiguar qué pasos se llevaron a cabo accediendo al registro de comandos. El registro de comandos es un archivo almacenado en toda computadora en que se haya instalado el programa. Este archivo se genera de forma automática al ejecutar el programa por primera vez, y contiene el listado de comandos de cada sesión junto con la fecha y hora a la que fueron ejecutados. Además, en este mismo registro se guardan las respuestas del servidor en forma de códigos, por lo que la información de los pacientes queda, de algún modo, codificada en forma de solicitudes y respuestas del servidor. Por otra parte, este archivo puede resultar útil para depurar posibles errores en las versiones sucesivas del programa. En la Figura 8 podemos ver una muestra de este registro con un error de acceso denegado, el cual se debe a la introducción de un nombre de usuario y/o contraseña incorrectos.

```
2019-07-26 18:16:53.32 Comando: INSERT INTO sesiones (nick, fechaLogin) VALUES (?,?) - Código: 1
2019-07-26 18:36:09.243 Comando: INSERT INTO sesiones (nick, fechaLogin) VALUES (?,?)
2019-07-26 18:36:09.243 Error: java.sql.SQLException: Access denied for user 'root'@'localhost' (using password: YES)
```

Figura 8: Registro de comandos de la aplicación.

En el caso en que un usuario introduzca un nombre de usuario y/o contraseña incorrectos, la aplicación informará de que uno de los dos campos es incorrecto, sin especificar cuál de ellos. El usuario podrá, sin embargo, ver la contraseña introducida siempre que lo desee (ver Figura 9). Esto es así para mantener cierta privacidad y evitar dar pistas sobre qué campo/s debe/n ser modificado/s.



(a) (b)

Figura 9: Ventana de inicio de sesión de la aplicación.

2.4.2. Funciones criptográficas hash: SHA-2

Durante la instalación del servidor establecimos como método de autenticación el plugin `caching_sha2_password`[22]. Este plugin utiliza la autenticación SHA-256 y otorga al servidor de una memoria caché. El hecho de que el servidor tenga una caché[23], implica que almacena datos temporalmente para que las solicitudes futuras de estos datos puedan ser atendidas con mayor rapidez, lo cual mejora el rendimiento del sistema. Por su lado, las funciones criptográficas hash hacen uso de las funciones hash, o funciones resumen, y se las conoce usualmente por el término hash. Este tipo de funciones procesan la información para producir un resumen de mensaje[24] que será el mismo siempre y cuando el mensaje de entrada sea el mismo, por lo que pueden utilizarse para validar una entrada comprobando que los datos no hayan sido alterados. Existen dos familias de funciones criptográficas hash[25]: aquellas que no utilizan una llave secreta, denominadas MDC (Manipulation Detection Code), y las que sí la utilizan, denominadas MAC (Message Authentication Code). Dentro de la familia de funciones MDC, encontramos dos grandes grupos[25] (ver Figura 10): las funciones resumen resistentes a colisiones (CRHF, Collision Resistant Hash Function) y las funciones resumen de un solo sentido (OWHF, One-Way Hash Function).

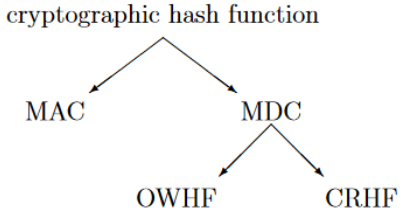


Figura 10: Taxonomía de las funciones criptográficas hash[25].

La familia de funciones OWHF[26] mapea los mensajes de manera que resulta computacionalmente inviable obtener el mensaje original a partir de su hash. Por su parte, las funciones CRHF[26] utilizan una variable aleatoria para mapear el mensaje, por lo que la dificultad que entraña encontrar dos mensajes que produzcan el mismo hash aumenta considerablemente (de ahí que sean resistentes a colisiones). Dado que no es posible reconstruir un mensaje a partir de su hash, este tipo de funciones se utilizan a menudo en criptografía para garantizar la seguridad en procesos de identificación con firmas digitales[27].

Dentro de la familia de funciones OWHF encontramos las llamadas funciones SHA[28] (Secure Hash Algorithm), publicadas por el Instituto Nacional de Estándares y Tecnología de Estados Unidos en 1993. Aunque existen cuatro versiones de esta familia de algoritmos[28], en este apartado nos centraremos en grupo de algoritmos SHA-2, del cual existen seis variantes distintas[29]: SHA-224, SHA-256, SHA-384, SHA-512 y sus variantes, SHA-512/224 y SHA-512/256. El número que acompaña al nombre hace referencia a la cantidad de bits que tendrá la palabra formada tras la compresión. Así pues, las funciones SHA-256 operan en bloques de 512 bits y generan un hash final de 256 bits[30] (32 bytes). Redes como Bitcoin[31] utilizan este tipo de funciones para verificar firmas digitales y para la creación de direcciones de pago. Por su parte, las variantes SHA-512/224 y SHA-512/256 generan un hash de 512 bits y lo truncan a 224 y 256 bits, respectivamente.

2.4.3. Conexión segura SSL

La capa de sockets seguros SSL (Secure Socket Layer) es un tipo de protocolo criptográfico[32] que se encarga de proporcionar conexiones seguras en una red, para asegurar la transferencia de datos entre un cliente y un servidor. Este tipo de conexión se utiliza a menudo en servidores web para asegurar transacciones de datos personales y bancarios[33]. Al utilizar el protocolo SSL, la aplicación que desea realizar la conexión necesita como mínimo de una llave y un certificado SSL para establecer la conexión. Al tratar datos personales de mucha sensibilidad, será necesario que nuestra aplicación pueda establecer conexiones seguras con el servidor. En MySQL es posible establecer conexiones encriptadas[34] pero, para poder utilizarlas, deberemos crear las llaves RSA y los certificados tanto del cliente como del servidor mediante el asistente *SSL Wizzard* de *MySQL Workbench* tras haber instalado el programa *OpenSSL* (ver ANEXO IV).

Los objetivos principales[35] del protocolo SSL son:

- **Integridad de datos:** los datos no deben ser alterados.

- **Privacidad de datos:** la privacidad de los datos queda asegurada a través de una serie de expedientes (unidad básica del protocolo), como son los expedientes de apretón de manos, expedientes CCS, expedientes de alerta y los expedientes de datos de aplicación.
- **Autenticación Cliente-Servidor**

Arquitectura SSL

El protocolo SSL fue diseñado para hacer uso del protocolo de control de transmisión[36] (TCP) para proveer una conexión punto-a-punto segura. Existen dos conceptos importantes dentro de este protocolo: la sesión SSL y la conexión SSL. Aunque a menudo nos referimos a SSL como un único protocolo, lo cierto es que consta de dos capas de protocolos[36]. En la Figura 11 podemos ver la posición que ocuparía este protocolo en los modelos OSI y TCP/IP.

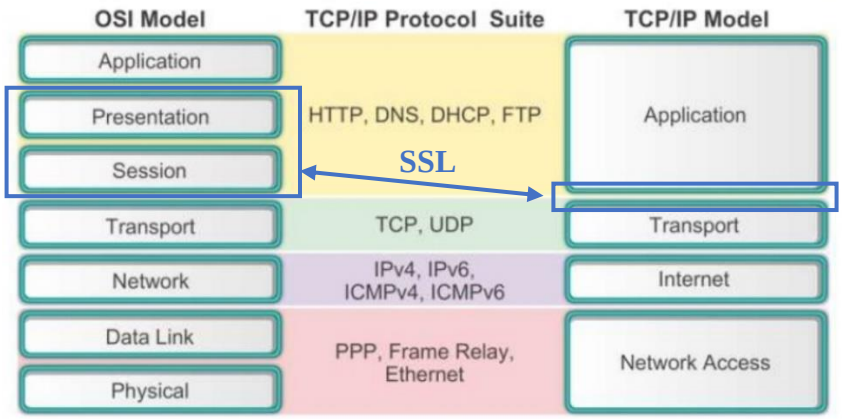


Figura 11: Correspondencia de la capa SSL en los modelos OSI y TCP/IP[55].

El protocolo SSL es el predecesor del protocolo TLS[35] (Transport Layer Security), cuya última versión fue publicada en 2018 y tiene como propósito general[36] proveer de herramientas de seguridad a la capa de transporte, equipándola de métodos para asegurar la privacidad, la autenticación y la integridad de los datos por debajo de la capa de transporte.

Transacción SSL

Para iniciar la comunicación entre cliente y servidor[37] (ver Figura 12), el cliente debe mandar un mensaje de saludo al servidor que contendrá la versión del protocolo SSL, el id de sesión (que inicialmente está vacío), las combinaciones de algoritmos criptográficos utilizados por el cliente en orden de preferencia y el método de compresión utilizado por el cliente (el cual puede ser nulo). Si el servidor no encuentra un algoritmo (criptográfico o de compresión) válido de entre los listados por el cliente, mandará una alerta del error y cerrará la conexión.

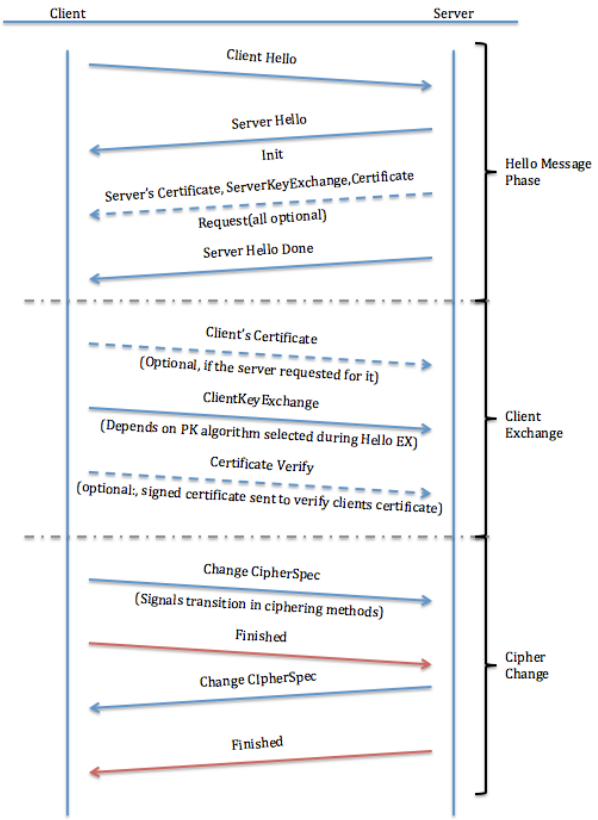


Figura 12: Intercambio y transferencia de paquetes del protocolo SSL[37].

En el caso en que todo haya ido bien, el servidor mandará un saludo al cliente con la respuesta a los parámetros solicitados por el cliente, en concreto: la versión del protocolo, el id de sesión (si se reanuda una sesión el id será el mismo que el mandado por el cliente, en caso contrario, el id de sesión tendrá un valor aleatorio), el algoritmo criptográfico escogido, el método de compresión seleccionado y una solicitud de certificado con la lista de certificados disponibles por parte del servidor para que el cliente seleccione uno. Una vez finalizado este intercambio de saludos, el servidor manda un mensaje avisando al cliente de que ha terminado y pasa a esperar una respuesta. Si los parámetros enviados por el servidor son aceptables, el cliente mandará su certificado, en caso de tenerlo, o una alerta de `no_certificate` que el servidor puede rechazar. Acto seguido, el cliente pasará a intercambiar su clave y, opcionalmente, un certificado firmado digitalmente[38] para verificar el certificado inicial solicitado por el servidor. Llegados a este punto, cliente y servidor pasarán a cambiar los algoritmos hash y de encriptación[36] para asegurar la conexión. En la Figura 13 podemos ver una captura de pantalla del *Wireshark* con una transacción SSL de una conexión remota al servidor para acceder a la base de datos.

130	13.237238	192.168.1.38	192.168.1.35	TCP	66 52529 → 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
131	13.237353	192.168.1.35	192.168.1.38	TCP	66 3306 → 52529 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM=1
132	13.244555	192.168.1.38	192.168.1.35	TCP	54 52529 → 3306 [ACK] Seq=1 Ack=1 Win=65536 Len=0
133	13.245604	192.168.1.35	192.168.1.38	MySQL	132 Server Greeting proto=10 version=8.0.16
134	13.299572	192.168.1.38	192.168.1.35	TCP	54 52529 → 3306 [ACK] Seq=1 Ack=79 Win=65536 Len=0
135	13.356586	192.168.1.38	192.168.1.35	MySQL	90 Login Request user=
136	13.397698	192.168.1.35	192.168.1.38	TCP	54 3306 → 52529 [ACK] Seq=79 Ack=37 Win=65536 Len=0
137	14.063881	192.168.1.1	224.0.0.1	IGMPv2	46 Membership Query, general
138	14.065273	192.168.249.1	224.0.0.1	IGMPv2	46 Membership Query, general
139	14.138573	192.168.1.38	192.168.1.35	TLSv1.2	252 Client Hello
140	14.139522	192.168.1.35	192.168.1.38	TLSv1.2	1514 Server Hello
141	14.139523	192.168.1.35	192.168.1.38	TLSv1.2	306 Certificate, Certificate Request, Server Hello Done
142	14.143532	192.168.1.38	192.168.1.35	TCP	54 52529 → 3306 [ACK] Seq=235 Ack=1791 Win=65536 Len=0
143	14.161511	192.168.1.38	192.168.1.35	TLSv1.2	328 Certificate, Client Key Exchange
144	14.165939	192.168.1.38	192.168.1.35	TLSv1.2	60 Change Cipher Spec
145	14.166017	192.168.1.35	192.168.1.38	TCP	54 3306 → 52529 [ACK] Seq=1791 Ack=515 Win=65024 Len=0
146	14.204227	192.168.1.38	192.168.1.35	TLSv1.2	123 Encrypted Handshake Message
147	14.204598	192.168.1.35	192.168.1.38	TLSv1.2	129 Change Cipher Spec, Encrypted Handshake Message
148	14.213590	192.168.1.38	192.168.1.35	TLSv1.2	347 Application Data
149	14.213930	192.168.1.35	192.168.1.38	TLSv1.2	107 Application Data

Figura 13: Captura de pantalla de la transacción SSL de una conexión remota.

2.4.4. Cifrado RSA

Una de las mayores aportaciones de la Teoría de Números en Computación[39] se encuentra en los sistemas criptográficos RSA. Este tipo de sistemas se denominan criptosistemas de llaves públicas o criptosistemas asimétricos[40] y utilizan un par de llaves para encriptar y desencriptar mensajes (ver Figura 14). El método de funcionamiento es el siguiente: el usuario que desea enviar un mensaje a un destinatario usa la llave pública del receptor para encriptar el mensaje. En la recepción, el destinatario desencripta el mensaje utilizando su llave privada, que sólo el conoce. De este modo, cualquiera puede enviar un mensaje encriptado utilizando únicamente información pública. Este concepto es el fundamento de la firma electrónica[27], donde existe la presunción de que sólo aquel que acepte el mensaje es dueño de la clave privada, puesto que el resto no podrá descifrar el mensaje.

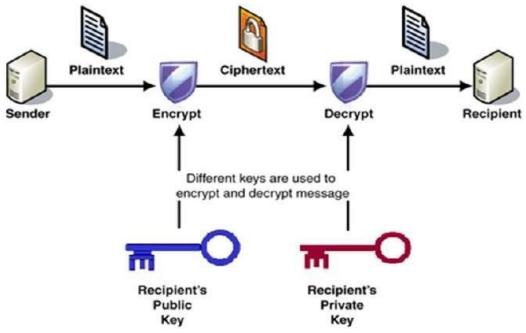


Figura 14: Criptografía de llaves públicas[41].

Del mismo modo, si se cifrara un mensaje utilizando la llave privada, este podría desencriptarse utilizando la llave pública. La razón de que esto sea así es que ambas llaves están relacionadas matemáticamente[40], por lo que un mensaje no puede descifrarse sin la llave complementaria (de ahí su asimetría). Aunque en teoría sería posible descifrar el mensaje, la búsqueda del mensaje original resultaría prohibitiva[39]. De cualquier modo, para evitar

suplantaciones de identidad se requiere una validación de las llaves mediante la validación de certificados y firmas digitales.

En este proyecto, se decidió crear las llaves RSA mediante el asistente *SSL Wizzard* de *MySQL Workbench* el cual, a su vez, hace uso del programa *OpenSSL* (ver ANEXO IV).

2.4.5. Infraestructura de clave pública, x509

Los certificados digitales[42] permiten que un individuo o entidad demuestre que es quien dice ser y que, por tanto, se encuentra en posesión de la llave privada asociada a su certificado. Así pues, un certificado de llave pública está asociado a una llave pública y uno o más atributos de identidad. De esta manera se garantiza que la llave pública pertenece a la entidad que envía el certificado y que, por tanto, está en posesión de la llave privada asociada. Aunque es posible crear nuestros propios certificados, sólo serán útiles a nivel legal si existe una Autoridad Certificadora[38] (CA) que los valide y ponga su firma digital al final de estos.

En criptografía, x509 es un estándar del UIT (Unión Internacional de Telecomunicaciones) publicado por primera vez en 1988. En la actualidad existen tres versiones de este estándar, cuya última versión fue revisada y publicada en 1996.

Formato del certificado x509 v3

El formato básico de un certificado x509 v3[42] consta de 10 campos (ver Figura 15):

- **Versión:** número de versión del certificado (1, 2 ó 3).
- **Número de serie del certificado:** este campo debe ser único y es asignado por la Autoridad Certificadora.
- **Identificador del algoritmo de firmado:** algoritmo empleado para firmar el certificado (RSA o DSA).
- **Nombre del emisor:** identidad de la Autoridad Certificadora que ha firmado y emitido el certificado.
- **Periodo de validez:** espacio de tiempo en que el certificado es válido (fecha inicial y final).
- **Nombre del sujeto:** identidad de la entidad sujeto de la certificación.
- **Información de clave pública del sujeto:** contiene la clave pública, sus parámetros y el identificador del algoritmo utilizado para generar la clave.
- **Identificador único del emisor:** este campo es opcional y contiene la identidad del emisor.

- **Identificador único del sujeto:** este campo es opcional y contiene la identidad de la entidad certificada.
- **Extensiones**.

Las extensiones permiten asociar información adicional[42] y constan de tres partes (ver Figura 15):

- **Tipo de extensión:** identificador del tipo de extensión (texto, fecha u otra estructura de datos).
- **Valor de la extensión:** valor del campo señalado en el tipo de extensión.
- **Indicador de importancia:** contiene un *flag*[43] indicando la importancia del campo de extensión y puede ser determinante a la hora de decidir si puede ser ignorado o no, en caso de no ser reconocido.

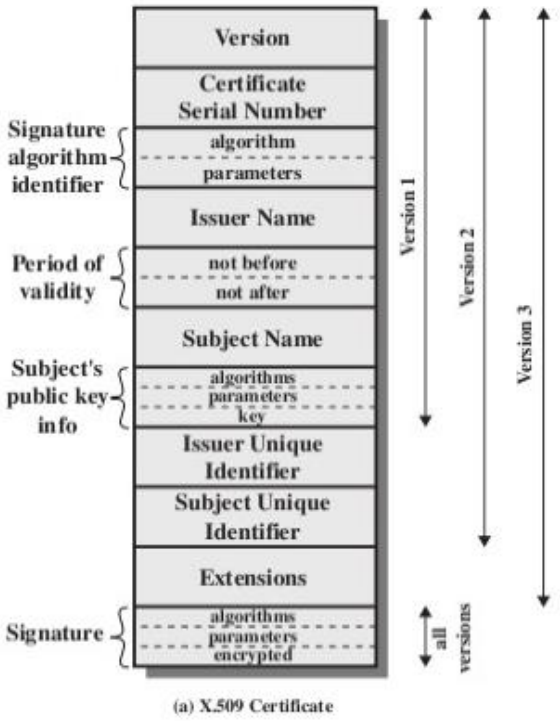


Figura 15: Estructura del certificado x509[56].

En este proyecto, los certificados fueron creados mediante el asistente *SSL Wizzard* de *MySQL Workbench* tras haber instalado el programa *OpenSSL* (ver ANEXO IV).

2.5. Arquitectura de software

En el desarrollo de software, la arquitectura de software hace referencia a un conjunto de elementos como son: el análisis, diseño e implementación de estructuras, para satisfacer los requisitos funcionales y no funcionales del sistema[44] (es decir, cumplir con las necesidades del cliente dentro de nuestro desarrollo de producto).

2.5.1. Arquitectura multicapa

La arquitectura multicapa plantea una clara organización en base a varios niveles de abstracción[44], de modo que el conjunto de elementos o subsistemas esté fundamentado en la capa que hay por debajo, proporcionando a su vez soporte a la capa superior. El ejemplo más sencillo de arquitectura multicapa es la arquitectura cliente-servidor, la cual consta de dos capas: en la primera encontramos el servidor y por encima de ella se encuentran los clientes que hacen uso de ese servidor. Para reducir la dependencia entre capas, se recomienda trabajar con capas cerradas[44] que, al utilizar únicamente recursos de la capa inferior, permiten realizar cambios con mayor facilidad viéndose afectada tan sólo la capa siguiente.

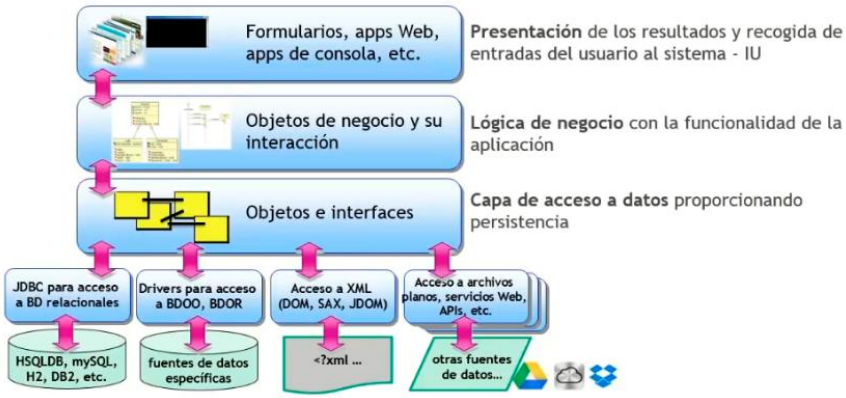


Figura 16: Arquitectura de software de tres capas[44].

La mayor parte de las arquitecturas software actuales suelen utilizar una arquitectura de tres capas[44] (ver Figura 16). En nuestro caso, la primera capa es la capa de presentación, la cual interactúa con el usuario. La segunda capa es la lógica del negocio y que se encarga de otorgar funcionalidad al sistema. Por último, la tercera capa es la de acceso a datos y es la que proporciona persistencia a los datos que pueden encontrarse en distintos formatos. Este tipo de arquitectura permite aislar la aplicación en componentes separados y claramente diferenciados, lo que facilita la distribución de la carga en distintas máquinas y procesos, mejorando así la dedicación de recursos.

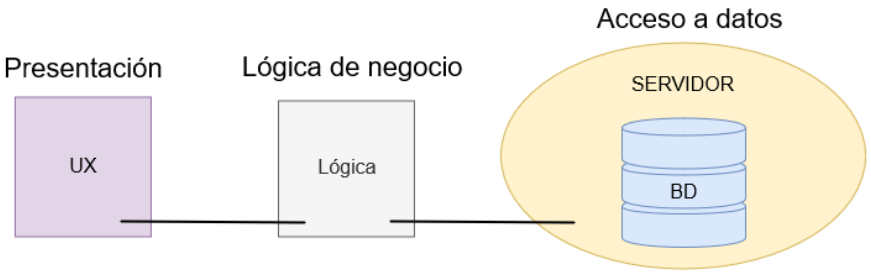


Figura 17: Esquema simplificado de la arquitectura multicapa del proyecto.

En la Figura 17 podemos ver un esquema simplificado de la estructura del proyecto implementado, si bien la capa de lógica del negocio ha sido segmentada en dos. La razón de dividir la lógica de negocio en dos partes fue mantener la funcionalidad de las vistas separada de la parte de la lógica que contiene la lógica de acceso a la base de datos. De este modo, para acceder a la base de datos harán falta dos clases distintas: `Logica.java` y `ConexionMySQL.java`. La primera contiene las funciones lógicas de acceso a la base de datos, mientras que la segunda contiene las funciones de conexión para insertar, extraer, actualizar o eliminar datos. De este modo, simplificamos el mantenimiento de estas clases minimizando la cantidad de archivos en los que realizar cambios y manteniendo cierto orden e independencia entre capas. Por otra parte, restringimos el número de instancias para llamar a las funciones de `Logica.java` mediante la creación de una instancia única o *singleton*[45].

2.5.2. Modelo–Vista–Controlador

Existen distintos tipos de ventanas a lo largo de la aplicación, como son: la ventana principal, las ventanas de Visita y las de Test. Durante el proceso de diseño quedó claro que era necesario establecer unas normas que permitieran mantener delimitados los distintos elementos y sus controladores, por lo que decidimos usar el patrón Modelo-Vista-Controlador[46] (MVC). Este patrón fue diseñado por primera vez por Trygve Reenskaug[47] en los años 70 como un estilo de arquitectura de interfaces gráficas.

En la Figura 18 podemos ver que el patrón MVC consta de tres elementos separados por limites abstractos[48]: el *Modelo*, la *Vista* y el *Controlador*. Si bien el *Modelo* maneja los datos, la lógica de negocio y las reglas de la aplicación, la *Vista* actúa sólo como interfaz gráfica que interactúa con el usuario. Sin embargo, el intermediario entre los elementos anteriores será el *Controlador*, que se encarga de gestionar la información y las posibles transformaciones o eventos que verá el usuario.

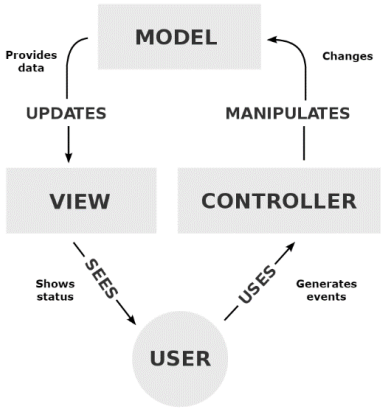
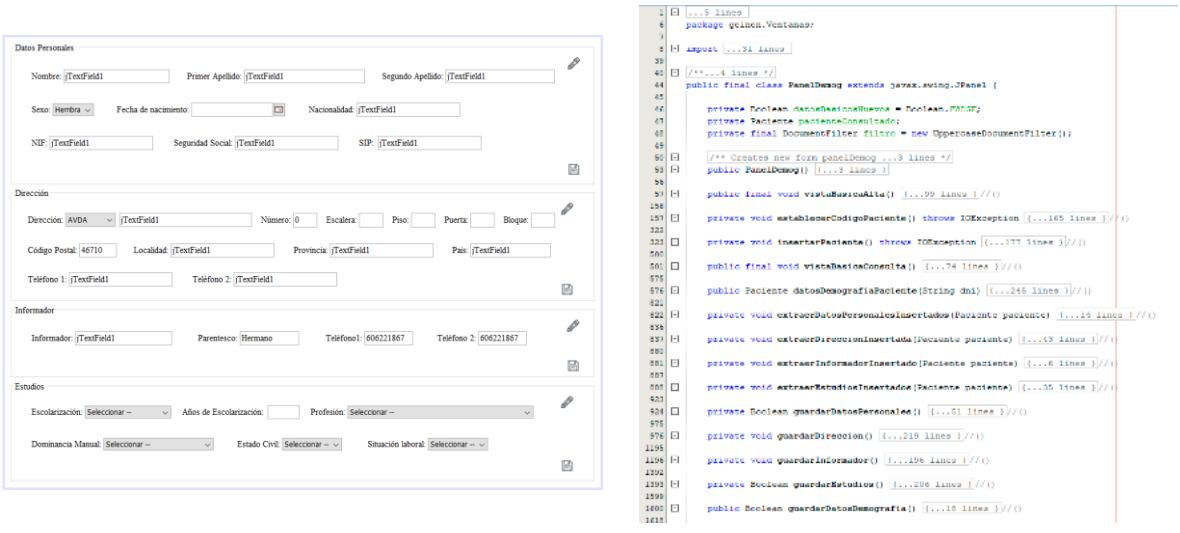


Figura 18: Diagrama de interacciones del patrón MVC[49].

En la Figura 19 y la Figura 20 podemos ver un ejemplo de la implementación de este tipo de patrón en la aplicación. La Figura 19 (a) muestra la vista del panel de demografía que verá el usuario en la ventana principal. En la Figura 19 (b) tenemos el modelo, que contiene la lógica del negocio. Sin embargo, el control de ambos elementos lo tiene la ventana principal (ver Figura 20), que es quién gestiona los eventos de entrada y salida. Aunque no lo mostraremos en este informe, todas las pestañas de la vista principal tienen el mismo funcionamiento. Es decir, en todas ellas se han incorporado paneles con sus correspondientes modelos, siendo la ventana principal la encargada de controlarlos a todos.



(a) (b)

Figura 19: (a) Vista y (b) Modelo del panel de demografía.

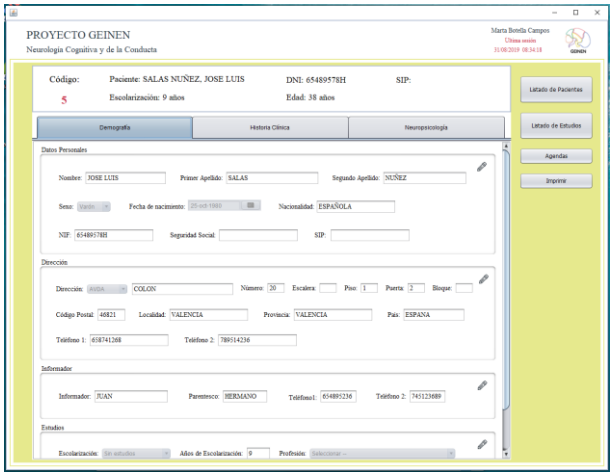


Figura 20: Ventana principal de la aplicación (Controlador del Modelo y la Vista).

2.6. Interfaz de usuario

El objetivo del diseño de interfaces de usuario es permitir que las personas que lo utilicen puedan controlar una aplicación o dispositivo. Para proporcionar una buena experiencia, un interfaz de usuario debe ser intuitivo y cómodo.

En este apartado veremos algunos elementos del sistema, como son:

- Ventana de Login
- Ventana de Pacientes y Estudios
- Ventana principal
- Visitas

2.6.1. Login

Al ejecutar el programa aparece la ventana de **Login** (ver Figura 21), en la que los profesionales médicos deberán acreditarse para poder acceder al contenido del programa, utilizando el nick y contraseña establecidos por el administrador. En caso de introducir una contraseña o usuario incorrectos, saltará un mensaje de error. Por otra parte, es posible visualizar la contraseña introducida marcando la casilla *Mostrar contraseña*.

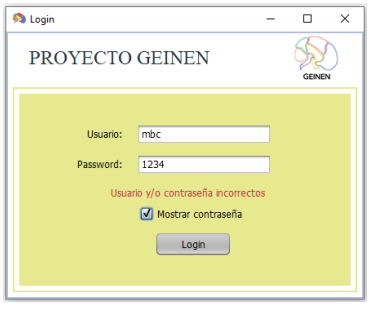


Figura 21: Ventana de Login.

2.6.2. Pacientes y estudios

Tras loguearse, aparece la ventana de **Pacientes y estudios** en la que los profesionales médicos deberán determinar la acción a realizar. Para acceder al historial médico de un paciente, deberán seleccionarlo haciendo doble click en la fila correspondiente del listado. En caso de no encontrarlo a simple vista, es posible filtrar el listado por: Apellidos, Nombre, NIF o SIP (ver Figura 22).

Para acceder al listado de estudios, el profesional médico puede clickar sobre el botón para tal efecto y seleccionar un estudio de la lista. Una vez más, es posible filtrar el listado en caso de que no se encuentre el código solicitado a simple vista (ver Figura 23 (a)). Al clickar sobre un estudio, aparece el botón *Editar estudio*, el cual permite editar el código y la descripción del estudio seleccionado (ver Figura 23 (b)). Para acceder al listado de individuos dentro de un estudio, el especialista deberá hacer doble click sobre un estudio de la lista. Hecho esto, aparecerá el listado de pacientes inscritos. Del mismo modo que con el listado de pacientes, es posible filtrar por Apellidos, Nombre; NIF y SIP para comprobar si un determinado paciente ha sido inscrito en dicho estudio. Por otra parte, si el profesional médico lo desea podrá generar un Excel con los datos de demografía de los pacientes inscritos en un determinado estudio (ver Figura 23 (c)).

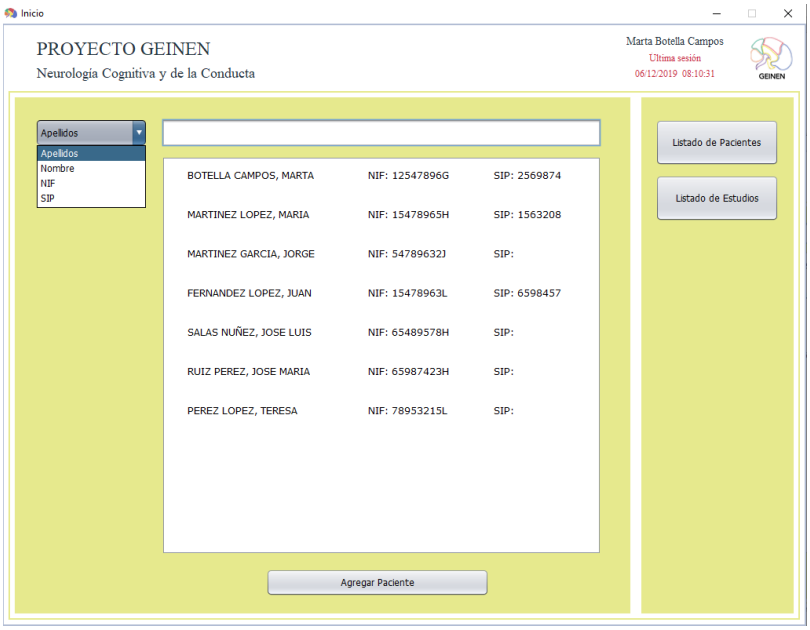
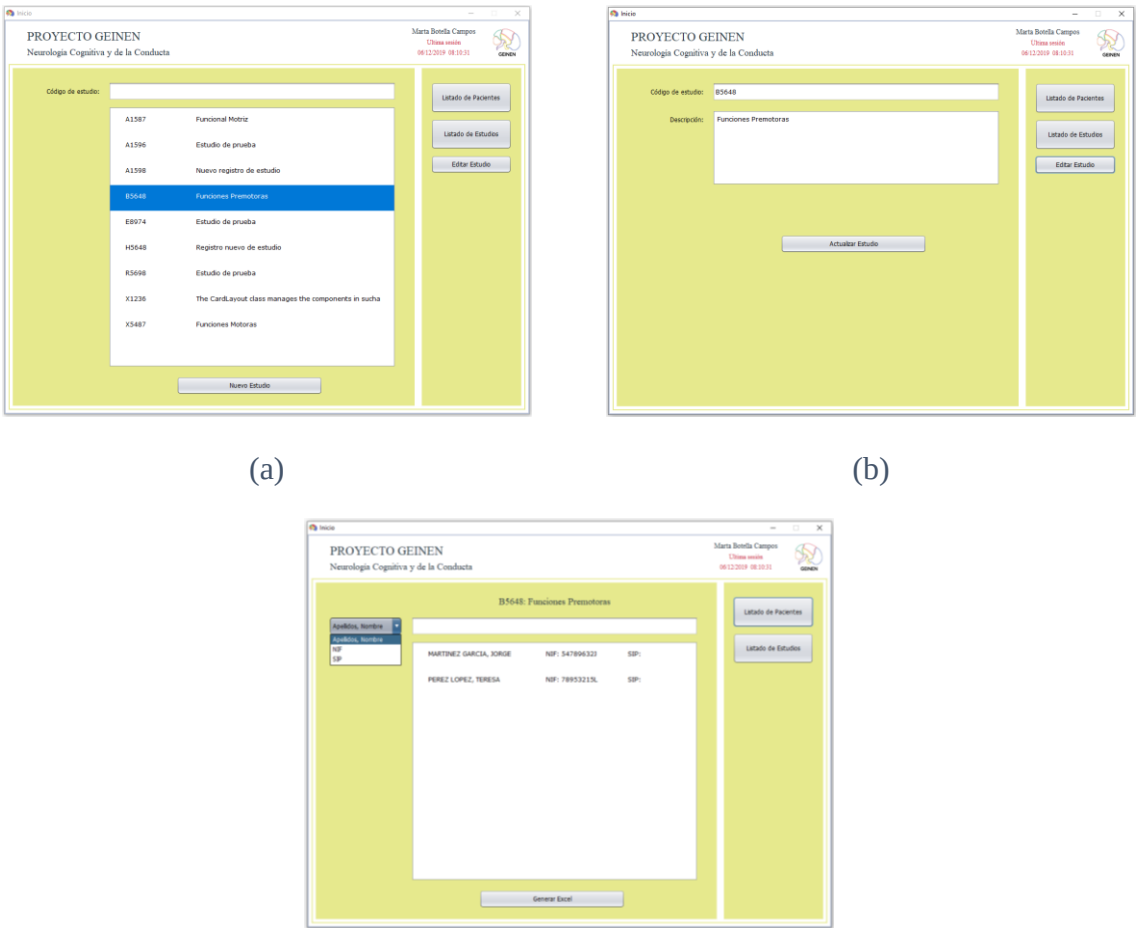


Figura 22: Listado de pacientes.



(a) (b)

(c)

Figura 23: Listado de estudios.

2.6.3. Ventana principal

Una vez seleccionado un paciente, accedemos a la **Ventana principal** del sistema. Esta ventana está compuesta por una cabecera con los datos básicos del paciente y tres pestañas: Demografía, Historia clínica y Neuropsicología.

Demografía

Por defecto, al entrar en el historial médico de un paciente mostramos sus datos demográficos para que el especialista pueda comprobarlos y/o modificarlos si lo desea (ver Figura 24). La demografía del paciente está compuesta por: Datos personales, Dirección, Datos del Informador y Estudios.

Historia clínica

La segunda pestaña muestra el listado de visitas realizadas junto con los estudios en los que se ha inscrito al paciente (ver Figura 25). Para seleccionar una visita, basta con seleccionar el tipo de visita en el desplegable y clickar el botón *Agregar*. Por otra parte, una vez se haya

realizado la visita *Primera (NRL)*, esta opción desaparecerá del listado para ser sustituida por el tipo de visita *Seguimiento*.

Neuropsicología

La tercera pestaña contiene una serie de pestañas cuyo nombre se corresponde con los bloques de test disponibles (ver Figura 26). En cada una de ellas se muestran tantas tablas como tipos de test puedan realizarse en ese bloque, con un listado de puntuaciones parciales y globales, además de los percentiles correspondientes cuando sea necesario. Por otra parte, es posible generar gráficas de evolución de cada uno de los test.

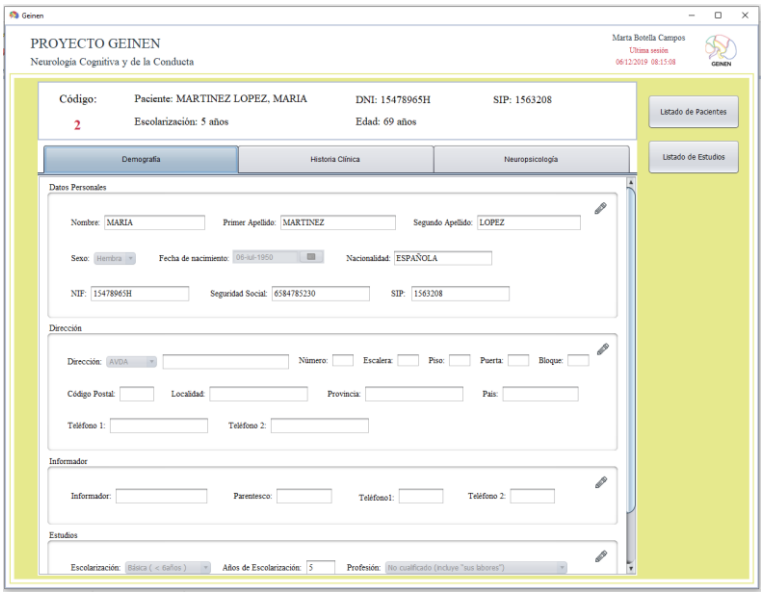


Figura 24: Datos personales del paciente (Demografía).

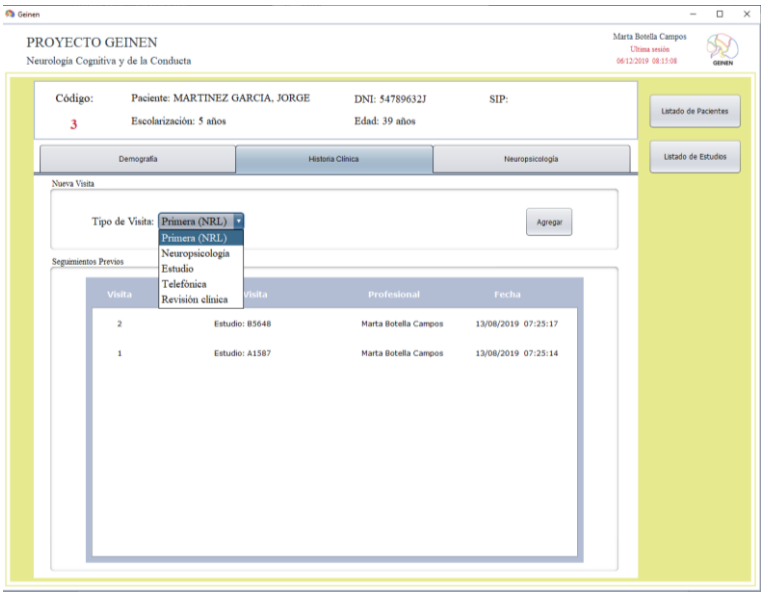


Figura 25: Historia clínica.

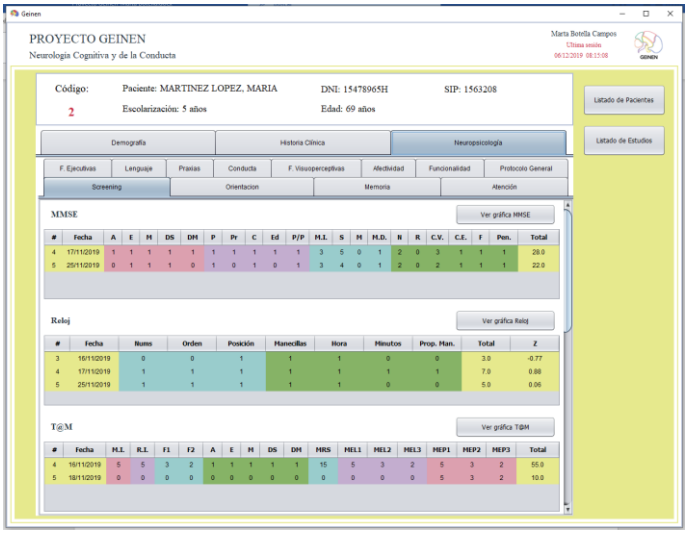


Figura 26: Neuropsicología.

2.6.4. Visitas

Aunque en este apartado no veremos todos los tipos de visitas y test posibles, hay que puntualizar que, en las visitas: *Primera (NRL)*, *Seguimiento* y *Neuropsicología*, es posible acceder a los test de los distintos bloques mediante un desplegable. Si en un determinado bloque existe más de un test disponible, aparecerá otro desplegable en el que seleccionar el test. Además, los test realizados durante una visita se muestran en un listado junto con la puntuación y su valoración (Normal o Alterado). En los casos más complejos en que los test están compuestos por puntuaciones y percentiles parciales, no se mostrará ni la puntuación ni la valoración. Para acceder a los test realizados el profesional médico deberá hacer doble click sobre el ítem de la lista. Por otra parte, es posible eliminar los test realizados en caso de que el especialista considere que el estado del paciente no es el adecuado para responder correctamente y hacer una valoración (ver Figura 27).

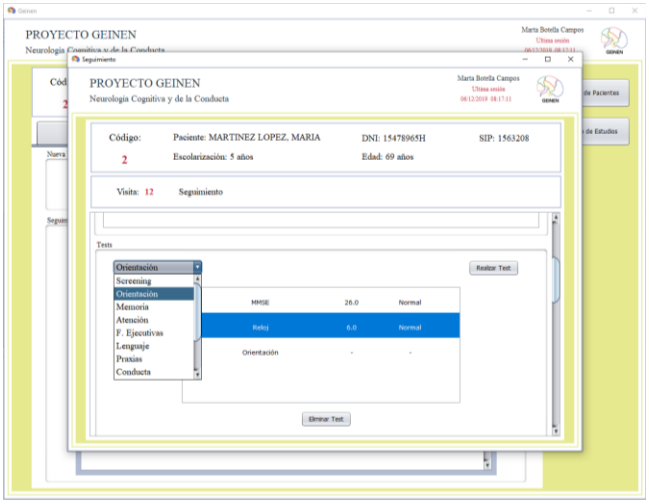


Figura 27: Listado de test en una visita.

3. Integración Continua

La integración continua es una práctica de desarrollo de software que requiere integrar el código varias veces al día con la intención de verificar el correcto funcionamiento del programa. Este modelo fue inicialmente propuesto por Martin Fowler[50] y permite detectar errores rápidamente y localizarlos fácilmente[51].

Como comentamos en el **Plan de trabajo** de la **Introducción** de este documento, se establecieron reuniones cada dos semanas con la intención de evaluar las diferentes partes del software y pulir detalles, además de corregir errores. De esta manera, permitimos a los profesionales médicos implicados en el proyecto disponer de tiempo suficiente para llevar a cabo pruebas con pacientes reales y comprobar que los datos obtenidos por el programa se corresponden con los obtenidos de forma manual.

3.1. Pruebas de software

Las pruebas de software[52] o *testing*, en inglés, son un proceso de evaluación de la funcionalidad de una aplicación con el objetivo de verificar y validar los distintos procesos que se llevan a cabo durante la ejecución del programa informático, y comprobar que se cumplen los requerimientos técnicos específicos establecidos en el proceso de diseño. El objetivo último, además de depurar el programa, es encontrar formas de mejorar la eficiencia, la precisión y la usabilidad del software.

Existen dos tipos básicos de pruebas en función de su ejecución:

- **Pruebas manuales:** el proceso se lleva a cabo de forma manual sin hacer uso de scripts ni herramientas automatizadas. En este caso, la persona encargada de llevar a cabo las pruebas asume el rol del especialista médico para testear el programa e identificar comportamientos inesperados o errores de proceso, haciendo uso de casos y escenarios típicos, además de improvisados.
- **Pruebas automáticas:** este proceso se lleva a cabo mediante el uso de scripts y herramientas automatizadas para llevar a cabo las pruebas. En este caso, aunque no hay rol del profesional médico, se trata de emular los distintos escenarios mediante código para comprobar que la respuesta del sistema es la esperada.

Existen dos técnicas básicas para llevar a cabo las pruebas de software:

- **Pruebas de caja negra:** en este tipo de pruebas, la persona que testea el programa no tiene acceso al código, sino que solo entra en contacto con el interfaz de usuario para comprobar su usabilidad y confort.
- **Pruebas de caja blanca**: este tipo de pruebas se llevan a cabo para comprobar que el comportamiento interno del programa cumple con los requerimientos técnicos establecidos a priori.

El proceso de evaluación de software se lleva a cabo atendiendo a los distintos niveles de las pruebas (ver Figura 28). Por lo tanto, el testing se llevará a cabo de forma incremental, empezando por las **pruebas unitarias**, donde se testean los distintos elementos de forma independiente para validar su comportamiento antes de integrarlos al grueso del programa. El siguiente paso será realizar las **pruebas de integración**, donde se comprueba que los distintos componentes individuales del sistema interactúan correctamente en su conjunto. Una vez validada esta fase, se ejecutan las **pruebas de sistema**, donde se testea el programa en su conjunto para comprobar que el comportamiento global del sistema es el esperado. Por último, se efectúan las **pruebas de aceptación**, con el fin de conseguir la conformidad en términos de requerimientos del sistema y usabilidad.

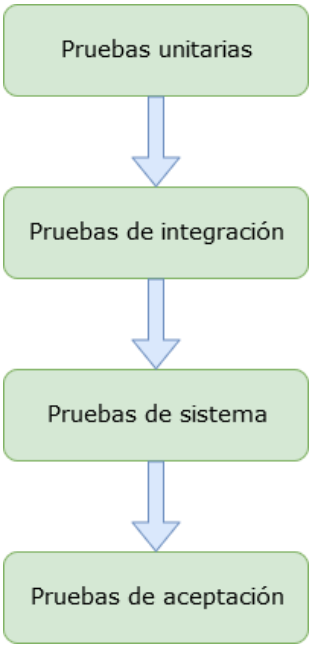


Figura 28: Niveles de pruebas de software.

3.2. Mejoramiento iterativo

El desarrollo iterativo[53] y creciente es un proceso de desarrollo de software en el que el desarrollador trata de sacar ventaja de lo aprendido en las distintas versiones y entregables. Para

llevar a cabo este proceso, el primer paso es realizar una implementación simple de los requerimientos del sistema y realizar mejoras de forma evolutiva. De esta forma, en cada iteración se llevan a cabo cambios en el diseño y se agregan nuevas funcionalidades y capacidades al sistema.

En este apartado mostraremos los cambios de diseño llevados a cabo durante las pruebas de desarrollo (*testing*):

- Permisos de edición
- Elementos visuales integrados

3.2.1. Permisos de edición

La primera medida llevada a cabo durante el proceso de testado de la aplicación fue permitir la edición de datos en las visitas y los test durante un periodo de 24 horas. Siempre que se cierre una ventana de visita o de test durante las primeras 24 horas, aparecerá un mensaje preguntando al especialista si desea guardar los cambios. En el caso de estar editando una visita, si el profesional médico no guarda los cambios, se eliminarán los test nuevos realizados y los cambios en el texto.

Pasadas las primeras 24 horas, los campos dejarán de ser editables y no podrán agregarse más test. En este sentido, es posible seleccionar un test dentro de una visita para consultarlo, pero no para modificarlo. Además, sólo será posible eliminar un test del registro durante las primeras 24 horas.

3.2.2. Elementos visuales integrados

Los elementos visuales integrados durante el proceso de mejoramiento iterativo son:

- Aviso: Introduzca SIP
- Imprimir y Guardar
- Cronómetros
- Ayudas visuales
- Puntuaciones
- Recordatorios
- Comentarios de las Visitas
- Gráficas

Aviso: Introduzca SIP

En ocasiones los pacientes y/o sus familiares olvidan traer todas las acreditaciones en la primera visita, por lo que se decidió permitir registrar pacientes sin necesidad de aportar el número de SIP. Aunque esta medida favorecerá la inclusión de pacientes a nivel nacional, en la Comunidad Valenciana suele preferirse adjuntar este dato. Por esta razón, siempre que se seleccione un paciente del que no se tenga el número de identificación SIP aparecerá una ventana en la esquina superior derecha, avisando al especialista de que este dato no ha sido introducido (ver Figura 29).

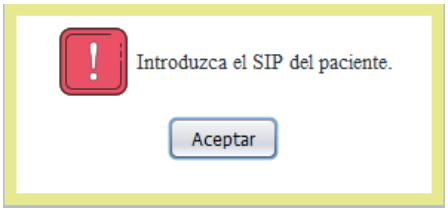


Figura 29: Introduzca SIP del paciente.

Imprimir y Guardar

En ocasiones, al realizar los test los pacientes necesitan una hoja en blanco en la que escribir, copiar o dibujar. Por esta razón, se decidió introducir botones en la parte superior del test para que el profesional médico pueda seleccionar la acción a realizar: Imprimir hoja en blanco, Guardar Test o Imprimir Test (ver Figura 30).

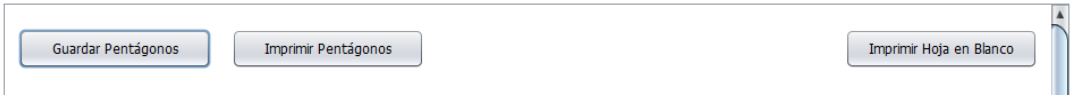


Figura 30: Imprimir hoja en blanco, Guardar Test o Imprimir Test.

Siempre que el especialista decida imprimir una hoja para el paciente, se generará un pdf con los datos del paciente, la fecha y la hora, y el número de visita (ver Figura 31).

Figura 31: Imprimir hoja para el paciente.

En el caso en que el especialista desee guardar las respuestas que el paciente ha registrado en las hojas que se le dieron, se podrá optar por guardar una imagen o un pdf. Para ello, el profesional médico deberá clickar sobre el botón *Guardar*, para abrir la ventana que le permitirá arrastrar las imágenes que desea añadir, o seleccionar un pdf. Además, si el especialista inserta imágenes, podrá girarlas a su antojo y navegar a través de ellas o eliminarlas clickando sobre

los iconos de la barra lateral derecha (ver Figura 32). Una vez guardados los elementos, se generará un pdf con el contenido seleccionado.

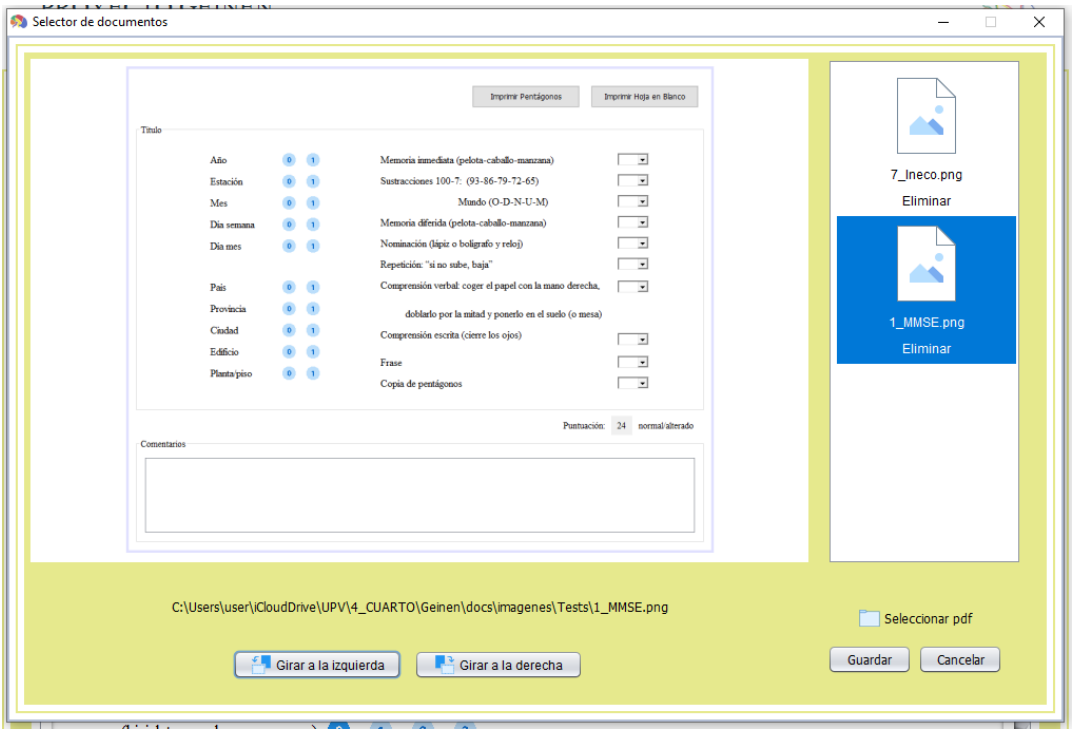


Figura 32: Guardar Test.

Cronómetros

En ocasiones existen partes de un test que deben realizarse en un marco de tiempo limitado. Sin embargo, los pacientes suelen verse sugestionados al comprobar que el especialista médico hace uso de un reloj, por lo que se decidió integrar cronómetros de cuenta atrás que permitan al especialista realizar la tarea sin por ello incomodar al paciente (ver Figura 33).

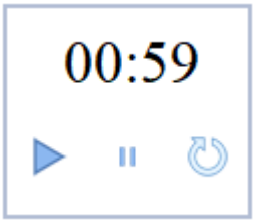


Figura 33: Cronómetro de cuenta atrás.

Existen test en los que se puntúa el tiempo que ha tardado el paciente en realizar una tarea. En estos casos, se introdujeron timers de cuenta progresiva (ver Figura 34). Al hacer click en el botón de inicio, el tiempo empezará a correr y se mostrará un círculo de puntos que gira cada segundo (ver Figura 34 (a)). En el caso en que el paciente realice la tarea, el profesional médico puede pulsar el botón para detener el tiempo y la rueda será sustituida por una marca de chequeo

verde (ver Figura 34 (b)). Sin embargo, siempre que el especialista considere que el paciente no ha terminado la tarea, podrá pulsar sobre la rueda y esta será sustituida por una cruz roja (ver Figura 34 (c)).

Figura 34: Cronómetros de cuenta progresiva.

Ayudas visuales

Existen casos en que el paciente debe repetir una lista de palabras que le ha sido leída previamente. Sin embargo, dado que estos pacientes suelen presentar cuadros de demencia, es posible que no recuerden la lista completa. Por esta razón, el profesional médico puede optar por darle pistas de categoría o de elección múltiple (ver Figura 35). Para facilitar la tarea, se decidió que, siempre que un paciente acertase una palabra de la lista, se ocultarían estas palabras de las listas de pistas.

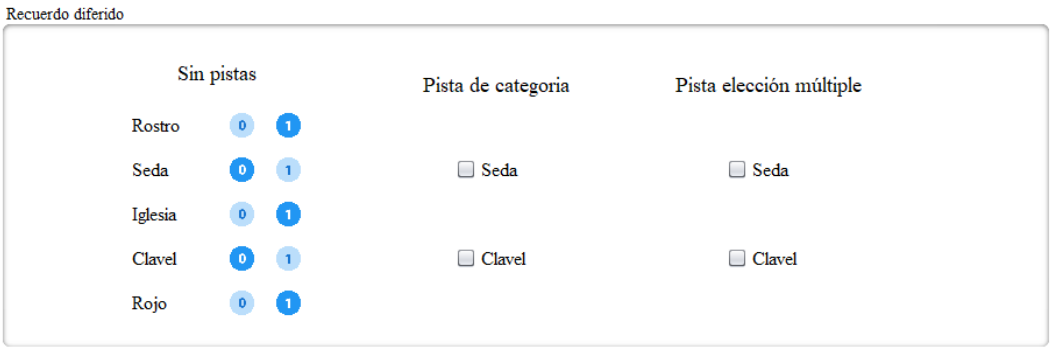


Figura 35: Ocultación de items acertados.

En otros casos, al paciente se le puede dar un segundo intento para decir una palabra o repetir una serie. En estas situaciones, además de ocultar la opción del segundo intento, aparecerá una marca de chequeo cuando el paciente acierte. Esta marca aparecerá también si el paciente acierta en el segundo intento. De lo contrario, la fila aparecerá seguida por una cruz roja (ver Figura 36).

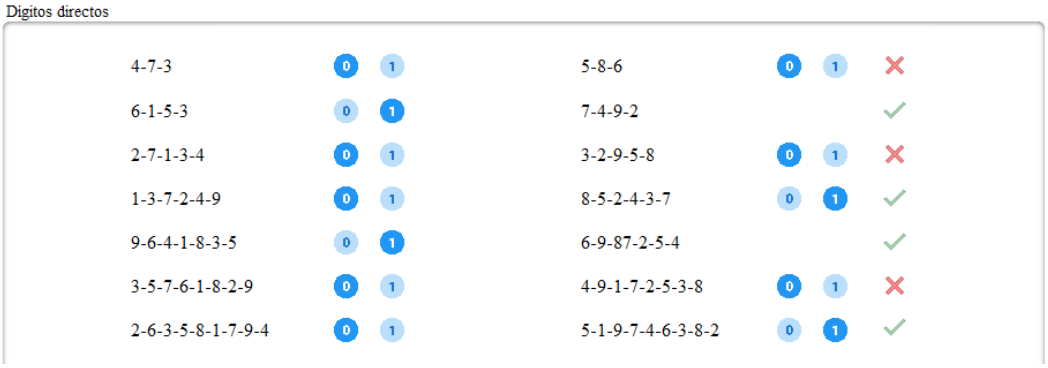


Figura 36: Marcas de fallo y acierto.

Algunos test consisten en preguntar cosas al paciente y comprobar si la respuesta coincide con la respuesta correcta. En la Figura 37 podemos ver que, por defecto, aparecen cruces rojas al lado de cada pregunta. Esto se hizo así para facilitar la tarea del especialista, que sólo tendrá que pulsar sobre uno de esos iconos siempre que el paciente acierte en su respuesta.

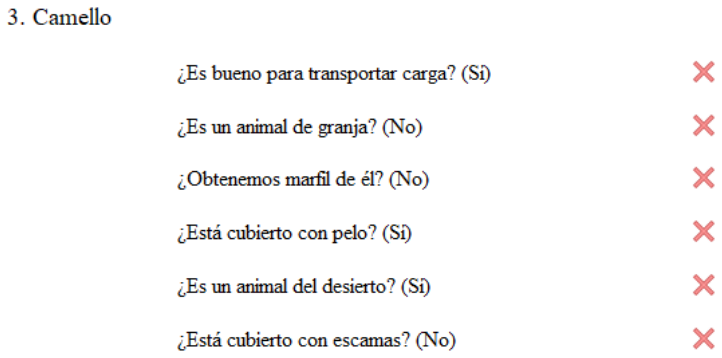


Figura 37: Marcas de fallo.

Puntuaciones

En los estudios de cognición es importante registrar la puntuación del paciente, pero también su percentil. Siempre que el percentil esté por debajo de 10, podremos asegurar que esa área de cognición está alterada, por lo que debajo de cada sección de los test aparecerá la puntuación y el percentil (ver Figura 38). Si el percentil es inferior a 10, estos datos serán resaltados en color rojo. En caso contrario, se mostrarán en negro.

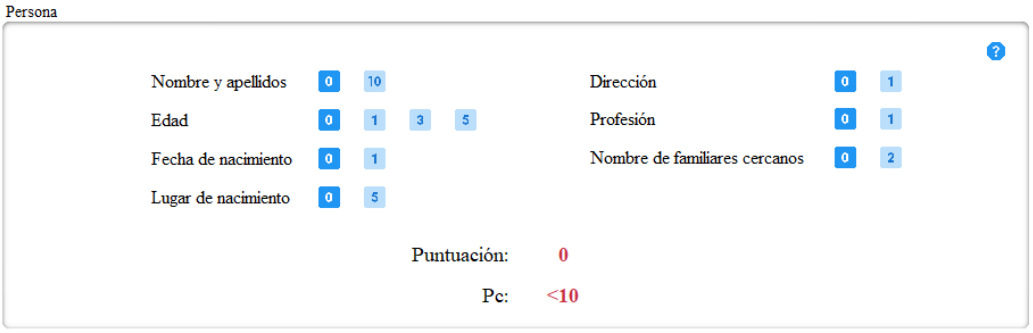


Figura 38: Puntuaciones y percentiles.

Recordatorios

Otro de los elementos introducidos en los test menos utilizados por los profesionales médicos es el botón de *Ayuda*. Al pulsar este botón aparece un panel con el recordatorio de la puntuación para que el especialista pueda realizar la corrección correctamente (ver Figura 39).

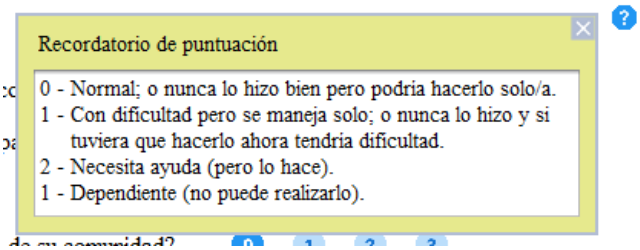


Figura 39: Recordatorio de puntuación.

Comentarios de las Visitas

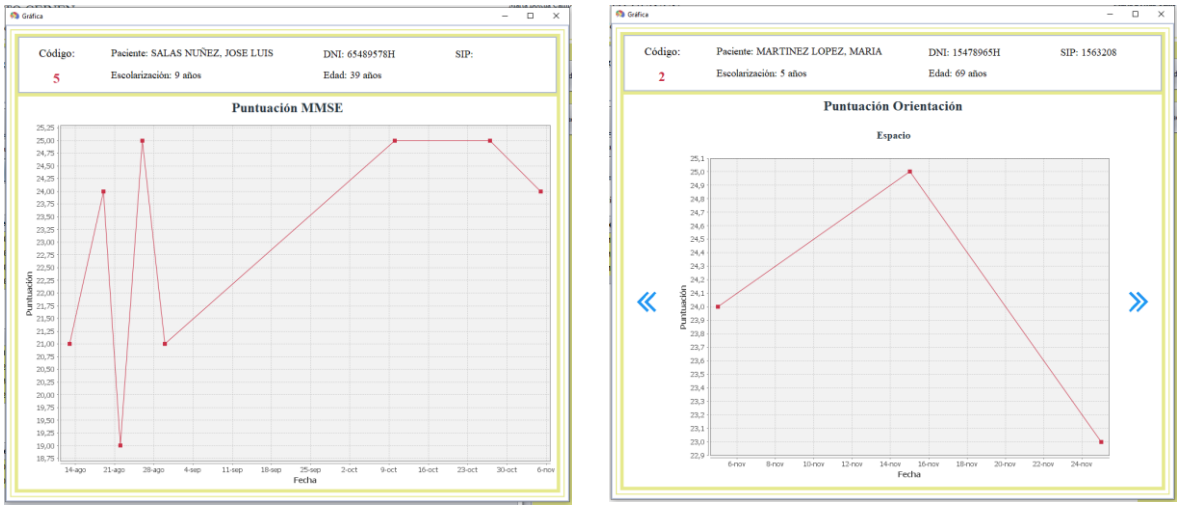
Todas las visitas y los test contienen un área de comentarios que el profesional médico puede rellenar. Sin embargo, para facilitar la tarea del especialista se decidió añadir los comentarios de los test en los comentarios de las visitas *Primera (NRL)*, *Seguimiento* y *Neuropsicología*. Estos comentarios aparecerán siempre que exista un comentario en un test registrado y se actualizará al guardar el test modificado (ver Figura 40). Además, es posible alternar comentarios de test y comentarios de la visita siempre que se respete la estructura: cabecera – comentarios – guiones.

Figura 40: Comentario de las visitas

Gráficas

Un aspecto importante en el seguimiento del paciente es el estudio de su evolución temporal. El software desarrollado permite la elaboración rápida de gráficas que permiten consultar el progreso de la enfermedad de un paciente.

Existen dos tipos de ventanas de gráficas de evolución: ventana simple (ver Figura 41 (a)) y ventana múltiple (ver Figura 41 (b)). La razón por la existen dos ventanas es que existen test con puntuación global y test con puntuaciones parciales. Por lo tanto, dependiendo del caso, se mostrará una ventana con una única gráfica o una ventana en la que navegar por las distintas gráficas de evolución que componen un test.



(a) (b)

Figura 41: Gráficas de evolución.

4. Líneas Futuras

Se prevé la ampliación del proyecto en una fase posterior tras presentarlo en el grupo de estudio de demencias de la Sociedad Española de Neurología para extender su uso a otros hospitales de España, solicitando un proyecto de investigación al Plan Estatal de Investigación Científica y Técnica y de Innovación 2017-2020 (Programa Estatal de I+D+i Orientada a los Retos de la Sociedad). De este modo, se podrá extender el software al ámbito nacional añadiendo funcionalidades necesitadas por otros hospitales y haciendo posible la interacción entre bases de datos de diferentes sistemas.

El objetivo último es tener una herramienta informática unificada a nivel nacional que facilite la interacción entre los diferentes profesionales de la neuropsicología, para crear una base de datos neuropsicológicos nacional que potencie los esfuerzos en la identificación de marcadores neuropsicológicos de riesgo de las enfermedades neurodegenerativas que cursan con demencia, para facilitar el diagnóstico precoz y favorecer otras vías de investigación.

5. Conclusión

La demencia es un síndrome degenerativo que conlleva un deterioro cognitivo, físico y conductual, que afecta a más de 50 millones de personas en la actualidad. Dado el marcado crecimiento de la población mayor de 65 años como consecuencia de la esperanza y calidad de vida, se espera que la tasa de dependencia de este sector de la población alcance el 60% en los próximos 30 años. La Organización Mundial de la Salud ha establecido la evaluación de la demencia como prioritaria, con la esperanza de que puedan ponerse en marcha medidas que contribuyan a reducir el riesgo de deterioro cognitivo antes de 2025.

En la actualidad, no existe una red estatal de datos neuropsicológicos de la población, sino que cada Comunidad Autónoma gestiona los datos de los pacientes atendidos de forma independiente. Además, a pesar de que el Sistema Nacional de Salud destaca por su calidad, la falta de iniciativas ha hecho que, en muchos casos, se siga llevando un registro en soporte papel, lo que acarrea dificultades de almacenamiento, gestión y acceso a los datos. Por otra parte, en la Comunidad Valenciana se utiliza un sistema de gestión generalista que, aunque permite mejorar la atención al paciente y asiste a los profesionales médicos en la actividad clínica, presenta carencias específicas en los distintos sectores de la actividad sanitaria.

Debido al impacto socioeconómico que las enfermedades y lesiones neurodegenerativas tienen en los pacientes, sus familiares y cuidadores, y la sociedad en general, el estudio de marcadores no invasivos mediante el uso de un software específico que agilice las valoraciones de los pacientes tendrá un impacto económico considerable, mejorando la eficiencia en la asistencia sanitaria y favoreciendo la investigación. El aumento del número de pacientes a los que se les haya realizado las necesarias exploraciones neuropsicológicas contribuirá a un mayor número de diagnósticos precoces que permitan el inicio de los tratamientos y posibiliten su participación en ensayos clínicos, lo que disminuirá la ansiedad provocada por la incertidumbre diagnóstica y permitirá al paciente organizar sus asuntos y voluntades de forma anticipada.

Gracias a la experiencia y cooperación de los profesionales médicos del Hospital Dr. Peset, fue posible integrar elementos en la aplicación que mejoraron su usabilidad, eficiencia y precisión, como fueron: los cronómetros, las ayudas visuales, las puntuaciones y sus correspondientes percentiles, la ventana de selección de imágenes y pdfs, los avisos, los recordatorios y las gráficas de evolución de la enfermedad de los pacientes. En este sentido, su ayuda y tiempo dedicados fueron inestimables, puesto que, además de mejorar el producto final, aportaron una visión realista sobre el terreno a la que no habría podido accederse de otra manera.

Por otra parte, dado que la privacidad del paciente y la seguridad de la información médica electrónica son aspectos fundamentales para el Sistema Nacional de Salud, al estar protegidas por diversas leyes y directivas estatales y comunitarias, se dotó al proyecto de elementos como: el registro de comandos y sesiones, la autenticación mediante el algoritmo criptográfico SHA-256, la capa de sockets seguros SSL que garantiza una conexión segura, el criptosistema de llaves públicas RSA y los certificados digitales de clave pública x509. El uso de estos elementos proporcionó conocimientos prácticos añadidos y la búsqueda de información al respecto que quizá no se habría realizado en otras circunstancias.

En el futuro, se espera llevar a cabo una ampliación de este proyecto que permita extender este software al ámbito nacional, para disponer de una herramienta unificada que proporcione datos neuropsicológicos de la población y potencie los esfuerzos realizados en este sentido, facilitando así el diagnóstico de pacientes en las etapas tempranas de la enfermedad y favoreciendo la investigación de las enfermedades que cursan con demencia.

Este proyecto no habría sido posible sin el apoyo, consejos y aportaciones de Felipe Vico Bondía, quien encontró tiempo y ánimo para analizar y cuestionar las distintas decisiones tomadas a lo largo del desarrollo de esta aplicación.

Bibliografía

[1] Enfermería de Ciudad Real. (2019). *Envejecimiento y demencia*. [online] Available at: https://www.enfermeriadeciudadreal.com/envejecimiento-y-demencia-604.htm [Accessed 1 Dec. 2019].

[2] Statista. (2019). *Tasa de dependencia de la población mayor de 64 años 2019-2068 | Statista*. [online] Available at: https://es.statista.com/estadisticas/630963/proyeccion-de-la-tasa-de-dependencia-de-la-tercera-edad-espana/ [Accessed 1 Dec. 2019].

[3] Who.int. (2019). *Demencia*. [online] Available at: https://www.who.int/es/news-room/fact-sheets/detail/dementia [Accessed 2 Dec. 2019].

[4] El médico interactivo. (2019). *El sector salud, decidido a entrar en lo digital – El médico interactivo*. [online] Available at: https://elmedicointeractivo.com/el-sector-salud-decidido-entrar-en-lo-digital/ [Accessed 4 Dec. 2019].

[5] diariofarma. (2019). *La digitalización entra en el sector salud a un ritmo desigual | @diariofarma*. [online] Available at: https://www.diariofarma.com/2018/02/27/la-digitalizacion-entra-sector-salud-ritmo-desigual [Accessed 4 Dec. 2019].

[6] Google.com. (2019). [online] Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjYoPvMypvmAhXdAGMBHYN3DYsQFjADegQIAhAC&url=http%3A%2F%2Fwww.san.gva.es%2Fdocuments%2F157385%2F637798%2F2.Orion_Clinic_Innovacion_en_la_gestion_de_los_cuidados.pptx&usg=AOvVaw1Ad5I-ekhCS1NKKzuzEyDX [Accessed 4 Dec. 2019].

[7] Softwaredecuidados.blogspot.com. (2019). *ORION CLINIC*. [online] Available at: http://softwaredecuidados.blogspot.com/2013/12/orion-clinic.html [Accessed 5 Dec. 2019].

[8] Actasanitaria.com. (2019). [online] Available at: https://www.actasanitaria.com/wp-content/uploads/2019/03/COR-2018-02838-00-00-AC-TRA-ES.pdf [Accessed 5 Dec. 2019].

[9] Vico Bondía, H. and Vico Bondía, F. (2019). *APLICACIÓN EN LA NUBE PARA LA GESTIÓN INTEGRAL DE EXPLORACIONES NEUROPSICOLÓGICAS – PROYECTO GEINEN*. 1st ed. Valencia: Polisabio.es, pp.3-4.

[10] Eckel, B. (2003). *Piensa en Java*. 2nd ed. PRENTICE HALL: Pearson Educación, p.22.

[11] Techopedia.com. (2019). *What is a VPN Connection? – Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/30743/vpn-connection [Accessed 28 Aug. 2019].

[12] Techopedia.com. (2019). *What is a Local Area Network (LAN)? – Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/5526/local-area-network-lan [Accessed 28 Aug. 2019].

[13] DB-Engines. (2019). *DB-Engines Ranking*. [online] Available at: https://db-engines.com/en/ranking [Accessed 26 Aug. 2019].

[14] Mysql.com. (2019). *MySQL: MySQL Customers*. [online] Available at: https://www.mysql.com/customers/ [Accessed 26 Aug. 2019].

[15] Ayuda Ley Protección Datos (LOPDGDD). (2019). *Guía de Protección de datos en Sanidad*. [online] Available at: https://ayudaleyprotecciondatos.es/2016/04/24/datos-sanitarios-seguridad/#Normativa_de_Proteccion_de_Datos [Accessed 28 Aug. 2019].

[16] Eur-lex.europa.eu. (2019). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo*. [online] Available at: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES [Accessed 28 Aug. 2019].

[17] Boe.es. (2019). *Ley Orgánica de Protección de Datos*. [online] Available at: https://www.boe.es/eli/es/lo/2018/12/05/3 [Accessed 28 Aug. 2019].

[18] Boe.es (2018) *Real Decreto-ley 5/2018*, [online] Available at: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-10751 [Accessed 29 Aug. 2019].

[19] Boe.es (2002) *Ley 41/2002*, [online] Available at: https://www.boe.es/buscar/doc.php?id=BOE-A-2002-22188 [Accessed 29 Aug. 2019].

[20] Lant Abogados. (2019). *Nuevo reglamento europeo de protección de datos*. [online] Available at: https://www.lant-abogados.com/nuevo-reglamento-europeo-de-proteccion-de-datos [Accessed 1 Sep. 2019].

[21] Pinzón Cepeda, R. (2019). *Trazabilidad*. [online] Monografias.com. Available at: https://www.monografias.com/trabajos81/trazabilidad/trazabilidad.shtml [Accessed 1 Sep. 2019].

[22] Dev.mysql.com. (2019). *MySQL: MySQL 8.0 Reference Manual :: 6.4.1.3 Caching SHA-2 Pluggable Authentication*. [online] Available at: https://dev.mysql.com/doc/refman/8.0/en/caching-sha2-pluggable-authentication.html [Accessed 27 Aug. 2019].

[23] ASALE, R. (2019). *Memoria caché*. [online] «Diccionario de la lengua española» - Edición del Tricentenario. Available at: https://del.rae.es/?id=OrlyaVd [Accessed 27 Aug. 2019].

[24] Ibm.com. (2013). *Función Resumen/Hash*. [online] Available at: https://www.ibm.com/support/knowledgecenter/es/SSGR73_7.0.0/com.ibm.wci.doc/ref_DigesHash.html [Accessed 29 Aug. 2019].

[25] Preneel, B. (1993). *CRYPTOGRAPHIC HASH FUNCTIONS: AN OVERVIEW*. [ebook] Leuven, Belgium: UK Leuven, p.2-3. Available at: https://www.esat.kuleuven.be/cosic/publications/article-289.pdf [Accessed 30 Aug. 2019].

[26] Angelov, G. (2019). *A Deep Dive into Cryptographic Hash Functions*. [online] KINGSLAND UNIVERSITY. Available at: https://kingslanduniversity.com/a-deep-dive-into-cryptographic-hash-functions/ [Accessed 29 Aug. 2019].

[27] Ibm.com. (2019). *Firmas digitales*. [online] Available at: https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55190_.htm [Accessed 29 Aug. 2019].

[28] Techopedia.com. (2019). *What is a Secure Hash Algorithm (SHA)? – Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/10328/secure-hash-algorithm-sha [Accessed 30 Aug. 2019].

[29] Csrc.nist.gov. (2014). *Hash Functions | CSRC*. [online] Available at: https://csrc.nist.gov/projects/hash-functions [Accessed 30 Aug. 2019].

[30] Domínguez Gómez, J. (2018). *Criptografía: Función SHA-256*. [ebook] pp.2-18. Available at:

https://foro.blockchainespana.com/download/file.php?id=30&sid=48d74e7ed7858d36f45c24a2e40b913f [Accessed 30 Aug. 2019].

[31] En.bitcoin.it. (2019). *SHA-256 – Bitcoin Wiki*. [online] Available at: https://en.bitcoin.it/wiki/SHA-256 [Accessed 30 Aug. 2019].

[32] Prof. Dr.-Ing. Georg Carle (2003/2004) 'Chapter 7 – Cryptographic Protocols', in (ed.) *Network Security*. [online] Available at: http://www.ccs-labs.org/~dressler/teaching/netzsicherheit-ws0304/07_CryptoProtocols_2on1.pdf: University of Tübingen, pp. 3-9. [Accessed 29 Aug. 2019].

[33] DigiCert (2019) *¿Qué son SSL, TLS y HTTPS?,* [online] Available at: https://www.websecurity.symantec.com/es/es/security-topics/what-is-ssl-tls-https [Accessed 29 Aug. 2019].

[34] Mysql.com (2019) *MySQL 8.0 Reference Manual – Configuring MySQL to Use Encrypted Connections*, [online] Available at: https://dev.mysql.com/doc/refman/8.0/en/using-encrypted-connections.html#mandatory-encrypted-connections [Accessed 29 Aug. 2019].

[35] Techopedia (2019) *Secure Sockets Layer (SSL),* [online] Available at: https://www.techopedia.com/definition/24025/secure-sockets-layer-ssl [Accessed 29 Aug. 2019].

[36] William Stallings (1998) 'The Internet Protocol Journal', *SSL: Foundation for Web Security*, 1(1), pp. [online] Available at: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-18/ssl.html [Accessed 29 Aug. 2019].

[37] Cisco (2019) *Introducción SSL con la transacción y el intercambio de paquetes de la muestra*, [online] Available at: https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-18/ssl.html [Accessed 29 Aug. 2019].

[38] Portal de Administración Electrónica Ministerio de Política Territorial y Función Pública Secretaría General de Administración Digital (2019) *Principales Autoridades de Certificación (AC)*, [online] Available at: https://firmaelectronica.gob.es/Home/Empresas/Autoridades-Certificacion.html [Accessed 27 Aug. 2019].

[39] OpenCourseWare, M. (2019). *2.4 RSA Encryption | Unit 2: Structures | Mathematics for Computer Science | Electrical Engineering and Computer Science | MIT OpenCourseWare*. [online] MIT OpenCourseWare. Available at: https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-042j-mathematics-for-computer-science-spring-2015/structures/tp6-2/ [Accessed 29 Aug. 2019].

[40] Ibm.com. (2019). *Criptografía de clave pública*. [online] Available at: https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm [Accessed 29 Aug. 2019].

[41] Tutorialspoint.com. (2019). *Public Key Encryption*. [online] Available at: https://www.tutorialspoint.com/cryptography/public_key_encryption.htm [Accessed 29 Aug. 2019].

[42] Talens-Oliag, S. (2019). *Introducción a los certificados digitales*. 1st ed. [ebook] Valencia: InfoCentre (http://www.infocentre.gva.es/), pp.1-2. Available at: https://www.uv.es/sto/49rtículos/BEI-2003-11/certificados_digitales.pdf [Accessed 31 Aug. 2019].

[43] Techopedia.com. (2019). *What is a Flag? – Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/3796/flag [Accessed 31 Aug. 2019].

[44] UPV (2019). *Arquitectura del software multicapa*. [video] Available at: https://www.youtube.com/watch?v=kHvxX1E9vIU [Accessed 29 Aug. 2019].

[45] Geary, D. (2003). *Java Design Patterns – How to navigate the deceptively simple Singleton pattern*. [online] JavaWorld. Available at: https://www.javaworld.com/article/2073352/core-java-simply-singleton.html [Accessed 29 Aug. 2019].

[46] Erik Gostischa-Franta, J. (2013). *Model View Controller Pattern*. [online] Best-practice Software Engineering. Available at: http://best-practice-software-engineering.ifs.tuwien.ac.at/patterns/mvc.html [Accessed 31 Aug. 2019].

[47] M. H. Reenskaug, T. (2019). *Trygve Home Page*. [online] Heim.ifi.uio.no. Available at: http://heim.ifi.uio.no/~trygver/ [Accessed 31 Aug. 2019].

[48] Servicio de Informática (Universidad de Alicante). (2019). *Modelo vista controlador (MVC).*. [online] Available at: https://si.ua.es/es/documentacion/asp-net-mvc-3/1-dia/modelo-vista-controlador-mvc.html [Accessed 31 Aug. 2019].

[49] En.wikipedia.org. (2019). *MVC-Process.svg*. [online] Available at: https://en.wikipedia.org/wiki/File:MVC-Process.svg [Accessed 31 Aug. 2019].

[50] martinfowler.com. (2019). *Continuous Integration*. [online] Available at: https://www.martinfowler.com/articles/continuousIntegration.html [Accessed 5 Dec. 2019].

[51] Thoughtworks.com. (2019). *Continuous integration | ThoughtWorks*. [online] Available at: https://www.thoughtworks.com/continuous-integration [Accessed 5 Dec. 2019].

[52] GeeksforGeeks. (2019). *Software Testing | Basics – GeeksforGeeks*. [online] Available at: https://www.geeksforgeeks.org/software-testing-basics/ [Accessed 6 Dec. 2019].

[53] Ecured.cu. (2019). *Metodología de desarrollo iterativo y creciente - EcuRed*. [online] Available at: https://www.ecured.cu/Metodolog%C3%ADa_de_desarrollo_iterativo_y_creciente [Accessed 6 Dec. 2019].

[54] Es.wikipedia.org. (2019). *Red de área local*. [online] Available at: https://es.wikipedia.org/wiki/Red_de_%C3%A1rea_local#/media/Archivo:Ethernet_LAN.svg [Accessed 28 Aug. 2019].

[55] Cisco (2019) CCNA RS_NB – Chapter 3, [online] Available at: https://www.slideshare.net/kazhuyo/nb-instructor-pptchapter3 [Accessed 29 Aug. 2019].

[56] Cutanda, D. (2019). *Fundamentos sobre Certificados Digitales - El estándar X.509 y estructura de certificados - Security Art Work*. [online] Security Art Work. Available at: https://www.securityartwork.es/2014/04/07/fundamentos-sobre-certificados-digitales-el-estandar-x-509-y-estructura-de-certificados/ [Accessed 7 Dec. 2019].