

Escuela

Politécnica

Superior

Gala M. Ga

MINISTERIO DE DEFENSA | [Dirección de la compañía]

C:\Users\Gala\Documents\TFG\universidad.png

Autor:

Roberto André Vega Guardado

Tutores:

Sergio Orts Escolano

Septiembre 2018

Trabajo Fin de Grado

Implementación de una plataforma online segura para su uso en telemedicina

grado en ingeniería informática

**Agradecimientos**

A mi tutor por todo el tiempo dedicado

para que el proyecto saliera adelante.

Y a mi compañera por todo el apoyo

y por acompañarme durante el largo trayecto.

**Motivación**

El motivo principal para emprender este proyecto era el de desarrollar un sistema seguro. Y así poder poner en practica los conocimientos de seguridad informática adquiridos en la carrera. Así surgió la idea de un sistema de telemedicina, donde los datos con los que se trabaja son muy importantes/sensibles y tienen que estar protegidos en todo momento.

Se fue desarrollando esa idea inicial hasta llegar al sistema planteado en este proyecto, un sistema online seguro para su uso en telemedicina. Con el objetivo de aportar un sistema donde se garantice la seguridad de los datos de los usuarios y además proporcionar una ayuda en la comunicación entre médico y paciente, es decir, proporcionar otra alternativa a que una persona acuda presencialmente a visitar a un médico, ya que mucha gente no tiene tantas facilidades para ello.

Personalmente opino que es una idea muy interesante con futuro para seguir desarrollándola, y que tarde o temprano acabaremos utilizando sistemas similares, tanto para facilitar el trabajo al médico como para comodidad personal nuestra.

**Índice de contenido**

[1. Introducción 9](#_Toc523913033)

[2. Objetivos 10](#_Toc523913034)

[2.1 Objetivos específicos 10](#_Toc523913035)

[2.2 Relación con asignaturas 11](#_Toc523913036)

[3. Estado del arte 12](#_Toc523913037)

[3.1 Sistemas similares 15](#_Toc523913038)

[3.1.1 Médicos y pacientes 15](#_Toc523913039)

[3.1.2 Policlínica IUMET 16](#_Toc523913040)

[3.1.3 Vida 16](#_Toc523913041)

[3.1.4 Sanitas 17](#_Toc523913042)

[3.1.5 Atrys 17](#_Toc523913043)

[3.1.6 HealthTap 18](#_Toc523913044)

[4. Materiales y métodos 19](#_Toc523913045)

[4.1 Herramientas y tecnologías software 19](#_Toc523913046)

[4.1.1 Documentación 19](#_Toc523913047)

[4.1.2 Diseño 19](#_Toc523913048)

[4.1.3 Desarrollo 19](#_Toc523913049)

[4.2 Herramientas Hardware 21](#_Toc523913050)

[4.3 Planificación 22](#_Toc523913051)

[4.3.1 Trello 23](#_Toc523913052)

[4.3.2 Diagrama de Gant 24](#_Toc523913053)

[5. Especificación de requisitos 27](#_Toc523913054)

[5.1 Casos de uso 27](#_Toc523913055)

[5.2 Requisitos funcionales 35](#_Toc523913056)

[5.3 Requisitos no funcionales 38](#_Toc523913057)

[6. Diseño y arquitectura 40](#_Toc523913058)

[6.1 Prototipo temprano 40](#_Toc523913059)

[6.2 Diagrama de clases 48](#_Toc523913060)

[6.3 Diagrama entidad relación 49](#_Toc523913061)

[6.4 Diseño final 50](#_Toc523913062)

[6.5 Arquitectura 58](#_Toc523913063)

[7. Seguridad 59](#_Toc523913064)

[7.1 Servidor 59](#_Toc523913065)

[7.2 Cliente 62](#_Toc523913066)

[8. Implementación 63](#_Toc523913067)

[8.1 API 63](#_Toc523913068)

[8.1.1 Login y registro 64](#_Toc523913069)

[8.1.2 Historial 64](#_Toc523913070)

[8.1.3 Consultas 65](#_Toc523913071)

[8.1.4 Mensajes 65](#_Toc523913072)

[8.1.5 Citas 66](#_Toc523913073)

[8.2 Cliente 67](#_Toc523913074)

[8.3 Registro y login 68](#_Toc523913075)

[8.4 Inicio 69](#_Toc523913076)

[8.5 Historial 69](#_Toc523913077)

[8.6 Consultas 70](#_Toc523913078)

[8.7 Cita 70](#_Toc523913079)

[8.8 Mensajes 71](#_Toc523913080)

[9. Conclusiones 73](#_Toc523913081)

[9.1 Revisión de objetivos 73](#_Toc523913082)

[9.2 Trabajos futuros 74](#_Toc523913083)

[10. Bibliografía 76](#_Toc523913084)

**Índice de Figuras**

[Ilustración 1: Tasa de uso de internet por países (We Are Social, 2018). 12](#_Toc524007355)

[Ilustración 2: Tablero de Trello con el estado del proyecto 24](#_Toc524007356)

[Ilustración 3: Timeline 26](#_Toc524007357)

[Ilustración 4: Diagrama de caso de uso 1 28](#_Toc524007358)

[Ilustración 5: Diagrama de caso de uso 2 28](#_Toc524007359)

[Ilustración 6: Diagrama de caso de uso 3 29](#_Toc524007360)

[Ilustración 7: Diagrama de caso de uso 4 29](#_Toc524007361)

[Ilustración 8: Diagrama de caso de uso 5 30](#_Toc524007362)

[Ilustración 9: Mockup login 41](#_Toc524007363)

[Ilustración 10: Mockup registro médico 42](#_Toc524007364)

[Ilustración 11: Mockup registro paciente 43](#_Toc524007365)

[Ilustración 12: Mockup inicio 44](#_Toc524007366)

[Ilustración 13: Mockup pedir cita 44](#_Toc524007367)

[Ilustración 14: Mockup mensajes 45](#_Toc524007368)

[Ilustración 15: Mockup historial 45](#_Toc524007369)

[Ilustración 16: Mockup ver consulta 46](#_Toc524007370)

[Ilustración 17: Mockup nueva consulta 47](#_Toc524007371)

[Ilustración 18: Diagrama de clases 48](#_Toc524007372)

[Ilustración 19: Diagrama entidad relación 49](#_Toc524007373)

[Ilustración 20: Login 50](#_Toc524007374)

[Ilustración 21: Registro 51](#_Toc524007375)

[Ilustración 22: Confirmación de login 51](#_Toc524007376)

[Ilustración 23: Inicio 52](#_Toc524007377)

[Ilustración 24: Nueva cita 53](#_Toc524007378)

[Ilustración 25: Ver citas 53](#_Toc524007379)

[Ilustración 26: Historial según la vista del médico 54](#_Toc524007380)

[Ilustración 27: Historial y consultas 55](#_Toc524007381)

[Ilustración 28: Ver consulta 55](#_Toc524007382)

[Ilustración 29: Nueva consulta 56](#_Toc524007383)

[Ilustración 30: Historial (paciente) 56](#_Toc524007384)

[Ilustración 31: Mensajes (enviados) 57](#_Toc524007385)

[Ilustración 32: Nuevo mensaje 57](#_Toc524007386)

[Ilustración 33: Arquitectura cliente-servidor (dos capas) 58](#_Toc524007387)

[Ilustración 34: Estructura del proyecto (cliente) 67](#_Toc524007388)

**Índice de tablas**

[Tabla 1: Ventajas e inconvenientes de la telemedicina 14](#_Toc523820240)

[Tabla 2: Entorno de producción (juniper.net) 22](#_Toc523820241)

[Tabla 3: Grupo de tareas del servidor 25](#_Toc523820242)

[Tabla 4: Grupo de tareas del cliente 25](#_Toc523820243)

[Tabla 5: Grupo de tareas memoria 25](#_Toc523820244)

[Tabla 6: Caso de uso 1 31](#_Toc523820245)

[Tabla 7: Caso de uso 2 32](#_Toc523820246)

[Tabla 8: Caso de uso 3 33](#_Toc523820247)

[Tabla 9: Caso de uso 4 34](#_Toc523820248)

[Tabla 10: Caso de uso 5 34](#_Toc523820249)

[Tabla 11: Requisito funcional 1 35](#_Toc523820250)

[Tabla 12: Requisito funcional 2 35](#_Toc523820251)

[Tabla 13: Requisito funcional 3 36](#_Toc523820252)

[Tabla 14: Requisito funcional 4 36](#_Toc523820253)

[Tabla 15: Requisito funcional 5 36](#_Toc523820254)

[Tabla 16: Requisito funcional 6 37](#_Toc523820255)

[Tabla 17: Requisito funcional 7 37](#_Toc523820256)

[Tabla 18: Requisito funcional 8 37](#_Toc523820257)

[Tabla 19: Requisito funcional 9 37](#_Toc523820258)

[Tabla 20: Requisito funcional 10 38](#_Toc523820259)

[Tabla 21: Requisito no funcional 1 38](#_Toc523820260)

[Tabla 22: Requisito no funcional 2 39](#_Toc523820261)

[Tabla 23: Requisito no funcional 3 39](#_Toc523820262)

[Tabla 24: Requisito no funcional 4 40](#_Toc523820263)

# Introducción

Las Tecnologías de la Información y Comunicación aplicadas a la atención en salud han impactado positivamente en el sector salud a nivel mundial en las últimas décadas. Cada vez es más notable el interés por la Telemedicina, una innovación que posiblemente jugará un papel importante en la evolución y transformación del sistema sanitario en los próximos años. El empleo de telemedicina puede solucionar problemas como el aumento de la demanda de servicios de salud o la necesidad de gestionar grandes cantidades de información (ehCOS, 2018).

En la actualidad gracias a los avances tecnológicos, un gran número de personas tiene acceso a Internet mediante un ordenador o un dispositivo móvil, lo que posibilita la telemedicina, pero con ello también aumenta el riesgo de que estas personas sufran robo de información y sus datos personales se vean comprometidos. Esto no solo afecta al usuario sino también a las empresas, la ciberseguridad se ha convertido en uno de los mayores retos que afrontan las organizaciones, sea cual sea su tamaño. Una mala gestión de la seguridad informática puede tener tanto impacto económico, como afectar a la reputación y la confianza de socios y clientes.

Por eso es importante proporcionar un sistema que garantice la seguridad de los datos del usuario y evitar en máxima medida que se vean comprometidos ante cualquier ataque. En el caso de la aplicación web de consulta telemática el factor de la seguridad cobra más importancia ya que se trabaja con datos sensibles como pueden ser el historial clínico de los usuarios o mensajes entre médico y paciente.

# Objetivos

## Objetivos específicos

El objetivo del trabajo es desarrollar un sistema de telemedicina seguro y de código abierto, que permita soportar la asistencia médica, independientemente de la distancia que separa a los que ofrecen el servicio, es decir, ofrecer una mejor comunicación entre médico y paciente sin la necesidad de que el paciente vaya a la consulta personalmente.

Además, el sistema también dispondrá de otras funcionalidades útiles para los profesionales sanitarios y los usuarios, como por ejemplo ver el historial clínico de un paciente y las correspondientes consultas anteriores, así como la posibilidad de crear nuevas. Tanto médicos como pacientes podrán crear una cita para acordar un día y una hora para una nueva consulta ya sea mediante videollamada o en persona si fuese necesario. También el personal sanitario podrá comunicarse con los pacientes mediante mensajes.

Al ser la seguridad uno de los principales objetivos, para la implementación y el desarrollo de este sistema se tendrán en cuenta todos los aspectos relacionados con este tema. A la hora de acceder al sistema se dispondrá de un doble factor de autenticación, mediante contraseña y validación de un código enviado por correo electrónico. Con respecto a la persistencia de datos, se cifrarán todos los datos relevantes mediante algoritmos criptográficos antes de almacenarlo en la base de datos para garantizar la seguridad de estos. Y en cuanto a la comunicación y transferencia de los datos, el sistema utilizará protocolo HTTPS para el intercambio de información entre los usuarios/aplicación.

## Relación con asignaturas

En este apartado se describirá la relación y el conocimiento que han aportado algunas de las asignaturas, cursadas a lo largo de la carrera, al proyecto.

**Seguridad en el diseño software (SDS)**

En esta asignatura es donde se dan los principales conocimientos de seguridad informática aplicados en el proyecto: criptografía, cifrados, funciones hash, seguridad a nivel de transporte, *malware*, ataques…

**Aplicaciones distribuidas en internet (ADI)**

En ADI es donde se enseña el desarrollo de APIs REST utilizando el lenguaje JavaScript. Además, se aprende acerca sobre el desarrollo en la parte cliente con JavaScript estándar y con *frameworks*. Para el proyecto se han utilizado las tecnologías usadas en esta asignatura tanto para el API como para la parte del cliente.

**Diseño de bases de datos (DBD)**

Los principales conocimientos de bases de datos aplicados en el proyecto se obtuvieron de esta asignatura. Poder diseñar un esquema entidad relación según los requisitos del sistema, creación de una base de datos desde cero…

**Análisis y especificación de sistemas software (AESS)**

En esta asignatura se aprende a realizar los diferentes diagramas del sistema, ya sean de clases, de casos de uso, de secuencia… Otro aspecto de la asignatura que se ha aplicado al proyecto es identificar y diferenciar los requisitos de la aplicación a desarrollar.

# Estado del arte

Hoy en día el uso de un dispositivo con acceso a internet es habitual dentro de la vida diaria de las personas. Cada vez es más habitual que las personas busquen comodidades o alternativas a través de la tecnología para facilitar hábitos de la vida cotidiana.

Según el informe del 2018 que presentan “*We Are Social”* y “*Hootsuite”* se destaca que Internet ha superado la cifra de los 4.000 millones de usuarios, lo que supone que más de la mitad de la población está conectada (We Are Social, 2018).



Ilustración 1: Tasa de uso de internet por países (We Are Social, 2018).

En concreto en España, los usuarios de Internet han aumentado en 2 millones, lo que supone ya el 85% de la población. Según el informe Sociedad Digital en España 2017 elaborado por la Fundación Telefónica detalla que el 98% de los jóvenes se conecta a diario a Internet, un porcentaje que en el caso de los adultos de entre 65 y 74 años es del 43,7% (Expansión, 2018). A este respecto, se añade que las personas mayores se están incorporando “con rapidez” a la sociedad digital, ya que su uso de Internet aumentó un 26% el último año (La Vanguardia, 2018).

Todo esto supone una facilidad para que la telemedicina sea una alternativa factible en el ámbito de la salud, ya que es un recurso tecnológico que posibilita la optimización de los servicios de atención en salud, ahorrando tiempo y dinero y facilitando el acceso a zonas distantes para tener atención de especialistas. Factores como la alta dispersión poblacional, las distancias y la escasez de especialistas en todas las áreas de la medicina dan pie a que la telemedicina hoy en día pueda desempeñar un papel fundamental en lo que concierne a la mejora sostenible de la salud de las comunidades, a nivel global.

Es una herramienta diseñada para el buen desempeño científico del personal de la salud, que no solucionará todos los problemas existentes en el sector sanitario y que en ningún caso pretende sustituir el criterio del médico tratante, pero que con la evolución de las nuevas tecnologías favorece la expansión y aplicación de los conceptos de globalidad e interoperabilidad en las organizaciones de salud, permitiendo e impulsando así entornos de organización y trabajo que van más allá de la aplicación de la telemedicina para la cobertura asistencial en zonas geográficamente remotas.

En la *Tabla 1* se puede observar un resumen de las ventajas y los inconvenientes de la telemedicina.

|  |  |
| --- | --- |
| Ventajas | Inconvenientes |
| Acorta las distancias entre especialista y paciente. | Escasa relación médico-paciente |
| Reducción de costes | Puede ser impersonal |
| Última tecnología al alcance de todos | La calidad de la información puede ser deficiente |
| Acceso a sitios remotos | Necesidad de capacitaciones adicionales |
| Educación continua más asequible | Calidad de la información de la salud incierta |
| Mejor comunicación entre los profesionales de la salud | La confidencialidad se puede ver comprometida |

Tabla 1: Ventajas e inconvenientes de la telemedicina

Según un articulo realizado por varios médicos de *ScienceDirect,* el mercado de la telemedicina, el llamado e-Healt y m-Healt, generó un volumen de negocio de más de 6000 millones de euros en 2015, según Jaime Hortelano, el consejero delegado de la consultora española CMC. La expansión de los dispositivos móviles ha establecido ya una base tecnológica para poder desarrollar rápidamente la telemedicina que muy pronto será un valor añadido de los servicios que ofrecen las aseguradoras (ScienceDirect, 2016).

Con respecto a la seguridad, hoy en día se ha vuelto un requisito indispensable para las empresas, debido a la cantidad de información sensible que viaja a través de Internet y a los ataques que impiden el normal funcionamiento del sistema. Por eso es importante proteger los datos de la manera más eficiente y usando las mejores prácticas de seguridad.

En este apartado destaca AES (Advanced Encryption Standard), ya que este método se considera muy seguro y eficiente, por eso se suele usar en varios protocolos y técnicas de transmisión como, por ejemplo, la protección WPA2 de las redes wifi.

Un motivo para la gran popularidad y propagación de este estándar de cifrado es el libre uso del método sin tarifas de licencia u otras limitaciones asociadas con la patente. Además, los requisitos referentes al hardware y al almacenamiento son relativamente bajos y es fácil de implementar (Rouse, 2017).

A continuación, dentro del mercado de las aplicaciones web y móviles, voy a analizar algunas de las aplicaciones de telemedicina más completas e interesantes.

## Sistemas similares

### Médicos y pacientes

“Médicos y pacientes” es una plataforma que permite a los usuarios acceder de forma segura y confidencial a su historial clínico y contactar con el medico telemáticamente entre otras funcionalidades (Médicos y pacientes, 2017).

Entre sus características hay que destacar:

* *Login* con clave o certificado digital
* Consulta de tarjeta sanitaria
* Consulta del centro de salud (mapa, números, etc.)
* Hospital de referencia
* Médico y enfermero de cabecera
* Citas electrónicas
* Ver historial clínico
* Datos de facturación farmacéutica
* Consulta online de determinadas dudas sobre su asistencia sanitaria (responde el médico)
* Ver información del paciente

### Policlínica IUMET

El Instituto Universitario de Medicina Telemática IUMET surge para dar a los Centros de Reconocimiento de Conductores (Politécnica IUMET, 2017). Entre sus servicios encontramos:

* Realizar consultas a los médicos especialistas de manera instantánea sobre las exploraciones psicofísicas a los conductores que acuden al Centro
* Obtener apoyo formativo que amplíe y afiance los conocimientos y habilidades de los facultativos del Centro de Reconocimiento
* Promover la investigación en el ámbito de la seguridad vial, a través de la coordinación y análisis de datos a gran escala
* Asesoramiento en adaptaciones para la conducción
* Teleoftalmología para Centros de Reconocimiento de Conductores
* Dispositivos de telecomunicación: dependiendo del tipo de telemedicina. el equipamiento puede estar compuesto por terminales telefónicos, estaciones de videoconferencia (como *tablets* con webcam incorporada u ordenadores con webcam externa)

### Vida

Vida es una aplicación para realizar consultas médicas a través de una videollamada directamente en la aplicación, en la que médicos experimentados y colegiados ofrecen ayuda médica y si es necesario, pueden prescribir una receta (Vida, 2017).

Entre sus características tenemos:

* Video consultas para:
  + Preocupaciones generales de salud
  + Alergias
  + Asma
  + Infecciones sinusales
  + Herpes labial
  + Resfriados
  + Infección del tracto urinario
* Reservar citas para la videoconsulta
* La primera consulta es gratis, después cada una tiene un coste de 10€
* El médico podrá recetar
* Es el doctor el que inicia la llamada
* Las consultas no tienen límite de tiempo

### Sanitas

La plataforma de sanitas dedicada a la telemedicina se llama BLUA, con ella puedes conectar los médicos y realizar consultas online con especialistas. Mediante la videoconsulta a través de un portátil, tablet o móvil ofrecen una atención médica personalizada (Sanitas, 2016).

Entre los servicios que ofrecen se encuentran:

* Cobertura de farmacia: reembolso del 50% de los gastos de farmacia.
* Cobertura en EE. UU
* Cobertura de reembolso 50.000: permiten acceder a un especialista que, aunque no esté en su cuadro médico y te reembolsan el 80% de los gastos médicos.
* Analítica a domicilio: reembolso de los gastos del personal de laboratorio a domicilio para mayor comodidad.
* Envío de medicamentos a domicilio.
* Asesor medico
* Programa de psicología y de nutrición

### Atrys

Atrys es una compañía biomédica dedicada a la prestación de servicios diagnósticos y tratamientos médicos de excelencia, cuyo objetivo es facilitar la terapia individualizada de los pacientes, así como el desarrollo de nuevas modalidades terapéuticas y herramientas diagnósticas (Atrys, 2018).

En el apartado de la telemedicina sus servicios en las especialidades médicas son:

* Radiología
* Cardiología
* Oftalmología
* Dermatología.

### HealthTap

HealthTap es una aplicación gratuita tanto para web como para móvil y algunas de sus características son las siguientes (HealthTap, 2017):

* Consultas virtuales con acceso las 24h a través de mensajes de voz, de texto o video.
* Posibilidad de que un especialista recete tratamientos al paciente
* recordatorios, listados
* Boletines personificados por doctores.
* Asesoramiento de especialistas

# Materiales y métodos

## Herramientas y tecnologías software

A continuación, se van a enumerar y describir brevemente las distintas herramientas software usadas para el desarrollo del sistema.

### Documentación

Para realizar la documentación y la planificación del proyecto se ha utilizado las siguientes herramientas:

* **Microsoft Word:** programa que ofrece creación de documentos y procesamiento de textos entre otras muchas características. Se ha usado para elaborar la memoria en su totalidad.
* **Monday:** es la herramienta que se ha utilizado para realizar la planificación del proyecto de una manera más visual, ya que permite crear grupos de tareas y ver el progreso con diagramas de tiempo, gráficos, calendarios, etc.

### Diseño

En el apartado de las herramientas de diseño que han intervenido en el desarrollo del sistema y de la documentación tenemos:

* **Draw.io:** es una aplicación de código abierto para la elaboración de diagramas de aplicaciones. Esta herramienta se ha utilizado para la mayoría de los diagramas del sistema, es decir, los diagramas de casos de uso, el diagrama de clases y para los prototipos tempranos.

### Desarrollo

Entre las herramientas comunes para el desarrollo del sistema, tanto del API, como de la parte del cliente web y de la base de datos, están las siguientes:

* **Git:** es un software de control de versiones para proyectos, que permite llevar un registro de los cambios realizados y así poder coordinar el trabajo con otras personas.
* **GitHub:** es una plataforma para alojar proyectos usando el sistema de control de versiones Git.

Para la parte del API y de la gestión de la base de datos se ha hecho uso de las siguientes tecnologías:

* **Visual Studio Code:** es un editor de código fuente gratuito y de código abierto desarrollado por Microsoft. Incluye soporte para la depuración, control integrado de Git, resaltado de sintaxis, finalización inteligente de código, fragmentos y refactorización de código (Wikipedia, 2018).
* **NodeJS:** es un entorno en tiempo de ejecución multiplataforma, de código abierto, para la capa del servidor que ejecuta código JavaScript fuera del navegador. Está basado en el lenguaje de programación ECMAScript, asíncrono y orientado a eventos, lo que lo hace útil para la creación de servidores web (Abernethy, 2011).
* **JavaScript:** lenguaje de programación interpretado orientado a objetos y basado en prototipos, el cual se utiliza tanto en la parte del servidor como en la del cliente.
* **ExpressJS:** es un *framework* para NodeJS de código abierto, proporciona métodos de utilidad para HTTP y *middleware*.
* **Postman:** es un programa multiplataforma utilizado para el desarrollo de APIs, ya que permite ejecutar peticiones, hacer pruebas, depurar, crear pruebas automatizadas y documentar un API. En el proyecto se ha utilizado también para documentar las peticiones junto con sus respuestas para tener la información en línea.
* **MySQL:** es un sistema de gestión de bases de datos relacional, gracias a su rendimiento, confiabilidad y facilidad de uso se ha convertido en el principal sistema de bases de datos en el mundo.
* **MySQLWorkbench:** es una herramienta visual unificada para arquitectos de bases de datos, desarrolladores y DBA. MySQL Workbench proporciona modelado de datos, desarrollo de SQL y herramientas integrales de administración para la configuración del servidor, administración de usuarios, respaldo y mucho más (MySQL, 2018).

Para la parte del cliente se han usado tecnologías comunes a la parte del API como son Visual Studio como editor de código y JavaScript como lenguaje. El resto de las herramientas son:

* **ReactJS:** es una librearía de JavaScript para crear interfaces de usuario interactivas basada en componentes que encapsulan un comportamiento, una vista y un estado, lo que proporciona facilidad de mantenimiento, depuración y escalabilidad.
* **Webpack:** es un paquete de módulos para JavaScript de código abierto, su principal objetivo es agrupar los archivos de JavaScript con sus dependencias y genera archivos estáticos para su uso en un navegador, pero también es capaz de transformar, agrupar o empaquetar.

## Herramientas Hardware

Para el correcto funcionamiento del sistema no es necesario hardware adicional aparte del servidor. La primera opción es tener alojado el API en un PaaS (*Plataform as a service*), lo que permite la automatización del ciclo de vida, configuración, despliegue y escalado de software, sin la complejidad de comprar, crear o administrar toda la infraestructura necesaria. La segunda opción es montar esa infraestructura por nuestra cuenta, en ese caso, en un entorno de producción un servidor *NodeJS* debería de tener las siguientes características:

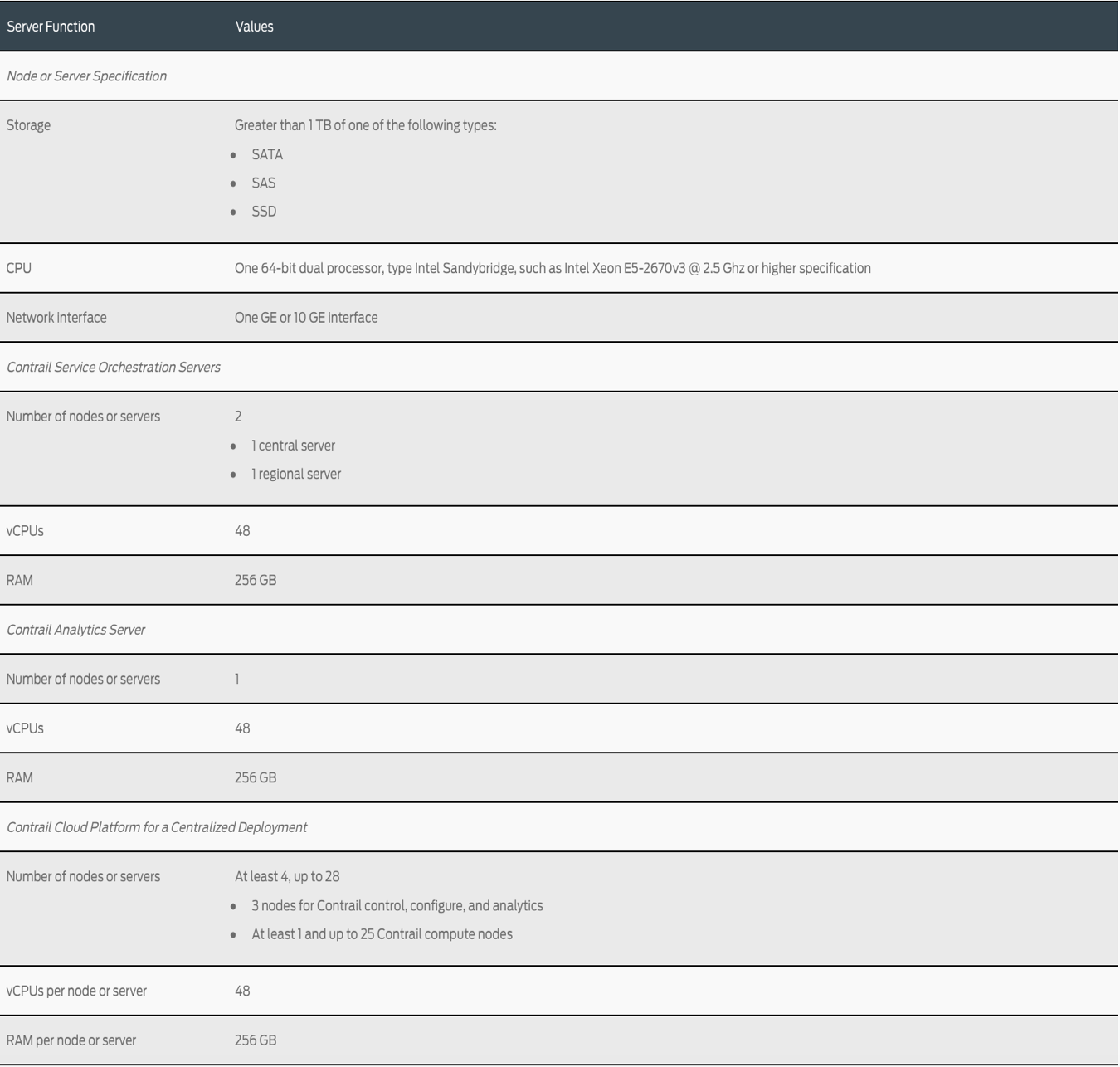


Tabla 2: Entorno de producción (Juniper, 2017)

## Planificación

Para la planificación del proyecto, se optó por dividir el proyecto en tres partes diferenciadas:

* API
* Cliente
* Documentación

A continuación, se explicará cómo se ha gestionado esta planificación y qué herramientas se han utilizado para ello.

### Trello

Para llevar la gestión de estas tres partes se ha utilizado la herramienta **Trello**, que resumidas cuentas es una plataforma para la administración de proyectos. En ella se ha creado un tablero del proyecto global con las tres partes, cada parte se diferencia con una etiqueta con un color diferente. Tenemos que las tareas etiquetadas con el color azul pertenecen a la parte del API, las de color rojo a la parte del cliente y las de color verde para la parte de la documentación.

En el tablero (*Ilustración 2*) se optó por poner cuatro columnas:

* Listado de tareas: aquí es donde están las tareas pendientes.
* En desarrollo: aparecen las tarjetas con las tareas que se están desarrollando y están en proceso.
* Pruebas: es la columna donde aparecen las tarjetas con las tareas que se han terminado, pero no se han probado en profundidad.
* Terminado: es la columna donde están las tareas terminadas.

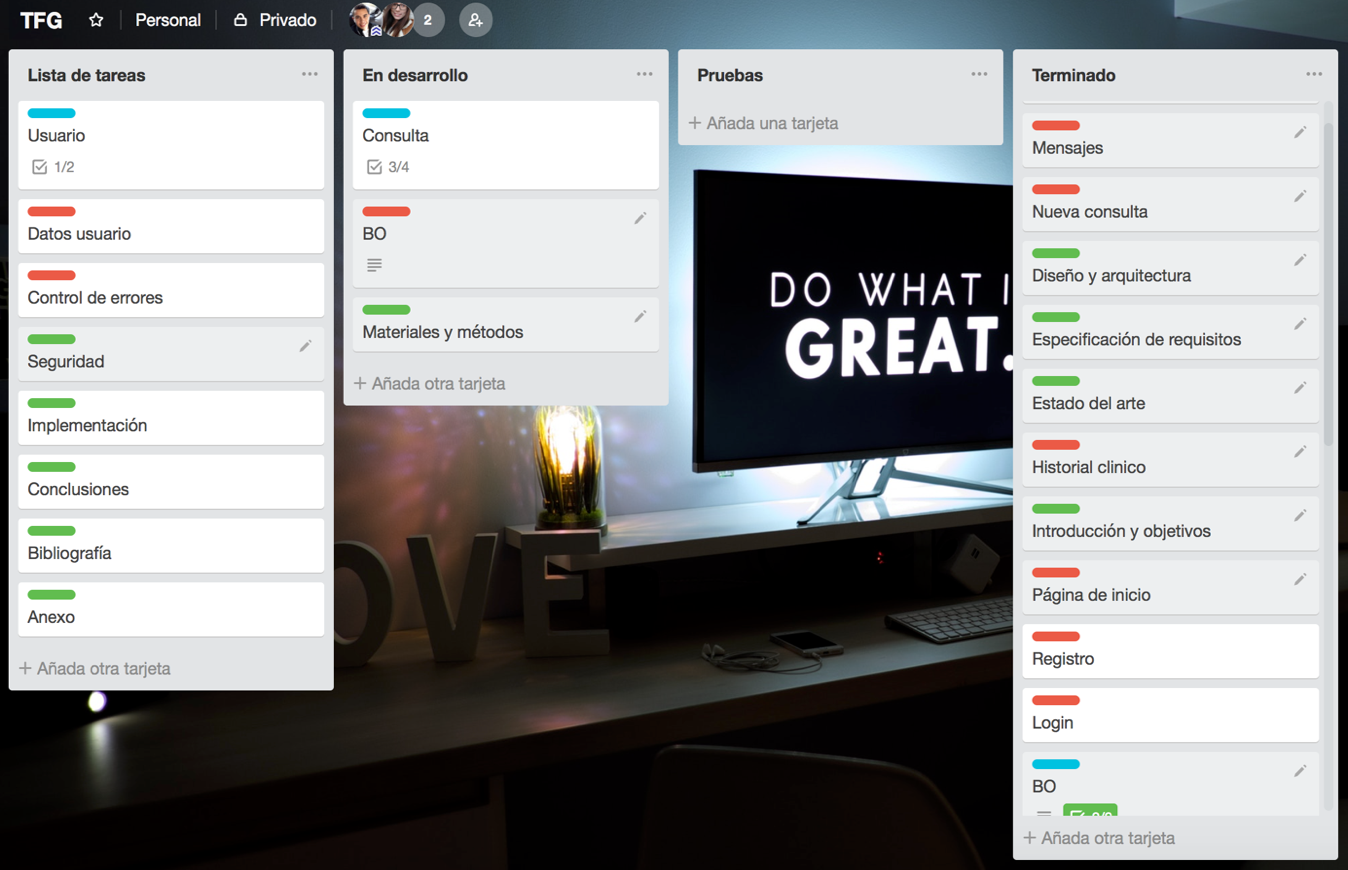
****

Ilustración 2: Tablero de Trello con el estado del proyecto

Cada parte del proyecto a su vez se ha dividido en elementos más pequeños, estos elementos son los llamados “historias de usuario”. Estas historias se han dividido en tareas mas pequeñas dentro de cada tarjeta utilizando los “checklist” que proporciona Trello.

En la *Ilustración 3* podemos observar que en la columna de en desarrollo coinciden tareas de las 3 partes, debido a que se ha intentado desarrollar las tres partes a la vez, aunque al principio se le diera más prioridad a desarrollar el API, por eso en la imagen la mayoría de las tareas asignadas al API están en la columna terminado.

### Diagrama de Gant

Para poder ver una planificación más visual del proyecto se ha utilizado un diagrama de Gantt, es una herramienta gráfica cuyo objetivo es planificar y exponer el tiempo de dedicación previsto para las diferentes tareas a lo largo de un tiempo total determinado.

Para la realización del diagrama se ha usado la herramienta de Monday, la cual permite crear tableros de muchas temáticas y observar el progreso con distintos tipos de vistas. Para el proyecto se optó por crear tres grupos: servidor, cliente y memoria.

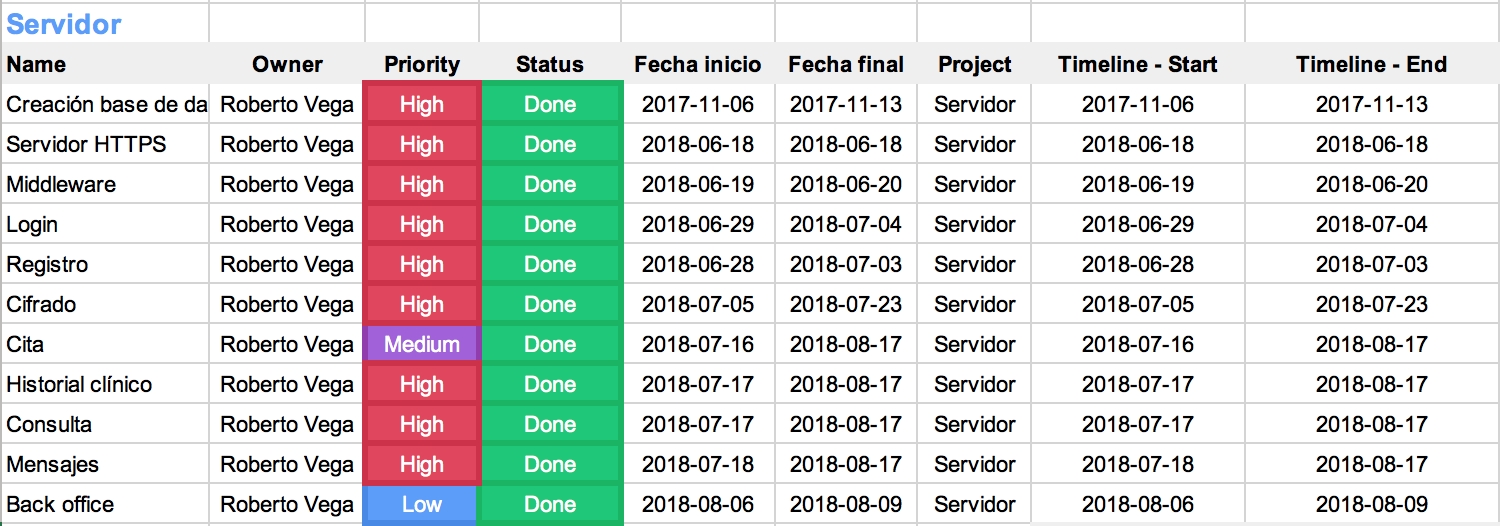


Tabla 3: Grupo de tareas del servidor

En la *Tabla 3* podemos observar el grupo de tareas del servidor, en ella aparecen el nombre de las tareas, el que las ha realizado, la prioridad de cada tarea y la fecha de inicio y final de cada una.

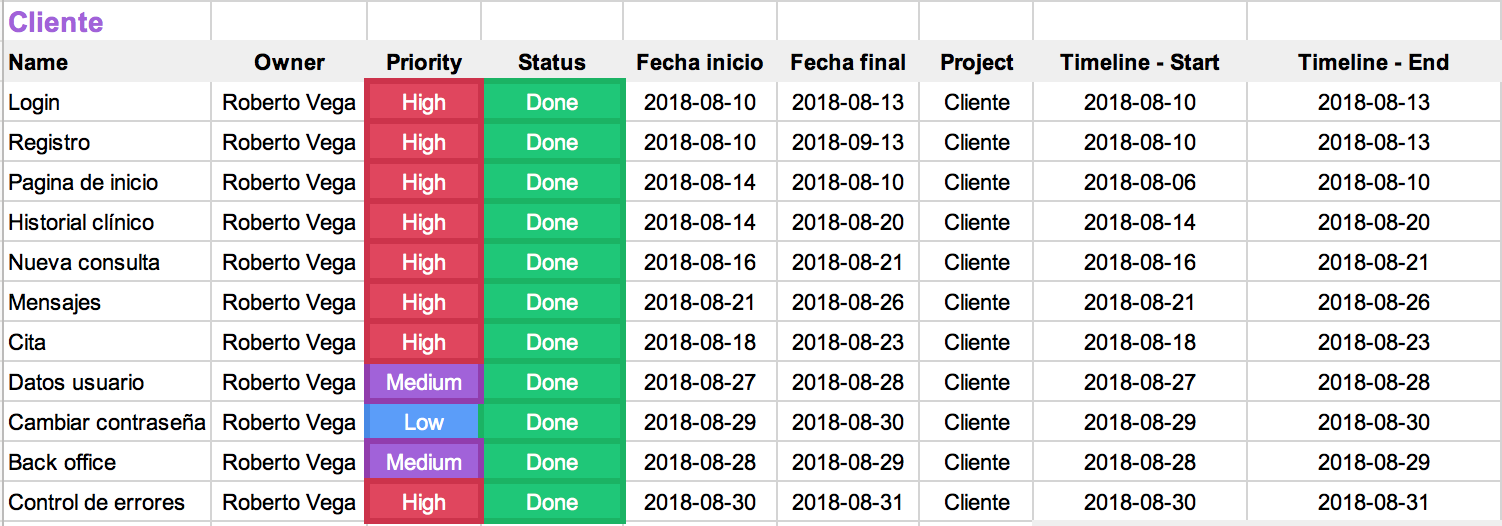


Tabla 4: Grupo de tareas del cliente

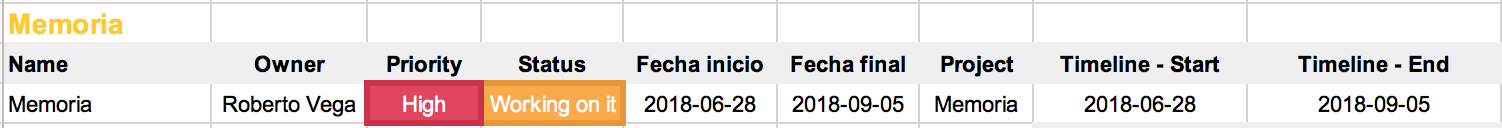


Tabla 5: Grupo de tareas memoria

En la *Tabla 4* tenemos las tareas de la parte del servidor con la misma información que en la del servidor. La diferencia está en la *Tabla 5* que, como se puede observar, se ha optado por poner solo una tarea que generaliza todo el apartado de la documentación.

Finalmente, en la *Ilustración 3* podemos observar el progreso general de las tareas de los tres grupos.

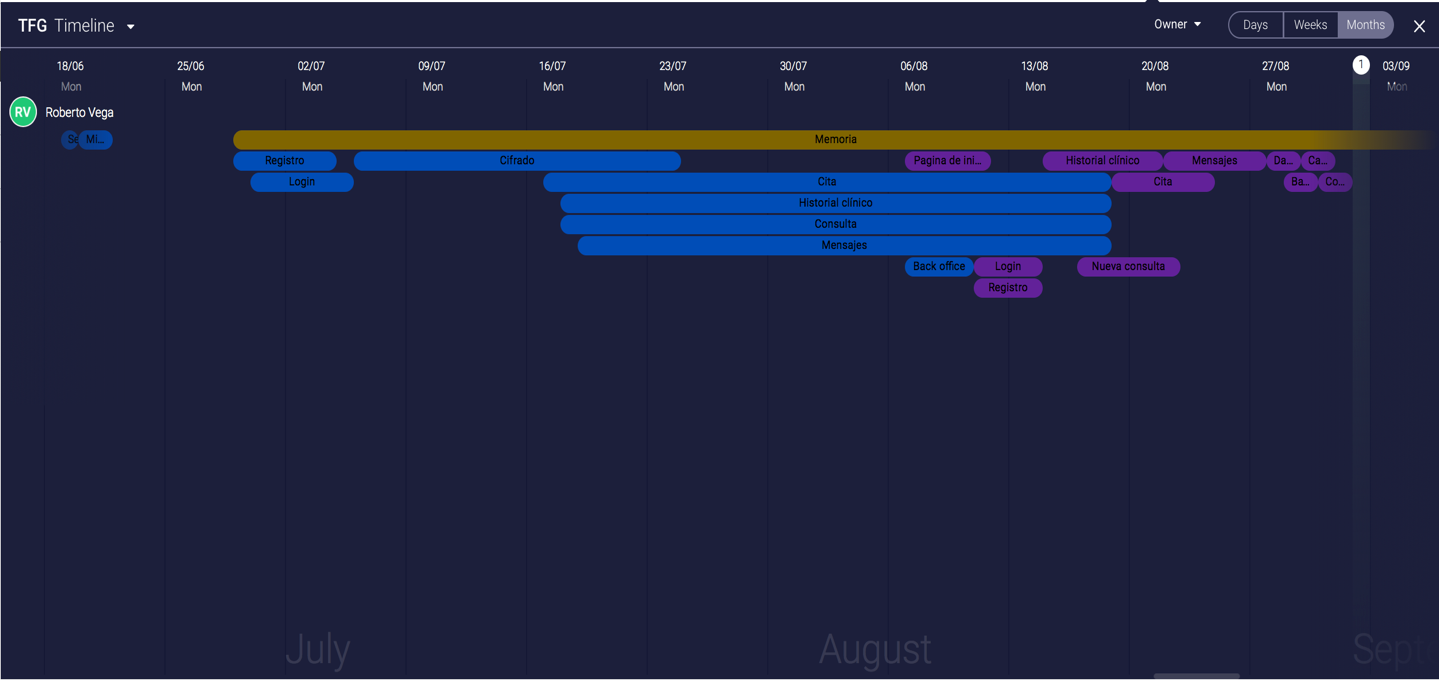


Ilustración 3: Timeline

Mirando la imagen podemos observar la secuencia del desarrollo del proyecto que se ha seguido. Al no haber seguido un desarrollo continuo, en el diagrama falta la primera tarea que es la de “creación de base de datos”, que como podemos ver en la *Tabla 3* se hizo al principio, mucho antes que el resto de las tareas es por eso por lo que no aparece en el diagrama de la *Ilustración 3,* donde solo aparece un rango de fechas. Las tareas aparecen según el color del grupo en el que estén: las azules pertenecen al servidor, las violetas a la parte del cliente y, por último, la tarea general de la documentación que aparece en amarillo.

# Especificación de requisitos

El análisis de requisitos sirve para describir los requerimientos del sistema, es decir, los servicios que ha de ofrecer el sistema, la utilidad que van a tener esos servicios para el usuario y las restricciones asociadas a su funcionamiento. El principal objetivo es facilitar la comunicación entre cliente, usuario y desarrollador.

Esta especificación es importante para el futuro éxito del sistema, ya que unos requisitos mal formulados dan como resultado un producto deficiente y/o de poca calidad. El coste de arreglar un producto deficiente es mucho mayor que el coste de un buen análisis y especificación de requisitos.

## Casos de uso

Los diagramas de casos de uso muestran una descripción visual de los pasos que han de llevarse a cabo para realizar un proceso del sistema. El objetivo principal de los casos de uso es describir la manera en que se usará el sistema, es decir, detallar las funcionalidades esenciales y así mejorar la compresión del sistema para desarrolladores, usuarios finales y expertos del dominio.

Un caso de uso contiene una descripción textual de todas las maneras que los actores previstos podrían trabajar con el software o el sistema, es decir, muestran los pasos que el actor debe seguir para poder realizar con éxito una tarea.

En nuestro caso en el sistema intervienen tres actores. El médico que, aparte de las funciones que comparte con el paciente, puede ver el historial clínico con las consultas asociadas y crear nuevas consultas. El paciente puede ver el historial de citas, crear una nueva cita, ver sus datos del historial clínico y enviar mensajes a otro usuario. Y finalmente el administrador tiene las funciones de validar un nuevo médico registrado y añadir el historial clínico de un nuevo paciente registrado.

Los diagramas de casos de uso del sistema son los siguientes:

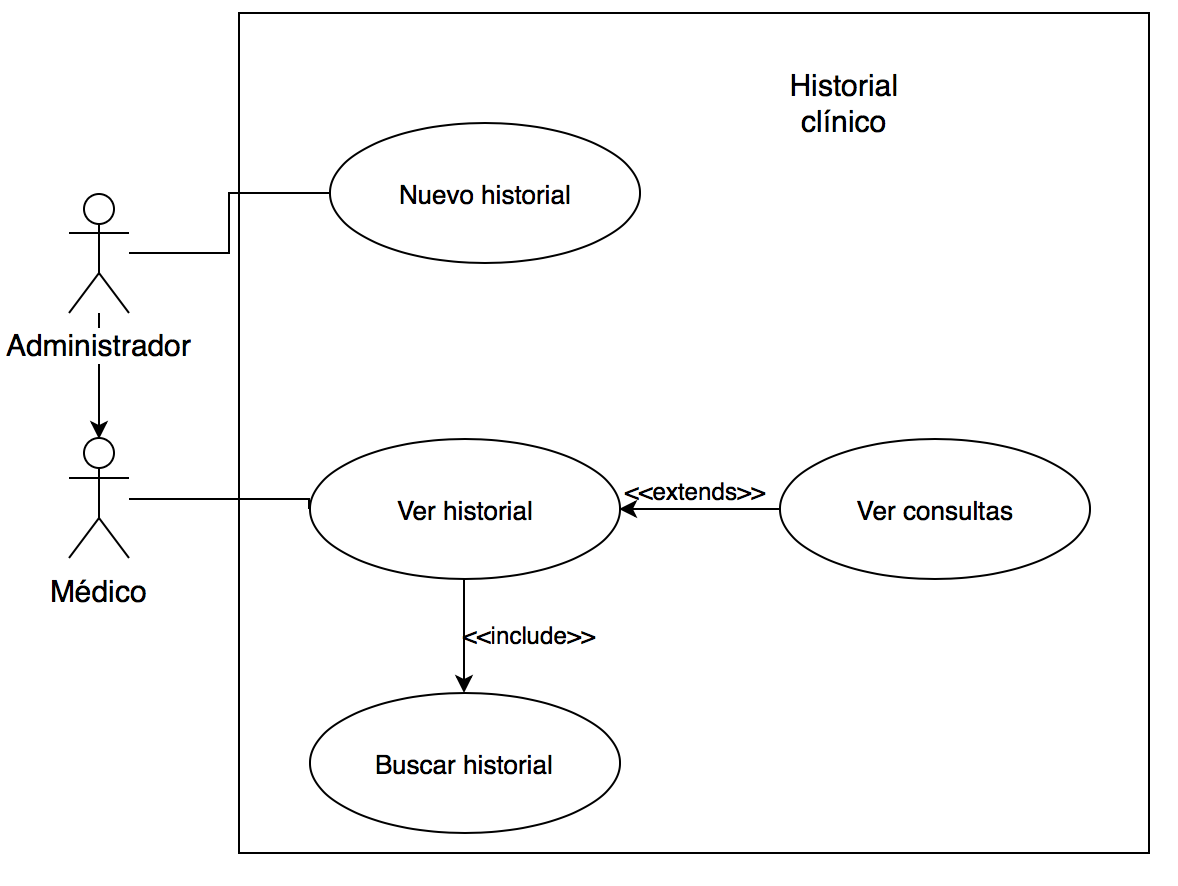


Ilustración 4: Diagrama de caso de uso 1

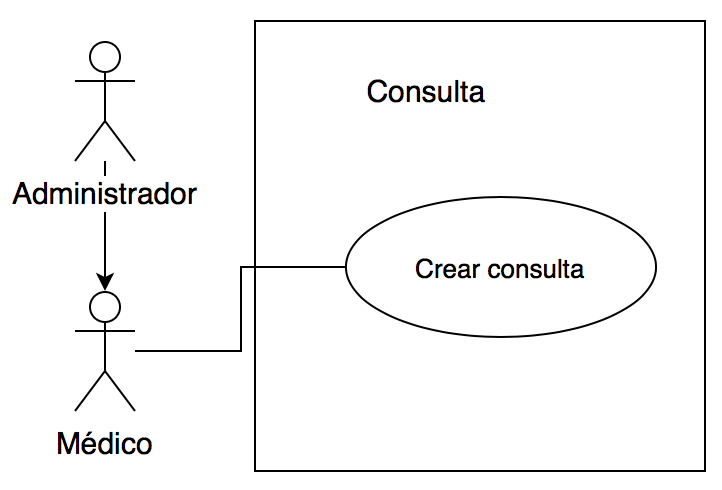


Ilustración 5: Diagrama de caso de uso 2

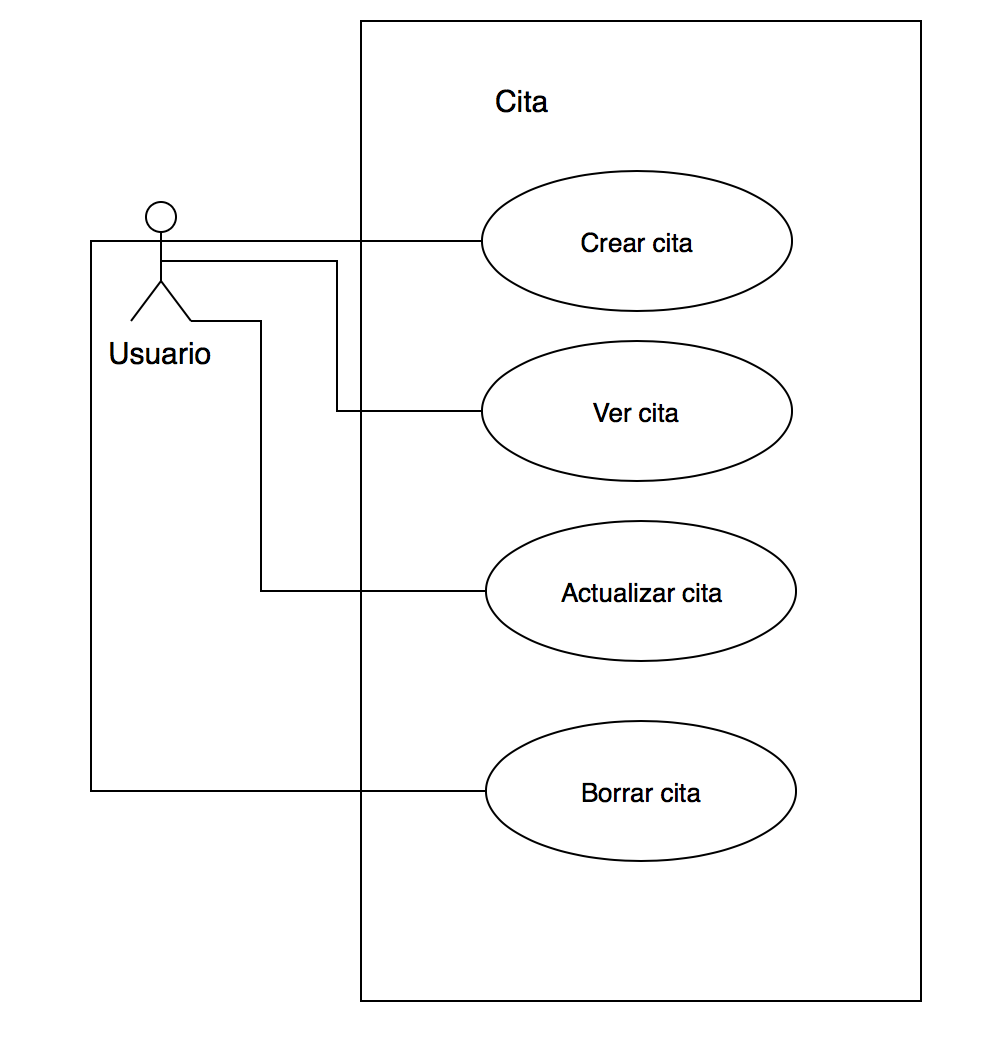


Ilustración 6: Diagrama de caso de uso 3

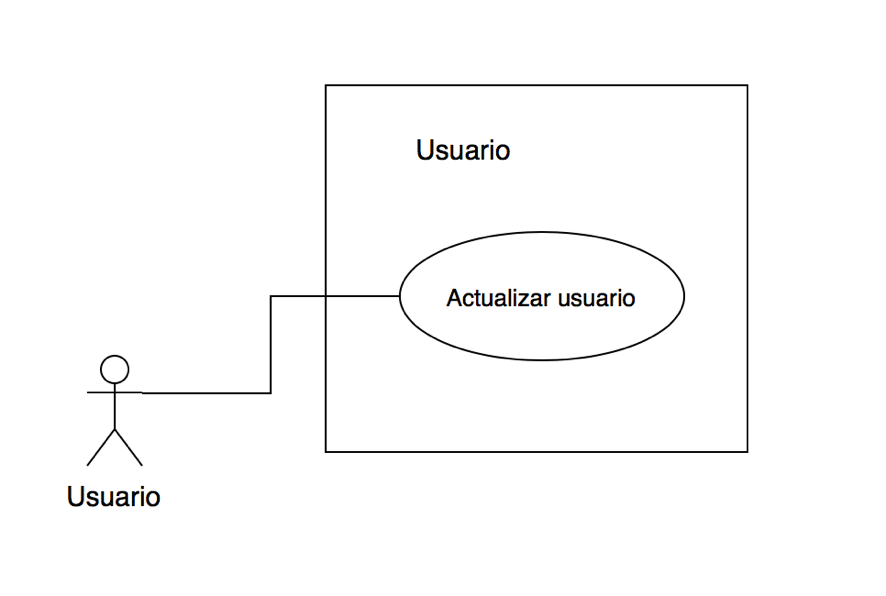


Ilustración 7: Diagrama de caso de uso 4

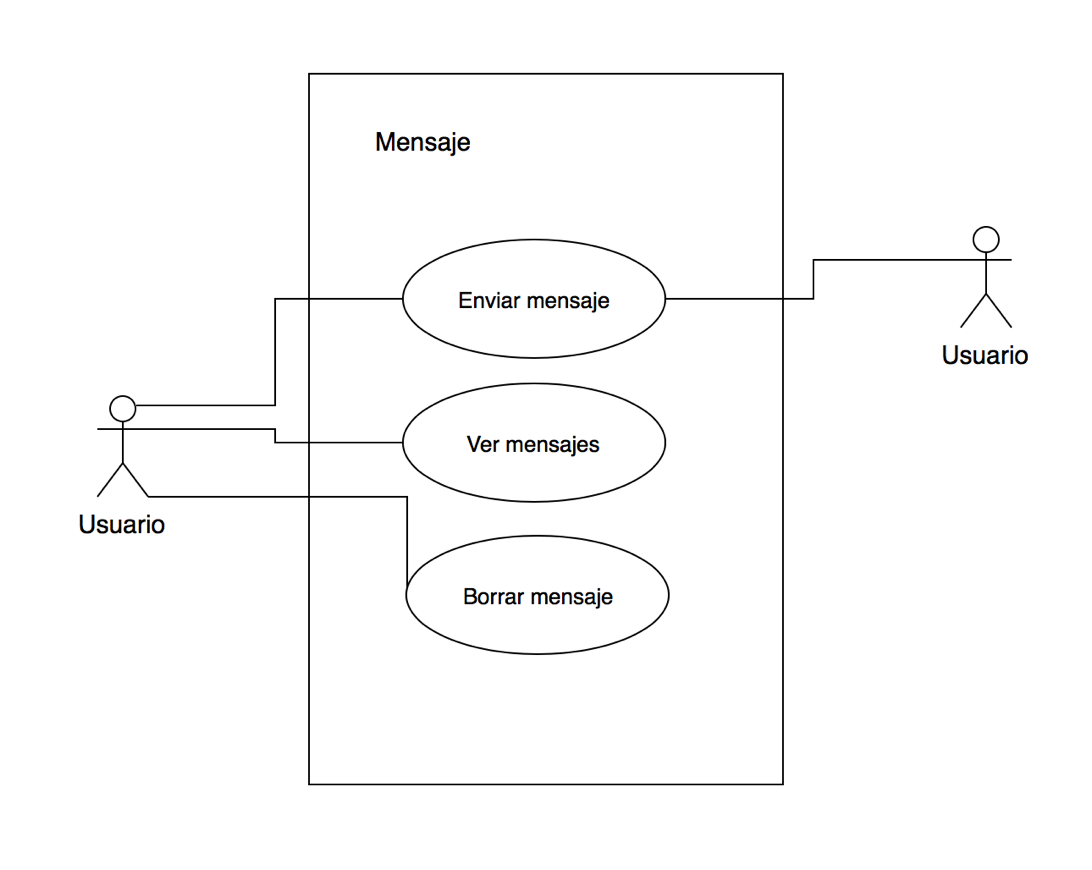


Ilustración 8: Diagrama de caso de uso 5

Los detalles de cada caso de uso se describen en su correspondiente tabla. En cada ellas podemos encontrar el título del caso de uso, el actor que realiza la tarea y el curso normal de la tarea especificando si algún paso de la secuencia se puede hacer de forma alternativa.

|  |  |
| --- | --- |
| Caso de uso | Ver el historial de un paciente |
| Actor | Médico |
| Curso normal | **Curso alternativo** |
| 1. El médico inicia sesión en el sistema. | 1.1 Si el médico no está registrado, se le informará que debe de hacerlo. |
| 2. El médico va al apartado de historial. |  |
| 3. El médico buscará la paciente según su SIP. |  |
| 4. El médico podrá ver el historial clínico y las consultas de ese paciente |  |

Tabla 6: Caso de uso 1

|  |  |
| --- | --- |
| Caso de uso | Añadir un nuevo historial |
| Actor | Administrador |
| Curso normal | **Curso alternativo** |
| 1. El administrador inicia sesión en el sistema. |  |
| 2. El administrador va al apartado de nuevo historial. |  |
| 3. El administrador introducirá los necesarios para el nuevo historial. |  |
| 4. El administrador guardará el nuevo historial. |  |

Tabla 7: Caso de uso 2

|  |  |
| --- | --- |
| Caso de uso | Nueva consulta |
| Actor | Médico |
| Curso normal | **Curso alternativo** |
| 1. El médico inicia sesión en el sistema. | 1.1 Si el médico no está registrado, se le informará que debe de hacerlo. |
| 2. El médico va al apartado del historial y luego al de nueva consulta. |  |
| 3. El médico introducirá los datos necesarios para la nueva consulta. |  |
| 4. El médico guardará la nueva consulta |  |

Tabla 8: Caso de uso 3

|  |  |
| --- | --- |
| Caso de uso | Citas |
| Actor | Médico y paciente |
| Curso normal | **Curso alternativo** |
| 1. El médico/paciente inicia sesión en el sistema. | 1.1 Si el médico/paciente no está registrado, se le informará que debe de hacerlo. |
| 2. El médico/paciente va al apartado de citas. |  |
| 3. El médico/paciente podrá ver las citas con la opción de filtrarlas según el tipo (videollamada o presencial), crear una nueva cita, actualizar y borrar una cita existente. |  |

Tabla 9: Caso de uso 4

|  |  |
| --- | --- |
| Caso de uso | Actualizar datos |
| Actor | Médico y paciente |
| Curso normal | **Curso alternativo** |
| 1. El médico/paciente inicia sesión en el sistema. | 1.1 Si el médico/paciente no está registrado, se le informará que debe de hacerlo. |
| 2. El médico/paciente va al apartado de mi cuenta y editar perfil. |  |
| 3. El médico/paciente tendrá la opción de cambiar su contraseña o su nombre y apellidos |  |

Tabla 10: Caso de uso 5

|  |  |
| --- | --- |
| Caso de uso | Mensajes |
| Actor | Médico y paciente |
| Curso normal | **Curso alternativo** |
| 1. El médico/paciente inicia sesión en el sistema. | 1.1 Si el médico/paciente no está registrado, se le informará que debe de hacerlo. |
| 2. El médico/paciente va al apartado de mensajes. |  |
| 3. El médico/paciente podrá ver sus mensajes recibidos o enviados, enviar uno nuevo o borrar alguno ya existente. |  |

Tabla 11: Caso de uso 6

## Requisitos funcionales

Los requerimientos funcionales son declaraciones de los servicios o funciones que proveerá el sistema, de la manera en que este reaccionará a entradas particulares. Una función es descrita como un conjunto de entradas, comportamientos y salidas.

A continuación, se muestran los requisitos funcionales del sistema mostrados en tablas, en ellas se muestra el nombre del requisito, una breve descripción y la prioridad de este.

|  |  |
| --- | --- |
| Nombre | Ver historial clínico |
| Descripción | Un médico podrá ver el historial clínico introduciendo la SIP de un paciente y con ello todas las consultas anteriores. |
| Prioridad | Alta |

Tabla 12: Requisito funcional 1

|  |  |
| --- | --- |
| Nombre | Crear una nueva consulta |
| Descripción | Un médico podrá crear una nueva consulta, rellenando un formulario con los datos necesarios, asociada al historial clínico de un paciente. |
| Prioridad | Alta |

Tabla 13: Requisito funcional 2

|  |  |
| --- | --- |
| Nombre | Pedir cita |
| Descripción | Un paciente o un médico podrá solicitar una cita en un día y una hora concretos. |
| Prioridad | Alta |

Tabla 14: Requisito funcional 3

|  |  |
| --- | --- |
| Nombre | Ver cita |
| Descripción | Un paciente o un médico podrá ver sus citas con la posibilidad de filtrarlas por el tipo de cita, ya sea videollamada o presencial. |
| Prioridad | Media |

Tabla 15: Requisito funcional 4

|  |  |
| --- | --- |
| Nombre | Actualizar cita |
| Descripción | Un paciente o un médico podrá actualizar la hora y el día de una cita ya existente. |
| Prioridad | Media |

Tabla 16: Requisito funcional 5

|  |  |
| --- | --- |
| Nombre | Borrar cita |
| Descripción | Un paciente o un médico podrá borrar una cita ya existente. |
| Prioridad | Media |

Tabla 17: Requisito funcional 6

|  |  |
| --- | --- |
| Nombre | Actualizar datos personales |
| Descripción | Un paciente o un médico podrá cambiar su contraseña o su nombre y apellidos. |
| Prioridad | Baja |

Tabla 18: Requisito funcional 7

|  |  |
| --- | --- |
| Nombre | Enviar un mensaje |
| Descripción | Un paciente o un médico podrán enviar un mensaje. |
| Prioridad | Alta |

Tabla 19: Requisito funcional 8

|  |  |
| --- | --- |
| Nombre | Ver mensajes |
| Descripción | Un paciente o un médico podrán ver sus mensajes recibidos o los enviados. |
| Prioridad | Alta |

Tabla 20: Requisito funcional 9

|  |  |
| --- | --- |
| Nombre | Borrar un mensaje |
| Descripción | Un paciente o un médico podrán borrar sus mensajes enviados. |
| Prioridad | Alta |

Tabla 21: Requisito funcional 10

## Requisitos no funcionales

Son aquellos requerimientos que no se refieren directamente a las funciones específicas que entrega el sistema, sino a las propiedades emergentes de este como la fiabilidad, la respuesta en el tiempo y la capacidad de almacenamiento. De forma alternativa, definen las restricciones del sistema como la capacidad de los dispositivos de entrada/salida y la representación de datos que se utiliza en la interfaz del sistema.

Los requisitos no funcionales también se muestran en tablas donde aparece el nombre, descripción y prioridad de cada requisito.

|  |  |
| --- | --- |
| Nombre | Seguridad |
| Descripción | * La aplicación al trabajar con datos muy sensibles debe garantizar la protección e integridad de esos datos. * El sistema debe trabajar con las implementaciones más actualizadas de algoritmos de cifrado para asegurarse que no tengan vulnerabilidades. |
| Prioridad | Alta |

Tabla 22: Requisito no funcional 1

|  |  |
| --- | --- |
| Nombre | Eficiencia |
| Descripción | * Toda funcionalidad del sistema y transacción de negocio debe responder al usuario en menos de 5 segundos. * Los datos modificados en la base de datos deben ser actualizados para todos los usuarios que acceden en menos de 2 segundos. |
| Prioridad | Alta |

Tabla 23: Requisito no funcional 2

|  |  |
| --- | --- |
| Nombre | Usabilidad |
| Descripción | * El sistema debe proporcionar mensajes de error que sean informativos y orientados a usuario final. * El sistema debe poseer interfaces gráficas intuitivas * La aplicación web debe poseer un diseño “responsive” a fin de garantizar la adecuada visualización en ordenadores, tablets y dispositivos móviles. |
| Prioridad | Alta |

Tabla 24: Requisito no funcional 3

|  |  |
| --- | --- |
| Nombre | Mantenibilidad |
| Descripción | El sistema estará desarrollado de tal forma de que se adapte bien al cambio, es decir, ante cualquier cambio, mejora o inclusión de nuevas funcionalidades en el sistema no conlleve mucho trabajo ni tiempo. |
| Prioridad | Alta |

Tabla 25: Requisito no funcional 4

# Diseño y arquitectura

El diseño es un parte fundamental de una aplicación web, puesto que la aplicación web es la parte del proyecto con la que va a interaccionar el usuario final. Por lo que tiene que ser intuitiva, fácil de usar y cumplir con sus expectativas.

A lo largo de este apartado se mostrarán los diagramas realizados para la futura implementación del diseño y las funcionalidades que el usuario final podrá disponer. Además, se muestra el diseño final y una explicación de la arquitectura del proyecto.

## Prototipo temprano

Los *mockups* son una representación visual y estática de un diseño. Aunque permitan una representación del diseño mas cercana a la realidad que otros prototipos no suponen un diseño final, si no mas bien una aproximación.

Los *mockups* no hacen referencia a todas las vistas de la web, solo a las principales para tener una idea de la estructura principal de la aplicación web. Por esto, si los comparamos con el diseño final podemos comprobar que existen variaciones.

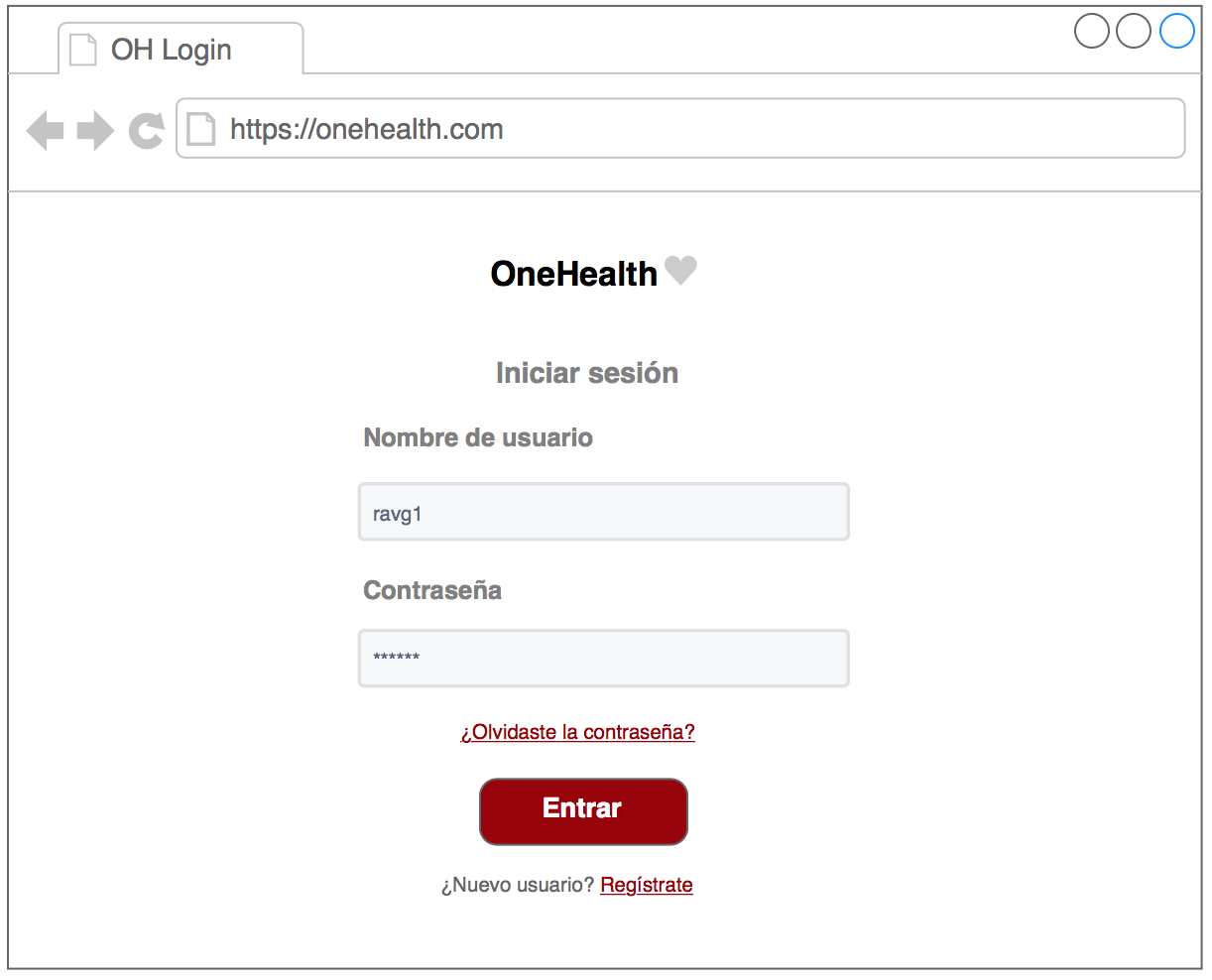
****

Ilustración 9: Mockup login

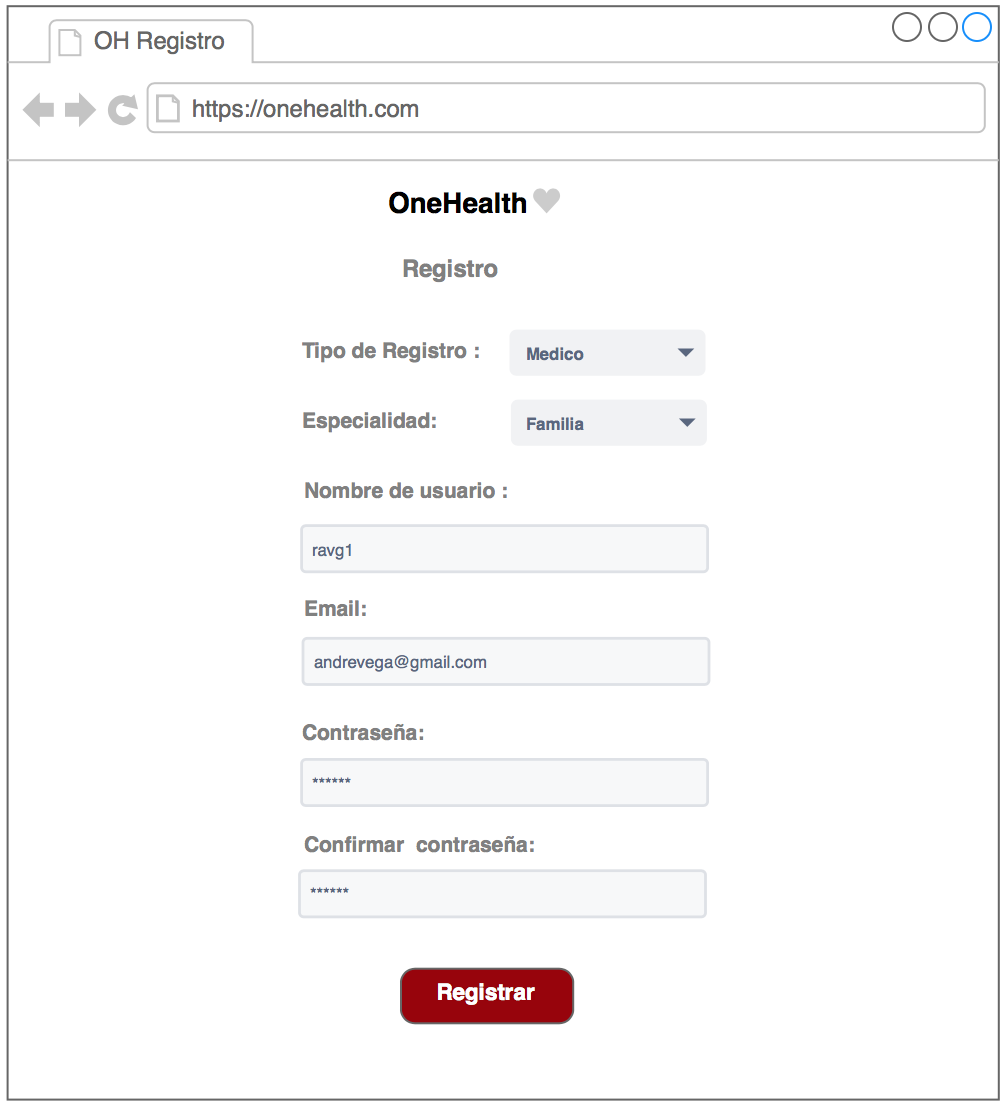


Ilustración 10: Mockup registro médico

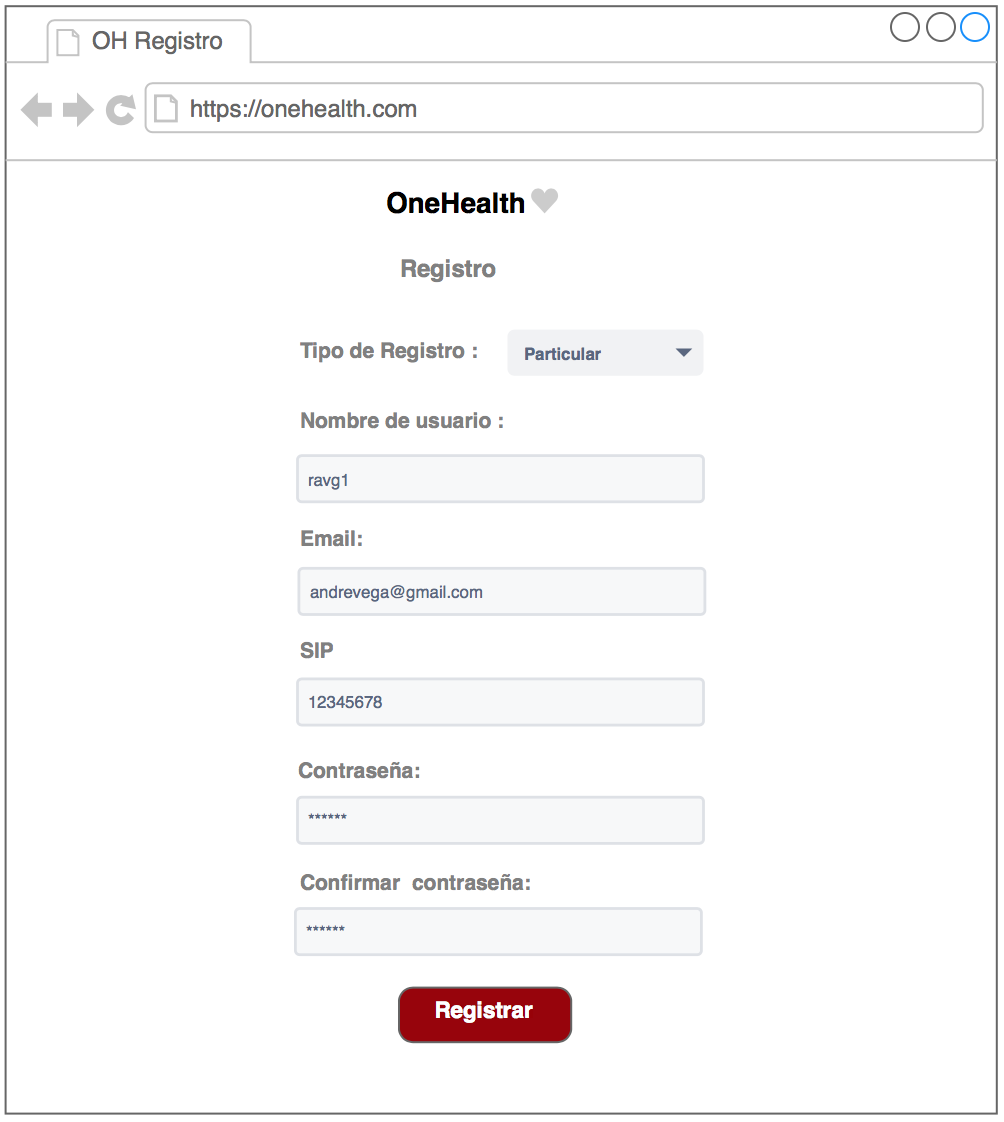


Ilustración 11: Mockup registro paciente

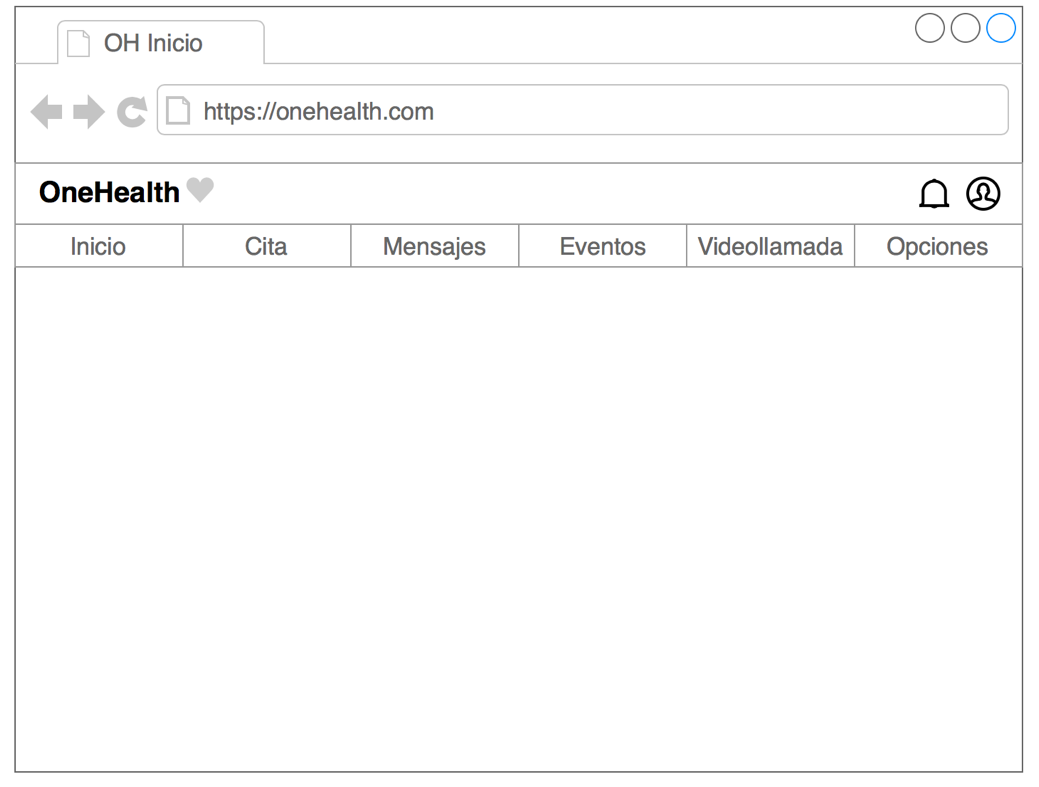


Ilustración 12: Mockup inicio

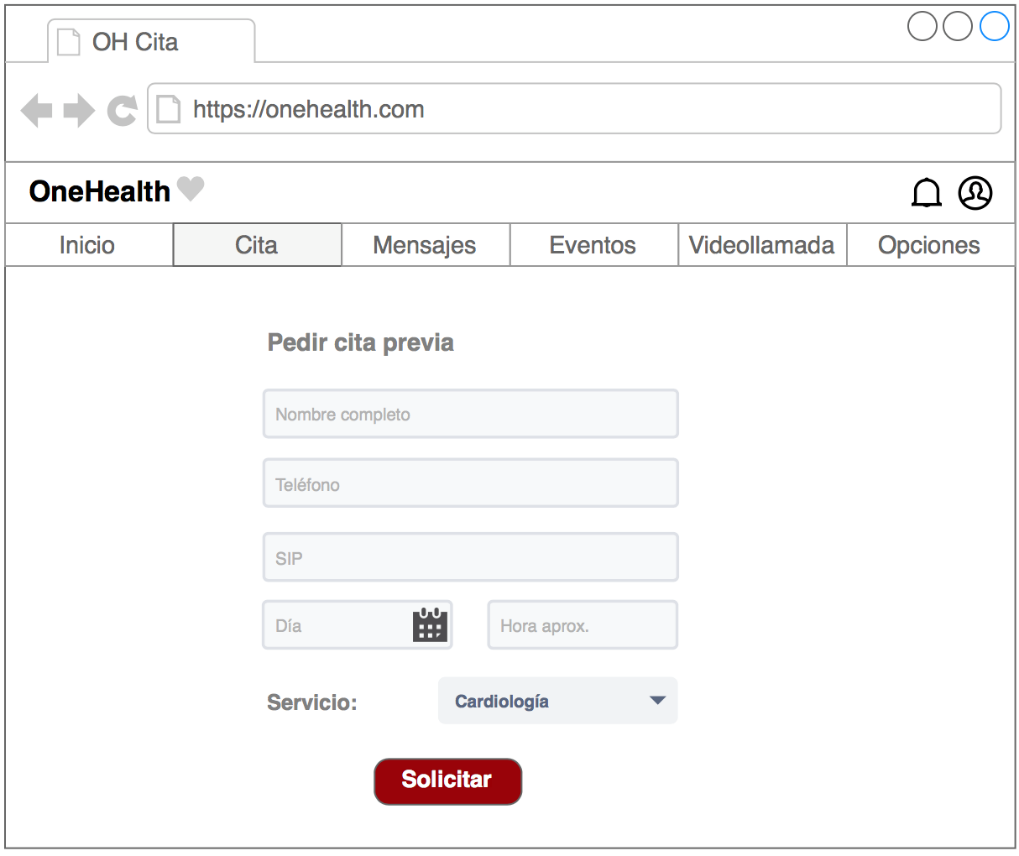


Ilustración 13: Mockup pedir cita

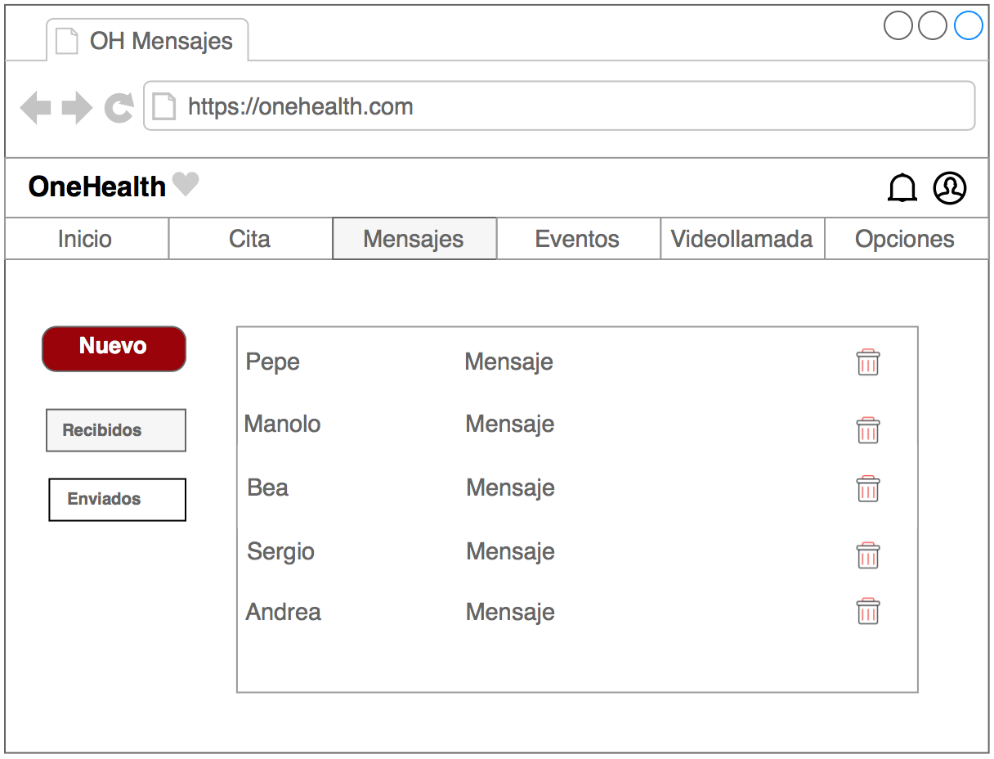


Ilustración 14: Mockup mensajes



Ilustración 15: Mockup historial

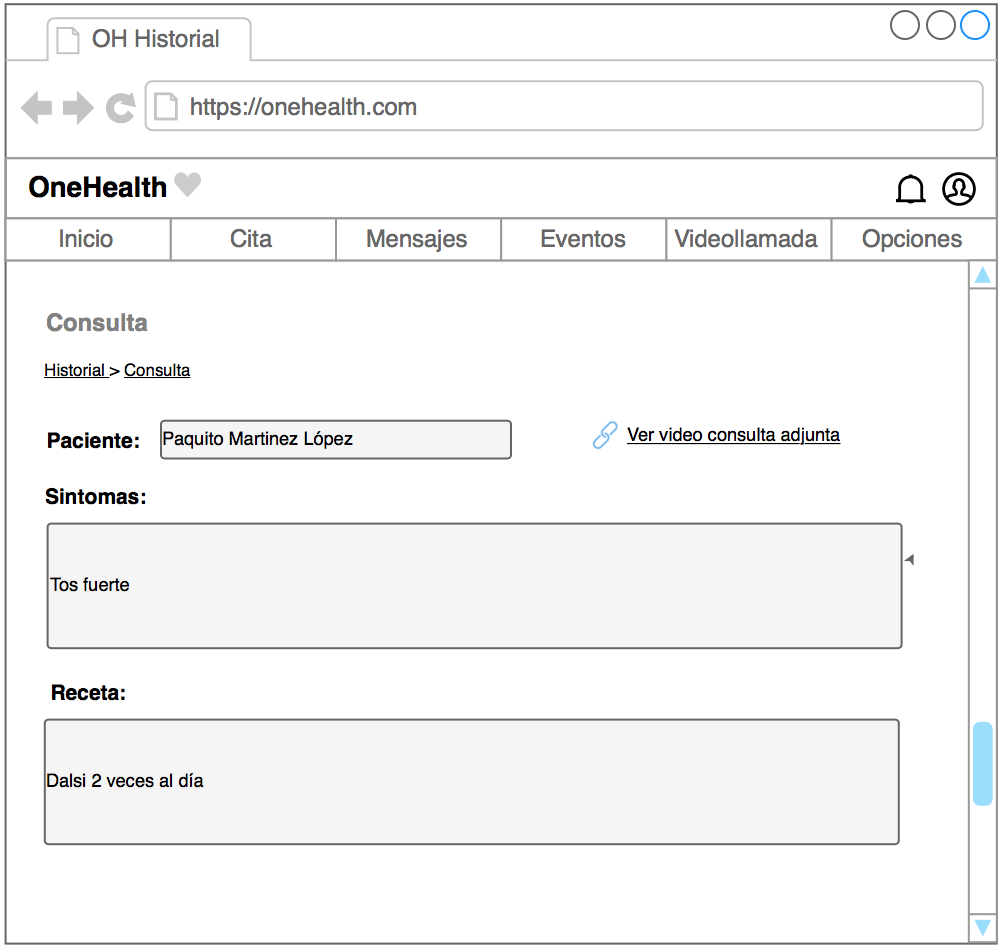


Ilustración 16: Mockup ver consulta

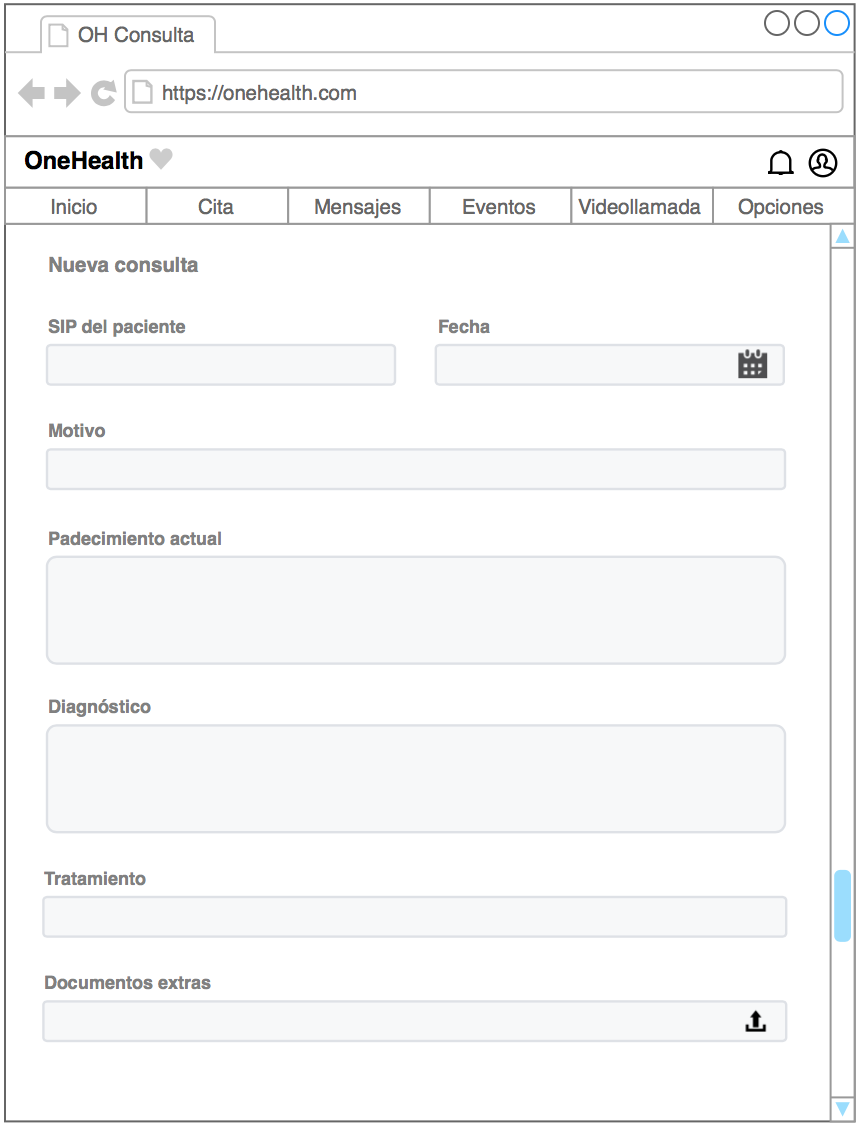


Ilustración 17: Mockup nueva consulta

## Diagrama de clases

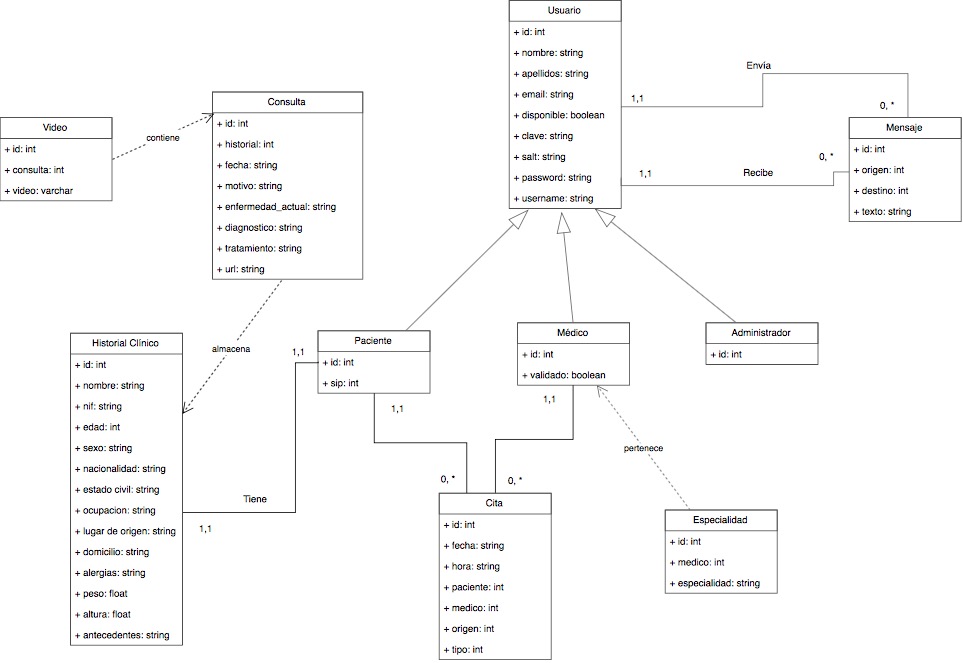
****

Ilustración 18: Diagrama de clases

## Diagrama entidad relación

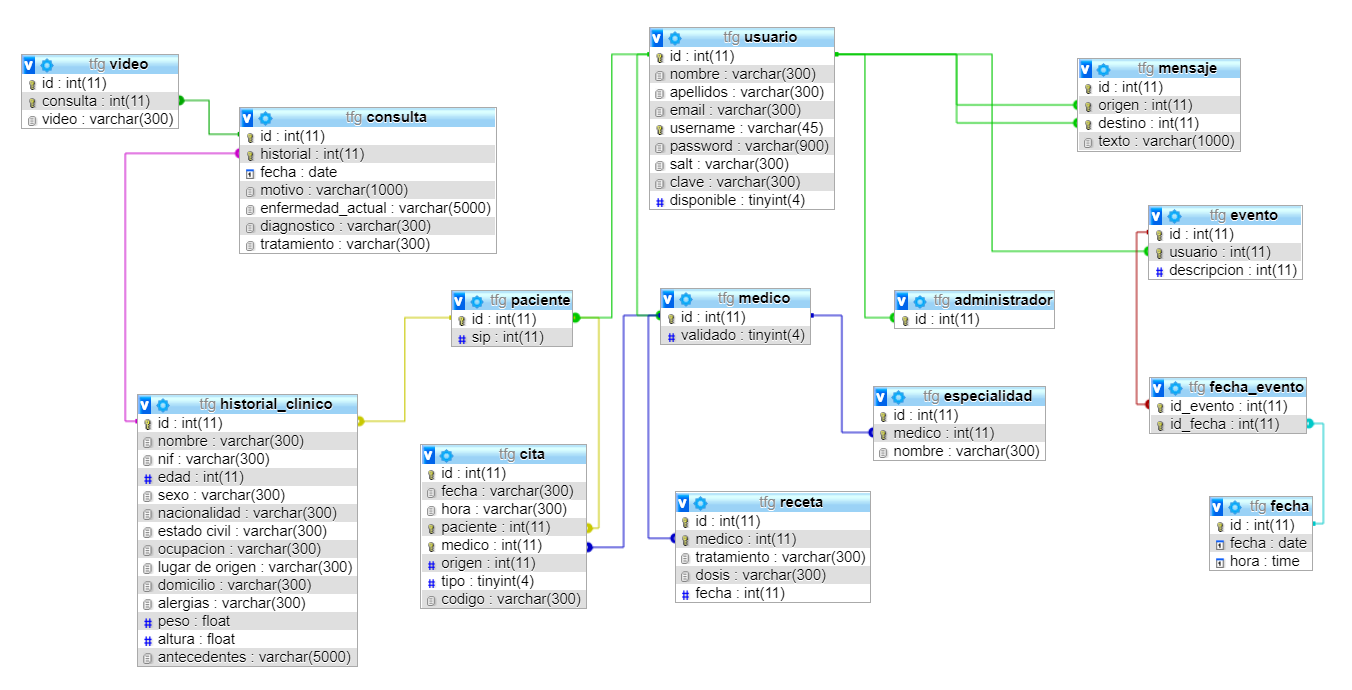


Ilustración 19: Diagrama entidad relación

## Diseño final

Durante el desarrollo de la aplicación algunas vistas han sufrido cambios y reducciones haciendo mas simple alguna de ellas.

A continuación, se mostrarán las vistas con el diseño final, incluyendo las que no estaban en los prototipos tempranos, además de una explicación con la secuencia del funcionamiento normal de la aplicación.

Las vistas de registro y *login* casi no han sufrido cambios con respecto a los prototipos, exceptuando en el registro, que se ha omitido el campo de confirmar contraseña. En esta parte el usuario tiene que elegir que tipo de registro quiere, de tipo médico o de usuario normal. En el caso de que sea de tipo médico, cuando se registre no podrá hacer los servicios exclusivos de un médico hasta que el administrador no lo valide.

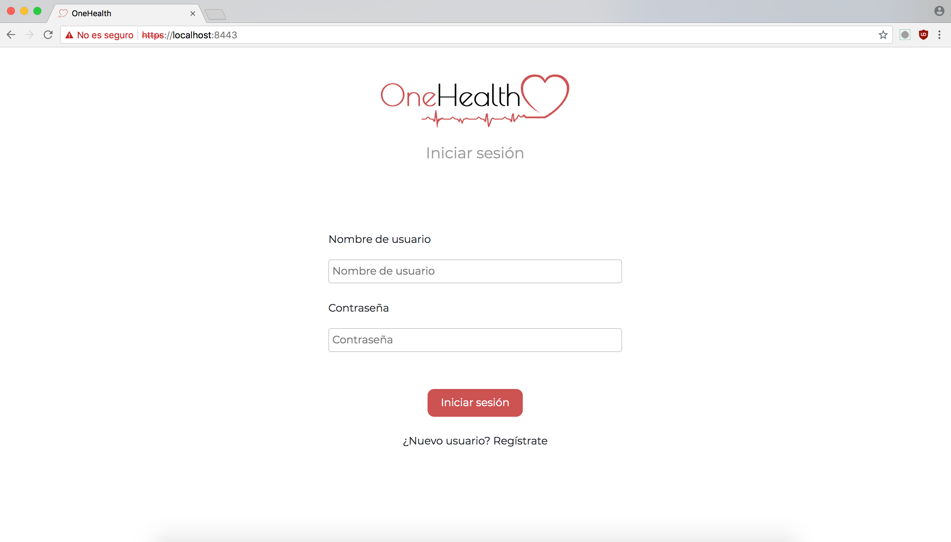


Ilustración 20: Login

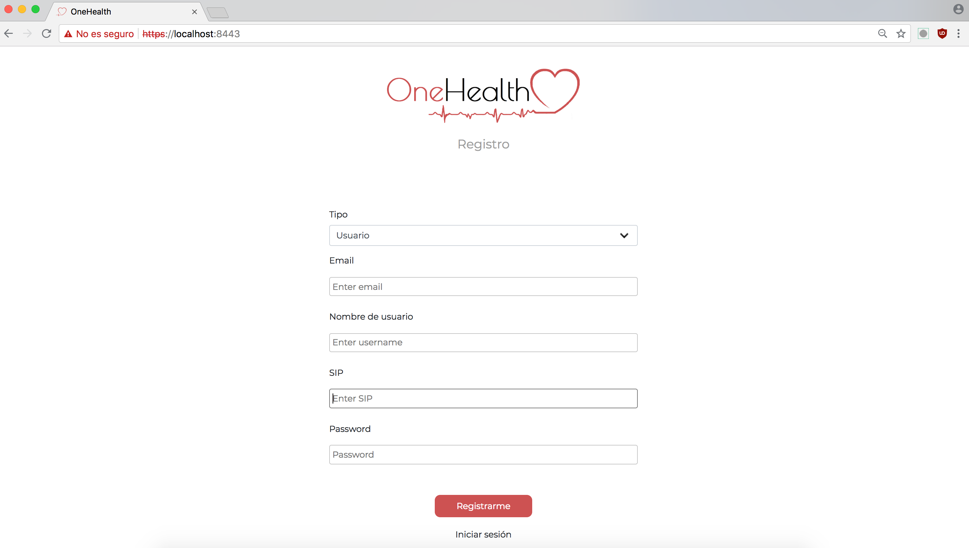


Ilustración 21: Registro

Cuando el usuario haya metido correctamente su nombre de usuario y contraseña para iniciar sesión, se le redirige a la vista de confirmación de *login (Ilustración 22).* En ella el usuario tiene que introducir el código que se le ha enviado a su correo electrónico, para comprobar que es él.

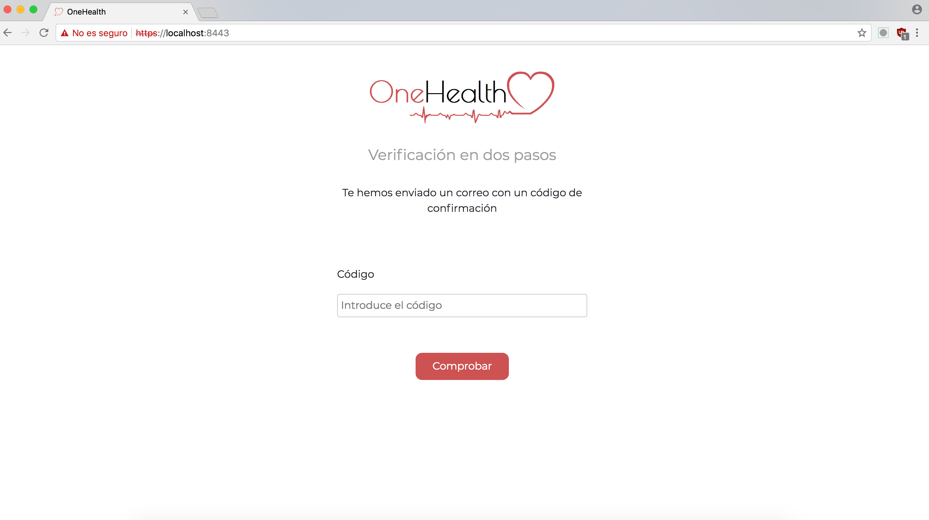


Ilustración 22: Confirmación de login

Una vez habiendo iniciado sesión, en la vista de inicio (*Ilustración 23*) vemos que hay noticias sobre la salud, y que el menú ha cambiado con respecto a los prototipos. Se ha quitado la opción de eventos y opciones ya que por limitación de tiempo eventos no se ha podido implementar, posponiéndolo para futuras mejoras. Y en cuanto a la de opciones se optó por poner más opciones en el apartado “Perfil”.



Ilustración 23: Inicio

La primera opción que tenemos después de inicio es la citas, en ella tenemos dos alternativas, pedir una nueva cita o ver las citas. Las dos opciones pueden realizar tanto médico como paciente.

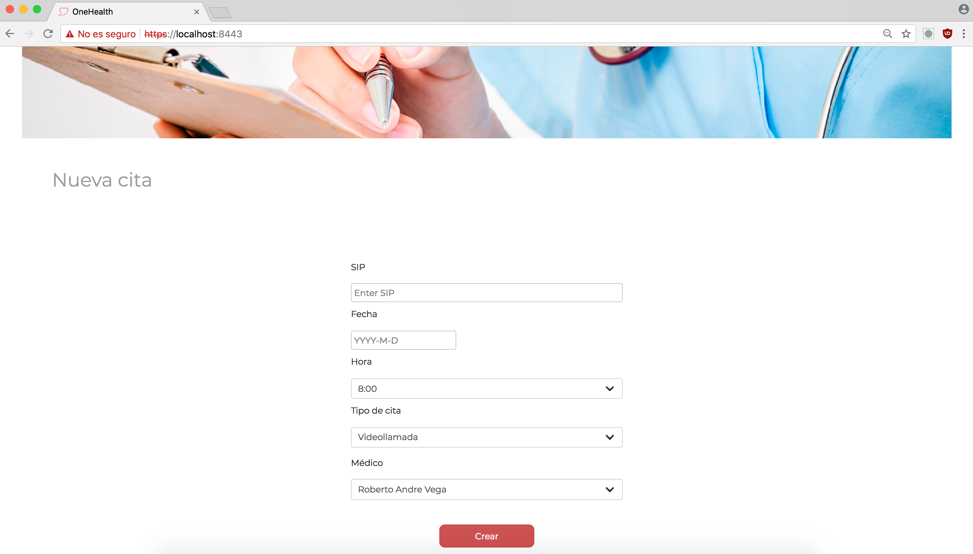


Ilustración 24: Nueva cita

En la opción de “nueva cita” (*Ilustración 24*) el usuario tiene que introducir la SIP del paciente, la fecha, seleccionar una hora, elegir el tipo de cita, ésta puede ser videollamada o presencial si es necesario y, por último, el nombre del médico con el que concretar la cita. Una vez rellenados los campos correctamente se le proporciona un código de la cita al usuario, que luego llegada la fecha de la cita lo tendrá que introducir para comprobar que la cita es válida y está dentro del rango de la fecha y hora establecido cuando se creó la cita.

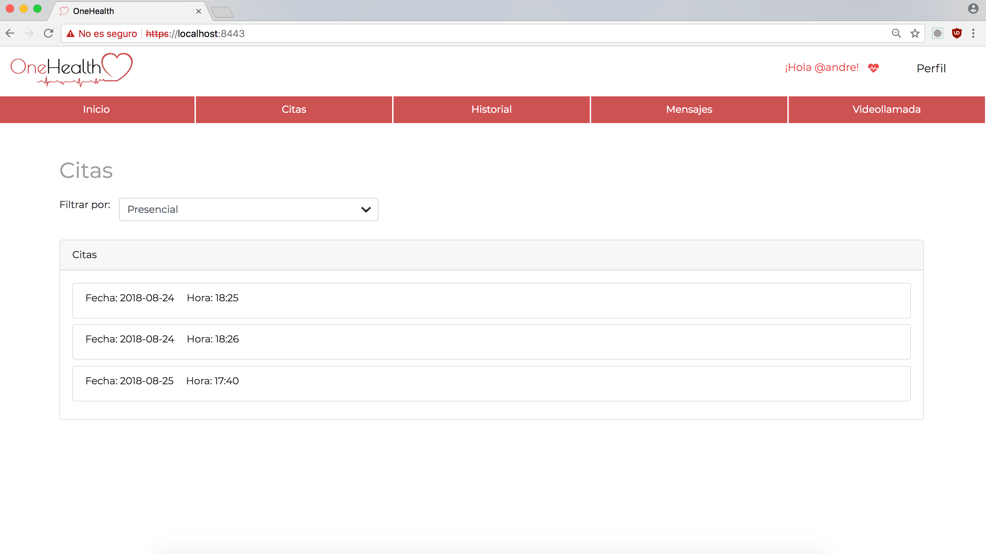


Ilustración 25: Ver citas

En la opción de ver citas, el usuario puede ver todas sus citas, parecido a un historial de citas, y filtrarlas según sean de tipo de videollamada o presencial.

La siguiente opción en el menú es la de historial, aquí las alternativas varían según el tipo de usuario que sea, si es médico tiene la opción de buscar el historial de un paciente mediante su SIP y crear una nueva consulta asociada al historial de un paciente.

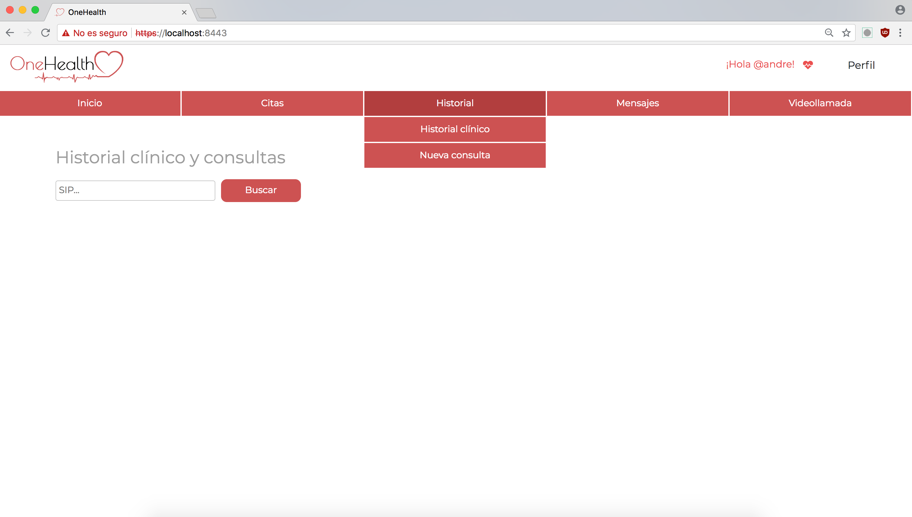


Ilustración 26: Historial según la vista del médico

Cuando el médico busca un historial clínico, le aparecen los datos del paciente y las consultas asociadas a ese historial (*Ilustración 27*).

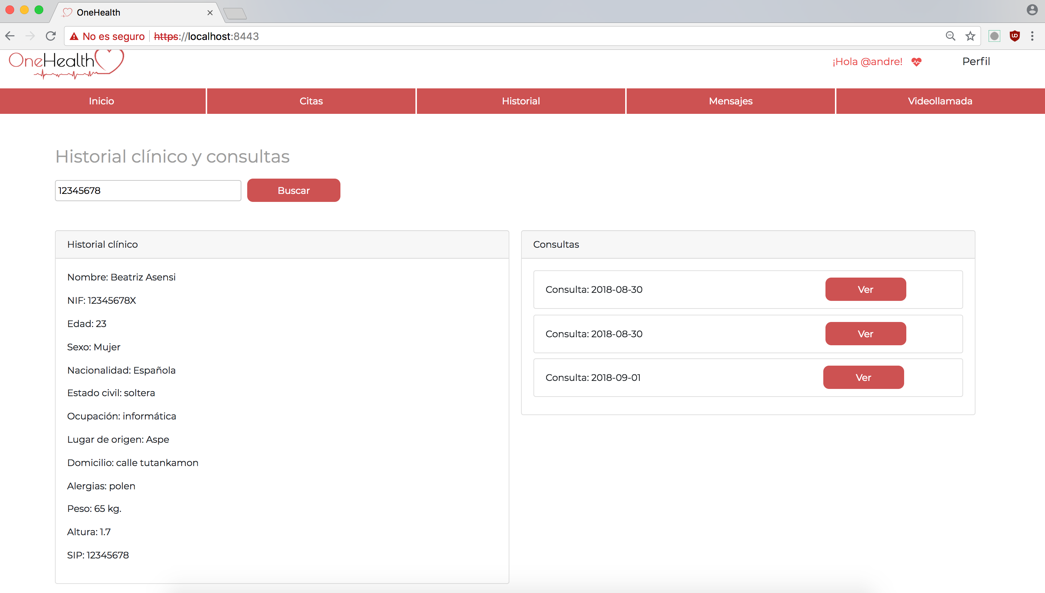


Ilustración 27: Historial y consultas

El médico tiene la posibilidad de acceder a todas las consultas, dentro de cada consulta le aparecerá la información con respecto a esa consulta, incluso un video de la videollamada en caso de que fuera de ese tipo.

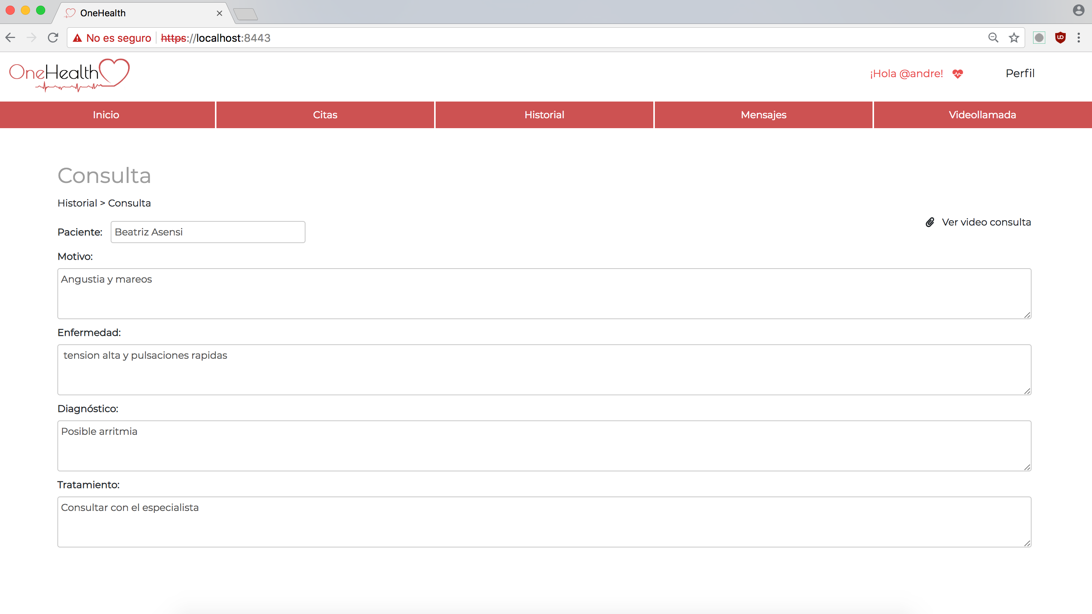


Ilustración 28: Ver consulta

Para crear una nueva consulta el médico tiene que rellenar los campos, siendo obligatorio el de la tarjeta SIP (*Ilustración 29)*.

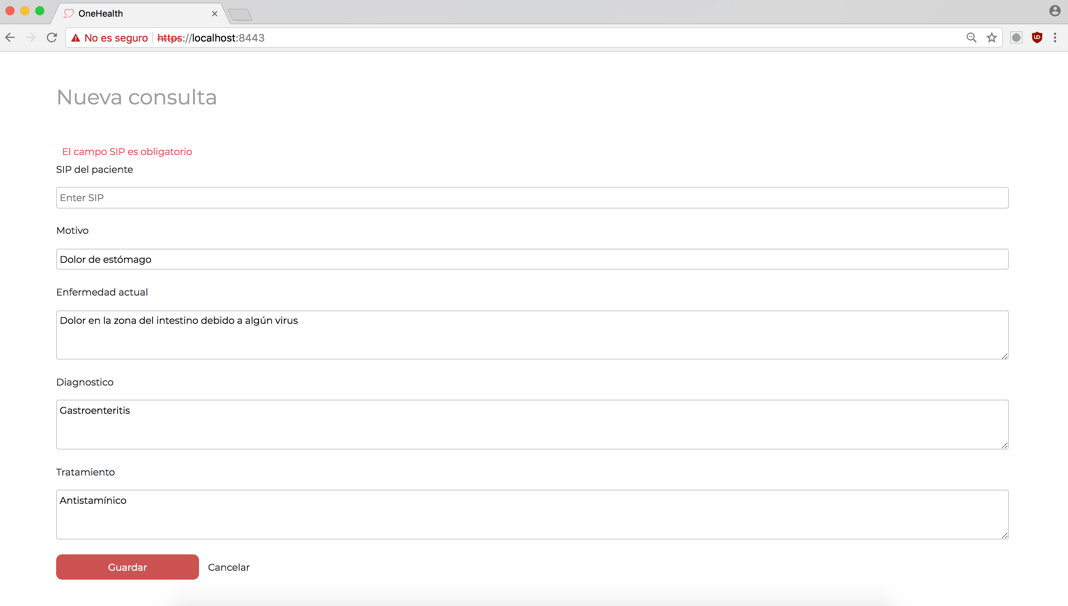


Ilustración 29: Nueva consulta

Si es un paciente, al hacer clic en la opción de historial, simplemente le aparecerán los datos personales de su historial exceptuando las consultas.

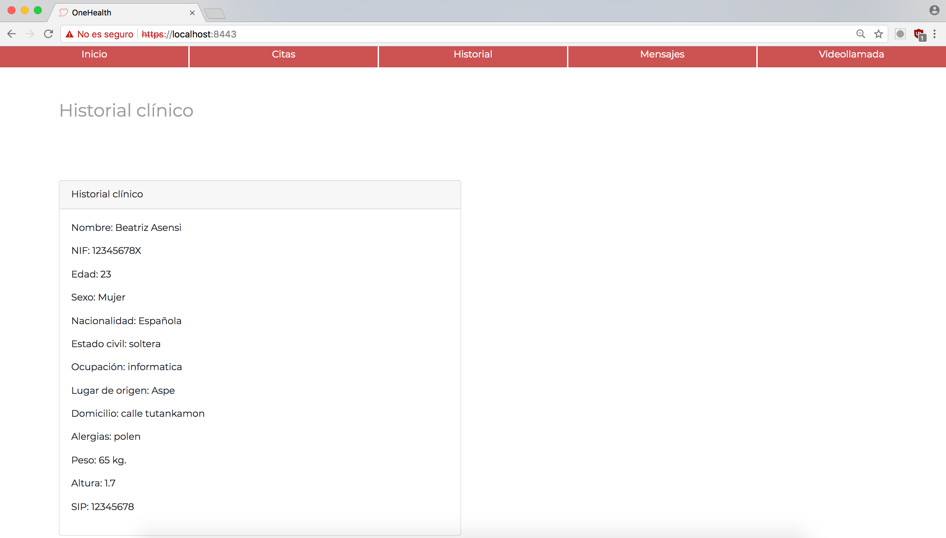


Ilustración 30: Historial (paciente)

La siguiente opción es la de mensajes, dicha opción esta disponible tanto para pacientes como para médicos. Paciente y médico podrán comunicarse a través de mensajes. Cada uno podrá enviar un nuevo mensaje, poniendo el nombre de usuario del destinatario, un asunto y el mensaje, todos campos obligatorios. Y también podrán ver sus mensajes recibidos y enviados, pudiendo borrar los enviados.

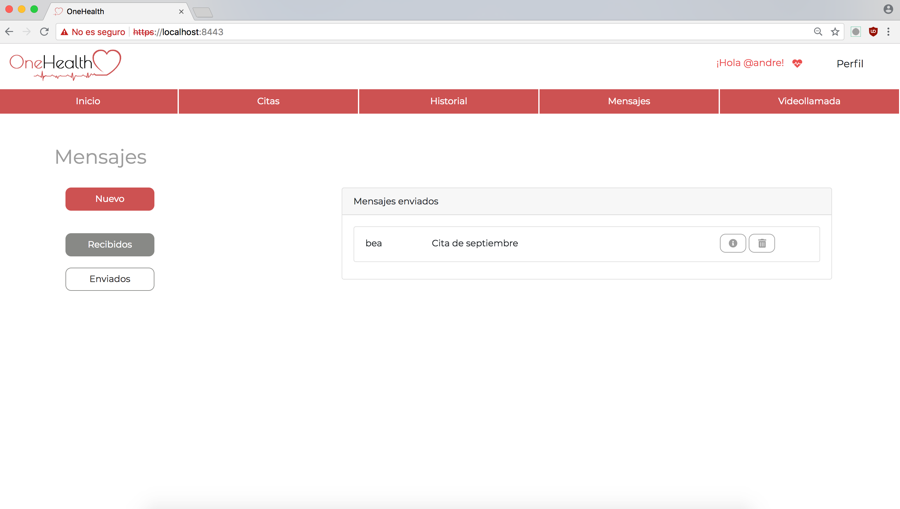


Ilustración 31: Mensajes (enviados)

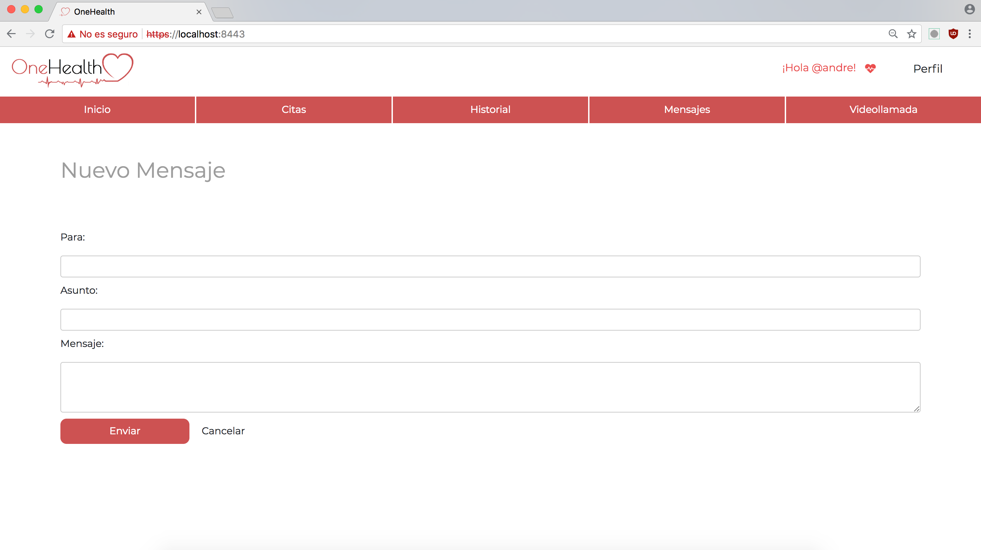


Ilustración 32: Nuevo mensaje

Por último, la opción de videollamada, que varía según el usuario sea médico o paciente. Si el usuario es de tipo paciente, se le pedirá el código de la cita que se le proporcionó al crear la cita, si es válido podrá empezar la videollamada. En el caso de que sea médico le aparecen un listado de pacientes conectados con la opción de poder llamarlos y un buscador para buscar un paciente mediante la tarjeta SIP.

## Arquitectura

La arquitectura de la cual se compone el proyecto es una arquitectura cliente-servidor, la cual es un modelo de comunicación que vincula varios dispositivos a través de una red. El cliente realiza peticiones al servidor y éste se encarga de responder a dichas peticiones, lo que posibilita que las tareas se distribuyan entre los servidores y los clientes. Este tipo de modelo permite que el servidor pueda ejecutarse en más de un equipo lo que facilita repartir la capacidad de procesamiento (Wikiwand, 2018).

La arquitectura del proyecto es de dos capas, ya que el servidor accede directamente a los datos y se los devuelve al cliente que hizo la petición.

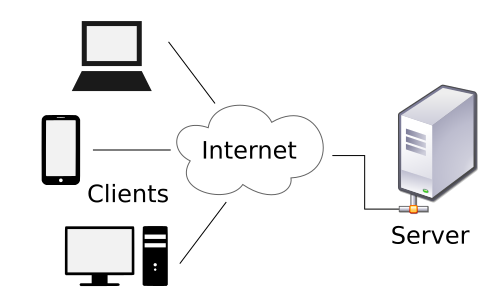


Ilustración 33: Arquitectura cliente-servidor (dos capas)

# Seguridad

En la actualidad la mayoría de la información se gestiona a través de internet, y muchos de esos datos suelen ser importantes para el usuario, como por ejemplo contraseñas, tarjetas de crédito, datos sanitarios, etc. Por eso, la seguridad en el sistema es uno de los principales propósitos a conseguir para el proyecto. Al trabajar con datos sensibles de usuarios es imprescindible mantener la integridad de dichos datos y dar una imagen de un sistema seguro, ya que, una mala gestión de la seguridad puede tener un impacto económico y además afectar a la reputación y la confianza de socios y clientes.

En este apartado se detallarán los aspectos de seguridad, tanto en el servidor como en el cliente, que se han implementado en el proyecto.

## Servidor

En el lado del servidor se han implementado las siguientes características relacionadas con la seguridad:

* **Conexión:** para asegurar la transferencia segura de datos se ha usado el protocolo HTTPS, el cual es un protocolo de aplicación basado en HTTP, pero destinado a la transferencia segura de datos.

HTTP es el protocolo que se utiliza para la comunicación entre cliente y servidor, pero tiene el problema que la transferencia de datos se hace en plano, es decir, sin cifrar. Por eso en el proyecto se ha optado por usar HTTPS, el cual se podría decir que es la versión segura de HTTP, ya que esta basado en SSL/TLS.

SSL/TLS (Secure Sockets Layer/Transmission Layer Security) son dos protocolos para enviar paquetes cifrados a través de internet. Ambos utilizan lo que se conoce como un sistema de infraestructura de clave pública (PKI) asimétrico. Un sistema asimétrico utiliza dos claves para encriptar comunicaciones, una clave pública y una clave privada. Cualquier cosa cifrada con la clave pública solo se puede descifrar con la clave privada y viceversa.

Con esto HTTPS crea un canal cifrado para la transferencia de información sensible, lo que significa que esos datos del usuario están cifrados y no pueden ser interceptados. Otra ventaja es que los visitantes pueden verificar el dueño legitimo del dominio y así poder confiar más en el sistema.

* **Certificados:** como se ha comentado anteriormente los certificados SSL sirven para establecer un canal seguro entre emisor y receptor, el problema es que algunos sitios no utilizan los certificados realmente seguros a día de hoy.

Los certificados SSL son firmados utilizando un hash de una única dirección, para garantizar la integridad de este (y garantizar que el certificado no se ha modificado). Siguen existiendo en Internet sitios que utilizan SHA-1, siendo SHA-1 inseguro, debido a vulnerabilidades, ya que existen colisiones que permiten *crackear* el protocolo 2000 veces más rápido de lo esperado (*Schneier, 2005*). La solución es usar un algoritmo de hash seguro, como SHA-2, en los certificados. En nuestro caso, en el proyecto se ha optado por usar SHA512 con el algoritmo de encriptación RSA.

RSA es un sistema criptográfico de clave pública, se considera uno de los algoritmos más seguros ya que nadie ha conseguido demostrar o rebatir su seguridad. Las claves públicas y privadas se calculan a partir de un número que se obtiene como producto de dos números primos grandes, por lo que un supuesto atacante se enfrenta a un problema de factorización de un coste computacional muy elevado.

* **Sistemas de autenticación**: en cuanto a la autentificación de los usuarios, en el proceso de *login* hay un **doble factor de autenticación**. Primero el usuario tiene que introducir su nombre de usuario y contraseña, y si todo está bien, se le envía un correo electrónico con un código generado aleatoriamente en el servidor, el usuario tiene que introducirlo, se comprueba su validez y ya puede iniciar sesión en el sistema.

Para la autenticación de los médicos, el médico en cuestión se tiene que registrar con normalidad eligiendo la opción correcta en el registro. Una vez registrado en el sistema para poder tener acceso a los servicios tiene que ser validado antes por un administrador del sistema, que se encargará de comprobar que en realidad es un médico cuando este aporte la documentación necesaria para corroborarlo.

Cuando el usuario ya ha iniciado sesión en el sistema, se utiliza la autenticación basada en ***token*.** Esta autenticación consiste en que cada petición HTTP que haga el usuario va acompañada de un *token* en la cabecera. Este *token* no es más que una firma cifrada que permite a nuestro API identificar al usuario, pero no se almacena en el servidor, si no en el lado del cliente y el API es el que se encarga de descifrar ese *token* y redirigir el flujo de la aplicación en un sentido u otro (Azaustre, 2017). Esto nos añade más seguridad, al no utilizar cookies para almacenar la información del usuario, podemos evitar ataques CSRF (Cross-Site Request Forgery) que manipulen la sesión que se envía al *backend*.

En el proyecto se ha optado por usar ***JSON Web Token (JWT)****.* Este *token* está compuesto por tres partes: la cabecera, que contiene el tipo (JWT) y la codificación utilizada (SHA256), el *payload* que es donde van los atributos del *token,* que en nuestro caso son los siguientes:

var payload = {

sub: user.id,

iat: moment().unix(), //cuando se ha creado el token

exp: moment().add(15, "days").unix() //cuando expira

}

Y la ultima parte es la de *signature,* la cualestá formada por los anteriores componentes (*Header y Payload*) cifrados en Base64 con una clave secreta (almacenada en nuestro API). Así sirve de hash para comprobar que todo está bien*.*

* **Métodos de cifrado:** en el proyecto se cifran todos los datos de los usuarios antes de ser almacenados en la base de datos con una clave única para cada usuario, generada aleatoriamente cuando el usuario se dio de alta en el sistema. El algoritmo que se ha utilizado es AES256 combinado con CBC. AES es un estándar de cifrado avanzado (*Advanced Encryption Standard*), que hoy en día es considerado uno de los cifrados más seguros y utilizados. El algoritmo se basa en varias sustituciones, permutaciones y transformaciones lineales, ejecutadas en bloques de datos de 16 bytes. Estas operaciones se repiten varias veces, llamadas “rondas”.

El modo de operación es CBC, el cual opera de forma que a cada bloque de texto se le aplica una operación XOR con el bloque previo ya cifrado. De este modo, cada bloque cifrado depende de todos los bloques de texto claros usados hasta ese punto. Además, se utiliza un vector de inicialización para que cada mensaje sea único (Wikipedia, 2018).

## Cliente

En el lado del cliente, gracias a la herramienta de *Webpack*, se usa también el protocolo HTTPS con certificados SSL SHA256, con el algoritmo de encriptación RSA, tal y como se hace en el servidor.

# Implementación

Como ya se ha comentado anteriormente el proyecto se divide en dos grandes partes, por un lado, el API (servicios) y por otro el cliente (aplicación web), por lo que para hablar de la implementación del sistema es necesario tener las dos partes en cuenta.

## API

El API como ya se ha dicho en otros apartados se ha desarrollado con *NodeJS* utilizando peticiones HTTPS con los métodos de petición para indicar la acción que se desea realizar para un recurso determinado.

Para la implementación es necesario saber el funcionamiento del sistema y el modelo de datos (*Ilustración 18*), para saber todos los elementos del proyecto y cómo interacción entre ellos.

Primero hay que destacar que todas las funciones del sistema giran en torno al usuario, ya que tiene relación con todas las acciones disponibles. Hay tres tipos de roles de usuario:

* **Paciente**: es el usuario estándar del sistema, tiene acceso a la mayoría de las funciones, exceptuando la de ver las consultas, donde también se pueden ver los videos asociados a las consultas, y la de crear una nueva consulta.
* **Médico**: es el usuario que tiene acceso a todas las funciones disponibles del sistema, con la diferencia del paciente de que tiene que ser validado por un administrador antes de poder tener acceso a dichas funciones.
* **Administrador**: el administrador del sistema se encarga de validar los nuevos médicos registrados y añadir los historiales de los pacientes.

Para controlar que cada usuario tenga acceso a sus respectivas tareas, se ha hecho uso de un *middleware* que controla las diferentes rutas de las funciones. Pero también existe el problema de que un usuario intente acceder a una ruta usando el nombre de usuario de otro usuario con otro rol diferente al suyo, para esto se ha implementado también un *middleware* que comprueba que ese usuario esta conectado al sistema*.* Las únicas rutas que no están bajo este control son las de registro, *login*, confirmación de *login* y listar especialidades (se usa en el registro del médico para poder listar todas las especialidades disponibles).

### Login y registro

Como seguridad en el registro se obliga al usuario a poner un nombre de usuario del que no exista, un correo electrónico válido y su tarjeta SIP, en el caso de que sea un paciente, además de una contraseña. Esta contraseña en el servidor no se guarda en claro en la base de datos, si no que se le aplica una codificación con SHA512. Si todo ha ido bien, se guarda el usuario y se genera una clave aleatoria que luego se usará para el cifrado de datos.

En la parte del *login* cuando el usuario introduce correctamente el nombre de usuario y contraseña, se genera un código aleatorio de cuatro números que se le envía al correo electrónico que puso en el registro. Una vez que el usuario haya introducido dicho código y se haya validado, se genera un *token* único para cada usuario, ya que se incluye el id de cada usuario, y con un tiempo de expiración de quince días. Cada vez que el cliente haga una petición debe incluir este *token* en la cabecera de *Authorization* y en el servidor se comprueba su validez. Cada vez que el usuario inicia sesión se actualiza el *token* y cuando se cierra la sesión se elimina.

var payload=jwt.decode(token, config.TOKEN\_SECRET)

if(payload.exp <= moment().unix()) {

return resp.status(401).send({message: "El token ha expirado"})

}

### Historial

En el apartado del historial clínico es diferente según el usuario, en el caso de que sea un paciente, se busca el historial según la *id* del usuario conectado, se desencriptan los datos con la clave de dicho usuario, y se devuelven solo los datos personales sin las consultas asociadas.

Si el usuario es de tipo médico se hace la petición a otra ruta donde se comprueba que efectivamente es un médico y no de otro tipo. En este caso el historial se busca mediante la tarjeta SIP del paciente y se devuelven todos los datos del historial, así como todas las consultas registradas a dicho historial.

Por último, en el caso del administrador una de sus funciones es la de añadir un nuevo historial, dentro de esta opción aparece un formulario con los datos necesarios del historial clínico, para identificar al usuario el administrador debe introducir, como campo obligatorio, el *id* con el que se ha almacenado ese usuario en la base de datos. Una vez introducidos los datos se hace la petición y en el servidor se cifran los datos con la clave del usuario introducido.

### Consultas

Las consultas son exclusivas del médico, cuando se busca un historial el servidor devuelve automáticamente las consultas asociadas, en el caso de tenerlas, para que el médico, si quiere, pueda verlas y así no hacer peticiones de mas al servidor.

La otra opción disponible es la crear una nueva consulta, en ella el médico tiene que rellenar unos campos con los datos de la consulta, siendo únicamente obligatorio el de la tarjeta SIP para poder identificar al usuario y con ello su historial, luego en el servidor se cifran los datos y se guarda la consulta correctamente.

### Mensajes

El servicio de mensajes es igual tanto para médico como para paciente, ambos pueden ver los mensajes recibidos y enviados, enviar un nuevo mensaje y borrar los mensajes. Los métodos de ver recibidos y ver enviados son muy parecidos, el de recibidos busca los mensajes donde el destinatario sea el usuario conectado, y descifra los datos con la clave del remitente del mensaje, es decir, el que lo envió. Y el de ver enviados simplemente busca los mensajes donde el remitente sea el usuario conectado, descifrando los mensajes con su propia clave, ya que él fue el que lo creó.

Para enviar un nuevo mensaje el usuario tiene que poner el nombre de usuario del destinatario de forma correcta, de lo contrario el método devolverá un error diciendo que no se ha encontrado al destinatario. Además de eso, tiene que poner el asunto del mensaje y el mensaje en sí, ambos campos obligatorios. Los datos en el servidor se cifran con la clave del usuario que ha enviado el mensaje.

El usuario también tiene la opción de borrar un mensaje, pero esta función está limitada a los mensajes enviados, ya que se comprueba que el usuario que quiere borrar el mensaje sea el que originalmente lo envió.

### Citas

El servicio de citas incluye las funciones de crear una nueva cita, ver las citas y borrar una cita.

El usuario puede ver todas las citas, o bien filtrarlas por el tipo de cita que sea, es decir, videollamada o presencial. Los métodos para listar las citas están organizados para listar las citas de un paciente y sus dos tipos, y para listar las citas de un médico y sus dos tipos. Es decir, que según sea médico o paciente se manda la petición a unos métodos u otros. Cada método descifra los datos de las citas con la clave del usuario que haya creado la cita y devuelve una información general sobre las citas. Para poder ver los detalles de cada cita se llama a otro método especifico al que se le pasa el *id* de una cita y que devuelve los detalles de esa cita.

Para crear una cita el usuario tiene que rellenar todos los campos que le aparecen en el formulario, ya que en este caso todos son obligatorios. La cita registra a un paciente identificado por la tarjeta SIP, un médico al que se tiene que elegir entre la lista de médicos disponibles que se ofrece y una fecha y hora concretos. Los datos en servidor se cifran con la clave del usuario que ha creado la cita. Una vez creada con éxito el servidor devuelve como respuesta un código que el usuario debe guardarse para que llegado el día y la hora, en el apartado de videollamada pueda entrar a la cita.

Si el usuario quiere cancelar una cita, tiene que irse al apartado de videollamada e introducir el código de la cita y en él le aparece la opción de cancelar la cita, se hace la petición pasando el *id* de la cita y se borra de la base de datos.

## Cliente

El cliente se ha desarrollado con *ReactJS,* que como se ha comentado anteriormente es una librería para crear interfaces basadas en componentes.

En la *Ilustración 34* podemos observar la estructura del proyecto de la parte del cliente. El archivo “index.html” es el único archivo *html* y es donde se colocan los componentes, en nuestro caso esta el componente” main.js”.

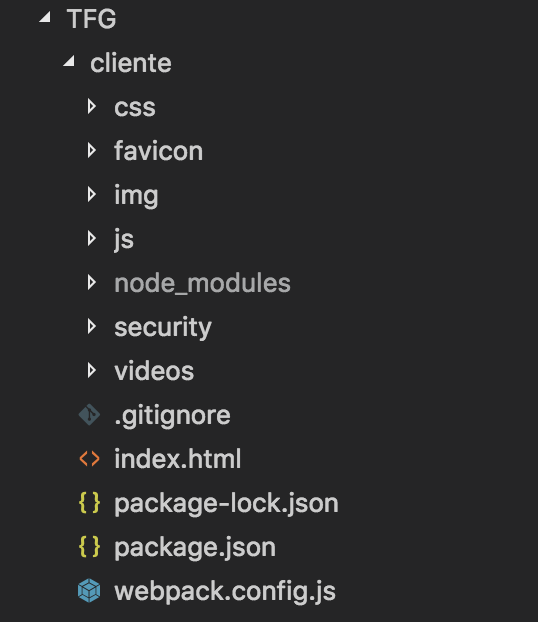


Ilustración 34: Estructura del proyecto (cliente)

Los componentes están en la carpeta “js”. En el componente “main”es donde están las librerías necesarias y donde se renderiza el primer componente. Este es el componente “index” el cual controla los estados de que indican si el usuario ha iniciado sesión, si esta *logueado* o si tiene que introducir el código de confirmación. Según sea el caso se renderiza el componente de inicio, login o confirmación de *login*.

var token = localStorage.getItem('token')

if(!this.state.logged &&token==null && !this.state.confirmado){

return<Login handleConfirmacion={this.confirmacion}/>

}else if(!this.state.logged&&token==null&&this.state.confirmado){

return <Confirmar handleLoginOK={this.loginOK}/>

}else{

return <Inicio handleLogout={this.logoutOK}/>

}

## Registro y login

En el componente *login* se hace la petición HTTPS correspondiente y si es correcta, se llama a una función del componente padre para que cambien el estado y renderice el componente inicio. También hay una opción mediante un enlace para renderizar el componente registro.

En el registro al tener dos opciones posibles de formulario, para el médico o para el paciente, hay un estado que va cambiando según el usuario selecciona un tipo u otro. En el caso del formulario del médico hay que listar las especialidades disponibles para que le aparezcan en el selector al usuario, para ello llamamos a la función que hace la petición desde el método “componentDidMount()” que es llamado automáticamente después del *render.*

componentDidMount(){

this.obtenerEspecialidades()

}

Si el registro ha sido correcto, se llama a una función del componente padre (*login*) y este a su vez llama a otra función del padre (index) para que renderice el componente inicio.

## Inicio

El componente inicio es el que controla todas las opciones del menú de la pagina de inicio (*Ilustración 23*) mediante estados. Además, también controla lo que devolver según el tipo de usuario que haya iniciado sesión. En el caso de que sea el administrador, se renderiza el componente administrador donde la vista cambia por completo, mostrándole solo sus funciones disponibles. En el caso del médico en el historial le aparece un desplegable con las opciones de historial y nueva consulta, las cuales al paciente no le aparecen.

## Historial

Dentro del componente historial se controla la información que se devuelve según el tipo de usuario que sea. Si es un médico, se muestra una vista para que pueda buscar el historial de un paciente, si la petición se ha hecho con éxito, se cambia el estado y se muestra el historial resultado de la búsqueda y sus consultas, en el caso de tenerlas. En el caso de que sea de tipo paciente, se necesita el historial antes de que se llame al *render,* ya que cuando el paciente haga clic en la opción del historial ya le tienen que aparecer sus datos, por ello, se inicializa una variable en el constructor al resultado de la función que hace la petición para obtener el historial según el *id* del usuario conectado.

## Consultas

Los componentes que intervienen en las consultas son el de listar las consultas y ver una consulta. El de listar consultas se llama desde el de historial y se encarga de recorrer el *array* de consultas que se le pasa desde historial y, para cada consulta, llamar al componente de ver consulta. Al cual se le pasan los datos de una sola consulta y que éste se encarga de mostrar, teniendo como resultado final una lista de consultas con los detalles que se quiera mostrar.

La opción de los médicos de nueva consulta simplemente es un formulario con el campo obligatorio de la tarjeta SIP, y con un estado que controla si el médico quiere cancelar o si la consulta se ha guardado correctamente, para redirigirle al inicio.

## Cita

Las dos opciones disponibles en el apartado de citas son listar las citas, con la posibilidad de filtrarlas, y nueva cita. Para listar las citas se tienen que hacer tres peticiones a tres métodos diferentes (todas las citas, las de videollamada y las presenciales) según el tipo de usuario. Los resultados de estos métodos hay que mostrarlos cuando se haya cargado el componente, para esto usamos el “componentDidMount()”, aquí se llama a las funciones que hacen las peticiones y se guardan los resultados en estados que luego mostraremos en el *render.* Por otro lado, para controlar el filtrado de las citas se usa un estado que cambia según el *value* del selector, así en el *render* se devuelve un resultado u otro según el valor de este estado.

Para crear una nueva cita, como pasaba con nueva consulta, simplemente es un formulario con la diferencia que si la petición es realizada con éxito devuelve el código de la cita resultante y redirige al inicio. Lo único a resultar en este componente es que se ha usado una librería externa para poder tener el *datepicker* y así, poder elegir la fecha con el calendario.

## Mensajes

Para poder listar los mensajes como sucedía en anteriores casos necesitamos los mensajes enviados y recibidos cuando cargue el componente, por eso volvemos a usar el “componentDidMount(), dentro de él se llama a las funciones que hacen la petición para obtener los mensajes y se guardan los resultados en estados. Luego en el *render* se listan dichos mensajes llamando a un componente mensaje al que se le pasan los datos de un mensaje, y este se encarga de mostrar los detalles que se considere.

La diferencia con otros componentes está en que en este caso un usuario puede borrar los mensajes enviados o enviar uno nuevo, lo que supone que se tiene que actualizar la lista de mensajes mostrada. Para actualizar la lista y volver a hacer las peticiones se hace uso del “componentDidUpdate(), el cual se llama automáticamente después de una actualización. Como solo queremos que se vuelva a hacer las peticiones tras la actualización de unos casos específicos, se usan estados para controlar estas situaciones.

componentDidUpdate(){

if(this.state.borrado){

this.mensajesRecibidos()

this.mensajesEnviados()

this.setState({borrado:false})

}else if(this.state.enviado){

this.mensajesRecibidos()

this.mensajesEnviados()

this.setState({enviado:false})

}

}

El componente de crear un nuevo mensaje es un formulario con todos los campos obligatorios, donde se controlan los estados para cancelar, en el que vuelve a la vista anterior, y para en el caso de que se envíe con éxito un nuevo mensaje, se cambia el estado de enviado para volver a cargar la lista mensajes otra vez.

# Conclusiones

## Revisión de objetivos

En el proyecto se propusieron diferentes objetivos, el principal era crear un sistema seguro y de código abierto para la comunicación entre medico y paciente sin la necesidad de estar los dos físicamente en el mismo sitio. Proveer funciones adicionales como, por ejemplo, crear citas eligiendo el medico y el tipo de cita que se quiera, dar la posibilidad de comunicarse entre ellos mediante mensajes, ver el historial médico y las consultas y poder crear nuevas. Y aparte de todo esto, conseguir que el sistema fuese lo más seguro posible.

Estos objetivos se han cumplido en su mayoría, teniendo como resultado un proyecto de código abierto y una integración completa de todas las funciones desarrolladas con la función de videollamada.

En la parte del API REST, se han desarrollado la mayoría de los servicios propuestos, exceptuando algunos adicionales como el cifrado de ficheros, teniendo disponibles los servicios de crear citas, ver citas, ver el historial clínico, ver consultas, añadir nuevas consultas, ver los mensajes recibidos y enviados y enviar nuevos mensajes. Aparte de eso se ha conseguido un API que puede ser reutilizada en otros proyectos, es decir, que no es exclusiva y tiene la posibilidad de que se le añadan nuevas características en el futuro.

En la parte de la aplicación web, se ha conseguido una interfaz de usuario intuitiva pero mejorable en ciertos aspectos, sobre todo de cara a mejorar la experiencia del usuario y reducir el numero de errores que pueda tener. Se pueden añadir funcionalidades que en el API están implementadas, pero en el cliente no se han llegado a añadir por falta de tiempo, como es el caso de editar una cita.

Con respecto a la seguridad, se han implementado varias medidas de seguridad importantes, cifrado de la conexión con los certificados SSL y cifrado de los datos antes de almacenarlos con AES256 con CBC. Además, la autenticación de los usuarios en el sistema y su validación se llevan a cabo de forma segura. Aún así, la seguridad es mejorable, por ejemplo, se puede cifrar la base de datos entera no solo los datos, ya que el sistema estaría expuesto ante un posible robo o acceso indebido al servidor. También se puede mejorar el cifrado, en lugar de usar AES con CBC se podría usar AES con GCM, que es otro modo de operación de cifrado en bloque que ha adoptado ampliamente gracias a su eficiencia y rendimiento.

El proyecto está disponible para todo el mundo en *GitHub*, en el repositorio tenemos una guía de despliegue y de instalación, una breve descripción del sistema junto con los servicios que ofrece y un apartado de posibles mejoras que se le pueden añadir. Enlace del repositorio:

<https://github.com/bap17/OneHealth>

## Trabajos futuros

El proyecto tiene muchas posibilidades de mejoras y ampliaciones como, por ejemplo, añadir la funcionalidad de subir ficheros adicionales a las consultas como ya se ha mencionado anteriormente. Al principio del proyecto se planteó también la idea de meter eventos del establecimiento donde esté en funcionamiento la aplicación, ya sea centro de salud u hospital. Esta característica está contemplada en el esquema relacional de la base de datos (*Ilustración 19*), por lo que solo habría que implementar la lógica de negocio en el API y añadir la funcionalidad al cliente.

Otra posible interesante característica es ofrecer al paciente y al médico un calendario con recordatorios de las citas pendientes, y en el caso del paciente también mostrarle los medicamentos que se tiene tomar al día, mandándole un aviso a la hora concreta en la cual se lo tendría que tomar. También, para hacer más completo el sistema, sería interesante ofrecer la posibilidad al médico de poder recetar medicamentos a los pacientes sin que tengan que estar físicamente.

Sería interesante también en la página de inicio de la web poner y dar prioridad a noticias, relacionadas con el centro en donde se le esté dando uso al sistema, sobre otras noticias más generales.

Por último, se considera importante también la futura implementación de ampliar el sistema a aplicación para dispositivos móviles.

# Bibliografía

Abernethy, Michael (2011). *¿Simplemente qué es Node.js?* Obtenido de

https://www.ibm.com/developerworks/ssa/opensource/library/os-nodejs/index.html

Atrys (22 de junio de 2018). *Telemedicina*. Obtenido de

<http://www.atryshealth.com/es/-qué-es-la-telemedicina-_1580>

Azaustre, Carlos (2017). *¿Qué es la autenticación basada en token?* Obtenido de

<https://carlosazaustre.es/que-es-la-autenticacion-con-token/>

Expansión (enero 2018). *Cifras de internet*. Obtenido de

<http://www.expansion.com/economia-digital/innovacion/2018/02/01/5a72e73a22601db2288b4658.html>

HealthTap (1 de noviembre de 2017). Obtenido de

<https://www.healthtap.com/what_we_make/overview>

Juniper (2017). *Minimum Hardware Requirements for Node Servers and Servers*. Obtenido de

<https://www.juniper.net/documentation/en_US/nfv2.1/topics/reference/ccpe-servers-hardware-spec.html>

La Vanguardia (febrero 2018). *El 68% de la población española se conecta a internet a diario*. Obtenido de

<https://www.lavanguardia.com/economia/20180205/44565836290/internet-poblacion.html>.

Murcia Salud (1 de noviembre de 2017). Obtenido de

<https://www.murciasalud.es/principal.php>

MySQL (15 de junio de 2018). *MySQL Workbench.* Obtenido de

<https://www.mysql.com/products/workbench/>

Politécnica IUMET (1 de noviembre de 2017). *Telemedicina.* Obtenido de

<http://www.iumet.es/servicios-telemedicina.php>

Rouse, Margaret (2017). *Advanced Encryption Standard (AES)*. Obtenido de

<https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>

Sanitas (octubre 2016). La *Telemedicina ya es una realidad con Sanitas y se llama BLUA.* Obtenido de

<https://sanitasventas.com/la-telemedicina-ya-realidad-sanitas-se-llama-blua/>

Schneier, Bruce (2005). *Cryptanalysis of SHA-1*. Obtenido de

<https://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html>

ScienceDirect (noviembre 2016*). Telemedicina, estado actual y perspectivas futuras en audiología y otología*. Obtenido de

<https://www.sciencedirect.com/science/article/pii/S0716864016301195>

Vida (1 de noviembre de 2017). *Videoconsultas médicas*. Obtenido de

<https://www.vida.es>

We are social (2018). *Global Report*. Obtenido de

<https://digitalreport.wearesocial.com>

Wikipedia (20 de julio de 2018). *Visual Studio Code.* Obtenido de

<https://www.wikipedia.org>

Wikipedia (6 de julio de 2018). *Modos de cifrado.* Obtenido de

<https://www.wikipedia.org>

Wikiwand (1 de julio de 2018). *Arquitectura cliente-servidor.* Obtenido de

<http://www.wikiwand.com/es/Cliente-servidor>