



Universidad
Zaragoza

Proyecto Fin de Carrera

SOLUCIÓN TECNOLÓGICA DE E-SALUD PARA TOMA DE MEDIDAS Y GESTIÓN DE USUARIOS EN CENTROS DE DÍA Y RESIDENCIAS DE LA TERCERA

Autor

SAMUEL LONGARES LOSILLA

Director

EDUARDO PRADO CLEMENTE

Ponente

IGNACIO MARTÍNEZ RUIZ

Escuela de Ingeniería y Arquitectura
Febrero 2014

Dedicatorias y agradecimientos

Agradecer a Nacho y Eduardo por su disponibilidad y ayuda prestada en todo momento.

También me gustaría agradecer al personal y compañeros de trabajo de la empresa Gooday Solutions, por el ambiente fantástico y los buenos momentos que hemos pasado.

No quisiera olvidarme de mis padres y hermana, así como el resto de mi familia y amigos por su apoyo en todo momento.

Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad
Samuel Longares Losilla - Eduardo Prado Clemente

*Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y
residencias de la tercera edad*
Samuel Longares Losilla - Eduardo Prado Clemente

RESUMEN DEL PROYECTO FIN DE CARRERA

“SOLUCIÓN TECNOLÓGICA DE E-SALUD PARA TOMA DE MEDIDAS Y GESTIÓN DE USUARIOS EN CENTROS DE DÍA Y RESIDENCIAS DE LA TERCERA”

Realizado por: Samuel Longares Losilla

Dirigido por: Eduardo Prado Clemente

En la actualidad, los entornos residenciales necesitan herramientas que mejoren el día a día, tanto del personal sanitario y de administración como de los residente. Estas herramientas están inmersas en la evolución digital, rompiendo con los métodos tradicionales analógicos y manuales, para obtener una serie de ventajas de eficiencia, eficacia, ahorro de papel, de tiempo y de costes que son prioritarias en la situación actual de los entornos residenciales. Los profesionales necesitan tiempo para atender a los residentes como es debido y, a su vez, los residentes necesitan calidad en la atención sanitaria que reciben.

En este contexto, en este Proyecto Fin de Carrera (PFC) se ha desarrollado una plataforma de gestión total para la monitorización de residentes y la generación de informes útiles para los médicos, completamente funcional e instalada en forma de proyecto piloto en una residencia aragonesa.

Para conseguirlo, un paso imprescindible ha sido completar la cadena de valor digital dando conectividad inalámbrica a los dispositivos médicos (evitando los cables que incomodan la tarea de desplazarlos y manipularlos), permitiendo que los datos vitales se digitalicen automáticamente (evitando anotaciones a mano y errores humanos en la transcripción) y dando servicios de valor añadido como la generación de informes y los avisos a familiares o centros médicos (permitiendo un ahorro de tiempo enorme).

Otra contribución indispensable ha sido la integración de multitud de tecnologías de primerísima actualidad trabajando de forma armónica. Muchas de ellas, tecnologías de código abierto (*open source*) y multiplataforma, que dan a la plataforma un potencial de desarrollo de nuevas funcionalidades y servicios enorme, así como una integración ágil con otras plataformas.

Por último, la plataforma proporciona una gestión de salud completa, desde la monitorización ubicua y el registro en un sistema de almacenamiento de datos que garantiza el acceso en cualquier momento y desde cualquier lugar a través de servicios web, hasta la generación de informes útiles que faciliten la labor de interpretación de los médicos. Se ha conseguido una plataforma fácil de usar, intuitiva, cómoda y agradable a la vista para conseguir una mejor adaptación del personal a los nuevos procesos de trabajo.

Como líneas futuras, algunas ya iniciadas, se plantea implementar nuevos módulos que proporcionen servicios de valor añadido, incorporar la identificación biométrica y la integración con redes sociales de salud.

SUMMARY

"eHEALTH SOLUTION FOR VITAL SIGNS MONITORING AND USERS MANAGEMENT IN DAYCARE CENTRES AND NURSING HOMES"

Realizado por: Samuel Longares Losilla

Dirigido por: Eduardo Prado Clemente

Nowadays, nursing home environments need tools to improve the daily life, both health and administration professionals and patients. These tools are embedded in the digital evolution, breaking with traditional analog and manual methods to obtain a number of advantages of efficiency, effectiveness, saving paper, time and costs are high on the current situation of nursing home environments. Practitioners need time to care for residents properly and, in turn, residents need quality health care.

Under these circumstances, in this Thesis (PFC) it is developed a complete management platform for monitoring residents and generating useful reports for doctors, fully functional and installed as a pilot project in an aragonese residence.

To achieve this, an essential step has been complete digital value chain providing wireless connectivity to medical devices (avoiding uncomfortable cables), digitalizing critical data automatically (without handwritten notes and avoiding transcription human errors) and providing value-added services such as reporting and notifications to family or medical centers (timesaving).

Another essential contribution has been the integration of many novel technologies working in harmony. Many of them are open source technologies and multi-platform, with a huge development potential of new features, services and agile integration with other platforms.

Finally, the platform provides a complete health management, ubiquitous monitoring and data storage system that ensures access anytime and anywhere through web services. Generating useful reports facilitating the task of interpreting by doctors. It has got an easy platform to use, intuitive, comfortable and pleasing to the eye for better alignment of professionals to new work processes.

As future lines, some of them already underway, it is proposed to implement new modules that provide value-added services, to incorporate biometric identification and integration with health social networks.

Índice de contenidos

Índice de contenidos.....	i
Índice de figuras.....	v
Índice de tablas.....	vi
Acrónimos.....	ix
1 Introducción y objetivos.....	1
1.1 Introducción y antecedentes.....	1
1.1.1 Tecnologías para la monitorización de residentes.....	2
1.1.2 Infraestructura para comunicaciones	3
1.1.3 Servicios de valor añadido.....	3
1.2 Motivación	5
1.3 Objetivos	5
1.4 Estructura de la memoria.....	6
2 Análisis y diseño	9
2.1 Análisis del problema	9
2.1.1 Toma de contacto con el centro residencial	9
2.1.2 Requisitos demandados	10
2.1.3 Requisitos observados.....	11
2.2 Diseño de la solución.....	13
2.2.1 Arquitectura global.....	13
2.2.2 Cliente	14
2.2.3 Servidor	21
3 Desarrollo e implementación.....	27
3.1 Cliente	27
3.1.1 Dispositivos médicos contemplados	27
3.1.2 Aplicación Android	30
3.1.3 Aplicación de gestión	33
3.2 Servidor	38
3.2.1 Base de datos MySQL.....	38
3.2.2 Servicio web	39
3.3 Despliegue	45
4 Resultados	47
4.1 Implantación real	49
4.1.1 Protocolo de actuación	49

4.2	Evaluación	50
5	Conclusiones y líneas futuras	51
5.1	Aportaciones al trabajo realizado	51
5.2	Cumplimiento de los objetivos propuesto	51
5.3	Valoración personal.....	52
5.4	Líneas futuras	53
6	Bibliografía	55
7	Anexo 1: Análisis de alternativas de diseño	57
7.1	Alternativas para la identificación/autenticación de usuarios.....	57
7.1.1	Autenticación basada en algo conocido.....	57
7.1.2	Autenticación basada en algo poseído.....	57
7.1.3	Autenticación basada en biometría	58
7.2	Alternativas para el diseño de una solución para la gestión de datos.....	59
7.2.1	Bases de datos relacionales (SQL)	59
7.2.2	Comparativa	59
7.3	Alternativas para el diseño de un servicio web	59
7.3.1	Simple Object Access Protocol (SOAP).....	60
7.3.2	Representational State Transfer (REST)	60
7.3.3	Comparativa	60
8	Anexo 2: Tecnologías.....	63
8.1	Android.....	63
8.1.1	Arquitectura	63
8.1.2	Estructura de la aplicación	64
8.1.3	Ciclo de vida de una actividad Android	64
8.1.4	Dispositivos disponibles	65
8.1.5	Desarrollo de aplicaciones	66
8.2	Bluetooth.....	66
8.2.1	Introducción al Bluetooth	66
8.2.2	Historia	66
8.2.3	Características del Bluetooth	67
8.2.4	Redes	69
8.3	Near Field Communication.....	71
8.3.1	Introducción al NFC	71
8.3.2	Especificaciones técnicas de NFC	71
8.3.3	Modos de funcionamiento	71
8.3.4	Establecimiento de la conexión.....	72

8.3.5	Arquitectura NFC y modos de funcionamiento.....	72
8.4	.NET Framework.....	73
8.5	MySQL	74
8.5.1	Relaciones SQL	74
8.6	SQLite	75
8.6.1	Introducción	75
8.6.2	Características	76
9	Anexo 3: Seguridad	77
9.1	Secure Socket Layer	77
9.2	Advanced Encryption Standard.....	79
9.2.1	Especificaciones.....	80
10	Anexo 4: Diseño de la interfaz de usuario e informes de ejemplo	83
10.1	Aplicación Android	83
10.2	Aplicación de gestión	85
10.3	Informes de ejemplo	92
11	Anexo 5: Encuestas	98
11.1	Encuestas previas para personal de administración.....	98
11.2	Encuestas previas para el personal sanitario	102
11.3	Encuestas de evolución para el personal de administración	106
11.4	Encuestas posteriores para el personal de administración	112
11.5	Encuestas posteriores para el personal sanitario	116
12	Anexo 6: Manuales de uso de dispositivos médicos y ficha técnica.....	120
12.1	Manuales de uso de dispositivos médicos	120
12.2	Ficha técnica	124

Índice de figuras

Figura 1: Bloques de una plataforma de gestión total de e-Salud	1
Figura 2: Arquitectura global de la plataforma	13
Figura 3: Diagrama de flujo de la aplicación Android	18
Figura 4: Diagrama de flujo de la aplicación de gestión.....	20
Figura 5: Estructura de una base de datos de una residencia de la tercera edad.....	21
Figura 6: Arquitectura ASP.NET.....	22
Figura 7: Características técnicas del termómetro utilizado.....	27
Figura 8: Características técnicas del pulsioxímetro utilizado.....	28
Figura 9: Características técnicas de la báscula utilizada.....	28
Figura 10: Características del tensiómetro/glucómetro utilizado	29
Figura 11: Diagrama de trabajo de la aplicación móvil.....	31
Figura 12: Configuración del cliente smtp para el envío de e-mails.....	34
Figura 13: Cuerpo personalizado del e-mail.....	34
Figura 14: Interfaz principal de la aplicación de gestión.....	35
Figura 15: Ejemplo de Background Worker	36
Figura 16: Ejemplo de petición http GET de la aplicación de gestión	37
Figura 17: Ejemplo de acceso a la base de datos mediante NHibernate.....	40
Figura 18: Ejemplo de acceso a la base de datos mediante secuencia SQL.....	41
Figura 19: Esquema de salteado y hasheado de contraseñas	43
Figura 20: Extracto de código para encriptación de contraseñas	43
Figura 21: Extracto de código de encriptado AES	44
Figura 22: Esquema de despliegue de la plataforma.....	45
Figura 23: Secuencia de uso de la aplicación móvil.....	47
Figura 24: Ejemplo de sms como aviso a familiar o centro médico	48
Figura 25: Ciclo de vida de una actividad Android.....	65
Figura 26: Redes Bluetooth. Piconet y Scatternet	69
Figura 27: Arquitectura del perfil puerto serie.....	70
Figura 28: Arquitectura NFC. Modos de operación	72
Figura 29: Modos de operación. Detalles.....	73
Figura 30: Capas del protocolo SSL.....	77
Figura 31: Protocolo de establecimiento de la conexión segura.....	79
Figura 32: Diagrama de bloques de estado del cifrado AES.....	80
Figura 33: Combinaciones posibles de los parámetros del cifrado AES	81
Figura 34: Pseudo-código del algoritmo de cifrado AES.....	82
Figura 35: Layout de entrada mediante tarjeta NFC	83
Figura 36: Layout de entrada manual.....	83
Figura 37: Layout de selección de residente	83
Figura 38: Layout de espera de conexión de dispositivo médico	83
Figura 39: Layout de adquisición de la medida	84
Figura 40: Layout medida adquirida	84
Figura 41: Layout medida enviada	84
Figura 42: Layout envío de sms	84
Figura 43: Formulario principal pestaña de residentes	85
Figura 44: Formulario principal pestaña de personal sanitario.....	85

Figura 45: Formulario principal pestaña de centros sanitarios	86
Figura 46: Formulario principal pestaña de tarjetas	86
Figura 47: Formulario principal pestaña de medidas	87
Figura 48: Formulario de nuevo residente	87
Figura 49: Formulario de ficha de residente	88
Figura 50: Formulario de nuevo personal sanitario	88
Figura 51: Formulario de ficha de personal sanitario	89
Figura 52: Formulario de nuevo centro sanitario	89
Figura 53: Formulario de acceso a la aplicación de gestión	90
Figura 54: Formulario de generación de informes periódicos	90
Figura 55: Formulario de generación de informes de incidencia aguda	91
Figura 56: Ejemplo informe de glucometría	92
Figura 57: Ejemplo informe de presión arterial	93
Figura 58: Ejemplo informe de pulsioximetría	94
Figura 59: Ejemplo informe de peso	95
Figura 60: Ejemplo informe de temperatura	96
Figura 61: Ejemplo informe glucosa por franjas horarias	97

Índice de tablas

Tabla 1: Resumen de las características frecuenciales, disposición de canales y modulación de Bluetooth.....	68
Tabla 2: Resumen de las distintas clases de emisores Bluetooth	69

Acrónimos

AES	Advanced Encryption Standard
API	Application Programming Interface
BW	Band With
CSR	Certificate Signing Request
EER	Entity Relationship Diagram
FTP	File Transfer Protocol
GFSK	Gaussian Frequency Shift Keying
HDP	Health Device Profile
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IIS	Information Internet Services
JSON	JavaScript Object Notation
LOPD	Ley Orgánica de Protección de Datos Personales
NDA	Non Disclosure Agreement
NFC	Near Field Communication
OMS	Organización Mundial de la Salud
ORM	Object Relational Mapping
OS	Operating System
OTG	On-the Go
PC	Personal Computer
PDF	Portable Document File
PFC	Proyecto Fin de Carrera
PID	Personal Identification
PK	Personal Key
REST	Representational State Transfer
SDK	Software Development Kit
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SPP	Serial Port Profile
SQL	Structured Query Language
SSL	Secure Socket Layer

TCP	Transmission Control Protocol
TIC	Tecnologías de la Información y las comunicaciones
UID	Unique Identifier
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLSI	Very Large Scale Integration
XML	Extensible Markup Language

1 Introducción y objetivos

1.1 Introducción y antecedentes

La Organización Mundial de la Salud (OMS) define la e-Salud como “el uso de las Tecnologías de la Información y la Comunicación (TICs) para la salud incluyendo el tratamiento de los pacientes, la investigación, la educación del personal sanitario, el seguimiento de las enfermedades” [1].

Las actividades de e-Salud han tenido un crecimiento importante en los últimos años, especialmente en proyectos piloto y estudios de viabilidad de los servicios propuestos [2]. Sin embargo, esto no se traduce en una implantación real de estas tecnologías en entornos residenciales que ayudaran a agilizar los procesos de seguimiento de pacientes y la gestión de dichos datos, que por el momento son bastante rudimentarios.

A modo de estado del arte y para refrendar estos hechos se ha realizado un estudio del estado tecnológico actual en centros de día y residencias de la tercera edad. Se va a dividir esta tecnología en tres grandes grupos que estarán previsiblemente en diferentes estados de desarrollo dentro de los entornos residenciales. Por un lado se evaluarán todo tipo tecnologías que ayuden en la monitorización de residentes. Por otro lado, se evaluará el nivel de desarrollo en la implantación de infraestructura para comunicaciones. Y por último se evaluará cual es el nivel de desarrollo en cuanto a servicios de valor añadido, sistemas de almacenamiento de la información y herramientas para la gestión de estos entornos residenciales.



Figura 1: Bloques de una plataforma de gestión total de e-Salud

1.1.1 Tecnologías para la monitorización de residentes

Las tecnologías para la monitorización de residentes pueden dividirse en dos grupos, dispositivos para la identificación de residentes y dispositivos para la monitorización de constantes vitales.

- **Dispositivos para la identificación/autenticación de residentes:** Este tipo de dispositivos engloba cualquier tipo de tecnología que pueda identificar/autenticar únicamente a una persona, en este caso a un residente. Los más comunes son pulseras o tarjetas con algún tipo de tecnología incorporada para autenticar personas, es decir, garantizan que ese dispositivo (pulsera, tarjeta, etc.) cuenta con las credenciales apropiadas para acceder al sistema aunque no asegura que la persona que lo posea sea quien dice ser. Otra forma de identificación son el uso de características biométricas como son la huella dactilar [3], el iris [4] o identificación por voz [6]. Estos últimos métodos sí que son realmente métodos de identificación única de personas ya que aseguran que esa persona es quien dice ser.
- **Dispositivos médicos:** En cuanto a los dispositivos médicos, se podrían realizar multitud de divisiones dependiendo de la característica a evaluar. En este caso se van a valorar dependiendo del tipo de conectividad que ofrecen. Los cuales se pueden dividir en tres grupos, dispositivos sin conectividad, con conectividad cableada y con conectividad inalámbrica.
 - a) *Sin conectividad:* Este grupo de dispositivos médicos hace referencia a aquellos que, si bien tienen carácter digital, no disponen de conectividad; es decir que no sacan ningún tipo de señal al exterior.
 - b) *Con conectividad cableada:* A diferencia de los anteriores estos sí que sacan señales al exterior aunque lo hacen mediante cable (RS-232, Ethernet, USB, etc.).
 - c) *Con conectividad inalámbrica:* Estos dispositivos médicos tienen las mismas características que los anteriores con la diferencia que sustituyen los molestos cables por tecnologías inalámbricas. Todos los grandes fabricantes de dispositivos médicos tienen al menos un modelo de cada tipo de dispositivo médico con conectividad Bluetooth [6]. Otro tipo de tecnología de comunicación inalámbrica que se está incorporando a los dispositivos médicos es ZigBee, sin embargo solo existen prototipos experimentales [7].

En cualquiera de los dos casos el nivel de implantación tecnológica es nulo. En el caso de la identificación de residentes los centros de día y/o residencias de la tercera edad no utilizan ningún dispositivo para la identificación/autenticación. Y en el caso de los dispositivos médicos son utilizados los que no poseen ningún tipo conectividad.

1.1.2 Infraestructura para comunicaciones

En lo que se refiere a infraestructura para comunicaciones se englobará tanto si existe conexión a internet ADSL, si existe algún tipo de red WiFi o si disponen de algún tipo de dispositivo con conexión a internet móvil mediante 3G o similares.

Se ha realizado una exhaustiva búsqueda de algún estudio estadístico acerca de este tema pero no se han encontrado. Por lo tanto se ha contactado con la red de residencias de Aragón. Desde la red de residencias de Aragón se nos ha asegurado que el nivel de implantación tecnológica de infraestructuras para comunicaciones es muy bajo. En la mayoría de las residencias y centros de día existe conexión a internet fijo pero en muy pocos existe red WiFi, que en cualquier caso solo alcanzaría a la zona más próxima al router, en ningún caso a la totalidad del centro.

1.1.3 Servicios de valor añadido

Cuando se habla de servicios de valor añadido para un entorno residencial, se hace referencia fundamentalmente a software para su gestión. En este aspecto existen varias soluciones para la gestión de entornos residenciales desde el punto de vista administrativo pero ninguno incorpora el tema de la Salud de los residentes. Este tipo de soluciones son utilizadas en centros con gran número de residentes en los que su administración puede resultar complicada, aunque el nivel de implantación de este tipo de tecnologías en entornos residenciales sigue siendo bajo. Sin embargo, por ser el único tipo de solución existente se va a detallar las características de los más relevantes.

1.1.3.1 ResiPlus

ResiPlus es un software de gestión desarrollado por la empresa ADD Informática [8]. Actualmente es el software de referencia en cuanto a centros residenciales y centros de día se refiere. Es una solución integral que les permite de forma ágil y sencilla centralizar, en una única herramienta, todas las áreas de gestión del centro. Permite registrar, controlar y comunicar todos los acontecimientos que sean de interés, ya sean del residente o del centro en general. A continuación se comentan brevemente las diferentes áreas que cubre esta solución.

- **Área médica:** Permite la anotación de información médica confidencial, disponibilidad de datos de las consultas anteriores con independencia del médico que lo atendió, estandarización de protocolos de actuación, creación de planes farmacológicos, planes de seguimiento.
- **Área enfermería:** Permitirá la creación de agendas personales, planes de seguimiento y registros de administración de fármacos así como valoración de cuidados.
- **Área personal técnico:** En esta área cada profesional del equipo tendrá su área de trabajo que les permitirá planificar sus actividades.

- **Área personal atención:** Permitirá a los gerocultores establecer alertas sobre que residentes no cumplen con las pautas específicas, comunicar incidencias y registrar los resultados de los cuidados y atenciones brindadas.
- **Área farmacia:** Control de stock de medicamentos, generación de pedidos a farmacia, gestor de recetas y llevar un historial de consumos.
- **Área económica:** Permitirá una gestión económica integral, cajas, bancos y facturación.
- **Área general:** Control de calidad como encuestas, estadísticas y sugerencias o reclamaciones. Permitirá llevar un inventario de enseres y planificación de dietas.
- **Área personal:** Esta área contiene datos generales como entregas de material, evolución de contratos, control de número de horas de trabajo y gestión de turnicidad de los trabajadores.
- **Área proveedores:** Control de ciclos de compra, consolidación de pedidos, albaranes y facturas. Toda la gestión relacionada con proveedores
- **Agenda:** Control de agendas compartidas, de profesionales y residentes.

1.1.3.2 Resiges

ResiGes es un software de gestión de residencias para la tercera edad y centros de día [9] desarrollado por la empresa que lleva su mismo nombre, Resiges. Estructura su interfaz en diferentes módulos de gestión.

- **Residentes:** Desde este módulo se permite la creación y modificación de la ficha de un residente con todos los datos necesarios para su completa gestión.
- **Salud:** Desde este módulo se pueden gestionar todos los temas referidos a la salud de los residentes. Programación de tratamientos farmacológicos y curas.
- **Habitaciones:** Desde este módulo se permite gestionar la ocupación de las habitaciones de la propia residencia o centro de día y asignarlas a los residentes.
- **Gestión:** Desde este módulo se puede gestionar todo lo referido a proveedores y facturación.
- **Personal:** Este módulo permite la gestión del personal que trabaja en la residencia o el centro de día.
- **Bajas:** En este módulo se puede ver un historial de los residentes que han pasado por la residencia o el centro de día.
- **Utilidades:** Desde este módulo se permite tener una agenda de contactos de los residentes o cualquier persona de contacto que se desee.

1.2 Motivación

De una necesidad expresa solicitada desde el colectivo de Residencias de Aragón a la empresa Goodday Solutions S.L. y la posibilidad de dotar una mejor atención a las personas mayores que están en los centros residenciales nace la idea de este proyecto fin de carrera. Se realizó un proceso inicial de recogida de requisitos a partir de los cuales se diseñó la solución. Se detectó que un ahorro de tiempo en los procesos de monitorización de constantes vitales y su posterior gestión proporcionaría a sus cuidadores un tiempo extra que podría ser dedicado a dar una mejor atención a los residentes.

La multitud de tecnologías que involucran este proyecto y su integración conjunta en una solución que funcione de forma armónica supuso uno de los mayores retos. Además del reto que supuso su realización en una empresa real como es Goodday, integrado en un grupo de trabajo cooperativo y multidisciplinar como ocurre en este tipo de empresas jóvenes.

Se pretende dotar a los centros residenciales de una plataforma de gestión total, tanto del proceso de monitorización ubicua de constantes vitales como de su posterior gestión. Para ello se dotará al centro de un gestor de salud que incluya un *kit* de dispositivos médicos que cubran todos los tipos de constantes vitales medidas en el día a día, una solución software para el mismo que gestione la monitorización y un servicio automatizado de aviso a familiares. Además se dotará de una solución software de gestión de estas medidas y en general de la administración del centro.

Como resultado de este PFC se obtendrá un prototipo compacto que incluya la aplicación móvil (instalada en Smartphone), la aplicación de gestión (instalada en PC) y el kit de dispositivos médicos, dispuestos en una plataforma de cómodo desplazamiento para el personal sanitario. Además, se prevé evaluar su viabilidad mediante encuestas técnicas, clínicas y de satisfacción, para desarrollar diversos estudios pilotos en varias residencias de la tercera edad, como paso previo para su posterior lanzamiento comercial.

1.3 Objetivos

El objetivo general de este PFC es el desarrollo, diseño, implementación, despliegue y evaluación de una solución tecnológica de e-Salud en residencias de la tercera edad que se prevé derivará en la implantación de un proyecto piloto. Este proyecto piloto pretende monitorizar la toma de medidas diarias de cada residente y, con toda esa información digitalizada, permitir la generación de informes útiles para el seguimiento continuado de la salud además de distintos servicios de valor añadido, como puede ser avisos a familiares, entre otros.

Los principales objetivos específicos del PFC serán los siguientes:

- Diseño, desarrollo e implementación de una aplicación Android sobre Smartphone, que posibilite la toma de medidas diarias de cada residente. La aplicación constará de varios módulos: un módulo de autenticación y control de acceso (implementado mediante tecnología Near Field Communication, NFC), un módulo de comunicación que permita tener conectividad inalámbrica, implementada mediante tecnología Bluetooth, con diversos dispositivos

médicos, así como conexión con el servidor vía WiFi, un módulo de visualización (en el que se gestione toda la información y se presenten los datos biométricos adquiridos de una forma visualmente agradable) y también se plantea llegar a integrar un módulo de identificación biométrica (basado en huella dactilar para identificar a cada uno de los residentes a los que se les van a tomar las medidas).

- Diseño, desarrollo e implementación de una aplicación de gestión para la administración de usuarios y medidas que proporcionará múltiples servicios de valor añadido. Este software de gestión permitirá, por un lado, la administración de residentes, la administración de gerocultores y sus tarjetas de acceso NFC asociadas y, por otro lado, la visualización de las medidas almacenadas y la generación de informes útiles para el personal sanitario.
- Diseño, desarrollo e implementación de un módulo servidor para el almacenamiento y tratamiento de los datos. Este servidor alojará, por un lado, una base de datos relacional (de tipo MySQL) y, por otro lado, un servicio web (implementado en ASP .NET) que gestione las peticiones a dicha base de datos provenientes tanto de la aplicación Android (sobre smartphone) como de la aplicación de gestión (implementada en .NET C# sobre PC). Además, este módulo incorporará una funcionalidad para permitir el envío automático de avisos a médicos y familiares.
- Evaluación de los resultados obtenido mediante un proceso de encuestas realizadas al personal de la residencia donde se realizará el proyecto piloto que sirva como primera referencia de su aceptación.

1.4 Estructura de la memoria

La presente memoria está estructurada en dos partes diferenciadas. Por un lado, una parte principal dedicada a detallar los aspectos relacionados con el desarrollo propio de los objetivos comentados en el apartado anterior y, por otro lado, una segunda parte (en forma de anexos) donde se discuten aspectos que, si bien no son fundamentales para la comprensión del proyecto, sí que son importantes a la hora de obtener una mejor visión del mismo así como para profundizar en sus aspectos más técnicos.

La parte principal del proyecto se divide a su vez en los siguientes capítulos:

- Introducción y objetivos, comprende todo lo necesario para saber el estado tecnológico de los entornos residenciales en la actualidad, así como la motivación para la realización de este PFC, los objetivos del PFC y la estructura de la memoria.
- Análisis y diseño, en el que se comienza analizando los requisitos tanto demandados por los centros como los observados en las visitas a los centros residenciales. A partir de este análisis y, justificando siempre la elección de tecnologías, se procede a detallar el diseño de la plataforma apoyándose en los anexos disponibles en la segunda parte de la memoria.
- Desarrollo e implementación, en el que se describe detalladamente todo el trabajo realizado para la implementación de la plataforma.

- Resultados y evaluación, en el que se describe tanto el resultado final obtenido como su implantación real como proyecto piloto y la evaluación de estos resultados.
- Conclusiones y líneas futuras de trabajo, en el que se presenta una reflexión sobre los resultados del proyecto, así como las posibles líneas futuras de trabajo para continuarlo.

Finalmente, la segunda parte de la memoria incluye los siguientes anexos:

- Anexo 1, en el que se justifican las distintas alternativas de diseño para la identificación/autenticación de usuarios, la gestión de datos, el servicio web y la elección de la tarjeta identificativa.
- Anexo 2, en el que se analizan en detalle las tecnologías utilizadas, Bluetooth, NFC, .NET Framework, Android y SQLite.
- Anexo 3, en el que se profundiza en las tecnologías de seguridad y criptografía utilizadas.
- Anexo 4, en el que se muestra el diseño de la interfaz de usuario.
- Anexo 5, en el que se muestran las encuestas realizadas en la residencia objeto del proyecto piloto.
- Anexo 6, en el que se muestran los manuales de uso de los dispositivos médicos realizados

2 Análisis y diseño

En este capítulo se van a estudiar los requisitos fundamentales que deberán ser cumplidos por la plataforma y cuál ha sido la solución adoptada para satisfacer cada uno de ellos. Para ello se ha tenido contacto con varias residencias de la tercera edad mediante reuniones de las que se han extraído las características fundamentales a cumplir por la plataforma. Para poder comprender el porqué de muchas de las soluciones adoptadas conviene ser mencionado que la solución ha venido siendo rediseñada a medida que se han ido conociendo información clave para su correcto diseño.

2.1 Análisis del problema

En este apartado se va a analizar el problema a abordar que se desprende de la identificación de una baja eficiencia y una gran pérdida de tiempo en los procedimientos cotidianos de toma de constantes vitales y su procesado posterior. Este problema fue identificado y trasladado por parte de la jefa de enfermería de una residencia aragonesa.

2.1.1 Toma de contacto con el centro residencial

Como ya se ha comentado anteriormente el diseño ha ido evolucionando con el paso del tiempo. Gran parte de estas evoluciones han nacido de la identificación de necesidades reales fruto de la continua comunicación con las residencias. En este apartado se va a intentar explicar la línea cronológica en la comunicación con los centros y las principales funcionalidades que se desprendieron de ellas.

En primer lugar se concertó una reunión con la jefa de enfermería de una de residencia referente en Aragón, ya que ella es la responsable de la coordinación de la toma de medidas y su posterior procesado. Ella había detectado una muy baja eficiencia y gran pérdida de tiempo en el proceso de medición de la glucosa, el cual se realizaba a los residentes del centro que padecen diabetes, algo más de treinta en su caso, tres veces al día, una en cada una de las comidas diarias. De esto se desprende la existencia de un volumen de datos grande, alrededor de las tres mil glucometrías mensuales.

Durante este primer contacto se hizo una labor de conocimiento del entorno de trabajo de un centro residencial, de inspección de la infraestructura existente en el centro residencial y de sus procesos de trabajo cotidianos, con el objetivo de comprender el día a día de estos centros para que el diseño de la plataforma se ajuste lo mejor posible a la forma de trabajar existente y así interfiera lo menos posible. El éxito o fracaso de este tipo de plataformas depende en muchas ocasiones de no tratar de imponer unos procesos de trabajos muy diferentes a los existentes.

De esta primera reunión se extrajeron los requisitos fundamentales a cumplir por la plataforma aunque, como se ha comentado anteriormente, las continuas conversaciones añadieron nuevos requisitos. Éstos pueden ser divididos en dos grandes bloques fundamentalmente, los requisitos a cumplir por la plataforma demandados por el centro residencial y los extraídos de la observación de los procesos y la infraestructura del centro residencial.

2.1.2 Requisitos demandados

En este apartado se van a enumerar los requisitos a cumplir por la plataforma que fueron demandados de forma explícita por el centro residencial. En la medida de lo posible estos requisitos se han intentado satisfacer tal y como se me trasladaron.

- **Proceso ágil de toma de medidas:** La baja eficiencia en el proceso, la gran pérdida de tiempo y el elevado volumen de glucometrías a realizar hacen de la agilización en la realización de éstas el requisito fundamental a cumplir por la plataforma.

Para entender esta baja eficiencia hizo falta conocer el protocolo seguido para la toma de medidas en un centro residencial. Para ello además de oírlo de boca de la jefa de enfermería del centro, la cual establece los protocolos a seguir, se estuvo observando *in situ* una de las rondas de medida de la glucosa tomando notas sobre las acciones a realizar, tiempos y datos relevantes en el proceso.

El hasta ahora proceso de medidas clásico tenía varios pasos:

1. El personal sanitario busca en recepción el historial médico del residente.
2. Con el historial, el sanitario busca al residente y le toma la medida.
3. La medida es apuntada a mano en el historial del residente.
4. El sanitario vuelve a recepción dónde archiva las medidas tomadas en papel para la futura generación de un informe.

Como se puede observar el proceso en sí no es nada eficiente ya que se pierde mucho tiempo en la búsqueda del historial del residente y la posterior generación de informes es muy tediosa ya que se tienen que transcribir a mano al ordenador y generar el informe a través de un documento *Excel* de forma muy rudimentaria.

Como se ha comentado anteriormente en una primera fase sólo se contempló la realización de glucometrías pero a medida que se fue avanzando en el desarrollo se identificó que este proceso de toma de medidas se repetía para todos los tipos de constantes vitales. Por esto se decidió ampliar los tipos de mediciones contemplados a todos los que un centro residencial realiza, que son: medición de la presión arterial, pulsioximetría, control de peso y medición de la temperatura, además de la glucometría. Esta ampliación del tipo de mediciones contempladas permite la unificación a la hora de generar informes de un residente.

- **Identificación de residentes:** Para el centro residencial un requisito fundamental a la hora de identificar a un residente para la toma de medidas, fue que los residentes no llevasen ningún tipo de accesorio añadido como pulseras o tarjetas. Por dos motivos principalmente, el primero es que los residentes tienden a no llevar estos objetos consigo como por ejemplo una tarjeta identificativa, el uso de unas pulseras identificativas se desechó ya que las personas mayores podrían dañarse con estas pulseras.
- **Identificación del personal sanitario:** Otro tema importante que se me trasladó fue el de la implementación de un sistema de identificación del

personal sanitario que realiza la toma de medidas con el fin de tener contemplado quién realiza cada medida. En este caso, el deseo fue que para acceder a la plataforma se hiciese mediante algún tipo de accesorio que permita al sanitario acceder a la plataforma para realizar las medidas con ubicuidad.

- **Generación de informes:** El último gran requerimiento por parte del centro residencial fue el de la generación de informes útiles para los médicos con las medidas realizadas a los residentes. En este punto, a diferencia de los anteriores en el que los requerimientos provenían del centro residencial Parque Dorado, la aportación de información provino tanto de Parque Dorado como de la Residencia Avenida.

El tema en el que los dos centros coincidían era en que la plataforma debía poder generar informes de cada residente individualmente, con el fin de poder ser trasmítidos al médico para que controle la evolución de cada residente. Sin embargo, cada uno de los centros tenía procesos diferentes para la generación de informes. Una residencias con muchos residentes, hace controles periódicos a sus residentes, por ejemplo generación de informes una vez al mes de todas las constantes vitales por separado. Mientras que las residencias más modestas acostumbran a generar informes con todas las constantes vitales cuando existe algún tipo de incidencia remarcable o por la que el residente tenga que ser enviado al hospital, además de la generación de informes periódicos.

Esto nos lleva a que se nos son requeridos dos tipos diferentes de informes, los que llamaríamos *informes periódicos* en los que se podría seleccionar el rango de fechas y el tipo de constante que se desea visualizar, y los informes por *incidencia aguda* los cuales permitirán visualizar todas las constantes vitales tomadas en un día concreto.

- **Aviso a familiares o centro médico:** Aunque no fue trasladado como indispensable para el funcionamiento de la plataforma, un servicio de aviso a familiares, contactos del centro médico y personal sanitario de la residencia en tiempo real dotaría a la plataforma de un gran valor añadido. El aviso debería contener el nombre y apellidos del residente junto con el tipo y el valor de la medida que se acaba de realizar.

2.1.3 Requisitos observados

Existen otros factores que no fueron transmitidos por el personal de los centros pero que determinarán el diseño final de la plataforma. En general estos requisitos serán mucho más específicos mientras que los anteriormente comentados van más en la línea de la idea global de funcionamiento.

A continuación se enumeran una serie de requisitos que va a tener que cumplir la plataforma marcados por la estructura intrínseca de un centro residencial:

- **Dispositivos médicos inalámbricos + bloque de comunicación inalámbrica:** Una vez se observó el proceso completo de toma de medidas del centro residencial, lo primero que salta a la vista es que no existe un lugar fijo para su realización, puede ser realizada tanto en el comedor del centro, como en la sala de estar o incluso en las habitaciones de los residentes. Esto nos lleva a que necesitamos dispositivos inalámbricos y con conectividad, además de algún sistema de identificación en itinerancia. Los que tienen actualmente, sean digitales o no, no tienen ningún tipo de conectividad lo cual es indispensable si se desean evitar errores humanos en la transcripción.
- **Solución online y offline para la toma de medidas:** El mismo día que se hizo el estudio de los procesos de toma de medidas, se fue realizando un control de conectividad WiFi en todos los puntos de toma de medidas antes mencionados. Se comprobó que la conexión a internet era aceptable en la sala de estar, la cual está cerca del *router WiFi*, pero ni en el comedor, ni mucho menos en las habitaciones existía conexión a internet.

Por lo tanto se pensó que la solución debería ser perfectamente funcional con y sin conexión a internet, lo que implica diseñar un sistema de almacenamiento local en caso de no poder enviarse una medida al servidor por no haber conexión a internet.

- **Dispositivo móvil como proxy:** Observando el proceso de toma de medidas actual se ve que el profesional sanitario encargado de realizar este proceso pierde mucho tiempo en realizar la búsqueda de los expedientes de los residentes pero no en el procesado de las medidas que acaba de realizar, simplemente las anota en el papel. Por lo tanto, se deduce que ellos no son los encargados de realizar el procesado sino que es la jefa de enfermería, como se corroboró en los dos centros con los que se ha contactado.

Esto nos lleva a que el dispositivo móvil, o más concretamente el software que se diseña para él tendrá que ser lo más ágil posible y sin nada de procesado. Por ello se ha pensado en usar un dispositivo pequeño que actúe básicamente como *proxy*, recibiendo la medida y enviándola junto con los datos del residente sin realizar ninguna acción sobre esta medida.

- **Base de datos muy interrelacionada y jerarquizada:** Otro aspecto que se observó y que, como la mayoría de este proyecto, fue evolucionando conforme se adquiría un mejor conocimiento del funcionamiento interno de un centro residencial. Un centro de este tipo tiene una estructura muy jerarquizada e interrelacionada entre todos los componentes del centro, residentes, y sus familiares, administradores, gerocultores, enfermeros y médicos. Todos ellos tienen funciones muy concretas y bien definidas en esta estructura.

Por lo tanto, esto nos llevó a que el sistema de almacenamiento de la información tendrá grandes interrelaciones entre todos ellos.

2.2 Diseño de la solución

Una vez se han establecido los requisitos que debe cumplir la plataforma, en este capítulo se va a proceder a explicar el porqué de la solución adoptada en detrimento de otras opciones.

2.2.1 Arquitectura global

En este capítulo se va a proceder a introducir a grandes rasgos los módulos que forman la arquitectura de la plataforma y nombrar las tecnologías adoptadas para cada una de las partes.

Como se puede ver en la figura 2, se ha adoptado una arquitectura típica *Cliente-Servidor*, en este caso clientes serán tanto la red móvil como el ordenador personal. El servidor es el encargado de almacenar y suministrar la información a los clientes, y estará compuesto por dos grandes bloques, la base de datos y el servicio web. Como se explicará más detalladamente en su capítulo correspondiente, su diseño ha sufrido múltiples cambios a la vez que se avanzaba en su desarrollo. Para el almacenamiento de la información se ha utilizado una base de datos MySQL y para la comunicación con los clientes (Ordenador personal y *Smartphone*) un servicio web.

Del lado del cliente existen tres grandes bloques, los dispositivos médicos, el *Smartphone* y el ordenador personal. Los dispositivos médicos tendrán conexión con el *Smartphone* vía *Bluetooth* que hará de proxy y se comunicará con el servicio web vía internet. Para ello hemos seleccionado un *Smartphone Android* para el que se diseñará una aplicación y que cuenta con una base de datos SQLite interna. Respecto al ordenador personal se diseñará una aplicación para ser instalada en un ordenador con sistema operativo *Windows* que permita gestionar toda la información de la residencia desde el mismo.

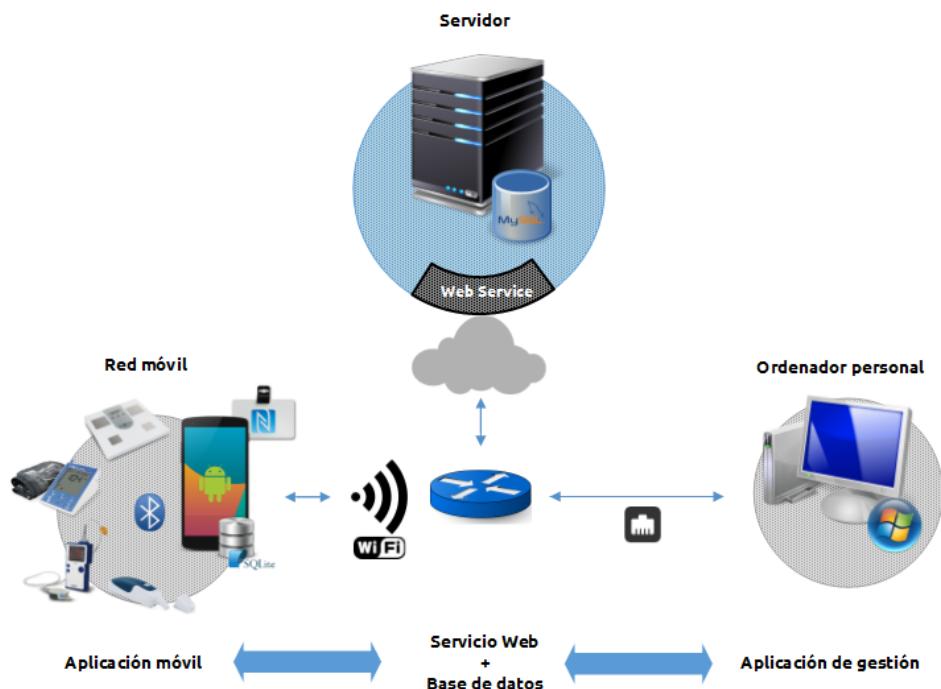


Figura 2: Arquitectura global de la plataforma

2.2.2 Cliente

A continuación se va a explicar el diseño de cada bloque del lado del cliente más exhaustivamente, comentando por qué de este diseño y sus ventajas e inconvenientes respecto a otras tecnologías ya existentes y se comentará la evolución en el diseño conforme se iba desarrollando.

2.2.2.1 Dispositivos médicos

Existen dos fases muy marcadas en la evolución que se ha seguido en la elección de los dispositivos médicos a utilizar. Una primera fase en la que se contempló un único tipo de medidas, la glucometría y una segunda fase en la que se extendió a todas las constantes vitales que son medidas en un centro residencial, presión arterial, temperatura, peso, pulsioximetría y la ya mencionada glucometría.

Con el fin de poder llegar a ser un producto comercial se valoró los dispositivos que iban a ser utilizados ya que existe una normativa que deberán cumplir. Pero primeramente hubo que elegir las características técnicas.

- **Bluetooth**

En cuanto al módulo de comunicación inalámbrica se hizo una amplia búsqueda de los dispositivos médicos que disponían de ella. Existen dos tipos de dispositivos médicos con un módulo de comunicación inalámbrica. Por un lado dispositivos con comunicación *Bluetooth* como el que se venía usando hasta el momento y por otro lado, dispositivos con comunicación *ZigBee* tecnología mucho menos avanzadas comercialmente como se explicó en el capítulo 1.1.1 , hablando en el ámbito médico.

Por tanto, se ha escogido *Bluetooth* frente a las otras alternativas, por la madurez que presenta este tipo de comunicación y la amplia gama de dispositivos existentes en comparación con *ZigBee*.

Una vez escogida la tecnología *Bluetooth* para la capa de transporte hay que elegir el tipo de dispositivo *Bluetooth* a emplear. En el ámbito de los dispositivos médicos, existen dos alternativas muy diferenciadas, en función de si estos son estándares o si no lo son. Cada una de estas alternativas, va a imponer la forma de llevar a cabo la comunicación *Bluetooth* (ver capítulo 8.2) en cuanto a lo que a las capas superiores de la pila se refiere, teniendo que emplear el perfil *Health Device Profile* (HDP) en el caso de dispositivos médicos estándares y el perfil *Serial Port Profile* (SPP) en el caso de dispositivos médicos no estándares.

En principio, parecería lógico escoger una gama de dispositivos médicos que usen el perfil médico de *Bluetooth* por estar estandarizado y hacer la integración en la solución más sencilla. Sin embargo, se ha elegido una gama de dispositivos no estándares que usan el perfil puerto serie (SPP) principalmente por dos motivos. El primero de ellos es que el número de dispositivos que implementan el perfil médico HDP es muy reducido [10] y el segundo y fundamental motivo es que la inmensa mayoría de los fabricantes no son europeos por lo que adquirirlos para uso comercial implica unas trabas legales y administrativas hoy por hoy inasumibles.

La elección de dispositivos que usan el perfil SPP implicará un trabajo de ingeniería inversa para interpretar el protocolo de comunicación propietario de cada uno de los dispositivos e implementarlo a nivel *software*. Estos protocolos se adquieren mediante la firma de acuerdos *Non Disclosure Agreement* (NDA) con los distribuidores.

2.2.2.2 *Smartphone*

Como se ha comentado al hacer referencia a la arquitectura general de la plataforma, se ha escogido un *Smartphone Android* el cual se utilizará como elemento intermedio entre los dispositivos médicos y el servidor. Existen varios requisitos de los anteriormente mencionados que han hecho que la elección sea esta frente a otras como podría ser una *Tablet Android* o algún tipo de dispositivo con otro sistema operativo como *iOS*, *Windows Phone* o *BlackBerry OS*.

A. Tecnologías

- **Dispositivo pequeño y con poca capacidad de procesado**

El requisito principal es conseguir una toma de medidas ágil en la que el dispositivo móvil haga una mera función de intermediario, *proxy*, sin realizar procesado de grandes volúmenes de datos, como por ejemplo elaboración de informes, gráficas o cualquier tipo de análisis. Por esto se desechó el uso de una *Tablet* que nos proporcionaría un abanico de opciones de visualización mucho más amplio, pero perderíamos manejabilidad que es lo que se necesita.

Por ello se pensó en el uso de un dispositivo más pequeño como un *Smartphone*.

- **Acceso a Internet**

Parece obvio, pero el dispositivo elegido deberá tener acceso a Internet para atender al requisito de la movilidad y a que el *Smartphone* se comunicará con el servicio web a través de peticiones *http* vía Internet.

Se optó por un *Smartphone* ya además de poseer comunicación mediante *WiFi*, está la opción de contratar una tarifa de internet móvil 3G en el caso de que un centro residencial no tuviese conexión *WiFi*. Esto dotaría a la plataforma de más flexibilidad a la hora de implantarla comercialmente.

- **Bluetooth**

En el capítulo 2.2.2.1 en el que se han detallado las características que van a tener los dispositivos médicos. Se ha dicho que usarán *Bluetooth* para comunicarse con el dispositivo móvil, por lo tanto éste deberá soportar este tipo de comunicación a su vez. No es un problema ya que todos los *Smartphones* cuentan con ésta tecnología pero ha de mencionarse por ser una característica fundamental.

- **Near Field Communication (NFC)**

Del requisito de que el personal sanitario que realiza las medidas se identifique/autentique en la plataforma mediante algún tipo de dispositivo llevable, se pensó que la autenticación podría realizarse usando una tarjeta identificativa que contuviese las credenciales de acceso a la plataforma y se leyese al aproximarla al lector. Este tipo de tecnologías está muy extendido en la vida cotidiana y la aceptación a su uso sería más favorable.

Se ha pensado en el uso de NFC por ser una tecnología emergente, de gran seguridad y que dotará a la plataforma de gran agilidad. Esto nos restringe la gama de *Smartphones* que se pueden usar, primero porque la tecnología NFC es una tecnología no contemplada, por el momento, en los sistemas operativos *iOS*, pero la gama de dispositivos *Android* que la soportan es muy amplia.

- **USB On-the-Go (OTG)**

La identificación de residentes mediante alguna característica biométrica como huella dactilar implica la adhesión de un lector ya que de los *Smartphones Android* ninguno contiene un lector de huella dactilar integrado. Sólo *Apple* con su *iPhone 5S* lo incluye, aunque no con los fines en el marco de este PFC, y ya hemos dicho que los sistemas operativos *iOS* han sido descartados. Por lo tanto sería necesario tener la posibilidad de adherir un lector de huella dactilar.

En el mercado se encuentra una gama bastante escasa de lectores que se puedan conectar a un *Smartphone Android* y en todo caso necesitan ser alimentados por el *Smartphone* para funcionar. Esto implica que el *Smartphone* tiene que ser capaz de ser *host* y alimentar otros dispositivos a través de su conector microUSB, la tecnología pensada para ello es llamada USB On-the-Go. La gama de *Smartphones* que soportan OTG es muy limitada ya que la batería es una de las grandes limitaciones de este tipo de dispositivos móviles que no están diseñados para alimentar a otros.

Sin embargo el uso de un *Smartphone* con esta característica ha quedado aplazado ya que la identificación mediante huella dactilar implica una inversión de tiempo que excedía la establecida en el plan de trabajo de este PFC.

- **SQLite**

Anteriormente se ha planteado la necesidad de una solución funcional tanto *online* como *offline*. Por tanto, las medidas tomadas en un momento en el que no exista conexión a Internet deberán ser almacenadas para su posterior envío y que así no haya pérdidas de información. Esto implica que el *Smartphone* deberá tener un contenedor de información. Planteando el uso de SQLite (todos los *Smartphones Android* poseen una) ya que es ideal para este tipo de sistemas operativos por su pequeño tamaño.

B. Aplicación Android

Se diseñará e implementará una aplicación *Android* para ser instalada en el *Smartphone* que constará de los cinco grandes bloques que se pueden ver en la figura 3. Como se puede observar el diagrama de flujo responde a una estructura muy vertical, es decir muy guiada, al estilo de una fábrica de producción en cadena, lo cual implica una alta eficiencia ya que prácticamente no se necesitan tomar decisiones acerca del flujo a seguir. A continuación se explicará la función que tendrá cada uno de estos bloques en la aplicación.

- **Autenticación de personal sanitario**

Se proporcionarán dos métodos para acceder a la plataforma. Aunque se nos pidió que el acceso a la plataforma fuese mediante una tarjeta de proximidad se ha creído conveniente incluir el clásico método de acceso de introducir usuario y contraseña.

Para la autenticación mediante tarjeta NFC se utilizará el identificador único (*Unique Identifier, UID*) el cual es único en el mundo e irá asociado a una única persona en nuestra plataforma.

En cuanto a la autenticación clásica simplemente se comprobará si las credenciales introducidas coinciden con las almacenadas en su perfil.

- **Identificación de residente**

Como ya se ha comentado la identificación mediante biometría se ha considerado inabordable, en términos temporales por la demora a la hora de conseguir un acuerdo NDA y la API de desarrollo. Para este PFC pero está como una línea futura a seguir. Por lo tanto se ha pensado en un módulo de selección manual en el que el personal sanitario pueda elegir de entre todos los residentes dados de alta en la plataforma.

- **Adquisición de medidas**

En este módulo se ha diseñado para que la adquisición de medidas mediante *Bluetooth* sea lo más transparente al usuario. La plataforma adquirirá las medidas sin importar el tipo de dispositivo médico siempre que sea uno de los contemplados y las mostrará en la pantalla del *Smartphone*.

- **Envío / Almacenamiento de medidas**

Este módulo, dependiendo de si existe conexión a Internet o no, enviará al servidor o almacenara en la base de datos local SQLite del *Smartphone* la medida previamente adquirida.

- **Aviso a familiares o centro médico**

El aviso a familiares, a los contactos de la residencia (administradores y médicos) y a los contactos del centro médico se realizará mediante el envío de un *sms* que podrá ser enviado a alguno de esos contactos.

También se proporcionará la posibilidad de la introducción manual de un número de teléfono.

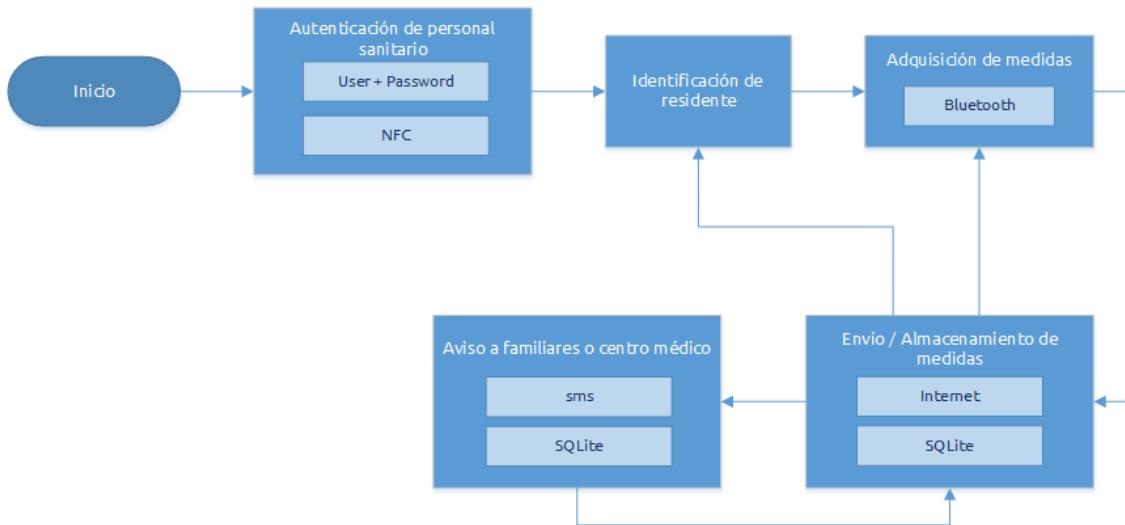


Figura 3: Diagrama de flujo de la aplicación Android

C. Base de datos SQLite

SQLite es un sistema de gestión de bases de datos relacional basado en SQL relativamente pequeña para sistemas de recursos limitados como son los *Smartphones*. Va ser utilizada para el funcionamiento *offline* de la aplicación. Para ello necesitaremos hacer una copia de la base de datos MySQL, aunque únicamente las tablas necesarias para poder funcionar. También se utilizará para almacenar las medidas y los sms no enviados.

Para que esta base de datos local esté lo más actualizada posible en el momento en que no haya conexión a internet se ha diseñado un sistema de sincronización. La aplicación actualizará la base de datos SQLite siempre al iniciar la aplicación, además podrá ser forzada una vez estemos en el módulo de autenticación de personal sanitario o en el de identificación de residentes.

En cuanto a la subida de datos pendientes al servidor (medidas y sms), en el caso que se detecte que existe conexión a internet se procederá a la comprobación de la existencia de estos datos pendientes. En caso afirmativo se enviarán y si el envío se ha realizado con éxito se eliminarán de la base de datos SQLite.

2.2.2.3 Ordenador personal

A. Tecnologías

Para la elección del tipo de dispositivo a utilizar para la gestión de medidas del centro residencial no hubo que evaluar tantas posibilidades ya que los centros residenciales ya tienen sus propios sistemas informáticos. Del *feedback* de estos centros se dedujo que el personal de administración utiliza uno o varios ordenadores personales y en todos los casos el sistema operativo es *Windows* pudiendo variar la versión instalada en cada uno de ellos. La versión más antigua identificada es *Windows XP* por lo que la aplicación que se diseñe deberá funcionar para esta versión y superiores hasta el actual y *Windows 8.1*.

Se ha decidido diseñar una aplicación de formularios (*Windows Forms*) en la cual se implementarán los módulos fundamentales.

B. Aplicación de gestión

La aplicación tendrá cuatro grandes módulos que serán accesibles desde su interfaz principal y que serán los necesarios para poder realizar una gestión eficiente de toda la plataforma. A ella se accederá mediante la introducción de unas credenciales de acceso conocidas. Como se puede apreciar en la figura 4, el diagrama de flujo es mucho más horizontal lo cual permitirá seleccionar entre múltiples acciones cual se va a realizar sin tener que volver a empezar.

- **Gestión de residentes**

Este módulo deberá proporcionar al personal de administración del centro sanitario todas las herramientas necesarias para poder realizar una gestión eficiente de este tipo de perfiles. Se podrán realizar tres tipos de acciones sobre el perfil de residente: crear un nuevo perfil, modificar un perfil existente y eliminar un perfil existente.

Además de los datos personales de cada perfil que serán obligatorios para la creación del mismo se permitirá asociar personas de contacto y direcciones al perfil.

- **Gestión de personal sanitario**

Para dar homogeneidad a la aplicación, se permitirán las mismas tres acciones sobre el perfil de personal sanitario que con el de residente, crear un nuevo perfil, modificar uno ya existente y eliminar un perfil existente. Este perfil tendrá asociado a su vez un rol que definirá sus funciones dentro del centro residencial y que restringirá su acceso a ciertas funciones de la plataforma dependiendo de su rango.

- **Gestión de acceso al sistema**

Existen dos métodos de acceso a la plataforma, mediante *Smartcard* (*Smartphone*) y mediante usuario y contraseña (*Smartphone* y *ordenador personal*) y este módulo permitirá realizar la gestión de quién y cómo accede a la plataforma.

En cuanto al método clásico, se proporcionará a cada profesional una contraseña generada aleatoriamente que se enviará la dirección de e-mail que se haya proporcionado. Mientras que el nombre de usuario siempre se será el DNI de cada uno que además lo identificará únicamente en todo el sistema. Tendrá que proporcionarse un método para resetear la contraseña en caso de olvido.

Para la gestión de *Smartcards* se proporcionará una interfaz exclusiva. Se podrán realizar cuatro acciones, dar de alta una tarjeta en el sistema asignando una etiqueta a su UID para simplificar su gestión, borrar una tarjeta del sistema, asociar a un profesional una tarjeta dada de alta y desasociar una tarjeta a un profesional. Se ha pensado en estas acciones ya que el personal sanitario es susceptible a cambios (altas y bajas), las tarjetas son limitadas y, de este modo podrían ser reutilizadas y, por último, siempre existirá la posibilidad de que un trabajador extravíe la tarjeta y, en este caso, habría que desasociársela así como darla de baja del sistema.

- **Generación de informes y pre-visualización de medidas**

En este caso, y como en casi todo el diseño, han existido dos fases: una primera en la que este módulo se diseñó para generar informes personales y periódicos. A medida que avanzaron las conversaciones comenzó una segunda fase en la que se diseñó también para poder generar informes en caso de incidencia aguda, solamente con las medidas recientes (de un único día) llevadas a cabo sobre un residente en concreto que por motivos de salud había de ser derivado al hospital. Estos informes serán generados en formato *pdf* para que no puedan ser fácilmente modificados una vez creados.

Además hablando con el personal de administración de los centros también se creyó conveniente introducir un interfaz en el que poder pre-visualizar las medidas que se están haciendo en el centro.

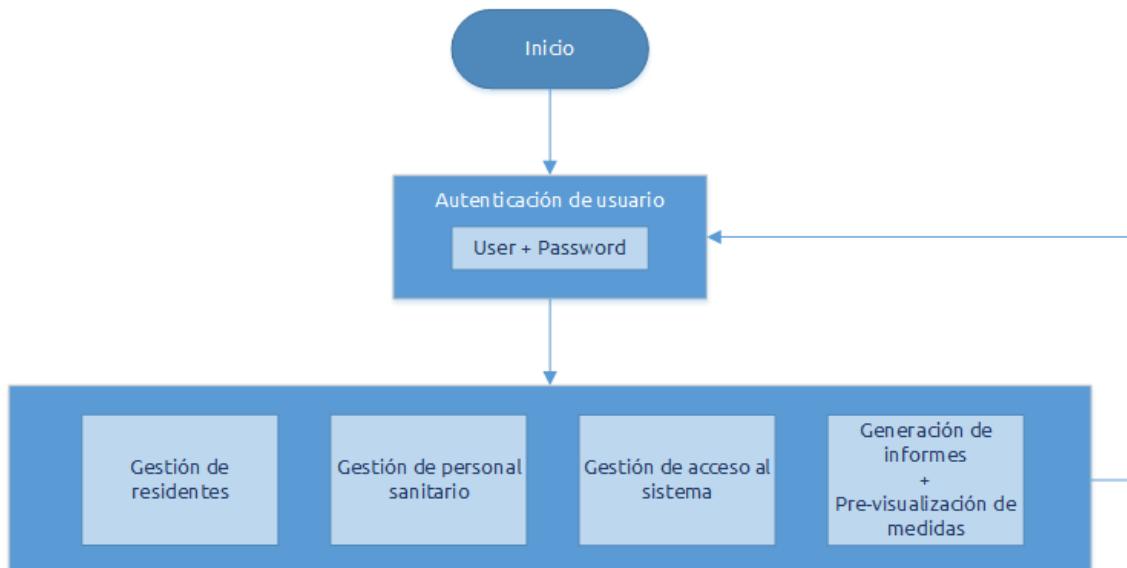


Figura 4: Diagrama de flujo de la aplicación de gestión

2.2.3 Servidor

Llamamos servidor al conjunto formado por la base de datos y el servicio web. La base de datos almacenará la información de la solución y el servicio web gestionará la entrada y salida de información de la base de datos y, por tanto, del servidor.

2.2.3.1 Base de datos MySQL

Como se puede ver en la figura 5, debido a la estructura real de un centro residencial existe la necesidad de una base de datos muy jerarquizada y fuertemente interrelacionada, lo que nos llevó a la elección de usar una base de datos relacional como *MySQL*. La información se almacenará en tablas conectadas mediante claves comunes reproduciendo la estructura real de la información de un centro residencial.

Se utilizará el software oficial *MySQL Workbench* para su desarrollo por su funcionamiento contrastado.

Las razones de esta elección se basan en lo siguiente:

- Fuertes interrelaciones entre los elementos que constituyen un centro residencial.
- Es multiplataforma, por lo tanto puede funcionar en diferentes sistemas y con diferentes lenguajes de programación.
- Ofrece protección frente a accesos indeseados.
- Es gratuita y proporciona un rendimiento similar a cualquier sistema de pago.

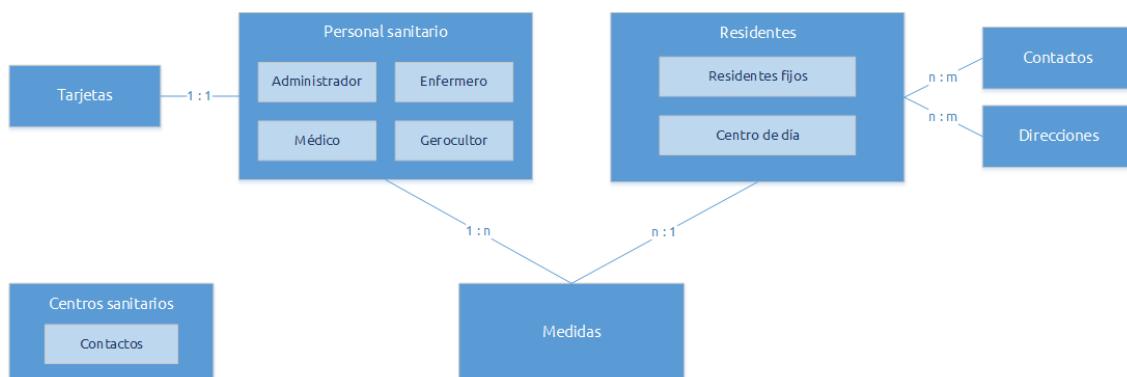


Figura 5: Estructura de una base de datos de una residencia de la tercera edad

2.2.3.2 Servicio web

Una vez se decide desarrollar un servicio web, hay que decidir sus características dependiendo del uso que se le vaya dar como la arquitectura y tecnología de desarrollo más apropiada, así como el tipo de seguridad que se va a incluir en el mismo.

2.2.3.2.1 Arquitectura

En el contexto móvil en el que se enmarca esta plataforma, se ha optado por una arquitectura tipo *REST*. Se ha optado por este tipo porque a diferencia de la arquitectura *SOAP* se centra en el uso de estándares *http* para la transmisión de datos sin necesidad de una capa adicional. Además el consumo de los datos, además de liviano, se articula de forma muy sencilla mediante peticiones *POST*, *PUT*, *GET* y *DELETE*.

Como contenedor de la información se utilizara *JSON* y, aunque también se podría utilizar *XML*, se ha optado por esta opción porque su lenguaje es mucho menos pesado. Esto nos permitirá mejorar la velocidad de acceso en un escenario de recursos escasos como es el móvil, aligerando la carga de datos que se transmiten.

2.2.3.2.2 Tecnología

Para la implementación de esta arquitectura se utilizará *ASP.NET Web API*. Se ha optado por esta tecnología porque facilita el desarrollo de servicios *http* para clientes de todo tipo y, en especial, para dispositivos móviles.

ASP.NET Web API es la plataforma idónea para la creación de servicios web *REST* en *.NET Framework 4.5*.



Figura 6: Arquitectura ASP.NET

2.2.3.2.3 Seguridad

El tema de la seguridad es clave en este tipo de aplicaciones tanto móviles como fijas y más aún cuando se manipulan datos sensibles como son los datos médicos protegidos por la *Ley Orgánica de Protección de Datos* (LOPD). La seguridad se concentrará en el lado del servidor. Una de las características de la arquitectura REST es que son sistemas sin estado, es decir que cada mensaje *http* contendrá toda la información necesaria para interpretarse. Por ello, se implementarán los siguientes sistemas de seguridad que garantizarán la completa fiabilidad de los datos recibidos.

- ***https***

Las credenciales de acceso viajarán en cada petición que el cliente realice al servidor. Por esto todas las comunicaciones se realizarán usando *Secure Sockets Layer (SSL)* para garantizar la total seguridad de los datos intercambiados. Para ello se compró un certificado SSL de autenticación.

Esto proporcionará autenticación del sitio web, además de protección contra ataques *man-in-the-middle* y encriptación bidireccional.

- ***Basic Authorization***

Las credenciales del usuario que accede a la plataforma viajan en cada petición para ser cotejadas con las almacenadas en la base de datos. Un error grave sería almacenar estas contraseñas en forma de texto limpio sin encriptar porque en caso de que alguien pudiese ver la base de datos conocería las credenciales de acceso. Por ello, se plantea almacenar estas contraseñas en forma de *hash* de la que, teóricamente, es imposible encontrar su función inversa. Además, se plantea crear un *salt* aleatorio para dificultar aún más que estas contraseñas sean des-encriptadas. Se propone el esquema de criptografía basado en el método *Basic Authorization* que se detallará en el capítulo 3.2.2.1 para almacenar las contraseñas.

- ***Advanced Encryption Standard (AES)***

En el momento en el que se pretende desarrollar una aplicación que manipulará y almacenará datos médicos aparecen trabas legales debido a que esta información médica no puede estar asociada a quien pertenece de forma directa. Esto implica la implementación de algún tipo de encriptación. Se ha elegido AES como algoritmo simétrico de encriptación para las medidas que se almacenarán como un texto encriptado.

Este es un método muy seguro para almacenamiento de datos ya que la clave (128bits) solo es conocida por el propietario. Aún no se conocen ataques satisfactorios sobre este algoritmo de encriptación (ver capítulo 9.2)

2.2.3.3 Despliegue

Debido a que el fin de esta plataforma es que pueda estar instalada en varios centros residenciales, aparece la problemática de cómo se haría el despliegue en cada uno de estos centros. Como es lógico, ésta realidad se hizo patente una vez el proyecto estaba muy avanzado, por lo tanto volveremos a hablar de las dos fases en el diseño.

- **Diseño individual**

Tal y como se diseñó la plataforma en una primera fase implicaba su personalización para cada centro residencial en que se instale. En concreto, esta personalización sería la de un servicio web escuchando en un puerto en concreto y una base de datos para cada centro sanitario.

Problemática de crecimiento

La instalación de la plataforma en una residencia implicará una serie de pasos que de tener que repetirse con asiduidad repercutiría en una gran pérdida de tiempo. A este proceso de puesta en marcha se le llama *Set-Up* e implicará la creación de una base de datos individual para cada centro y la publicación en el servidor un servicio web que apunte a esta base de datos. Y por tanto adaptar las dos aplicaciones para que utilicen la base de datos y el servicio web que les corresponde.

Además aparece el problema de la actualización de versiones para la plataforma, en el caso en el que se deseara dotar a los centros con una versión de la solución más avanzada y con más funcionalidades supondría tener que actualizar uno a uno todos los centros teniendo que ir personalmente a realizar la actualización.

- **Diseño común**

Este nuevo diseño consiste en tener una base de datos para cada centro y adaptar el servicio web para que todas las aplicaciones lo utilicen y sean dirigidas a la base de datos que les corresponde. Para esto se ha pensado crear una base de datos intermedia con los datos de los centros residenciales y las credenciales de acceso a su base de datos. De este modo las aplicaciones se descargarán estas credenciales y las utilizarán para acceder a su base de datos.

Como vemos, esto solo solucionaría el problema de la creación de múltiples servicios web pero, aún quedaría el problema de las actualizaciones. El mayor problema es la actualización de la aplicación de gestión la cual estará instalada localmente en el ordenador personal del centro. Por ello se plantearon dos opciones:

Funcionamiento en remoto

Esto quiere decir que la aplicación no estaría físicamente en su ordenador sino que se crearía un acceso remoto a la aplicación que estaría localizada en nuestro servidor y por tanto podríamos modificarla. Este sistema se ha probado y solucionaría el problema de tener que ir a instalar la actualización al centro sanitario correspondiente pero se ha comprobado que al funcionar a través de internet, primero necesitarían una conexión rápida y estable y además nos

obligaría a prescindir de muchas funciones gráficas que se ven limitadas por no poder refrescarse a una velocidad aceptable mediante la red.

Publicación de actualizaciones

La solución que se ha adoptado es la de publicación de actualizaciones en nuestro servidor. De modo que cada vez que se inicie la aplicación en los centros, lo primero que hará será comprobar si existen actualizaciones en nuestro servidor y, en caso afirmativo, se actualizará automáticamente la aplicación evitando de este modo una actualización manual e individual.

La herramienta elegida para la publicación, instalación y actualización automática de la aplicación de escritorio es *ClickOnce* de *Microsoft*. La aplicación para le *Smartphone* también se actualiza automáticamente a través de nuestro servidor descargando automáticamente el paquete de instalación (*apk*) del servidor. En el capítulo 3.3 se darán más detalles de cómo ha sido implementado este sistema de actualizaciones automáticas.

3 Desarrollo e implementación

3.1 Cliente

Para ser coherentes es explicará la implementación del lado del cliente en el mismo orden en el que se introdujeron en el capítulo de diseño.

3.1.1 Dispositivos médicos contemplados

Como se planteó en el capítulo de diseño, se ha buscado una gama de dispositivos que cubran todos los requisitos y se ha integrado una serie de módulos para la conectividad de estos dispositivos a través de una aplicación Android. Para ello se ha consiguió contactar con un distribuidor que nos proporcionará dispositivos médicos del fabricante *ForaCare*.

- **Termómetro**

Este termómetro *Bluetooth* puede enviar medidas en tiempo real de las mediciones de temperatura al *Smartphone*.



IR20
Ear Thermometer

SPECIFICATIONS	
Temperature Measurement Sites	Ear Temperature
Temperature Range	32°C - 43°C
Accuracy	±0.2°C (±0.4°F) for the measurement at 36°C-39°C (96.8°F-102.2°F) ±0.3°C (±0.5°F) outside above temperature range
Display Resolution	0.1°C or 0.1°F
Temperature Unit	°C or °F set by factory
Backlight Screen	Equipped (dual color backlights)
Fever/over Range Warning	Equipped
Probe Cover Detector	Equipped
Memory Capacity	10
Power Saving	3 min
Power Source	2 x AAA
Battery Life	1000 measurements
Dimension	160.5 (W) x 45.9 (H) x 32.5 (D) mm
Data Transmission	Bluetooth
Weight	100 g (with battery)
Units per Carton	30
Net Weight per Carton	10.5 kg
Gross Weight per Carton	11.5 kg
Carton Size	46.5 x 45 x 38 cm

Figura 7: Características técnicas del termómetro utilizado

- **Pulsioxímetro**

Este pulsioxímetro enviará medidas de la saturación de oxígeno en sangre y del pulso cardíaco al *Smartphone* vía *Bluetooth*.



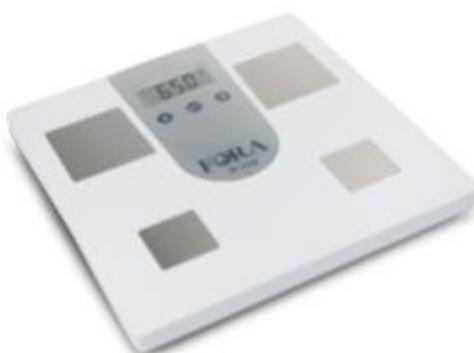
Product Specifications:

Pulse Oximeter	
Measurement Range:	0% to 100%
SpO ₂ Resolution:	1%
SpO ₂ Accuracy :	70% to 100% range: ±2%; <69% unspecified
SpO ₂ Method :	Dual Wavelength LED
Pulse Rate Range:	30 to 250bpm
Accuracy of Pulse Rate:	±1bpm or ±1%, whichever is greater
Mode of Operation:	Continuous
LED Display:	SpO ₂ ; 3 Digits, HR: 3 Digits, Pulse-Strength Bar
Status Indicate:	Probe Good, Battery Status
External Output:	Bluetooth V2.0, SPP (Series Port Profile)
Alarm Range Setting:	SpO ₂ High/Low , Pulse Rate High/Low
Pulse Volume Adjust:	2 Level or Off
LED Light Adjust:	2 Level
Power Source:	4 x AA Alkaline Battery
Battery Usage Life:	40 hours typical operation
Dimension:	140 L x70 W x 32 H(mm)
Weight:	240g with batteries
Storage/Transportation Condition:	-20°C to 55°C (-4°F to 131°F); 0% to 95% RH, non-condensing
Operating Condition:	-10°C to 50°C (14°F to 122°F) for the device; 5°C to 40°C (41°F to 104°F) for the probe
Degree of Protection:	Type BF
Water-Resistance:	Against Water Splash, IPX2
Mechanical Impact-Resistance:	Against Repeat Impact from 1 M Height
EMC Standard:	EN60601-1-2
Safety Standard:	EN60601-1
Performance Standard:	ISO9919

Figura 8: Características técnicas del pulsioxímetro utilizado

- **Báscula**

Esta báscula *Bluetooth* proporciona mediciones de peso al *Smartphone* vía *Bluetooth*.



W310

Dimension (inches) : 13.2 x 13.2 x 1.44"
Weight capacity: 180kg / 396 lb / 28 st:13lb
Auto-on/off function
Resolution : 0.1kg / 0.2lb / 0.2lb
Weighing Unit: kg/ lb/ st

Figura 9: Características técnicas de la báscula utilizada

- **Tensiómetro / Glucómetro**

Este dispositivo tiene dos modos de funcionamiento, uno en el que funciona como tensiómetro en el cual envía medidas de presión arterial y pulso cardíaco al *Smartphone* y otro modo en el que actúa como glucómetro en el que enviará mediciones de glucosa en sangre al *Smartphone* en ambos casos vía *Bluetooth*.



D40 Series

Blood Glucose Plus Blood Pressure Monitoring System

Basic Features	Blood Test Volume (μL)	0.6
	Reaction Time (seconds)	5
	Measurement Range	20 - 600 mg/dL (1.1-33.3 mmol/L)
	Code	No Coding
	Enzyme Type	GOD
	Hematocrit Range	20 to 60%
	Memory	604
	Accuracy of Pressure	$\pm 3\text{mmHg}$ or $\pm 2\%$ of reading
	Accuracy of Heart Rate	$\pm 4\%$ of reading
	BP Measuring Unit	mmHg
	Wrist / Arm Type	Arm
	HR Detection	Yes
	Automated Average Function	Yes
	Auscultatory Mode	-
Advanced Features	Calendar / Clock When Off	Yes
	Talking Function	Advanced
	Strip Ejection	Yes
	AGPC Recording	Yes
	QC Record	Yes
	Daily Alarm	-
	Alternative Site Testing	Yes
	Ketone Warning	Yes $\geq 240 \text{ mg/dL}$ (13.3 mmol/L)
	BPM Day Average	7/14/21/28/50/90 days
	Data Output	D40c: USB; D40d: USB/Bluetooth; D40i: USB & CPRS
Specification	User Number (BP)	4
	Power Source	4 x AA / 6V Adaptor / Li-Ion (special order)
	Dimension (inch)	5.79 x 4.13 x 3.15
	Weight (lb) without batteries	0.86

Figura 10: Características del tensiómetro/glucómetro utilizado

3.1.2 Aplicación Android

La aplicación está programada con el entorno de trabajo *Eclipse* y en lenguaje de programación *Java*. Se ha diseñado el interfaz gráfico, los *layouts*, y sobre él se han programado los módulos descritos en la fase de diseño. Mi labor fue la de integración de la aplicación en la plataforma.

Con el fin de clarificar el funcionamiento de la aplicación, se va a describir el proceso de funcionamiento para luego explicar más concretamente cada módulo.

Proceso de funcionamiento.

- a) La pantalla de inicio realiza la sincronización con la base de datos y realiza una copia local en la SQLite, también comprueba si existen actualizaciones en el servidor.
- b) La pantalla de verificación comprobará si el Bluetooth y el NFC están activados y en el caso en el que no estén te permitirá activarlos desde la misma pantalla.
1. Lo primero que aparece una vez se inicia la aplicación es una pantalla que nos pide que acerquemos la tarjeta NFC al *Smartphone* para acceder a la plataforma.
2. Una vez nos hayamos autenticado pasaremos al módulo de identificación de residentes, en el que podremos ver una lista con los nombres, una foto y la habitación en la que están. Tocando sobre la pantalla encima del residente que se desea medir se pasará a la pantalla de adquisición de medidas.
3. La aplicación una vez esté en esta pantalla estará esperando para adquirir una medida de cualquiera de los dispositivos médicos contemplados.
4. Toma de medidas. El gerocultor tomará la medida con cualquiera de los dispositivos médicos contemplados. Una vez termine el proceso, el dispositivo intentará enviar la medida vía *Bluetooth*.
5. Una vez la aplicación ha adquirido la medida, se muestra por pantalla y se procederá a su envío al servidor o almacenado en la base de datos SQLite dependiendo de si existe conexión a internet. En cualquier caso la aplicación mostrará un mensaje explicativo de lo que ha pasado con la medida.
6. Después de una cuenta atrás de unos pocos segundos para que el gerocultor pueda ver que la medida se ha tomado correctamente, se muestra una pantalla de selección en la que el gerocultor podrá elegir entre repetir una medida al mismo residente, tomar una medida a otro residente distinto o enviar la medida que acaba de ser realizada a un contacto.



Figura 11: Diagrama de trabajo de la aplicación móvil

- **Autenticación de personal sanitario**

Como se dijo en el capítulo de diseño se permiten dos formas de autenticación, mediante tarjeta y mediante usuario y contraseña. Se puede cambiar de uno a otro deslizando el panel de la parte inferior.

NFC

Si estamos en la pantalla de autenticación mediante tarjeta, la aplicación se encontrará a la espera de que una tarjeta NFC irrumpa en el campo de detección del *Smartphone*. Una vez se ha detectado una tarjeta se procede a leer su UID. El siguiente paso es comprobar si existe conexión a internet, ya que si no la hubiese se procedería a la autenticación *offline*. La única diferencia entre la autenticación *online* y *offline* es que la comprobación se hará con las contraseñas almacenadas en la base de datos alojada en el servidor mediante una petición al servicio web o con las contraseñas almacenadas en la base de datos SQLite del móvil que podrían no estar sincronizadas.

Una vez se ha leído el UID y exista o no conexión a internet se procederá a realizar la autenticación básica (*Basic Auth*) a la que se le pasarán las credenciales en el formato *uid:a23ce4223g*. En caso de autenticación satisfactoria se dará paso al siguiente módulo.

Usuario + contraseña

Como se puede ver en el anexo 4, se proporciona una entrada de texto para cada uno de los campos. La aplicación estará esperando a que se pulse el botón de *ENTRAR* para realizar el mismo proceso que en caso anterior. Se leen las credenciales escritas en los cuadros de texto, se comprueba si existe conexión a internet y se procede a realizar la autenticación básica (*Basic Auth*) pero en este caso las credenciales se enviarán en formato *DNI:Password*.

- **Identificación de residente**

La identificación de residentes se realizará mediante la selección manual en una lista con todos los residentes que habrán sido descargados de la base de datos alojada en el servidor mediante la petición correspondiente al servicio web realizada durante el proceso de sincronización tanto automática como forzada.

- **Adquisición de medidas**

Este módulo intentará establecer conexión con todos los dispositivos médicos que estén pareados con el *Smartphone* mediante su dirección MAC. Una vez se haya conectado un dispositivo empezará a interpretar el protocolo de comunicación asociado al tipo de dispositivo que se está conectando utilizando su perfil puerto serie (SPP). De este modo se leerá la medida o medidas, dependiendo del tipo de dispositivo médico.

- **Envío / Almacenamiento de medidas**

La medida realizada se enviará a la base de datos mediante la petición correspondiente al servicio web junto con el identificador del residente a que se le ha tomado y el del profesional que se la ha tomado.

- **Aviso a familiares**

El aviso a familiares se hará mediante *sms* a través de la compañía *Twilio*, una *Cloud Communications Company* que nos permitirá enviar *sms* a través internet. Para su implementación se hará uso de la API propiedad de dicha compañía.

Se permitirá el envío de mensajes a cualquiera de los contactos del residente objeto de la medida, a ciertos contactos de la residencia en función de los roles (administradores y médicos), a las personas de contacto de los centros médicos asociados al centro residencial o también se podrá introducir un número de móvil manualmente.

De igual modo que para la adquisición de medidas, en caso de no existir o fallar la conexión a internet, el SMS quedará almacenado en la base de datos SQLite del móvil y se enviará automáticamente cuando haya disponible conexión a internet.

3.1.3 Aplicación de gestión

La aplicación de gestión se ha implementado haciendo uso del entorno de trabajo *Visual Studio 2012* en lenguaje de programación C#. Debido a que, por lo general, los ordenadores existentes en los centros residenciales no están actualizados se decidió programarlo para *framework 2.0* o por lo que será compatible con sistemas operativos desde *Windows XP Service Pack 1* hasta el reciente *Windows 8.1* y sucesivos. Mi labor fue la de su desarrollo, implementación e integración en la plataforma.

A diferencia de la aplicación móvil la cual es muy guiada, la aplicación de gestión posee un interfaz gráfico principal desde el cual son accesibles todos los módulos. El interfaz principal está dividido en pestañas como se puede ver en la figura 14. Se ha intentado que fuese lo más intuitiva y homogénea posible.

- **Gestión de residentes**

Se permitirá la creación, edición y eliminación de perfiles de residente. En el anexo 4 (interfaz de usuario) se pueden ver los formularios para la introducción de datos. Además en el interfaz principal se podrá visualizar una lista con todos los residentes activos y un resumen de su ficha personal pasando el ratón por encima de la lista.

- **Gestión de personal sanitario**

Para dar homogeneidad a la aplicación el aspecto visual tanto del interfaz principal como de las acciones que se pueden realizar es muy similar al de gestión de residentes (ver anexo 4)

- **Gestión de acceso al sistema**

Se ha separado el interfaz principal en dos partes bien diferenciadas como se dijo en el capítulo de diseño. Por un lado acciones para dar de alta y baja una tarjeta en el sistema y por el otro las acciones de vinculación y desvinculación de la tarjeta a un profesional. El interfaz también se ha hecho muy intuitivo como se puede (ver anexo 4).

Además se ha implementado un servicio para el envío de e-mail en caso de olvido de contraseña. Se resetea la contraseña generando una de forma aleatoria y se envía a la dirección que se proporcionó al crear el perfil.

```

private EmailService()
{
    //smtp.gmail.com
    smtp = new SmtpClient("mail.gmx.com", 587);
    smtp.EnableSsl = true;
    smtp.UseDefaultCredentials = false;
    smtp.Credentials = new NetworkCredential("COMPANY.MAIL@gmx.com", "PASSWORD");
    smtp.Timeout = 10000;
    //ServicePointManager.ServerCertificateValidationCallback = delegate { return true; };

    Thread consumer = new Thread(() =>
    {
        while (true)
        {
            var pm = q.Get();
            SendEmailPassword(pm);
        }
    });
    consumer.IsBackground = true;
    consumer.Start();
}

```

Figura 12: Configuración del cliente smtp para el envío de e-mails

```

EmailService.Instance.EnqueueMessage(caregiver.Email,
password, caregiver.Id, caregiver.FirstName, caregiver.LastName);

private void SendEmailPassword(PasswordMessage pm)
{
    var message = new MailMessage();

    message.To.Add(pm.To);
    message.Subject = "Nueva contraseña de acceso a
Golden para " + pm.Firstname + " " +
pm.Lastname + " (" + pm.Dni + ")";

    message.From = new MailAddress("goodday.solutions@gmx.com");

    message.Body = "La nueva contraseña de acceso para "
+ pm.Firstname + " " + pm.Lastname + " con DNI " +
pm.Dni + " para la residencia " + LogInfo.NursingHomeName + " es: " + pm.Password;
}

```

Figura 13: Cuerpo personalizado del e-mail

- Generación de informes y pre-visualización de medidas**

Este módulo se ha dividido en dos partes, la pre-visualización de medidas que será accesible desde el interfaz principal (ver anexo 4) y la generación de informes que será accesible desde la ficha personal de cada residente. Para ver el modelo de informe generado (ver anexo 4).

Para resaltar las medidas fuera de lo normal y así hacer más fácil la tarea de identificar estas anomalías, aparecerán resaltadas en rojo las medidas fuera del rango de valores que la Organización Mundial de la Salud considera como valores normales.

DNI	Nombre	Apellidos	Piso	Habitación	Cama
67248867H	Manuel	Aliende Gacón	1	121	1
75085328B	Carlos	Bermudez Valiente	3	308	1
53182137L	Pedro	Bueno Lavina	1	102	1
55106811F	Salvador	Chueca Puga	1	101	2
47737028E	Pedro	Dumas Boquerizo	3	322	1
17448138Q	Jorge	Gómez Losilla	4	412	2
76913506B	Rosario	Gómez Pláonas	1	104	1
66731860M	Carlos Alberto	Julián Hernan	3	111	2
11788200X	Jose Luis	Leguna Lainez	3	310	2
28603242M	Alicia	López Cárcoles	1	105	1
63589673D	Laura	López López	2	232	1
11111111H	Mariisa	Martínez Bernabé	2	201	2
47042229F	Olga	Martínez Chueca	1	121	2
76548209T	Rogelio	Motos Revilla	4	412	2
27610987Q	Vicente	Muñoz Moreno	4	415	2
66500174K	Martina	Ochoa Gonzalez	4	406	1
52245545X	Julio	Pignatelli Bernardo	1	121	2
47928803T	Daniel	Romeo Lama	1	106	1
70939268T	Laura	Ruesga Pérez	1	501	1
2222222J	Manolo	Ruiz López	1	101	1

Bienvenido a tu panel de control. Desde aquí podrás gestionar todos los usuarios de tu residencia
[Cerrar sesión](#)

Filtrar:

Carlos Bermudez...
 DNI: 75085328B
 Habitación: 308

Gestión de usuarios

Hola Sandra

Residentes Personal sanitario Centros sanitarios Tarjetas Medidas

Mostrar históricos Mostrar grupos

ACTUALIZAR

VER FICHA

DAR DE BAJA

AÑADIR RESIDENTE

Figura 14: Interfaz principal de la aplicación de gestión

- **Background Workers**

Uno de los puntos más importantes de la aplicación de gestión y que contribuyen a dar sensación de fluidez es el uso de *Background Workers*. Generalmente, las aplicaciones de formularios que consumen datos de una base de datos alojada en un servidor y que, por tanto, tienen que realizar accesos a la misma, suelen atascarse hasta que termina la ejecución del acceso que dependiendo del volumen de datos y la conexión a internet puede resultar en un tiempo considerable.

Los *Background Workers* son utilizados para crear nuevos hilos de ejecución en los que se realizan operaciones que implican un gran tiempo de ejecución como por ejemplo los accesos a la base de datos. De este modo no se interrumpe el hilo principal de la aplicación. Nos permitirán reportar al hilo principal los progresos de la ejecución y así poder informar al usuario final. También se permite crear tanto hilos de ejecución como se quieran lo que nos permitirá realizar varios accesos simultáneos a la base de datos.

```
private BackgroundWorker reloadResidentsWorker = null;

// Reload residents worker
reloadResidentsWorker = new BackgroundWorker();
reloadResidentsWorker.DoWork += ReloadResidentsWorkerOnDoWork;
reloadResidentsWorker.ProgressChanged += ReloadResidentsWorker-
OnProgressChanged;
reloadResidentsWorker.RunWorkerCompleted += ReloadResi-
dentsWorkerOnRunWorkerCompleted;
reloadResidentsWorker.WorkerReportsProgress = true;

private void ReloadResidentsWorkerOnDoWork(object sender,
DoWorkEventArgs e)
{
    // Petición a la base de datos
}

private void ReloadResidentsWorkerOnRunWorkerCompleted(object
sender, RunWorkerCompletedEventArgs e)
{
    // Cambios gráficos una vez terminado el acceso
}

private void ReloadResidentsWorkerOnProgressChanged(object
sender, ProgressChangedEventArgs e)
{
    // Cambios gráficos durante el acceso a través de
}
```

Figura 15: Ejemplo de Background Worker

- **Primer usuario**

El tratamiento del primer usuario del sistema es un tema importante porque ayudará a que los centros residenciales puedan iniciar el funcionamiento de la aplicación por sí mismos. En el diagrama de flujo descrito en el capítulo de diseño se observa que el primer módulo es el de autenticación. La problemática surge en caso de no existir ningún usuario registrado ya que resultaría imposible acceder a la plataforma. Por ello antes de cargar el módulo de autenticación se hace una comprobación de si la base de datos de usuarios está vacía. En tal caso la aplicación mostrará un formulario desde el que se creará el primer usuario que tendrá rol de administrador.

- **Accesos a la base de datos**

El acceso a la base de datos se realizará a través del servicio web mediante peticiones *http*. A diferencia de la aplicación móvil en la que generalmente son de consumo de datos (GET), en la aplicación de gestión tiene que poder generar, editar y borrar datos de la base de datos, además de consumirlos. Lo que implicará un gran número de peticiones.

```
public IList<Resident> GetResidentsWebService(String username, String password, bool historical)
{
    IList<Resident> resis = new List<Resident>();
    String stream;
    HttpWebRequest httpWebRequest;
    // Create the web httpWebRequest
    if (historical)
    {
        httpWebRequest = WebRequest.Create(url + "residents?filter=inactive") as HttpWebRequest;
    }
    else {
        httpWebRequest = WebRequest.Create(url + "residents?filter=active") as HttpWebRequest;
    }

    httpWebRequest.Method = "GET";
    // Add authentication to httpWebRequest
    httpWebRequest.Credentials = new NetworkCredential(LogInfo.NursingHomeId + ":" + LogInfo.NursingHomePassword,
        LogInfo.Caregiver.Id + ":" + LogInfo.Password);
    try
    {
        // Get response
        using (HttpWebResponse response = httpWebRequest.GetResponse() as HttpWebResponse)
        {
            // Get the response stream

            StreamReader reader = new StreamReader(response.GetResponseStream());
            stream = reader.ReadToEnd();
            resis = JsonConvert.DeserializeObject<IList<Resident>>(stream);
        }
    }
    catch (WebException we)
    {
        ExceptionUtility.StoreWebException(we, MethodBase.GetCurrentMethod().Name, httpWebRequest);
        throw we;
    }
    catch (Exception e)
    {
        ExceptionUtility.StoreException(e, MethodBase.GetCurrentMethod().Name, httpWebRequest);
        throw e;
    }
    return resis;
}
```

Figura 16: Ejemplo de petición http GET de la aplicación de gestión

3.2 Servidor

En este capítulo se va a explicar cómo se ha implementado el lado del servidor, que como hemos comentado varias veces consta de una base de datos relacional MySQL y un servicio web.

3.2.1 Base de datos MySQL

La base de datos se ha intentado que reproduzca fielmente la estructura real de un centro sanitario para ello se van a describir primero los bloques del diagrama Entidad-Relación (EER) para luego describir las relaciones existentes entre ellos.

- **Diagrama EER**

El diagrama EER es la forma abstracta de describir una base de datos relacional que almacena los datos en tablas. A continuación se detallan los diferentes bloques y tablas que contiene el diagrama pero no se podrá ver gráficamente por ser propiedad de la empresa Goodday Solutions.

Bloque de residentes: Este bloque contendrá toda la información necesaria para identificar únicamente al residente dentro del centro residencial como son el DNI, datos personales, habitación dentro del centro, etc.... De especial importancia será su número de DNI el cual al ser único para cada persona se utilizará como identificador con el que se realizarán las relaciones entre tablas.

Podrán ser diferenciados entre fijos y de centro de día dependiendo de si tienen asignada una habitación o en su lugar la secuencia C.D. (Centro de día). También tendrá un campo que identificará si el residente está activo o pertenece al grupo de históricos que por alguna razón ya no pertenecen al centro

Bloque de personal sanitario: El bloque de personal sanitario, al igual que el de residentes, contendrá la información necesaria para su identificación dentro del centro. El DNI tendrá igual importancia y se utilizará para realizar las relaciones con otras tablas aunque el e-mail cobra una gran importancia porque se utiliza para el envío y reseteo de contraseñas.

A cada perfil se le asignará un rol que será utilizado para establecer sus privilegios dentro de la plataforma.

Bloque de medidas: En el bloque de medidas se almacenarán todos los datos necesarios para que puedan ser interpretadas por los médicos, valor, tipo, así como la fecha y hora a la que se tomaron y los identificadores de a quién pertenece esa medida y por quién fue tomada.

Bloque de tarjetas: Esta tabla contendrá únicamente tres campos: el identificador único de la tarjeta (*Unique IDentifier*, UID), un campo de texto para etiquetar las tarjetas e identificarlas más fácilmente en la plataforma y, por último, contendrá el identificador del profesional (DNI) al que está asignada, si lo está, en caso de no estar asignada este campo tendrá valor nulo.

Bloque de centros sanitario: Todos los datos de un centro sanitario como su nombre y su dirección, además de los datos de las personas de contacto de este centro.

Bloque de contactos de residentes: Contendrá el nombre, la relación familiar que les une, el número de teléfono, el e-mail y el identificador del residente del que es familiar.

Bloque de direcciones: Por no ser imprescindible y además poder poseer más de una se creó el bloque de direcciones que contendrá además el residente al que pertenece.

- **Relaciones**

A continuación se detallan como son las relaciones entre los diferentes bloques (ver capítulo 8.5):

Residentes **1:N** Medidas que se le han realizado.

Personal sanitario **1:1** Tarjetas

Personal sanitario **1:N** Medidas que ha llevado a cabo.

Centros sanitarios **1:N** Contactos de centro sanitario.

Residentes **N:M** Personas de contacto.

Residentes **N:M** Direcciones

3.2.2 Servicio web

El servicio web también ha sido programado, del mismo modo que la aplicación de gestión, utilizando el entorno *Visual Studio* así como el lenguaje de programación C#. La diferencia es que el servicio web se desplegará en el servidor de la empresa que posee el sistema operativo *Windows Server 2012*, por lo tanto se utilizará el *Framework 4.5* con el que es compatible la nueva *ASP.NET Web API* que facilitará el desarrollo del servicio web.

El bloque central son los controladores que, básicamente, definen las llamadas al servicio web y gestionan sus respuestas.

- **Controladores**

El servicio trabajara con peticiones que, como se ha comentado en el capítulo de diseño, en una arquitectura *REST* son: *POST*, *PUT*, *DELETE* y *GET*. En la llamada irán todos los parámetros para decodificarla, es decir, para saber el tipo de petición que es, que es lo que se está pidiendo, así como las credenciales de autenticación y en el caso particular de peticiones de tipo *POST* o *PUT* el contenedor de datos JSON correspondiente con la información a almacenar.

- **Comunicación con la base de datos**

En la forma de comunicación con la base de datos hubo dos fases como en casi todo el proyecto. Una primera en la que se hizo uso de una *Object-Relational Mapping* (ORM) para luego cambiar a consultas puras *SQL*.

1^a Fase: ORM

Se utilizó NHibernate en un primer momento. Es una herramienta para .NET en lenguaje C# que permite el mapeo a consultas SQL de forma muy fácil y rápida. Además de realizar el mapeo de las tablas de la base de datos a objetos mucho más manejables, también resulta mucho más fácil el añadir criterios de búsqueda sin tener que construir una instrucción SQL muy larga. Su punto fuerte es la facilidad de uso.

El problema del uso de este tipo de técnicas es la poca flexibilidad que ofrecen a la hora de realizar cambios en el diseño de la base de datos además de la baja eficiencia que presentan en términos de accesos a ella.

```
// GET /api/residents/{id}/profile
// Devuelve la información básica de un residente
[GoldenAuth]
[HttpGet]
[ActionName("profile")]
public ResidentDTO GetById(string id)
{
    NursingHomeInfoAuth nhinfo = GoldenAuthAttribute.NHInfo;
    var repository = new Repository<Resident>();
    var criteria = DetachedCriteria.For<Resident>();
    criteria.Add(Restrictions.Eq("id", id));
    var resident = repository.FindOne(criteria, nhinfo.HibernateConnection);

    if (resident == null)

        throw new HttpResponseException(HttpStatusCode.NotFound);

    return Mapper.Map<ResidentDTO>(resident);
}
```

Figura 17: Ejemplo de acceso a la base de datos mediante NHibernate

2ª Fase: SQL

En la segunda fase se cambió a lenguaje *SQL*, el cual a pesar de resultar más tediosa la construcción de estas peticiones es mucho más eficiente que usar un ORM en términos de *tiempo-volumen de datos-nº de accesos*.

Como se puede ver comparando los dos extractos de código el utilizar una ORM realiza más sencilla la tarea de programación pero es poco eficiente y en el momento en el que se quiere hacer una ampliación de la base de datos es poco flexible e implica muchos cambios.

```
// GET /api/residents/{id}/profile
// Devuelve la información básica de un residente
[GoldenAuth]
[HttpGet]
[ActionName("profile")]
Oreferencias
public ResidentDTO GetById(string id)
{
    NursingHomeInfoAuth nhinfo = GoldenAuthAttribute.NHInfo;

    DatabaseHelper db = new DatabaseHelper();
    MySqlConnection connection = db.InitializeDB(nhinfo.NursingHomeDBName, nhinfo.NursingHomeDBUID, nhinfo.NursingHomeDBDecryptedPass);
    MySqlCommand command = new MySqlCommand("", connection);

    command.CommandText = "SELECT id, first_name, last_name, room, birthdate, sex, photo, bed, floor, health_number, health_membership_t
    command.Parameters.Clear();
    command.Parameters.AddWithValue("@id", id);

    DataTable dataTableResidents = db.Select(command);

    DataRow rowResident = dataTableResidents.Rows[0];
    ResidentDTO resident = new ResidentDTO();

    resident.Id = rowResident["id"].ToString();
    resident.FirstName = rowResident["first_name"].ToString();
    resident.LastName = rowResident["last_name"].ToString();
    resident.Room = rowResident["room"].ToString();
    resident.Birthdate = (DateTime)rowResident["birthdate"];
    resident.Sex = rowResident["sex"].ToString();
    resident.Photo = rowResident["photo"].ToString();
    resident.Bed = rowResident["bed"].ToString();
    resident.Floor = rowResident["floor"].ToString();
    resident.HealthNumber = rowResident["health_number"].ToString();
    resident.HealthMembershipType = rowResident["health_membership_type"].ToString();

    return resident;
}
```

Figura 18: Ejemplo de acceso a la base de datos mediante secuencia SQL

3.2.2.1 Seguridad

Como ya se comentó en el apartado de diseño, la seguridad es un tema clave pensando en una implantación real debido a la sensibilidad de los datos que se manejan. A continuación se va a detallar la implementación de los métodos de seguridad antes descritos.

- ***https***

El mecanismo habitual para el uso de certificados de servidor web y por tanto el que se ha seguido es el siguiente. Se ha de generar una solicitud de firma de certificado de seguridad (*Certificate signing request*, CSR) para un dominio web en concreto y esta solicitud ha de ser enviada a una Autoridad de Certificación. Dicha autoridad verificará la información contenida dicho CSR y, en caso de aprobación, devolverá al solicitante el certificado ya firmado y validado. La información que se precisa para la generación del CSR incluye la URL del servidor (dominio, i.e. www.example.com), datos de la empresa, en este caso Goodday Solutions S.L y la generación de una pareja de claves pública/privada. Con esta información se realiza una petición CSR. Una vez se recibe el certificado firmado se instala en el servidor y se configura el servicio web para que pase a usar https en lugar de http y para que emplee dicho certificado.

- ***Basic Authorization***

En cuanto a la comprobación de credenciales para acceder a la plataforma, lo más importante no es la comparación en sí, ya que esto sería trivial, sino la forma en la que se almacenan las credenciales en la base de datos.

Se ha diseñado un sistema robusto frente a robos de la base de datos. A la hora de almacenar la contraseña de acceso elegida por el usuario en ningún caso es conveniente almacenarla directamente sin tratarla. El sistema que se ha implementado utiliza el *hasheado* y *salteado* de contraseñas.

Almacenado de contraseñas

Siguiendo la estructura de la figura de abajo, el almacenado de contraseñas se divide en 3 pasos:

1. En el primer paso tenemos la contraseña que se ha introducido *en limpio* (Plaintext Password), y un *salt* aleatorio (Random Salt).
2. En el segundo paso se aplican funciones *hash* a cada uno de los dos términos anteriores por separado. El resultado de hacer la operación *hash* al *salt* (Hashed Salt) se almacenará en la base de datos.
3. Por último los dos resultados anteriores (*Hashed Password* y *Hashed Salt*) se concatenarán y se le aplicará la operación *hash* otra vez. Este resultado (*Final Hashed Password*) se almacenará en la base de datos.

Hash: La función *hash* es una operación matemática aplicada comúnmente en criptografía ya que para cada entrada a la función sólo existe una salida y lo más importante, no tiene inversa, es decir sólo se puede aplicar en un sentido. Por lo tanto es imposible reconstruir la contraseña original a partir de su resultado.

Salt: El *salt* no es más que una cadena de longitud y valores aleatorios.

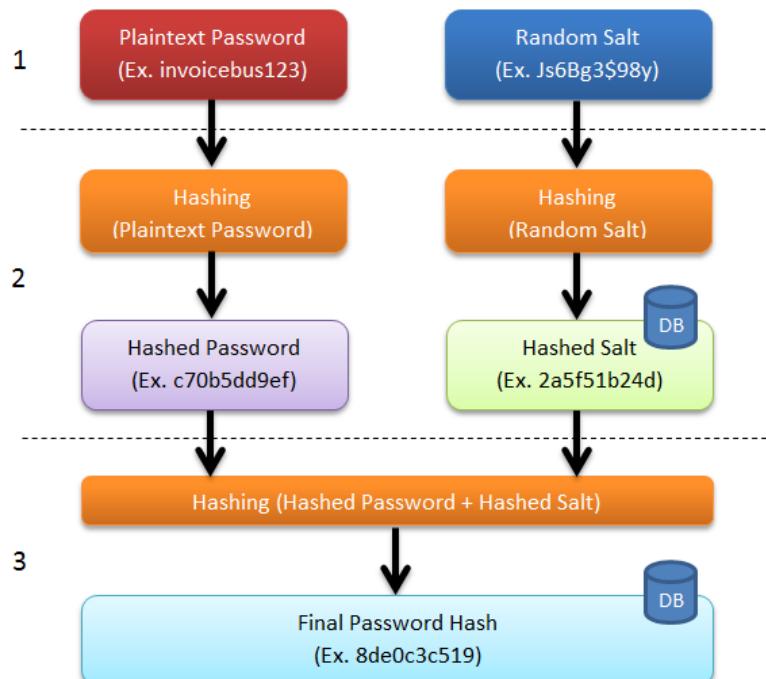


Figura 19: Esquema de salteado y hasheado de contraseñas

```

caregiver.Salt = Cryptography.CreateSalt ();
caregiver.PasswordHash = Cryptography.GetHashedPassword (password, caregiver.Salt);

```

Figura 20: Extracto de código para encriptación de contraseñas

- ***Advanced Encryption Standard***

En cuanto al algoritmo AES para el cifrado de datos médicos se ha implementado el algoritmo de encriptado y desencriptado tal y como se explica en el capítulo 9.2 de los anexos. A continuación se muestra un extracto del código generado.

Este código es aplicado cada vez que llega una medida al servidor de modo que no es posible asociarla al residente al que pertenece.

```
// Se crea un objeto Rijndael con una clave y un tamaño de bloque específicos
using (AesManaged aesAlg = new AesManaged())
{
    aesAlg.Key = Key; // Clave de 128 bits
    aesAlg.IV = IV; // Tamaño de boque

    // Creamos el encriptador con la la clave y el tamaño de bloque
    ICryptoTransform encryptor = aesAlg.CreateEncryptor(aesAlg.Key, aesAlg.IV);

    // Creamos el flujo de datos para la encriptación
    using (MemoryStream msEncrypt = new MemoryStream())
    {
        using (CryptoStream csEncrypt = new CryptoStream(msEncrypt, encryptor, CryptoStreamMode.Write))
        {
            using (StreamWriter swEncrypt = new StreamWriter(csEncrypt))
            {

                // Escribimos los datos en el almacén de datos
                swEncrypt.WriteLine(plainText);
            }
            encrypted = msEncrypt.ToArray();
        }
    }
    StringBuilder s = new StringBuilder();
    foreach (byte item in encrypted)
    {
        s.Append(item.ToString("X2"));
    }
    // Devolvemos los datos encriptados como una cadena de texto

    return s.ToString();
}
```

Figura 21: Extracto de código de encriptado AES

3.3 Despliegue

El despliegue de la plataforma comprende todas las acciones a realizar para que los usuarios finales puedan hacer uso de la misma. Como se dijo en el apartado de diseño cada centro tendrá su propia base de datos lo cual no desempeña más problema que el tener que crearla cada vez que se va a implantar en un centro. Donde se ha implementado un desarrollo más complejo pero mucho más eficiente es en cómo hacer llegar las dos aplicaciones (escritorio y *smartphone*) y sus respectivas actualizaciones en caso de existir una versión más reciente de la misma.

En un primer paso, la primera vez que va a ser instalada la solución se proporcionará a los centros una *url* con la que se accederá a nuestro servidor y unas credenciales para que descarguen e instalen la aplicación por primera vez.

Para la actualización de versiones, desde el ordenador del desarrollador se publicará vía FTP una nueva versión en el repositorio correspondiente en el servidor. En el caso de la aplicación de gestión, el software de desarrollo (Visual Studio 2012) tiene la opción de integrar la herramienta *ClickOnce* de Microsoft comentada anteriormente por lo que bastaría con configurar correctamente un sitio web con publicación FTP en el servidor. En el caso de la aplicación móvil, el software de desarrollo (Eclipse) no lo permite por lo que se realizará de forma manual.

Ambas aplicaciones cada vez que se inicien harán una petición al servicio web para que les proporcione la última versión publicada. En caso de que no coincida con la que se está ejecutando, se realizará otra petición para la descarga de la última versión, que se instalará. De este modo, los centros residenciales siempre tendrán la versión más actualizada posible de una forma sencilla, totalmente automatizada y transparente para el usuario final.

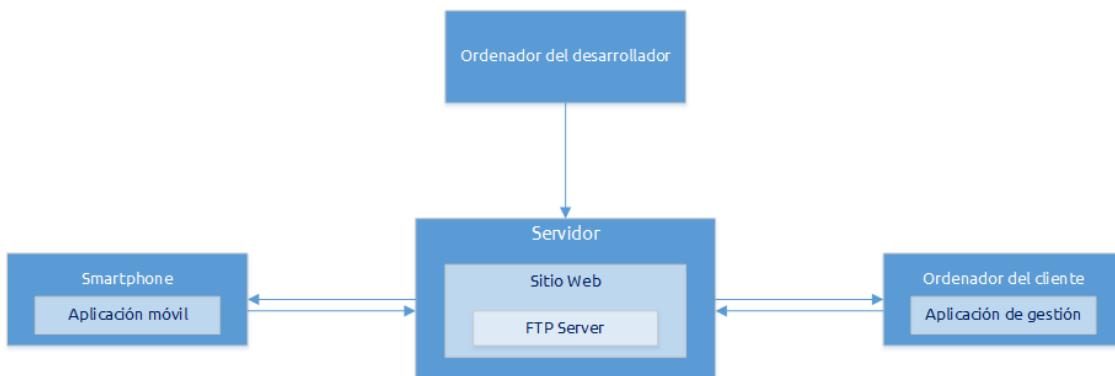


Figura 22: Esquema de despliegue de la plataforma

4 Resultados

De la realización de este PFC se ha obtenido una plataforma de gestión total para la monitorización de constantes vitales dentro de un centro residencial, así como su gestión administrativa. La cual se puede decir que es completamente funcional y que su uso real está siendo realmente satisfactorio como se extrae de la evaluación del proceso realizada.

Como resultado del PFC se va a dar una nueva forma de gestión de los centros residenciales y la monitorización de las medidas de sus residentes con el que se reducirán los fallos humanos y se aumentará enormemente la eficiencia del personal sanitario. En capítulos anteriores se ha descrito el proceso de cada aplicación de forma independiente, por lo tanto, a continuación se va a cerrar el círculo y se va a presentar el proceso completo desde que se controlan las constantes de un residente hasta que esa medida se ve reflejada en un informe.

- **Paso 1:** Aplicación móvil (ver figura 24)

- **Autenticación de personal sanitario:** El profesional sanitario se autentica mediante su tarjeta NFC.
- **Identificación de residentes:** Se selecciona el residente al que se le va a realizar el control de alguna de las constantes vitales.
- **Toma de medidas:** El profesional sanitario toma la medida al residente
- **Envío de medidas:** La medida se envía automáticamente al servidor
- **Avisos:** Posibilidad de avisos en tiempo real mediante sms (ver figura 24)



Figura 23: Secuencia de uso de la aplicación móvil



Figura 24: Ejemplo de sms como aviso a familiar o centro médico

- **Paso 2:** Aplicación de gestión

- **Autenticación de personal de administración:** El profesional de administración se autentica mediante la introducción de sus credenciales de acceso.
- **Gestión de usuarios:** El profesional de administración podrá gestionar los perfiles de los usuarios del centro, tanto residentes como personal sanitario
- **Gestión de acceso al sistema:** Permite la administración de las tarjetas NFC.
- **Generación de Informes:** El profesional de administración genera un informe con las medidas que se han realizado.

4.1 Implantación real

La implantación de la plataforma en un centro residencial supuso un gran reto, hubo que preparar un protocolo de actuación para la instalación *in situ* además de preparar manuales de uso a modo de guía rápida. También se quiso realizar una evaluación por medio de encuestas que mida la satisfacción y aceptación de la nueva plataforma que se les va a instalar.

En este capítulo se relata cómo fue la implantación real de la plataforma en la Residencia Avenida la cual se realizó de forma profesional.

4.1.1 Protocolo de actuación

- **Previa:** Comprobación de las características técnicas de las instalaciones
 - Entrega y recogida de la ficha de requisitos técnicos (ver anexo 6, capítulo 12.1)
 - Despliegue de una base de datos específica para la residencia o centro de día.
 - Preparación del kit de dispositivos y tarjetas NFC.
 - Instalación de aplicación Android en Smartphone.
- **Presentación:** con representantes tanto del personal sanitario como del personal de administración.
 - Introducción personal
 - Introducción del proceso que se va a seguir para la instalación durante los próximos minutos.
 - Explicación del proceso a seguir en caso de incidencia durante la primera semana de aclimatación.
- **Instalación:** Incluye la instalación técnica de la plataforma en las infraestructuras del centro residencial, así como una breve explicación y demostración del proceso de uso y la resolución de dudas sobre la plataforma y su utilización.
 - Instalación de la aplicación de gestión en el ordenador en el que va a ser utilizada
 - Comprobación de la versión del Framework de .NET instalada y e instalación si existiera algún problema con dicha versión.
 - Explicación general de su uso diario
 - Autenticación mediante DNI y contraseña
 - Alta, baja y modificación de usuarios
 - Breve explicación del proceso de gestión de la asignación de tarjetas NFC a los perfiles de personal sanitario (explicación más extensa con ayuda del Smartphone posteriormente)
 - Comprobación de que la base de datos está vacía
 - Configuración de WiFi en el Smartphone
 - Explicación de uso de la aplicación móvil (la aplicación irá pre-instalada)
 - Identificación mediante NFC
 - Prueba de funcionamiento con todos los dispositivos médicos utilizando el usuario de prueba.

- Comprobación de que la medida ha sido almacenada en la base de datos y es accesible desde la aplicación de escritorio mediante la generación de un informe.
- Entrega de los manuales de uso rápido
- Instalación de la aplicación de escritorio en otros ordenadores si el centro lo desea.
- **Evaluación:** Explicación del proceso de evaluación tanto al personal sanitario como al personal de administración.
 - Explicación completa del proceso de evaluación mediante encuestas
 - Encuestas de evaluación previas, de evolución y posteriores
 - Entrega de encuesta previa para su realización en el momento y recogida de la misma.
 - Entrega de encuestas de evolución y posterior para su realización durante la primera semana de uso. Recogida al finalizar el proceso.

4.2 Evaluación

Como se ha dicho en capítulo anterior se ha querido realizar una evaluación de la satisfacción de los usuarios con la plataforma. Esta evaluación se ha dividido en dos partes, una que evaluará la satisfacción de uso de la plataforma propiamente dicha y otra que evaluará simplemente aspectos gráficos de la aplicación. Las encuestas realizadas por el personal de la residencia se pueden ver en el anexo 5.

- **Evaluación de uso:** Este proceso de evaluación se va a realizar mediante la realización de dos encuestas, ya que para poder evaluar si la plataforma mejora las prestaciones del proceso antiguo, se necesita tener una valoración de ese proceso.

Para la evaluación del proceso antiguo se realiza la encuesta llamada *previa*. Se ha diseñado una encuesta para el personal de administración que evaluará como es su trabajo a la hora de dar de alta usuarios, generar informes, etc. Y otra encuesta para el personal sanitario que evaluará el proceso de toma de medidas y su transcripción manual al soporte de almacenamiento que se utilice.

Para la evaluación del nuevo proceso se ha diseñado una encuesta llamada *posterior* también para los dos grupos de usuarios. Que evaluarán los nuevos procesos de las acciones que les conciernen.

- **Evaluación del diseño gráfico:** Este proceso se va a realizar mediante la realización de una única encuesta por parte del personal sanitario y otra por parte del personal de administración, serán las llamadas de *evolución*. El objetivo de las mismas es conocer, además de si el diseño es agradable para los usuarios, si las acciones a realizar son fácilmente reconocibles, si es fácil el acceso a los diferentes módulos y demás aspectos de usabilidad.

Por ello se han creado dos diferentes encuestas. La referente al personal de administración evaluará principalmente la aplicación de gestión que será la que será utilizada por este grupo de personas. Y la encuesta referente al personal sanitario evaluará la aplicación móvil ya que éstos serán los encargados de realizar la toma de medidas.

5 Conclusiones y líneas futuras

5.1 Aportaciones al trabajo realizado

En este PFC se ha desarrollado una plataforma de gestión total del proceso de monitorización de las constantes vitales en entornos residenciales. Permitiendo la digitalización de los datos de forma automática, la generación de informes útiles para los médicos y dar un servicio de avisos a familiares o centros médicos en caso de incidencia. Con el consecuente ahorro de tiempo en la realización de este proceso que permitirá a los gerocultores invertir el tiempo ahorrado en mejorar la atención de los residentes.

Como se ha comentado, en la actualidad existen herramientas para la administración de centros residenciales, pero ninguna que integre el proceso de toma de medidas, digitalización de los datos automática y generación de informes útiles. Por lo tanto la integración de este proceso con una herramienta de gestión cierra el círculo de digitalización de los datos médicos, lo cual es una gran aportación tanto para los entornos residenciales como para Goooday Solutions, la empresa dónde se ha desarrollado.

Destaca el diseño, desarrollo, implementación, despliegue y evaluación de una herramienta funcional y que integra multitud de tecnologías, todas ellas muy novedosas y de muy diferentes ámbitos. Ya que al realizarse una implantación real han existido multitud de trabas legales a cumplir

Por último comentar que esta plataforma ha sido diseñada para centros residenciales y se ha comprobado su funcionamiento de forma correcta pero que gracias a la arquitectura escogida facilita su escalabilidad y podría ser adaptada a entornos más complejos como podría ser una clínica privada o un hospital público. Con el consecuente ahorro que supondría en los mismos el que la realización de la historia clínica sería automática, lo cual supone una de los mayores gastos de tiempo para un enfermero.

5.2 Cumplimiento de los objetivos propuesto

Cabe destacar que la plataforma ya ha sido instalada en un centro residencial en el que está funcionando con resultados muy satisfactorios, lo cual supone el cumplimiento del objetivo principal de este proyecto. En muchas ocasiones este es el paso más complicado y muchas buenas ideas acaban no llevándose a la práctica, pero en este caso gracias a la apuesta tan fuerte que ha hecho Goooday con este proyecto, ha sido posible.

En cuanto a los objetivos concretos:

- **Diseño, desarrollo e implementación de una aplicación Android para Smartphone:** Se ha cumplido el objetivo de la realización los módulos de autenticación y control de acceso mediante NFC, el módulo de comunicación con los dispositivos médicos mediante Bluetooth.

- **Diseño, desarrollo e implementación de una aplicación de gestión para la administración de usuarios y medidas:** Se ha cumplido el objetivo completamente en todos sus módulos, incluso se han añadido funcionalidades extra en todos los módulos como son los motores de ayuda de búsqueda mediante filtrado y agrupado por multitud de características. Además de la creación de un interfaz moderno e intuitivo que hace que su uso sea mucho más sencillo.
- **Diseño, desarrollo e implementación de un módulo servidor para el almacenamiento y tratamiento de datos:** Se ha cumplido el objetivo completamente, incluso se cambió el diseño inicial para que la búsqueda en la base de datos fuese mucho más eficiente y rápida. Con esto se consiguió una plataforma más fluida.
- **Implantación real y evaluación de la plataforma:** Se ha cumplido ya que se ha implantado en una residencia de Aragón y se realizó un proceso de evaluación mediante encuestas.

5.3 Valoración personal

A título personal, este proyecto fin de carrera ha resultado ser una experiencia sumamente gratificante tanto a nivel profesional como personal.

En primer lugar, a nivel profesional, considero que los conocimientos adquiridos me serán de mucha utilidad en el ámbito profesional. Debido a las características de este proyecto, he tenido la oportunidad de aprender numerosas tecnologías (algunas con más profundidad que otras), todas ellas de rabiosa actualidad y enorme potencial (Android, NFC, Bluetooth, MySql, SQLite, .NET, servicios web REST, etc.). Por otra parte, la temática general del proyecto me apasiona (e-Salud) y, desde mi punto de vista, es uno de los ámbitos de más demanda en la actualidad y en el futuro.

En segundo lugar, a nivel personal, estoy muy contento con el ambiente y el grupo humano que me he encontrado en la empresa Goooday Solutions S.L. Sin duda, me han facilitado al máximo la tarea que me ocupaba, con su interés y dedicación. Además, he tenido la oportunidad de comprobar la realidad de las jóvenes empresas innovadoras, en las cuales el grupo de trabajo ha de ser lo más interdisciplinar posible, donde los proyectos son llevados por la totalidad de sus componentes permitiéndome observar una inmejorable perspectiva global de respuesta ante diferentes proyectos.

Por otra parte, me gustaría resaltar que estoy muy satisfecho con mi respuesta personal al problema inicial de la falta de conocimientos de todas las tecnologías empleadas a lo largo de este PFC así como la resolución de diversos problemas durante su desarrollo.

Finalmente, la plataforma desarrollada en este PFC está funcionando de forma profesional una residencia de Aragón y como se desprende de la evaluación realizada estoy muy satisfecho con el resultado obtenido.

5.4 Líneas futuras

La plataforma se ha realizado de forma modular de manera que futuras ampliaciones o mejoras no suponga un mucho trabajo. Existe una gran capacidad de mejora en lo que a funcionalidades de administración en la aplicación de gestión se refiere. Por ello tanto en el servicio web, en la base de datos y en la aplicación de gestión ya se tuvo en cuenta la inclusión de estas posibles ampliaciones.

- **Identificación mediante huella dactilar:** Tal y como se planteó al inicio de este proyecto, la identificación mediante huella dactilar para la identificación de residentes reduciría el riesgo de errores humanos en la fase de selección.
- **Proceso de evaluación:** Debido a que el proyecto piloto se realizó en una única residencia el proceso de evaluación realizado no dispone de las suficientes muestras. Una vez esté implantado en más residencias o centros de días se pretende realizar un proceso de evaluación con una metodología más rigurosa.
- **Módulos de valor añadido:** Se plantea el desarrollo de ciertos módulos que dotaran a la plataforma de más funcionalidades. Por ejemplo módulo de posología, módulo de curas y módulo de tratamientos farmacológicos.
- **Agenda:** Programación de agendas para gerocultores y personal de administración. Acceso a las mismas desde el Smartphone. Asociación de acciones programadas a cada residente con el gerocultor que la realizará.
- **Notificaciones:** Implementación de un servicio de notificaciones al Smartphone de cualquiera de los módulos programables.
- **Integración con redes sociales:** Se planta la integración con algún tipo de red social médica de la que pudiesen participar tanto personal sanitario como residentes y familiares.

6 Bibliografía

1. World Health Organization (WHO, OMS en español). *Health Topics. eHealth.* <http://www.who.int/topics/ehealth/en/>
2. B. Friedman et al. *Patient satisfaction, empowerment, and health and disability status effects of a disease management-health promotion nurse intervention among Medicare beneficiaries with disabilities.* The Gerontologist, vol. 49, pp. 778-792.2009.
3. S.M.Musa; Roy G. Perry Coll. of Eng., Prairie View A&M Univ., Prairie View, TX, USA, T.D.Q.Jefferson, M.N.O. Sadiku. *A simple model for biometric identification technology using fingerprint scanning.* Southeastcon, 2012 Proceedings of IEEE. 10.1109/SECon.2012.6197071
4. Padma Polash, P.; Ahsanullah Univ. of Sci. & Technol., Dhaka; Maruf Monwar, M. *Human iris recognition for biometric identification.* Computer and information technology, 2007. iccit 2007. 10th international conference on. 10.1109/ICCITECHN.2007.4579354
5. Engelberg, S.; Saidoff, Y.; Israeli, Y. *Voice identification through spectral analysis.* Instrumentation & Measurement Magazine, IEEE (Volume:9 , Issue: 5). 10.1109/MIM.2006.1708353
6. Continua Health Alliance. <http://www.continuaalliance.org/>
7. Continua Health Alliance. <http://mobihealthnews.com/2577/continua-picks-zigbee-bluetooth-le-for-health-devices-sensors/>
8. Página web oficial de ResiPlus. <http://www.addinformatica.com/en/>
9. Página web oficial Resiges. <http://www.resiges.com/>
10. J.Noueihed, R. Diemer, S. Chakraborty, S. Biala. *Comparing Bluetooth HDP and SPP for Mobile Health Devices.* BSN '10 Proceedings of the 2010 International Conference on Body Sensor Networks. 978-0-7695-4065-8
11. L.C. Guillou et al. *The smart card: A standardized security device to public cryptology.* Contemporary Cryptology: The Science of Information Integrity, IEEE Press, 1992
12. Roger Merckling and Anne Anderson. *RFC 57.0: Smart Card Introduction.* 1994
13. David Everett. *Identity verification and biometrics.* Computer Security Reference Book. Butterworth-Heinemann. 1992
14. Eric Guerrino et al. *User authentication and encryption overview.* 1997
15. Rafael Navarro Marset. Departamento de Sistemas Informáticos y computación de la Universidad Politécnica de Valencia. *REST vs WEB Services.* Modelado, Diseño e Implementación de Servicios Web. 2006-2007
16. Microsoft Developer Network. *SOAP, REST y más.* MSDN Magazine. Julio 2009

17. Android Developers. Intent.
<http://developer.android.com/reference/android/content/Intent.html>
18. Bluetooth quick reference guide. <https://www.bluetooth.org/en-us>
19. Bluetooth features and technical description. <https://www.bluetooth.org/en-us>
20. NFC-Forum. <http://www.nfc-forum.org>
21. V. Nilsson and E. Rolf. *Near Field Communication (NFC) for Mobile Phones.* Master's Thesis, Lund University. August 2006.
22. MySQL. *MySQL 5.0 Reference Manual.*
<http://dev.mysql.com/doc/refman/5.0/es/index.html>
23. MySQL. *MySQL Workbench.*
<http://dev.mysql.com/doc/workbench/en/index.html>
24. SQLite. *SQLite Features.* <http://www.sqlite.org/features.html>

7 Anexo 1: Análisis de alternativas de diseño

7.1 Alternativas para la identificación/autenticación de usuarios

Los métodos de autenticación de usuarios a una plataforma pueden dividirse en tres grandes grupos dependiendo del qué se utiliza para verificar la identidad.

7.1.1 Autenticación basada en algo conocido

El método de autenticación clásico y más básico consiste en la verificación de su identidad mediante la comprobación de que conoce las credenciales de acceso que *a priori* sólo ese usuario conoce. Esto consiste en la introducción de una contraseña secreta. Éste método es el más vulnerable ante cualquier tipo de ataque, pero su bajo coste la hace la más utilizada en entornos que no precisan de una alta seguridad. En general la mayoría de las redes de seguridad media/baja hacen uso de este tipo de métodos. También suelen ser usadas como método complementario a otro mecanismo de autenticación.

En los esquemas de autenticación basados en algo conocido se cumple el mismo protocolo de actuación. Existe una entidad activa y otra pasiva. Las dos entidades acuerdan unas credenciales de acceso que han de mantenerse en secreto para que la autenticación sea fiable. Cuando la entidad activa desea autenticarse debe mostrar el conocimiento de las credenciales a la entidad pasiva que permitirá o no el acceso al sistema en función de si la autenticación ha sido satisfactoria o no.

Como se ha dicho este sistema es de una seguridad muy débil, basta con que una de las entidades comparta las credenciales con un tercero para que toda la seguridad se pierda o que alguien lea estas credenciales mediante un ataque.

7.1.2 Autenticación basada en algo poseído

Hace más de veinte años un periodista francés llamado Roland Moreno patentaba la integración de un procesador en una tarjeta de plástico; sin duda, no podía imaginar el abanico de aplicaciones de seguridad que ese nuevo dispositivo, denominado *chipcard*, estaba abriendo. Desde entonces, cientos de tarjetas monedero más sencillas hasta el control de accesos de todo tipo; cuando las *chipcards* se les incorporó un procesador inteligente nacieron las *smartcards* [11,12], una gran revolución en el ámbito de la autenticación de usuarios.

Desde el punto de vista formal, una tarjeta inteligente es un dispositivo de seguridad del tamaño de una tarjeta de crédito, resistente a la adulteración, que ofrece funciones para un almacenamiento seguro de la información y también para el procesamiento de la misma en base a tecnología *Very Large Scale Integration* (VLSI). En la práctica, las tarjetas inteligentes poseen un chip empotrado en la propia tarjeta que puede implementar un sistema de ficheros cifrado y funciones criptográficas, y además que las diferencia de las simples tarjetas de crédito, que solamente incorporan una banda magnética donde va almacenada cierta información del propietario de la tarjeta.

Cuando el usuario poseedor de una *smartcard* desea autenticarse necesita introducir la tarjeta en un hardware lector. Los dos dispositivos se identifican entre sí con un protocolo a dos bandas en el que es necesario que ambos conozcan la misma clave (*Company Key o Chipcard Communication Key*, CK o CKK), lo que elimina la posibilidad de utilizar tarjetas de terceros para autenticarse ante el lector de una determinada compañía. Además esta clave puede utilizarse para asegurar la comunicación entre la

Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad

Samuel Longares Losilla - Eduardo Prado Clemente

tarjeta y el dispositivo lector. Una vez identificarse las dos partes, puede requerirse la identificación personal (PID) de la tarjeta, y el usuario tendrá que teclear su PIN, iniciándose entonces un protocolo desafío-respuesta: se envía el PID a la máquina y ésta desafía a la tarjeta, que responde al desafío utilizando una clave personal del usuario (*Personal Key, PK*). Si la respuesta es correcta, el host ha identificado la tarjeta y el usuario obtiene acceso al recurso pretendido.

Las ventajas de utilizar tarjetas inteligentes como medio para autenticar usuarios son muchas frente a las desventajas. Se trata de un modelo ampliamente aceptado entre los usuarios, rápido, y que incorpora hardware de alta seguridad tanto para almacenar datos como para realizar funciones de cifrado. Su uso es factible tanto para controles de acceso físico como para controles de acceso lógico a los hosts, y se integra fácilmente con otros mecanismos de autenticación como las contraseñas. Además, en caso de desear bloquear el acceso de un usuario, no tenemos más que retener su tarjeta cuando la introduzca en el lector o marcarla como inválida en una base de datos. Como principal inconveniente de las *smartcards* destacar el coste adicional que supone para una organización el comprar y configurar la infraestructura de dispositivos lectores y las propias tarjetas. Además, que un usuario pierda su tarjeta es bastante fácil, y durante el tiempo que no disponga de ella o no pueda acceder a la plataforma, hará que establecer reglas especiales que puedan comprometer su seguridad (y por supuesto se ha de marcar como tarjeta inválida en una base de datos central, para que un potencial atacante no pueda utilizarla).

A parte de los problemas que puede implicar el uso de *smartcards* en sí, contra la lógica de una tarjeta inteligente existen diversos métodos de ataque, como realizar ingeniería inversa- destructiva- contra el circuito de silicio (y los contenidos de la *Read Only Memory, ROM*), adulterar la información guardada en la tarjeta o determinar por diferentes métodos el contenido de la memoria EEPROM.

7.1.3 Autenticación basada en biometría

A pesar de la importancia de la criptología en cualquiera de los módulos de identificación de usuarios comentados anteriormente, existen otra clase tipo en los que no se aplica esta ciencia, o al menos su aplicación es secundaria. Es más, parece que en un futuro no muy lejano estos serán los que se van a imponer en la mayoría de situaciones en las que se haga necesario autenticar un usuario: son más amigables para él (no va a necesitar recordar *passwords* o números de identificación complejos, y, como se suele decir, el usuario puede olvidar una tarjeta de identificación en casa, pero nunca se olvidará de su mano o su ojo) y son mucho más difíciles de falsificar que una simple contraseña o una tarjeta magnética; las principales razones por la que no se han impuesto ya en nuestros días es su elevado precio, fuera del alcance de muchas organizaciones , y su dificultad de mantenimiento.

Estos módulos son los denominados biométricos [13, 14], basados en características físicas del usuario a identificar. El reconocimiento de formas, la inteligencia artificial y el aprendizaje son las ramas de la informática que desempeñan el papel más importante en los módulos de identificación biométricos; la criptología se limita aquí a un uso secundario, como el cifrado de una base de datos de patrones retinales, o la transmisión de una huella dactilar entre un dispositivo analizador y una base de datos. La autenticación basada en características físicas existe desde que existe el hombre y, sin darnos cuenta, es la que más utiliza nosotros en su vida cotidiana: a diario identificamos a personas por los rasgos de su cara o por su voz. Aquí el agente reconocedor lo tiene fácil porque es una persona, pero en el modelo aplicable a redes

o sistemas Unix el agente ha de ser un dispositivo que, según las características del sujeto a identificar, le permita o deniegue acceso a un cierto recurso.

7.2 Alternativas para el diseño de una solución para la gestión de datos

Para analizar las alternativas de diseño de una solución para la gestión de datos y elegir la óptima para este PFC (siempre buscando soluciones abiertas y gratuitas), se contemplan bases de datos relacionales (*Structured Query Language, SQL*) y bases de datos no relacionales (*Not only SQL, NoSQL*).

7.2.1 Bases de datos relacionales (SQL)

Están basadas en el modelo relacional propuesto por Codd en 1967. El motor (programa que permite gestionar el acceso y las operaciones sobre la base de datos) actúa sobre la información agrupada en estructuras denominadas tablas (formadas por filas y columnas) que representan entidades de un modelo de datos. Los valores únicos de determinadas filas permiten relacionar desde el punto de vista lógico una tabla o entidad con otras. Para operar con los datos almacenados en bases de datos relacionales se utiliza un lenguaje estándar denominado SQL.

7.2.1.1 Bases de datos no relacionales (NoSQL)

No están basadas en el modelo relacional clásico. El motor no trabaja sobre tablas de estructura fija de filas y columnas, sino sobre información estructurada en filas que pueden tener distinto tamaño componiendo finalmente un documento con un cierto formato como puede ser *JavaScript Object Notation (JSON)* u otros tipos. Por lo general, utilizan un modelo clave-valor para almacenar y recuperar la información por lo que el motor es mucho más robusto, simple y rápido, pero no soportan operaciones como JOIN (operación que permite recuperar información combinada de más de una tabla) ni utilizan el SQL como lenguaje de manipulación de los datos.

7.2.2 Comparativa

Como muchos ámbitos, no solo técnicos, ambos enfoques pueden ser perfectamente válidos. No necesariamente tiene que ser uno mejor que el otro axiomáticamente y la conveniencia de emplear uno u otro va a depender de las características del problema que se pretenda resolver. Una base de datos relacional (SQL) puede ser muy útil cuando disponemos de gran cantidad de información y, además, toda ella está muy relacionada, es decir, existen muchas dependencias en conjunto global de la información. En el caso de la plataforma que se está desarrollando en este PFC, la información sanitaria tanto de pacientes como del personal está fuertemente relacionada. Parece claro por tanto, que se va a necesitar una base de datos de tipo SQL para abordar todas esas relaciones.

7.3 Alternativas para el diseño de un servicio web

Para comenzar a analizar las alternativas para el diseño de un servicio web, es preciso introducirlas primero para, posteriormente, compararlas y tomar una decisión. Básicamente existen dos alternativas [15, 16] que son, por un lado el protocolo *Simple Object Access Protocol (SOAP)* y por otro la filosofía *Representational State Transfer (REST)*. El método tradicional de diseñar servicios web es SOAP mientras que, a pesar de que REST como filosofía es bastante antigua, REST como arquitectura es la forma más reciente, novedosa y con más auge que existe actualmente. A pesar de esto, REST no tiene por qué ser la solución óptima para todos los escenarios sino que es preciso

analizar lo que ofrecen cada uno de estos métodos. A la hora de realizar una búsqueda de información sobre estas dos alternativas, queda claro que cada una de ellas tiene sus seguidores y detractores. Además existen bastantes diferencias entre ambos que requieren de un bastante conocimiento previo en la materia y, como no es el caso, lo que se ha hecho para la elección es aglutinar en este anexo aquellas que realmente pueden resultar de una utilidad clara en el contexto de la plataforma que se pretende diseñar en esta PFC.

7.3.1 Simple Object Access Protocol (SOAP)

SOAP es un protocolo basado en XML, para realizar llamadas a procedimientos/métodos de forma remota (*Remote Procedure Call*). Utiliza cualquier protocolo que permita transportar mensajes de texto, en formato XML, siendo HTTP el más utilizado. Su especificación describe el contenido que debe tener un mensaje formato *eXtensible Markup Language* (XML) para ser usado en una llamada remota. Cualquier aplicación que cumpla la especificación puede llamar y proveer servicios sin importar en qué lenguaje o plataforma esté implementado, lo único necesario es que la aplicación sea capaz de interpretar el mensaje SOAP que recibe, realizar el procesado que el mensaje requiera, y devolver otro mensaje SOAP con la respuesta.

7.3.2 Representational State Transfer (REST)

REST es una arquitectura basada en recursos en la que cada uno de ellos dispone de un identificador único denominado *Uniform Resource Identifier* (URI). Estos recursos pueden ser entidades, colecciones o cualquier cosa que el diseñador crea que merece la pena que tenga su propia URI. No implementa sus propios métodos sino que hace uso de los verbos http (POST, PUT, GET y DELETE) que están ya estandarizados. El formato en el que los datos se intercambian no está restringido a uno solo sino que tiene bastante flexibilidad, siendo muy comunes formatos como JSON o XML.

7.3.3 Comparativa

Una vez introducidas cada una de las dos alternativas, a continuación se va a exponer las razones concretas por las que se ha elegido como solución de diseño REST y no SOAP. En el contexto de este PFC, las razones por las que se ha elegido REST son las siguientes:

- **Flexibilidad y simplicidad:** La metodología REST, al hacer uso de una interfaz ampliamente usada y conocida como es la URI, es una forma muy sencilla e intuitiva de acceder a cualquier tipo de recurso. Un ejemplo de URI, relacionado con la plataforma que se pretende diseñar, podría ser <https://miservidor:puerto/residents>. Cualquier aplicación autorizada, ya sea cliente o servidor, que soporte HTTP podría realizar una petición HTTP GET y recibir, por ejemplo los nombres de todos los residentes almacenados en la base de datos. Como se puede observar, es muy sencillo e intuitivo acceder a los recursos y, además, es muy flexible desde el punto de vista que permite emplear casi cualquier formato de datos pudiendo elegir así el que más convenga. SOAP por el contrario, requiere de un importante conocimiento del protocolo del que hace uso, así como restringe el formato de datos a XML.
- **Uso de ancho de banda:** Las peticiones y respuestas en una arquitectura REST, pueden ser muy cortas mientras que en SOAP es necesario aplicarles formato XML provocando que, por ejemplo, para la misma respuesta a una misma petición, SOAP necesite diez veces más Bytes que REST. En el contexto de la *Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad*

plataforma a diseñar, hay que pensar que un dispositivo móvil, cuenta con recursos limitados desde una batería con una cierta capacidad cuyo gasto hay que tratar de optimizar por todos los medios hasta una tarifa de datos (si no hace uso de la WiFi) restringida a una cierta cantidad de información. Además, se necesita que la plataforma sea ágil por lo que cuanto menos haya que esperar para recibir la información mucho mejor.

- **Seguridad:** Aunque parece que SOAP, a nivel empresarial, dispone de ciertas herramientas más específicas para controlar la seguridad, el hecho de que las llamadas a procedimientos remotos las realice a través de puertos estándares de HTTP, no permite tener un control para un posible filtrado de distintos tipos de llamadas. Sin embargo, con metodología REST, las condiciones de seguridad pueden ajustarse analizando la cabecera HTTP permitiendo, por ejemplo, que una petición GET siempre se considere segura o que las peticiones POST se examinen cuidadosamente. Además REST soporta tanto HTTP como HTTPS.
- **Complejidad en el lado del cliente:** A la hora de realizar peticiones a un servicio web REST, es mucho más sencillo que hacerlo con SOAP ya que este último requiere de una librería específica y de un periodo de aprendizaje mucho mayor del que sería necesario para saber cómo formar una petición HTTP. Esto es muy importante, ya que de esta manera permite reaprovechar el servicio web haciendo mucho más sencillo el diseño de nuevas plataformas que hagan uso de él.

8 Anexo 2: Tecnologías

8.1 Android

Android es una solución completa de software de código libre para teléfonos y dispositivos móviles. Es un paquete que engloba un sistema operativo, un runtime de ejecución basado en Java, una serie de librerías de bajo y medio nivel y un conjunto inicial de aplicaciones destinadas al usuario final. Se distribuye bajo una licencia Apache versión 2 (ASL2), una licencia libre permisiva que permite la integración con soluciones de código propietario.

Los primeros dispositivos con Android aparecieron en el último trimestre de 2008, aunque una versión preliminar del SDK, acompañado de un emulador y documentación de desarrollo, se encuentra disponible desde el 12 de noviembre de 2007.

Android buscaba (y lo ha conseguido) causar impacto en la industria de la comunicación móvil, estableciendo una plataforma abierta que permita un acceso fácil a prácticamente todas las funcionalidades hardware de los dispositivos en los que esté instalado, así como proveyendo de serie a los desarrolladores con librerías que favorezcan la creación ágil y rápida de aplicaciones. Se ha hecho especial énfasis en que las aplicaciones creadas por terceros no tendrán ningún tipo de desventaja en cuanto a funcionalidad y acceso al dispositivo frente a las aplicaciones "nativas" que se distribuyen originalmente con Android.

8.1.1 Arquitectura

Android proporciona un paquete completo de software a todos los niveles:

- Un *kernel* Linux que sirve como base de la pila de software y se encarga de las funciones más básicas del sistema: gestión de drivers, seguridad, comunicaciones, etc.
- Una capa de librerías de bajo nivel en C y C++, como *SQLite* para persistencia de datos; *SGL*, desarrollada por *Skia* (adquisición de Google); *OpenGL ES* para gestión de gráficos 3D, con aceleración 3D opcional y *WebKit* como navegador web embebido y motor de HTML.
- Un *framework* para el desarrollo de aplicaciones, dividido en subsistemas como el *package manager*, gestión del hardware del teléfono anfitrión (*telephony manager*) o acceso a APIs sofisticadas de geolocalización o mensajería XMPP. También incluye un sistema de vistas para manejar el interfaz de usuario de las aplicaciones, que ofrece posibilidad de visualización de mapas o renderizado HTML directamente en el interfaz gráfico de la aplicación.
- Una suite de aplicaciones (navegador, agenda, gestión del teléfono).

Las aplicaciones Android están programadas en Java, pero no corriendo sobre Java ME, sino sobre Dalvik, una máquina virtual Java desarrollada ex profeso por Google y optimizada para dispositivos empotrados y en la que los códigos fuente se compilan a ficheros de *bytecode .dex*. La creación de una virtual machine propia es un movimiento estratégico que permite a Google evitar conflictos con Sun por la licencia de la máquina virtual, así como asegurarse el poder innovar y modificar ésta sin tener que batallar dentro del *Java Community Process*.

8.1.2 Estructura de la aplicación

La estructura de una aplicación Android está definida por la interacción de distintos componentes, haciendo énfasis en la "agrupación débil" de distintas piezas. La aplicación hará uso de las distintas APIs expuestas por Android, de forma que los componentes encargados de realizar cada tarea puedan ser manipulados o reemplazados sin problemas, asegurando la máxima flexibilidad. Por ejemplo, una aplicación puede permitir al usuario elegir fotos mediante el componente "Galería" o, por ejemplo, reemplazar esa "Galería" por una selección de fotos a través de un servicio online. Los principales componentes de una aplicación serían:

- **Activity:** Representa cada una de las principales tareas que el usuario puede llevar a cabo en la aplicación. Típica (aunque no necesariamente) corresponderá a una pantalla específica de la aplicación y, también normalmente, una *Activity* será el punto de entrada (pantalla inicial) de nuestra aplicación. Desde ella se invocarán las vistas específicas o *layouts* para la aplicación.
- **Intents:** La comunicación entre las distintas Activities se lleva a cabo mediante una herramienta de Android que se conoce como *Intent* [17]. Básicamente, un *Intent* permite indicarle a Android que se pretende realizar alguna tarea a través de una *Activity* construida específicamente para esa situación. Existen muchos tipos de *Intents*, desde el generado por Android al descubrir una tarjeta NFC en el campo de acción al dispositivo hasta el que se produce al llamar a otra actividad. Además, en ciertos tipos de *Intents* es posible incluso añadir información que la Actividad destino pudiera necesitar.
- **IntentReceiver:** Permite a la aplicación declarar ciertos *callbacks* que responderán a cambios en el estado del terminal (mediante *Intents*). Por ejemplo, llamada o email recibido, cambio en la geolocalización, etc.
- **Service:** Una tarea que corre en el *background* que puede y debe ejecutarse sin interacción con el usuario. Una aplicación puede mandar los mensajes necesarios a un determinado servicio activo.
- **ContentProvider:** Establece una capa que permite a las distintas aplicaciones compartir datos. Con independencia del almacenamiento local que utilicen para sus propósitos, las aplicaciones necesitan declarar *ContentProviders* para poner a disposición de otros procesos los datos que consideren necesarios.

Estas son algunas de las principales, pero no las únicas piezas de construcción de la aplicación. También es interesante que se defina como pieza de primer nivel, el sistema de notificaciones en pantalla, que se recomienda como principal vía de comunicación con el usuario.

8.1.3 Ciclo de vida de una actividad Android

Las actividades que componen una aplicación Android tienen un ciclo de vida muy claro el cual viene determinado por una serie de estados y sus transiciones. Estos estados presentan nombres muy intuitivos como *onCreate*, *onStart*, *onPause*, etc., por lo que la figura 24 que muestra este ciclo de vida no requiere de mucha más explicación.

Es un aspecto muy importante que todo desarrollador ha de controlar ya que sino las aplicaciones pueden comenzar a trabajar muy lentamente, pudiendo incluso bloquearse.

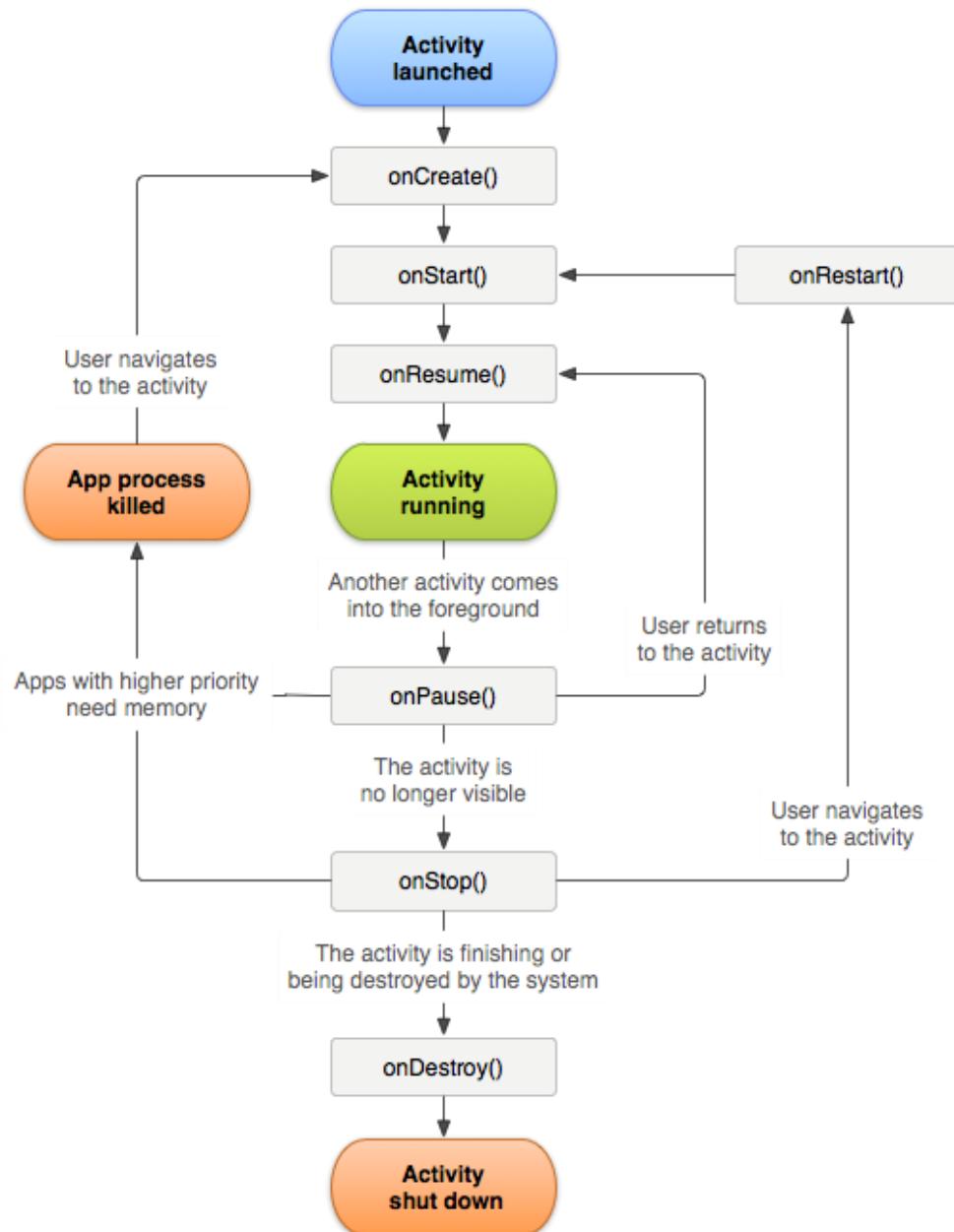


Figura 25: Ciclo de vida de una actividad Android

8.1.4 Dispositivos disponibles

Android ha conseguido “explotar” en los últimos años siendo actualmente el SO móvil más utilizado por lo que la variedad de dispositivos disponibles en cuanto a tamaño, características y versiones es enorme. Ha dejado de ser fruto de cábalas y especulaciones, para convertirse en una realidad y ocupar la mayor cuota de mercado, superando incluso, según las últimas estadísticas de ventas, al exitoso iPhone de Apple. De la mano de HTC, que apostó por él desde el principio y ha colaborado con Google en su lanzamiento y expansión (fabricando tanto los *Dev Phones*, primeros dispositivos móviles Android, como el reciente HTC One), el resto de fabricantes se han subido al tren de Android y han desarrollado terminales con el nuevo sistema operativo siendo Samsung el más importante en la actualidad. Además, está en constante evolución en cuanto a sus versiones, la última de ellas llamada *KitKat* (lanzada a finales de 2013).

Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad

Samuel Longares Losilla - Eduardo Prado Clemente

8.1.5 Desarrollo de aplicaciones

Para el desarrollo de aplicaciones de Android, Google proporciona una herramienta llamada *Android Developer Tools* (basada en Eclipse) que facilita el trabajo, ofreciendo herramientas como emuladores, acceso al sistema de archivos, gestión de hilos en ejecución, consola, etc. Por lo tanto, para comenzar a trabajar, lo primero que debe hacerse es descargar dicha herramienta de la página oficial de desarrolladores Android (<http://developer.android.com>).

8.2 Bluetooth

8.2.1 Introducción al Bluetooth

Bluetooth es una tecnología de corto alcance simple, segura y que desde hace unos años podemos encontrar en muchos ámbitos de nuestra vida. Esta tecnología es muy flexible en el sentido de que la podemos encontrar en casi cualquier tipo de dispositivo desde teléfonos móviles, ordenadores y productos de entretenimiento para el hogar hasta dispositivos médicos. Su objetivo principal es llegar a eliminar los cables con los que habitualmente conectamos los dispositivos que usamos ganando indudablemente en comodidad y movilidad pero sin perder la seguridad que estos nos proporcionaban.

Bluetooth no deja de ser una especificación para Redes Inalámbricas de área personal (WPAN) que ofrece la posibilidad de transmitir voz y datos de forma simultánea entre dispositivos empleando como medio un enlace por radiofrecuencia en la banda de los 2.4 GHz. Esta frecuencia de radio es una de las bandas reservadas ISM (*Industrial, Scientific and Medical*) que no requieren licencia.

Las razones del éxito de la tecnología Bluetooth y que le ha llevado a consolidarse en el mercado atienden a cuestiones como que es posible integrarla en un gran número de dispositivos de muy diversa índole, elimina los molestos cables y conectores con los que estábamos acostumbrados a lidiar, ofrece la posibilidad de crear reducidas redes personales, permite realizar tareas de sincronización entre equipos y, todo esto, a un coste relativamente bajo.

Como fuente de información para la realización los siguientes apartados relacionados con Bluetooth y de esta manera adquirir los conocimientos previos necesarios, se ha acudido a la literatura tecnológica pertinente [18, 19].

8.2.2 Historia

Todo comenzó a mediados de la década los 90, cuando la empresa Ericsson inició una investigación que pretendía estudiar la viabilidad de un interfaz radio, de bajo coste y consumo, que permitiera interconectar teléfonos móviles y otros tipos de dispositivos de forma inalámbrica. Como resultado de este estudio se diseñó un enlace radio de corto alcance llamado MC Link que, unos años más tarde, despertaría el interés de otros importantes fabricantes de equipos móviles lo que originaría la formación de un grupo llamado *Bluetooth Special Interest Group* (Bluetooth SIG). La idea era lograr un conjunto adecuado de áreas de negocio, ya que se hallaban en el grupo líderes del mercado de varios sectores. Este grupo estaba formado por compañías como Agere, Ericsson, IBM, Intel, Microsoft, Motorola, Nokia y Toshiba y su objetivo era desarrollar las especificaciones para Bluetooth 1.0, que se publicaron en julio de 1999.

8.2.3 Características del Bluetooth

8.2.3.1 Frecuencia, disposición de canales y modulación

Como se ha introducido anteriormente, Bluetooth opera en la banda no regulada ISM de los 2.4 GHz, por lo que esta banda puede ser empleada por numerosos y diferentes dispositivos ya sean industriales, científicos o médicos.

La elección de esta frecuencia de operación, presenta el inconveniente de que es posible que en un mismo lugar exista más de un dispositivo emitiendo en esta banda. Por ejemplo, en una misma casa podemos tener un teléfono inalámbrico, la puerta del garaje, un monitor de seguimiento para un bebé, un teléfono móvil usando Bluetooth e incluso la WiFi de casa todas ellas emitiendo en la banda de 2.4 GHz.

Por tanto, un dispositivo Bluetooth previsiblemente va a funcionar en un entorno ruidoso, es decir, numerosos dispositivos emitiendo en la banda ISM, con un alcance típico de unos 10 metros y, además, sin requerir línea de visión directa. Por tanto, ha de haber algún tipo de mecanismo que asegure que un dispositivo Bluetooth no sea interferido por otros dispositivos que emitan a la misma frecuencia que él. La solución a este problema pasa por emplear una modulación de espectro ensanchado con saltos en frecuencia (*Frequency Hopping Spread Spectrum*).

8.2.3.1.1 Espectro ensanchado en Bluetooth

Una vez se han introducido las principales formas de realizar una modulación de espectro ensanchado, es momento de ver como se concreta en Bluetooth.

Anteriormente se ha adelantado que la solución a los problemas de operación de dispositivos Bluetooth en entornos ruidosos pasaba por emplear una modulación de espectro ensanchado por salto en frecuencia. Por tanto, particularizando este tipo de técnica de espectro ensanchado para el caso de la tecnología Bluetooth, divide la banda ISM a 2.4 GHz en 79 canales cada uno de 1 MHz de ancho de banda. Estos canales se numeran del 0 al 78 comenzando exactamente en 2.402 GHz aceptando una en frecuencia a partir de la central para cada canal ± 75 kHz. Cumple con la regulación concerniente a señal fuera de banda dejando para ello bandas de guarda inferior y superior de 2 MHz y 3.5 MHz respectivamente. Cabe destacar que países como España, Francia y Japón, Bluetooth no dispone de 79 canales sino que queda restringido a solamente 23 debido a regulaciones existentes en estos países.

Se producen hasta 1600 saltos de canal por segundo permaneciendo en cada uno de ellos únicamente 625 microsegundos (time slot). Esta secuencia de saltos, como se ha comentado anteriormente, es conocida únicamente por el emisor y el receptor y, si se aplica a Bluetooth, quiere decir que cualquier dispositivo que no pertenezca a la misma *piconet*, no va a conocer esta secuencia de saltos y, por tanto, no va a poder efectuar una comunicación.

La modulación que se emplea es de tipo *Gaussian Frequency Shift Keying* (GFSK) a 1 Mbps con un producto ancho de banda por tiempo de transmisión de bit para el filtro paso bajo gaussiano igual a $BT=0.5$ que determina la forma de dicho filtro. Un uno binario es representado por una desviación positiva en frecuencia mientras que un cero binario se representa mediante una desviación negativa en frecuencia. El uso de este tipo de modulación FSK consigue reducir el espectro fuera de banda ocupado empleando el espectro de una forma más eficiente.

Como se puede ver, usar espectro ensanchado por salto en frecuencia aumenta considerablemente la seguridad de Bluetooth ya que si una tercera parte no autorizada quiere monitorizar la comunicación, sería impracticable que lo hiciera en los 79 canales disponibles entre los que se va saltando siguiendo un orden que no conoce.

En la tabla 1 se resumen las características de Bluetooth comentadas en este *Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad*

Samuel Longares Losilla - Eduardo Prado Clemente

apartado.

Bluetooth	Especificaciones
Rango de frecuencia	2.4 – 2.4835 GHz (ISM)
Tipo de modulación	GFSK
GFSK BT	0.5
Número de canales	79
Disposición de canales	$f=2402+k$ MHz, $k=0,\dots,78$
BW canal	1 MHz
Banda de guarda superior	3.5 MHz
Banda de guarda inferior	2 MHz
Tolerancia en frecuencia	± 75 KHz desde la central de portadora
Tasa de saltos	1600 saltos/segundo
Time slot	625 microsegundos

Tabla 1: Resumen de las características frecuenciales, disposición de canales y modulación de Bluetooth

8.2.3.2 Transmisión

La velocidad de transmisión se encuentra alrededor de 1 Mb/s, un valor inferior a otros estándares radio como 802.11b (11 Mb/s), aunque algo superior a la transmisión infrarroja.

Bluetooth utiliza un esquema de división en el tiempo para obtener una transmisión full-dúplex. Su protocolo de banda base es una combinación de conmutación de paquetes y conmutación de circuitos, y posee cuatro canales: tres canales síncronos de voz y un canal asíncrono de datos. Cada canal de voz permite un enlace síncrono de 64 kb/s. El canal asíncrono permite un enlace asimétrico de 721 kb/s y 57.6 kb/s en la respuesta, o un enlace simétrico de 432.6 kb/s.

8.2.3.3 Potencia

La velocidad de transmisión se encuentra alrededor de 1 Mb/s, un valor inferior a otros estándares radio como 802.11b (11 Mb/s), aunque algo superior a la transmisión infrarroja.

Bluetooth utiliza un esquema de división en el tiempo para obtener una transmisión full-dúplex. Su protocolo de banda base es una combinación de conmutación de paquetes y conmutación de circuitos, y posee cuatro canales: tres canales síncronos de voz y un canal asíncrono de datos. Cada canal de voz permite un enlace síncrono de 64 kb/s. El canal asíncrono permite un enlace asimétrico de 721 kb/s y 57.6 kb/s en la respuesta, o un enlace simétrico de 432.6 kb/s.

8.2.3.4 Alcance

El estándar Bluetooth define tres tipos de emisores, todos compatibles entre ellos y que se diferencian en la potencia de transmisión que son capaces de ofrecer (tabla 2).

Incluso emitiendo a baja potencia, Bluetooth no requiere línea de visión (LoS)

entre los dispositivos que van a llevar a cabo la comunicación y atravesará sin problemas las paredes de, por ejemplo, una casa haciendo que sea útil para manejar dispositivos en diferentes habitaciones.

Clase	Tipo (potencia)	Potencia (mW)	Alcance (metros)
Clase 1	Alta	100 mW	Aprox. 100.
Clase 2	Media	2.5 mW	Aprox. 10
Clase 3	Baja	1 mW	Aprox. 1

Tabla 2: Resumen de las distintas clases de emisores Bluetooth

8.2.4 Redes

Cuando un dispositivo Bluetooth se conecta a otros compartiendo un mismo canal de comunicación, forman una pequeña red denominada *piconet*. Estas redes se componen de un dispositivo maestro que impone la frecuencia de saltos y de uno o más (hasta siete) dispositivos esclavos. No obstante, hasta 255 dispositivos pasivos pueden permanecer conectados a la *piconet*, de manera inactiva.

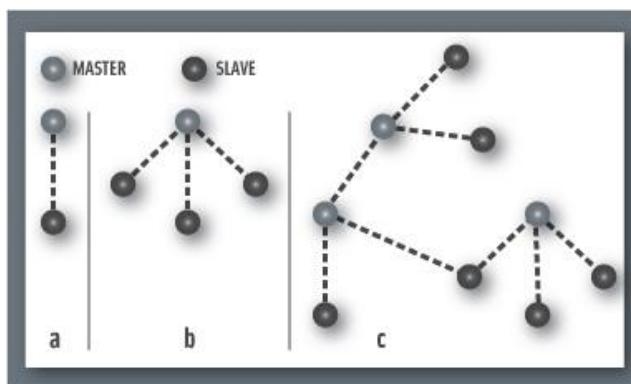


Figura 26: Redes Bluetooth. Piconet y Scatternet

A su vez, los esclavos pueden estar interconectados a diferentes *piconets*, formando una *scatternet*. En la Figura 43 puede verse un ejemplo de la misma en la cual se puede ver un único esclavo (a), varios esclavos (b) y una *scatternet* (c).

8.2.4.1 Perfiles Bluetooth

A parte de los protocolos descritos anteriormente, el estándar define lo que se denomina como perfiles Bluetooth (*Bluetooth Profiles*). Un perfil define un conjunto de características funcionales para cada aplicación que lo use y se utiliza para garantizar la interoperabilidad entre varios dispositivos Bluetooth que contemplan los mismos perfiles. Un dispositivo dispondrá de al menos un perfil como por ejemplo un manos libres para el coche aunque, muchos otros, soportaran múltiples perfiles como por ejemplo un teléfono móvil. De la pila de protocolos vistos en el apartado anterior, un perfil puede verse como una selección vertical de ella definiendo tanto las diferentes capas de protocolos empleados como las características de cada uno de ellos.

Existen multitud de perfiles disponibles en el estándar y una de las grandes diferencias de esta tecnología con respecto a otra es la capacidad de adaptación a futuras necesidades, es decir, si aparece una nueva aplicación para la cual la actual

especificación no da respuesta, basta con incluir un nuevo perfil adecuado para ella y así solucionar el problema. Además, el hecho de seguir las directrices proporcionadas por los perfiles los desarrolladores pueden crear aplicaciones compatibles con todos los dispositivos que se ajusten al perfil ganando en interoperabilidad.

Describir la totalidad de los perfiles disponibles es una osadía por lo que parece mucho más interesante hacerlo para el *Serial Port Profile* (SPP) que es el empleado en este PFC.

8.2.4.1.1 Serial Port Profile

El perfil puerto serie define los protocolos y procedimientos que utilizarán los dispositivos que utilizan Bluetooth a modo de RS232 (o similar) como emulación de un cable en serie.

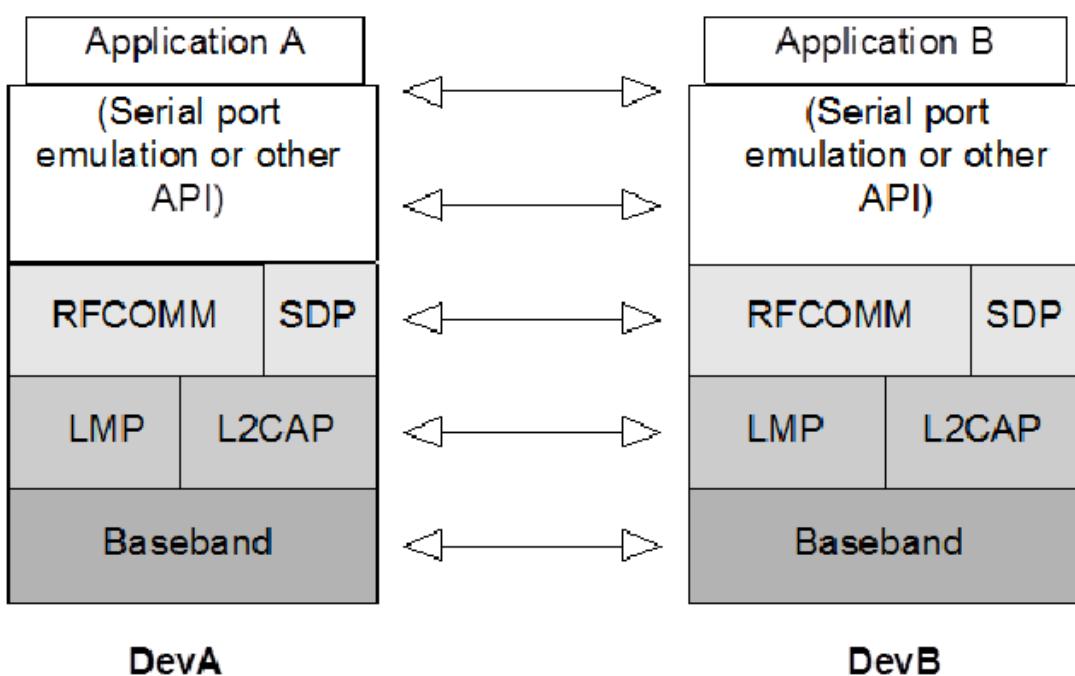


Figura 27: Arquitectura del perfil puerto serie

Banda base, LMP, y L2CAP son la capa OSI 1 y 2 protocolos Bluetooth. RFCOMM es la adaptación a Bluetooth de GSM TS 07.10, que proporciona un protocolo de transporte para la emulación de puerto serie. SDP es el protocolo de descubrimiento de Bluetooth.

La capa de emulación de puerto se muestra en la figura de arriba es la entidad emulando el puerto serie, o proporcionando una API para aplicaciones.

Las aplicaciones de ambos lados son las aplicaciones, capaces y queriendo comunicarse a través de un cable serie (que en este caso se emula). Sin embargo, las aplicaciones no saben acerca de procedimientos de Bluetooth para la creación de cables serie emulados, es por eso que necesitan ayuda de algún tipo de aplicación de ayuda Bluetooth - consciente en ambos lados. (Estas cuestiones no se abordan de manera explícita en este perfil, la principal preocupación en este caso es para la interoperabilidad de Bluetooth.) De igual modo, sin embargo, las aplicaciones no heredadas desean llevar a cabo las comunicaciones en serie a través de Bluetooth también deben cumplir con el comportamiento especificado en este perfil.

8.3 Near Field Communication

8.3.1 Introducción al NFC

Near Field Communication, NFC, es una tecnología emergente basada en otra llamada *Radio Frequency Identification* (RFID). Se espera que la tecnología NFC experimente un gran desarrollo e implantación durante los próximos años aunque, de un tiempo a esta parte, se vienen desarrollando pruebas de campo empleando esta tecnología. Por ejemplo, durante los Juegos Olímpicos de Londres 2012 se desplegó toda una infraestructura de pago móvil vía NFC en la que participaron empresas como VISA y Samsung. Actualmente, el desarrollo de NFC está siendo dirigido por el NFC Forum, una organización compuesta por 150 empresas que trabajando juntas y aunando esfuerzos tratan de impulsar y desarrollar esta tecnología de comunicaciones de campo cercano.

Como fuente de información para la realización del presente anexo y de esta manera adquirir los conocimientos previos necesarios, se ha acudido a la literatura tecnológica [20, 21].

8.3.2 Especificaciones técnicas de NFC

A continuación se va a realizar un resumen de las características técnicas de la tecnología NFC.

NFC opera dentro de la banda ISM (*Industrial, Scientific and Medical*) de radio frecuencia de 13,56 MHz disponible globalmente sin restricción y sin necesidad de licencia para su uso, con un ancho de banda de casi 2 MHz.

Es una tecnología de plataforma abierta estandarizada en la ISO/IEC 18092 y la ECMA-340. Estos estándares especifican los esquemas de modulación, codificación, velocidades de transferencia y formato de la trama de la interfaz RF de dispositivos NFC, así como los esquemas de inicialización y condiciones requeridas para el control de colisión de datos durante la inicialización para ambos modos de comunicación, activo y pasivo. También definen el protocolo de transporte, incluyendo los métodos de activación de protocolo y de intercambio de datos.

La distancia de trabajo con antenas compactas estándar es aproximadamente 10 cm, aunque generalmente es efectivo cercano a los 5 cm. Las velocidades de transmisión que soporta esta tecnología son de 106, 212, 424 u 848 kbits/s.

La comunicación NFC es bidireccional, por lo tanto los dispositivos NFC son capaces de transmitir y recibir datos al mismo tiempo.

8.3.3 Modos de funcionamiento

Los modos de funcionamiento de la tecnología NFC son activo y pasivo por lo que no se va a entrar en detalle en cada uno de ellos. Ahora bien, lo que sí es interesante y novedoso es que un dispositivo NFC, dispone de la habilidad de funcionar en ambos modos lo cual hace que sean únicos dentro de otras tecnologías de comunicación sin contacto. Esto posibilita a los dispositivos a actuar como tarjetas sin contacto o como lectores. Por tanto, un teléfono móvil habilitado con NFC puede ser usado por ejemplo, para enviar información de pago a un lector y realizar una compra o para leer información de una valla o poster publicitario con una etiqueta adherida.

8.3.4 Establecimiento de la conexión

La conexión NFC se produce en 5 etapas:

- **Descubrimiento:** En esta fase los dispositivos inician la etapa de rastrearse el uno al otro y posteriormente su reconocimiento.
- **Autenticación:** En esta parte los dispositivos verifican si el otro dispositivo está autorizado o si deben establecer algún tipo de cifrado para la comunicación.
- **Negociación:** En esta parte del establecimiento, los dispositivos definen parámetros como la velocidad de transmisión, la identificación del dispositivo, el tipo de aplicación, sus características y, si es el caso, también definen la acción a ser solicitada.
- **Transferencia:** Una vez negociados los parámetros para la comunicación, se puede decir que ya se ha realizado exitosamente pudiéndose pasar ya a realizar el intercambio de datos.
- **Confirmación:** El dispositivo receptor confirma el establecimiento de la comunicación y la transferencia de datos.

La tecnología NFC no está destinada para la transferencia masiva de datos, pero se puede utilizar para la configuración de otras tecnologías inalámbricas de mayor ancho de banda como *Bluetooth*, *WiFi* o *WiFi Direct* con la ventaja de que si se utiliza NFC el tiempo de establecimiento de la comunicación es muy inferior que si se utilizaran estas otras tecnologías por sí solas para efectuar el enlace.

8.3.5 Arquitectura NFC y modos de funcionamiento

La tecnología NFC es muy flexible, adaptable y eficiente debido a que puede trabajar en tres diferentes configuraciones lo cual le hace única entre las tecnologías de comunicaciones inalámbricas. En la figura 27 se resume la arquitectura NFC diferenciando cada una de las tres configuraciones en las que puede trabajar.

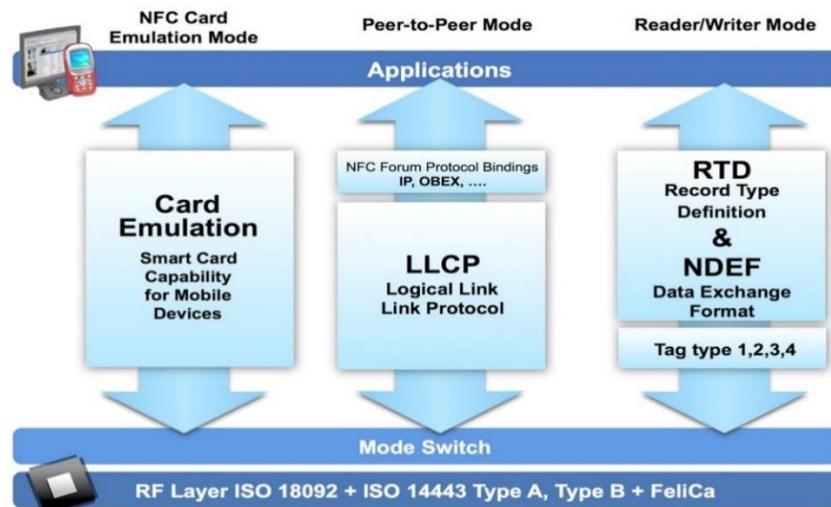


Figura 28: Arquitectura NFC. Modos de operación

- **Modo Emulación de Tarjeta Inteligente:** Este modo permite que un dispositivo móvil con NFC pueda actuar emulando a una tarjeta sin contacto. Para usar este modo, el dispositivo NFC que pretenda actuar de emulador tendrá que contar con un elemento seguro donde poder almacenar una o más tarjetas de este tipo. Este modo de

Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad

Samuel Longares Losilla - Eduardo Prado Clemente

funcionamiento permite, por ejemplo, realizar pagos de todo tipo con el móvil, almacenando en dicho elemento seguro nuestras tarjetas de crédito.

- **Modo de Comunicación Peer-to-Peer (P2P):** Se emplea para el intercambio de datos o establecimiento de las comunicaciones entre dispositivos NFC. Cuando la cantidad de datos intercambiada es relativamente pequeña (hasta unos pocos kilobytes) se usa el mismo protocolo NFC. Para la transmisión de cantidades mayores de información, como se ha comentado anteriormente, NFC es utilizado para establecer los parámetros de una conexión inalámbrica más avanzada como puede ser Bluetooth o WiFi.
- **Modo Lectura/Escritura:** Este modo proporciona la habilidad de leer y escribir etiquetas RFID pasivas empleando un dispositivo NFC. Un ejemplo de utilidad de este modo es el de un poster inteligente en el cual si alguien quisiera conocer más información sobre él no tendría más que aproximar su dispositivo móvil a él.

En la figura 28 se resume cada uno de estos modos de funcionamiento. Cabe destacar que en dicha figura, para el modo emulación de tarjeta inteligente, el elemento seguro aparece como UICC (tarjeta SIM).

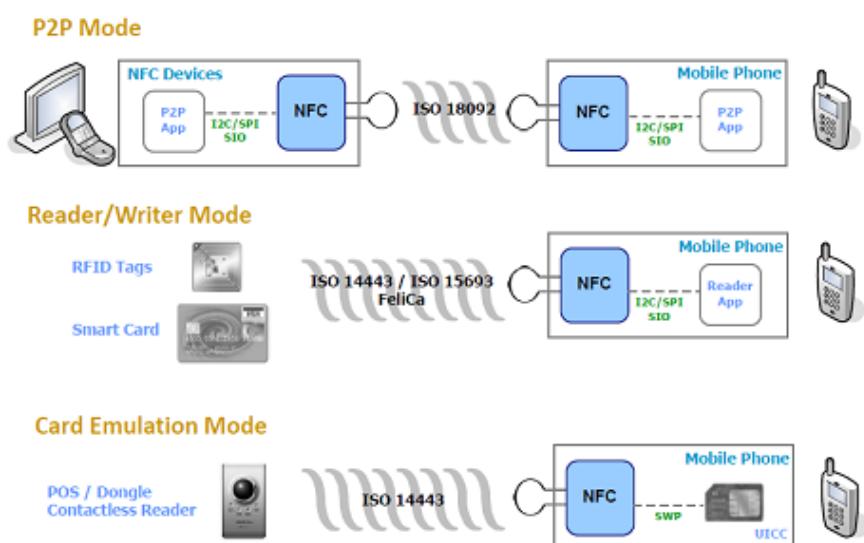


Figura 29: Modos de operación. Detalles

8.4 .NET Framework

.NET Framework es una tecnología que soporta la construcción y ejecución de aplicaciones y servicios Web XML. .NET Framework está diseñado para cumplir los siguientes objetivos:

- Proporcionar un entorno de programación orientado a objetos consistente donde el código se almacena y ejecuta de forma local, pero distribuido mediante internet o remotamente.
- Proporcionar un entorno de ejecución de código que reduzca al mínimo el despliegue del software y conflictos de versiones.
- Proporcionar un entorno de ejecución de código que promueva la ejecución segura de código, incluyendo el código creado por terceros.
- Proporcionar un entorno de ejecución de código que elimine los problemas de rendimiento de los entornos de secuencias de comandos o interpretados.

- Hacer la experiencia del desarrollador consistente a través de diversos tipos de aplicaciones, como las aplicaciones basadas en Windows y aplicaciones basadas en Web.
- Construir todas las comunicaciones siguiendo los estándares para asegurar que el código basado en .NET Framework se puede integrar con cualquier otro código.

8.5 MySQL

MySQL [22,23] es un sistema de gestión de datos relacional, licenciado bajo la GPL de la GNU. Su diseño multihilo le permite soportar una gran carga de forma muy eficiente. MySQL fue creada por la empresa sueca MySQL AB, mantiene el copyright del código fuente del servidor SQL, así como también de la marca. Aunque MySQL es software libre, MySQL AB distribuye una versión comercial de MySQL, que no se diferencia de la versión libre más que en el soporte técnico que se ofrece, y la posibilidad de integrar este gestor en un software propietario, ya que de no ser así, se vulneraría la licencia GPL. Este gestor de bases de datos es, probablemente, el gestor más usado en el mundo del software libre, debido a su gran rapidez y facilidad de uso. Esta gran aceptación es debida, en parte a que existen infinidad de bibliotecas y otras herramientas que permiten su uso a través de gran cantidad de lenguajes de programación, además de su fácil instalación y configuración.

Las principales características de este gestor de bases de datos son las siguientes:

- Aprovecha la potencia de sistemas multiprocesador gracias a su implementación multihilo.
- Soporta gran cantidad de tipos de datos para las columnas.
- Dispone de APIs en gran cantidad de lenguajes.
- Gran portabilidad entre sistemas.
- Soporta hasta 32 índices por tabla.
- Gestión de usuarios y passwords, manteniendo un muy buen nivel de seguridad en los datos.

8.5.1 Relaciones SQL

- **Clave primaria (PK):** Una clave primaria (*Primary key*) es un identificador único en una entidad y, por tanto, identificará inequívocamente a una instancia o elemento dentro de ella.
- **Clave foránea (FK):** Una clave foránea (*Foreign key*) establece una relación entre dos entidades, identificando una instancia de una entidad referida a una instancia de otra entidad. Más concretamente, puesto que las entidades disponen de campos que establecen sus propiedades, identifica a uno o varios campos (claves primarias) de una instancia de una entidad denominada referido y los relaciona con uno o más campos de una instancia de otra entidad denominada referenciada.

En la implementación de la base de datos relacional para la plataforma de gestión de cuidados de enfermería, ambos tipos de claves han sido usadas, así como varios tipos de relaciones. A continuación van a ser analizadas de forma breve, los tipos de relaciones que aparecen en esta base de datos mediante un ejemplo de cada una de ellas.

8.5.1.1 Relación 1:1

Este tipo de relación, asocia una sola instancia de una entidad con una sola instancia de otra entidad. Por ejemplo, un profesional sanitario sólo tendrá una tarjeta NFC asociada. Por lo tanto resulta bastante intuitivo saber qué tipo de relación se necesita para cada caso concreto y basta con analizar sus dependencias.

Además, para establecer esta relación, es necesario emplear las claves (primaria y foránea) comentadas anteriormente. Las claves primarias son sus identificadores en la tabla. El identificador del profesional sanitario será a su vez clave primaria en su propia tabla y clave foránea en la tabla de tarjetas. De este modo se asocia la tarjeta al identificador de un profesional.

8.5.1.2 Relación 1:N

Este tipo de relación ofrece la posibilidad de poder asociar una instancia de una entidad con una o más instancias de otra entidad. Por ejemplo un residente podrá tener más de una medida asociada, como es lógico.

Para establecer esta relación por medio de sus claves, se utilizarán sus claves primaria y foránea. En este caso será el identificador del residente el que actuará como clave foránea en las medidas que tenga asociadas. De este modo un mismo residente puede ser asociado a más de una medida.

8.5.1.3 Relación N:M

Este tipo de relación es básica para la plataforma puesto que, un residente puede tener varias personas de contacto asociadas a su perfil, pero a su vez una persona de contacto puede ser a su vez contacto de varios residentes. Por tanto la solución a esto pasa por establecer relaciones N:M.

Para establecer una relación de este tipo en el entorno de desarrollo de bases de datos que se está empleando (*MySQL Workbench*) hay que hacerlo en dos pasos. Primero, hay que crear un entidad intermedia que contenga las claves foráneas de las entidades entre las cuales se desea establecer una relación N:M y, posteriormente, configurar una relación 1:N entre dicha entidad y cada una de las anteriores.

8.6 SQLite

8.6.1 Introducción

SQLite es un proyecto de dominio público creado por D. Richard Hipp que implementa una pequeña librería de aproximadamente 500Kb programada en lenguaje C, que funciona como un sistema de gestión de base de datos relacionales .A diferencia de los motores de base de datos convencionales con la arquitectura cliente-servidor, SQLite es independiente, ya que no se comunica con un motor de base de datos, sino que las librerías de SQLite pasan a integrar la aplicación .La misma utiliza las funcionalidades de SQLite a través de llamadas simples a sub rutinas y funciones. Esto reduce la latencia en el acceso a la base de datos, debido a que las llamadas a funciones son más eficientes que la comunicación entre procesos. El conjunto de la base de datos (definiciones, tablas, índices, y los propios datos), son guardados como un solo fichero estándar, en la máquina local.

8.6.2 Características

Abajo están presentadas varias ventajas de SQLite [24]:

- Tamaño: SQLite tiene una pequeña memoria y una única biblioteca es necesaria para acceder a bases de datos, lo que lo hace ideal para aplicaciones de bases de datos incorporadas
- Rendimiento de base de datos: SQLite realiza operaciones de manera eficiente y es más rápido que MySQL y PostgreSQL
- Portabilidad: SQLite se ejecuta en muchas plataformas y sus bases de datos pueden ser fácilmente portadas sin ninguna configuración o administración
- Estabilidad: SQLite es compatible con ACID, reunión de los cuatro criterios de Atomicidad, Consistencia, Aislamiento y Durabilidad
- SQL: SQLite implementa un gran sub-conjunto de la ANSI - 92 SQL estándar, incluyendo sub-consultas, generación de usuarios, vistas y triggers
- Interfaces: SQLite cuenta con diferentes interfaces del API, las cuales permiten trabajar con C++, PHP, Perl, Python, Tcl, groovy, etc.
- Precio: SQLite es de dominio público, y por tanto, es libre de utilizar para cualquier propósito sin coste y se puede redistribuir libremente.

9 Anexo 3: Seguridad

9.1 Secure Socket Layer

El objetivo principal del protocolo SSL es proporcionar privacidad y fiabilidad entre dos aplicaciones que se comunican. El protocolo está compuesto de dos capas. El nivel más bajo el cual está por encima de algún protocolo de comunicaciones fiable (ej. TCP [RFC0793]) es el registro de SSL. El protocolo de registro de SSL se utiliza para la encapsulación de diferentes protocolos de nivel superior. Permite que el servidor y el cliente autenticarse y negociar los algoritmos de encriptación y las claves criptográficas antes de empezar a transmitir datos. Una de las ventajas de SSL es que es de aplicación independiente al protocolo. Un protocolo de nivel más alto puede utilizar capas superiores de forma transparente.

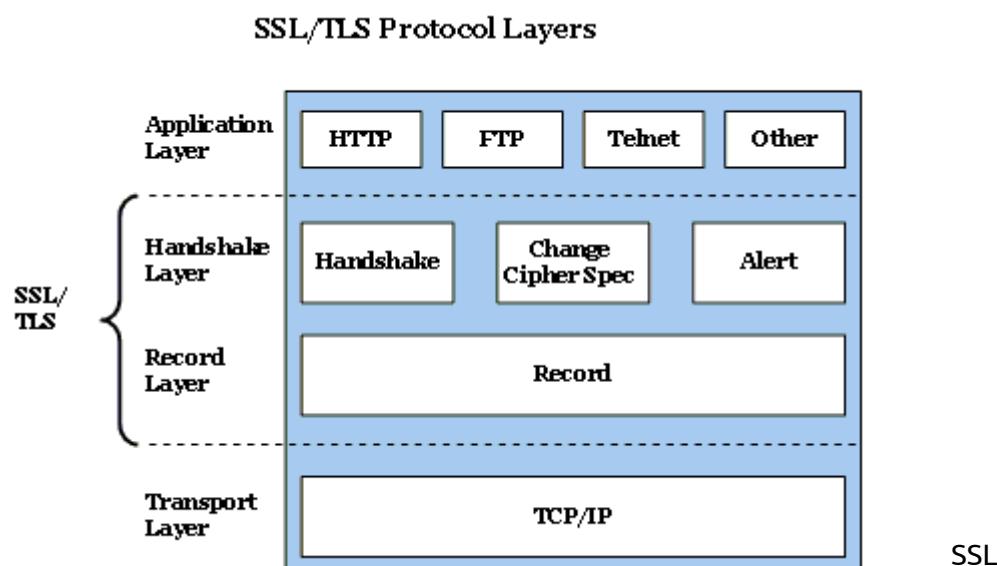


Figura 30: Capas del protocolo SSL

proporciona numerosos beneficios a clientes y servidores, incluyendo:

- **Fuerte autenticación, privacidad del mensaje y la integridad.** La característica principal de SSL es la capacidad de asegurar los datos transmitidos mediante el cifrado. SSL también ofrece autenticación de servidor y, opcionalmente, autenticación de cliente para probar la identidad de las partes que participan en la comunicación segura. También proporciona integridad de datos a través de un valor de comprobación de integridad. Además de proteger contra la divulgación de datos a través del cifrado, el protocolo de seguridad SSL / TLS se puede utilizar para proteger contra ataques de disfraces, los ataques de la brigada man-in- the-middle o un cubo, ataques de rollback, y ataques de repetición.
- **Interoperabilidad.** SSL / TLS funciona con la mayoría de los navegadores Web, como Microsoft Internet Explorer y Netscape Navigator, y en la mayoría de los sistemas operativos y servidores Web, incluyendo el sistema operativo Microsoft ® Windows, UNIX, Novell, Apache (versión 1.3 y posteriores), Netscape Enterprise Server y Sun Solaris. Además, a menudo integrado en los lectores de noticias, servidores LDAP, y una variedad de otras aplicaciones.

- **Flexibilidad del algoritmo.** SSL / TLS proporciona opciones para los mecanismos de autenticación, los algoritmos de cifrado y algoritmos de hash que se utilizarán durante la sesión segura.
- **Facilidad de despliegue.** SSL se utiliza de forma transparente por muchas aplicaciones en Windows Server 2003. Utilizar SSL para la exploración segura cuando se utiliza Internet Explorer e Internet Information Services (IIS) es tan fácil como seleccionar una casilla de verificación.
- **Facilidad de uso.** Debido a SSL se implementa debajo de la capa de aplicación, la mayor parte de sus operaciones son completamente invisible para el cliente. Esto permite que el cliente tenga poco o ningún conocimiento de las comunicaciones seguras y aun así estar protegido contra los atacantes

El protocolo Secure Sockets Layer (SSL) utiliza una combinación de cifrado de clave pública y la clave simétrica. El cifrado de claves simétricas es mucho más rápido que el cifrado de clave pública. Sin embargo, el cifrado de claves públicas proporciona mejores técnicas de autenticación. Una sesión de SSL siempre comienza con un intercambio de mensajes denominado Protocolo de enlace SSL. El protocolo de enlace permite al servidor autenticar al cliente mediante el uso de técnicas de clave pública y, a continuación, permite que el cliente y el servidor cooperen en la creación de claves simétricas utilizadas para cifrado rápido, descifrado y detección de manipulaciones durante la siguiente sesión. Opcionalmente, el protocolo de enlace también permite que el cliente se autenticarse en el servidor.

Los pasos implicados en el protocolo de enlace SSL son los siguientes (tenga en cuenta que los pasos siguientes suponen el uso de los conjuntos de cifrado enumerados en los conjuntos cifrados con intercambio de claves de RSA: Triple DES, RC4, RC2, DES):

1. El cliente envía al servidor, el número de versión del cliente SSL, configuración de cifrado, los datos específicos de la sesión y otra información que el servidor debe comunicarse con el cliente mediante SSL.
2. El servidor envía al cliente el número de versión del servidor SSL, configuración de cifrado, los datos específicos de la sesión y otra información que el cliente debe comunicarse con el servidor a través de SSL. El servidor envía también su propio certificado y si el cliente solicita un recurso del servidor que requiere autenticación de cliente, el servidor solicita el certificado del cliente.
3. El cliente utiliza la información enviada por el servidor para autenticar el servidor (consulte la autenticación del servidor para obtener más detalles). No se puede autenticar el servidor, el usuario se advierte del problema e informó que no se puede establecer una conexión cifrada y autenticada. Si el servidor se puede autenticar correctamente, el cliente continúa con el paso 4.
4. Con todos los datos generados en el protocolo de enlace hasta el momento, el cliente (con la cooperación del servidor, dependiendo de la clave que se utiliza) crea el pre-master secreto para la sesión, cifra con la clave del servidor público (obtenida el certificado del servidor, enviado en el paso 2) y, a continuación, envía el pre-master secreto cifrado al servidor.
5. Si el servidor solicitó autenticación del cliente (es decir, un paso opcional en el protocolo de enlace), el cliente firma también otro bloque de datos que es único para este protocolo de enlace y conocidos por el cliente y el servidor. En este caso, el cliente envía los datos firmados y el certificado del cliente al servidor junto con el pre-master secreto cifrado.

6. Si el servidor solicitó autenticación del cliente, el servidor intenta autenticar el cliente (Véase autenticación de cliente para obtener más detalles).
7. El cliente y el servidor utilizan el master secreto principal para generar las claves de sesión, que son claves simétricas que se utilizan para cifrar y descifrar la información que se intercambia durante la sesión SSL y para comprobar su integridad (es decir, para detectar los cambios en los datos entre el momento en que se envió y el tiempo se recibe sobre la conexión SSL).
8. El cliente envía un mensaje al servidor para informar de que los mensajes futuros del cliente serán cifrados con la clave de sesión.
9. El servidor envía un mensaje al cliente para informar de que los futuros mensajes desde el servidor serán cifrados con la clave de sesión.
10. El protocolo de enlace SSL ahora está completo y se inicia la sesión.
11. Esta es la condición de operación normal del canal seguro.

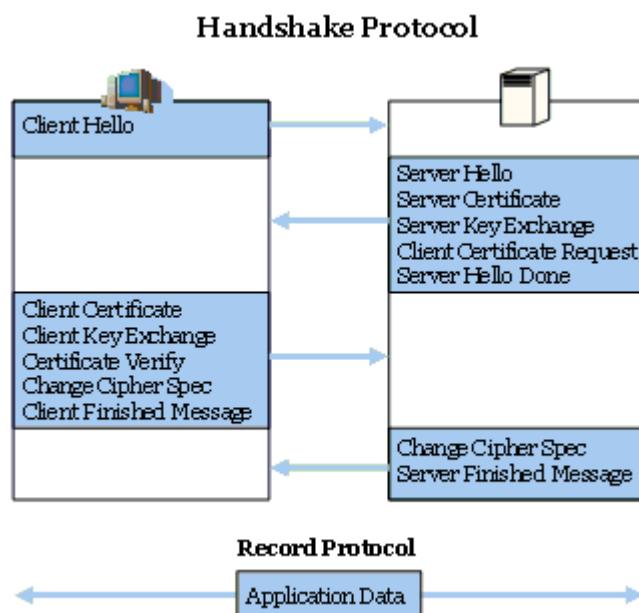


Figura 31: Protocolo de establecimiento de la conexión segura

9.2 Advanced Encryption Standard

Este estándar especifica el algoritmo Rijndael, un sistema de cifrado simétrico de bloques que puede procesar los bloques de datos de 128 bits, utilizando claves de cifrado con longitudes de 128, 192 y 256 bits. Rijndael fue diseñado para manejar tamaños de bloque de alimentación y longitudes de clave, sin embargo, no se adoptan en esta norma.

La entrada y la salida para el algoritmo AES consisten cada una de las secuencias de 128 bits (dígitos con valores de 0 o 1). Estas secuencias a veces se conocen como bloques y el número de bits que contienen se conocen como su longitud. La clave de cifrado para el algoritmo AES es una secuencia de 128, 192 o 256 bits. Otro de entrada, salida y longitudes de clave de cifrado no están permitidos por esta norma.

Se numerarán Los bits dentro de tales secuencias se comienza en cero y terminando en uno menos que la longitud de la secuencia (longitud de bloque o *Solución tecnológica de e-Salud para toma de medidas y gestión de usuarios en centros de día y residencias de la tercera edad*

longitud de la clave). El número i apagado a algo que se conoce como su índice y estará en uno de los rangos de $0 \leq i < 128$, $0 \leq i < 192$ o $0 \leq i < 256$ dependiendo de la longitud del bloque y la longitud de la clave (especificado arriba).

La unidad básica para su procesamiento en el algoritmo AES es un byte, una secuencia de ocho bits tratados como una sola entidad. La entrada, la salida y la Clave de Cifrado se procesan como matrices de bytes que se forman dividiendo estas secuencias en grupos de ocho bits contiguos para formar matrices de bytes. Para una entrada, de salida o Clave de Cifrado denotado por a , los bytes de la matriz resultante se hará referencia utilizando uno de las dos formas, a_n o $a[n]$, donde n va a estar en uno de los siguientes rangos:

Longitud de la clave = 128 bits, $0 \leq n < 16$ Longitud del bloque = 128 bits, $0 \leq n < 16$

Longitud de la clave = 192 bits, $0 \leq n < 24$

Longitud de la clave = 256 bits, $0 \leq n < 32$

9.2.1 Especificaciones

- El estado

A nivel interno, las operaciones de la AES algoritmo se realizan en una matriz bidimensional de bytes llamado **estado**. El Estado está formado por cuatro filas de bytes, cada uno con N_b bytes, donde N_b es la longitud del bloque dividido por 32. En el conjunto del estado es representado por el símbolo S , cada byte individual tiene dos índices, su número de fila r en el rango $0 \leq r < 4$ y su número de la columna c en el rango $0 \leq c < N_b$. Esto permite referirse a un byte individual del estado como sea $S_{r,c}$ o $S[r, c]$. Por esta norma, $N_b = 4$, es decir, $0 \leq c < 4$.

Al inicio del cifrado y el cifrado inverso se describe, la entrada - la matriz de bytes $in_0, in_1, \dots, in_{15}$ - se copia en la matriz de estado, como se ilustra en la figura 31. Las operaciones de cifrado y su inversa se llevan a cabo en este conjunto del estado, después de lo cual su valor final se copia a la salida - la matriz de bytes $out_0, out_1, \dots, out_{15}$.

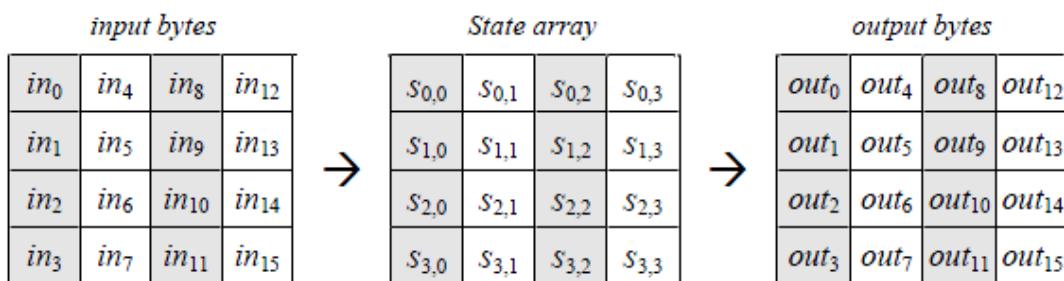


Figura 32: Diagrama de bloques de estado del cifrado AES

- Algoritmo

Para el algoritmo AES, la longitud del bloque de entrada, el bloque de salida y el estado es de 128 bits. Esto está representado por $N_b = 4$, lo que refleja el número de palabras de 32 bits (número de columnas) en el estado.

Para el algoritmo AES, la longitud de la clave de cifrado, K , es 128, 192, o 256 bits. La longitud de la clave está representado por $N_k = 4, 6, \text{ o } 8$, que refleja el número de palabras de 32 bits (número de columnas) en la clave de cifrado.

Para el algoritmo AES, el número de rondas a realizar durante la ejecución del algoritmo depende en el tamaño de clave. El número de rondas está representado por N_r , en donde $N_r = 10$ cuando $N_k = 4$, $N_r = 12$ cuando $N_k = 6$, y $N_r = 14$ cuando $N_k = 8$.

Las únicas combinaciones de *longitud de clave-bloque-número de rondas* que se ajustan a esta norma se dan en la figura 32.

	Key Length (N_k words)	Block Size (N_b words)	Number of Rounds (N_r)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Figura 33: Combinaciones posibles de los parámetros del cifrado AES

Al inicio del cifrado la entrada se copia en el conjunto de estado. Despues de la adición inicial de la clave circular, el conjunto del estado se transforma mediante la implementación de una operación circular 10, 12 o 14 veces (dependiendo de la longitud de la clave), con la clave final que difieren ligeramente de las primeros $N_r - 1$ rondas. El estado final se copia a la salida.

La función circular se parametriza mediante una clave que consiste en una matriz de una dimensión de las palabras de cuatro bytes que se obtienen al aplicar la rutina de ampliación de claves.

El cifrado se describe en el pseudo-código en la figura 33. Las transformaciones individuales SubBytes(), ShiftRows(), MixColumns(), y AddRoundKey().

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
    byte state[4,Nb]

    state = in

    AddRoundKey(state, w[0, Nb-1])

    for round = 1 step 1 to Nr-1
        SubBytes(state)
        ShiftRows(state)
        MixColumns(state)
        AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
    end for

    SubBytes(state)
    ShiftRows(state)
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

    out = state
end
```

Figura 34: Pseudo-código del algoritmo de cifrado AES

10 Anexo 4: Diseño de la interfaz de usuario e informes de ejemplo

10.1 Aplicación Android



Figura 35: Layout de entrada mediante tarjeta NFC



Figura 36: Layout de entrada manual

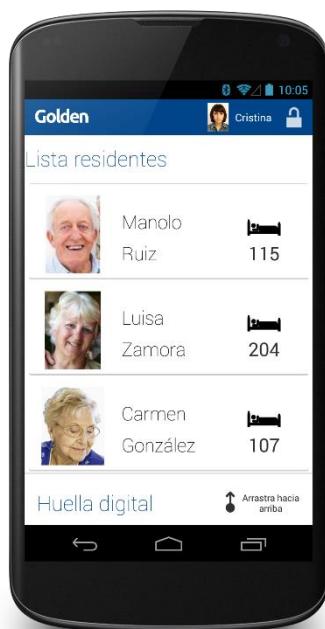


Figura 37: Layout de selección de residente



Figura 38: Layout de espera de conexión de dispositivo médico



Figura 39: Layout de adquisición de la medida

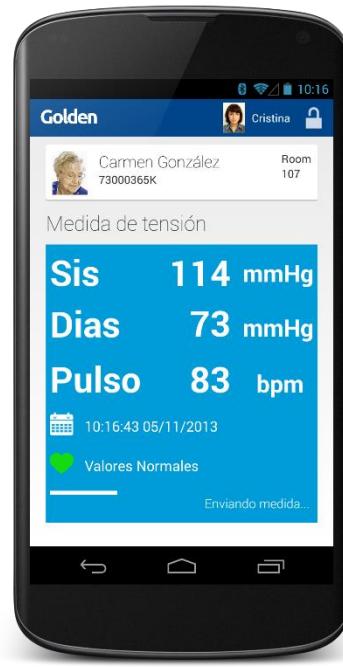


Figura 40: Layout medida adquirida

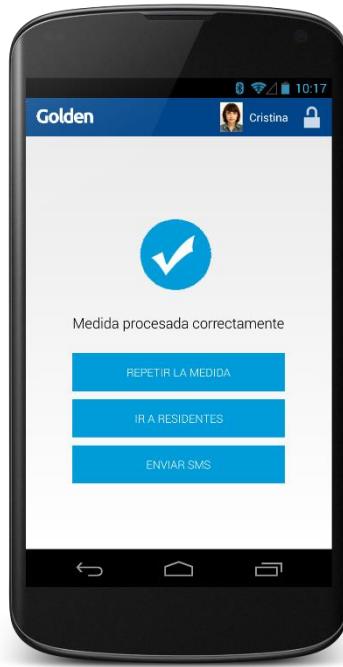


Figura 41: Layout medida enviada



Figura 42: Layout envío de sms

10.2 Aplicación de gestión

Gestión de usuarios

Hola Sandra

Bienvenido a tu panel de control. Desde aquí podrás gestionar todos los usuarios de tu residencia.

Cerrar sesión 

Mostrar históricos Mostrar grupos Filtrar:

DNI	Nombre	Apellidos	Piso	Habitación	Cama
67248867H	Manuel	Aliende Gacón	1	121	1
75085328B	Carlos	Bermudez Valiente	3	308	1
53182137L	Pedro	Bueno Lavina	1	102	1
55106811F	Salvador	Chueca Puga	1	101	2
47737028E	Pedro	Dumas Boquerizo	3	322	1
17448138Q	Jorge	Gómez Losilla	4	412	2
76913506B	Rosario	Gómez Plaños	1	104	1
66731860M	Carlos Alberto	Julién Hernan	3	111	2
11788200X	Jose Luis	Laguna Lainez	3	310	2
28603242M	Alicia	López Córcoles	1	105	1
63589673D	Laura	López López	2	232	1
11111111H	Marisa	Martínez Bernabé	2	201	2
47042229F	Olga	Martínez Chueca	1	121	2
76548209T	Rogelio	Motos Revilla	4	412	2
27610987Q	Vicente	Muñoz Moreno	4	415	2
66500174K	Martina	Ochoa González	4	406	1
52245545X	Julio	Pignatelli Bernardo	1	121	2
47928803T	Daniel	Romeo Lema	1	106	1
70939288T	Laura	Ruesga Pérez	1	501	1
22222222J	Manolo	Ruiz López	1	101	1

ACTUALIZAR VER FICHA DAR DE BAJA AÑADIR RESIDENTE



Carlos Bermudez...
DNI: 75085328B
Habitación: 308

Figura 43: Formulario principal pestaña de residentes

Gestión de usuarios

Hola Sandra

Bienvenido a tu panel de control. Desde aquí podrás gestionar todos los usuarios de tu residencia.

Cerrar sesión 

Mostrar históricos Mostrar grupos Filtrar:

DNI	Nombre	Apellidos	Teléfono	Email	Tipo	Tarjeta
11003007Z	David	Blanco Soler	621334411	davidblis@hotmail.com	Enfermero	goodday3
07749093W	Carmela	Fermín Gordillo	686668426	eduprado88@gmail.com	Enfermero	gdform
56669273X	Teresa	Fernandez Trujillo	699887766	kkk@gmail.com	Enfermero	
73012367V	Prueba	Foto	666666666	javiapasc@gmail.com	Administrador	goodday2
88246590Y	Olga	Fuentes Fontana	600991122	oj@correo.com	Enfermero	Goodday Prue...
22222222J	Jose Luis	García García	675554445	mdefrancisco@goodday.es	Gerocultor	gdday 2
18168735T	Francisco	González García	685552200	fgonzalez@goodday.es	Administrador	
17751323S	Sergio	López Martín	656344343	beltransrg@gmail.com	Administrador	
89373050H	Benito	Martínez Cifuentes	666666666	lo@yahoo.es	Médico	
11111111H	Sandra	Odriozola Marco	675554445	admin@goodday.es	Administrador	vsfs
74461195Y	Maria del Mar	Velázquez	600000004	edtado@gmail.com	Administrador	goodday1

ACTUALIZAR VER FICHA DAR DE BAJA AÑADIR PERSONAL



David Blanco Soler
DNI: 11003007Z
Cargo: Enfermero

Figura 44: Formulario principal pestaña de personal sanitario

Gestión de usuarios

Hola Sandra

Residentes Personal sanitario Centros sanitarios Tarjetas Medidas

Bienvenido a tu panel de control. Desde aquí podrás gestionar todos los usuarios de tu residencia.

Cerrar sesión



Nombre	Tipo	Teléfono fijo	Teléfono móvil	Email	Tipo de vía	Dirección	C.P.	Población	Provincia
Actur Noreste	Hospital	976050505	666666666	acturnoreste@esalud.es	Avenida	Asunción	50012	Zaragoza	Zaragoza
Actur SurOeste	Centro de salud	976050505	666666666	actursur@esalud.es	Calle	Inventada	50013	Zaragoza	Zaragoza
Actur Sur	Centro de salud	976050505	666666666	actursur@esalud.es	Calle	Inventada	50013	Zaragoza	Zaragoza
Actur Noreste	Centro Sanitario	976976976	666666667	acturnoreste@esalud.es	Calle	Adolfo aznar	50013	Zaragoza	Zaragoza

ACTUALIZAR

VER FICHA

ELIMINAR CENTRO

AÑADIR CENTRO

Figura 45: Formulario principal pestaña de centros sanitarios

Gestión de usuarios

Hola Sandra

Residentes Personal sanitario Centros sanitarios Tarjetas Medidas

Bienvenido a tu panel de control. Desde aquí podrás gestionar todos los usuarios de tu residencia.

Cerrar sesión



Asignación de tarjetas

Recargar lista

DNI	Nombre	Apellido	Tarjeta Asignada
11003007Z	David	Blanco Soler	goodday3
07749093W	Carmela	Fernán Gordillo	gdform
50669273X	Teresa	Fernandez Trujillo	
73012367V	Prueba	Foto	goodday2
88246590Y	Olga	Fuentes Fontana	Goodday Prueba 1
2222222J	Jose Luis	García García	gdday 2
18168735T	Francisco	González García	
17751323S	Sergio	López Martín	
89373050H	Benito	Martínez Cifuentes	
11111111H	Sandra	Odrizola Marco	vfs
74461195Y	Maria del Mar	Velázquez	goodday1

Selecciona personal sanitario de la tabla y pulsa para desasignar una tarjeta

ASIGNAR

DESASIGNAR

Activación de tarjetas

Identificador único

Etiqueta personalizada

Tipo

Personal

AGREGAR

Selección una tarjeta

goodday3

BORRAR

Figura 46: Formulario principal pestaña de tarjetas

Gestión de usuarios

Hola Sandra

Bienvenido a tu panel de control. Desde aquí podrás gestionar todos los usuarios de tu residencia.

Cerrar sesión

Filtrar:

DNI	Nombre	Apellidos	Piso	Hab.	Cama	Fecha y hora	Tipo	Valor	Unidad	Gerocultor
75085328B	Carlos	Bermudez Valiente	3	308	1	07/01/2014 10:50:32	Pulso	70	pul/min	2222222J
75085328B	Carlos	Bermudez Valiente	3	308	1	07/01/2014 10:50:32	Saturación de oxígeno	97	%	2222222J
53182137L	Pedro	Bueno Lavina	1	102	1	07/01/2014 10:57:57	Pulso	70	ppm	2222222J
53182137L	Pedro	Bueno Lavina	1	102	1	07/01/2014 10:57:57	Saturación de oxígeno	98	%	2222222J
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 13:49:39	Glucosa	99	mg/dL	1111111H
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 13:39:58	Glucosa	85	mg/dL	3333333P
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 13:42:00	Glucosa	85	mg/dL	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	08/01/2014 13:45:36	Pulso	98	ppm	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	08/01/2014 13:45:36	Saturación de oxígeno	98	%	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	08/01/2014 14:05:30	Pulso	98	ppm	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	08/01/2014 14:05:30	Saturación de oxígeno	98	%	3333333P
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 14:13:38	Glucosa	99	mg/dL	1111111H
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 14:13:23	Pulso	95	ppm	3333333P
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 14:13:23	Saturación de oxígeno	95	%	3333333P
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 14:17:20	Glucosa	99	mg/dL	1111111H
75085328B	Carlos	Bermudez Valiente	3	308	1	08/01/2014 14:16:55	Glucosa	85	mg/dL	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	08/01/2014 14:21:57	Glucosa	100	mg/dL	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	08/01/2014 14:37:30	Glucosa	100	mg/dL	3333333P
75085328B	Carlos	Bermudez Valiente	3	308	1	09/01/2014 9:04:14	Glucosa	85	mg/dL	3333333P
53182137L	Pedro	Bueno Lavina	1	102	1	09/01/2014 9:11:41	Pulso	98	ppm	3333333P

Tipo:

Figura 47: Formulario principal pestaña de medidas

Residente

A través de este diálogo puedes añadir un nuevo residente. Por favor, rellena todos los campos y haz clic en el botón AÑADIR.



Información del residente

DNI	Nombre	Apellidos	Situación
<input type="text"/>	<input type="text"/>	<input type="text"/>	Habitación <input type="text"/> Piso <input type="text"/> Cama <input type="text"/>

Fecha de nacimiento

<input type="button" value="Dia"/>	<input type="button" value="Mes"/>	<input type="button" value="Año"/>	<input type="radio"/> Hombre <input type="radio"/> Mujer	Tipo <input type="text"/> Núm. <input type="text"/>
------------------------------------	------------------------------------	------------------------------------	--	---

Direcciones de contacto

Tipo de vía	Dirección	C.P.	Población	Provincia	País	<input type="button" value="Nuevo"/>

Personas de contacto

Nombre	Relación	Teléfono móvil	Teléfono fijo	Correo electrónico	<input type="button" value="Nuevo"/>

Figura 48: Formulario de nuevo residente

Ficha de residente

Información del residente

DNI	Nombre	Apellidos
11111111H	Marisa	Martínez Bernabé
Fecha de nacimiento	Sexo	
5 / 11 / 2013	Mujer	



Información sanitaria

Afilación (Tipo - Número)	Situación
SEGURIDAD SOCIAL - 1111111111111111AR	Habitación 201 Piso 2 Cama 2

Direcciones de contacto

Tipo de vía	Dirección	C.P.	Población	Provincia	País
calle	Condes de Aragón	Zaragoza	50000	Zaragoza	España

Personas de contacto

Nombre	Relación	Teléfono móvil	Teléfono fijo	Correo electrónico
Jesús	Hijo	666666666	976666666	jesus.hijo@mail.com

CANCELAR **EDITAR** **GENERAR INFORME**

Figura 49: Formulario de ficha de residente

Personal sanitario

A través de este diálogo puedes añadir personal sanitario. Por favor, rellena todos los campos y haz clic en el botón AÑADIR.



DNI

Nombre

Teléfono móvil

Fecha de nacimiento
 Día Mes Año

Tipo

Apellido

Correo electrónico

Sexo
 Hombre Mujer

CANCELAR **AÑADIR**

Figura 50: Formulario de nuevo personal sanitario

Personal sanitario

A través de este diálogo puedes editar tu personal sanitario. Por favor, rellena todos los campos y haz clic en el botón EDITAR.


Editar foto

DNI <input type="text" value="11003007Z"/>	Tipo <input type="text" value="Enfermero"/>
Nombre <input type="text" value="David"/>	Apellido <input type="text" value="Blanco Soler"/>
Teléfono móvil <input type="text" value="621334411"/>	Correo electrónico <input type="text" value="davidbs@hotmail.com"/>
Fecha de nacimiento <input type="text" value="19"/> <input type="text" value="10"/> <input type="text" value="1920"/>	Sexo <input checked="" type="radio"/> Hombre <input type="radio"/> Mujer

CANCELAR EDITAR

Figura 51: Formulario de ficha de personal sanitario

Centro sanitario

A través de este diálogo puedes crear un nuevo centro sanitario. Por favor, rellena todos los campos y haz clic en el botón CREAR.

Centro	Contacto
Nombre <input type="text"/>	Tlf. fijo <input type="text"/>
Tipo <input type="text"/>	Tlf. móvil <input type="text"/>
	Email <input type="text"/>

Dirección

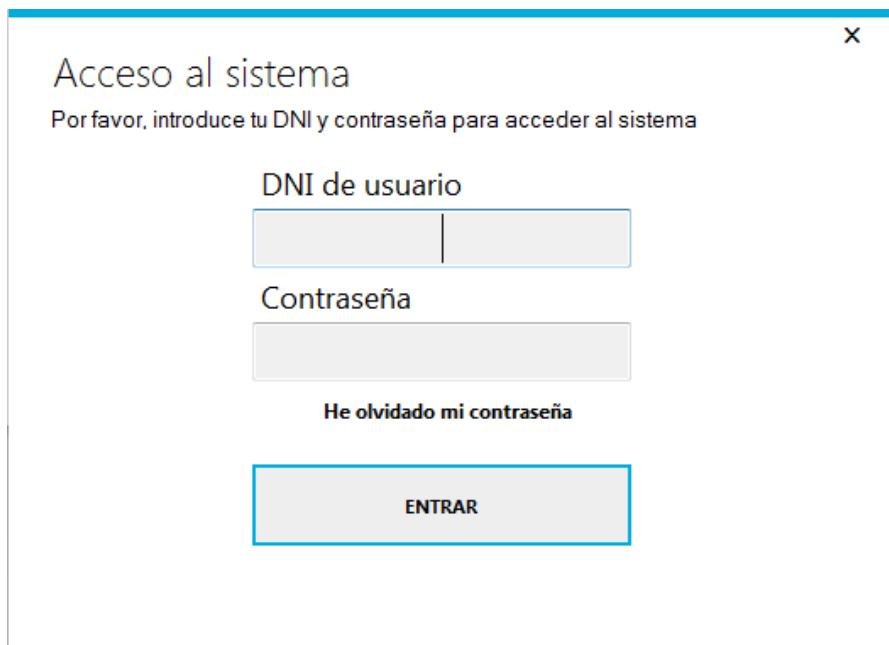
Tipo de vía <input type="text"/>	Dirección <input type="text"/>	C.P. <input type="text"/>	Población <input type="text"/>	Provincia <input type="text"/>	País <input type="text"/>
--	--	-------------------------------------	--	--	-------------------------------------

Personal de contacto

Nombre	Rol	Especialidad	Tlf. fijo	Tlf. móvil	Email
<input type="text"/>					
<input type="text"/>					
<input type="text"/>					
<input type="text"/>					

Nuevo CANCELAR CREAR

Figura 52: Formulario de nuevo centro sanitario



Acceso al sistema

Por favor, introduce tu DNI y contraseña para acceder al sistema

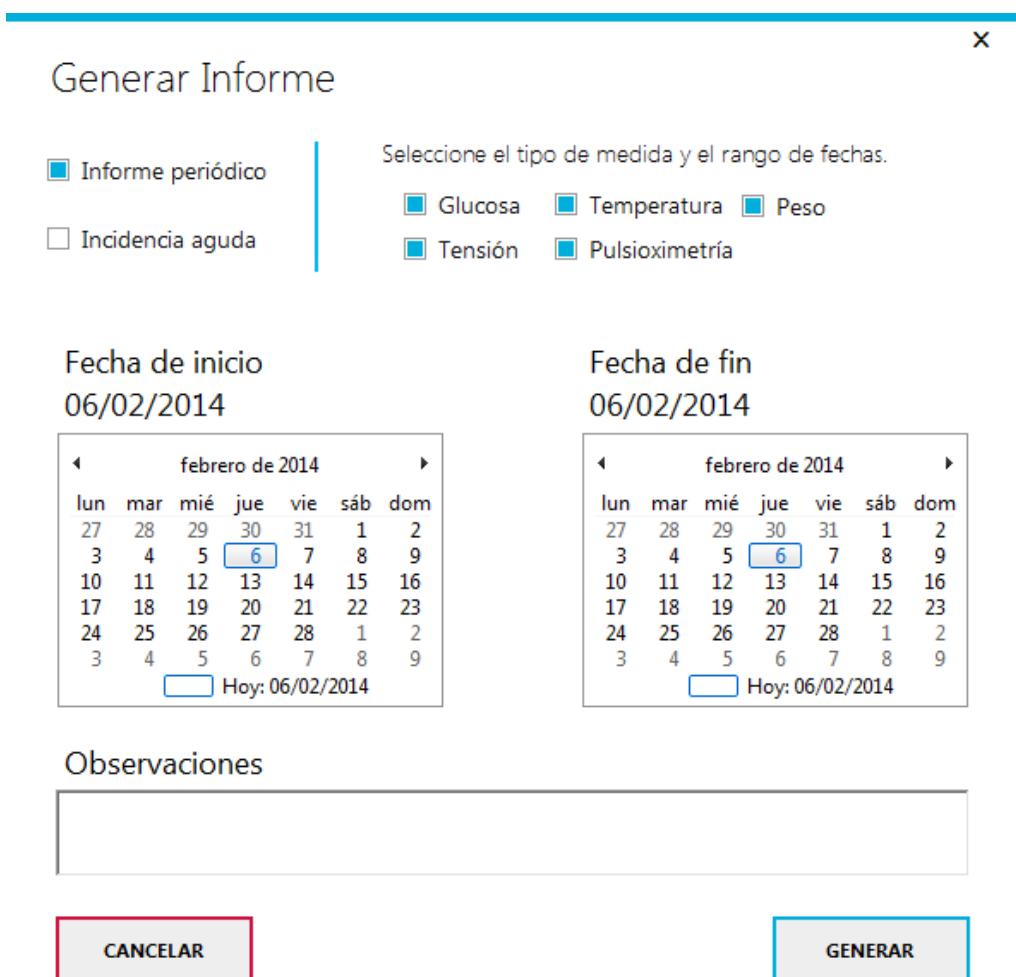
DNI de usuario

Contraseña

[He olvidado mi contraseña](#)

ENTRAR

Figura 53: Formulario de acceso a la aplicación de gestión



Informe periódico Incidencia aguda

Seleccione el tipo de medida y el rango de fechas.

Glucosa Temperatura Peso
 Tensión Pulsioximetría

Fecha de inicio
06/02/2014

febrero de 2014						
lun	mar	mié	jue	vie	sáb	dom
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

Hoy: 06/02/2014

Fecha de fin
06/02/2014

febrero de 2014						
lun	mar	mié	jue	vie	sáb	dom
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

Hoy: 06/02/2014

Observaciones

CANCELAR **GENERAR**

Figura 54: Formulario de generación de informes periódicos

X

Generar Informe

Informe periódico Incidencia aguda

Se generará un informe que incluirá todas las medidas realizadas en el día indicado.

Fecha de inicio
06/02/2014

lun	mar	mié	jue	vie	sáb	dom
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	1	2
3	4	5	6	7	8	9

Hoy: 06/02/2014

Observaciones

CANCELAR GENERAR

Figura 55: Formulario de generación de informes de incidencia aguda

10.3 Informes de ejemplo



D/DÑA Carlos Bermudez Valiente
 Control glucémico obtenido entre las fechas:
 viernes, 25 de enero de 2013 al martes, 21 de enero de 2014.
 Fecha de impresión: martes, 21 de enero de 2014

Fecha	Hora	Glucosa
16/12/2013	08:49:51	90 mg/dL
16/12/2013	08:54:44	99 mg/dL
16/12/2013	08:54:58	100 mg/dL
16/12/2013	10:18:10	85 mg/dL
19/12/2013	17:46:16	100 mg/dL
19/12/2013	18:43:30	258 mg/dL
28/12/2013	13:51:41	100 mg/dL
30/12/2013	11:21:05	200 mg/dL
08/01/2014	13:44:39	99 mg/dL
08/01/2014	13:39:58	85 mg/dL
08/01/2014	13:42:00	85 mg/dL
08/01/2014	14:13:38	99 mg/dL
08/01/2014	14:17:20	99 mg/dL
08/01/2014	14:16:55	85 mg/dL
09/01/2014	09:04:14	85 mg/dL
09/01/2014	09:33:38	99 mg/dL
09/01/2014	09:45:53	85 mg/dL
09/01/2014	10:10:21	90 mg/dL
09/01/2014	10:13:20	90 mg/dL
09/01/2014	10:16:43	90 mg/dL
09/01/2014	12:12:56	99 mg/dL
09/01/2014	12:21:45	99 mg/dL
09/01/2014	12:57:13	99 mg/dL
09/01/2014	12:54:50	85 mg/dL
09/01/2014	12:56:52	85 mg/dL
09/01/2014	12:58:44	85 mg/dL
09/01/2014	13:05:33	85 mg/dL
09/01/2014	13:12:43	99 mg/dL
09/01/2014	13:16:38	99 mg/dL
09/01/2014	13:37:26	85 mg/dL
09/01/2014	13:43:39	90 mg/dL
09/01/2014	13:52:22	95 mg/dL
09/01/2014	13:58:54	90 mg/dL
10/01/2014	09:06:26	90 mg/dL
10/01/2014	09:47:47	95 mg/dL
10/01/2014	10:03:19	120 mg/dL
10/01/2014	11:09:11	90 mg/dL

Figura 56: Ejemplo informe de glucometría



D/DÑA Carlos Bermudez Valiente

Control de tensión arterial obtenido entre las fechas:

viernes, 25 de enero de 2013 al martes, 21 de enero de 2014.

Fecha de impresión: martes, 21 de enero de 2014

Fecha	Hora	Sistólica	Diastólica	Pulso
16/12/2013	08:50:11	90 mmHg	90 mmHg	90 ppm
16/12/2013	08:55:27	128 mmHg	100 mmHg	100 ppm
16/12/2013	11:06:23	161 mmHg	96 mmHg	59 pul/min
30/12/2013	11:21:56	120 mmHg	70 mmHg	70 ppm
14/01/2014	10:36:47	90 mmHg	90 mmHg	90 ppm
16/01/2014	09:22:11	100 mmHg	100 mmHg	100 ppm

* Los valores marcados en rojo significan:

Presión sistólica: menor que 100 y mayor que 140.

Presión diastólica: menor que 60 y mayor que 90.

Observaciones:

Figura 57: Ejemplo informe de presión arterial



D/DÑA. Carlos Bermudez Valiente

Control de pulsioximetría obtenido entre las fechas:

viernes, 25 de enero de 2013 al martes, 21 de enero de 2014.

Fecha de impresión: martes, 21 de enero de 2014

Fecha	Hora	Pulso	SPO2
16/12/2013	08:51:09	98 ppm	98 %
16/12/2013	08:56:48	100 ppm	100 %
30/12/2013	11:23:33	90 ppm	98 %
07/01/2014	10:50:32	70 pul/min	97 %
08/01/2014	14:13:23	95 ppm	95 %
09/01/2014	10:22:58	98 ppm	98 %
09/01/2014	13:22:46	98 ppm	98 %
09/01/2014	14:04:19	95 ppm	95 %
16/01/2014	14:28:24	98 ppm	98 %
17/01/2014	12:09:00	98 ppm	98 %

* Los valores marcados en rojo significan: saturación de oxígeno en sangre menor que 90.

Observaciones:

Figura 58: Ejemplo informe de pulsioximetría



D/DÑA Carlos Bermudez Valiente

Control de peso obtenido entre las fechas:

viernes, 25 de enero de 2013 al martes, 21 de enero de 2014.

Fecha de impresión: martes, 21 de enero de 2014

Fecha	Hora	Peso
16/12/2013	08:50:51	100.2 kg
16/12/2013	08:56:04	100.5 kg
16/12/2013	08:56:22	90 kg
30/12/2013	11:22:32	120 kg
14/01/2014	12:54:24	68.4 kg
14/01/2014	13:18:13	68.3 kg
14/01/2014	13:25:07	68.4 kg
16/01/2014	09:12:24	90 kg
16/01/2014	09:19:16	100 kg
16/01/2014	12:47:34	95 kg

Observaciones:

Figura 59: Ejemplo informe de peso



D/DÑA Carlos Bermudez Valiente

Control de temperatura obtenido entre las fechas:

viernes, 25 de enero de 2013 al martes, 21 de enero de 2014.

Fecha de impresión: martes, 21 de enero de 2014

Fecha	Hora	Temperatura
16/12/2013	08:50:32	38 °C
16/12/2013	08:55:48	37.5 °C
16/12/2013	11:01:05	36.2 °C
16/12/2013	11:14:11	24.2 °C
16/12/2013	11:27:44	36.1 °C
19/12/2013	18:04:40	36.4 °C
30/12/2013	09:59:48	35.9 °C
30/12/2013	11:21:28	35 °C
10/01/2014	10:03:36	38 °C
14/01/2014	12:20:46	36.8 °C
14/01/2014	13:59:36	36.2 °C
14/01/2014	14:05:49	36.2 °C

* Los valores marcados en rojo significan: valor de temperatura menor que 35 y mayor que 37.

Observaciones:

Figura 60: Ejemplo informe de temperatura



D./DÑA Manolo Ruiz

Control glucémico obtenido del domingo, 01 de septiembre de 2013 al martes, 01 de octubre de 2013.

Fecha	Desayuno	Comida	Cena
01/09/2013	123 mg/dL	139 mg/dL	102 mg/dL
02/09/2013	102 mg/dL	143 mg/dL	126 mg/dL
03/09/2013	134 mg/dL	111 mg/dL	89 mg/dL
04/09/2013	123 mg/dL	146 mg/dL	131 mg/dL
05/09/2013	57 mg/dL	90 mg/dL	127 mg/dL
06/09/2013	157 mg/dL	113 mg/dL	135 mg/dL
07/09/2013	179 mg/dL	213 mg/dL	165 mg/dL
08/09/2013	132 mg/dL	122 mg/dL	126 mg/dL
09/09/2013	145 mg/dL	132 mg/dL	127 mg/dL
10/09/2013	134 mg/dL	112 mg/dL	119 mg/dL
11/09/2013	133 mg/dL	138 mg/dL	156 mg/dL
12/09/2013	131 mg/dL	103 mg/dL	94 mg/dL
13/09/2013	118 mg/dL	105 mg/dL	148 mg/dL
14/09/2013	117 mg/dL	125 mg/dL	121 mg/dL
15/09/2013	132 mg/dL	176 mg/dL	197 mg/dL
16/09/2013	164 mg/dL	143 mg/dL	156 mg/dL
17/09/2013	137 mg/dL	134 mg/dL	123 mg/dL
18/09/2013	117 mg/dL	117 mg/dL	141 mg/dL
19/09/2013	112 mg/dL	157 mg/dL	143 mg/dL
20/09/2013	140 mg/dL	130 mg/dL	127 mg/dL
21/09/2013	137 mg/dL	100 mg/dL	87 mg/dL
22/09/2013	52 mg/dL	70 mg/dL	99 mg/dL
23/09/2013	111 mg/dL	145 mg/dL	133 mg/dL
24/09/2013	125 mg/dL	124 mg/dL	114 mg/dL
25/09/2013	126 mg/dL	140 mg/dL	137 mg/dL
26/09/2013	155 mg/dL	142 mg/dL	130 mg/dL
27/09/2013	121 mg/dL	125 mg/dL	112 mg/dL
28/09/2013	123 mg/dL	143 mg/dL	134 mg/dL
29/09/2013	121 mg/dL	103 mg/dL	110 mg/dL
30/09/2013	122 mg/dL	147 mg/dL	178 mg/dL

Observaciones:

Los días señalados en rojo se ha precisado administración de Glucagón SBC

Figura 61: Ejemplo informe glucosa por franjas horarias

11 Anexo 5: Encuestas

11.1 Encuestas previas para personal de administración

Encuesta previa para la administración

Nombre: FLOR BANUE
 Edad: 46 años
 Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Actual sistema de gestión de residentes	Puntuación				
1. Facilidad para introducción de datos de un nuevo residente en el sistema de gestión.	1	2	3	4	5
2. Facilidad y rapidez a la hora de encontrar datos de un residente concreto en el sistema de gestión.	1	2	3	4	5
3. Importancia de la protección de los datos de los residentes.	1	2	3	4	5
4. Seguridad de protección de datos en el sistema de gestión.	1	2	3	4	5
5. Valoración general del sistema de gestión de residentes.	1	2	3	4	5

Actual sistema de gestión de personal sanitario	Puntuación				
6. Facilidad para la introducción de datos de un nuevo cuidador en el sistema de gestión.	1	2	3	4	5
7. Facilidad y rapidez a la hora de encontrar datos de un cuidador en el sistema de gestión.	1	2	3	4	5
8. Importancia del control de los cuidadores. Por ejemplo: Control de que cuidador hizo un control de glucosa a un residente concreto.	1	2	3	4	5
9. Importancia de la protección de los datos de los cuidadores.	1	2	3	4	5

10. Seguridad de protección de datos en el sistema de gestión.	1	2	(3)	4	5
11. Valoración general del sistema de gestión de cuidadores.	1	(2)	3	4	5

Actual sistema de gestión de las medidas	Puntuación				
12. Facilidad y rapidez para la introducción de nuevas medidas en el sistema de gestión.	1	2	(3)	4	5
13. Fiabilidad de las medidas introducidas en el sistema (Valoración de la posibilidad de fallos humanos en la transcripción).	1	(2)	3	4	5
14. Facilidad y rapidez a la hora de encontrar una medida o un grupo de medidas concretas de un residente en el sistema de gestión.	1	(2)	3	4	5
15. Facilidad y rapidez a la hora de generar un informe con las medidas de un residente que el médico demande usando el sistema de gestión.	1	2	(3)	4	5
16. Fiabilidad de los datos al generar un informe (Valoración de la posibilidad de fallos humanos en la generación de informes).	1	2	3	(4)	5
17. Importancia de la protección de datos en el sistema de gestión de medidas	1	2	(3)	4	5
18. Valoración general del sistema de gestión de las medidas.	1	(2)	3	4	5

Valoración general	Puntuación				
19. Protección de datos del actual sistema de gestión de datos.	1	2	(3)	4	5
20. Facilidad de uso del actual sistema de gestión de datos.	1	(2)	3	4	5
21. Valoración del actual sistema general de gestión de datos.	(1)	2	3	4	5

Encuesta previa para la administración

Nombre: JANINA FIGUEROAEdad: 34 añosSexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Actual sistema de gestión de residentes	Puntuación				
1. Facilidad para introducción de datos de un nuevo residente en el sistema de gestión.	1	(2)	3	4	5
2. Facilidad y rapidez a la hora de encontrar datos de un residente concreto en el sistema de gestión.	(1)	2	3	4	5
3. Importancia de la protección de los datos de los residentes.	1	2	3	4	(5)
4. Seguridad de protección de datos en el sistema de gestión.	1	2	(3)	4	5
5. Valoración general del sistema de gestión de residentes.	1	(2)	3	4	5

Actual sistema de gestión de personal sanitario	Puntuación				
6. Facilidad para la introducción de datos de un nuevo cuidador en el sistema de gestión.	1	(2)	3	4	5
7. Facilidad y rapidez a la hora de encontrar datos de un cuidador en el sistema de gestión.	(1)	2	3	4	5
8. Importancia del control de los cuidadores. Por ejemplo: Control de que cuidador hizo un control de glucosa a un residente concreto.	1	2	(3)	4	5
9. Importancia de la protección de los datos de los cuidadores.	1	(2)	3	4	5

10. Seguridad de protección de datos en el sistema de gestión.	1	(2)	3	4	5
11. Valoración general del sistema de gestión de cuidadores.	1	2	(3)	4	5

Actual sistema de gestión de las medidas	Puntuación				
12. Facilidad y rapidez para la introducción de nuevas medidas en el sistema de gestión.	1	(2)	3	4	5
13. Fiabilidad de las medidas introducidas en el sistema (Valoración de la posibilidad de fallos humanos en la transcripción).	1	2	(3)	4	5
14. Facilidad y rapidez a la hora de encontrar una medida o un grupo de medidas concretas de un residente en el sistema de gestión.	(1)	2	3	4	5
15. Facilidad y rapidez a la hora de generar un informe con las medidas de un residente que el médico demande usando el sistema de gestión.	1	2	3	(4)	5
16. Fiabilidad de los datos al generar un informe (Valoración de la posibilidad de fallos humanos en la generación de informes).	1	(2)	3	4	5
17. Importancia de la protección de datos en el sistema de gestión de medidas	1	2	(3)	4	5
18. Valoración general del sistema de gestión de las medidas.	(1)	2	3	4	5

Valoración general	Puntuación				
19. Protección de datos del actual sistema de gestión de datos.	1	(2)	3	4	5
20. Facilidad de uso del actual sistema de gestión de datos.	1	2	(3)	4	5
21. Valoración del actual sistema general de gestión de datos.	1	(2)	3	4	5

11.2 Encuestas previas para el personal sanitario

Encuesta previa para el personal sanitario

Nombre: FLOR BAILE
 Edad: 46
 Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Proceso previo a la toma de medidas	Puntuación
1. Tiempo invertido en la búsqueda de expedientes de los residentes.	1 2 3 4 5
2. Tiempo invertido en la ordenación de los expedientes para su posterior uso.	1 2 3 4 5
3. Tiempo invertido en la preparación de los utensilios necesarios para el proceso de tomas de medidas.	1 2 3 4 5
4. Tiempo total invertido previo a la toma de medidas.	1 2 3 4 5

Proceso de toma de medidas	Puntuación
5. Tiempo invertido en la búsqueda del residente al que se le va tomar la medida.	1 2 3 4 5
6. Predisposición del residente al que se le va a tomar la medida con el actual proceso.	1 2 3 4 5
7. Facilidad de uso de los dispositivos utilizados.	1 2 3 4 5
8. Facilidad de manejo de los accesorios utilizados.	1 2 3 4 5
9. Tiempo invertido en el proceso.	1 2 3 4 5
10. Tiempo invertido en el proceso de transcripción de medidas al expediente del residente.	1 2 3 4 5

11. Tiempo entre la realización de la medida a dos residentes.	1	(2)	3	4	5
12. Tiempo total invertido en el proceso de toma de medidas.	1	2	(3)	4	5
13. Eficiencia del proceso.	1	(2)	3	4	5

Proceso posterior a la toma de medidas	Puntuación
14. Facilidad de almacenamiento de los expedientes con las medidas tomadas anteriormente.	1 (2) 3 4 5
15. Tiempo invertido en almacenar los expedientes de los residentes.	(1) 2 3 4 5
16. Tiempo total invertido en proceso posterior a la toma de medidas.	1 (2) 3 4 5

Valoración general	Puntuación
17. Tiempo total invertido en el proceso.	1 (2) 3 4 5
18. Eficiencia del todo el proceso	1 2 (3) 4 5
19. Valoración general del proceso.	1 (2) 3 4 5

Encuesta previa para el personal sanitario

Nombre: JANINA FIGUEROLAEdad: 34Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Proceso previo a la toma de medidas	Puntuación				
1. Tiempo invertido en la búsqueda de expedientes de los residentes.	1	2	3	4	5
2. Tiempo invertido en la ordenación de los expedientes para su posterior uso.	1	2	3	4	5
3. Tiempo invertido en la preparación de los utensilios necesarios para el proceso de tomas de medidas.	1	2	3	4	5
4. Tiempo total invertido previo a la toma de medidas.	1	2	3	4	5

Proceso de toma de medidas	Puntuación				
5. Tiempo invertido en la búsqueda del residente al que se le va tomar la medida.	1	2	3	4	5
6. Predisposición del residente al que se le va a tomar la medida con el actual proceso.	1	2	3	4	5
7. Facilidad de uso de los dispositivos utilizados.	1	2	3	4	5
8. Facilidad de manejo de los accesorios utilizados.	1	2	3	4	5
9. Tiempo invertido en el proceso.	1	2	3	4	5
10. Tiempo invertido en el proceso de transcripción de medidas al expediente del residente.	1	2	3	4	5

11. Tiempo entre la realización de la medida a dos residentes.	1	(2)	3	4	5
12. Tiempo total invertido en el proceso de toma de medidas.	1	(2)	3	4	5
13. Eficiencia del proceso.	1	(2)	3	4	5

Proceso posterior a la toma de medidas	Puntuación				
14. Facilidad de almacenamiento de los expedientes con las medidas tomadas anteriormente.	1	2	(3)	4	5
15. Tiempo invertido en almacenar los expedientes de los residentes.	1	(2)	3	4	5
16. Tiempo total invertido en proceso posterior a la toma de medidas.	1	2	3	4	5

Valoración general	Puntuación				
17. Tiempo total invertido en el proceso.	1	(2)	3	4	5
18. Eficiencia del todo el proceso	1	(2)	3	4	5
19. Valoración general del proceso.	1	(2)	3	4	5

11.3 Encuestas de evolución para el personal de administración

Encuesta de evolución para la administración

Nombre: FLOR BAILE
 Edad: 46 AÑOS
 Sexo: Femenina

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Sistema de gestión de residentes	Puntuación
1. Facilidad para encontrar la opción de introducir un nuevo residente.	1 2 3 4 5
2. Facilidad para introducir un nuevo residente en el sistema de gestión.	1 2 3 4 5
3. Valoración de si los campos introducidos son suficientes para la gestión de los residentes.	1 2 3 4 5
4. Facilidad para editar el perfil de un residente.	1 2 3 4 5
5. Facilidad de uso del sistema de gestión de residentes.	1 2 3 4 5
6. Diseño visual del sistema de gestión de residentes.	1 2 3 4 5
7. Valoración general del sistema de gestión de residentes	1 2 3 4 5

Sistema de gestión de personal sanitario	Puntuación
8. Facilidad para encontrar la opción de introducir un nuevo personal sanitario.	1 2 3 4 5
9. Facilidad para introducir un nuevo personal sanitario en el sistema de gestión.	1 2 3 4 5
10. Valoración de si los campos introducidos son suficientes para la gestión del personal sanitario.	1 2 3 4 5

11. Facilidad para editar el perfil de un personal sanitario.	1	2	3	4	(5)
12. Facilidad de uso del sistema de gestión de personal sanitario.	1	2	3	4	(5)
13. Diseño visual del sistema de gestión de personal sanitario.	1	2	3	4	(5)
14. Valoración general del sistema de gestión de personal sanitario.	1	2	3	4	(5)

Sistema de gestión de las medidas	Puntuación				
15. Facilidad para encontrar la opción de generar un informe de medidas de un residente.	1	2	3	(4)	5
16. Facilidad a la hora de seleccionar un rango de fechas del que se desea el informe.	1	2	3	4	(5)
17. Utilidad de poder introducir observaciones en el informe.	1	2	3	4	(5)
18. Diseño visual del sistema de gestión de medidas.	1	2	3	(4)	5
19. Facilidad para generar un nuevo informe de medidas.	1	2	3	4	(5)
20. Diseño visual del informe generado.	1	2	3	(4)	5
21. Valoración general del sistema de gestión de medidas.	1	2	3	4	(5)

Sistema de gestión de tarjetas	Puntuación				
22. Facilidad para agregar una nueva tarjeta al sistema de gestión de tarjetas.	1	2	3	4	(5)
23. Facilidad para eliminar una tarjeta del sistema de gestión de tarjetas.	1	2	3	4	(5)
24. Facilidad para asignar una tarjeta de identificación al personal sanitario.	1	2	3	(4)	5
25. Facilidad para desasignar una tarjeta de identificación al personal sanitario.	1	2	3	4	(5)
26. Utilidad de asignar/desasignar tarjetas.	1	2	3	4	(5)
27. Diseño visual del sistema de gestión de tarjetas.	1	2	3	4	(5)
28. Valoración de la seguridad que introduce un sistema de control de personal sanitario.	1	2	3	4	(5)

29. Valoración general del sistema de gestión de tarjetas de identificación.	1	2	3	4	5
--	---	---	---	---	---

Valoraciones generales del sistema	Puntuación
30. Tiempos de espera cuando una operación implica introducir datos en la base de datos.	1 2 3 4 5
31. Intuitividad de las frases que aparecen cuando una operación implica una espera de tiempo.	1 2 3 4 5
32. Tamaño de letra de las frases que aparecen cuando una operación implica una espera de tiempo.	1 2 3 4 5
33. Tamaño de letra de las tablas que aparecen en la aplicación de gestión.	1 2 3 4 5
34. Tamaño de letra de títulos y fichas de usuario.	1 2 3 4 5

Observaciones:

Encuesta de evolución para la administración

Nombre: SANINA FIGUEROAEdad: 34 añosSexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Sistema de gestión de residentes	Puntuación				
1. Facilidad para encontrar la opción de introducir un nuevo residente.	1	2	3	(4)	5
2. Facilidad para introducir un nuevo residente en el sistema de gestión.	1	2	3	4	(5)
3. Valoración de si los campos introducidos son suficientes para la gestión de los residentes.	1	2	3	4	(5)
4. Facilidad para editar el perfil de un residente.	1	2	3	4	(5)
5. Facilidad de uso del sistema de gestión de residentes.	1	2	3	4	(5)
6. Diseño visual del sistema de gestión de residentes.	1	2	3	4	(5)
7. Valoración general del sistema de gestión de residentes	1	2	3	4	(5)

Sistema de gestión de personal sanitario	Puntuación				
8. Facilidad para encontrar la opción de introducir un nuevo personal sanitario.	1	2	3	(4)	5
9. Facilidad para introducir un nuevo personal sanitario en el sistema de gestión.	1	2	3	(4)	5
10. Valoración de si los campos introducidos son suficientes para la gestión del personal sanitario.	1	2	3	4	(5)

11. Facilidad para editar el perfil de un personal sanitario.	1	2	3	4	5
12. Facilidad de uso del sistema de gestión de personal sanitario.	1	2	3	4	5
13. Diseño visual del sistema de gestión de personal sanitario.	1	2	3	4	5
14. Valoración general del sistema de gestión de personal sanitario.	1	2	3	4	5

Sistema de gestión de las medidas	Puntuación				
15. Facilidad para encontrar la opción de generar un informe de medidas de un residente.	1	2	3	4	5
16. Facilidad a la hora de seleccionar un rango de fechas del que se desea el informe.	1	2	3	4	5
17. Utilidad de poder introducir observaciones en el informe.	1	2	3	4	5
18. Diseño visual del sistema de gestión de medidas.	1	2	3	4	5
19. Facilidad para generar un nuevo informe de medidas.	1	2	3	4	5
20. Diseño visual del informe generado.	1	2	3	4	5
21. Valoración general del sistema de gestión de medidas.	1	2	3	4	5

Sistema de gestión de tarjetas	Puntuación				
22. Facilidad para agregar una nueva tarjeta al sistema de gestión de tarjetas.	1	2	3	4	5
23. Facilidad para eliminar una tarjeta del sistema de gestión de tarjetas.	1	2	3	4	5
24. Facilidad para asignar una tarjeta de identificación al personal sanitario.	1	2	3	4	5
25. Facilidad para desasignar una tarjeta de identificación al personal sanitario.	1	2	3	4	5
26. Utilidad de asignar/desasignar tarjetas.	1	2	3	4	5
27. Diseño visual del sistema de gestión de tarjetas.	1	2	3	4	5
28. Valoración de la seguridad que introduce un sistema de control de personal sanitario.	1	2	3	4	5

29. Valoración general del sistema de gestión de tarjetas de identificación.	1	2	3	4	5
--	---	---	---	---	---

Valoraciones generales del sistema	Puntuación				
30. Tiempos de espera cuando una operación implica introducir datos en la base de datos.	1	2	3	(4)	5
31. Intuitividad de las frases que aparecen cuando una operación implica una espera de tiempo.	1	2	3	(4)	5
32. Tamaño de letra de las frases que aparecen cuando una operación implica una espera de tiempo.	1	2	3	4	(5)
33. Tamaño de letra de las tablas que aparecen en la aplicación de gestión.	1	2	3	(4)	5
34. Tamaño de letra de títulos y fichas de usuario.	1	2	3	4	(5)

Observaciones:

11.4 Encuestas posteriores para el personal de administración

Encuesta posterior para la administración

Nombre: FIR BAILE
 Edad: 46 años
 Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Nuevo sistema de gestión de residentes	Puntuación
1. Facilidad para introducción de datos de un nuevo residente en el sistema de gestión.	1 2 3 4 5
2. Facilidad y rapidez a la hora de encontrar datos de un residente concreto en el sistema de gestión.	1 2 3 4 5
3. Valoración de la seguridad de protección de datos en el sistema de gestión.	1 2 3 4 5
4. Valoración general del sistema de gestión.	1 2 3 4 5

Nuevo sistema de gestión de personal sanitario	Puntuación
5. Facilidad para la introducción de datos de un nuevo cuidador en el sistema de gestión.	1 2 3 4 5
6. Facilidad y rapidez a la hora de encontrar datos de un cuidador en el sistema de gestión.	1 2 3 4 5
7. Valoración de la seguridad de protección de datos en el sistema de gestión.	1 2 3 4 5
8. Valoración del nuevo sistema de control de cuidadores mediante tarjeta de identificación.	1 2 3 4 5
9. Valoración general del sistema de gestión de cuidadores.	1 2 3 4 5

Nuevo sistema de gestión de las medidas	Puntuación				
10. Facilidad y rapidez para la introducción de nuevas medidas en el sistema de gestión.	1	2	3	4	5
11. Fiabilidad de las medidas introducidas en el sistema.	1	2	3	4	5
12. Facilidad y rapidez a la hora de encontrar una medida o un grupo de medidas concretas de un residente en el sistema de gestión.	1	2	3	4	5
13. Facilidad y rapidez a la hora de generar un informe con las medidas de un residente que el médico demande usando el sistema de gestión.	1	2	3	4	5
14. Fiabilidad de los datos al generar un informe	1	2	3	4	5
15. Valoración general del sistema de gestión de las medidas.	1	2	3	4	5

Nuevo sistema de gestión de tarjetas	Puntuación				
16. Facilidad y rapidez para agregar/eliminar una tarjeta de identificación en el sistema de gestión.	1	2	3	4	5
17. Facilidad y rapidez para asignar/desasignar una tarjeta de identificación a un personal sanitario en el sistema de gestión.	1	2	3	4	5
18. Valoración general del sistema de gestión de tarjetas y control del personal sanitario.	1	2	3	4	5

Nuevo sistema de gestión de datos	Puntuación				
19. Valoración general del sistema de gestión de datos.	1	2	3	4	5

Encuesta posterior para la administraciónNombre: JANINA FIGUEROAEdad: 34Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntué cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Nuevo sistema de gestión de residentes	Puntuación
1. Facilidad para introducción de datos de un nuevo residente en el sistema de gestión.	1 2 3 4 <u>5</u>
2. Facilidad y rapidez a la hora de encontrar datos de un residente concreto en el sistema de gestión.	1 2 3 <u>4</u> 5
3. Valoración de la seguridad de protección de datos en el sistema de gestión.	1 2 3 4 <u>5</u>
4. Valoración general del sistema de gestión.	1 2 3 4 <u>5</u>

Nuevo sistema de gestión de personal sanitario	Puntuación
5. Facilidad para la introducción de datos de un nuevo cuidador en el sistema de gestión.	1 2 3 4 <u>5</u>
6. Facilidad y rapidez a la hora de encontrar datos de un cuidador en el sistema de gestión.	1 2 3 4 <u>5</u>
7. Valoración de la seguridad de protección de datos en el sistema de gestión.	1 2 3 4 <u>5</u>
8. Valoración del nuevo sistema de control de cuidadores mediante tarjeta de identificación.	1 2 3 4 <u>5</u>
9. Valoración general del sistema de gestión de cuidadores.	1 2 3 4 <u>5</u>

Nuevo sistema de gestión de las medidas						Puntuación
10. Facilidad y rapidez para la introducción de nuevas medidas en el sistema de gestión.	1	2	3	4	5	
11. Fiabilidad de las medidas introducidas en el sistema.	1	2	3	4	5	
12. Facilidad y rapidez a la hora de encontrar una medida o un grupo de medidas concretas de un residente en el sistema de gestión.	1	2	3	4	5	
13. Facilidad y rapidez a la hora de generar un informe con las medidas de un residente que el médico demande usando el sistema de gestión.	1	2	3	4	5	
14. Fiabilidad de los datos al generar un informe	1	2	3	4	5	
15. Valoración general del sistema de gestión de las medidas.	1	2	3	4	5	

Nuevo sistema de gestión de tarjetas						Puntuación
16. Facilidad y rapidez para agregar/eliminar una tarjeta de identificación en el sistema de gestión.	1	2	3	4	5	
17. Facilidad y rapidez para asignar/desasignar una tarjeta de identificación a un personal sanitario en el sistema de gestión.	1	2	3	4	5	
18. Valoración general del sistema de gestión de tarjetas y control del personal sanitario.	1	2	3	4	5	

Nuevo sistema de gestión de datos						Puntuación
19. Valoración general del sistema de gestión de datos.	1	2	3	4	5	

11.5 Encuestas posteriores para el personal sanitario

Encuesta posterior para el personal sanitario

Nombre: FLOR BAT/FE
 Edad: 46 años
 Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntué cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Proceso previo a la toma de medidas	Puntuación				
1. Tiempo invertido en la búsqueda de expedientes de los residentes con el nuevo sistema.	1	2	3	4	5
2. Tiempo invertido en la ordenación de los expedientes para su posterior uso con el nuevo sistema.	1	2	3	4	5
3. Tiempo invertido en la preparación de los utensilios necesarios para el proceso de tomas de medidas con el nuevo sistema.	1	2	3	4	5
4. Tiempo total invertido previo a la toma de medidas con el nuevo sistema.	1	2	3	4	5

Proceso de toma de medidas	Puntuación				
5. Tiempo invertido en la búsqueda del residente al que se le va tomar la medida con el nuevo sistema.	1	2	3	4	5
6. Predisposición del residente al que se le va a tomar la medida con el nuevo proceso de toma de medidas.	1	2	3	4	5
7. Facilidad de uso de los nuevos dispositivos utilizados.	1	2	3	4	5
8. Facilidad de manejo de los accesorios utilizados en el nuevo proceso.	1	2	3	4	5
9. Tiempo invertido en el nuevo proceso.	1	2	3	4	5

10. Tiempo invertido en el proceso de transcripción de medidas al expediente del residente con el nuevo sistema.	1	2	3	4	5
11. Tiempo entre la realización de la medida a dos residentes con el nuevo sistema.	1	2	3	4	5
12. Tiempo total invertido en el proceso de toma de medidas con el nuevo sistema.	1	2	3	4	5
13. Eficiencia del proceso de toma de medidas con el nuevo sistema.	1	2	3	4	5

Proceso posterior a la toma de medidas	Puntuación
14. Facilidad de almacenamiento de los expedientes con las medidas tomadas anteriormente con el nuevo sistema.	1 2 3 4 5
15. Tiempo invertido en almacenar los expedientes de los residentes con el nuevo sistema.	1 2 3 4 5
16. Tiempo total invertido en proceso posterior a la toma de medidas con el nuevo sistema.	1 2 3 4 5

Valoración general	Puntuación
17. Tiempo total invertido en el nuevo proceso.	1 2 3 4 5
18. Eficiencia del todo el nuevo proceso.	1 2 3 4 5
19. Valoración general.	1 2 3 4 5

Encuesta posterior para el personal sanitario

Nombre: JANINA FIGUEROAEdad: 34Sexo: FEMENINO

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

1	Mal/Nada
2	Regular/Poco
3	Bien/Suficiente
4	Muy bien/Bastante
5	Excelente/Mucho

Puntúe cada característica seleccionando con un círculo una de las puntuaciones situadas a la derecha según su criterio de calidad, como en el ejemplo anterior. En la tabla situada arriba se especifica a qué criterio corresponde cada número.

Proceso previo a la toma de medidas	Puntuación
1. Tiempo invertido en la búsqueda de expedientes de los residentes con el nuevo sistema.	1 2 3 4 <u>5</u>
2. Tiempo invertido en la ordenación de los expedientes para su posterior uso con el nuevo sistema.	1 2 3 4 <u>5</u>
3. Tiempo invertido en la preparación de los utensilios necesarios para el proceso de tomas de medidas con el nuevo sistema.	1 2 3 4 <u>5</u>
4. Tiempo total invertido previo a la toma de medidas con el nuevo sistema.	1 2 3 4 <u>5</u>

Proceso de toma de medidas	Puntuación
5. Tiempo invertido en la búsqueda del residente al que se le va a tomar la medida con el nuevo sistema.	1 2 3 4 <u>5</u>
6. Predisposición del residente al que se le va a tomar la medida con el nuevo proceso de toma de medidas.	1 2 3 <u>4</u> 5
7. Facilidad de uso de los nuevos dispositivos utilizados.	1 2 3 <u>4</u> 5
8. Facilidad de manejo de los accesorios utilizados en el nuevo proceso.	1 2 3 <u>4</u> 5
9. Tiempo invertido en el nuevo proceso.	1 2 3 4 <u>5</u>

10. Tiempo invertido en el proceso de transcripción de medidas al expediente del residente con el nuevo sistema.	1	2	3	4	5
11. Tiempo entre la realización de la medida a dos residentes con el nuevo sistema.	1	2	3	4	5
12. Tiempo total invertido en el proceso de toma de medidas con el nuevo sistema.	1	2	3	4	5
13. Eficiencia del proceso de toma de medidas con el nuevo sistema.	1	2	3	4	5

Proceso posterior a la toma de medidas	Puntuación
14. Facilidad de almacenamiento de los expedientes con las medidas tomadas anteriormente con el nuevo sistema.	1 2 3 4 5
15. Tiempo invertido en almacenar los expedientes de los residentes con el nuevo sistema.	1 2 3 4 5
16. Tiempo total invertido en proceso posterior a la toma de medidas con el nuevo sistema.	1 2 3 4 5

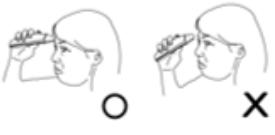
Valoración general	Puntuación
17. Tiempo total invertido en el nuevo proceso.	1 2 3 4 5
18. Eficiencia del todo el nuevo proceso.	1 2 3 4 5
19. Valoración general.	1 2 3 4 5

12 Anexo 6: Manuales de uso de dispositivos médicos y ficha técnica

12.1 Manuales de uso de dispositivos médicos

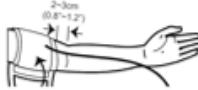
Paso 0. Abra la aplicación y espere a que se inicie.	Paso 1. Aproxime la tarjeta a la parte trasera del móvil para autenticarse.	Paso 2. Deslícese por la pantalla para seleccionar el residente a medir.
Paso 3a. Introducción automática. El móvil recibirá la medida enviada por el dispositivo. Paso 3b. Introducción manual. Deslice hacia arriba el panel inferior.		Paso 3b. Seleccione la medida y pulse sobre el cuadro de texto para introducirla.
Paso 4. Visualice la medida en pantalla mientras se envía de forma automática.	Paso 5. Seleccione la siguiente acción a realizar.	Opcional. Tiene la opción de enviar SMS si tiene activo el servicio.
Presione el botón para cerrar la sesión del cuidador. Asegúrese de cerrar su sesión cuando haya finalizado su actividad.	Se recomienda usar la aplicación conectado a Internet.	Si el residente que busca no aparece en la lista, presione el botón de sincronizar .

Termómetro

Frente	Paso 1. Encienda el dispositivo presionando el botón de la pantalla.	Paso 2. Coloque la punta del termómetro en la frente del residente y mantenga presionado el botón de la parte superior durante unos segundos.	Paso 3. Suelte el botón superior, el termómetro emitirá un pitido y realizará el envío de la medida, iluminándose la luz azul en la parte inferior.
			
Oído	Paso 1. Retire el cubrimiento del extremo y encienda el dispositivo.	Paso 2. Introduzca el dispositivo en el oído del residente y mantenga presionado el botón de la parte superior.	Paso 3. Cuando el termómetro emita un pitido, suelte el botón. El termómetro empezará a enviar la medida.
			

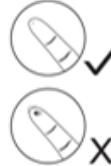
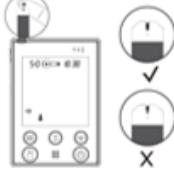
Nota: El dispositivo no funcionará correctamente si no se siguen estos pasos para tomar la medida. Si esto sucede, por favor empiece de nuevo desde el principio.

Tensiómetro

Paso 0. Conecte el tubo de la banda al hinchador y coloque la banda para medir.	Paso 0. Ajuste la banda en el brazo izquierdo del residente de forma que la línea roja quede 2 o 3 cm. por encima del codo. La banda debe de encontrarse a la misma altura que el corazón.	Paso 1. Cuando la banda de medir esté bien colocada, presione el botón de encender  .
		
Paso 2. La banda comenzará a hincharse automáticamente. Espere tranquilo mientras el dispositivo realiza la toma de medida.	Paso 3. La medida se habrá realizado correctamente cuando la banda empiece a desinflarse y la medida aparezca en pantalla.	Paso 4. A continuación, el dispositivo comenzará el envío, iluminándose una luz azul. Cuando el dispositivo haya terminado, se apagará automáticamente.
		

Nota: El dispositivo no funcionará correctamente si no se siguen estos pasos para tomar la medida. Si esto sucede, por favor empiece de nuevo desde el principio.

Glucómetro

Paso 1. Con el dispositivo apagado, inserte la tira reactiva en la ranura.	Paso 2. Espere hasta que el monitor muestre el símbolo de la tira y la gota de sangre.	Paso 3. Obtenga la muestra de sangre del paciente.
		
Paso 4. Coloque la muestra de sangre en la tira reactiva colocada en el dispositivo.	Paso 5. El dispositivo empezará una cuenta atrás y mostrará su medida en pantalla. A continuación, empezará a enviar la medida automáticamente.	Paso 6. Cuando el dispositivo se apague automáticamente, expulse la tira reactiva deslizando el eyector del lateral izquierdo.
		

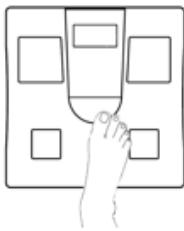
Note: El dispositivo no funcionará correctamente si no se siguen estos pasos para tomar la medida. Si esto sucede, por favor empiece de nuevo desde el principio.

Pulsioxímetro

Paso 1. Presione el botón de encender 	Paso 2. Inserte el dedo del residente en la pinza para medir, colocando el cable hacia abajo
	
Paso 3. Cuando los valores aparezcan en pantalla y el pitido sea más intenso, la medida se habrá realizado.	Paso 4. Presione el botón de encender durante unos segundos hasta que el dispositivo se apague. El dispositivo empezará a enviar la medida automáticamente, iluminándose una luz azul.
	

Note: El dispositivo no funcionará correctamente si no se siguen estos pasos para tomar la medida. Si esto sucede, por favor empiece de nuevo desde el principio.

Báscula

Paso 1. Golpee suavemente la báscula con el pie para encenderla.	Paso 2. Espere hasta que aparezca 0.0 kg en la pantalla.	Paso 3. Súbase encima de la báscula mientras el dispositivo realiza la medida.
		
Paso 4. Podrá bajarse de la báscula cuando la pantalla empiece a parpadear.	Paso 5. Tras unos segundos, el dispositivo comenzará a enviar automáticamente la medida.	Nota: El dispositivo no funcionará correctamente si no se siguen estos pasos para tomar la medida. Si esto sucede, por favor empiece desde el principio.
		

Nota: El dispositivo no funcionará correctamente si no se siguen estos pasos para tomar la medida. Si esto sucede, por favor empiece de nuevo desde el principio.

12.2 Ficha técnica

Nombre de la residencia	
Número de plazas (residentes)	
Número de personal sanitario <i>incluyendo nº de usuarios de tarjeta NFC</i>	
Contacto comercial <i>incluyendo mail y teléfono</i>	
Contacto técnico <i>incluyendo mail y teléfono</i>	
Dirección	
Fecha prevista para SET-UP	

A. DATOS TÉCNICOS

Conexión a Internet	Sí/No	Observaciones
¿Tiene conexión a Internet (ADSL)? ¿en todos los ordenadores?		
¿Qué conexión tiene contratada? ¿con qué compañía?		
¿Tiene acceso alguien de la residencia a gestionar el <i>router</i> ? (por ej: cambiar la contraseña)		
¿Tiene conexión Wi-Fi?		
¿Qué cobertura/alcance tiene la WiFi? (por ej: lugar/es de las tomas)		
Equipos informáticos y software	Sí/No	Observaciones
¿Cuántos ordenadores tienen en la residencia? ¿En cuáles se instalará?		
¿Qué sist. operativo tienen instalado? ¿Qué arquitectura x64 ó x86?		
¿Tienen instalado software de gestión?		
Servidores y bases de datos	Sí/No	Observaciones
¿Hay servidores en la propia residencia? Los datos de residentes y de personal, ¿están almacenados en formato digital? ¿En qué formato?		
¿Cómo se plantea introducir los datos ya existentes en la nueva base de datos?		

B. PROCEDIMIENTOS DE MEDIDAS

Toma de medidas manual	Observaciones
¿Cómo se toma el peso ? (nº veces por día, horas de cada toma, lugar de tomas, tipos de residente, perfil de gerocultor)	
¿Cómo se toma la temperatura ? (nº veces por día, horas de cada toma, lugar de tomas, tipos de residente, perfil de gerocultor)	
¿Cómo se toma la presión arterial ? (nº veces por día, horas de cada toma, lugar de tomas, tipos de residente, perfil de gerocultor)	
¿Cómo se toma la pulsioximetría ? (nº veces por día, horas de cada toma, lugar de tomas, tipos de residente, perfil de gerocultor)	