LOPD Compliance and ISO 27001 Legal Requirements in the Health Sector

L. E. Sánchez, A. S. Olmo, E. Álvarez, E. F. Medina and M. Piattini

***Abstract*— In a society based on information, the Safety Management Systems (ISMS) are increasingly critical for businesses. Within the Management of Information Security issues are very critical in certain sectors, such as the processing of personal data for the Health Sector, where a bad use of them can mean irreparable damage to their owners and organizations are obligation to protect them. This paper presents a real case of success that allowed to solve issues related to privacy of patient information at the time of making the quotation of these consultations, as well as compliance with the Organic Law for the protection of Personal Data (OLPD) in environments health and other benefits of the implemented solution.**

***Keywords*— OLPD, ISO27001, ISMS, Health, Privacy, Personal Data.**

I. Introducción

PARA LAS empresas y las administraciones públicas, es muy importante implantar controles de seguridad que les permitan conocer y controlar los riesgos a los que pueden están sometidas [1, 2], ya que la implantación de estos controles supone obtener importantes mejoras para estas organizaciones [3], así como ayudarles a evitar importantes sanciones económicas. Pero la implantación de estos controles no es suficiente, siendo necesaria la presencia de sistemas que gestionen la seguridad a lo largo del tiempo, de modo que les permita reaccionar ágilmente ante nuevos riesgos, vulnerabilidades, amenazas, etc. [4, 5]. Sin embargo, es frecuente que las organizaciones no tengan sistemas de gestión de la seguridad, o que si los tienen, estos estén elaborados sin unas guías adecuadas, sin documentación y con recursos insuficientes [6, 7]. Además, la mayor parte de las herramientas de seguridad disponibles en el mercado ayudan a solucionar parte de los problemas de seguridad, pero son pocas las que abordan el problema de la gestión de la seguridad de una manera global e integrada. De hecho, la enorme diversidad de estas herramientas y su falta de integración suponen un enorme coste en recursos para poderlas gestionar.

Por lo tanto, a pesar de que la realidad ha demostrado que para que las organizaciones puedan utilizar las tecnologías de la información y las comunicaciones con garantías es necesario disponer de guías, métricas y herramientas que les permitan conocer en cada momento su nivel de seguridad y las vulnerabilidades que aún no han sido cubiertas [8], la situación actual es que siguen existiendo muchos elementos críticos [9] sin cubrir a la hora de gestionar aspectos relacionados con la seguridad de la información.

Dentro de estas vulnerabilidades y centradas en un sector crítico como es el sanitario, toma especial relevancia la protección de los datos personales de los pacientes [10-12], ya que esta información es de gran valor para las mafias que trafican con datos médicos. Aunque existen normativas especificas para el tratamiento de la información personal de los pacientes como la LOPD (Ley Orgánica de Protección de Datos Personales) en España, o la HIPAA (Ley de Portabilidad y Responsabilidad del Seguro Médico) [13] en US, y algunas investigaciones demuestran que es uno de los aspectos que mejor se gestiona dentro del SGSI de los hospitales [14, 15], nuestra experiencia ha demostrado que esta norma no se aplica de forma correcta en muchos casos.

En el caso español, después del asesinato del Narcotraficante Colombiano Leónidas Vargas mientras estaba ingresado por un problema pulmonar en el Hospital 12 de Octubre de Madrid (España), hubo un importante cambio en el nivel de concienciación de los riesgos que supone el tratamiento de los datos personales de los pacientes, cambiando la forma de gestionar los mismos en todos los hospitales, siendo ahora obligatorio el consentimiento expreso del paciente a la hora de comunicar su nombre o ubicación física a cualquier persona.

Pero aun así existen algunos aspectos que han quedado fuera de estos cambios y que siguen poniendo en riesgo la información crítica del paciente. Uno de estos fallos a la hora de gestionar es información se da en los sistemas de gestión de citas hospitalarias. Por ejemplo, el llamar a un paciente por su nombre mientras espera en una consulta de Oncología, puede suponer que ese paciente sea penalizado a la hora de obtener posteriormente un seguro de vida, o incluso que pierda su trabajo por el riesgo potencial del coste derivado de las bajas por enfermedad.

La propia Agencia de Protección de datos Española, consciente de estos riesgos, presentó un escrito denominado "Reflexiones en torno a la protección de datos de carácter personal" [16], en el que hacía especial hincapié en el tratamiento de estos datos en el sector sanitario, recomendando:

- Identificar a los pacientes utilizando un código, de forma que el control de accesos y la gestión de la

L. E. Sánchez, Departamento I+D+i, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, lesanchez@sicaman-nt.com

A. Santos-Olmo, Departamento I+D+i, Sicaman Nuevas Tecnologías, Tomelloso (Ciudad Real), España, asolmo@sicaman-nt.com

E. Alvarez, Departamento I+D+i, Fundación In-nova S.L, Toledo, España, ealvarez@in-nova.org

E. Fernandez-Medina, Grupo de Investigación GSyA, Universidad de Castilla-la Mancha, Ciudad Real, España, Eduardo.FdezMedina@uclm.es

M. Piattini, Grupo de Investigación Alarcos, Universidad de Castilla-la Mancha, Ciudad Real, España, Mario.Piattini@uclm.es

información se facilite enormemente, y sólo dispongan de acceso a los datos identificativos el personal sanitario que preste directamente la asistencia sanitaria o aquéllas personas que, por razón de su trabajo, precisen de su conocimiento: datos disociados de una persona identificable.

- Disociar los datos y no mantener los datos identificativos, cuando no sea necesario, para la gestión de la información: datos irreversiblemente disociados de una persona identificable.
- Adoptar códigos tipo, protocolos de actuación, con el máximo consenso posible, que analicen de forma global la información sanitaria.
- Promover la creación en los centros sanitarios o en las asociaciones en las que estos participen, de comités éticos que puedan ayudar a resolver dudas derivadas de la práctica.

Este articulo se centra en la solución planteada para solucionar ese aspecto de la gestión de la seguridad con respecto al tratamiento de la información de los pacientes al llamarlos a consulta dentro del sector sanitario, analizando no sólo la solución, sino otros aspectos positivos derivados de la misma, como la mejora en la gestión de las colas de pacientes, que es un aspecto crítico para reducir los costes de gestión sanitaria [17].

El artículo continúa en la Sección 2, describiendo brevemente la forma en que diferentes países del mundo han afrontando el reto de proteger la privacidad de sus ciudadanos, en especial en materia sanitaria. En la Sección 3 describiremos brevemente los retos planteados y objetivos que se han perseguido a lo largo de la investigación. En la Sección 4 se describe la solución planteada. En la Sección 5 se muestra el funcionamiento de la solución implantada finalmente. En la Sección 6 se describen los principales beneficios obtenidos con la solución planteada. Finalmente, en la Sección 7 concluimos indicando cuáles serán las principales líneas de trabajo que desarrollaremos en el futuro.

II. LEGISLACIÓN PARA LA PRIVACIDAD DE LOS DATOS PERSONALES

Durante las últimas décadas, y especialmente desde el comienzo de la era de la información, todos los gobiernos a nivel mundial han entendido la importancia que tiene mantener la privacidad y dar una adecuada protección a los datos personales, ya que en una era en que la información es el activo de mayor valor, un mal uso por parte de esa información puede suponer graves perjuicios personales. Estos riesgos son mucho mayores en ciertos sectores donde la información es crítica, como es el caso del sector sanitario, donde el acceso a la información puede suponer la exclusión social de las personas, además de importantes daños económicos.

En el caso de Europa, la protección de los datos personales ha tenido una enorme importancia a lo largo de toda la constitución del espacio Europeo [18, 19], dictándose en el año 1995 la directiva 95/46/CEE, relativa a la "protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" y que pasó a convertirse en un derecho fundamental de los europeos al reconocerse así en el artículo 8.1 de la Carta de Derechos Fundamentales de la Unión Europea, proclamada en Niza el 7 de diciembre de 2000, según la cual "Toda persona tiene Derecho a la protección de los datos de carácter personal que le conciernan" [20]. En el caso de UK la privacidad de los datos personales se mantiene sobre la "Data Proteccion Act – 1998".

Dentro del marco de la Unión Europea, España y Portugal marcan una excepción en materia de privacidad al tener influencia de dos zonas, por un lado la UE y por otro Latinoamérica:

- En el caso Español, la privacidad viene regulada por el Artículo 18.4 de Constitución Española (de 27 de diciembre de 1978) según el cual "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Además existe una fuerte legislación para proteger la privacidad de los ciudadanos, basada en la Ley Orgánica de Protección de Datos Personales (LOPD), que es una de las más restrictivas y exigentes del mundo y que se sustenta sobre la Ley Orgánica 15/1999 de 13 de Diciembre, el Real Decreto 1720/2007 de 21 de Diciembre y la Ley 2/2011 del 4 de Marzo. En materia de datos de salud: la ley 41/2002 de 14 de noviembre regula la autonomía del paciente y sus derechos y obligaciones en materia de información y documentación clínica.
- Portugal: Existe una previsión constitucional específica sobre el derecho a la protección de datos desde 1976, en el artículo 35 de la Constitución de la República Portuguesa, que fue modificado en 1997 para adaptarlo a la Directiva 95/46/CE. La privacidad también se sustenta sobre la Ley de Protección de Datos Personales 67/98 de 26 de Octubre que también se encuentra adaptada a la directiva Europea.

En el caso de Latinoamérica, la privacidad de la información también ha sido una preocupación constante [21].

- En el caso de Argentina, la privacidad viene protegida mediante el Artículo 43 de la Constitución Nacional y la Ley nº 25.326, sancionada en el año 2000 y reglamentada en el año 2001.
- En el caso de Brasil, la Constitución Federal prevé el acceso a datos (art. 5º, LXXII), la protección de la intimidad y la vida privada (art. 5º, X); la inviolabilidad de las comunicaciones donde se sitúan los datos (art. 5º XII) y por la Ley nº 9.507/97 que reglamenta el habeas data.
- En el caso de Chile no existe norma expresa, pero la construcción jurídica de la protección de datos personales se basa en el artículo 19 n°4 de la Constitución Política de la República y en la Ley 19.628 "Sobre protección de la vida privada", publicada el 28 de agosto de 1999, modificada por la

Ley N° 19.812, de 13 de junio de 2002. En el ámbito sanitario, el art. 24 de la Ley 19.628 modificó al artículo 127 del Código Sanitario estableciendo que ""las recetas médicas y análisis o exámenes de laboratorios clínicos y servicios relacionados con la salud son reservados. Sólo podrá revelarse su contenido o darse copia de ellos con el consentimiento expreso del paciente, otorgado por escrito. Quien divulgare su contenido indebidamente, o infringiere las disposiciones del inciso siguiente, será castigado en la forma y con las sanciones establecidas en el Libro Décimo. Lo dispuesto en este artículo no obsta para que las farmacias puedan dar a conocer, para fines estadísticos, las ventas de productos farmacéuticos de cualquier naturaleza, incluyendo la denominación y cantidad de ellos. En ningún caso la información que proporcionen las farmacias consignará el nombre de los pacientes destinatarios de las recetas, ni el de los médicos que las expidieron, ni datos que sirvan para identificarlos".

- Colombia: El artículo 15 de la Constitución, modificado por el acto legislativo N° 02 del 18 de diciembre de 2003 dice lo siguiente: "Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificarlas informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas". Otras leyes orientadas a mantener la privacidad en el ámbito legal Colombiano son el artículo 95 de la Ley 270 de 1996 (estatutaria de la administración de justicia) ,que ordena que los procesos que se tramiten con soporte informático garantizarán la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley. El Literal c del artículo 32 de la ley 527 de 1999, el artículo 25 del decreto 1747 de 2002 y el Literal 11 del artículo 13 del decreto 1742 del 2002 para el Comercio Electrónico y firmas digitales. Por último, actualmente se encuentra en estudio el proyecto de ley estatutaria Nº143 de 2003 por la cual se dictan disposiciones para la protección de datos personales y se regula la actividad de recolección, tratamiento y circulación de los mismos.
- Costa Rica: La Carta Constitucional costarricense no contempla específicamente el derecho a la autodeterminación informativa o el derecho a la protección de datos de carácter personal como un derecho específico. Sólo existe la previsión tradicional del derecho a la intimidad en su artículo 24, que concentra la protección al ámbito de intimidad del hogar, de las comunicaciones y de los documentos privados, dejando a la ley la regulación de las interceptaciones telefónicas y el secuestro de documentos. Actualmente existe un proyecto presentado y en trámite legislativo denominado "Ley de protección de la persona frente al tratamiento de sus datos personales".
- Ecuador: La privacidad se garantiza mediante el artículo 23 y 94 de la constitución de 1998 y el artículo 9 de la Ley de Comercio Electrónico.
- El Salvador: Existe poca legislación en materia de privacidad, estando ésta sustentada tan sólo por el artículo 2 de la Constitución, el cual establece en su inciso segundo que se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. Asimismo, en el artículo 20 del Reglamento General de la Ley Penitenciaria se dice que son datos personales especialmente protegidos "Los datos de carácter personal del interno, relativos a opiniones políticas, convicciones religiosas o filosóficas y sobre su salud, y solamente podrán ser entregados o difundidos a personas, instituciones u organismos de carácter público o privado del país o del extranjero, previo consentimiento por escrito del interno; salvo que por razones de interés general lo disponga alguna ley".
- Nicaragua: No existen normas específicas. La privacidad de los ciudadanos está basada en los artículos 5 y 26 de su constitución.
- Republica de Panamá: Actualmente no tiene normas específicas para proteger la privacidad de sus ciudadanos.
- Perú: Es posiblemente el país de Latinoamérica que más esfuerzos ha realizado para regular y proteger los datos personales de sus ciudadanos. Estos están protegidos por el articulo 2 y 200 de la Constitución política de 1993, además de por un amplio conjunto de leyes especificas y de la existencia de un anteproyecto de ley para la "Protección de Datos Personales". Entre sus leyes podemos destacar Ley General de Salud, Ley 26842 del 20 de julio de 1997 que establece que "toda persona está obligada a proporcionar a la Autoridad de Salud la información que le sea exigible de acuerdo a Ley con las excepciones que establece la Ley; y toda persona usuaria de los servicios de salud, tiene derecho a exigir la reserva de la información relacionada con el acto médico y su historia clínica, con las excepciones de Ley. Art. XIV del Título Preliminar, Art. 5°, 15°".
- República Oriental de Uruguay: La privacidad queda protegida por los artículos 10, 28 y 72 de la Constitución de 1967, así como por la ley nº 17.838. En el ámbito sanitario el derecho a la privacidad de los ciudadanos queda protegido por los decretos Nº 258/992 de 9 de junio de 1992 sobre derechos del paciente y Nº 396/003 de 30 de setiembre de 2003 sobre historia clínica electrónica.
- Republica Bolivariana de Venezuela: La privacidad queda protegida por los artículos 28, 60 y 281 de la Constitución de 1999, así como por la ley contra los

delitos informáticos en sus artículos 20 al 22.

En el caso de América del Norte, también ha sido una preocupación la privacidad, destacando especialmente la legislación de USA en este campo.

- Estados Unidos Mexicanos: El artículo 16 de la Constitución de los Estados Unidos Mexicanos señala que nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones. La privacidad también se sustenta sobre la Ley Federal de Transparencia y Acceso a la Información Pública publicada el 11 de junio de 2002. Y en el caso sanitario, existe una ley específica, denominada "Ley de Salud Pública", que regula cómo y quiénes tienen acceso a los expedientes médicos de los ciudadanos.
- Estados Unidos: Desde la década de los 90, y con los avances tecnológicos, el Congreso de Estados Unidos entendió la importancia de tener leyes que mantuvieran la privacidad en el tratamiento de la información personal de sus ciudadanos, por lo que comenzó a emitir leyes al respecto, principalmente con un carácter sectorial como la HIPAA, GLBA, SB 1386, COPPA y varias "State Breach laws", lo que lo convirtió en uno de los países donde es más complejo cumplir los principios de privacidad. Dentro de este conjunto de normas, podemos destacar la HIPAA (Health Insurance Portability and Accountability Act) creada en 1996 para mantener la privacidad en el sector sanitario. La HIPAA es de obligado cumplimiento no solo para los hospitales, sino también para todos sus proveedores. Hay dos cláusulas HIPAA que se relacionan específicamente con la privacidad y seguridad de su información médica (PHI - Protected Health Information):
  - Regla de privacidad: Que permite que el personal médico use y revele la información médica protegida para su tratamiento, pago y operaciones de atención médica sin autorización escrita.
  - Regla de seguridad: Especifica un conjunto de procesos empresariales y requisitos técnicos que los proveedores, planes médicos y oficinas de compensación deben seguir para garantizar la seguridad de la información médica privada. Está orientada en tres áreas: Salvaguardas administrativas, físicas y técnicas.
- Canadá: La legislación Canadiense en materia de privacidad es más parecida a la adoptada por la Unión Europea que por Estados Unidos, regulándose actualmente por la "Canada's Personal Information Protection and Electronic Documents Act" del año 2000. Existen trabajos muy destacados del marco de la privacidad en Canadá, destacando los escritos por Ann Cavoukian y, en especial, algunos para el sector sanitario donde se menciona la existencia de la PHIPA (Personal Health Information Protection Act) de 2004 [22, 23].

Pero la privacidad de los datos en el sector Sanitario no sólo es una preocupación del ámbito Europeo y Americano. Otros países como Japón, Australia o Malasia [24] han desarrollado leyes específicas que actualmente están modificando para adaptar a los cambios que las mejoras tecnológicas traen consigo.

- Japón: Se han realizado estudios sobre la privacidad de los datos de los ciudadanos, protegidos mediante la "Japan's Personal Information Protection Law" de 2003, y en especial de los datos sanitarios [25], llegando a la conclusión de que es uno de los ámbitos donde los datos requieren una mayor seguridad.
- Australia: La privacidad de los datos queda protegida mediante la "Australia's Privacy Act" de 1988, que fue extendida en el año 2000 mediante la introducción del "National Privacy Principles (NPPs)" [24] para incluir las peculiaridades del sector sanitario.
- Malasia: La legislación vigente no garantiza la privacidad, incluyendo la legislación para el sector sanitario. Su actual legislación se basa en la "Ley de Protección de Datos de Carácter Personal" de 1998, que no fue aprobada hasta el año 2001 a raíz de los atentados de USA. Aún así y conscientes de que esta ley es insuficiente, están trabajando actualmente para redactar una nueva ley que permita mantener de forma eficiente la privacidad [24].

En general, y como hemos podido ver en este recorrido de la privacidad en diferentes países, lo que tienen en común es que existe una inquietud global por proteger los datos personales de los ciudadanos, dado que los gobiernos son conscientes de los enormes riesgos que un mal uso de los mismos puede suponer. Pero, a pesar de eso, muy pocos países han conseguido afrontar de una forma unificada el tratamiento de los datos personales, y menos todavía se han centrado en emitir leyes específicas para el tratamiento de datos tan delicados como los del sector sanitario.

III. Problemática detectada

En Junio del 2007, Pedro Antonio Bonal, Subdirector de Informática del Complejo Hospitalario de Toledo (España), planteó al Departamento de I+D+i de la compañía Sicaman Nuevas Tecnologías el reto de encontrar una solución eficiente a una problemática que seguía sin resolverse en el sector sanitario español, realizar una gestión ***legal, eficiente y de bajo coste*** de las colas de pacientes al realizar la citación a consulta de los mismos.

El equipo informático del Hospital Virgen de la Salud había detectado varias problemáticas importantes y que desde su punto de vista suponían riesgos graves para el funcionamiento del hospital:

- Objetivo 1 - Cumplimiento de la normativa LOPD: A menudo la llamada a los pacientes a consulta en los hospitales o centros sanitarios se realiza de viva voz (Difusión de datos). Según la Ley Orgánica de Protección de Datos Española (LOPD), los datos de

los pacientes que acuden a una consulta están considerados datos privados de nivel alto, por lo que tanto la difusión como la publicación de los mismos vulnera el artículo 10 de la citada ley y constituye por tanto una falta grave, que según el artículo 44 de la misma norma puede originar sanciones de entre 60.000€ y 300.000€. Se necesita, por tanto, un sistema que permita avisar a los pacientes y llamarlos a consultas de una forma totalmente anónima y que garantice el cumplimiento de la normativa LOPD.

- Objetivo 2 - Racionalización del flujo de los pacientes dentro del centro sanitario (ver Fig. 1): El gran crecimiento que experimentan los hospitales y centros de salud en cuanto a nuevos servicios, consultas y pacientes a tratar, unido al hecho de tener que ubicar físicamente las salas de espera junto a las consultas, da lugar frecuentemente a problemas de ergonomía y saturación de los centros. Se necesita, por tanto, un sistema que permita la ubicación flexible de las salas de espera en función de las necesidades cambiantes de los centros hospitalarios y que ayude de esta forma a racionalizar el flujo de los pacientes por el mismo. La gestión de las colas de pacientes en el sector sanitario tiene la problemática adicional de que no son colas cíclicas, sino colas que se enlazan con otras consultas teniendo que volver los pacientes a insertarse en medio de la cola. Esto hace que la gestión correcta de las colas de pacientes sea muy complicada [26, 27] y aunque se han realizado estudios para intentar optimizarlas [28], estos no están siendo aplicados en la práctica, debido a que el funcionamiento de un hospital requiere no sólo de formulaciones matemáticas y soluciones tecnológicas, sino también de factores humanos.
- Objetivo 3 - Identificar de forma inequívoca al paciente: En fases posteriores del proyecto se deseaba encontrar una forma para que, además, el paciente se pudiera autenticar sin poner en riesgo la privacidad de sus datos.
- Objetivo 4 - Coste reducido: La solución debía tener un coste reducido acorde a la crisis mundial que se estaba viviendo y debería representar un elevado ROI (Retorno de la Inversión).
- Objetivo 5 – Simplicidad: Dado que la solución estaba dirigida en parte a personas de edad avanzada, en la mayor parte de los casos con pocos conocimientos tecnológicos, la solución debería ser sencilla de utilizar.
- Objetivo 6 – Escalabilidad: La solución debería poderse integrar con el resto de aplicaciones sanitarias existentes y conectarse con el HIS del Sistema Hospitalario existente. Igualmente, la solución debería sostenerse sobre una arquitectura que pudiera crecer y aportar nuevos servicios, como el de "Inteligencia de Negocio".
- Objetivo 7 – Seguridad: La solución planteada debería ser segura, cumpliendo los requerimientos exigidos en el sector sanitario.

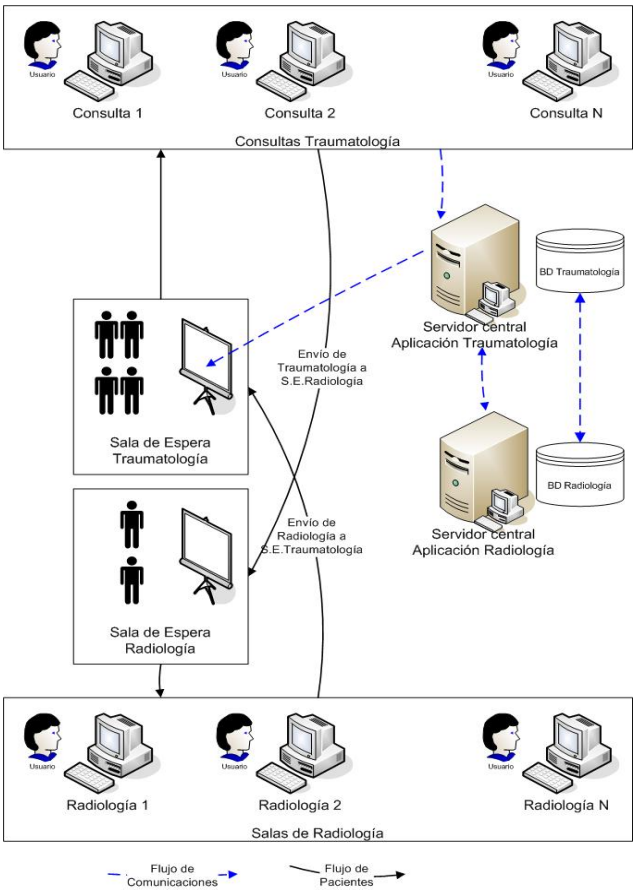

Figura 1. Esquema de flujo de paciente entre los servicios de traumatología y radiología.

Una vez revisados los Sistemas Hospitalarios de diferentes regiones de España, así como la literatura existente en materia de protección de datos en el sector sanitario a nivel mundial, llegamos a la conclusión que no existia ninguna solución que permitiera solucionar los siete objetivos propuestos de forma satisfactoría, debido principalmente a los siguientes problemas:

- Los sistemas de gestión de colas existentes eran genéricos, estaban orientados a gestionar colas individuales de pacientes y no colas entrelazadas como son las sanitarias.
- Las soluciones existentes eran soluciones técnicas, mientras que aquí se requería una solución no sólo técnica, sino que tuviera en cuenta también factores legales y sociales, ya que las personas (tanto pacientes como médicos) debían sentirse cómodos con la solución.
- Las soluciones existentes partieron de ambientes genéricos y entendían que cualquier sector se gestiona de igual forma, sea una cola en Hacienda o en Sanidad.

IV. Solución planteada

La complejidad de los objetivos planteados hizo que tuviera que crearse un complejo equipo multidisciplinar para poder afrontar la solución con garantías, cumpliendo todos los objetivos y dando una solución definitiva a la problemática que pudiera exportarse posteriormente a nivel mundial. Este equipo debería tener experiencia en el sector privado, tanto en la fabricación de software como en el campo de las telecomunicaciones, además de conocimientos del funcionamiento y la problemática real del sector sanitario, y se debería contar además con equipos de investigación avanzada en Seguridad e Ingeniería del Software, que pudieran resolver la problemática planteada en cuanto a escalabilidad, simplicidad y seguridad. Para ello se constituyo un equipo formado, entre otros, por las siguientes personas y competencias:

- Por parte de la compañía Sicaman Nuevas Tecnologías en calidad de coordinadora del proyecto: Luis Enrique Sánchez Crespo como coordinador del área de I+D+i, Antonio Santos-Olmo como responsable de Desarrollo de Software, Jose Vicente Carretero como responsable de la Arquitectura Software y Jose Antonio Parra como responsable del análisis del proyecto para su expansión internacional, además de un potente equipo de programación.
- Por parte del Complejo Hospitalario de Toledo: Se contó con todo el equipo informático liderado por Pedro Antonio Bonal en calidad de Subdirector de Informática, con apoyo de Miguel Ángel Mareque en calidad de Director de Informática, Juan Miguel Severino como Jefe de Servicio de Informática y José López-Rey Hernández como Técnico de Gestión de Sistemas.
- Por parte de la fundación In-nova: Esther Álvarez Gonzalez como responsable de investigación en la parte de telecomunicaciones y responsable del análisis de la situación en materia de privacidad en la región latinoamericana.

Adicionalmente, y dada la complejidad del proyecto, se recurrió al apoyo de dos de los mayores grupos de investigación existentes en España:

- El Grupo Alarcos, liderado por Mario Piattini Velthuis, al ser uno de los principales referentes en investigación en el campo de la Ingeniería de Software a nivel mundial.
- El Grupo GSyA, liderado por Eduardo Fernandez-Medina Patón, al ser uno de los principales referentes en investigación en el campo de la Gestión de la Seguridad a nivel mundial.

El proyecto se denomino inicialmente GeCo (Gestión de Colas), y se renombró en 2010 bajo el nombre comercial de citaSalud (www.citaSalud.es), siendo la primera solución integral de gestión de esperas hospitalarias que permite racionalizar el flujo de los pacientes dentro de los hospitales, a partir del registro de los mismos mediante DNIe o tarjeta Sanitaria, cumpliendo con la privacidad de la información y por tanto con la LOPD.

Para la solución planteada se decidió analizar la problemática específica de cada uno de los objetivos de forma separada y posteriormente unificar las soluciones parciales en una solución global:

- Análisis objetivo 1: Para afrontar el primer objetivo, orientado a mantener la confidencialidad de los pacientes, se analizaron las diferentes medidas que se habían tomado a nivel mundial en materia de privacidad y legislación relacionada con la protección de datos de los pacientes, así como lo que se estaba haciendo en otros Hospitales Españoles. La conclusión a las que se llegó es que actualmente la mayor parte de los hospitales seguían sin resolver esa problemática. En la mayor parte de los hospitales revisados, el sistema de funcionamiento a la hora de citar a los pacientes en las consultas era publicar un tablón fuera de la misma con la lista de pacientes citados, y una enfermera procedía cada cierto tiempo a llamar por su nombre a cada nuevo paciente para que entrara en la consulta. Esta forma de funcionar producía dos graves problemas: El incumplimiento total de la LOPD y, por tanto, de la privacidad de los pacientes, ya que toda persona podía conocer el nombre y apellidos de las personas que asistían a cada consulta, y por otro lado que la mayor parte de la gente se posicionaba en los alrededores de las consultas para poder oír bien su nombre y las salas de esperas se mantenían vacías, mientras que los pasillos que daban acceso a las consultas sufrían bloqueos por la acumulación de pacientes, lo que derivaba en un aumento de estrés tanto de los pacientes como del personal encargado de gestionar las listas. Además, las personas con discapacidades (muletas, sillas de rueda, etc.) no podían tener libre acceso hasta las consultas.
- Solución objetivo 1: La solución pasaría por asignar a cada persona un número o código alfanumérico, en lugar de llamarla por su nombre.
- Análisis objetivo 2: Como hemos comentado anteriormente, uno de los principales problemas al gestionar las colas de los pacientes en los ambientes sanitarios, es que éstas no son independientes, sino que están interrelacionadas. Un paciente es recibido en una consulta de medicina general, y posteriormente derivado a una consulta de especialización donde le realizan una prueba específica. Posteriormente, el paciente tiene que regresar a la consulta de medicina general y pedir permiso al resto de pacientes que están esperando para entrar. Este flujo está interrelacionado con los problemas plateados en el objetivo 1, especialmente el alto nivel de estrés derivado de la situación provocaba que frecuentemente se prodijeran problemas de entendimiento entre los pacientes. Algunos hospitales habían intentado solucionar este problema poniendo colas genéricas y números consecutivos, pero esa solución terminaba presentado

otras problemáticas adicionales, como que los pacientes estimaran el tiempo que tardarían en atenderlos en base a los números restantes, o que cuando regresaban de un servicio al que eran derivados tenían que obtener otros números, o ponerse en la puerta y esperar a que el médico saliera para poder entrar, lo que derivaba en nuevos conflictos con los pacientes que estaban esperando. No se detectó ningún hospital que hubiera encontrado una solución satisfactoria.

- Solución objetivo 2: La solución no es trivial, ya que se debe tener en cuenta la "picaresca" de los pacientes que calculan los números restantes para aprovechar el tiempo y después intentan colarse si han perdido su turno. Otra modalidad de pacientes que se identificó calculaba su número y dejaba de prestar atención, dedicándose a iniciar conversaciones, que evitaban que el resto de pacientes pudieran oír su cita. Además, la interrelación de colas debería hacer que un paciente pueda reincorporarse con el mismo número sin que ello levante suspicacias en el resto de pacientes. Por lo tanto la solución está en definir un algoritmo que genere identificadores para los pacientes formados por letras y números y que estos no puedan encontrar la secuencia de generación, de forma que se vean obligados a mantener el silencio, prestar atención y no puedan cuestionar las decisiones de los médicos a la hora de alterar el orden de llegada en base a decisiones de urgencias medicas, o de derivaciones a especialidades.
- Análisis objetivo 3: El tercero de los objetivos se plateó como necesario, aunque se podría implementar en una fase posterior. Se trataba de encontrar una forma de autenticar a los pacientes a la hora de darles su número, teniendo en cuenta que el sistema no contaría con personas que pudieran verificar su identidad. Por lo tanto, se tenía que encontrar algún sistema que contuviera un certificado de autenticación y que a la vez fuera sencillo de utilizar, dado que los usuarios no eran expertos en tecnología.
- Solución objetivo 3: En este caso se encontró una solución para el caso español, aunque más difícil de implementar a nivel mundial. Actualmente, España es un país pionero en la implantación del eDNI [29] con más de 30.000.000 de eDNI repartidos entre sus ciudadanos. Esto permite seleccionar este documento como estándar para dar la cita y evitar errores a la hora de determinar las consultas. El eDNI tiene la ventaja de contener dos certificados (Autenticación y Firma), y tiene validez legal según la Ley de Firma Electrónica Española 59/2003. Este es un documento que obligatoriamente se tiene que portar, según la legislación Española, por lo que se convierte en el documento ideal para que una persona pueda obtener su cita, tan sólo introduciendo el eDNI en un dispositivo físico que le expedirá el ticket con el que realizará todo el proceso medico.
- Análisis objetivo 4: La situación mundial de estancamiento económico requería que la solución que se planteara tuviera un coste muy reducido y ayudara al sector sanitario a dar un mejor servicio a los ciudadanos, sin que ello se tradujera en un mayor coste. Para solucionar este objetivo se analizaron dos aspectos principales: los costes de la solución (Hardware y Software) y los ahorros que podía ofrecer la solución en horas internas de gestión del personal de administración.
- Solución objetivo 4: Los costes asociados al Hardware se redujeron lo máximo posible, siempre manteniendo la calidad necesaria y obligada por el cumplimiento de las normas de seguridad especificadas en ambientes sanitarios. Respecto al Software, se implementó una solución basada en tecnología Open Source que evitaba los costes de licencias y suponía importantes ahorros de coste. Finalmente, la integración con los sistemas HIS del Hospital permitió que cada implantación ahorrara el trabajo de un administrativo, ya que el sistema realizaba de forma automática labores que antes tenían que hacerse manualmente. Esto hizo que el ROI calculado fuera de unos 6 meses, mientras que el ROI medio en soluciones tecnológicas es de 5 años, lo que supone que la solución planteada no sólo mejoraba la calidad del servicio, sino que en un periodo de tiempo muy corto permitía que los sistemas hospitalarios ahorraran dinero.
- Análisis objetivo 5: Del lado del paciente, el sistema está orientado a personas mayores, por lo que tenía que ser muy sencillo de utilizar y entender, teniendo en cuenta que podía ser utilizado por personas analfabetas, o inmigrantes que no hablaran Castellano, etc. Del lado del médico, el sistema debía ser capaz de tomar decisiones y poder citar a los pacientes de una forma sencilla, sin que el nuevo sistema supusiera mayor carga de la ya soportada.
- Solución objetivo 5: La solución planteada pasaba por integrar un kiosco de expedición de tickets que permitiera eDNI en el caso de gente que no pudiera escribir sus datos de identificación, o por motivos de comodidad no quisiera hacerlo, y posteriormente el número de ticket que se emitía sería locutado en varios idiomas adaptados a las poblaciones lingüísticas mayoritarias asignadas a ese hospital.
- Análisis objetivo 6: El proyecto debería ser escalable para poderse integrar con el resto del HIS Hospitalario, y poder crecer con nuevas funcionalidades. Para ello se analizaron diferentes arquitecturas software, en colaboración con los expertos de Ingeniería del Software del grupo de investigación Alarcos.
- Solución objetivo 6: Finalmente se determinó una arquitectura abierta y escalable, basada en Java, que permitía enlazar de una forma sencilla mediante

servicios Web con el HIS Hospitalario.

- Análisis objetivo 7: En un sector como el sanitario, es vital que las soluciones tecnológicas que se desarrollen sean seguras, ya que una caída del sistema puede suponer el bloqueo de toda la operativa del hospital. De igual forma, el acceso a la información del sistema puede poner en riesgo la privacidad de los datos personales.
- Solución objetivo 7: Para solucionar este problema se contó con el grupo de investigación GSyA, especializado en Seguridad, y se adoptó la metodología MEDUSAS (Mejora y Evaluación del Diseño, Usabilidad, Seguridad y mAntenibilidad del Software), que permitió verificar que la implantación realizada cumplía con los estándares de seguridad, además de los de mantenibilidad y usabilidad.

El análisis realizado sobre cada objetivo y la solución planteada dió lugar a la solución final de lo que hoy se denomina citaSalud (www.citasalud.es), la cual está formada por un terminal de autoservicio, un sistema de cartelería electrónica, un servidor de locuciones y un software de agenda médica y de informes que integran directamente con el sistema de gestión hospitalaria, garantizando la llamada anónima y contribuyendo a la mejora de la calidad de servicio y el cumplimiento de la LOPD. Frente a los sistemas tradicionales de gestión de colas, citaSalud ofrece una arquitectura 100% web totalmente integrada con el eDNI y el sistema de gestión hospitalario, lo que permite reducir costes administrativos, mejorar los tiempos de recepción de pacientes y obtener una información muy valiosa para la futura mejora de otros procesos.

Figura 2. Sistema de emisión de tickets.

A partir de esta visión de la situación actual del mercado y de las necesidades de seguridad de las empresas, se ha centrado el objetivo de esta investigación en elaborar una solución que permita citar pacientes cumpliendo con los requerimientos legales impuestos por la LOPD y los objetivos enunciados inicialmente.

De forma general, el sistema de gestión de esperas citaSalud es una solución software-hardware compuesta por:

- Un sistema de emisión de tickets (Fig. 2) que está formado por un terminal de Autoservicio (Terminal táctil) que admite tarjeta sanitaria, DNI y Código de barras de cita.
- Un sistema de pantallas informativas personalizables (Fig. 3) que incluye: i) el Grid de pacientes en consulta; ii) llamada a consulta; iii) mensajes informativos; iv) incidencias; y v) videos informativos.

Figura 3. Pantallas informativas.

- Un servidor de locuciones (Fig. 4) que ofrece las siguientes ventajas: i) utiliza los altavoces de las pantallas; ii) servidor de conversión texto-voz; iii) posibilidad de varias voces; iv) traducción de locuciones a varios idiomas; v) funcionalidad de locuciones con traducción dinámica para médicos en consulta.

Figura 4. Servidor de locuciones multi-idioma.

- Un software de agenda médica (Fig. 5): Contiene información de pacientes citados (Nombre y tiempo de espera, Historial, Estado: En espera, ausente, en especialidad, resultados listos) y permite la interacción con los pacientes (Llamada a paciente, Devolver a la sala de espera, Derivación a especialidad y Finalización Consulta).

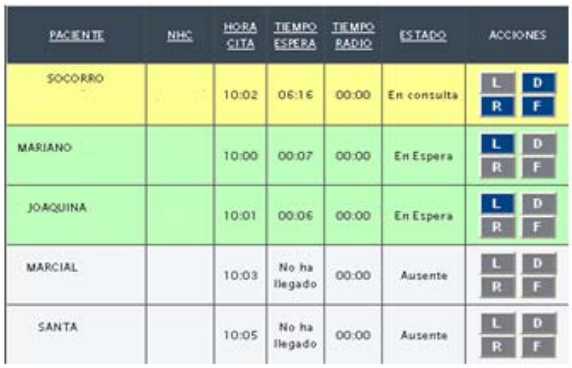

Figura 5. Software de agenda medica.

- Un sistema de generación de informes (Fig. 6): basado en la solución de inteligencia de negocio y sustentado en la herramienta Open Source Pentaho.

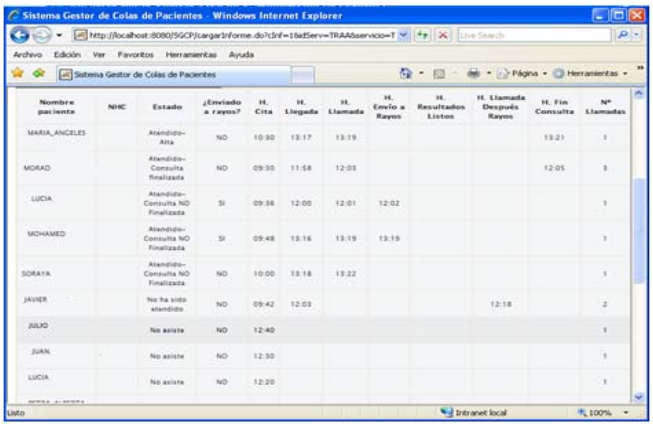

Figura 6. Sistema de generación de informes.

Conectados entre sí a través de protocolo HTTP según el esquema que se muestra en la Fig. 7:

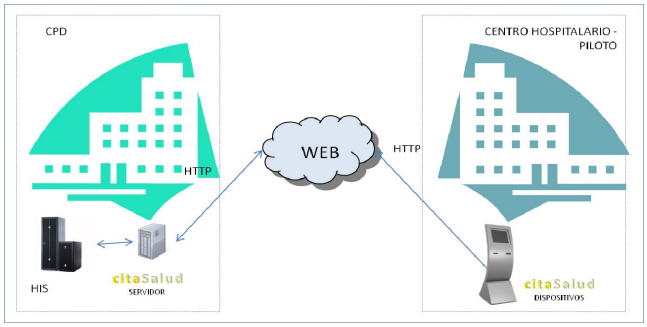

Figura 7. Mecanismo de conexión de citaSalud en un sistema multicentro.

Dentro del Hospital se instalarán dispositivos en las salas de espera así como en la zona de admisión según el siguiente esquema de la Fig. 8.

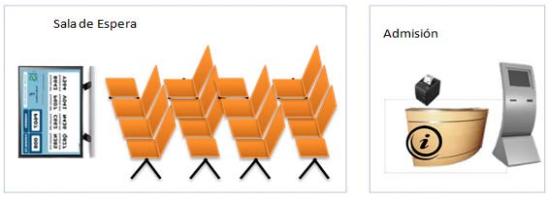

Figura 8. Distribución física de citaSalud.

Toda la identificación de los pacientes en el centro hospitalario se realiza en el sistema citaSalud a través de un lector de tarjetas híbrido, que admite tarjeta sanitaria y DNI electrónico. De esta forma, a través del DNI electrónico cualquier paciente se identifica de forma única en cualquier centro hospitalario. Para ello se ha desarrollado un módulo que integra el dispositivo lector de tarjetas con el sistema de gestión hospitalario.

El sistema citaSalud incorpora las siguientes funcionalidades:

- Llamada anónima a consulta: El sistema permitirá llamar al paciente de una forma anónima a través de un identificador o número de ticket de manera que se cumpla con la normativa LOPD que obliga a no publicar ni difundir los nombres de las personas que acuden a consulta.
- Solicitud de turno de forma confidencial: La solicitud del turno se realizará a través de un terminal de autoservicio o directamente en el punto de información lo que garantiza que para obtener turno en consulta el paciente no necesite mencionar en público el nombre de la consulta a la que asiste preservando su derecho a la intimidad.
- Gestión automática de colas de esperas: El servidor citaSalud proveerá de un sistema de gestión de colas que proponga al médico o enfermero de forma automática la siguiente persona a la que llamar a consulta. De esta forma, el sistema garantiza que los pacientes en espera serán atendidos de forma óptima y siguiendo los mismos criterios, independientemente de la consulta a la que se asista.
- Priorización de pacientes: Dependiendo de las circunstancias y a criterio del médico este podrá priorizar el paso a consulta de los pacientes que desee, sin que esto se evidencie entre el resto de pacientes que está en espera. Esta funcionalidad permite atender a pacientes que necesiten ser atendidos de forma urgente y soliciten cita el mismo día.
- Generación manual y automática de tickets: Los tickets que indican el turno a los pacientes podrán ser generados de forma automática a través de un terminal de autoservicio, o de forma manual y asistida a través de los celadores distribuidos en los puntos de información que se destinen a tal fin. Esta dualidad en la forma de emitir tickets, permite garantizar la alta disponibilidad del sistema en situaciones en las que no

se encuentre disponible algún dispensador de tickets.

- Autoservicio: El terminal de autoservicio permitirá que los pacientes soliciten turno de forma automática. El terminal con pantalla táctil ofrece también la posibilidad de incorporar otras aplicaciones on-line del centro o corporativas dirigidas a los pacientes.
- Conexión con el sistema de gestión hospitalaria: El sistema citaSalud se comunicará con el sistema de gestión hospitalaria. Esta comunicación deberá permitir a citaSalud: i) Obtener los datos de los servicios activos en el centro; ii) Consultar las agendas de todas las consultas de cada uno de los servicios y iii) Disponer de la información relativa a los resultados de pruebas clínicas solicitadas para un paciente derivado a dichas pruebas en el transcurso de una consulta (Sólo en la versión para centros Hospitalarios).
- Enlace con la historia clínica electrónica: La agenda médica de citaSalud permite enlazar con el historial clínico electrónico. Mediante un enlace disponible sobre el Número de Historia Clínica (NHC) que se muestra para cada paciente incluido en la agenda, de forma que el facultativo puede acceder al mismo de forma inmediata.
- Llamada automática de pacientes: A través de un botón de la agenda médica de citaSalud, los médicos o enfermeros podrán llamar de forma automática al siguiente paciente que deba pasar a consulta, sin necesidad de presenciarse en la sala de espera. Mediante esta funcionalidad, el número de ticket y la consulta a la que el paciente debe acudir a consulta se presentará en el monitor de la sala de espera, agilizando la llamada a consulta.
- Gestión de ausencias: El sistema proporcionará en tiempo real el estado de los pacientes que: o bien no han acudido al centro, o bien han acudido después de su hora de citación, dándole el tratamiento adecuado y actualizando las estadísticas según corresponda en cada uno de los casos.
- Devolución a sala de espera: En aquellos casos en los que después de llamar a un paciente este no acuda a consulta, el médico o enfermero podrá realizar una "devolución a sala de espera". Mediante esta funcionalidad el responsable de la consulta podrá llamar al paciente varias veces de forma que se garantice: i) No queden pacientes "huérfanos" esperando ser atendidos; ii) No pierdan su turno aquellos pacientes que habiendo acudido a consulta no hayan estado atentos a su llamada o se hayan ausentado de forma momentánea de la sala de espera.
- Derivación automática desde consulta a pruebas médicas: El sistema permite, a los médicos o enfermeros, enviar a los pacientes que lo necesiten a consultas especiales para la realización de pruebas médicas (radiología, ecografía, etc.) en el mismo día. Dichos pacientes podrán volver a ser atendidos y llamados a consulta una vez que los resultados de las pruebas consten en el sistema informático del hospital.
- Informes históricos de atención de pacientes en consulta: El sistema almacenará toda la información histórica de los pacientes que han sido citados para consulta. Se podrán consultar informes con la siguiente información filtrando por: servicio, agenda médica y día y obteniendo la siguiente información: i) Hora a la que fue citado el paciente; ii) Hora a la que acudió al centro médico / hospital; iii) Hora a la que fue llamado y número de llamadas; iv) Hora a la que fue atendido; v) Hora a la que fue derivado para la realización de pruebas; vi) Hora a la que los resultados de las pruebas estuvieron disponibles; vii) Hora a la que fue vuelto a llamar después de realizarse las pruebas; y viii) Hora de finalización de consulta.
- Estadísticas de tiempo de espera y tiempo en consulta: Podrá consultarse por agenda médica y día la siguiente información estadística agregada: i) Total de pacientes atendidos; ii) Total de pacientes que no acudieron; iii) Total de pacientes derivados a consultas; iv) Tiempo medio de espera por paciente después de la hora de citación; v) Tiempo medio de espera por paciente previo a la hora de citación; y vi) Tiempo medio de atención en consulta por paciente.
- Información en tiempo real de las personas que asisten a consulta: El sistema proveerá información en pseudo-tiempo real (1 min.) del estado de los pacientes citados a consulta: i) Citados: Aún no ha llegado la hora de citación y no se han registrado en el centro; ii) En espera: Han recogido su ticket están esperando ser atendidos; iii) Ausentes: No han acudido al centro o no han recogido ticket; iv) Derivados a pruebas: Tras ser atendidos en consulta han sido derivados a otra consulta para realizarse pruebas médicas. (Solo versión para centros hospitalarios); v) Resultados listos: Los resultados de las pruebas solicitadas para el paciente están listos y el paciente está disponible para ser llamado de nuevo a consulta. (Solo versión para centros hospitalarios); vi) Finalizado: Se ha finalizado la consulta; y vii) Devuelto a espera: El paciente se ha identificado y tiene ticket pero no ha respondido a la llamada de su turno.
- Locución de llamadas a pacientes: Opcionalmente el sistema citaSalud puede emitir una locución para cada paciente que es llamado a consulta. Esta funcionalidad permite que los pacientes que no tengan una buena visibilidad de la pantalla por diferentes motivos puedan recibir igualmente la información que se muestra en pantalla. Igualmente soluciona el problema del idioma en zonas con una parte importante de población extranjera.
- Por otro lado, los objetivos referidos a escalabilidad y seguridad se solucionaron utilizando una arquitectura de desarrollo basada en tecnología Open Source (Fig. 9).

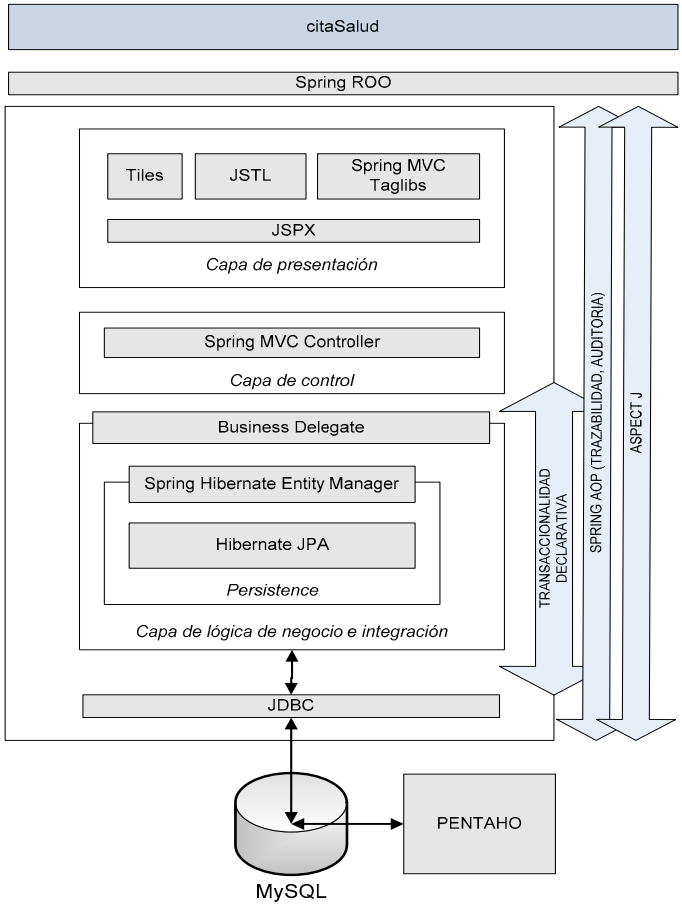

Figura 9. Arquitectura de desarrollo de citaSalud.

V. FUNCIONAMIENTO DE LA SOLUCIÓN

La solución planteada se ha enfocado para que tenga un funcionamiento sencillo orientado a la diversidad de los usuarios. A continuación se muestra el funcionamiento de las diferentes fases de la solución planteada:

- Fase I (ver Fig. 10): El paciente llega al hospital y solicita en admisión por medio de su tarjeta sanitaria o su eDNI el ticket de la cita que previamente ha solicitado por internet. Una vez recibido el ticket, el paciente pasa a la sala de espera hasta que llegue su turno. Internamente, cuando el paciente solicita el ticket el sistema realiza cuatro pasos: i) conecta admisión con el HIS Hospitalario para confirmar que el paciente tiene una cita previa; ii) Asigna al paciente su número de ticket; iii) citaSalud actualiza los datos de la pantalla; y iv) se actualizan las agendas de los médicos y las estadísticas del sistema.

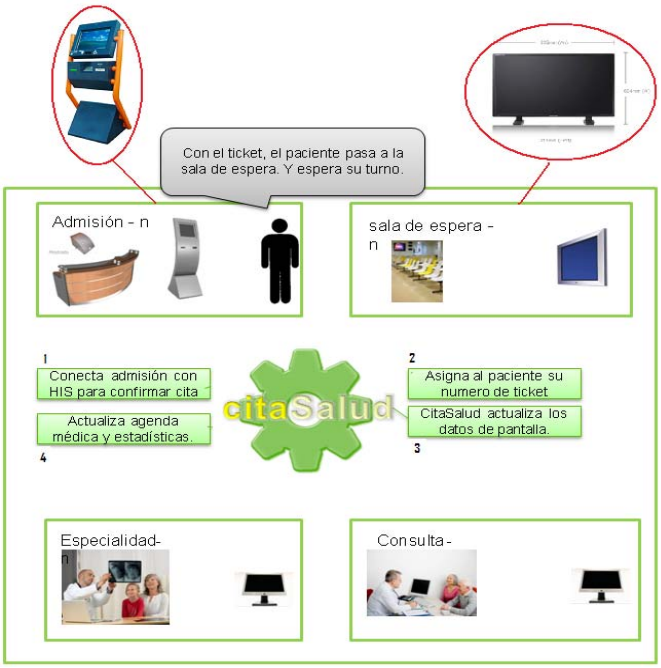

Figura 10. Fase I. Funcionamiento de citaSalud.

- Fase II: Una vez que el sistema ha verificado la cita y emitido el ticket, al médico le aparece en su terminal el nuevo paciente, con un código de color asignado. El médico puede dar paso al siguiente paciente, o por razones medicas adelantar a un paciente en la lista, siempre teniendo en cuenta que se guardará información de trazabilidad de las alteraciones que realice en la lista con respecto al algoritmo previamente definido, para las auditorías internas posteriores.

Figura 11. Fase II. Funcionamiento de citaSalud.

- Fase III: El paciente ve y escucha su número en el monitor de la sala de espera, indicándole la consulta a la que tiene que dirigirse.

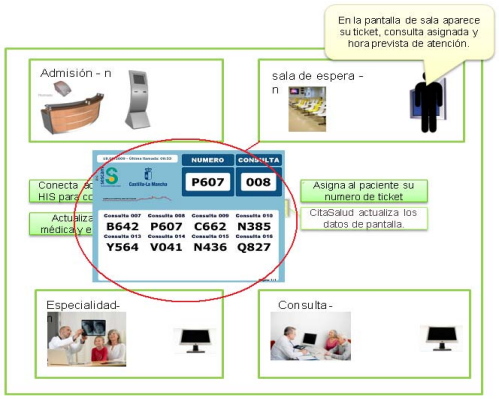

Figura 12. Fase III. Funcionamiento de citaSalud.

- Fase IV: El médico recibe al paciente y determina si finaliza el caso o lo deriva a un médico de especialidad. En este segundo caso, el paciente irá con el mismo ticket a la consulta de especialidad. Una vez realizada la prueba se marchara de nuevo a la sala de espera, y cuando los resultados prueba estén disponibles el sistema cambiará el estado, de forma que el paciente volverá a aparecer automáticamente en el sistema de espera.

VI. Ventajas y Mejoras para la Organización

La implantación del sistema de citaSalud ayudó a solucionar los 7 objetivos propuestos inicialmente. Las principales ventajas que obtiene una organización con la solución propuesta son:

- Evita sanciones por incumplimiento de LOPD: La implantación del sistema citaSalud en los hospitales permite asignar un número de ticket a toda la persona que acude a la consulta para de esta forma realizar una llamada anónima al paciente preservando la intimidad y evitando sanciones.
- Mejora la agenda de los médicos: Con el objetivo de mejorar la gestión de las agendas médicas, citaSalud provee a los médicos de una aplicación web que visualiza en tiempo real la lista de pacientes citados a su consulta y el estado de los mismos: en espera, ausente, etc. Mediante esta aplicación, el médico o enfermero puede llamar a un paciente a su consulta directamente desde su terminal haciendo que el número de ticket aparezca en el monitor de la sala. De esta forma los pacientes acuden a su consulta sin intervención de los auxiliares o enfermeros.
- Mejora de la calidad de servicio: La provisión de datos en tiempo real, el registro de datos históricos y los informes sobre el tiempo en espera y el tiempo en consulta de los pacientes ha ayudado significativamente a mejorar la calidad global del servicio médico.
- Ahorro de costes: citaSalud contribuye a ahorrar costes optimizando los recursos humanos y físicos destinados a la gestión de colas de espera. De esta forma y facilitando el autoservicio se permite que los profesionales médicos dediquen su tiempo a labores de mayor valor añadido dentro del centro hospitalario garantizando un rápido retorno de la inversión.
- Para analizar con mayor detalle estas ventajas se ha realizado un análisis DAFO de la solución (Tabla 1).

TABLA I. COMPARICIÓN DE CITASALUD CON OTRAS SOLUCIONES ANALIZADAS.

	Debilidades	**Fortalezas**
citaSalud	• Requiere un proceso de integración.	• Integra con el sistema de gestión hospitalaria. • Admite tarjeta sanitaria y DNIe • Solución integral: Hardware y software. • Arquitectura 100% web
Otros sistemas de gestión de esperas.	• No integra con el sistema de gestión hospitalaria. • No utilizan DNIe. • Arquitectura cliente-servidor	• La implantación es más rápida.
	Amenazas	**Oportunidades**
citaSalud	• Dificultades para integrar aplicaciones de terceros con el sistema de gestión hospitalaria.	• Uso cada vez mayor del DNIe. • Acceso mediante DNIe a otros servicios en línea del hospital. • Necesidad de integrar con el sistema de gestión hospitalaria.
Otros sistemas de gestión de esperas.	• Utilización cada vez mayor del DNIe. • Necesidad de integrar con el sistema de gestión hospitalaria.	

VII. Conclusiones y trabajos futuros

En este artículo se ha presentado un caso real de éxito realizado sobre el Hospital Virgen de la Salud de Toledo (España) de una investigación iniciada en 2007 y cuya primera fase ha finalizado en 2010.

En el artículo también se ha presentado una parte de la solución implantada, centrada en los pacientes. Existen otras partes de la investigación que por motivos de espacio no han podido ser expuestas en el presente artículo.

Aunque la investigación se inicio en 2007, la problemática sigue existiendo actualmente en todo el sector sanitario, y es de gran importancia abordarla al afectar a la privacidad de la información de los pacientes, al nivel de satisfacción de los mismos y suponer grandes costes para el sistema sanitario.

Además de todas las ventajas expuestas en el apartado anterior, el proceso implementado ha permitido detectar desviaciones significativas en la operativa médica, ayudando también a mejorar su forma de trabajo.

Las características ofrecidas por el proceso y su orientación a solucionar un problema de alto impacto social como es la privacidad de los datos personales de los pacientes han hecho que sea muy bien recibida en todo el sector sanitario, tanto por los pacientes como por el personal sanitario. Además, con este proceso se obtienen resultados a corto plazo y se reducen los riesgos de seguridad y costes de gestión, además de ayudar a reducir los niveles de estrés y aumentar el nivel de satisfacción del servicio prestado.

Actualmente se está analizando la posibilidad de integrar este proceso dentro de la metodología de Gestión de la Seguridad denominada MGSM [30-33], y de la herramienta que da soporte a la metodología [34], como parte del proceso global de Gestión de Seguridad que soportan los SGSIs en el sector sanitario.

La primera fase de la investigación ha sido un éxito al cumplir con todos los objetivos inicialmente planteados, y actualmente ya se encuentra en fase de comercialización a nivel internacional bajo la marca citaSalud (www.citaSalud.es). Las dos grandes líneas derivadas de esta investigación pretenden, por un lado, integrar este proceso relacionado con la privacidad de los pacientes con el resto del sistema del SGSI Hospitalario, ayudando a determinar otros aspectos que pongan en riesgo la información sanitaria y que actualmente no se estén contemplando, y como segunda línea la extracción de inteligencia de negocio de toda la información que se está recogiendo en el sistema para determinar nuevos mecanismos de ofrecer un servicio más seguro y de mayor calidad a los pacientes, pero siempre con un ROI a muy corto plazo, de forma que esas mejoras no se traduzcan en mayores costes.

Finalmente, mencionar que el proyecto hubiera sido imposible de realizar sin la ayuda prestada por todos los equipos de trabajo que se han involucrado en el proyecto, en especial por la ayuda prestada por el equipo de informática, médicos y administrativos del Hospital Virgen de la Salud de Toledo (España).

AGRADECIMIENTOS

Agradecimiento especial a todo el equipo informática del hospital Virgen de la Salud de Toledo, que ha participado en el desarrollo de la investigación y ha servido de centro piloto para la implantación del mismo. Esta investigación es parte de los proyectos MEDUSAS (IDI-20090557) y ORIGIN (IDI-2010043) financiado por el CDTI y el FEDER, BUSINESS (PET2008-0136) concedido por el Ministerio Español de Ciencia y Tecnología y MARISMA (HITO-2010-28), SISTEMAS (PII2I09-0150-3135) y SERENIDAD (PII11-0327-7035) financiado por la Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-la Mancha.

Referencias

[1] Kluge, D. *Formal Information Security Standards in German Medium Enterprises.* in *CONISAR: The Conference on Information Systems Applied Research*. 2008.

[2] Dhillon, G. and J. Backhouse, *Information System Security Management in the New Millennium.* Communications of the ACM, 2000. **43**(7): p. 125-128.

[3] Park, C.-S., S.-S. Jang, and Y.-T. Park, *A Study of Effect of Information Security Management System[ISMS] Certification on Organization Performance.* IJCSNS International Journal of Computer Science and Network Security., 2010. **10**(3): p. 10-21.

[4] Barlette, Y. and V. Vladislav. *Exploring the Suitability of IS Security Management Standards for SMEs*. in *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual*. 2008. Waikoloa, HI, USA.

[5] Fal, A.M., *Standardization in information security management* Cybernetics and Systems Analysis 2010. **46**(3): p. 181-184.

[6] Wiander, T. and J. Holappa, *Theoretical Framework of ISO 17799 Compliant. Information Security Management System Using Novel ASD Method.*, in *Technical Report*, V.T.R.C.o. Finland, Editor. 2006.

[7] Parente, S. and R. Loureiro, *Safety and Security in Professional and Non-Professional E-Health and Their Impact on the Quality of Health Care*, in *E-Health Systems Quality and Reliability: Models and Standards* I. Global, Editor. 2010. p. 118-124.

[8] Wiander, T. *Implementing the ISO/IEC 17799 standard in practice – experiences on audit phases.* in *AISC '08: Proceedings of the sixth Australasian conference on Information security.* 2008. Wollongong, Australia.

[9] Lomprey, G.R., *Critical Elements of an Information Security Management Strategy*, C. Report, Editor. 2008.

[10] Pardo, G.O., *Legal problems associated with the health information. The Clinical History.*, in *Cuad. Bioét. XVII*. 2006.

[11] Iraburu, M., *Confidentiality and privacy.* Anales del Sistema Sanitario de Navarra, 2006. **29**(3).

[12] Ferrer-Roca, O., F. Marcano, and A. Diaz-Cardama, *Quality labels for e-health*, in *IET Communications. Telemedicine and E-Health Communication Systems.* 2008, The Institution of Engineering and Technology. p. 202-207.

[13] HIPAA (2008) *Medical Dictionary Definition Retrieved May 20, 2008 from*. **Volume**,

[14] Woo-Sung Park, et al., *Analysis of Information Security Management Systems at 5 Domestic Hospitals with More than 500 Beds.* HIR - Healthc Inform Research, 2010: p. 90-99.

[15] Özkan, Ö., *Attitudes and opinios of people who use medical services about privacy and confidentiality of health information in electronic environment*, in *Medical Informatics*. 2011.

[16] Moreno, J.X.H., M.d.M.P. Velasco, and À.S. Viñolas, *Reflexiones en torno a la protección de datos de carácter personal.* NUEVAS POLÍTICAS PÚBLICAS. Anuario multidisciplinar para la modernización de las Administraciones Públicas, 2005.

[17] Zhao, L. and B. Lie, *Modeling and Simulation of Patient Flow in Hospitals for Resource Utilization*, in *49th Scandinavian Conference on Simulation*. 2008.
[18] Guarda, P., *Data Protection, Information Privacy, and Security Measures: an essay on the European and the Italian Legal Frameworks*. Ciberspaizo e dir., 2008: p. 65-92.
[19] Purtova, N., *Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights*. Netherlands Quarterly of Human Rights, 2010. **28**(2): p. 179-198.
[20] Canales Gil, A., *El derecho fundamental a la protección de datos de carácter personal*, in *Revista Jurídica de Castilla y León*. 2007.
[21] AGPD, *Cuadro comparativo: Desarrollos normativos nacionales en materia de protección de datos.*, in *III Encuentro Iberoamericano de Protección de datos.*, R.I.d.P.d. Datos., Editor. 2004.
[22] Cavoukian, A. and P.G. Rossos, *Personal Health Information: A Practical Tool for Physicians Transitioning from Paper-Based Records to Electronic Health Records*. Information and Privacy Commissioner of Ontario, 2009.
[23] Cavoukian, A. and K.E. Emam, *A Positive-Sum Paradigm in Action in the Health Sector*. PbD. , 2010.
[24] Sarabdeen, J. and M. Ishak, *E-health Data Privacy: How far is it protected?* Communications of the IBIMA, 2008. **1**: p. 110-117.
[25] Horie, S., et al., *Handling of workers' health information by employers in compliance with Personal Information Protection Law in Japan* International Congress Series, 2006. **1294**: p. 205-208.
[26] Mital, K.M., *Queuing analysis for outpatient and inpatient services: a case study*. Management Decision, 2010. **48**(3): p. 419 - 432.
[27] Belson, D., *Managing a Patient Flow Improvement Project*. International Series in Operations Research & Management Science, 2006. **91**: p. 429-452.
[28] Creemers, S. and M. Lambrecht, *Healthcare queueing models*, F.o.B.a.E.D.o.D.S.a.I.M. (KBI). Editor. 2008: Belgium.
[29] INTECO, *DNI Electrónico. Acercándote la Administración.*, I.I.N.d.T.d.l. Comunicacíon., Editor. 2010.
[30] Sánchez, L.E., et al. *Security Management in corporative IT systems using maturity models, taking as base ISO/IEC 17799*. in *International Symposium on Frontiers in Availability, Reliability and Security (FARES'06) in conjunction with ARES*. 2006. Viena (Austria).
[31] Sánchez, L.E., et al. *MMISS-SME Practical Development: Maturity Model for Information Systems Security Management in SMEs*. in *9th International Conference on Enterprise Information Systems (WOSIS'07)*. 2007b. Funchal, Madeira (Portugal). June.
[32] Sánchez, L.E., et al. *Developing a model and a tool to manage the information security in Small and Medium Enterprises*. in *International Conference on Security and Cryptography (SECRYPT'07)*. 2007a. Barcelona. Spain.: Junio.
[33] Sánchez, L.E., et al. *Developing a maturity model for information system security management within small and medium size enterprises*. in *8th International Conference on Enterprise Information Systems (WOSIS'06)*. 2006. Paphos (Chipre). March.
[34] Sánchez, L.E., et al. *SCMM-TOOL: Tool for computer automation of the Information Security Management Systems*. in *2nd International conference on Software and Data Technologies (ICSOFT'07)*. . 2007c. Barcelona-España Septiembre.

Luis Enrique Sánchez is PhD and MsC in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla-La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Professional Services and R&D departments of the company Sicaman Nuevas Tecnologías S.L. COIICLM board or committee member and responsible for the professional services committee. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Antonio Santos-Olmo is MsC in in Computer Science and is an Assistant Professor at the Escuela Superior de Informática of the Universidad de Castilla- La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain), MSc in Information Systems Audit from the Polytechnic University of Madrid, and Certified Information System Auditor by ISACA. He is the Director of Software Factory departments of the company Sicaman Nuevas Tecnologías S.L. His research activities are management security system, security metrics, data mining, data cleaning, and business intelligence. He participates in the GSyA research group of the Department of Computer Science at the University of Castilla- LaMancha, in Ciudad Real (Spain). He belongs to various professional and research associations (COIICLM, ATI, ASIA, ISACA, eSEC, INTECO, etc).

Esther Álvarez President of Private Foundation In-nova and Research of the UPM. Consultant in strategic communications programs radio, mobile and wireless both public and private sectors and in civil and military. Currently a member of the board of the Delegation of COIT (Association of Telecommunications Engineers) CLM, representative of Castilla La Mancha in the groups of the free and COIT New Technologies of the National Coordinator of the Treatment Research Chair in Digital Image at the Madrid Polytechnic University of Madrid. PhD in Information Systems specializing in Business ETSI Industriales (UPM) and the Specialty Program Communications Signals, Systems and Radiocommunications Department SSR ETSI Telecomunicaciones (UPM). It Telecommunications Engineering from UPM. Specialty Communications..

Eduardo Fernández-Medina holds a PhD. and an MSc. in Computer Science from the University of Sevilla. He is an Associate Professor at the Escuela Superior de Informática of the University of Castilla-La Mancha in Ciudad Real (Spain) (Computer Science Department, University of Castilla La Mancha, Ciudad Real, Spain)- his research activity being in the field of security in information systems, and particularly in security in business processes, databases, datawarehouses, and web services. Fernández-Medina is co-editor of several books and chapter books on these subjects, and has published several dozens of papers in national and international conferences (BPM, UML, ER, ESORICS, TRUSTBUS, etc.). He is author of several manuscripts in national and international journals (Decision Support Systems, Information Systems, ACM Sigmod Record, Information Software Technology, Computers & Security, Computer Standards and Interfaces, etc.). He leads the GSyA research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain and belongs to various professional and research associations (ATI, AEC, AENOR, etc.).

Mario Piattini is MSc and PhD in Computer Science from the Technical University of Madrid and is a Certified Information System Auditor (CISA) and Certified Information Security Manager by ISACA (Information System Audit and Control Association). He is a professor in the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. Author of several books and papers on databases, software engineering and information systems, he leads the ALARCOS research group of the Department of Computer Science at the University of Castilla-La Mancha, in Ciudad Real, Spain. He is author of several books and papers on databases, security, software engineering and information systems. He leads the ALARCOS research group of the Department of Computer Science at the University of Castilla- La Mancha, in Ciudad Real (Spain). His research interests are: advanced database design, database quality, software metrics, object-oriented metrics and software maintenance.