HITA - Healthcare IT Audit

Nombre Estudiante: Urtzi Larrazabal Santos

Grado en Ingeniería Informática

Nombre Consultor: Xavier Martínez Munné

Data Entrega: 13/01/2016

FICHA DEL TRABAJO FINAL

Título del trabajo:	Healthcare IT Audit
Nombre del autor:	Urtzi Larrazabal Santos
Nombre del consultor:	Xavier Martínez Munné
Fecha de entrega (mm/aaaa):	13/01/2016
Área del Trabajo Final:	Gestión de proyectos informáticos
Titulación:	*Grado en Ingeniería Informática*

Resumen del Trabajo (máximo 250 palabras):

El objetivo de este trabajo, es diseñar y desarrollar un sistema mediante el cual los profesionales de IT de los hospitales puedan valorar los sistemas informáticos que se requieran implantar en su red. Hoy en día, prácticamente la totalidad de proyectos de *electromedicina*, *telemedicina*, gestión de infraestructuras, etc…incluyen sistemas que se deben conectar a la red informática, sin que estos cumplan con los niveles de seguridad, estabilidad, integridad o incluso disponibilidad que la organización estipula como necesarios.

El sistema desarrollado consta de una serie de formularios web referentes al proyecto a implantar, y que tanto el proveedor como el cliente podrán utilizar en cada proyecto, de manera que finalmente se genere un informe con valoraciones y puntuaciones sobre las fortalezas y debilidades del proyecto presentado.

Para su diseño, se ha consultado con profesionales de varios hospitales de ámbito nacional, así como con proveedores de soluciones y sistemas para hospitales. Tras estudiar toda la información recogida se ha realizado un diseño lógico del sistema a desarrollar, en base al cual se desarrollará la solución final.

En cuanto a la arquitectura del sistema, se han evaluado varias opciones para su desarrollo. Finalmente se ha descartado la opción de realizar una aplicación de escritorio, a favor del desarrollo de una aplicación web, debido a su mayor flexibilidad y compatibilidad con diferentes sistemas.

Abstract (in English, 250 words or less):

The purpose of this work is to design and develop a system that would enable the IT hospital professionals to value the network and computer systems that are required to be introduced in their network. Nowadays, almost all clinical engineering, telemedicine, infrastructure management projects, etc. include systems that need to be connected to the corporate network, even if these systems are not able to reach the security, stability, integrity or availability standards required by the company.

The developed system is made of several web forms regarding to the set up project, that both the supplier and the customer can use in each project, so that finally a report with ratings and scores on the strengths and weaknesses of the project submitted is generated.

For the purpose of the design of the project has been consulted professionals of several hospitals statewide and solution and systems providers for hospitals. After considering all the information gathered, it was made a logical system design to be developed, based on which the final solution will be carried out.

In terms of system architecture, several options for development have been evaluated. The option of making a rule application has finally ruled out. Instead, it has opted for the development of a web application, due to its greater flexibility and compatibility with different systems.

Palabras clave (entre 4 y 8):

Electromedicina, Ingeniería, Médica, Seguridad, Hospitales, Auditoria, Requisitos

Índice

Tabla de contenido

1.Introducción

1.1 Contexto y justificación del trabajo

Los hospitales son organizaciones donde la modernización de sus sistemas de *electromedicina* o ingeniería médica tradicionales, implica la implantación e integración de estos con los sistemas informáticos ya existentes. Esto no resulta sencillo cuando históricamente las compañías de soluciones de *electromedicina* y laboratorios, únicamente diseñan sistemas con un propósito y fin específico, sin importar el entorno en el que se implantan.

Pongamos el ejemplo de un analizador de hematología que analiza muestras y registra los resultados en su propio sistema o base de datos. A menudo ocurre que este tipo de sistemas no tiene en cuenta la integración del mismo en los sistemas principales ya existentes en el hospital. No se presta atención en cómo se cumplen con los requisitos necesarios respecto al diseño actual de la red informática, las políticas de seguridad establecidas en la organización, las obligaciones establecidas por la *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)*, además de la *Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica* o sin tener en cuenta la obligaciones de alta disponibilidad necesarias en un centro que trabaja 24x7x365.

Esta situación hace que los hospitales integren continuamente sistemas informáticos de forma inadecuada desde el inicio.

La integración y la interoperabilidad nunca han sido prioritarias en el desarrollo de las *HCE* (*Historia Clínica Electrónica*, en inglés *EHR*, por las siglas de *Electronic Health Record*), pero desde hace unos años esto ha pasado a ser de prioridad absoluta, ya que hoy en día prácticamente todos los hospitales disponen de una *Historia Clínica Electrónica (*Imagen 1)

Imagen 1. Historia clínica electrónica de primaria: implantación de sistemas que permiten consultar la HCE de toda la comunidad autónoma. SN 2006 -2011

(Red, 2012)

Por otro lado, generalmente de las HCE operan en redes cerradas y no se conectan fácilmente con otros sistemas externos. Históricamente además, los fabricantes de software han tenido pocos incentivos para abrir estos sistemas, a pesar de que un flujo libre de información y datos podría aportar grandes beneficios sobre la coordinación de la atención en salud entre diferentes sistemas y organizaciones. Digamos que en la mayoría de los casos, los sistemas se han desarrollado a medida según las necesidades de cada centro, así que ha existido siempre un escaso enfoque en el intercambio de información.

En definitiva, hoy en día casi cualquier equipo de ingeniería médica, o proyecto informático en un hospital, requiere la integración con la HCE y otros sistemas.

Para afrontar esta situación, existen una serie de estándares de comunicación para el intercambio electrónico de información clínica, como pueden ser *Web Services* de diseño a medida, el estándar *HL7*, el estándar *DICOM* para el intercambio, visualización, almacenamiento, impresión y transmisión de pruebas de imágenes, etc.

Pero además del cumplimiento con los métodos y estándares citados, debe existir un procedimiento de obligado cumplimiento para todo proyecto informático que requiera la implantación de un sistema en la red informática de cualquier hospital. Esto es así, tanto para proyectos clínicos que requieran la integración con la HCE, como proyectos de electromedicina que no lo requieran, incluso aquellos que sean puramente de gestión y administración de infraestructuras y recursos de la propia organización, como por ejemplo:

- Sistemas de video vigilancia
- Sistemas de control de temperaturas de neveras y ambiente
- Sistemas de control de presión atmosférica en quirófanos
- Sistemas de videoconferencias
- Sistemas de gestión de turnos en las consultas
- Sistemas de digitalización de historias clínicas

En este trabajo, se elaborará una herramienta que dará como resultado un informe detallado sobre el nivel de cumplimiento de todo proyecto informático respecto a los requisitos de políticas y seguridad informática establecidas en cada organización. El procedimiento será *customizable*, de forma que pueda ser utilizado por cualquier hospital del estado y cualquier organización tanto pública como privada. (Imagen 2)

Desde este momento, en este documento se hará referencia a esta herramienta como HITA (Healthcare IT Audit).

Imagen 2. Consejerías de Sanidad y Servicio de Salud de las comunidades autonomas.

(Sanidad, 2013)

Por otro lado, todo proveedor que participe en una licitación de un sistema informático para un centro sanitario, podrá verificar en qué nivel de cumplimiento de requisitos se encuentra su sistema, así como como el propio hospital o centro de salud podrá utilizar este sistema para evaluar técnicamente las diferentes ofertas. Es decir, esta herramienta dará como resultado unos niveles de cumplimiento para cada nuevo proyecto, de forma que se puedan tomar decisiones en base a sus niveles de referencia.

Según lo anteriormente indicado, los sistemas de información clínica trabajaban normalmente aislados. Sin embargo, hoy en día los CIS se relacionan con otros sistemas de información.

A continuación, se enumeran los sistemas que habitualmente se relacionan con un CIS:

- **HIS** (*Sistema de Información Hospitalaria / Hospital Information System*): El sistema de información del hospital proporciona la información demográfica del paciente y sus identificadores como paciente. Consta de varios subsistemas o módulos especializados (Admisión, Laboratorio, Farmacia, Hospitalización, Emergencia, Consulta externa y otros) que responden a las diferentes áreas del centro, teniendo como característica principal su interacción.

  Un HIS facilita el control y almacenamiento de toda la información referente a un paciente hospitalizado, desde el momento que éste ingresa al centro hospitalario y durante todo el período de estancia y atención en el mismo.

- **HCE** (*Historia Clínica Electrónica*): Almacena los documentos relevantes para la asistencia del paciente a lo largo de su vida. En definitiva, se trata de un repositorio de información, mantenido electrónicamente, con los datos de salud de toda la vida de un paciente, guardados de tal manera que puedan ser accedidos por múltiples usuarios del registro médico.

  Desde el CIS se accede a la HCE durante la estancia del paciente en el hospital. El CIS es proveedor de documentos para el HCE (Por ejemplo, un informe de alta se crea en el CIS y se almacena en la HCE para siempre.)

- **LIS** *(Sistema de Información de Laboratorio/ Laboratory Information Systems*): Sistema de información para laboratorios, que gestiona los resultados de los analizadores de muestras, automatizando al máximo el procesamiento de las pruebas. El LIS envía los resultados al CIS.

- **PACS** (*Picture Archiving and Communication System / Sistema de Archivado y Transmisión de Imágenes*): Sistema informático para el archivado digital de imágenes médicas.

- **RIS** (*Radiological Information System / Sistema de Información Radiológica*): Este sistema ofrece las herramientas adecuadas para el control de todo el proceso radiológico concerniente a un paciente, desde la petición del estudio hasta la realización, entrega y distribución de su informe diagnóstico, pasando por la recogida de las incidencias y consumos que conlleva la realización de dicha exploración. Todo RIS debe llevar asociado un PACS donde almacenar las imágenes.

  El RIS es el sistema que permite la integración y comunicación entre todas las aplicaciones dentro de la gestión hospitalaria que respondan a los departamentos de diagnóstico por imágenes. Dicha solución se comunica con el HIS y con todas las modalidades de exploración que producen imágenes en formato DICOM, con el fin de enviarle a cada imagen información que la identifique

  Podríamos decir que el RIS es un sistema administrativo y el PACS un sistema clínico. Entre los sistemas HIS, RIS y PACS debe haber una comunicación bidireccional, en la que cada uno pueda transferir e intercambiar información clínica. Es por esto que se hace necesaria la interoperabilidad empleando estándares como HL7 y DICOM (Imagen 3)

Imagen 3. Interoperabilidad entre los diferentes sistemas hospitalarios.

(Scielo)

Además de los sistemas citados, existen un sinfín de sistemas y dispositivos conectados a la red informática, que en la mayoría de los casos requieren la integración con varios de los sistemas principales ya mencionados.

Ejemplo 1:

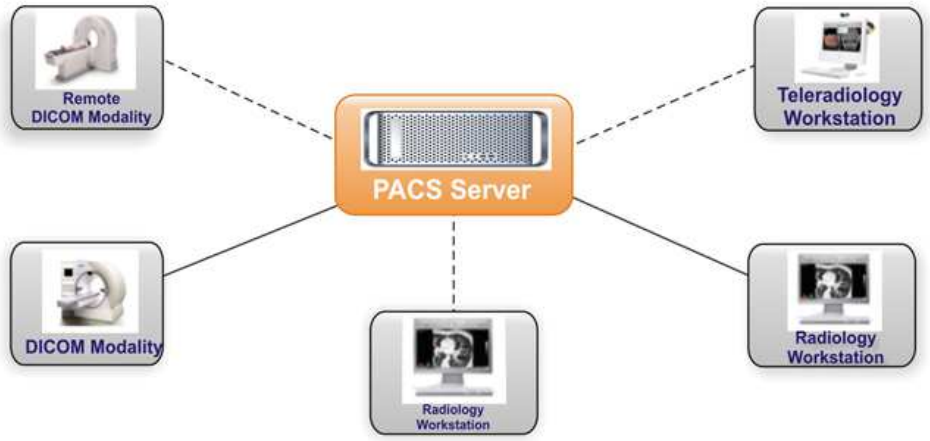
Los sistemas de Farmacia deben estar sincronizados con el CIS de forma que se registre la prescripción médica para cada paciente, o de igual forma los resultados de un espirómetro, electrocardiograma… deben estar accesibles en la historia clínica.

Se debe tener en cuenta que muchos de estos dispositivos requieren estar conectados a la red del hospital. El problema surge cuando estos dispositivos, que normalmente incluyen un PC, no cumplen con las medidas de seguridad y políticas establecidas en la organización.

Ejemplo 2:

En esta imagen (Imagen 4) se reflejan diferentes dispositivos conectados a la red informática para consultar o compartir información con el PCAS. Vemos que hay varias estaciones de trabajo, que en definitiva son PC implantados por el fabricante del sistema radiológico, que generalmente se implantan sin tener en cuenta los requerimientos establecidos por el departamento de IT del hospital.

Imagen 4. Interoperabilidad de los diferentes sistemas con la imagen radiológica.



Por este motivo, ante una situación de este tipo, existe la necesidad de conocer el grado de cumplimiento de estos equipos respecto a las políticas informáticas de cada organización.

1.2 Objetivos del Trabajo

1. Elaborar un documento de requisitos mínimos de seguridad y legales para presentar a los proveedores de proyectos informáticos y a la propia dirección de los hospitales. Este documento tendrá un formato de informe con las correspondientes graficas e información.

2. Elaborar el prototipo funcional de una herramienta que permita a los responsables de IT de los hospitales, verificar el nivel de cumplimiento de requisitos mínimos legales y técnicos en cada nuevo proyecto informático, o de ingeniería médica que vaya acompañado de sistemas informáticos, o simplemente esté conectado a la red de datos informática.

3. Elaborar el prototipo funcional de una herramienta que verifique el nivel de cumplimiento de requisitos de un sistema que ya haya sido implantado por el proveedor. De esta forma se podrá contrastar y verificar la diferencia entre el cumplimiento de requisitos real de lo ofertado, y lo finalmente implantado.

4. Diseñar este prototipo orientado al ámbito sanitario, pero creando una estructura modular que permita su uso en otros ámbitos de interés. Es decir, este proyecto se centrará en el ámbito sanitario, pero si profesionales de IT del ámbito educativo, industrial, automoción, etc. lo consideran útil, podrán adaptarla a sus necesidades.

1.3 Enfoque y método seguido

Para la elaboración del documento o informe de requisitos, se tomarán como referencia la LOPD, la Ley de autonomía del paciente, así como los diferentes documentos de requisitos ya existentes en varios hospitales de referencia.

Para el desarrollo de la aplicación, se plantea desarrollar una herramienta específica en forma de “checklist”. La herramienta a desarrollar mostrará unos formularios y cuestionarios, los cuales recibirán unos *inputs* manualmente por parte del usuario, para que ésta muestre como resultado un informe final detallado, indicando el nivel de cumplimiento de requisitos técnicos y legales del proyecto auditado.

Del mismo modo, el sistema deberá ser flexible y *customizable* para que sea capaz de diferenciar proyectos informáticos que gestionen datos de paciente, que únicamente hagan de *middleware, o que* simplemente sean controladores de un equipo de ingeniería o *electromedicina.*

1.4 Planificación del Trabajo

Para la realización de trabajo será necesario contactar con proveedores de ingeniería para la medicina y hospitales, así como con personal de IT de varios hospitales del estado. En base al conocimiento propio, tras la experiencia

adquirida durante 7 años en la administrador de sistemas en un hospital público, y en base al *feedback* recibido por parte de proveedores y otros expertos, se diseñará una aplicación basada en formularios. Dicha aplicación proporcionará a los responsables de IT de hospitales, una herramienta para exigir el cumplimiento de ciertos niveles técnicos y legales aplicable a cualquier licitación o proyecto de ingeniería y *electromedicina* que requieran la implantación de sistemas informáticos.

A continuación se detallan los hitos a conseguir en cada fase:

Hito 1: PAC 1 - Entrega del Plan de trabajo

- Lectura de literatura sobre tesis recientes sobre ingeniería informática en el ámbito hospitalario.
- Lluvia de ideas. Seleccionar dos temas candidatos.
- Evaluar las dos ideas seleccionadas y elegir una.
- Descripción del Trabajo Final de Grado (TFG).
    - Contexto y justificación del Trabajo.
- Objetivos del Trabajo.
    - Definir los objetivos generales.
    - Definir los objetivos específicos.
- Enfoque y método a seguir.
- Planificación del Trabajo.
    - Temporización general detallando cada uno de los hitos a cumplir.
    - Diagrama de Gantt, detallando el tiempo dedicado a cada tarea.
- Documentación de la PAC 1.
- Entrega de la PAC 1.

Hito 2: PAC 2 - Entrega primera fase Ejecución del Plan de trabajo

- Estudio de la LOPD.
- Selección de Hospitales y conseguir contactos de IT.
- Contactar IT de Hospitales y recoger información.
- Contactar con proveedores de electromedicina y laboratorios.
- Realizar esquema de problemas y necesidades comunes.
- Definir estructura del prototipo a desarrollar.
- Estudiar opciones de funcionalidad y formato.
- Selecciona tecnología y formato para el desarrollo.
- Documentación de la PAC2.
- Entrega de la PAC 2.

Hito 3. PAC 3. Entrega segunda fase Ejecución del Plan de trabajo

- Desarrollo del prototipo propuesto.
- Entregar beta a responsables IT de Hospitales.
- Recibir feeedback y estudiar cambios.
- Realizar cambios propuestos.

- Documentar PAC3.
- Entregar PAC3.

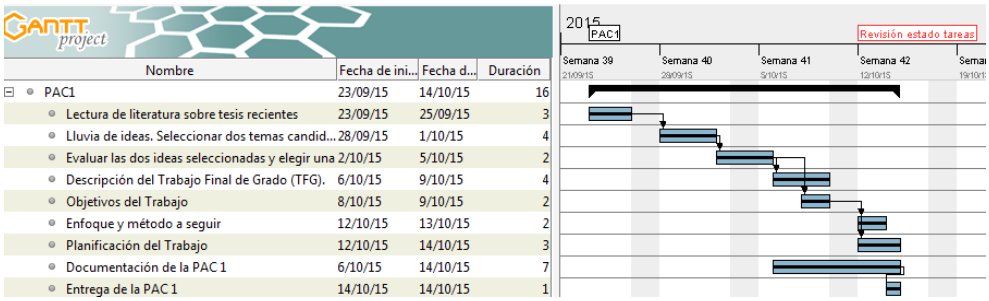
Hito 4. Entrega final del trabajo. Memoria, presentación y defensa

- Enfoque y método seguido.
- Breve sumario de productos obtenidos.
- Breve descripción de los otros capítulos de la memoria.
- Documentación de la Memoria.
- Preparación de la Defensa.
- Grabación de la Defensa.
- Autoinforme del Trabajo.
- Entrega de la Memoria y la Defensa.

Planificación del proyecto (Adjunta el proyecto en PDF)

Hito 1

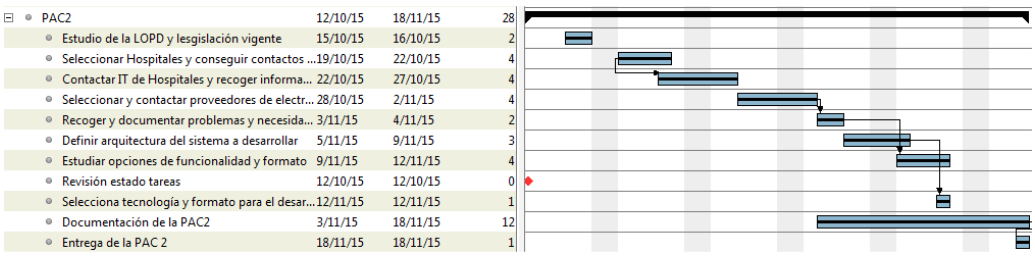
Imagen 5. Detalle de la planificación para cumplir el Hito 1



Nombre	Fecha de ini...	Fecha d...	Duración
PAC1	23/09/15	14/10/15	16
Lectura de literatura sobre tesis recientes	23/09/15	25/09/15	3
Lluvia de ideas. Seleccionar dos temas candid...	28/09/15	1/10/15	4
Evaluar las dos ideas seleccionadas y elegir una	2/10/15	5/10/15	2
Descripción del Trabajo Final de Grado (TFG).	6/10/15	9/10/15	4
Objetivos del Trabajo	8/10/15	9/10/15	2
Enfoque y método a seguir	12/10/15	13/10/15	2
Planificación del Trabajo	12/10/15	14/10/15	3
Documentación de la PAC 1	6/10/15	14/10/15	7
Entrega de la PAC 1	14/10/15	14/10/15	1

Hito 2

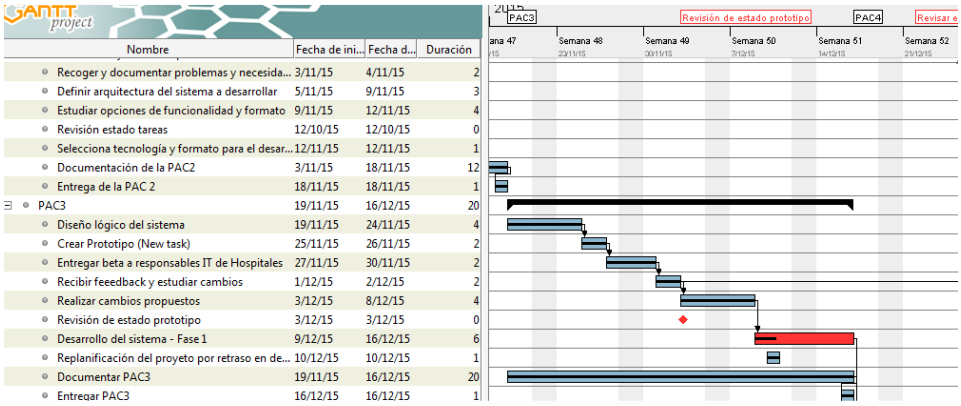
Imagen 6. Detalle de la planificación para cumplir el Hito 2



PAC2	12/10/15	18/11/15	28
Estudio de la LOPD y lesgislación vigente	15/10/15	16/10/15	2
Seleccionar Hospitales y conseguir contactos ...	19/10/15	22/10/15	4
Contactar IT de Hospitales y recoger informa...	22/10/15	27/10/15	4
Seleccionar y contactar proveedores de electr...	28/10/15	2/11/15	4
Recoger y documentar problemas y necesida...	3/11/15	4/11/15	2
Definir arquitectura del sistema a desarrollar	5/11/15	9/11/15	3
Estudiar opciones de funcionalidad y formato	9/11/15	12/11/15	4
Revisión estado tareas	12/10/15	12/10/15	0
Selecciona tecnología y formato para el desar...	12/11/15	12/11/15	1
Documentación de la PAC2	3/11/15	18/11/15	12
Entrega de la PAC 2	18/11/15	18/11/15	1

Hito 3

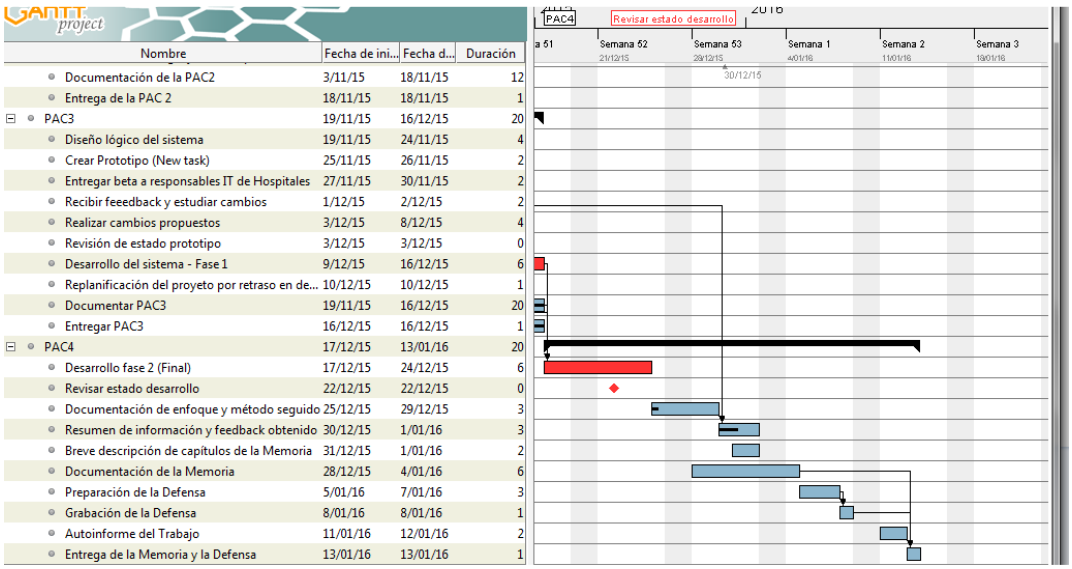
Imagen 7. Detalle de la planificación para cumplir el Hito 3



Nombre	Fecha de ini...	Fecha d...	Duración
Recoger y documentar problemas y necesida...	3/11/15	4/11/15	2
Definir arquitectura del sistema a desarrollar	5/11/15	9/11/15	3
Estudiar opciones de funcionalidad y formato	9/11/15	12/11/15	4
Revisión estado tareas	12/10/15	12/10/15	0
Selecciona tecnología y formato para el desar...	12/11/15	12/11/15	1
Documentación de la PAC2	3/11/15	18/11/15	12
Entrega de la PAC 2	18/11/15	18/11/15	1
PAC3	19/11/15	16/12/15	20
Diseño lógico del sistema	19/11/15	24/11/15	4
Crear Prototipo (New task)	25/11/15	26/11/15	2
Entregar beta a responsables IT de Hospitales	27/11/15	30/11/15	2
Recibir feeedback y estudiar cambios	1/12/15	2/12/15	2
Realizar cambios propuestos	3/12/15	8/12/15	4
Revisión de estado prototipo	3/12/15	3/12/15	0
Desarrollo del sistema - Fase 1	9/12/15	16/12/15	6
Replanificación del proyeto por retraso en de...	10/12/15	10/12/15	1
Documentar PAC3	19/11/15	16/12/15	20
Entregar PAC3	16/12/15	16/12/15	1

Hito 4

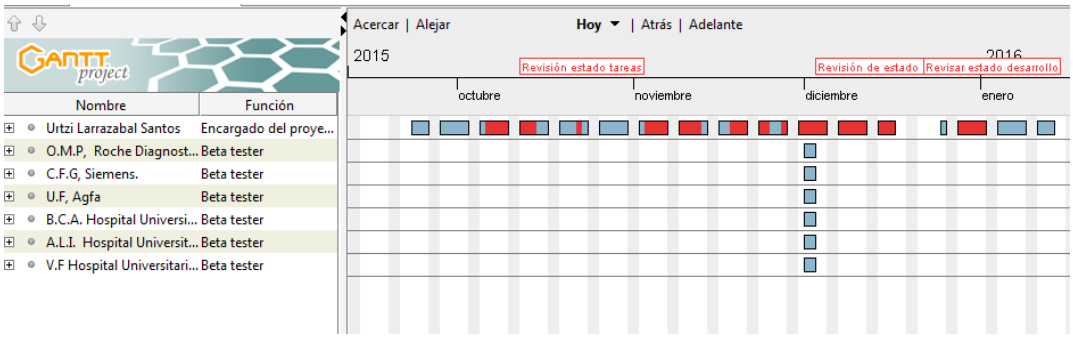
Imagen 8. Detalle de la planificación para cumplir el Hito 4



Nombre	Fecha de ini...	Fecha d...	Duración
Documentación de la PAC2	3/11/15	18/11/15	12
Entrega de la PAC 2	18/11/15	18/11/15	1
PAC3	19/11/15	16/12/15	20
Diseño lógico del sistema	19/11/15	24/11/15	4
Crear Prototipo (New task)	25/11/15	26/11/15	2
Entregar beta a responsables IT de Hospitales	27/11/15	30/11/15	2
Recibir feeedback y estudiar cambios	1/12/15	2/12/15	2
Realizar cambios propuestos	3/12/15	8/12/15	4
Revisión de estado prototipo	3/12/15	3/12/15	0
Desarrollo del sistema - Fase 1	9/12/15	16/12/15	6
Replanificación del proyeto por retraso en de...	10/12/15	10/12/15	1
Documentar PAC3	19/11/15	16/12/15	20
Entregar PAC3	16/12/15	16/12/15	1
PAC4	17/12/15	13/01/16	20
Desarrollo fase 2 (Final)	17/12/15	24/12/15	6
Revisar estado desarrollo	22/12/15	22/12/15	0
Documentación de enfoque y método seguido	25/12/15	29/12/15	3
Resumen de información y feedback obtenido	30/12/15	1/01/16	3
Breve descripción de capítulos de la Memoria	31/12/15	1/01/16	2
Documentación de la Memoria	28/12/15	4/01/16	6
Preparación de la Defensa	5/01/16	7/01/16	3
Grabación de la Defensa	8/01/16	8/01/16	1
Autoinforme del Trabajo	11/01/16	12/01/16	2
Entrega de la Memoria y la Defensa	13/01/16	13/01/16	1

Diagrama de recursos:

Imagen 9. Detalle de los recursos para cada tarea



Nombre	Función
Urtzi Larrazabal Santos	Encargado del proye...
O.M.P, Roche Diagnost...	Beta tester
C.F.G, Siemens.	Beta tester
U.F, Agfa	Beta tester
B.C.A. Hospital Universi...	Beta tester
A.L.I. Hospital Universit...	Beta tester
V.F Hospital Universitari...	Beta tester

1.5 Breve sumario de productos obtenidos

Para la ejecución de este proyecto se requiere recoger información de expertos de IT en hospitales, así como de proveedores de sistemas de ingeniería médica, soluciones y sistemas para hospitales. Con toda esta información y usando como base legal los artículos descritos por la LOPD, se desarrollará un prototipo de herramienta capaz de evaluar y auditar cualquier proyecto informático para su implantación en centros sanitarios y hospitales.

En cuanto al desarrollo del prototipo, se plantea un desarrollo que permita su uso online o incluso de forma portable.

1.6 Breve descripción de los otros capítulos de la memoria

Hito 2: PAC 2 - Entrega primera fase Ejecución del Plan de trabajo

- **Estudio de la LOPD**

  Se estudiará la ley vigente referente a la gestión de datos de pacientes, así como los niveles de seguridad exigidos a hospitales.

- **Selección de hospitales y contactos de profesionales de IT**

  Además de los hospitales de Euskadi mencionados anteriormente, se requiere contactar con un mínimo de dos hospitales de referencia del resto del estado.

- **Contacto con profesionales de IT de hospitales y recoger información**

  Se pretende hablar telefónicamente o por videoconferencia para intercambiar experiencias.

- **Contacto con proveedores de ingeniería médica y laboratorios**

  Igualmente, se requiere conocer los problemas que se encuentran los proveedores a la hora de desarrollar ingeniería y sistemas para hospitales.

- **Realización de esquema de problemas y necesidades comunes.**

  Con la información recogida se realizará un esquema de la información relevante y necesaria para incluir en la herramienta.

- **Definición de estructura de la herramienta a desarrollar**

  En esta fase se estudiará estructuralmente como diseñar la herramienta: páginas, secciones, apartados, pantallas, etc.

- **Estudio de opciones de funcionalidad y formato**

  Se debe realizar un estudio de usabilidad y portabilidad del sistema para que pueda ser utilizado desde cualquier entorno y centro.

- **Selección de tecnología y formato para el desarrollo.**

  Finalmente se decidirá qué tecnología de diseño y desarrollo será la más adecuada para la ejecución del sistema.

- Documentación de la PAC2

- Entrega de la PAC 2

Hito 3. PAC 3. Entrega segunda fase Ejecución del Plan de trabajo

- **Desarrollo del software propuesto**

  Esta será la fase más duradera y costosa, en la cual se realizará el propio desarrollo del prototipo funcional.

- **Entrega de versión beta a responsables IT de Hospitales y proveedores.**

  Una vez desarrollada una versión con funcionalidad básica se hará llegar a los responsables de IT y proveedores contactados anteriormente, para que trabajen y prueben esta versión beta.

- **Estudiar *feedback* de los *Beta tester* y estudiar cambios**

  Se recogerán los errores detectados, las opiniones y conclusiones de cada experto, estudiando y valorando todas las sugerencias de mejora.

- **Realizar cambios propuestos**

  En esta fase se tendrá en cuenta el feedback obtenido y se realizarán los cambios adecuados.

- Documentación PAC3
- Entrega PAC3

Hito 4. Entrega final del trabajo. Memoria, presentación y defensa

- **Finalización del prototipo**
- **Testeo del prototipo desarrollado**
- **Enfoque y método seguido.**

  Se describirá cómo surgió la idea del trabajo, como se detectó la necesidad a cubrir, y cómo se ha enfocado el proyecto.

- **Breve sumario de productos obtenidos.**

  Para realizar este proyecto se debe obtener información en lugar de productos

- **Breve descripción de los otros capítulos de la memoria.**
- **Documentación de la Memoria.**
- **Preparación de la Defensa.**
- **Grabación de la Defensa.**
- **Auto-informe del trabajo.**
- **Entrega de la Memoria y la Defensa.**

2. Desarrollo de HITA

2.1 Definición de requerimientos

En este apartado se detallan los pasos dados para detallar las necesidades detectadas, así como recolectar toda la información necesaria proporcionada por los diferentes *stakeholders* para desarrollar el proyecto. Del mismo modo se detallan las conclusiones obtenidas tras el análisis de los mismos, reflejando además la información que se ha seleccionado como referencia para el diseño del proyecto.

2.1.1 Contactos con hospitales

Hasta el momento se ha conseguido contactar con los responsables de IT de los siguientes hospitales:

- *B.J.F.* del *Hospital Universitario de Basurto* (Bizkaia)
- *B.C.A.* del *Hospital Universitario de Cruces* (Bizkaia)
- *A.L.I.* del *Hospital Universitario de Araba*
- *C.A.V.* del Hospital de Zaragoza
- *A.I.G*. de la *Organización Central de Osakidetza*
- *V.F del Hospital Universitario de Gran Canaria Doctor Negrín*

Durante las reuniones mantenidas con estas personas, se han intercambiado experiencias en el ámbito de los proyectos informáticos para hospitales así como las tendencias actuales en la *electromedicina*. Así mismo, se han destacado los principales problemas que suele existir con los proveedores, que por lo que se ha podido constatar son comunes a todos los casos. En general, resultan ser sistemas diseñados para un propósito médico concreto, sin tener en cuenta la seguridad ni las políticas establecidas en las redes informáticas de los hospitales.

Otro de los problemas comunes que se ha detectado en todos los casos, deriva de la poca implicación que es requerida a menudo de los responsables de IT a la hora de tomar parte en la licitación y adjudicación de proyectos. Generalmente, ocurre que la dirección médica requiere cumplir unas necesidades médicas, siendo esta a prioridad absoluta por encima de cualquier valoración técnica. Cuando los proveedores presentan sus soluciones de ingeniería médica, rara vez tiene peso en la toma de decisiones el análisis que pueda hacer el servicio de IT en cuanto a la normativa y políticas de seguridad informática que cumplan o incumplan esos sistemas.

Tras exponer el propósito de la aplicación de apoyo a desarrollar en este proyecto de final de carrera, todos evalúan positivamente la existencia de una herramienta de auditoria como HITA, de forma que los responsables de IT puedan elaborar un informe de forma sencilla y ágil sobre cada nuevo proyecto

a implantar. De esta forma, existirá siempre un criterio común para valorar cada oferta y la dirección podrá en todo momento evaluar las diferencias técnicas existente entre cada proyecto presentado.

En la actualidad, cada organización busca sus propios métodos para evaluar los nuevos sistemas a implantar, que básicamente consisten en una hoja Excel o un documento PDF con una serie de características apuntadas.

2.1.2 Contactos con proveedores

Se ha conseguido contactar con diferentes responsables de proyectos informáticos, de empresas proveedoras de sistemas para la medicina.

- *G.F.* de la compañía *Roche Diagnostics*
- *O.M.P.* de la compañía *Roche Diagnostics*
- *A.M.B* de la compañía *Werfen*
- *C.F.G* de la compañía *Siemens*.
- *J.A* de la compañía *Tecnomedia Sistemas*

Al igual que con los hospitales, durante las teleconferencias y reuniones mantenidas con estas personas, se han intercambiado experiencias en el ámbito de los proyectos informáticos para hospitales, así como las tendencias actuales en la *electromedicina*. Por otro lado, se ha compartido y revisado conjuntamente varios pliegos públicos referentes a proyectos de ingeniería médica para los distintos hospitales en los que han trabajado.

En el caso de los proveedores, se detecta otro problema común en todos los casos. Generalmente, estas empresas dedican gran esfuerzo económico en I+D para innovar y desarrollar sistemas de ingeniería médica. Pero paradójicamente, ninguna de ellas dedica grandes esfuerzos a la integración informática. Resulta que analizadores que cuestan millones de euros, están acompañados de un software realmente simple y con escaso enfoque de integración y seguridad.

Afortunadamente, se está mejorando cada vez más en este aspecto, aunque aún es significativa la poca calidad de los sistemas informáticos asociados a estos proyectos de presupuestos tan elevados.

Además de la gran utilidad para hospitales, los proveedores ven muy adecuada la existencia de una herramienta pública y abierta de auditoria de sistemas informáticos para centros sanitarios, de forma que tanto el personal técnico como los comerciales puedan mostrar un informe a sus superiores donde se vea el grado madurez de sus sistemas en cuanto a seguridad, políticas y normativa informática.

2.1.3 Características necesarias para el cumplimiento de la LOPD

Se ha buscado y estudiado toda la información posible existente en Internet respecto a la problemática de seguridad informática existente actualmente en la sanidad. Se han revisado los informes de la *AEPD* (Agencia Española de Protección de Datos) (agpd, 2010).

Del mismo modo, se han analizado auto-informes de seguridad de varios hospitales, así como artículos de prensa referentes al robo de información ocurrido en algunos hospitales. (Elmundo, 2013)

Finalmente, se ha estudiado la legislación actual en cuanto al uso y manejo de los datos de ciudadanos clasificados como nivel bajo, medio, y alto según la LOPD. Concretamente, se ha analizado la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la referida ley. A continuación se detallan aquellos artículos y puntos de interés para el desarrollo de la herramienta.

Título VIII. DE LAS MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. CAPÍTULO I - DISPOSICIONES GENERALES

Real Decreto 1720/2007- Artículo 80. NIVELES DE SEGURIDAD.

> *Las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto.*
> *Real Decreto 1720/2007 - Artículo 81. APLICACIÓN DE LOS NIVELES DE SEGURIDAD.*
> *3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:*
> *a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.*
> *5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:*
> *a) Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.*
> *b) Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesoria se contengan aquellos datos sin guardar relación con su finalidad.*
>
> *6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple*

declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

Es decir, los datos de pacientes de los hospitales y centros de salud están considerados como datos que requieren un nivel de protección alto. Con lo cual, se les deberán aplicar las medidas protectoras exigidas para los ficheros automatizados cuyo contenido este clasificado tanto en el nivel alto, medio, así como en el bajo.

Cuando se audite un sistema de un nuevo proyecto, interesa conocer si este almacena datos sin identificación, o si almacena datos demográficos de ciudadanos, o si almacena datos de salud de los ciudadanos, etc. y en que condiciones.

Tabla1: tipo de datos y medidas obligatorias para cada caso

	TIPO DE DATOS	OBLIGACIONES
BASICO	• *Afecta a todos los ficheros o tratamientos de datos de carácter personal.* • *Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual (cuando la única finalidad es realizar una transferencia dineraria a las entidades de las que los afectados sean asociados; o caso de ficheros que de forma accesoria contengan estos datos).* • *Grado de discapacidad o invalidez (salud) sólo para el cumplimiento de deberes públicos.*	• *Documento de seguridad* • *Régimen de funciones y obligaciones del personal* • *Registro de incidencias* • *Identificación y autenticación de usuarios* • *Control de acceso* • *Gestión de soportes* • *Copias de respaldo y recuperación, verificación semestral* • *Almacenamiento de ficheros no automatizados o en papel bajo llave.* • *Pruebas sin datos reales*
MEDIO	• *Infracciones administrativas o penales.* • *Prestación de servicios de información sobre solvencia patrimonial y crédito. Cumplimiento o incumplimiento de obligaciones dinerarias.* • *Administraciones Tributarias.* • *Prestación de servicios financieros.* • *Entidades Gestoras y Servicios Comunes de la Seguridad Social, en el ejercicio de sus competencias en materia de recaudación.* • *Definición de las características o de la personalidad (evaluación del comportamiento).*	• *Medidas de seguridad de nivel básico* • *Responsable de Seguridad* • *Auditoría bienal* • *Medidas adicionales de Identificación y autenticación de usuarios (límite reintentos de acceso)* • *Control de acceso físico* • *Medidas adicionales de gestión de soportes(registro entrada y salida)* • *Registro de incidencias (anotación y autorización para los procedimientos de recuperación)*
ALTO	• *Ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.* • *Fines policiales sin consentimiento.* • *Actos de violencia de género.* • *Operadores de servicios de comunicaciones electrónicas (datos de tráfico y de localización).*	• *Medidas de seguridad de nivel básico y medio* • *Seguridad en la distribución de soportes(cifrado)* • *Registro de accesos (tanto para ficheros automatizados como en soporte papel).* • *Medidas adicionales de copias de respaldo (copia en lugar diferente)*

- *Cifrado de telecomunicaciones*
- *Almacenamiento de ficheros no automatizados o en papel bajo llave y en áreas de acceso restringido*

Real Decreto 1720/2007 - Artículo 83. PRESTACIONES DE SERVICIOS SIN ACCESO A DATOS PERSONALES.

> *El responsable del fichero o tratamiento adoptará las medidas adecuadas para limitar el acceso del personal a datos personales, a los soportes que los contengan o a los recursos del sistema de información, para la realización de trabajos que no impliquen el tratamiento de datos personales.*
>
> *Cuando se trate de personal ajeno, el contrato de prestación de servicios recogerá expresamente la prohibición de acceder a los datos personales y la obligación de secreto respecto a los datos que el personal hubiera podido conocer con motivo de la prestación del servicio.*

Es decir, cuando un proveedor implanta un sistema en el cual se almacenen datos personales de pacientes, estos nunca deberán acceder a los mismos a no ser que se haya recogido e indicado expresamente en el contrato.

En la implantación de sistemas hospitalarios, por ejemplo, Historia Clínica, el proveedor que realiza la implantación tendrá acceso a todos los datos de carácter personal de los ciudadanos. Además, estos sistemas que manejan datos de paciente a menudo generan errores, que lógicamente serán corregidos por expertos de dicha empresa. Es por ello, que en la adjudicación de un proyecto de este tipo, se deben establecer las condiciones legales y de confidencialidad necesarias. Este sería un ejemplo de la adjudicación de un proyecto referente a la Historia Clínica Electrónica:

En consideración al tipo de información procesada, el adjudicatario está obligado a mantener la más absoluta confidencialidad sobre todos aquellos datos y documentos a que tenga acceso con motivo de la adjudicación. A ellos accederán exclusivamente las personas estrictamente imprescindibles para el desarrollo de las tareas inherentes a la misma. Todas ellas serán advertidas del carácter confidencial y reservado de la información a la que tendrán acceso.

Todos los ficheros que se pongan a disposición del adjudicatario para la ejecución del contrato son propiedad de Osakidetza y están registrados y sometidos a la salvaguarda que establece la legislación vigente, en especial la relativa a la protección de datos personales. Toda cesión a terceros será perseguida en los tribunales.

Osakidetza se reserva el derecho de establecer cualquier tipo de marcaje de los ficheros que se dejarán al adjudicatario, de manera que sus características puedan constituirse como prueba que posibilite localizar el origen y los responsables de las eventuales cesiones.

Bajo ningún caso ni circunstancia el adjudicatario podrá suministrar a terceros ni utilizar para sí ni para otros los datos facilitados por Osakidetza para fines distintos a los contemplados en el objeto del presente contrato.

El adjudicatario estará obligado a poner en conocimiento de Osakidetza, inmediatamente después de ser detectada, cualquier sospecha de eventuales errores que se puedan producir en el sistema de seguridad de la información.

El adjudicatario faculta a Osakidetza para que al terminar el proyecto pueda responsabilizarlo y/o repercutirle los costes derivados de posibles reclamaciones ocasionadas por negligencia y/o falta de confidencialidad del mismo.

Adicionalmente y como condición general, todos los servicios prestados deberán contar con las medidas de seguridad y de confidencialidad adecuadas al grado de sensibilidad de la información suministrada, de acuerdo con lo descrito en la LOPD.
(Osakidetza)

Por otro lado, en el caso de los hospitales públicos se aplica el contrato de confidencialidad dispuesto en la *Ley 30/2007, de 30 de octubre, de Contratos del Sector Público*.

Para los casos en los que un proveedor de un sistema informático, no deba acceder bajo ningún concepto a datos de pacientes, deberá estar expresamente indicado. Por ejemplo, en el pliego de bases técnicas de un proyecto real, se indica un apartado de confidencialidad de este estilo:

En consideración al tipo de información procesada, el adjudicatario está obligado a mantener la más absoluta confidencialidad sobre todos aquellos datos y documentos a que tenga acceso objeto de este contrato durante un plazo de 5 años (según Art. 124, apartado 2 LCSP 30/2007). A ellos accederán exclusivamente las personas estrictamente imprescindibles para el desarrollo de las tareas inherentes a la misma. Todas ellas serán advertidas del carácter confidencial y reservado de la información a la que tendrán acceso.

Todos los ficheros que se pongan a disposición del adjudicatario para la ejecución del contrato son propiedad de Osakidetza y están registrados y sometidos a la salvaguarda que establece la legislación vigente. Toda cesión a terceros será perseguida en los tribunales.

La prestación de servicios no contempla el acceso por parte del adjudicatario a datos personales responsabilidad de Osakidetza por lo que Osakidetza adoptará las medidas necesarias para evitar el mismo.

Osakidetza se reserva el derecho de establecer cualquier tipo de marcaje de los ficheros que se dejarán al adjudicatario, de manera que sus características puedan constituirse como prueba que posibilite localizar el origen y los responsables de las eventuales cesiones.

Real Decreto 1720/2007 - Artículo 85. ACCESO A DATOS A TRAVÉS DE REDES DE COMUNICACIONES.

> *Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.*

Es decir, se deberá asegurar el mismo control de acceso a los datos de pacientes, ya sea desde la propia red local, como desde la WAN.

Título VIII. DE LAS MEDIDAS DE SEGURIDAD EN EL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL. CAPÍTULO III - MEDIDAS DE SEGURIDAD APLICABLES A FICHEROS Y TRATAMIENTOS AUTOMATIZADOS

Sección Primera - Medidas de seguridad de nivel básico:

Real Decreto 1720/2007 - Artículo 91. CONTROL DE ACCESO.

> *1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.*
>
> *2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.*
>
> *3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.*
>
> *4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.*
>
> *5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.*

De acuerdo con lo anterior, deberán estar claramente establecidos y revisados los permisos que deba tener un usuario en cada momento.

Real Decreto 1720/2007 - Artículo 93. IDENTIFICACIÓN Y AUTENTICACIÓN.

> *1. El responsable del fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación y autenticación de los usuarios.*
>
> *2. El responsable del fichero o tratamiento establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.*
>
> *3. Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.*
>
> *4. El documento de seguridad establecerá la periodicidad, que en ningún*

caso será superior a un año, con la que tienen que ser cambiadas las contraseñas que, mientras estén vigentes, se almacenarán de forma ininteligible.

Es decir, se debe evitar el uso de usuarios genéricos siempre que se acceda a sistemas con datos de pacientes, ya que toda acción sobre estos datos deberá estar detalladamente registrada. Además, se deberá establecer políticas de seguridad respecto a las contraseñas de los usuarios, con el fin de cumplir los requisitos indicados en el artículo.

Real Decreto 1720/2007 - Artículo 94. COPIAS DE RESPALDO Y RECUPERACIÓN.

1. Deberán establecerse procedimientos de actuación para la realización como mínimo semanal de copias de respaldo, salvo que en dicho período no se hubiera producido ninguna actualización de los datos.

2. Asimismo, se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad.

3. El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y de recuperación de los datos.

4. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tratamiento realizado y se anote su realización en el documento de seguridad.

Si está previsto realizar pruebas con datos reales, previamente deberá haberse realizado una copia de seguridad.

Según la disposición anterior, tanto en el caso de datos de nivel básico, medio, como alto, se debe realizar como mínimo un *backup* semanal de los datos de pacientes. Los datos almacenados deberán estar en un formato ininteligible y deberán poderse recuperar al momento.

Sección Segunda - Medidas de seguridad de nivel medio:

Real Decreto 1720/2007 - Artículo 98. IDENTIFICACIÓN Y AUTENTICACIÓN.

> *El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.*

Es decir, el sistema deberá alertar o bloquear el acceso cuando un usuario o persona no autorizada realice sin éxito intentos continuos para acceder al sistema.

Sección Tercera - Medidas de seguridad de nivel alto:

Real Decreto 1720/2007 - Artículo 103. REGISTRO DE ACCESOS.

> *1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.*
>
> *2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.*
>
> *3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.*
>
> *4. El período mínimo de conservación de los datos registrados será de dos años.*
>
> *5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.*
>
> *6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:*
>
> *a) Que el responsable del fichero o del tratamiento sea una persona física.*
>
> *b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.*
>
> *La concurrencia de las dos circunstancias a las que se refiere el*

apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

Esto es, toda aplicación o proceso informático que acceda a los datos de pacientes deberá generar un log o registro, detallando el acceso realizado tal como se indica en este artículo y con las condiciones mencionadas en este artículo.

Real Decreto 1720/2007 - Artículo 104. TELECOMUNICACIONES.

Cuando, conforme al artículo 81.3 deban implantarse las medidas de seguridad de nivel alto, la transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Es decir, los datos de carácter personal clasificados de nivel alto, que viajen entre hospitales, o entre proveedores y hospitales, deberán viajar siempre encriptados. Esto también es aplicable para los casos en los que un proveedor ofrece soporte remotamente. La conexión entre redes de proveedores y clientes por sentido común debería ser siempre cifrada, pero en este caso es una obligación por ley.

Ley Orgánica 15/1999 - Artículo 9. SEGURIDAD DE LOS DATOS.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Es decir, los datos de carácter personal que se almacenan en los servidores deben estar debidamente protegidos para garantizar su disponibilidad, integridad y autenticidad.

2.1.4 Herramientas parecidas existentes

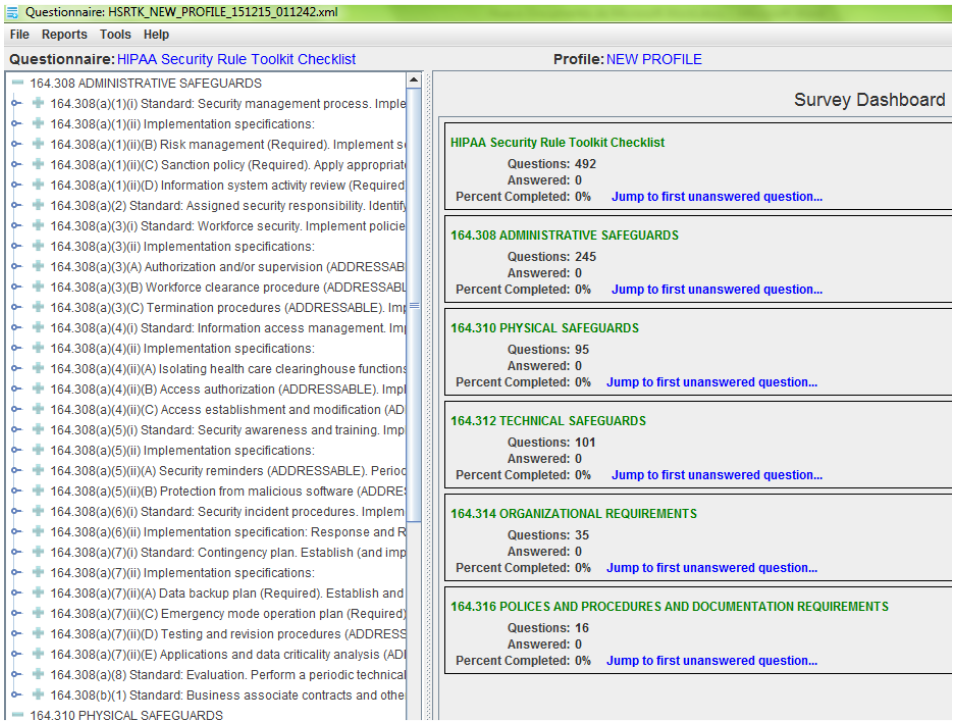
Para enfocar el diseño de la herramienta a desarrollar en este proyecto, se investiga en Internet la existencia de aplicaciones parecidas, para estudiarlas como referencia. Finalmente, se encuentra únicamente una aplicación que podría ser similar en muchos aspectos y cumple objetivos muy parecidos, pero aplicable a la legislación de los Estados Unidos.

Esta herramienta es la *HIPAA Security Rule Toolkit* publicada por el *NIST* (*National Institute of Standards and Technology*), la cual es una agencia del *U.S. Dept. of Commerce*. Se trata de una herramienta de escritorio, la cual permite a las organizaciones interesadas, cargar una serie de formularios y *checklist* para realizar una auto-auditoria, con el fin de conocer su grado de cumplimiento con lo establecido por la HIPAA.

El *HIPAA Security Rule Toolkit* es básicamente una herramienta que pueden usar las organizaciones que manejan datos de salud de ciudadanos, para conocer si estas cumplen con las obligaciones legales o no.

Concretamente, es una aplicación gratuita que se instala localmente en un PC, la cual consta de formularios con un total de 492 preguntas divididas en cinco apartados: *Administrative Safeguard, Physical Safeguards, Technical Safeguards, Organizational Requirements, Policies and Procedures and Documentation Requirements*.

Imagen 10: Pantalla principal de la aplicación HIPAA Security Rule Toolkit



The law requires "covered entities" and business associates to follow the HIPAA Security Rule. Covered entities include government agencies involved in health records, health care providers, health plans such as health insurance issuers and Medicaid and Medicare programs, health care clearinghouses and Medicare prescription drug card sponsors.
http://www.nist.gov/itl/csd/20111122_hipaa_tools.cfm

2.1.5 Conclusiones

Durante las reuniones mantenidas con proveedores y técnicos de IT de otros hospitales, se concluye que el principal problema en España es que no existe una "regulación real" de los sistemas informáticos para la medicina. No se realizan controles ni auditorías por parte de las entidades o autoridades competentes. En cuanto a los sistemas desarrollados por los proveedores, a estos no se les exige ninguna certificación especial, con lo que pueden vender sistemas informáticos que no cumplen con los requisitos necesarios, tanto legales, como técnicos.

También se concluye que resulta complicado para los departamentos de IT conocer qué obligaciones legales debe cumplir cada sistema nuevo a implantar, dependiendo de si se almacenan datos de paciente o no, de si los datos de carácter personal simplemente transitan por un middleware sin que se almacenen, etc. La propia legislación resulta complicada de aplicar y en la práctica ningún centro dispone de un departamento jurídico que estudie y apruebe si cada sistema informático cumple o no con la legislación. La experiencia dice que los proveedores tampoco dedican esfuerzos en sus sistemas para que cumplan con los requisitos legales.

Por todo esto, se estima necesaria una forma sencilla y genérica que pueda ayudar a todo departamento de IT, así como a los proveedores, a evaluar un determinado sistema para conocer si este, cumple o no con unos requisitos mínimos de seguridad y técnicos. Además, se estima necesario un procedimiento o herramienta que permita comparar dos propuestas técnicas de diferentes proveedores, y concluir con datos, cual de ellas cumple mejor las obligaciones y necesidades mencionadas.

Para ello se cree oportuno crear una herramienta que realice un cuestionario similar al "HIPAA Security Rule Toolkit" pero no tan genérico. Es decir, solo interesan los aspectos puramente técnicos referente al sistema a evaluar, no a su entorno.

El propósito del HITA no es auditar a una organización entera, sino auditar un sistema concreto. No se pretende auditar si un determinado Hospital o centro sanitario en el que se implantará un sistema de ingeniería médica, dispone de medidas de seguridad anti incendios en el CPD, si el acceso al mismo está restringido, si existe un registro de accesos, etc. tal y como se hace con el HIPAA.
Por el contrario, si interesa conocer las medidas de seguridad que incorpora el propio sistema a implantar, y si estas son suficientes para cumplir con la legislación Española en cuanto a la protección de datos de pacientes.

2.2 Análisis

En este capítulo se detallarán los estudios y análisis realizados para definir finalmente la arquitectura y el diseño estructural de la aplicación.

2.2.1 Arquitectura del sistema

Para la elaboración de este proyecto, el primer paso para diseñar la arquitectura del sistema, es decidir si se desarrollará un sistema de escritorio o Web.

Para el fin de este proyecto, se han estudiado previamente las ventajas y desventajas para cada opción, reflejándolas en la siguiente tabla:

Tabla2: comparativa entre soluciones de escritorio y Web

	Característica	Web	Escritorio
1	**Personalización, actualización y soporte**	*Es suficiente con realizar los cambios en el servidor WEB*	*Hay que realizarlos en cada estación de trabajo (PC) donde se tenga la aplicación*
2	**Multiplataforma**	*Se puede acceder desde cualquier sistema operativo.*	*Solo se puede usar en el S.O. para el que haya sido compilado.*
3	**Disponibilidad**	*Se pierde el acceso a la aplicación ante una caída de red.*	*Acceso permanente a la aplicación, aun cuando haya una caída de red.*
4	**Accesibilidad y cobertura**	*Cualquier lugar con acceso a Internet*	*Solo en el PC donde se haya instalado previamente el software*
5	**Capacidad de usuarios concurrentes**	*Alta, la limitación la pondrá el servidor.*	*Dependerá del número de PC en los que se haya instalado el sistema.*
6	**Portabilidad**	*El sistema puede ser usado con cualquier navegador de Internet*	*Solo funciona en el sistema operativo para el cual se haya compilado.*
7	**Infraestructura y movilidad**	*Solo se requiere de un navegador con conexión a Internet*	*Restringido a la ubicación del PC local.*
8	**Seguridad eléctrica y lógica**	*Es responsabilidad del administrador de sistemas donde resida la aplicación.*	*Es responsabilidad del administrador de la compañía y de cada usuario que usa el sistema localmente.*

Se estima que, excepto la mayor disponibilidad que ofrece un sistema de escritorio ante una caída de red, el resto de factores analizados son favorables a realizar un desarrollo Web. Por otro lado, debido a que este nunca será un sistema crítico que deba estar en alta disponibilidad, se estima que este factor no será decisivo.

Por lo tanto, al contrario que el *HIPAA Security Rule Toolkit, el HITA* se desarrollará como aplicación Web, de forma que pueda ser consultado Online desde cualquier dispositivo y plataforma.

El sistema no usará base de datos, ni ficheros que almacenen datos. Es decir, será una aplicación *Online* que podrá ser usada de forma anónima por cualquier interesado en auditar o analizar un proyecto informático para hospitales en España, el cual mostrará un informe final con los resultados, sin que se almacene en el servidor ningún dato introducido del mismo.

2.2.2 Lenguaje de desarrollo

A continuación se estudia el lenguaje de programación más adecuado para el tipo de sistema a desarrollar. Tras consultarlo con varios desarrolladores de aplicaciones Web (R.F.M. y S.Q.G. del Hospital Universitario de Cruces), se descarta el desarrollo en un lenguaje que ejecute código en el lado servidor. Esto se decide así, ya que la herramienta se puede ejecutar en el lado cliente cumpliendo con todas las funcionalidades necesarias. Es decir, no se requiere más que un navegador que ejecute el código y conexión a Internet.

Por lo que finalmente se decide realizar el desarrollo en código *HTML* y *JavaScript*. Destacamos entre las ventajas del lenguaje *JavaScripts* lo siguiente: creación de páginas web dinámicas, menús desplegables, efectos visuales sencillos, facilidad para manipular datos y crear aplicaciones web, todo ello utilizando poca memoria y manteniendo un tiempo de descarga rápido.

Además, una de las desventajas de este lenguaje está en que el propio código será visible para todo aquel que acceda a la página. Aun así, este factor no es un problema ya que el proyecto estará abierto para que pueda ser consultado públicamente.

Por otro lado, desarrollándolo de esta manera, se facilitará la implantación de la aplicación en cualquier servidor web, ya que bastará con copiar las carpetas y ficheros que lo forman, en el servidor correspondiente.

Para facilitar el desarrollo y diseño de la herramienta, se usará una versión trial del software *Axure*. Esta herramienta permite principalmente diseñar y maquetar páginas web, pero también permite incluir funciones y tareas, por lo que es adecuada para la ejecución del proyecto. Aunque el código que genera no es él más eficiente, debido a que su propósito no es realmente el entorno de producción, pero para este caso donde el uso del prototipo tendrá un uso muy limitado y especifico, se considera suficiente.

2.3 Diseño

Tras reuniones mantenidas con proveedores y responsables de IT, se cree oportuno crear esta herramienta incluyendo un cuestionario similar al "HIPAA Security Rule Toolkit" pero con no más de 50 preguntas referentes a las características técnicas del sistema a auditar. Se decide este número porque la experiencia vivida por todos, indica que un cuestionario mayor haría que una evaluación o auditoria de este tipo resultase realmente pesada, y lo que se persigue es motivar el uso de la misma. Por el contrario, con menos preguntas, no se obtendría un análisis adecuado del sistema a estudiar.

2.3.1 Estructura

La herramienta será portable por lo que constará básicamente de una carpeta llamada HITA, dentro de la cual existirán todas las páginas HTML, imágenes, carpetas, etc. que compondrán la herramienta.

Estructura de la herramienta:

- *main.html* → Página principal que contendrá un menú superior y un *frame* donde se mostrarán el resto de páginas.

  El menú contendrá las siguientes entraras y submenús:

  - Main: mostrará la página principal (portda.html)
  - Editor: mostrará la página de edición de preguntas y respuestas (questions.html)
  - Formulario: contendrá dos submenús:
    - Ficha general: mostrará el formulario donde se introducirán los datos generales referentes al sistema o proyecto a evaluar.
    - Checklist sanidad: mostrará el formulario con las 50 preguntas a contestar. (checklist001.html)
  - Informes: contendrá dos submenús:
    - Informe estándar: mostrará un informe genérico.
    - Informe sanidad: mostrará un informe orientado a entornos sanitarios, dividido en las categorías que se detallan mas adelante.

- *portada.html* → Página que aparecerá dentro del frame principal, conteniendo una breve descripción de la herramienta.

- *fichaGeneral.html*→ formulario donde introducir los datos generales del sistema a analizar. Los campos que mostrará serán los siguientes:

    - Auditor: nombre de la persona que realiza la evaluación.

    - Proyecto/Sistema: nombre del proyecto a evaluar.

    - Empresa: nombre de la empresa propietaria del sistema informático a evaluar.

    - Responsable proyecto: nombre del responsable del proyecto a evaluar.

    - Responsable técnico: nombre del responsable técnico del proyecto a evaluar.

    - Descripción proyecto/sistema: breve descripción de la solución o sistema informático a evaluar, detallando las necesidades que cubre, así como una breve descripción de cómo consigue alcanzar dichos objetivos.

    - Hardware: listado del hardware que se incluye en la implantación del sistema a evaluar. (Servidores, estaciones de trabajo, periféricos, analizadores, equipos de electromedicina, etc.)

    - Software: listado de todo el software que se incluye en la implantación de la solución. (Desarrollo propio, bases de datos, drivers específicos, soluciones antivirus, etc.)

    - Requisitos adicionales: Listado de todos los requisitos técnicos adicionales que no se incluyen en la solución ofertada. (Hardware, Sistemas Operativos, Software adicional, licencias, etc.)

- *questions.html* → página donde se mostrarán y se editarán tanto las preguntas con las respuestas a las mismas.

  Constará de 50 cajas de texto con las preguntas junto con otras 50 cajas de texto con las respuestas sugeridas para cada caso.

  Las preguntas irán enumeradas del 1 al 50 y las respuestas irán tabuladas debajo de cada una de ellas.

  Al final de la página habrá un botón para guardar los cambios y un indicador con la fecha y hora de la última modificación.

- *checklist001.html* → página que contendrá las 50 preguntas relativas a sistemas informáticos en entornos sanitarios. Las preguntas se dividirán en las siguientes secciones:

- Arquitectura:
    - Características referente a servidores
    - Características referente a estaciones de trabajo
- Seguridad:
    - Características referente a servidores
    - Características referente a estaciones de trabajo
- Red: Características referentes al tipo de uso y seguridad en la red interna.
- Integración: características referentes a las tecnologías utilizadas para la integración de los diferentes sistemas.
- Gestión:
    - Características referente a servidores
    - Características referente a estaciones de trabajo
- Dispositivos:

  Cada sección irá en un cuadro de 6 columnas y las filas correspondientes al número de preguntas de cada tipo.

  Las 6 columnas se dividen de la siguiente manera:

    - 1. Enumeración de cada pregunta.
    - 2. Contenido de la pregunta.
    - 3. Casilla con un botón de opción para responder afirmativamente a la pregunta.
    - 4. Casilla con un botón de opción para responder negativamente a la pregunta.
    - 5. Casilla donde se indicara el peso que tendrá la pregunta.
    - 6. Casilla donde se indicará la puntuación obtenida en base a la respuesta de la pregunta.

  Al final del formulario se incluirá un botón de “Enviar” para procesar los datos y proceder a ver el informe final.

- *reportEstandar.html → página que contendrá el reporte final de propósito genérico. Contendrá los siguientes elementos:*

- Gráfica tipo barra horizontal donde se mostrará la “Valoración máxima posible”

- Gráfica tipo barra horizontal donde se mostrará la “Puntuación obtenida” tras la evaluación.

- Cuadros de texto donde se muestre la información introducida en el formulario fichaGeneral.html.

- Fecha y hora en la que se ha realizado en informe.

- Resultado cuestionario: cuadro de 3 columnas y 56 filas donde se mostrará:

    - 1. La enumeración de cada pregunta
    - 2. El contenido de la pregunta y la respuesta ofrecida por la herramienta.
    - 3. Una imagen de “check” si se ha respondido afirmativamente a la pregunta, o una imagen de un aspa si se ha respondido negativamente a la pregunta.

- Botón de impresión: botón para imprimir la página. Ejecutará el código *JavaScript:window.print()*

- *reportSanidad.html* → página que contendrá el reporte final de propósito específico para centros sanitarios y hospitales. Contendrá los siguientes elementos:

    - Gráfica tipo barra horizontal, donde se mostrará la “Valoración máxima posible”

    - Gráfica tipo barra horizontal, donde se mostrará la “Puntuación obtenida” tras la evaluación.

    - Seis gráficas tipo barra horizontal, que mostrará la relación de preguntas contestadas afirmativamente, clasificadas por las siguientes categorías:

        - Arquitectura
        - Seguridad
        - Red
        - Integración
        - Gestión
        - Dispositivos

    - Cuadros de texto donde se muestra la información introducida en el formulario fichaGeneral.html.

    - Fecha y hora en la que se ha realizado en informe.

- Resultado cuestionario: cuadro de 3 columnas y 56 filas donde se muestra:

    - 1. La enumeración de cada pregunta
    - 2. El contenido de la pregunta y la respuesta ofrecida por la herramienta.
    - 3. Una imagen de “check” si se ha respondido afirmativamente a la pregunta, o una imagen de un aspa si se ha respondido negativamente a la pregunta.

- Botón para imprimir la página. Ejecutará el código JavaScript:window.print()

La aplicación se diseña incluyendo por defecto una serie de preguntas, referentes a las características de sistemas de ingeniería médica o sistemas informáticos para hospitales. Pero el mismo hospital podrá darle un uso diferente a la herramienta. Si por ejemplo, los sistemas a analizar no tienen relación con la medicina, ni con la ley de protección de datos, etc. Este sería el caso por ejemplo, de todos los sistemas de mantenimiento de las propias instalaciones (control climatización, control de sistemas eléctricos…). En estos casos, seguramente la checklist que deba verificarse al estudiar un nuevo proyecto informático será diferente a la desarrollada en este proyecto.

2.3.2 Contenido e información

En este apartado se detalla el contenido y la información concreta que se incluye en cada una de las páginas mencionadas en el apartado anterior.

*2.3.2.1 Contenido página principal (*portada.html*)*

Está página se carga dentro del *frame* principal, donde se incluye una breve descripción de la herramienta, así como de su uso. El texto es el siguiente:

HITA (Healthcare IT Audit), es una herramienta creada para ayudar a los responsables de IT a evaluar y auditar cualquier proyecto que requiera la implantación de sistemas informáticos en la red de su organización. Su principal propósito es poder generar un informe donde se detallen las fortalezas y debilidades de cualquier proyecto nuevo que se requiera implantar en una organización. Del mismo modo, podrá ser utilizada por los proveedores de sistemas informáticos con el fin de evaluar su propio producto y conocer lo cerca o lejos que se encuentra respecto a las necesidades y requerimientos del cliente.

Aunque la herramienta es extensible a cualquier tipo de organización, por defecto, se ha alimentado con información específica para uso en centros sanitarios y hospitales.

HITA consta principalmente de un listado de preguntas referentes a la arquitectura, seguridad, integración, red, gestión y características de los diferentes dispositivos conectados a la red.

Para cada una de estas preguntas, se requiere contestar afirmativa o negativamente a las mismas, según el sistema evaluado cumpla o no con cada condición expuesta.

Dependiendo de la contestación a cada pregunta, la herramienta mostrará el correspondiente comentario o sugerencia, indicando especialmente aquellos puntos en los que no se cumplan las obligaciones legales en cuanto a protección de datos de carácter personal, así como sugerencias referentes a la seguridad de los sistemas.

Los pasos para su uso son los siguientes:

1. Acceder al menú "Editar" para revisar el listado de preguntas y respuestas. Si se realiza algún cambio, pulsar el botón "Guardar"

2. Acceder al menú "Checklist" y pulsar en el submenú "Ficha general". Aquí se deberán rellenar los datos solicitados de formas que se tenga la información básica necesaria referente al sistema a evaluar. Una vez rellenados todos los campos, pulsar en "Guardar"

3. Ir al menú "Checklist", y seleccionar el formulario deseado donde se deberá contestar a cada una de las preguntas. Cada pregunta tiene por defecto un peso de valor 1, en caso que se cumpla con el requisito en cuestión. En aquellas preguntas que se estimen más importantes y críticas se podrá poner un valor mayor. El sistema evaluado sumará 0 puntos en cada una de las preguntas donde no se cumpla con el requisito expuesto.
Una vez contestado todo el formulario, se deberá pulsar en "Enviar".

4. Tras el paso anterior, se abrirá el correspondiente Informe final.

2.3.2.2 Preguntas y respuestas (questions.html)

En esta página se gestionan todas las preguntas y respuestas que serán usadas después en las checklist.

Por defecto, la herramienta carga una serie de preguntas orientadas al ámbito sanitario, además del contenido sugerido por los proveedores y *Beta testers:*

- Pregunta 1: ¿El servidor será compatible con entorno virtual?
    - *Respuesta 1: La virtualización ofrece protección contra errores de hardware, gestión dinámica de recursos, simplifica la migración de servidores, posibilita copias de estado (Snapshot), mejora la gestión de backups, etc.*

- Pregunta 2: ¿Se incluye una solución backup específica?

    - *Respuesta2: Para realizar el backup con la solución corporativa, se deberá documentar la información que habrá que añadir en las políticas de salvaguarda de la organización.*

- Pregunta 3: Si se almacenan datos de paciente ¿se realizará backup de los datos un mínimo de una vez semanalmente??

    - *Respuesta 3: Incumplimiento del "Real Decreto 1720/2007 - Artículo 94. COPIAS DE RESPALDO Y RECUPERACIÓN"*

- Pregunta 4: ¿Dispone de redundancia de fuentes de alimentación?

    - Respuesta 4: Si el sistema incluye servidores sin fuente de alimentación redundante, no se garantiza la alta disponibilidad.

- Pregunta 5: ¿Existirá *teaming* de interfaces de red?

    - *Respuesta 5: Si el sistema incluye servidores sin interfaces de red redundante y trabajando en "teaming", no se garantiza la alta disponibilidad.*

- Pregunta 6: ¿Puede incorporarse al dominio corporativo?

    - *Respuesta 6: No se podrán aplicar las políticas de gestión, actualizaciones y seguridad corporativa.*

- Pregunta 7: ¿Alguno de los servicios requiere ser iniciado de forma interactiva, o se inician todos en el arranque del sistema?

    - *Respuesta 7: Tras un reinicio no controlado del servidor, deberían iniciarse todos los servicios automáticamente sin intervención humana.*

- Pregunta 8: Si alguno de los servicios o procesos necesarios para ejecutar el sistema se cae ¿el servidor dispone de un control automático para intentar volver a levantarlo?

    - *Respuesta 8: Si uno de los servicios o procesos necesarios para ofrecer el servicio se cae, el sistema debería disponer de un sistema automático (watchdog o equivalente) para detectar esta caída y restaurar el servicio.*

- Pregunta 9: ¿El servidor será compatible con entorno virtual?

    - *Respuesta 9: La virtualización ofrece protección contra errores de hardware, gestión dinámica de recursos, simplifica la migración de servidores, posibilita copias de estado (Snapshot), mejora la gestión de backups, etc.*

- Pregunta 10: ¿Puede el software cliente ejecutarse en un PC incluido en el dominio corporativo?

    - *Respuesta 10: Si el software cliente no se ejecuta en un PC incluido en el dominio corporativo, no se podrán aplicar las medidas y políticas de seguridad corporativas.*

- Pregunta 11: ¿Existe limitación de clientes concurrentes por licencias?

    - *Respuesta 11: Se deberá documentar la gestión de licencias, indicando claramente las restricciones de las mismas.*

- Pregunta 12: ¿Existe algún servicio propio del sistema a implantar que se ejecute con el usuario administrador o *root*?

    - *Respuesta 12: La ejecución de servicios y procesos con permisos de administrador o root, pueden comprometer la seguridad del sistema ante infecciones de virus o uso malintencionado.*

- Pregunta 13: Además del usuario administrador o *root* ¿requiere el sistema otros usuarios locales con privilegios de administrador?

    - *Respuesta 13: La ejecución de servicios y procesos con usuarios con permisos de administrador o root, pueden comprometer la seguridad del sistema ante infecciones de virus o uso malintencionado.*

- *Pregunta 14: ¿El servidor almacena datos de pacientes?*

    - *Respuesta 14: Se deberá documentar la información de pacientes que se gestiona y el tratamiento que se da a la misma.*

- Pregunta 15: En caso que el servidor almacene datos de paciente ¿están en una base de datos o fichero encriptado?

    - *Respuesta 15: Incumplimiento del "Artículo 9 (Ley Orgánica 15/1999)": garantizar la seguridad de los datos de carácter personal y evitar su ALTERACIÓN, pérdida, tratamiento o acceso no autorizado.*

- Pregunta 16: En caso que el servidor almacene datos de paciente ¿el acceso a la base de datos o fichero está restringido solo a usuarios autorizados?

    - *Respuesta 16: Incumplimiento del "Artículo 9 (Ley Orgánica 15/1999)": garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o ACCESO NO AUTORIZADO.*

- Pregunta 17: En caso que el servidor almacene datos de paciente ¿existe un log de accesos que registre las acciones que realizan los usuarios, así como la fecha e identidad del mismo?

    - *Respuesta 17: Incumplimiento del "Artículo 9 (Ley Orgánica 15/1999)": garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.*

❖ Pregunta 18: En caso que el servidor no almacene datos de paciente ¿existe un log de accesos al sistema que identifique la fecha y el usuario que ha accedido?

    - *Respuesta 18: En la medida de lo posible, se estima necesario registrar los accesos que se realizan en un sistema para detectar un posible uso irregular del mismo.*

- Pregunta 19: Si el sistema incluye un servidor ¿es éste compatible con soluciones antivirus?

    - *Respuesta 19: No se deberá conectar a la red corporativa ninguna estación de trabajo sin protección antivirus, por lo que se requiere un documento detallado de exclusiones necesarias para que el sistema funcione con un sistema antimalware.*

❖ Pregunta 20: ¿Permite el servidor ser monitorizado vía SNMP?

    - *Respuesta 20: La monitorización de servidores y dispositivos es necesaria para conocer su estado y actividad en todo momento, pudiéndose garantizar una gestión proactiva además de la reactiva.*

- Pregunta 21: ¿El servidor requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?

    - *Respuesta 21: Compartir carpetas en los servidores requiere un control periódico de las autorizaciones a las mismas, no recomendándose nunca los accesos con permisos de escritura, salvo en servidores de ficheros.*

❖ Pregunta 22: Si el servidor requiere compartir alguna carpeta compartida en de disco, con permisos de lectura y escritura ¿tiene activa la auditoria de accesos a los ficheros de dicho recurso?

    - *Respuesta 22: Si es requisito la compartición de carpetas en un servidor con permisos de escritura, se requiere la activación de auditoria de accesos a las mismas, con el fin de identificar el origen de la pérdida o modificación de la información.*

- Pregunta 23: ¿Se almacena algún tipo de dato de pacientes localmente en el PC?

    - *Respuesta 23: Nunca debería almacenarse información de pacientes en sistemas que físicamente no estén en un CPD o ubicación con las correspondientes medidas de seguridad físicas y lógicas.*

❖ Pregunta 24: ¿El acceso al software cliente requiere autenticación?

    - *Respuesta24: Tanto si se almacenan datos de paciente como si no, será necesario un control de accesos a los mismos con el fin de evitar usos no autorizados.*

- Pregunta 25: Si desde el software cliente se accede a datos de paciente ¿obliga este a cambiar la contraseña como mínimo una vez al año?

    - *Respuesta 25: Incumplimiento "Real Decreto 1720/2007 - Artículo 93. IDENTIFICACIÓN Y AUTENTICACIÓN". La periodicidad de cambio de contraseña NO SERÁ SUPERIOR A UN AÑO, mientras estén vigentes, y se almacenarán de forma ininteligible.*

❖ Pregunta 26: ¿La contraseña se almacena localmente o en un servidor de forma ininteligible?

    - *Respuesta 26: Incumplimiento del "Real Decreto 1720/2007 - Artículo 93. IDENTIFICACIÓN Y AUTENTICACIÓN". La periodicidad de cambio de contraseña no será superior a un año, mientras estén vigentes, y SE ALMACENARÁN DE FORMA ININTELIGIBLE.*

- Pregunta 27: Si el sistema almacena datos de pacientes ¿dispone el sistema protección ante continuos intentos fallidos para acceder al sistema?

    - *Respuesta 27: Incumplimiento del Real Decreto 1720/2007 - Artículo 98. IDENTIFICACIÓN Y AUTENTICACIÓN. Se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.*

❖ Pregunta 28: ¿El PC requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?

    - *Respuesta 28: Se debe evitar que los sistemas requieran compartir carpetas en las estaciones de trabajo, debiéndose usar para ello los correspondientes servidores, garantizando un control de acceso, copias de respaldo, etc.*

- Pregunta 29: ¿Es el software cliente compatible con soluciones antivirus?

- *Respuesta 29: No se deberá conectar a la red corporativa ninguna estación de trabajo sin protección antivirus, por lo que se requiere un documento detallado de exclusiones necesarias para que el sistema funcione con un sistema antimalware.*

❖ Pregunta 30: Si el sistema requiere la instalación de estaciones de trabajo no corporativas ¿el acceso a la BIOS de las mismas dispone de contraseña?

- *Respuesta 30: Se requiere bloquear en la medida de lo posible el uso de los puertos USB, con el fin de evitar el uso de los mismos para el intercambio de ficheros con riesgo de infección, así como el arranque de la estación con un S.O. Live por personas no autorizadas..*

- Pregunta 31: ¿El sistema requiere ser accesible desde fuera de la red corporativa para su normal funcionamiento?

  - *Respuesta 31: Se deberá controlar la activación de los accesos por SSH o RDP, así como el usuario administrador o root para su administración.*

❖ Pregunta 32: ¿El sistema requiere acceder desde la LAN interna a algún servidor externo?

- *Respuesta 32: Se deberá documentar las IP, URL y puertos a los que el sistema requiere acceder para su funcionamiento normal.*

- Pregunta 33: ¿Se requiere de algún tipo de tráfico *Broadcast* para el envío de información a los dispositivos que forman el sistema a implantar?

  - *Respuesta 33: El tráfico Broadcast está limitado a subredes y VLAN, por lo que si el sistema lo requiere, deberá documentarse al detalle su uso y características.*

❖ Pregunta 34: ¿Existe una estimación aproximada de la cantidad de tráfico que generará el sistema?

- *Respuesta 34: Siempre que sea posible, se requiere conocer la cantidad de tráfico aproximada que generará el sistema.*

- Pregunta 35: ¿El sistema requiere la integración con alguno de los sistemas asistenciales?

  - *Respuesta 35: Se deberá documentar en detalle el uso que se hará de los datos del HIS.*

❖ Pregunta 36: En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante HL7?

- *Respuesta 36: Indicar protocolo de integración alternativo usado.*

- Pregunta 37: En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante DICOM?

  - *Respuesta 37: Necesario para la integración con servidores de imágenes (PACS)*

❖ Pregunta 38: En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante *Web Services*?

  - *Respuesta 38: No se podrán aplicar las políticas de gestión, actualizaciones y seguridad corporativa.*

- Pregunta 39: ¿Se usará un interface tipo ILO para la administración remota de los servidores?

  - *Respuesta 39: Si se incluye un servidor físico, deberá poderse acceder al mismo a través del interface ILO o similar para tener acceso de consola.*

❖ Pregunta 40: ¿Se dará soporte remoto mediante una conexión VPN o encriptada? (Obligatorio si se almacenan datos de pacientes).

  - *Respuesta 40: Incumplimiento del "Real Decreto 1720/2007 - Artículo 104. TELECOMUNICACIONES". La transmisión de datos de carácter personal a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando dichos datos.*

- Pregunta 41: ¿Tras la implantación del proyecto se entrega documentación de administración básica?

  - *Respuesta 41: Se requiere la entrega de documentación de administración básica del sistema.*

❖ Pregunta 42: ¿Se ofrece facilidades para realizar algún plan de contingencia para momentos en los que el sistema esté caído?

  - *Respuesta 42: Ante caídas de servicio o pérdida de red, se valoran positivamente posibles medidas de contingencia localmente a través de las estaciones de trabajo u otras opciones.*

- Pregunta 43: ¿El sistema dispone de mecanismos de monitorización y alertas ante posibles problemas que revisará el proveedor?

  - *Respuesta 43: Se valora positivamente la monitorización del estado de los sistemas por parte del proveedor, con el fin de ofrecer un soporte proactivo en todo momento.*

- Pregunta 44: ¿Se requiere la instalación de algún software específico para realizar su administración remota?

    - *Respuesta 44: La administración remota debe realizarse siempre con la solución VPN o segura ofrecida por el cliente.*

- Pregunta 45: ¿Alguno de los dispositivos requiere de conversor serie/Ethernet para conectarse a la red?

    - *Respuesta 45: Se requiere evitar el uso de dispositivos tipo MOXA, Lantronic, etc. ya que añaden puntos de posibles fallos en las comunicaciones de los dispositivos.*

- Pregunta 46: ¿Existen dispositivos conectados a la red corporativa, administrados remotamente mediante un protocolo no seguro? (html, ftp, telnet)

    - *Respuesta46: La administración de todos los dispositivos debe realizarse por medio de protocolos seguros (https, ssh, sftp, etc.)*

- Pregunta 47: ¿Para administrar el dispositivo se requiere de usuario y contraseña robusta?

    - *Respuesta 47: La contraseña para administrar los dispositivos deberá contener intercalados un mínimo de ocho caracteres alfanuméricos en mayúsculas, minúsculas.*

- Pregunta 48: ¿Los interfaces de los dispositivos conectados a la red soportan modos de 100 Mbps Full Duplex?

    - *Respuesta 48: Se requiere que los dispositivos usen interfaces compatibles con velocidades de 1Gbps o superiores.*

- Pregunta 49: ¿Los interfaces de los dispositivos conectados a la red soportan modos de 1 Gbps Full Duplex?

    - *Respuesta 49: Se requiere que los dispositivos usen interfaces compatibles con velocidades de 1Gbps o superiores.*

- Pregunta 50: Si alguno de los dispositivos del sistema requiere conexión Wi-Fi ¿Soporta autenticación a la red mediante certificados?

    - *Respuesta 50: Se requiere el uso de certificados para autenticarse en la red Wi-Fi.*

2.3.2.3 Formulario (cheklist001.html)

A continuación, se detalla la clasificación que se realiza de las preguntas pre cargadas en la herramienta (questions.html) es decir, tal y como aparecen en esta página:

- **Arquitectura**

  Referente a servidores:

  - Pregunta 1: ¿El servidor será compatible con entorno virtual?

  ❖ Pregunta 2: ¿Se incluye una solución backup específica?

  - Pregunta 3: Si se almacenan datos de paciente ¿Se realizará backup de los datos un mínimo de una vez semanalmente?

  ❖ Pregunta 4: ¿Dispone de redundancia de fuentes de alimentación?

  - Pregunta 5: ¿Existirá *teaming* de interfaces de red?

  ❖ Pregunta 6: ¿Puede incorporarse al dominio corporativo?

  - Pregunta 7: ¿Alguno de los servicios requiere ser iniciado de forma interactiva, o se inician todos en el arranque del sistema?

  ❖ Pregunta 8: Si alguno de los servicios o procesos necesarios para ejecutar el sistema se cae ¿el servidor dispone de un control automático para intentar volver a levantarlo?

  Referente a estaciones de trabajo:

  - Pregunta 9: ¿El servidor será compatible con entorno virtual?

  ❖ Pregunta 10: ¿Puede el software cliente ejecutarse en un PC incluido en el dominio corporativo?

  - Pregunta 11: ¿Existe limitación de clientes concurrentes por licencias?

- **Seguridad**

  Referente a servidores:

  ❖ Pregunta 12: ¿Existe algún servicio propio del sistema a implantar que se ejecute con el usuario administrador o *root*?

  - Pregunta 13: Además del usuario administrador o *root* ¿requiere el sistema otros usuarios locales con privilegios de administrador?

❖ *Pregunta 14: ¿El servidor almacena datos de pacientes?*

- Pregunta 15: En caso que el servidor almacene datos de paciente ¿están en un a base de datos o fichero encriptado?

❖ Pregunta 16: En caso que el servidor almacene datos de paciente ¿el acceso a la base de datos o fichero está restringido solo a usuarios autorizados?

- Pregunta 17: En caso que el servidor almacene datos de paciente ¿existe un log de accesos que registre las acciones que realizan los usuarios, así como la fecha e identidad del mismo?

❖ Pregunta 18: En caso que el servidor no almacene datos de paciente ¿existe un log de accesos al sistema que identifique la fecha y el usuario que ha accedido?

- Pregunta 19: Si el sistema incluye un servidor ¿es este compatible con soluciones antivirus?

❖ Pregunta 20: ¿Permite el servidor ser monitorizado vía SNMP?

- Pregunta 21: ¿El servidor requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?

❖ Pregunta 22: Si el servidor requiere compartir alguna carpeta compartida en de disco, con permisos de lectura y escritura ¿tiene activa la auditoria de accesos a los ficheros de dicho recurso?

Referente a estaciones de trabajo:

- Pregunta 23: ¿Se almacena algún tipo de dato de pacientes localmente en el PC?

❖ Pregunta 24: ¿El acceso al software cliente requiere autenticación?

- Pregunta 25: Si desde el software cliente se accede a datos de paciente ¿obliga este a cambiar la contraseña como mínimo una vez al año?

❖ Pregunta 26: ¿La contraseña se almacena localmente o en un servidor de forma ininteligible?

- Pregunta 27: Si el sistema almacena datos de pacientes ¿dispone el sistema protección ante continuos intentos fallidos para acceder al sistema?

❖ Pregunta 28: ¿El PC requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?

- Pregunta 29: ¿Es el software cliente compatible con soluciones antivirus?

❖ Pregunta 30: Si el sistema requiere la instalación de estaciones de trabajo no corporativas ¿el acceso a la BIOS de las mismas dispone de contraseña?

➢ **Red**

- Pregunta 31: ¿El sistema requiere ser accesible desde fuera de la red corporativa para su normal funcionamiento?

❖ Pregunta 32: ¿El sistema requiere acceder desde la LAN interna a algún servidor externo?

- Pregunta 33: ¿Se requiere de algún tipo de tráfico *Broadcast* para el envío de información a los dispositivos que forman el sistema a implantar?

❖ Pregunta 34: ¿Existe una estimación aproximada de la cantidad de tráfico que generará el sistema?

➢ **Integración**

- Pregunta 35: ¿El sistema requiere la integración con alguno de los sistemas asistenciales?

❖ Pregunta 36: En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante HL7?

- Pregunta 37: En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante DICOM?

❖ Pregunta 38: En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante *Web Services*?

➢ **Gestión y Administración**

Referente a servidores:

- Pregunta 39: ¿Se usará un interface tipo ILO para la administración remota de los servidores?

❖ Pregunta 40: ¿Se dará soporte remoto mediante una conexión VPN o encriptada? (Obligatorio si se almacenan datos de pacientes).

- Pregunta 41: ¿Tras la implantación del proyecto se entrega documentación de administración básica?

❖ Pregunta 42: ¿Se ofrece facilidades para realizar algún plan de contingencia para momentos en los que el sistema esté caído?

Referente a estaciones de trabajo:

- Pregunta 43: ¿El sistema dispone de mecanismos de monitorización y alertas ante posibles problemas que revisará el proveedor?

❖ Pregunta 44: ¿Se requiere la instalación de algún software específico para realizar su administración remota?

➢ **Dispositivos**

- Pregunta 45: ¿Alguno de los dispositivos requiere de conversor serie/Ethernet para conectarse a la red?

❖ Pregunta 46: ¿Existen dispositivos conectados a la red corporativa, administrados remotamente mediante un protocolo no seguro? (html, ftp, telnet)

- Pregunta 47: ¿Para administrar el dispositivo se requiere de usuario y contraseña robusta?

❖ Pregunta 48: ¿Los interfaces de los dispositivos conectados a la red soportan modos de 100 Mbps Full Duplex?

- Pregunta 49: ¿Los interfaces de los dispositivos conectados a la red soportan modos de 1 Gbps Full Duplex?

❖ Pregunta 50: Si alguno de los dispositivos del sistema requiere conexión Wi-Fi ¿soporta autenticación a la red mediante certificados?

2.4 Diseño lógico del prototipo

En esta sección se describe cual es el funcionamiento lógico de la aplicación.

El propósito de la herramienta no es valorar si el sistema a estudiar dispone de una buena implementación de una característica concreta, o si cumple adecuadamente con los objetivos por los cuales se ha adquirido, ya que eso lo deberá detallar el proveedor al presentar su propuesta sobre el pliego de condiciones publicado, mediante las correspondientes presentaciones de sus productos. Sin embargo, mediante HITA se sabrá en un primer estudio, de cada propuesta, si un sistema concreto cumple o no con unos requisitos mínimos en cuanto a seguridad y buenas prácticas informáticas.

2.4.1 Sistema de puntuación

La herramienta ofrece la opción de definir el grado de importancia de cada característica mediante un valor de importancia y una puntuación obtenida. Es decir, ya que todos los proyectos o sistemas no son iguales, no manejan la misma cantidad de información, el mismo tipo de datos sensibles a ser protegidos, etc. el estudio no será el mismo para todos los casos. Es por ello por lo que, en la herramienta se debe especificar para cada característica, un peso o valor concreto. Este peso, es por defecto igual a 1 para los casos en los que la respuesta sea afirmativa, y a 0 para los casos en los que sea negativa.

Ejemplo 1:

1. Característica 1: ¿El sistema cuenta con auditoria y log de accesos?
2. Característica 2: ¿Se permite monitorizar el sistema vía SNMP?

Suponiendo que ambas preguntas tienen la misma relevancia en el proyecto a estudiar, ambas tendrán el mismo peso.

Si la respuesta a la pregunta es afirmativa, es decir, que efectivamente *el sistema dispone de auditoria y log de accesos*, entonces la puntuación individual para esta característica será finalmente de 1.

Por el contrario, si la respuesta a la pregunta es negativa, es decir, que *el sistema no dispone de auditoria y log de accesos*, entonces la valoración individual para esa característica será de 0.

Ejemplo 2:

1. Característica 1: ¿El sistema cuenta con auditoria y log de accesos?
2. Característica 2: ¿Se permite monitorizar el sistema vía SNMP?

Suponiendo que la primera se trata de una característica considerada como muy importante para este proyecto, esta se puntuará con un peso alto. Si en la evaluación se está asignado un valor máximo de 10 a las características de mayor importancia, a esta cuestión se le asignará entonces un peso de 10.

Si la respuesta a la pregunta es afirmativa, es decir, que efectivamente el sistema dispone de auditoria y log de accesos, entonces la valoración individual para esa característica será finalmente de 10 puntos.

Si la respuesta a la pregunta es negativa, es decir, que el sistema no dispone de auditoria y log de accesos, la valoración individual para esa característica será entonces de 0 puntos.

Por otro lado, suponiendo que la segunda característica se trate de una característica considerada como menos importante para este proyecto, aunque el sistema evaluado disponga de la misma, esta se puntuará con un peso bajo. Como se indicaba anteriormente, por defecto tendrá un valor de 1 punto.

Es decir, aunque el sistema a estudiar dispone de ambas características, en este caso, se le da mayor importancia a la primera.

La tabla tipo TCO para con los datos calculados con esta versión de HITA sería similar a esta:

Tabla 3: Ejemplo de puntuación calculada en la evaluación de un sistema.

Característica	Respuesta (Si/No)	Valoración	Puntuación
Arquitectura			
Característica 1	Si	1	1
Característica 2	No	5	0
Característica 3	Si	0	0
Seguridad			
Característica 4	Si	3	3
Característica 5	Si	2	2
Característica 6	No	1	0
Red			
Característica 7	No	6	0
Característica 8	Si	1	1
Característica 9	Si	0	0
Integración			
…	…	…	0
Característica 50	Si	4	4
Total			**11**

Ejemplo 3:

Un hospital publica las bases para la obtención de un sistema de almacenamiento y dispensación automática de medicamentos para su servicio de Farmacia. A dicha licitación se presentan tres empresas, cada una de ellas ofreciendo su propio sistema de ingeniería médica, además de su correspondiente sistema informático.

A: Propuesta de sistema presentado por la empresa A.
B: Propuesta de sistema presentado por la empresa B.
C: Propuesta de sistema presentado por la empresa C.

Tabla 4: Ejemplo de puntuación calculada en la evaluación de tres sistemas diferentes para un mismo proyecto.

	Respuestas				Puntuación obtenida		
Característica	**A**	**B**	**C**	**Valor**	**A**	**B**	**C**
Característica 1	Si	No	Si	3	3	0	3
Característica 2	No	Si	Si	5	0	5	5
Característica 3	Si	Si	Si	1	1	1	1
Característica 4	Si	Si	Si	3	3	3	3
Característica 5	Si	Si	Si	2	2	2	2
Característica 6	No	No	Si	1	0	0	1

Característica 7	No	Si	No	6	0	6	0
Característica 8	Si	No	Si	1	1	0	1
Característica 9	Si	No	Si	0	0	0	0
Característica 10	Si	No	No	4	4	0	0
Total					**14**	**17**	**16**

Como se observa en la tabla anterior, la empresa A cumple con 7 de las características solicitadas, la empresa B tan solo 5 de las características solicitadas, mientras que la empresa C cumple con 8 de las características solicitadas.

Sin embargo, en este ejemplo resulta ganadora la empresa B, ya que aunque su sistema no disponga de tantas funcionalidades, cumpliendo con menos de las características solicitadas, es la única de las tres que presenta un sistema que dispone de la característica 7, lo cual hace que obtenga la mayor puntuación. Este hecho se considera crítico por el hospital, por ello le asigna dicho valor.

2.4.2 Navegación y uso

En esta sección se describen los pasos que se deben dar para un uso correcto de la aplicación. Del mismo modo, se detallan las operaciones y acciones que realiza la misma ante determinadas interacciones.

2.4.2.1 Primer paso

Una vez iniciada la aplicación se interactúa con la herramienta mediante el menú superior. El primer paso obligatorio, será entrar en el menú “Editor” para editar el listado de preguntas y respuestas que se usarán en los siguientes pasos.

Por defecto, la aplicación carga siempre las mismas 50 preguntas y respuestas. Si se desean usar otras diferentes se deberán modificar en esta pantalla.

El orden de tabulación empieza por la primera pregunta, continua por la respuesta a la misma y así sucesivamente hasta llegar a la pregunta número 50.

Una vez modificado el contenido se pulsará el botón de “Guardar” para almacenar los cambios. El contenido de cada pregunta es almacenado en una variable global, es decir, existen 50 variables con una nomenclatura del tipo *varQuestion01, varQuestion02, varQuestion03*, etc.

Del mismo modo, para cada respuesta, la aplicación utiliza otras 50 variables globales con una nomenclatura del tipo *varAnswer01, varAnswer02, varAnswer03*, etc.

Tanto las variables *varQuestion* como las *varAnswer*, tienen en el inicio un valor pre asignado, es por ello que la herramienta mostrará siempre este contenido cada vez que se arranque el navegador.

2.4.2.1 Segundo paso

Una vez editadas las preguntas, se debe abrir el submenú “Ficha general” situado dentro del menú “Formulario”.

En esta página, se rellenan todos los campos solicitados, ya que aunque en el prototipo no son obligatorios, son necesarios para mostrar la información correspondiente más adelante al generar los informes.

En este formulario el orden de tabulación comienza por el primer campo “Auditor” y termina en orden por el último campo “Requisitos adicionales”

Por otro lado, existe un *tooltip* asociado a cada caja de texto que describe la información solicitada en cada una de ellas.

El contenido de cada campo se almacena en una variable global de texto.

2.4.2.1 Tercer paso

Tras rellenar los datos básicos del proyecto a evaluar en el paso anterior, se deberá acceder al submenú “Checklist sanidad” situado dentro del menú “Formulario”, para acceder al formulario donde se contestan y puntuan las correspondientes preguntas.

Al cargarse la página, *Axure* ofrece un evento llamado “onPageLoad” dentro del cual se asigna el contenido de las variables *varQuestion* y *varAnswer* a cada casilla de la tabla mostrada.

A continuación, se debe indicar el peso que se le asigna a cada pregunta dependiendo de su importancia. Por defecto, las 50 preguntas mostradas tienen el mismo peso, se muestran con un valor de 1.

Tras el paso anterior, se debe contestar a cada una de las preguntas mediante los botones de opción, indicando para cada caso, si el sistema a evaluar cumple o no con la característica cuestionada.

Aunque *Axure* no dispone de variables booleanas, se han creado 50 variables con una nomenclatura del tipo *varBooleanQ01, varBooleanQ02, varBooleanQ03*, etc… asignándose el valor “False” en caso que se haya contestado a la pregunta negativamente, o “True” en caso que se haya contestado afirmativamente.

Cada vez que se contesta una pegunta, se calcula su valor mostrándose en la columna “Puntuación”. Del mismo modo, cada vez que se modifica manualmente la columna valor, se realiza el mismo cálculo teniendo en cuenta el estado de la respuesta, es decir, si se había contestado afirmativamente a la

pregunta, la puntuación será la indicada en la casilla “Valor”. Si por el contrario la respuesta está sin contestar, o la contestación es negativa, la puntuación será igual a 0.

Finalmente se deberá pulsar en el botón “Guardar” para que se almacenen todos los datos. En este punto además, la aplicación realiza la suma de las puntuaciones obtenidas para cada una de las categorías (Arquitectura, Seguridad, Red, Integración, Gestión y Dispositivos). Esta información se almacena en variables globales que serán usadas después a la hora de mostrar las gráficas de los informes.

2.4.2.1 Cuarto paso

Una vez que le herramienta ya dispone de todos los datos necesarios para generar el informe, se podrá seleccionar entre dos tipos de informes. El primero de propósito general, y el segundo más orientado al entorno sanitario (en este prototipo la diferencia está en las gráficas dibujadas y los campos mostrados)

En caso que se haya seleccionado el informe de propósito general, se muestra una gráfica donde se indica el valor máximo obtenible, y el valor obtenido. Además, se muestra toda la información referente al proyecto insertada previamente en la página fichaGeneral.html.

Tras esta información, existe un botón “Mostrar respuesta” mediante el cual se podrá ver el resultado de cada pregunta, indicando una imagen de *check* verde cuando su respuesta ha sido afirmativa, o un aspa roja en caso contrario. Para los casos en los que la respuesta haya sido negativa, se mostrará bajo a cada pregunta, la respuesta sugerida, incluso el artículo de la legislación actual que se incumple.

Del mismo modo que en el caso anterior, se ofrece un informe con un formato diferente, en principio pensado para entornos sanitarios. La gran diferencia entre ambos informes está en las gráficas que se muestran. En este caso además de mostrar la puntuación general y la puntuación obtenida, se muestra la puntuación máxima posible y la obtenida para cada sub apartado del *checklis*t.

2.5 Prototipo

Se ha utilizado una versión trial del software *Axure* para realizar un prototipo, que además de permitir realizar el diseño y maquetación visual, permite dotar al prototipo de la funcionalidad necesaria.

El resultado que ofrece esta herramienta no es el más optimo, ya que genera mucho código que podría ser evitado o depurado, pero para el propósito de este proyecto es suficiente.

Una primera fase de este desarrollo es el que se ha enviado a los proveedores y hospitales que han mostrado interés en hacer de *Beta tester*. Concretamente:

- *O.M.P*, de la compañía *Roche Diagnostics*
- *C.F.G*, de la compañía *Siemens*.
- *U.F, de la empresa Agfa*
- *B.C.A.* del *Hospital Universitario de Cruces* (Bizkaia)
- *A.L.I.* del *Hospital Universitario de Araba*
- *C.A.V.* del Hospital de Zaragoza
- *V.F del Hospital Universitario de Gran Canaria Doctor Negrín*

El prototipo enviado, realmente no tenía desarrollada toda la lógica de le herramienta, pero lo realmente interesante era su contenido, por lo que las impresiones recibidas han sido muy satisfactorias.

Califican de excelente la herramienta, valorando la utilidad real para su uso en su propia organización. Entre las sugerencias recibidas destacan las siguientes:

- Concretar cuando una característica o la carencia de ella incumple una ley o no.

  Aunque en la planificación inicial no estaba contemplado, ahora el informe final indicará aquellos artículos de la legislación que no cumpla cada sistema auditado.

- Ofrecer la opción de sacar varios tipos de informes, según el tipo de proyecto u organización, o realizando una clasificación concreta de las preguntas.

  La herramienta ofrecerá ahora un nuevo informe (ya detallado anteriormente en este documento). Es decir, existirá un informe estándar donde no se hará ninguna clasificación por tipo de pregunta, además de otro en el que existirá una clasificación concreta.

- Para la checklist de entornos sanitarios, se han sugerido una serie de preguntas interesantes (ya incluidas en el checklist detallado anteriormente en este documento)

- Así mismo, varios de ellos sugieren la posibilidad de crear diferentes checklist con opción de guardado, o la posibilidad de crear checklist de forma dinámica pudiendo ser guardadas para su posterior uso.

  Realmente, la herramienta carga las preguntas de forma dinámica, ya que el listado de preguntas y respuestas se pueden editar y guardar. Pero Axure no permite leer información de ficheros por lo que se utilizan variables globales donde se almacenan las preguntas y respuestas. Es decir, la herramienta arranca con unas preguntas y respuesta concretas, estas podrán ser modificadas, pero una vez cerrada la aplicación, se pierden todos los cambios. Esta es una de las sugerencias que se indicarán mas adelante en el documento, como posible característica de mejora para una versión no beta, o prototipo.

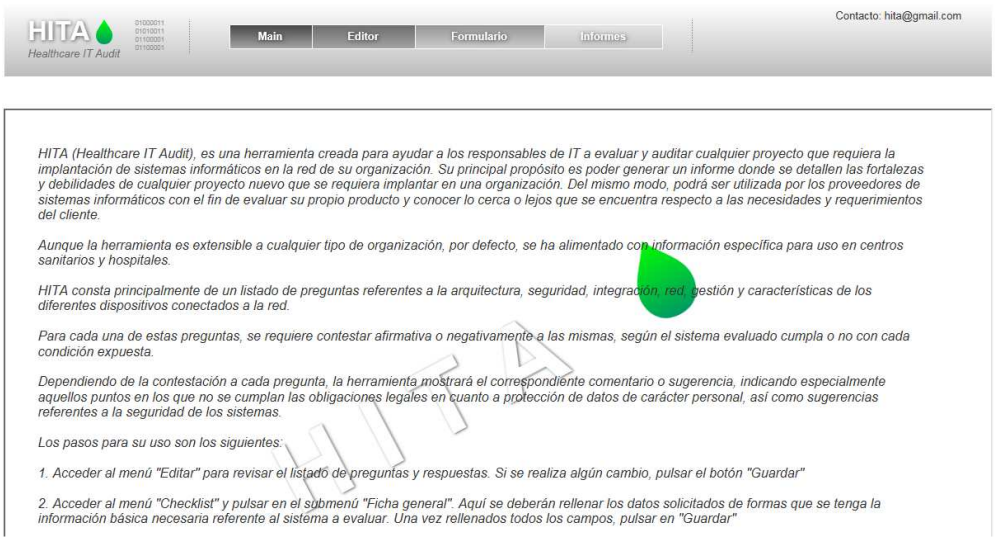
A continuación se muestran las diferentes páginas tal como se han maquetado en Axure.

2.5.1 Página principal (main.html)

Imagen 11: Página principal del prototipo HITA

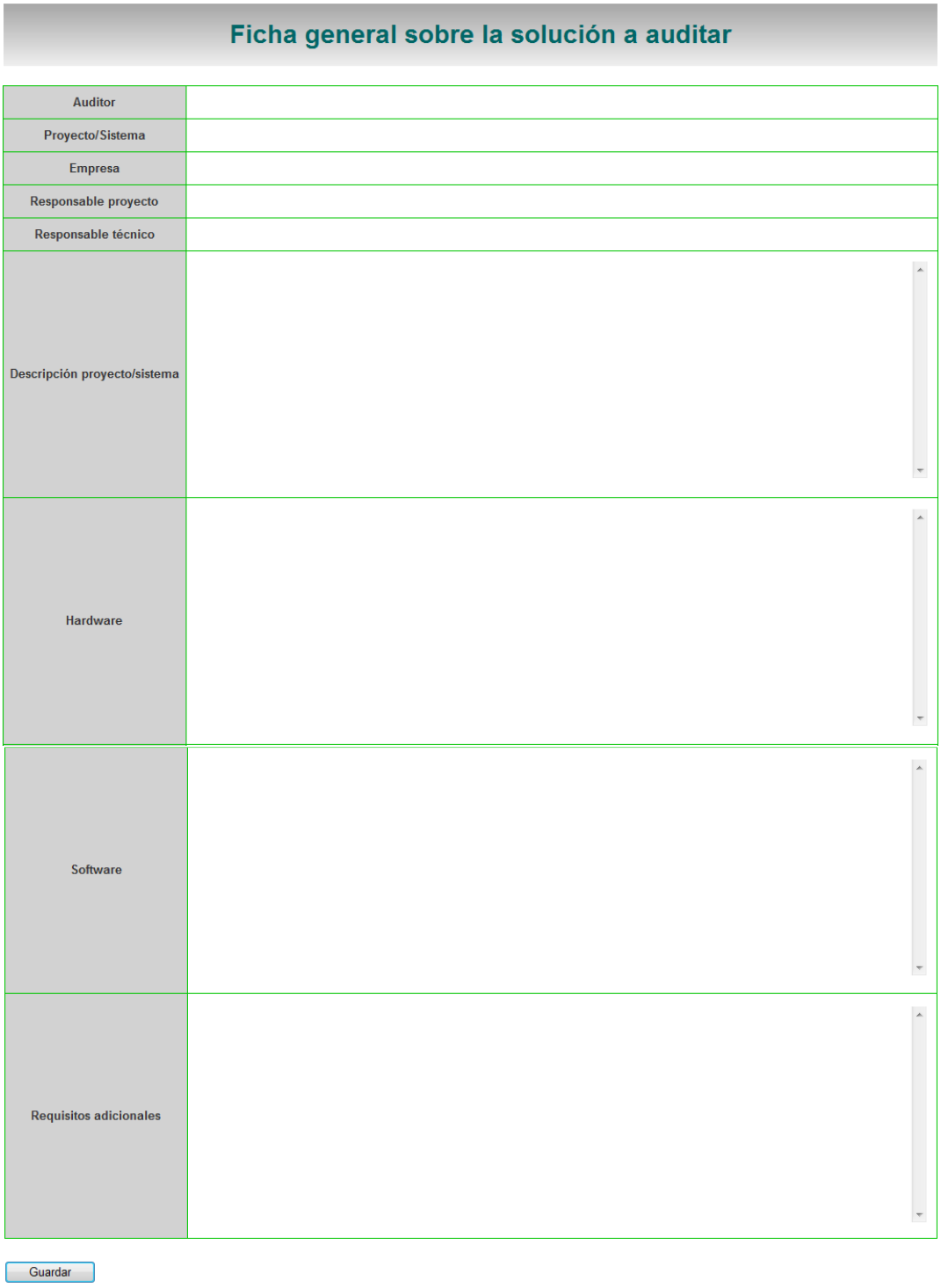
2.5.2 Portada (portada.html)

Imagen 12: Portada del prototipo HITA



2.5.3 Formulario – Ficha general (fichaGeneral.html)

Imagen 13: Página “Ficha General” del prototipo HITA



2.5.3 Checklist (checklist001.html)

Imagen 14: Página de *checklist* del prototipo HITA

Checklist para soluciones en entorno sanitario

Arquitectura

	Características Servidores	Si	No	Valor	Puntuación
1	¿El servidor será compatible con entorno virtual?	○	○	1	0
2	¿Se incluye una solución backup específica?	○	○	1	0
3	Si se almacenan datos de paciente ¿se realizará backup de los datos un mínimo de una vez semanalmente?	○	○	1	0
4	¿Dispone de redundancia de fuentes de alimentación?	○	○	1	0
5	¿Existirá teaming de interfaces de red?	○	○	1	0
6	¿Puede incorporarse al dominio corporativo?	○	○	1	0
7	Alguno de los servicios requiere ser iniciado de forma interactiva, o se inician todos en el arranque del sistema?	○	○	1	0
8	Si alguno de los servicios o procesos necesarios para ejecutar el sistema se cae ¿el servidor dispone de un control automatico para intentar volver a levantarlo?	○	○	1	0
	Características PC	**Si**	**No**	**Valor**	
9	¿El software es compatible con el sistema operativo y customización corporativa de la organización?	○	○	1	0
10	¿Puede este estar en el dominio corporativo?	○	○	1	0
11	¿Existe limitación de clientes concurrentes por licencias?	○	○	1	0

Seguridad

	Características Servidores	Si	No	Valor	Puntuación
12	¿Existe algún servicio propio del sistema a implantar que se ejecute con el usuario administrador o root?	○	○	1	0
13	Además del usuario administrador o root ¿requiere el sistema otros usuarios locales con privilegios de administrador?	○	○	1	0
14	¿El servidor almacena datos de pacientes?	○	○	1	0
15	En caso que el servidor almacene datos de paciente ¿están en un a base de datos o fichero encriptado?	○	○	1	0
16	En caso que el servidor almacene datos de paciente ¿el acceso a la base de datos o fichero está restringido solo a usuarios autorizados?	○	○	1	0
17	En caso que el servidor almacene datos de paciente ¿existe un log de accesos que registre las acciones que realizan los usuarios, así como la fecha e identidad del mismo?	○	○	1	0
18	En caso que el servidor no almacene datos de paciente ¿existe un log de accesos al sistema que identifique la fecha y el usuario que ha accedido?	○	○	1	0
19	¿Es el sistema compatible con soluciones antivirus?	○	○	1	0
20	¿Permite el servidor ser monitorizado vía SNMP?	○	○	1	0
21	¿El servidor requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?	○	○	1	0
22	Si el servidor requiere compartir alguna carpeta compartida en de disco, con permisos de lectura y escritura ¿tiene activa la auditoria de accesos a los ficheros de dicho recurso?	○	○	1	0
	Características PC	**Si**	**No**	**Valor**	
23	¿Se almacena algún tipo de dato de pacientes localmente en el PC?	○	○	1	0
24	¿El acceso al software cliente requiere autenticación?	○	○	1	0
25	Si desde el software cliente se accede a datos de paciente, obliga esta a cambiar la contraseña como mínimo una vez al año?	○	○	1	0
26	¿La contraseña se almacena localmente o en un servidor de forma ininteligible?	○	○	1	0
27	Si el sistema almacena datos de pacientes ¿dispone el sistema protección ante continuos intentos fallidos para acceder al sistema?	○	○	1	0
28	¿El PC requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?	○	○	1	0
29	¿Es el software cliente compatible con soluciones antivirus?	○	○	1	0
30	¿El acceso a la BIOS dispone de contraseña?	○	○	1	0

Red

	Caracteristicas	Si	No	Valor	Puntuación
31	¿El sistema requiere ser accesible desde fuera de la red corporativa para su normal funcionamiento?			1	0
32	¿El sistema requiere acceder desde la LAN interna a algún servidor externo?			1	0
33	¿Se requiere de algún tipo de tráfico Broadcast para el envío de información a los dispositivos que forman el sistema a implantar?			1	0
34	¿Existe una estimación aproximada de la cantidad de tráfico que generará el sistema?			1	0

Integración

	Caracteristicas Servidores	Si	No	Valor	Puntuación
35	¿El sistema requiere la integración con alguno de los sistemas asistenciales?			1	0
36	En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante HL7?			1	0
37	En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante DICOM?			1	0
38	En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante Web Services?			1	0

Gestión y Administración

	Caracteristicas Servidores	Si	No	Valor	Puntuación
39	¿Se usará un interface ILO para la administración remota?			1	0
40	¿Se dará soporte remoto mediante una conexión VPN o encriptada? (Obligatorio si se almacenan datos de pacientes).			1	0
41	¿El sistema dispone de mecanismos de monitorización y alertas ante posibles problemas?			1	0
42	¿Se ofrece facilidades para realizar algún plan de contingencia para momentos en los que el sistema esté caído?			1	0
	Caracteristicas PC				
43	Para realizar su administración remota, se requiere la activación de escritorio remoto?			1	0
44	Se requiere la instalación de algún software específico para realizar su administración remota?			1	0

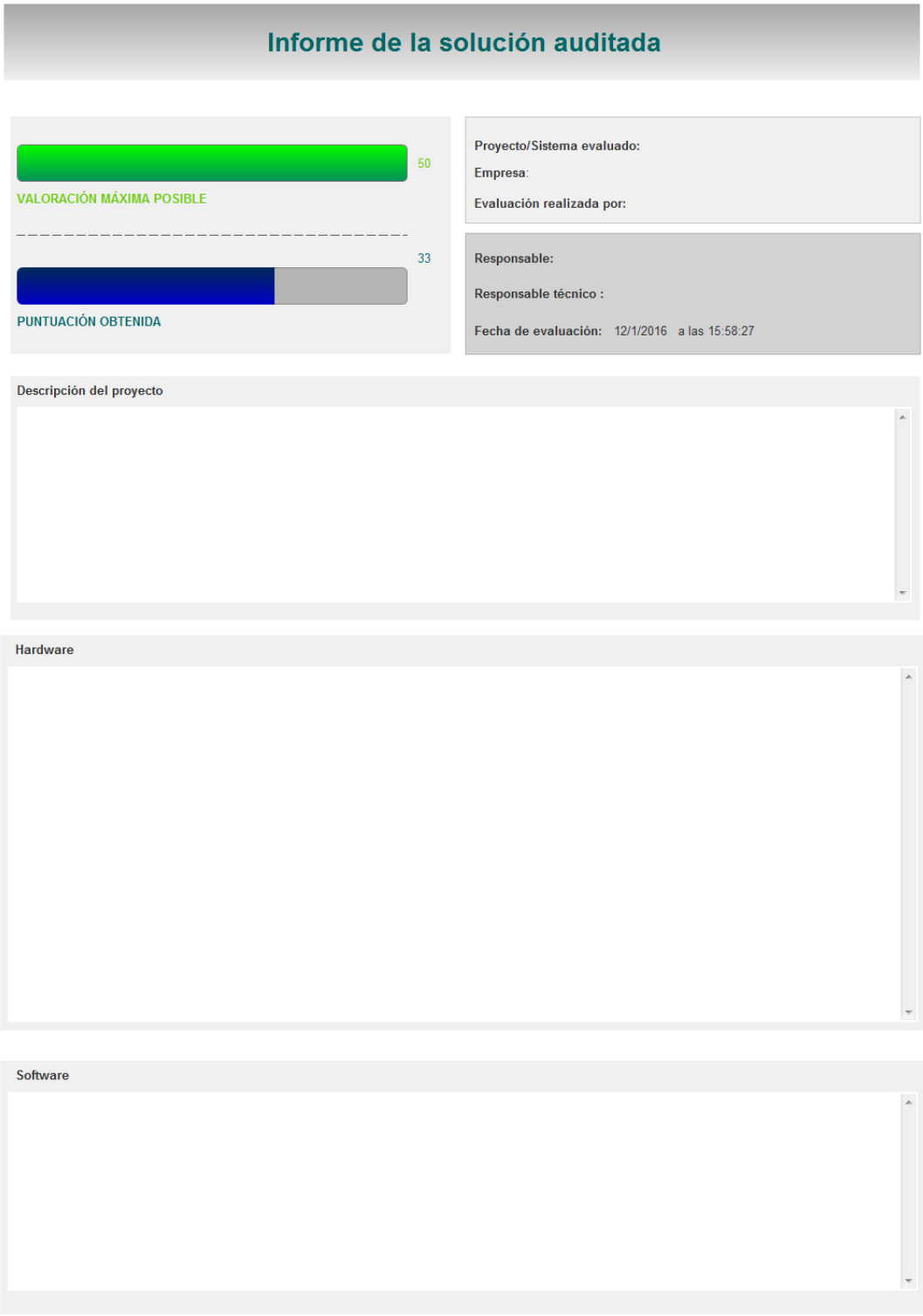
Dispositivos (Electromedicina, Ingenieria Electrónica, Analizadores, etc...)

	Caracteristicas Dispositivos	Si	No	Valor	Puntuación
45	¿Alguno de los dispositivos requiere de conversor serie/Ethernet para conectarse a la red?			1	0
46	El dispositivo se administra remotamente mediante un protocolo no seguro? (html, ftp, telnet)			1	0
47	Para administrar el dispositivo se requiere de usuario y contraseña robusta?			1	0
48	¿Los interfaces de los dispositivos conectados a la red soportan modos de 100 Mbps Full Duplex?			1	0
49	¿Los interfaces de los dispositivos conectados a la red soportan modos de 1 Gbps Full Duplex?			1	0
50	Si alguno de los dispositivos del sistema requiere conexión WIFI ¿soporta métodos de autenticación 802.1X mediante certificados?			1	0

Enviar

2.5.4 Informe estándar (informeEstandar.html)

Imagen 15: Informe Estándar del prototipo HITA



Requisitos adicionales

	Característica	
1	¿El servidor será compatible con entorno virtual?	✓
2	¿Se incluye una solución backup específica?	✓
3	Si se almacenan datos de paciente ¿se realizará backup de los datos un mínimo de una vez semanalmente?	✓
4	¿Dispone de redundancia de fuentes de alimentación? Si el sistema incluye servidores sin fuente de alimentación redundante, no se garantiza la alta disponibilidad.	✗
5	¿Existirá teaming de interfaces de red? Si el sistema incluye servidores sin interfaces de red redundante y trabajando en "teaming", no se garantiza la alta disponibilidad.	✗
6	¿Puede incorporarse al dominio corporativo? No se le pordrán aplicar las politicas de gestión, actualizaciones y seguridad corporativa.	✗
7	Alguno de los servicios requiere ser iniciado de forma interactiva, o se inician todos en el arranque del sistema?	✓
8	Si alguno de los servicios o procesos necesarios para ejecutar el sistema se cae ¿el servidor dispone de un control automatico para intentar volver a levantarlo?	✓
9	¿El software es compatible con el sistema operativo y customización corporativa de la organización?	✓
10	¿Puede este estar en el dominio corporativo?	✓

11	¿Existe limitación de clientes concurrentes por licencias?	✓
12	¿Existe algún servicio propio del sistema a implantar que se ejecute con el usuario administrador o root?	✓
13	Además del usuario administrador o root ¿requiere el sistema otros usuarios locales con privilegios de administrador?	✓
14	¿El servidor almacena datos de pacientes?	✓
15	En caso que el servidor almacene datos de paciente ¿están en un a base de datos o fichero encriptado? Incumplimiento del "Artículo 9 (Ley Orgánica 15/1999)": garantizar la seguridad de los datos de carácter personal y evitar su ALTERACIÓN, pérdida, tratamiento o acceso no autorizado.	✗
16	En caso que el servidor almacene datos de paciente ¿el acceso a la base de datos o fichero está restringido solo a usuarios autorizados? Artículo 9 (Ley Orgánica 15/1999)	✗
17	En caso que el servidor almacene datos de paciente ¿existe un log de accesos que registre las acciones que realizan los usuarios, así como la fecha e identidad del mismo? Artículo 9 (Ley Orgánica 15/1999)	✗
18	En caso que el servidor no almacene datos de paciente ¿existe un log de accesos al sistema que identifique la fecha y el usuario que ha accedido?	✓

19	¿Es el sistema compatible con soluciones antivirus?	✓
20	¿Permite el servidor ser monitorizado vía SNMP?	✓
21	¿El servidor requiere compartir alguna carpeta de su disco con permisos de lectura y escritura? Compartir carpetas en los servidores requiere un control periódico de las autorizaciones a las mismas, no recomendándose nunca los acceoss con permisos de escritura, salvo en servidores de ficheros.	✗
22	Si el servidor requiere compartir alguna carpeta compartida en de disco, con permisos de lectura y escritura ¿tiene activa la auditoria de accesos a los ficheros de dicho recurso?	✗
23	¿Se almacena algún tipo de dato de pacientes localmente en el PC? Nunca debería almacenarse información de pacientes en sistemas que físicamente no estén en un CPD o ubicación con las correspondientes medidas de seguridad físicas y lógicas.	✗
24	¿El acceso al software cliente requiere autenticación? Tanto si se almacenan datos de paciente como si no, será necesario un control de accesos a los mismos con el fin de evitar usos no autorizados.	✗
25	Si desde el software cliente se accede a datos de paciente, obliga esta a cambiar la contraseña como mínimo una vez al año? Incumplimiento "Real Decreto 1720/2007 - Artículo 93. IDENTIFICACIÓN Y AUTENTICACIÓN". La periodicidad de cambio de contraseña NO SERÁ SUPERIOR A UN AÑO, mientras estén vigentes, y se almacenarán de forma ininteligible.	✗
26	¿La contraseña se almacena localmente o en un servidor de forma ininteligible? Incumplimiento del "Real Decreto 1720/2007 - Artículo 93. IDENTIFICACIÓN Y AUTENTICACIÓN". La periodicidad de cambio de contraseña no será superior a un año, mientras estén vigentes, y SE ALMACENARÁN DE FORMA ININTELIGIBLE..	✗
27	Si el sistema almacena datos de pacientes ¿dispone el sistema protección ante continuos intentos fallidos para acceder al sistema? Incumplimiento del Real Decreto 1720/2007 - Artículo 98. IDENTIFICACIÓN Y AUTENTICACIÓN.Se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.	✗
28	¿El PC requiere compartir alguna carpeta de su disco con permisos de lectura y escritura?	✓
29	¿Es el software cliente compatible con soluciones antivirus?	✓

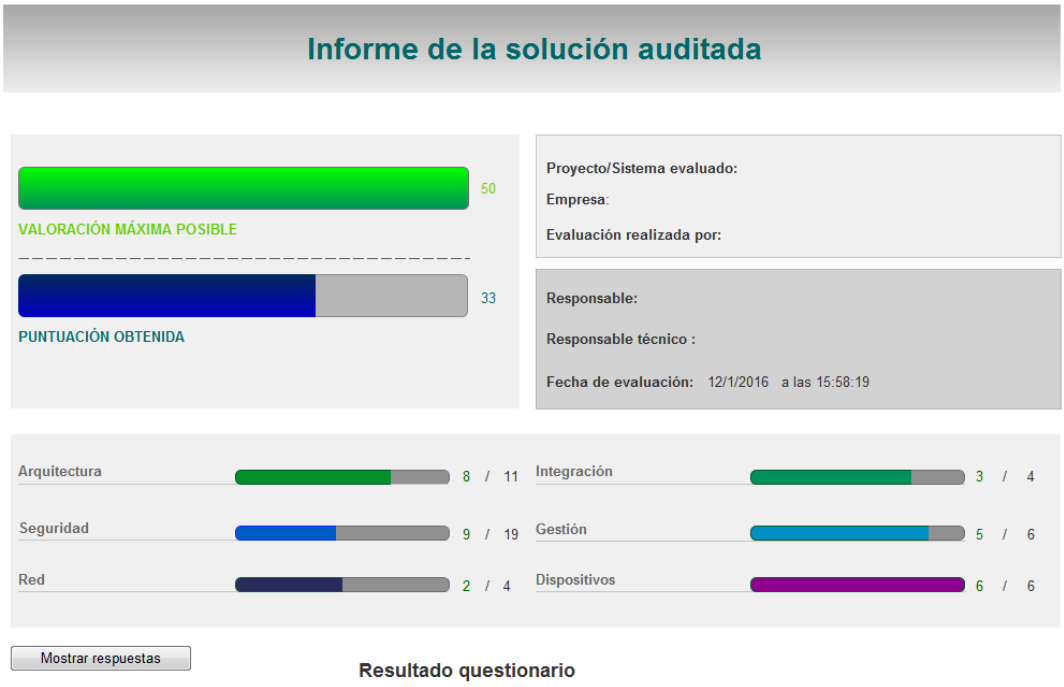
30	¿El acceso a la BIOS dispone de contraseña?	✓
31	¿El sistema requiere ser accesible desde fuera de la red corporativa para su normal funcionamiento?	✓
32	¿El sistema requiere acceder desde la LAN interna a algún servidor externo?	✓
33	¿Se requiere de algún tipo de tráfico Broadcast para el envío de información a los dispositivos que forman el sistema a implantar? El tráfico Broadcast está limitado a subredes y VLAN, por lo que si el sistema lo requiere, deberá documentarse al detalle su uso y caracateristicas.	✗
34	¿Existe una estimación aproximada de la cantidad de tráfico que generará el sistema? Siempre que sea posible, se requiere conocer la cantidad de tráfico aproximada que generará el sistema.	✗
35	¿El sistema requiere la integración con alguno de los sistemas asistenciales? Se deberá documentar en detalle el uso que se hará de los datos del HIS.	✗
36	En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante HL7?	✓
37	En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante DICOM?	✓
38	En caso de requerir la integración con uno de los sistemas asistenciales ¿se integra mediante Web Services?	✓
39	¿Se usará un interface ILO para la administración remota?	✓
40	¿Se dará soporte remoto mediante una conexión VPN o encriptada? (Obligatorio si se almacenan datos de pacientes). Real Decreto 1720/2007 - Artículo 104. TELECOMUNICACIONES.	✗

40	¿Se dará soporte remoto mediante una conexión VPN o encriptada? (Obligatorio si se almacenan datos de pacientes). Real Decreto 1720/2007 - Artículo 104. TELECOMUNICACIONES.	✗
41	¿El sistema dispone de mecanismos de monitorización y alertas ante posibles problemas?	✓
42	¿Se ofrece facilidades para realizar algún plan de contingencia para momentos en los que el sistema esté caído?	✓
43	Para realizar su administración remota, se requiere la activación de escrtorio remoto?	✓
44	Se requiere la instalación de algún software específico para realizar su administración remota?	✓
45	¿Alguno de los dispositivos requiere de conversor serie/Ethernet para conectarse a la red?	✓
46	El dispositivo se administra remotamente mediante un protocolo no seguro? (html, ftp, telnet)	✓
47	Para administrar el dispositivo se requiere de usuario y contraseña robusta?	✓
48	¿Los interfaces de los dispositivos conectados a la red soportan modos de 100 Mbps Full Duplex?	✓
49	¿Los interfaces de los dispositivos conectados a la red soportan modos de 1 Gbps Full Duplex?	✓
50	Si alguno de los dispositivos del sistema requiere conexión WIFI ¿soporta autenticación a la red mediante certificados?	✓

Imprimir

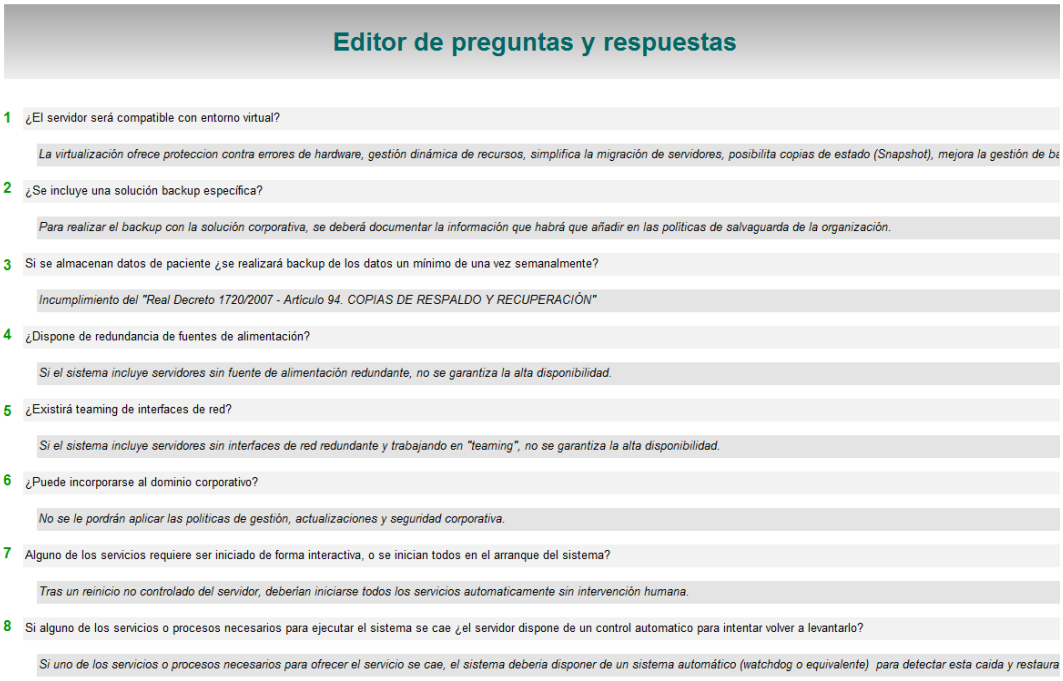
2.5.4 Informe sanidad (informeSanidad.html)

Imagen 16: Informe para ámbito sanitario del prototipo HITA



2.5.5 Edición de preguntas y respuestas (questions.html)

Imagen 17: Editor de preguntas y respuestas del prototipo HITA



3 Conclusiones

Durante el desarrollo del proyecto, se ha confirmado y contrastado el problema existente de forma generalizada, respecto al escaso control por parte de los hospitales, autoridades y de los proveedores en relación al cumplimiento de una medidas básicas de seguridad informática, así como del cumplimiento legislativo.

Se han revisar numerosas licitaciones públicas de sistemas de ingeniería médica para hospitales, y en prácticamente todas se detecta la ausencia de requisitos concretos referentes a seguridad informática. Esta situación se ha contrastado tanto con otros hospitales del Estado como con proveedores de ámbito internacional, y se concluye que no es solo un problema local, dado que, en mayor o menor medida, el problema existe de forma global.

El feedback recibido por parte de los hospitales y proveedores ha sido numeroso y con aportaciones realmente interesantes para la elaboración de este trabajo. Además, se considera este proyecto como algo realmente necesario y que presumiblemente sea de uso continuo en sus organizaciones.

En cuanto a la planificación del proyecto, no ha resultado sencilla. No se han cumplido todos los hitos tal y como estaban planificados. Esto ha sido así principalmente debido a la dificultad de compatibilizar la planificación de las entregas por partes y el trabajo a turnos.

Pero por otro lado, también se reconoce un leve fallo de planificación toda vez que la pretensión inicial era codificar la herramienta manualmente, sin usar herramientas de apoyo, lo que requiere la ayuda de algún desarrollador con más conocimiento en JavaScript.

Asimismo, en el curso del desarrollo del proyecto han surgido nuevas necesidades e ideas que han ido cambiando el enfoque del mismo. Por ejemplo, tras el feedback recibido se estima oportuno que la herramienta a desarrollar referencie al articulado de la legislación aplicable en cada elemento de la checklist. De forma que cuando un sistema no cumple con un requisito legal, la herramienta indique exactamente el artículo de la norma vigente que se está incumpliendo. Idea que inicialmente no estaba planteada.

En términos generales, se considera cumplidos los objetivos marcados en este trabajo, si bien es cierto que han sobrevenido nuevas ideas a medida que se ha ido desarrollando el mismo, aunque finalmente solo se ha decidido incorporar algunas.

4 Glosario

Accesos autorizados

Autorizaciones concedidas a un usuario para la utilización de los diversos recursos. En su caso, incluirán las autorizaciones o funciones que tenga atribuidas un usuario por delegación del responsable del fichero o tratamiento o del responsable de seguridad.

Autenticación

Procedimiento de comprobación de la identidad de un usuario.

Axure

Herramienta para diseño y maquetación de páginas web.

CIS

Sistema de información clínico. Programa de software que gestiona los servicios de información médicos, administrativos, financieros y jurídicos de un hospital o unidad clínica. Estos sistemas almacenan, organizan y transmiten información que sirven de apoyo para la toma de decisiones clínicas y de gestión.

Control de acceso

Mecanismo que en función de la identificación ya autenticada permite acceder a datos o recursos.

Copia de respaldo

Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.

DICOM

Siglas de Digital Imaging and Communication in Medicine. Estándar internacional diseñado inicialmente para la transferencia, manipulación y almacenamiento de imágenes médicas, que con el tiempo ha ido incorporando otros formatos como audio, vídeo, imágenes 3D o gráficas de señales biomédicas (ECG, EEG, EMG, etc.). Los archivos DICOM incluyen junto con los archivos de datos, información referente a las condiciones de estudio.

Fichero automatizado

La LOPD referencia de esta forma a todo fichero con datos de carácter personal, que esté informatizado. Es decir, un fichero informático con datos de ciudadanos.

Fichero no automatizado

La LOPD referencia de esta forma a todo fichero con datos de carácter personal, que no esté informatizado. Es decir, una hoja o cualquier otro soporte físico con datos de ciudadanos.

HCE

Historia Clínica Electrónica. Registro mecanizado de los datos sociales, preventivos y médicos de un paciente, obtenidos de forma directa o indirecta y constantemente puestos al día.

Un repositorio digital de información estructurada de salud que puede ser compartida a través de sistemas conectados en red. La HCE generalmente incluye datos demográficos, de afiliación y personales del paciente, antecedentes personales y familiares, el historial médico, de medicación y de vacunas, las alergias conocidas, los resultados de pruebas de laboratorio, y los estudios de imagen médica u otro tipo de pruebas.

HIPAA

La HIPAA es la Ley de Responsabilidad y Transferibilidad de Seguros Médicos (Health Insurance Portability and Accountability Act)

HIPAA Security Rule Toolkit

Herramienta de auto-auditoria referente al cumplimiento con los establecido en la HIPAA.

HIS

Sistemas de información hospitalarios (siglas: SIH, o HIS en inglés), denominado también expediente electrónico. Consiste en un programa o programas de cómputo instalados en un hospital que permite llevar un control de todos los servicios prestados a los pacientes, detallar el coste de la atención prestada a cada paciente, llevar un expediente clínico en forma electrónica, facilita el acceso y obtiene los datos sobre el tratamiento del paciente de forma más segura, con prontitud y eficiente.

HL7

Conjunto de estándares orientados a facilitar el intercambio electrónico de información clínica.

Identificación

Procedimiento de reconocimiento de la identidad de un usuario.

JavaScript

JavaScript (abreviado comúnmente "JS") es un lenguaje de programación interpretado, dialecto del estándar ECMAScript. Se define como orientado a objetos 3 basado en prototipos, imperativo, débilmente tipado y dinámico.

LOPD

Ley Órgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas. (Wikipedia)*

Sistemas empleados para digitalizar el almacenamiento de información y los flujos de trabajo en organizaciones sanitarias

Responsable del fichero

Según se define en la propia LOPD: *Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente*

Responsable de seguridad

Persona o personas a las que el responsable del fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.

ROOT

En sistemas operativos del tipo Unix, root es el nombre convencional de la cuenta de usuario que posee todos los derechos en todos los modos (mono o multi usuario). Normalmente esta es la cuenta de administrador

SNMP

El Protocolo Simple de Administración de Red o SNMP (del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red.

Sistema de información

Conjunto de ficheros, tratamientos, programas, soportes y en su caso, equipos empleados para el tratamiento de datos de carácter personal.

Usuario

Sujeto o proceso autorizado para acceder a datos o recursos. Tendrán la consideración de usuarios los procesos que permitan acceder a datos o recursos sin identificación de un usuario físico.

5 Bibliografía

Javier Yetano Lagunaa, E. L. (07 de Junio de 2007). *Revista Española Española de Cardiología*. Recuperado el 15 de Noviembre de 2015, de http://www.revespcardiol.org/es/documentacion-clinica-aspectos-legales-fuente/articulo/13108422/

- **BOE.** (2002) Ley 41/2002, d. 1. (s.f.). Obtenido de https://www.boe.es/buscar/act.php?id=BOE-A-2002-22188

- **BOE.** (2007) Real Decreto 1720/2007, d. 2. (2007). por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En BOE.

- **Red.** (2012). *Las TIC en el Sistema Nacional de Salud*. Recuperado el 15 de 11 de 2015, de Las TIC en el Sistema Nacional de Salud: www.red.es/redes/sala-de-prensa/centro-de-documentacion

- **BOE**.(1986) Ley 14/1986, de 25 de abril, General de Sanidad. BOE de 29 de abril de1986.

- **AGPD.**(2014) Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD). BOE núm. 298, de 14 de diciembre de 1999. (TEXTO CONSOLIDADO Última modificación: 5 de marzo de 2011) https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

- **BOE.** (2002) Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica. BOE de 15 de noviembre de 2002

- **Wikipedia**. (2015) https://es.wikipedia.org/wiki/ISO/IEC_27002

- **Aenor**.(2009).http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0028064#.Vm1Rq79In9o

- **U.S. Department of Health & Human Services**.(2015) http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html

6 Anexos

Anexo I: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal,

Título II. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Art. 8 LOPD

DATOS RELATIVOS A LA SALUD.

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9 LOPD

SEGURIDAD DE LOS DATOS.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 44 LOPD

TIPOS DE INFRACCIONES.
1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:
a) No atender, por motivos formales, la solicitud del interesado de

rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos
.
j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso legítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no

proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

(Cidesl)

ANEXO II: La Ley básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica

Esta ley, a diferencia de la LOPD, es específicamente sanitaria. Entre otros, establece los siguientes principios referentes a la información generada de cada paciente.

El paciente tiene derecho a la información sobre su salud en todo lo relativo al diagnóstico, pronóstico, pruebas y alternativas de tratamiento con sus riesgos y consecuencias. También serán informadas las personas vinculadas al enfermo, por razones familiares o de hecho, en la medida en que el paciente lo permita de manera expresa o tácita. Como norma general, la información se proporcionará verbalmente y se dejará constancia en la HC. El médico responsable del paciente es el que garantiza este derecho a la información.

El paciente tiene derecho al consentimiento informado. Toda actuación en el ámbito de la salud de un paciente necesita el consentimiento libre y voluntario del afectado, una vez recibida la información adecuada y las alternativas propias del caso. El consentimiento informado será verbal por regla general, pero será por escrito en caso de intervención quirúrgica o de procedimientos diagnósticos o terapéuticos invasivos.

Los datos existentes en la HC son confidenciales, por lo que ninguna persona no autorizada accederá a ellos. Toda persona que, por razón de su oficio, elabore o tenga acceso a la información y a la documentación contenida en la HC (es decir, el personal sanitario relacionado con la asistencia al paciente) está obligada a guardar la reserva debida.
El paciente (o la persona autorizada por él) tiene derecho al acceso a la documentación de la HC. Salvo excepciones que se especifiquen, no tienen derecho al acceso a la documentación de la HC las personas vinculadas al enfermo, por razones familiares o de hecho, si no están autorizadas por escrito por éste.

La ley establece ciertas limitaciones al derecho de acceso de un ciudadano a su HC, pues establece que «el derecho al acceso del paciente a la documentación de la HC no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en la elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus observaciones, apreciaciones o anotaciones subjetivas».

Esta limitación permitiría que un médico pudiese impedir a un paciente el acceso a la parte de su HC donde consten sus anotaciones subjetivas.
Las HC deben conservarse un mínimo de 5 años desde la fecha de alta del último episodio. Esta ley, en el punto 1 del artículo 17, fija que «los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en su soporte original, para la debida asistencia al paciente

durante el tiempo adecuado a cada caso y, como mínimo, 5 años contados desde la fecha del alta de cada proceso asistencial».

Por tanto, por un lado, es legal conservar los documentos de una HC en soporte electrónico y destruir el papel o la placa radiográfica. Por otro lado, un centro sanitario podría destruir las historias clínicas si llevan más de 5 años desde el alta del último episodio (excepto los casos en que la correcta asistencia futura del paciente así lo aconseje). Este punto del artículo 17 también limita el derecho a la rectificación o cancelación de los datos de una HC por parte del paciente porque el centro sanitario tiene la obligación de conservarla.
(Javier Yetano Lagunaa, 2007) (Ley 41/2002)