Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Esquema Nacional de Seguridad: Protección de una infraestructura crítica hospitalaria

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Pedro José Arnedo Montó

Tutor: Juan Vicente Oltra Gutiérrez

2016-2017

"Cuando se está en medio de las adversidades, ya es tarde para ser cauto."

Lucio Anneo Séneca.

Resumen

En este proyecto se lleva a cabo un estudio de la normativa que envuelve al Esquema Nacional de Seguridad y su aplicación en una infraestructura crítica hospitalaria. Después del análisis, se plantea la implementación de una aplicación en lenguaje Java que ayude a los auditores a controlar que dicha normativa se cumple de una forma adecuada.

Palabras clave: Esquema, Nacional, Seguridad, Hospital, Java, Auditor.

Abstract

This project carries out a study of the regulations that involve the National Security Scheme and its application in a critical hospital infrastructure. After the analysis, the implementation of an application in Java language is proposed to assist auditors to control that the regulation is fulfilled in a suitable form.

Keywords: Scheme, National, Security, Hospital, Java, Auditor.

Tabla de contenidos

Índice de tablas

Tabla de ilustraciones

1. Introducción

En la actualidad garantizar la seguridad de las personas se ha convertido en un reto cada vez más difícil. Con la aparición de las nuevas tecnologías encontramos nuevas formas de prevención y protección, pero también nuevos riesgos para los derechos de las personas que es necesario tener en cuenta. En un mundo cada vez más informatizado un ataque a un sistema informático de cualquier tipo podría suponer grandes pérdidas, no solo económicas o materiales sino también humanas. Aunque parezca ciencia ficción, cada vez más, la protección de la vida de las personas pasa primero por la protección de los sistemas de la información.

1.1 Motivación

Los hospitales son considerados infraestructuras criticas ya que la destrucción o inhabilitación de los mismos supondría un gran impacto en la salud de las personas. En la sociedad actual, y particularmente en España que posee un sistema de sanidad publica muy competente a la vez que saturado, la perdida de alguno de estos centros por causas diversas supondría una disminución de la calidad de vida de los ciudadanos e incluso podría suponer problemas irreparables para muchos de ellos.

La finalidad de este proyecto es aplicar los conocimientos adquiridos en el grado, junto con los adquiridos durante la investigación en materia legal llevada a cabo durante la realización del proyecto, para aportar una pequeña ayuda a la protección de dicho sistema sanitario intentando facilitar el trabajo a aquellos que se encargan de que todo cumpla con las normas establecidas.

1.1.1 Motivación personal

La elección de dicho proyecto no ha sido fortuita ni por descarte, siempre he estado interesado en llevar al máximo la finalidad de la tecnología, que no es otra que facilitarnos la vida al ser humano. Durante los años que he estado estudiando este grado siempre me ha causado curiosidad las diferentes formas en las que la tecnología puede ayudarnos en nuestro día a día. Además, en estos años he estado preparándome para afrontar la oposición a Policía Nacional, lo que me proporciona una base en aspectos y temas legales.

Este proyecto me proporciona forma de juntar mis estudios académicos con mi vocación profesional y posiblemente sirva de ayuda a otras personas cuyo objetivo sea garantizar la seguridad de la población.

1.2 Estructura

El proyecto está estructurado en dos partes principales claramente diferenciadas pero complementarias entre si. La primera parte podemos llamarla la parte teórica del proyecto en la cual se ha analizado el contexto normativo pasado, actual y futuro para poder comprender los aspectos legales que envuelven el trabajo. En esta parte se desarrollan muchos de los conceptos necesarios para entender los requisitos de la parte práctica del proyecto. Se han resumido varias leyes de forma clara y concisa sobre lo que afecta al trabajo y se han obviado los conceptos de poca relevancia con el fin de entender mejor las normas.

La segunda parte o parte práctica del proyecto es en la cual se aplica lo estudiado en la parte anterior para diseñar una aplicación. En esta parte se muestran los conocimientos aprendidos durante el grado en materia de diseño e implementación de aplicaciones, junto con una pequeña parte de diseño y gestión de bases de datos. Después se muestra el resultado de la aplicación implementada explicando su funcionamiento.

Al final se muestran las conclusiones del proyecto junto con la bibliografía utilizada en la realización del mismo.

2. Contexto jurídico

Para realizar el presente trabajo se ha tenido que tener en cuenta una serie de normas legislativas para establecer un marco legal en torno al tema del trabajo. Las normas que se detallan a continuación son a la vez importantes para el desarrollo de la aplicación práctica pues nos van a dar los elementos necesarios para resolver las cuestiones sobre legalidad y seguridad.

2.1 Ámbito europeo

El ámbito europeo proporciona una serie de directivas o recomendaciones sobre el tema a tratar, todas ellas van orientadas a la protección de las libertades de las personas, así como sus derechos.

2.1.1 Directiva 95/46/CE

El objetivo de esta directiva como se indica en el apartado 1 del artículo 1 es el siguiente:

> Los Estados miembros garantizarán, con arreglo a las disposiciones de la presente Directiva, la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales

En lo que respecta a nuestro tema podemos marcar como artículo importante a tener en cuenta el apartado 1 del artículo 8 en el cual se menciona lo siguiente:

> Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

Dicho apartado tiene ciertas excepciones en las cuales no se aplicaría lo mencionado, dichos casos son situaciones muy particulares en las cuales la aplicación de la norma provoque la supresión de otros derechos más importantes a sí mismo o a otras personas, o casos en los cuales se causen más problemas que beneficios. Podemos citar algunas de ellas en el apartado 2 del mismo artículo:

> c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento
>
> e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesarios para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

Y también encontramos otra excepción en el apartado 3 del mismo artículo:

> El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.

A partir del 25 de mayo de 2018, Con motivo de la entrada en vigor del Reglamento 2016/679 de la UE, quedará derogada esta ley como se indica en el artículo 94 de dicho reglamento.

2.1.2 Reglamento (UE) 2016/679

En el reglamento 679/2016 del 27 de abril se establecen una serie de normas con respecto al tratamiento de datos de personas físicas dando más control a los interesados sobre su información privada. Esta norma debe de ser interpretada por cada país miembro con respecto a su norma propia, es decir, la AEPD deberá legislar a partir de las directrices que establece este reglamento.

El reglamento se aplica al tratamiento de datos personales total o parcialmente automatizado y también al tratamiento no automatizado de datos destinados a estar contenidos en un fichero. El ámbito de aplicación contiene algunas excepciones para casos en los que se comprometa la seguridad de la unión o seguridad nacional, con fines de prevención, investigación o enjuiciamiento, así como, la protección de la seguridad pública. Tampoco será de aplicación en los ámbitos domésticos o personales ni en el ejercicio de una actividad que no le sea de aplicación el derecho de la unión europea.

En España aún no se ha aplicado el reglamento con motivo de la falta de gobierno en el año 2016, pero la agencia española de protección de datos ha adelantado que se va a llevar a cabo un cambio de paradigma en este ámbito. Los cambios deberán de ser realizados tanto por la AEPD en cuanto a normativa, como por las empresas e instituciones en cuanto a aplicación de la norma.

La norma es extensa contiene 173 consideraciones previas y 99 artículos organizados en 11 capítulos. Las principales novedades que incorpora esta norma son las siguientes:

- Aparecen nuevos derechos de los interesados: Transparencia, Información, Acceso, Rectificación, Supresión, Limitación, Portabilidad y Oposición.
- Se incluyen como datos de carácter sensible, los datos biométricos o genéticos, y se consideran nuevos tipos de datos que se deben proteger como la dirección de protocolo de internet (IP) o los identificadores de sesión, los seudónimos y los datos que se recojan para la elaboración de un perfil de una persona física.
- Existirá un responsable de tratamiento que será una persona física o jurídica cuya función será determinar los fines y medios del tratamiento. A su vez existirá un encargado del tratamiento que será la persona física o jurídica que tratará los datos personales.
- Los datos personales serán tratados de manera licita y real de acuerdo con el interesado, recogidos con fines determinados y adecuados y pertinentes con dichos fines. Los datos recogidos serán exactos y deberán estar actualizados. Los datos no podrán mantenerse más tiempo del necesario para el fin para el cual fueron recogidos y serán tratados garantizado una seguridad adecuada.
- El responsable deberá demostrar el consentimiento del interesado, el interesado deberá prestar su consentimiento libremente, de forma inteligible y en lenguaje claro y sencillo. El interesado tendrá derecho a retirar su consentimiento cuando lo desee.

- El interesado tendrá el derecho de portabilidad de los datos, es decir tiene derecho a recibir los datos del responsable al que se los facilitó y transmitirlos a otro responsable.
- El responsable deberá aplicar las medidas necesarias para garantizar el tratamiento adecuado de los datos y tendrá que poder demostrarlo. Tendrá que llevar un registro de las actividades llevadas a cabo bajo su responsabilidad poniéndola a disposición de la autoridad que controle que se cumple el reglamento.
- El responsable de tratamiento deberá notificar a la autoridad de control toda violación de la seguridad de los datos a menos de que esta no constituya una violación de los derechos de las personas.
- Se evaluará el impacto de las operaciones en materia de protección de datos antes del tratamiento de los mismos.
- Cuando la evaluación mencionada anteriormente revele que el tratamiento de los datos entraña algún riesgo para la seguridad de los mismos el responsable deberá consultar previamente a la autoridad de control. Si la autoridad de control considera que el tratamiento de los datos infringe el reglamento deberá asesorar al responsable.
- Existirá un delegado de protección nombrado por el responsable y el encargado de protección en los casos que establece el reglamento. Sus funciones serán las de asesoramiento al responsable o encargado del tratamiento, la supervisión del cumplimiento de este reglamento, cooperar y actuar de contacto con la autoridad de control.
- Se podrán realizar transferencias de datos siempre que se garantice que el receptor de dichos datos garantice la seguridad y protección de los mismos.
- Existirá una cooperación entre la unidad de control principal y las autoridades de control interesadas prestándose asistencia mutua y realizando operaciones conjuntas.
- Se crea el Comité Europeo de Protección de Datos que garantizará la aplicación de este reglamento y actuará con total independencia en el desempeño de sus funciones.

2.1.3 Recomendación 2008/594/CE

La siguiente recomendación propone una serie de orientaciones para implantar un sistema de informes médicos transfronterizos de forma que se pueda atender a los pacientes dentro de la Comunidad Europea de la forma más correcta y eficaz.

Hace especial énfasis en la protección de datos en los apartados del 10 al 15 en los cuales, de acuerdo con las normativas comunitarias, alerta a los estados miembros que al tratarse de informes médicos transfronterizos es más fácil que la información sensible sea revelada accidentalmente a terceros y propone la creación de un marco jurídico en el cual se establezcan las bases de unos historiales médicos seguros que protejan la intimidad de los pacientes así como permitiéndole a estos determinar qué información y como quieren que se muestre.

Por último, indica que, ante la implementación de todo sistema de protección de datos de carácter sensible, es necesario realizar una evaluación previa de los riesgos y posteriormente realizar auditorías con el fin de supervisar una aplicación satisfactoria; creando, si fuera necesario, un observatorio de supervisión de la interoperabilidad de los sistemas de protección.

2.1.4 Reglamento (UE) 910/2014

El reglamento 910/2014 establece las condiciones en las que se deberán de encontrar los medios de identificación electrónica de personas físicas y jurídicas que pertenezcan a un sistema de identificación electrónica de otro Estado miembro estableciendo normas sobre los servicios de confianza como lo son las transacciones electrónicas. El reglamento se aplica a los sistemas de identificación electrónica notificados por los Estados miembros y a los que presten servicio de certificación dentro de la Unión.

Para notificar un sistema de identificación electrónico un Estado miembro deberá presentar ante la Comisión una documentación que incluye:

- Una descripción del sistema, incluyendo los niveles de seguridad del mismo, que según se expone en el artículo 8 del mismo reglamento, se establecen tres niveles de seguridad para el sistema: Bajo, sustancial y alto. En el nivel bajo se pretende reducir el riesgo de uso indebido o la alteración de la identidad. En el nivel sustancial se pretende reducir sustancialmente el riesgo de uso indebido o de alteración de identidad y en el nivel alto se pretende evitar el riesgo de uso indebido o de alteración de la identidad. Además de los niveles de seguridad la descripción deberá incluir el emisor o emisores de los medios de identificación.
- El régimen de supervisión y el régimen de responsabilidades tanto de la parte que expide los medios de identificación como de la parte que utilice el procedimiento de autenticación.
- Las autoridades responsables del sistema
- La información sobre la o las identidades que gestionan el registro de los datos de identificación

- Una descripción sobre cómo se cumplen los requisitos expuestos en el artículo 12 del mismo reglamento.
- Una descripción de la autenticación en la que se describan las garantías de disponibilidad y se definan las condiciones de acceso a ella.
- Las disposiciones relativas a la suspensión del sistema.

Otro de los objetivos del reglamento es establecer un marco jurídico para las firmas electrónicas, los sellos electrónicos, los sellos de tiempo electrónicos, los documentos electrónicos, los servicios de entrega electrónica certificada y los servicios de certificados para la autenticación de sitios web.

2.1.5 Directiva 2011/24/UE

Esta directiva tiene como objeto la aplicación de los derechos de los pacientes en lo que respecta a la asistencia médica transfronteriza, así como facilitarles una asistencia médica segura y de calidad.

La norma garantiza el derecho de los pacientes a acceder a su información médica entre otros, y proporciona al personal médico una serie de garantías sobre la autenticidad de dicho historial, preocupándose incluso de que haya un entendimiento entre el personal que prescribe el tratamiento al paciente y el personal que le proporciona dicho tratamiento de forma que no haya ningún tipo de negligencia.

2.2 Ámbito nacional

En el ámbito nacional encontramos una serie de normas que amplían o especifican las anteriores normas europeas mencionadas con objeto de crear un marco jurídico más concreto en nuestro país y ajustándolas a nuestro marco legal ya existente.

2.2.1 Ley Orgánica 15/1999

La Ley Orgánica de Protección de Datos de 1999 fue creada con el fin de regular los datos de carácter personal protegiendo el honor, la intimidad y las libertades públicas de las personas físicas, así como sus derechos fundamentales.

Esta ley se aplica a todos los datos que hacen referencia a personas físicas ya sea en formato físico o electrónico, quedando excluidos algunos casos como datos de uso doméstico o casos más específicos como son el terrorismo o el crimen organizado.

Esta ley fue desarrollada posteriormente por el Real Decreto 1720/2007 que establece las medidas de seguridad que se deben de aplicar a los documentos automatizados para garantizar una correcta protección de datos. Estas medidas están clasificadas en tres

niveles: Básico, medio y alto, dependiendo del tipo de datos y de su sensibilidad o importancia. En el caso de una infraestructura critica hospitalaria como es el caso concreto de este trabajo, aplicara el nivel alto de protección de datos.

La Agencia Española de protección de Datos creada en 1994 es el organismo encargado de supervisar que se cumple la ley en todos sus casos, estableciendo sanciones para aquellos organismos o personas que no la cumplen. Las sanciones también se dividen en tres niveles dependiendo de la gravedad del hecho cometido.

Todas las personas, ya sean jurídicas, autónomos o colectivos que recopilen datos de terceros tienen la obligación de informar a dichas personas de que sus datos van a ser recopilados, y necesitan su consentimiento. En algunos casos relativos a la ideología, salud, creencias y/o afiliación sindical, necesitan un consentimiento expreso y/o por escrito dependiendo del caso. Además, se comprometen a la protección de dichos datos y a utilizarlos y/o comunicarlos a terceros solo para el fin para el que fueron recopilados.

2.2.2 Ley 41/2002

La ley 41/2002 tiene por objeto la regulación de los derechos y obligaciones de los pacientes, usuarios y profesionales, así como de los centros ya sean públicos o privados en materia de información y documentación clínica. Tiene como principios la dignidad de las personas, el respeto a la autonomía, voluntad e intimidad que imperaran en la obtención, utilización, archivo, custodia y transmisión de la información clínica.

Su artículo 14 es en el cual define y establece las directivas para el archivo del historial clínico:

> Artículo 14. Definición y archivo de la historia clínica.
>
> 1. La historia clínica comprende el conjunto de los documentos relativos a los procesos asistenciales de cada paciente, con la identificación de los médicos y de los demás profesionales que han intervenido en ellos, con objeto de obtener la máxima integración posible de la documentación clínica de cada paciente, al menos, en el ámbito de cada centro.
>
> 2. Cada centro archivará las historias clínicas de sus pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que consten, de manera que queden garantizadas su seguridad, su correcta conservación y la recuperación de la información.
>
> 3. Las Administraciones sanitarias establecerán los mecanismos que garanticen la autenticidad del contenido de la historia clínica y de los cambios operados en ella, así como la posibilidad de su reproducción futura.
>
> 4. Las Comunidades Autónomas aprobarán las disposiciones necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar su destrucción o su pérdida accidental."

En su artículo 15 apartado 1 menciona de forma genérica cual deber ser el contenido de dicho historial clínico:

> La historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Todo paciente o usuario tiene derecho a que quede constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud tanto en el ámbito de atención primaria como de atención especializada.

En su artículo 16 defiende la importancia del acceso a la historia clínica por los profesionales con el fin de prestar al paciente la mejor atención posible. Esto queda reflejado especialmente en los apartados 1 y 2:

> 1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.
>
> 2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

En su artículo 17 sigue hablando de la importancia de la conservación de los historiales clínicos ya se encuentren en el formato que sea como expresa en el apartado 1:

> Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.

Por eso es de vital importancia establecer métodos competentes de acceso, gestión y recuperación de la información en casos de perdida, esto va a ser uno de los objetivos del trabajo, el control de que se cumple todo lo necesario para que los profesionales puedan acceder a los historiales de los pacientes para brindarles la mejor atención, así como una tolerancia a fallos y una persistencia de datos lo suficientemente buena para que no se pierdan este tipo de datos.

Por último, en su artículo 18 matiza el derecho de los pacientes a acceder a su historial clínico ya sea por ellos mismos o por otra persona con autorización para ello, como se menciona a continuación:

> Artículo 18. Derechos de acceso a la historia clínica.
>
> 1. El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que

figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos.

2. El derecho de acceso del paciente a la historia clínica puede ejercerse también por representación debidamente acreditada.

3. El derecho al acceso del paciente a la documentación de la historia clínica 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 su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.

4. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o, de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso, el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.

2.2.3 Real Decreto 3/2010

El Real Decreto 3/2010 regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica con respecto a lo que expresa el artículo 42 de la Ley 11/2007 (derogada a fecha del 2 de octubre de 2016 por la disposición derogatoria 2.b de la ley 39/2015). El artículo 42 de la ley 11/2007 menciona lo siguiente:

Artículo 42. Esquema Nacional de Interoperabilidad y Esquema Nacional de Seguridad.

1. El Esquema Nacional de Interoperabilidad comprenderá el conjunto de criterios y recomendaciones en materia de seguridad, conservación y normalización de la información, de los formatos y de las aplicaciones que deberán ser tenidos en cuenta por las Administraciones Públicas para la toma de decisiones tecnológicas que garanticen la interoperabilidad.

2. El Esquema Nacional de Seguridad tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la presente Ley, y está constituido por los principios básicos y requisitos mínimos que permitan una protección adecuada de la información.

3. Ambos Esquemas se elaborarán con la participación de todas las Administraciones y se aprobarán por Real Decreto del Gobierno, a propuesta de la Conferencia Sectorial de Administración Pública y previo informe de la Comisión Nacional de Administración Local, debiendo mantenerse actualizados de manera permanente.

4. En la elaboración de ambos Esquemas se tendrán en cuenta las recomendaciones de la Unión Europea, la situación tecnológica de las diferentes Administraciones Públicas, así como los servicios electrónicos ya existentes. A estos efectos considerarán la utilización de estándares abiertos, así como, en su caso y de forma complementaria, estándares que sean de uso generalizado por los ciudadanos.

El esquema nacional de seguridad se aplicará como regla general a sedes electrónicas, registros electrónicos, sistemas de información electrónica accesibles por los

ciudadanos, sistemas electrónicos a través de los cuales los ciudadanos ejercen sus derechos y cumplen sus deberes, y por último a sistemas de información encargados de recabar información y estado del procedimiento administrativo. En el caso de una infraestructura crítica hospitalaria será de aplicación plena en el caso de que esta posea la consideración de identidad de derecho público, es decir, este vinculada a la Administración General del estado.

El propósito principal del ENS es la protección la información de los servicios que componen la Administración Pública proporcionando un sistema de confianza, para ello se marcan los siguientes objetivos:

- Crear las condiciones necesarias de confianza en el uso de medios electrónicos a través de medidas que garanticen la seguridad de la información.

- Establecer una política de seguridad en la utilización de medios electrónicos constituyendo una serie de principios básicos y requisitos mínimos que mencionaremos más adelante.

- Introducir los elementos comunes que servirán de guía de actuación en las Administraciones Públicas en materia de seguridad de la información.

- Aportar un lenguaje común para facilitar la comunicación de las Administraciones Públicas.

- Aportar un tratamiento homogéneo de la seguridad par a facilitar la cooperación de diversas entidades en la prestación de servicios.

- Facilitar un tratamiento continuado de la seguridad.

El Esquema Nacional de Seguridad establece unos principios básicos relativos a la seguridad a la hora de usar medios electrónicos en las administraciones públicas y trata de dar confianza a los ciudadanos en el ejercicio de sus derechos y deberes. Dichos principios están expuestos en el artículo 4 del Real Decreto y son los siguientes:

a) Seguridad integral: La seguridad será constituida por todos los elementos técnicos, humanos, materiales y organizativos que compongan el sistema y se pondrá la máxima atención en la concienciación de las personas que intervienen en el proceso. (art. 5)

b) Gestión de riesgos: La gestión de riesgos será parte esencial del proceso y permitirá mantener el entorno lo más controlado posible minimizando los riesgos hasta niveles aceptables. (art. 6).

c) Prevención, reacción y recuperación: Las medias de prevención deberán eliminar o minimizar los riesgos para evitar que afecten gravemente al sistema. Las medidas de reacción junto con las de detección se encargarán de encontrar el problema a tiempo y solucionarlo minimizando los daños. Por último, las medidas de recuperación trataran de restaurar la información que haya n sido perdidos o estén corruptos. (art.7)
d) Líneas de defensa: deben de estar orientadas a ganar tiempo de reacción ante los incidentes inevitables, reduciendo al máximo la probabilidad de perder todo el sistema y minimizando el impacto final en el mismo. (art. 9)

e) Reevaluación periódica: las medidas se evaluarán y se actualizarán debido a la constante evolución de los riegos incluso haciendo un replanteamiento de la seguridad si fuera necesario. (art. 8)

f) Función diferenciada: se dividen los responsables de información, servicio y seguridad para una mayor eficiencia. El responsable de la información se encargará de determinar los requisitos de la misma, el responsable de servicios determinara los requisitos de estos y, por último, el de seguridad se encargará de tomar las decisiones para que dichos requisitos se cumplan. (art. 10)

Además de unos principios básicos, el ENS establece unos requisitos mínimos que han de cumplirse siempre en proporción a los riesgos identificados en cada sistema, pudiendo omitirse algunos en sistemas sin riesgo significativo. Estos requisitos mínimos se encuentran en el apartado 1 del artículo 11:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.

c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

Estos requisitos mínimos serán aplicados conforme a lo dispuesto en el artículo 27, que menciona que al aplicarse estos requisitos sobre datos de carácter personal se aplicara lo dispuesto en la Ley 15/1999 LOPD y establece que dichos requisitos podrán ser ampliados si fuera necesario teniendo en cuenta la tecnología y la información manejada.

En el artículo 43 expone la clasificación de los sistemas en categorías conforme a lo dispuesto en el Anexo I, la clasificación está establecida en tres categorías según la valoración del impacto que tendría un incidente en los sistemas de información y servicios. El trabajo gira en torno a este artículo y a los Anexos I, II y III, por tanto, serán desarrollados posteriormente más exhaustivamente.

2.3 Ámbito autonómico

En el ámbito autonómico de la comunidad valenciana tenemos una norma que regula la sanidad dentro de la comunidad valenciana.

2.3.1 DOGV Ley 10/2014

La presente ley nace con la idea de garantizar un sistema de salud basado en la igualdad, prevención y protección de la salud tanto individual como colectiva.

En el capítulo V encontramos los sistemas de información que la ley propone para llevar a cabo una correcta identificación de los pacientes entre los cuales se encuentra la tarjeta SIP que tiene por objeto la correcta identificación de las personas, con todos sus datos importantes para este fin, así como su número del Sistema de Información

Poblacional. Del SIP deriva la Tarjeta Sanitaria Individual que acredita a su titular al uso de las prestaciones en sanidad a las que tenga derecho de acuerdo con la norma estatal.

En el artículo 46 se garantiza el derecho a la historia clínica y a su acceso, ya sea en formato físico o electrónico, siendo, esta última, mencionada en el apartado 6:

> La historia clínica electrónica se gestionará a través de un sistema de información corporativo, que garantizará la calidad, la accesibilidad y la seguridad, así como la coordinación y la continuidad asistencial.

En cuanto a la custodia de las historias clínicas, se encargará la dirección del centro sanitario en el que se encuentran, así como, el personal sanitario que actué de forma individual será el responsable de las historias médicas de sus pacientes. (Apartado 8)

El acceso a las historias clínicas deberá estar siempre disponible y contar con la confidencialidad y la protección necesaria para evitar la filtración o destrucción de datos como esta expresado en los apartados del 9 al 12:

> 9. Se deberán adoptar todas las medidas técnicas y organizativas necesarias para garantizar el derecho de acceso a la historia clínica, proteger los datos personales recogidos y evitar su destrucción o su pérdida accidental, así como el acceso, alteración, comunicación o cualquier otro tratamiento no autorizado.
>
> 10. El derecho de acceso por parte del paciente a la documentación de la historia clínica 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 su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas.
>
> 11. Los centros sanitarios y los facultativos de ejercicio individual sólo facilitarán el acceso a la historia clínica de los pacientes fallecidos a las personas vinculadas a él, por razones familiares o, de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. No se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros.
>
> 12. Para garantizar los usos futuros de la historia clínica, especialmente el asistencial, se conservará el tiempo mínimo establecido en la normativa básica estatal, contado desde la fecha del alta de cada proceso asistencial o desde el fallecimiento del paciente.

Como se puedo comprobar en el ámbito autonómico las normas se rigen por los mismos principios que en el ámbito estatal y europeo con las particularidades del contexto en el cual se han creado. En todo caso lo que la ley quiere reflejar es la importancia de la protección de la intimidad de los pacientes, así como otorgarles la libertad para ejercer sus derechos y, ante todo, que reciban un servicio de calidad y de una forma segura.

3. Estándares internacionales

La seguridad de la información y más concretamente los registros e historiales médicos electrónicos de salud se deben de ajustar a unos estándares para garantizar la seguridad y facilitar la interoperabilidad entre ellos. El objetivo de los estándares es construir un modelo homogéneo que ayude a la conservación, la disponibilidad y la comprensión de los registros, para así mejorar la atención a los pacientes.

3.1 UNE-ISO/IEC 27001

El estándar ISO/IEC 27001 especifica los requisitos que debe tener un sistema que garantice la seguridad de la información. Además, incluye los requisitos necesarios para la detección y resolución de los riegos de seguridad. Los requisitos son aplicables a todas las organizaciones independientemente de sus características. Los requisitos están divididos en siete bloques y deben de cumplirse todos para poder afirmar que el sistema está conforme con esta norma.

El primer bloque se refiere a los requisitos en el contexto de la organización, la cual debe determinar las partes interesadas relevantes del sistema y los requisitos de dichas partes que son importantes para su seguridad. La organización debe definir los límites y la aplicabilidad del sistema de seguridad para establecer su alcance y debe mejorar dicho sistema de forma continua de acuerdo con los requisitos de la norma.

En el segundo bloque se establece que la dirección del sistema debe de asegurar que se cumplen los requisitos mencionados anteriormente gestionando los roles y asegurando los recursos necesarios para conseguir los resultados previstos. Además, la dirección debe de establecer una política de seguridad que cumpla con los requisitos y en la cual esté disponible para todas las partes interesadas como información documentada.

En el bloque de planificación, la organización debe de determinar los riesgos y oportunidades necesarios para poder asegurar los requisitos de seguridad del sistema. Asimismo, debe planificar las acciones que se han de llevar a cabo para tratar dichos riesgos y evaluar la eficacia de dichas acciones. Se deben identificar, analizar y evaluar los riesgos para la seguridad de la información en el sistema documentado todo el proceso, y se debe de definir y realizar un proceso de tratamiento de dichos riesgos. La organización debe de establecer los objetivos de seguridad que tienen que cumplirse ajustándolos a los niveles adecuados. Dichos objetivos deben de ser coherentes con el sistema y deben de estar actualizados.

El cuarto bloque establece que la organización debe de establecer y proporcionar los recursos necesarios para poder satisfacer las necesidades del sistema de gestión de seguridad. Debe de determinar las competencias de las personas encargadas de la seguridad y garantizar su formación. Dichas personas deben de ser conscientes de su papel dentro de la gestión de la seguridad y los riesgos de no cumplir con los requisitos. Además, se debe de garantizar las comunicaciones necesarias para la seguridad.

En el quito bloque se menciona que la organización debe de llevar un control de los procesos necesarios para llevar a cabo las acciones y cumplir con los objetivos de seguridad del sistema. También debe de llevar un control de los riesgos de dichas acciones e implementar un plan de tratamiento de dichos riesgos.

La evaluación de la seguridad de la información viene detallada en el sexto bloque. La organización debe de evaluar la eficacia del sistema de gestión de la seguridad, determinando en todo momento que se debe evaluar, los métodos que se deben de seguir, las personas que deben de realizar la evaluación y cuando se debe de realizar. Además de todo esto la organización debe de realizar auditorías internas para asegurar que el sistema cumple con los requisitos. La dirección debe de revisar el sistema de gestión de la seguridad periódicamente para asegurarse que cumple con lo establecido en esta norma.

En el anexo A de la norma encontramos los puntos de control necesarios para una correcta evaluación del sistema, guardando estrecha relación con los puntos de control aplicados por el Esquema Nacional de Seguridad.

3.2 ISO/IEC 27002

La norma ISO/IEC 27002 contiene un conjunto de buenas prácticas para garantizar la seguridad en los sistemas de información. Fue creada a partir de la norma ISO/IEC 27001 como una guía para identificar e implantar las políticas, evaluarlas y mantenerlas de acuerdo con los requisitos que debe cumplir un sistema seguro.

La norma establece 14 grupos de directrices que se deben de seguir para una implementación de un sistema de información seguro. La norma no es certificable por sí misma, solo es una ayuda para los responsables de implantar el sistema que les permite hacerlo cumpliendo con los requisitos de la norma ISO/IEC 27001.

El equivalente en normativa española es la norma UNE-71501, esta norma dividida en tres partes, al igual que su equivalente internacional es una guía que presenta los modelos y conceptos para la gestión de la seguridad.

3.3 ISO/12052 DICOM

El estándar ISO/12052 establece la forma de almacenar, transmitir y gestionar las imágenes médicas. El estándar incluye un protocolo de comunicaciones basado en TCP/IP y un formato de archivo específico para este fin. Este formato permite que hardware de distintos fabricantes puedan transmitir datos e imágenes de los pacientes.

La finalidad de estándar es facilitar la interoperabilidad de los equipos y sistemas médicos que traten con imágenes médicas pertenecientes a los historiales de los pacientes.

3.4 ISO/10781 EHR

La ISO/10781 EHR establece un modelo para el uso de los historiales médicos electrónicos en un sistema de información de salud. Estos registros pueden compartirse en red entre los distintos entornos encargados de la atención médica.

Apuesta por un modelo de almacenamiento que permita recoger todos los datos clínicos de los pacientes con exactitud a través del tiempo. Dado que se trata de un archivo modificable se pueden recoger todos estos datos en un mismo archivo eliminando la posibilidad de documentos duplicados, desactualizados y/o erróneos.

Ilustración 1: Ejemplo de historial médico electrónico

4. Análisis de necesidades

El esquema nacional de seguridad es más o menos restrictivo en función de en qué infraestructura se aplica. La categoría de un sistema viene determinada en función del impacto en la organización que supondría un incidente de seguridad. Para realizar una categorización correcta del sistema el Real Decreto 3/2010 propone en su Anexo I, cinco dimensiones de seguridad a tener en cuenta: Disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad. A la vez, establece tres niveles de seguridad: Bajo, medio y alto para cada dimensión.

Las medidas de seguridad a tener en cuenta en un sistema varían en función de la categoría del sistema y también lo hace la forma en que son aplicadas.

Un hospital, podemos afirmar con toda la información extraída de los documentos oficiales, que se trata de una infraestructura crítica con un nivel de seguridad alto por diversos motivos:

- La disponibilidad de la información acerca de los pacientes en los hospitales es de vital importancia para llevar a cabo un diagnóstico y tratamiento correcto, que será siempre la prioridad de este tipo de organizaciones.
- La autenticidad e integridad de la información debe de estar garantizada, es necesario que dicha información solo pueda ser modificada por personal autorizado y competente.
- De acuerdo con la ley y por el hecho de que esta información contiene datos de carácter sensible es necesario garantizar la confidencialidad de los datos y que solo puedan ser accedidos por el paciente o por el personal médico autorizado en cada caso, siempre con el fin para el cual fueron recopilados.

Teniendo en cuenta que se trata de un nivel alto de protección, vamos a proceder a enlazar cada medida de seguridad con los requisitos necesarios para que cumpla dicha medida.

4.1 Marco organizativo

Apartado	Medida	Requisitos
org.1	Política de seguridad	Requiere de una política de seguridad escrita aprobada por el órgano superior competente. Dicha política deberá contener: • Los objetivos o misión de la organización. • El marco legal en el que se desarrollan las actividades • Los roles o funciones de seguridad con sus responsabilidades. • La estructura de los comités para la gestión de la seguridad. • Directrices para la documentación de la seguridad, su gestión y acceso. • Referencias y coherencia con el R.D. 1720/2007
org.2	Normativa de seguridad	Requiere de una serie de documentos que describan la normativa de seguridad que precise: • El uso correcto de equipos, servicios e instalaciones. • Lo que se considerará uso indebido. • La responsabilidad del personal con respecto al cumplimiento de las normas.
org.3	Procedimientos de seguridad	Requiere una serie de documentos que detallen como llevar a cabo las tareas habituales, quien debe realizar dichas tareas y como identificar y reportar los comportamientos anómalos.

org.4	Proceso de autorización	Requiere de un proceso formal de autorizaciones que cubra todos los elementos del sistema de información.

Tabla 1: Requisitos de marco organizativo

4.2 Marco operacional

4.2.1 Planificación

Apartado	Medida	Requisitos
op.pl.1	Análisis de riesgos	Requiere un análisis de riesgos formal que identifique y valore los activos más valiosos y las amenazas posibles.
op.pl.2	Arquitectura de seguridad	Requiere una documentación especifica de las instalaciones con los puntos de acceso y las áreas. Requiere una documentación del sistema con los equipos, las redes y los puntos de acceso. Requiere documentación de las líneas de defensa del sistema. Requiere documentación de sistema de autenticación e identificación de usuarios. Requiere documentación sobre los controles técnicos internos en la que se detalle cómo se controlan los datos una vez están en el sistema. Requiere una documentación del sistema de gestión actualizada y aprobada periódicamente. Toda esta documentación debe de estar aprobada por la dirección.
op.pl.3	Adquisición de nuevos componentes	Requiere la existencia de un plan formal de adquisición de nuevos componentes que atienda al análisis de riesgos y a la arquitectura de seguridad de los puntos anteriores y que contemple las necesidades técnicas de formación y de financiación conjunta. Además, este plan deberá estar aprobado por la dirección.
op.pl.4	Dimensionamiento / Gestión de capacidades	Requiere un estudio de las necesidades de dimensionamiento que cubra las necesidades de procesamiento, almacenamiento, comunicación, personal e instalaciones. Dicho estudio debe de estar aprobado por la dirección.
op.pl.5	Componentes certificados	Requiere el uso preferente de sistemas, productos y equipos certificados conforme a normas europeas por identidades independientes de reconocida solvencia.

Tabla 2: Requisitos de Planificación

4.2.2 Control de acceso

Apartado	Medida	Requisitos
op.acc.1	Identificación	Requiere que cada usuario o proceso que accede al sistema tenga un identificador único. Dicho

		identificador se debe saber a quién corresponde y que derechos tiene, y debe de mantenerse solo el tiempo necesario e inhabilitarse cuando el usuario deje la organización.
op.acc.2	Requisitos de acceso	Requiere que los recursos del sistema estén protegidos por algún mecanismo que impida el acceso a entidades no autorizadas.
op.acc.3	Segregación de funciones y tareas	Debe de existir una segregación de funciones y tareas que contemple la incompatibilidad entre: • Tareas de desarrollo y tareas de operación. • Tareas de configuración y tareas de operación. • Tareas de auditoria con el resto de tareas del sistema.
op.acc.4	Proceso de gestión de derechos de acceso	Requiere que la modificación de privilegios venga precedida de una solicitud por escrito del responsable del recurso al que se le va a conceder el acceso.
op.acc.5	Mecanismo de autenticación	Requiere la identificación del mecanismo de autenticación en cada recurso del sistema. Los identificadores deben se suspenderse tras un periodo de inactividad. Deben de utilizarse claves concertadas o contraseñas. Debe exigirse el uso de dispositivos físicos personalizados o biometría cuyo algoritmo este certificado.
op.acc.6	Acceso local (local logon)	Se debe prevenir la revelación de información del sistema. Se limita el número de intentos fallidos de acceso registrando los accesos fallidos y con éxito. Requiere informar al usuario de sus obligaciones después de obtener acceso. Requiere informar al usuario de su ultimo acceso con éxito. Requiere una limitación de horario de acceso, así como del lugar de acceso. Se deben de establecer puntos en los que el sistema requiera una renovación de la autenticación del usuario.
op.acc.7	Acceso remoto (remote login)	Requiere que se garantice la seguridad del sistema en un acceso remoto. Se debe de documentar que puede hacerse remotamente y se deben de autorizar previamente todos los accesos.

Tabla 3: Requisitos de control de acceso

4.2.3 Explotación

Apartado	Medida	Requisitos
op.exp.1	Inventario de activos	Se debe de disponer de un inventario actualizado con los activos del sistema en el cual se identifiquen la naturaleza de estos y su responsable.

		Requiere que los componentes desmantelados se retengan en el inventario.
op.exp.2	Configuración de seguridad	Requiere de un procedimiento de fortificación previo a la entrada en operación del sistema. En las situaciones que pongan en riesgo la seguridad se debe informar al usuario y que este preste su consentimiento. Requiere de una configuración por defecto segura. Requiere de un procedimiento de revisión de la configuración.
op.exp.3	Gestión de la configuración	Requiere que la configuración se gestione de forma continua.
op.exp.4	Mantenimiento	Requiere de un plan de mantenimiento físico y lógico con un procedimiento documentado que indique la frecuencia el responsable de la revisión y los componentes a revisar
op.exp.5	Gestión de cambios	Todos cambios en el sistema deben de llevar un control continuo.
op.exp.6	Protección frente a código dañino	Requiere de mecanismos de prevención y protección contra ataques con código dañino y debe de realizar un mantenimiento de dicho mecanismo.
op.exp.7	Gestión de incidencias	El sistema debe de disponer de un proceso integral para poder gestionar y hacer frente a todo tipo de incidentes que comprometan la seguridad del sistema.
op.exp.8	Registro de la actividad de los usuarios	Requiere de mecanismos que garanticen la hora a la que se realiza el registro de usuarios. Requiere que se registren todas las actividades que dichos usuarios realizan en el sistema. El nivel de detalle de dicho registro se establece en el análisis de riesgos.
op.exp.9	Registro de la gestión de incidencias	Requiere el registro de todas las actividades que tengan relación con la gestión de incidencias.
op.exp.10	Protección de los registros de actividad	Los registros del sistema deben de estar protegidos y su almacenamiento debe de estar garantizado.
op.exp.11	Protección de claves criptográficas	Las claves criptográficas deben de ser generadas por medios aislados del sistema de explotación. Durante su ciclo de vida dichas claves deben de estar protegidas, y al terminar dicho ciclo deben de ser archivadas en medios aislados. Los medios de generación y custodia deben de estar protegidos, certificados y con algoritmos certificados por el CCN. Requiere de un registro de las actuaciones de cada clave durante su ciclo de vida.

Tabla 4: Requisitos de explotación

4.2.4 Servicios externos

Apartado	Medida	Requisitos
op.ext.1	Contratación y acuerdos de nivel de servicio	Requiere el análisis de los riesgos de la contratación de un servicio externo. En dicho

		análisis deben de describirse las características del servicio, lo que se considerará calidad mínima y las responsabilidades de ambas partes.
op.ext.2	Gestión diaria	Requiere de un sistema rutinario para medir el cumplimiento de las obligaciones del servicio. Requiere de un procedimiento para neutralizar las deviaciones del margen de tolerancia. Requiere el establecimiento de un mecanismo de coordinación para llevar a cabo las tareas de mantenimiento. Requiere un mecanismo de coordinación en caso de incidencia o desastre.
op.ext.9	Medios alternativos	Requiere de un plan dentro del plan de continuidad, que permita reemplazar el servicio contratado por otro que ofrezca las mismas garantías de seguridad en caso de indisponibilidad del servicio contratado.

Tabla 5: Requisitos de servicios externos

4.2.5 Continuidad del servicio

Apartado	Medida	Requisitos
op.cont.1	Análisis de impacto	Requiere la realización de un análisis de impacto que identifique los requisitos de disponibilidad de cada servicio y los elementos críticos para la prestación de dichos servicios.
op.cont.2	Plan de continuidad	Requiere de un plan de continuidad que establezca las acciones que se deben de llevar a cabo en caso de interrupción de los servicios prestados. Dicho plan debe de identificar las funciones, responsabilidades y actividades a realizar, los medios alternativos deben de estar previstos y planificados y las personas implicadas deben de recibir la formación específica requerida en su caso.
op.cont.3	Pruebas periódicas	Se deben realizar pruebas periódicamente para localizar y corregir los errores y deficiencias que puedan existir en el plan de continuidad.

Tabla 6: Requisitos de continuidad del servicio

4.2.6 Monitorización del sistema

Apartado	Medida	Requisitos
op.mon.1	Detección de intrusión	Requiere de herramientas de prevención y detección de intrusión.
op.mon.2	Sistema de métricas	Requiere de un sistema de métricas que midan el desempeño real de seguridad del sistema.

Tabla 7: Requisitos de monitorización del sistema

4.3 Medidas de protección

4.3.1 Protección de instalaciones e infraestructuras

Apartado	Medida	Requisitos

mp.if.1	Áreas separadas y con control de acceso	El equipamiento debe ser instalado en áreas separadas y especificas con control de acceso.
mp.if.2	Identificación de las personas	El acceso a las zonas donde haya equipamiento que pertenece al sistema debe de estar controlado identificando a las personas y guardando un registro de las entradas y salidas. Dichas personas deben de portar una identificación visible. Las funciones de control y gestión del acceso deben de recaer en 3 personas diferentes. Los visitantes deben de ir acompañados en todo momento.
mp.if.3	Acondicionamiento de los locales	Los locales donde se ubiquen los sistemas deben de disponer de unas condiciones adecuadas de temperatura y humedad. Además, deben de contar con protección frente a los riesgos y accidentes. Requiere de un mapa del cableado de la instalación con los cables adecuadamente etiquetados. Debe de existir equipamiento de acondicionamiento redundante disponible para ser utilizado en caso de fallo.
mp.if.4	Energía eléctrica	El suministro de potencia debe de estar garantizado. Se debe disponer de las tomas eléctricas necesarias y se debe de garantizar el adecuado funcionamiento de las luces de emergencia. Se debe garantizar el suministro en caso de fallo el tiempo suficiente para la terminación de procesos y guardado de la información. Requiere de un contrato con un proveedor de energía eléctrica alternativo.
mp.if.5	Protección frente a incendios	Los locales donde se ubiquen los sistemas de la información deben de estar protegidos contra incendios accidentales o intencionados conforme a la normativa industrial pertinente.
mp.if.6	Protección frente a inundaciones	Los locales donde se ubiquen los sistemas de la información deben de estar protegidos contra incidentes accidentales o provocados causados por la acción del agua.
mp.if.7	Registro de entrada y salida de equipamiento	Las salidas y entradas de equipamiento deben de estar debidamente documentadas identificando a la persona que lo lleva a cabo. Dichos registros deben de estar disponibles el tiempo que la dirección establezca y las gestiones deben recaer en tres personas distintas.
mp.if.9	Instalaciones alternativas	Deben de estar disponibles instalaciones alternativas para poder continuar con las funciones del sistema en caso de fallo de las instalaciones habituales.

Tabla 8: Requisitos de protección de instalaciones e infraestructuras

4.3.2 Gestión de personal

Apartado	Medida	Requisitos
mp.per.1	Caracterización del puesto de trabajo	Cada puesto de trabajo debe de estar caracterizado. Las responsabilidades y los requisitos que deben de satisfacer las personas que ocupen dicho puesto deben de estar definidos. Los requisitos deben de tenerse en cuanta para la selección de personal.
mp.per.2	Deberes y obligaciones	Se debe de informar a cada persona que ocupe un determinado puesto de trabajo de sus deberes y obligaciones en materia de seguridad especificando las medidas de seguridad del puesto. Con respecto a las personas contratadas de un tercero deben de ser informados de sus deberes y obligaciones, además de establecer los deberes y obligaciones de cada una de las partes y de disponer de un procedimiento de resolución de incidentes relacionados con el incumplimiento de dichas obligaciones. Debe de existir un acuerdo de confidencialidad firmado.
mp.per.3	Concienciación	Se deben de realizar acciones dentro de un plan de concienciación para concienciar periódicamente al personal de su responsabilidad a la hora de garantizar la seguridad del sistema. Dicho plan debe de estar financiado y debe de existir constancia de que cada persona lo ha recibido y seguido.
mp.per.4	Formación	El personal debe de ser formado regularmente en las materias que necesite para el desempeño de sus funciones, dicha formación debe de cubrir la configuración del sistema y la detección y reacción ante incidentes. Requiere que haya constancia de dicho plan formativo.
mp.per.9	Personal alternativo	Requiere la existencia y disponibilidad de personal alternativo que cubra el puesto en caso de ausencia del personal habitual. Dicho personal debe de proporcionar las mismas garantías de seguridad que el personal habitual.

Tabla 9: Requisitos de gestión de personal

4.3.3 Protección de equipos de trabajo

Apartado	Medida	Requisitos
mp.eq.1	Puesto de trabajo despejado	En los puestos de trabajo solo deberá estar el material necesario para la actividad que se está realizando. El resto de material de nivel medio que no se está utilizando deberá estar almacenado en un lugar cerrado.
mp.eq.2	Bloqueo de puesto de trabajo	Requiere el bloqueo del puesto de trabajo tras un cierto tiempo de inactividad que requerirá una nueva autenticación por parte del usuario. Tras un tiempo superior al anterior se deberán

		de cerrarse las sesiones abiertas de dicho puesto.
mp.eq.3	Protección de equipos portátiles	Los equipos que abandonen las instalaciones deben de protegerse llevando un inventario de los mismos y deben de estar dotados de los mecanismos de detección necesarios que permitan saber si el sistema ha sido manipulado. La información de nivel alto almacenada en el disco duro debe de estar protegida mediante cifrado.
mp.eq.3	Medios alternativos	Requiere la existencia y disponibilidad de medios alternativos para el tratamiento de información en caso de fallo de los sistemas habituales. Dichos medios deben de tener las mismas garantías de seguridad que los medios habituales. Se debe establecer un tiempo máximo para que dichos medios alternativos entren en funcionamiento.

4.3.4 Protección de las comunicaciones

Apartado	Medida	Requisitos
mp.com.1	Perímetro seguro	Requiere de un cortafuego que separe la red interna del exterior. Dicho cortafuego debe de constar de dos o más equipos de diferentes fabricantes dispuestos en cascada y deben de ser redundantes.
mp.com.2	Protección de la confidencialidad	Para la comunicación por fuera del propio domino de seguridad requiere el uso de VPN (redes privadas virtuales) cuyos algoritmos estén acreditados por el CCN. Se deben de utilizar preferentemente dispositivos hardware y productos certificados para la utilización de la VPN.
mp.com.3	Protección de la autenticidad y de la integridad	La autenticidad del otro extremo de la comunicación debe de estar garantizada antes del intercambio de información. Deben de tomarse medidas para la prevención de ataques del tipo MITM (Man In The Midle).
mp.com.4	Segregación de redes	La red debe de estar segmentada existiendo un control de la entrada los usuarios que llegan a cada segmento de la red y de la salida de información. El punto de interconexión entre los segmentos debe de estar asegurado y monitorizado.
mp.com.9	Medios alternativos	Requiere la existencia y disponibilidad de medios alternativos de comunicación que actúen en caso de fallo de los sistemas habituales. Dichos medios deben disponer de las mismas garantías de seguridad que los medios habituales.

Tabla 10: Requisitos de protección de las comunicaciones

4.3.5 Protección de los soportes de información

Apartado	Medida	Requisitos
mp.si.1	Etiquetado	Los dispositivos de la información deben de estar etiquetados indicando el nivel de seguridad de la información contenida. Los usuarios deben de entender el significado de las etiquetas sin que están revelen nada de la información contenida dentro del dispositivo.
mp.si.2	Criptografía	Requiere del uso de mecanismos criptográficos para todos los dispositivos extraíbles. Los algoritmos deben de estar certificados y acreditados por el CCN.
mp.si.3	Custodia	Los soportes de información deben de estar protegidos y controlados por la organización. Cada dispositivo debe de poseer una historia desde su primer uso hasta el fin de su vida útil y posterior destrucción.
mp.si.4	Transporte	Requiere de un registro de entrada y otro de salida que registre al transportista que lleva a cabo el transporte. Requiere de un procedimiento rutinario que coteje las salidas con las llegadas. La información de mayor nivel debe de estar protegida criptográficamente y las claves deben de estar gestionadas de forma segura.
mp.si.5	Borrado y destrucción	Los soportes que vayan a ser reutilizados o liberados deben de ser borrados de forma segura, en caso de no poderse llevar a cabo dicho borrado deben de ser destruidos. Se deben utilizar preferentemente productos certificados.

Tabla 11: Requisitos de protección de los soportes de información

4.3.6 Protección de las aplicaciones informáticas

Apartado	Medida	Requisitos
mp.sw.1	Desarrollo	Las aplicaciones que vayan a utilizarse en el sistema deben de ser desarrolladas en un sistema diferente y separado. No deben existir herramientas de desarrollo en el entorno de producción. La metodología de desarrollo debe de estar reconocida y debe de tener en cuenta los aspectos de seguridad del sistema durante todo el proceso. Debe de aplicar un procedimiento documentado para la inspección del código desarrollado.
mp.sw.2	Aceptación y puesta en servicio	Requiere de un plan de pruebas de la aplicación antes de poner la aplicación en funcionamiento. Dicho plan de pruebas debe de: • Comprobar que se cumplen los criterios de seguridad. • Comprobar que no compromete la seguridad de otros componentes del sistema. • Contemplar que las pruebas se realicen en un entorno aislado.

		• No debe de utilizar datos reales. Antes de la entrada en funcionamiento debe de realizarse un análisis de vulnerabilidades que contenga: • Una prueba de penetración. • Un análisis de coherencia para la integración de procesos. • La posibilidad de realizar una auditoría de código fuente.

Tabla 12: Requisitos de protección de las aplicaciones informáticas

4.3.7 Protección de la información

Apartado	Medida	Requisitos
mp.info.1	Datos de carácter personal	Los datos de carácter personal del sistema deben de estar debidamente identificados y se debe de aplicar la normativa vigente (L.O. 15/1999 LOPD).
mp.info.2	Calificación de la información	La información debe de estar calificada conforme a la naturaleza de la misma. La política de seguridad debe de establecer quién es el responsable de cada información manejada por el sistema y los criterios que se deben de seguir para cada nivel de seguridad distinto. Requiere la existencia de procedimientos que describan en detalle la forma de etiquetar y tratar la información. Dicho procedimiento debe de contemplar el acceso, almacenamiento, etiquetado, transmisión, realización de copias y cualquier otra actividad relacionada.
mp.info.3	Cifrado	La información de alto nivel debe de permanecer cifrada durante su almacenamiento y transmisión, y únicamente estará en claro durante su uso.
mp.info.4	Firma electrónica	Requiere de una política de firma electrónica aprobada por el órgano superior competente. Los documentos que requieren capacidad probatoria deben de estar formados electrónicamente. Los algoritmos empleados deben de estar certificados por el CCN. Los certificados deben de estar reconocidos. La firma electrónica debe de estar validada y verificada durante el tiempo requerido por la actividad. Los dispositivos de creación de firma deben de ser seguros.
mp.info.5	Sellos de tiempo	Requiere el uso de sellos de tiempo para aquella información que se pueda utilizar en un futuro como información actual. Los datos de la fecha deben de ser tratados con la misma seguridad que la información fechada. Los sellos de tiempo deben renovarse regularmente hasta que la información ya no sea

		requerida.
mp.info.6	Limpieza de documentos	Requiere de un procedimiento para limpiar la información contenida dentro de documentos que vayan a ser transferidos a otro dominio.
mp.info.9	Copias de seguridad (backup)	Requiere la realización de copias que permitan la recuperación de datos perdidos accidental o deliberadamente. Dichas copias de seguridad: • Deben abarcar toda la información de trabajo de la organización. • Deben contener todas las aplicaciones incluidos los sistemas operativos. • Deben incluir los datos de configuración, servicios, aplicaciones, equipos y similares. • Debe de incluir las claves utilizadas para preservar la confidencialidad • Debe de existir un proceso para la recuperación de las copias. • Debe verificarse periódicamente que la información está dispuesta a ser recuperada en cualquier momento de necesidad. • Las copias deben de estar almacenadas en un lugar independiente de la ubicación del sistema de forma que los riegos previstos no puedan producirse simultáneamente en ambos lugares.

Tabla 13: Requisitos de protección de la información

4.3.8 Protección de los servicios

Apartado	Medida	Requisitos
mp.s.1	Protección del correo electrónico	La información distribuida mediante correo electrónico debe de estar protegida. La información de encaminamiento de mensajes y establecimiento de conexión debe de estar protegida. La organización debe de estar protegida contra el correo no deseado, el ataque de virus y el código móvil. El uso del correo electrónico debe de estar sujeto a una normativa documentada que contemple las limitaciones de uso privado. Se deben de llevar a cabo actividades de concienciación y formación frente al uso responsable del correo electrónico. La disponibilidad del correo debe de estar garantizada.
mp.s.2	Protección de servicios y aplicaciones web	Requiere que los subsistemas dedicados a la publicación de información se encuentren protegidos ante las amenazas. El acceso a la información debe de estar protegido por algún sistema de control que imposibilite obtener dicha información sin autenticarse. El servidor no debe ofrecer ninguna otra forma

		de acceso que no sea a través de autenticado. Deben de prevenirse los ataques de manipulación de la URL y de las cookies de los usuarios. Se deben prevenir los ataques por inyección de código, los intentos de escalado de privilegios, los ataques de manipulación de caches y los ataques de cross site scripting. Los datos publicados deben ser limpiados según lo dispuesto en el punto [mp.info.6] Deben de realizarse auditorias sobre la seguridad y pruebas de presentación del sistema.
mp.s.8	Protección frente a la denegación de servicio	El sistema debe de estar provisto de más potencia que la requerida para soportar toda la carga de información que está previsto que reciba. Se deben incorporar tecnologías y mecanismos que protejan al sistema de ataques de DoS (Denial of Service). Requiere un procedimiento de reacción frente a ataques de DoS. Se debe de proteger el sistema para evitar que se lancen ataques a terceros desde el mismo.
mp.s.9	Medios alternativos	Debe de garantizarse la existencia y disponibilidad de medios alternativos con las mismas garantías de seguridad que los medios habituales y se debe de establecer un tiempo máximo para que dichos medios entren en funcionamiento.

Tabla 14: Requisitos de protección de los servicios

Los requisitos mostrados anteriormente son solo un resumen sintetizado a partir de la normativa del Esquema Nacional de Seguridad. Para profundizar más en este tema el Centro Criptológico Nacional dispone de una serie de guías (CCN-STIC-800) para la implementación de estas medidas. Se pueden consultar en la misma página del CCN (https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html)

5. Aplicación práctica

Para la aplicación del esquema nacional de seguridad el Centro Criptológico Nacional propone una serie de guías que ayudan a los organismos a cumplir con las normativas. Como se ha mencionado con anterioridad, la realización de auditorías para comprobar que dicha normativa se cumple es obligado para todos los organismos que apliquen el esquema en sistemas de categoría media o alta. Las auditorias deben de ser realizadas por un equipo competente que demuestre que tiene los conocimientos necesarios. Con

el fin de ayudar a este equipo a realizar mejor su trabajo en el entorno de una infraestructura hospitalaria se ha realizado la implementación de una aplicación de escritorio.

5.1 Análisis

A la hora de pensar en una aplicación que ayude a los auditores a realizar su trabajo, lo primero que debemos tener en cuenta es que se trate de una aplicación sencilla, se presupone que los auditores son personas con conocimientos informáticos altos, pero el objetivo es facilitarles el trabajo no causarles pérdidas de tiempo. Por ello la interfaz de la aplicación debía de ser intuitiva y manejable.

La herramienta tiene que satisfacer las siguientes necesidades:

- Poder contener la información requerida para un informe de auditoría de un sistema.
- Poder guardar dicha información en un formato que después la misma aplicación pueda leer.
- Poder generar un informe preliminar que ayude al auditor a realizar el informe final.
- Ser portable.
- Ser tolerante a los cambios en la normativa.

5.2 Tecnologías utilizadas

Para la realización de este proyecto se han utilizado diversas tecnologías, se han intentado utilizar tecnologías que además de adecuadas resultaran conocidas o estudiadas durante los años de grado, aunque algunos conocimientos se han profundizado más durante la realización del proyecto. Las tecnologías empleadas más destacadas son:

5.2.1 Java

La aplicación está programada en lenguaje Java. Este es un lenguaje orientado a objetos desarrollado por Sun Microsistems en 1991. Java es un lenguaje compilado-interpretado ya que compila el código convirtiéndolo en un *bytecode* que más tarde es interpretado por la máquina virtual de java JVM (Java Virtual Machine). Esto le proporciona una de sus mayores ventajas: La portabilidad.

Además de por su portabilidad que le permite ser ejecutado en la gran mayoría de entornos hemos elegido Java para el proyecto por ser de fuente abierta y disponer de

gran cantidad de librerías que, durante el proyecto o en un futuro, nos serían de utilidad. Otros motivos para elegir Java es que ha sido objeto de estudio durante el grado y hay gran cantidad de documentación acerca de este lenguaje.

Ilustración 2: Logotipo de Java.

5.2.2 SQL

SQL o Simple Query Language es un lenguaje de gestión de bases de datos relacionales que permite realizar diferentes tipos de operaciones en ellas. Fue definido en 1974 por Donald Chamberlin, aunque ha sufrido diversas modificaciones y mejoras hasta lo que conocemos hoy en día. Se trata de un lenguaje estructurado y declarativo que estaca por su sencillez a la hora de realizar las consultas y por facilitar la interacción entre el usuario y la base de datos. En 1986 se adoptó como estándar para los lenguajes relacionales por lo que se integra perfectamente con Java, que dispone de librerías para la conexión con la base de datos. Como gestor de base de datos utilizaremos MySQL, un gestor de bases de datos relacionales de código abierto integrado dentro de XAMPP.

Ilustración 3: Logotipo MySQL.

5.2.3 XML

El lenguaje de marcas extensible (eXtensible Markup Languaje) fue desarrollado por el World Wide Web Consortium (W3C) para almacenar datos de forma legible. Se ha convertido en un estándar para el intercambio de información y la integración de datos entre diferentes plataformas. Hemos elegido XML para nuestra aplicación porque proporciona una forma sencilla de almacenar los datos introducidos por el usuario,

guárdalos en un documento .xml y posteriormente ser leídos e interpretados de nuevo por la aplicación en caso de que el usuario lo desee.

5.2.4 Texto

IText es una librería que proporciona a los usuarios integrar funciones en su código Java para manipular PDF's. Se trata de una librería de código abierto que integraremos en nuestro proyecto para poder generar los informes de las auditorias en PDF.

Ilustración 4: Logotipo de IText

5.2.5 Eclipse

Se trata de un entorno de desarrollo de código abierto compuesto por una plataforma principal, una plataforma de bunding, el SWT o Standard Widget Toolkit, JFace para el manejo de archivos y el Workbench de eclipse. Eclipse emplea módulos para ampliar su funcionalidad a gusto del usuario. Para programar en Java el SDK de eclipse proporciona una serie de herramientas de desarrollo y un IDE con un compilador de Java.

Hemos elegido Eclipse en su versión Neon.3 para este proyecto debido a la experiencia de su uso en proyectos anteriores y por la facilidad a la hora de manejar proyectos e importar librerías.

Ilustración 5: Logotipo de Eclipse.

5.2.6 Java FX

Java FX es una plataforma diseñada para crear aplicaciones interactivas en lenguaje Java. Las aplicaciones desarrollas en JavaFX pueden ser ejecutadas en una gran cantidad de dispositivos. Esta escrito como una API de java por lo que se integra perfectamente en este lenguaje. Utiliza FXML, leguaje declarativo basado en XML para construir las interfaces de usuario. Permite añadir todos los controles necesarios para añadir la funcionalidad de la aplicación, además de integrar CSS para añadir el estilo deseado por el desarrollador. Por ello hemos elegido esta tecnología para proporcionar una interfaz a nuestra aplicación.

5.2.7 Scene Builder

Es una herramienta de diseño de aplicaciones de forma visual (drag & drop), permite a los usuarios diseñar rápidamente sus aplicaciones JavaFX sin necesidad de programarlas a mano. Permite generar un área de trabajo en la cual puedes arrastrar componentes de la interfaz y ajustar sus características. Posteriormente genera el código FXML que se integra en la aplicación Java. Se trata de una herramienta gratuita, sencilla y potente.

Ilustración 6: Logotipo Scene Builder.

5.2.8 XAMPP/ PHP MyAdmin

XAMPP es una plataforma de software libre gratuita fácil de instalar y configurar. Dentro de XAMPP encontramos PHP MyAdmin, una herramienta desarrollada en PHP con la cual podemos manejar bases de datos MySQL. En nuestro proyecto lo hemos utilizado para simular una base de datos local que sirva de modelo para las bases de datos a las que se conectará nuestra aplicación.

Ilustración 7: Logotipo de XAMPP

5.3 Diseño

5.3.1 Interfaz

El diseño de la interfaz se ha realizado con Scene Builder y consta de cuatro ventanas o interfaces: Una ventana inicial que será la primera ventana que vea el usuario al iniciar la aplicación, dos ventanas para introducir datos que ayuden a completar el informe y una ventana principal que será con la que más interactuará el usuario a la hora de utilizarla.

Para dotar de más personalidad a la aplicación y como detalle de diseño personal se le ha otorgado a la aplicación el nombre de “Haudi” y sea diseñado un logotipo para la

Ilustración 8: Logotipo de la aplicación.

ventana de inicio y un icono para el resto de ventanas.

La ventana de inicio tiene una funcion básica y es presentar la aplicación al usuario, contiene el logotipo de la aplicación y cuatro botones para que el usuario elija si desea comenzar una auditoria nueva , continuar una empezada anteriormente, modificar la ubicación de la base de datos de la cual se van a tomar las medidas y requisitos para la auditoria o por último cerrar la aplicación cuando lo desee.

Ilustración 9: Ventana inicial.

Después de la ventana inicial tenemos la ventana principal, esta ventana es la base de toda la aplicación, en ella los usuarion rellenan todos los datos con respecto a las medias de seguridad y la forma en que dichas medidas se aplican al sistema, asi como escribir comentarios para cada medida. Como cada medida tiene unos requisitos, estos van variando en función de que el usuario interactua con los botones “Anterior” y “Siguiente”. Tambien pueden acceder directamente a una medida en concreto gracias al menu de la parte superior, en dicho menu tambien tenen un desplegable de “herramientas” entre las cuales se encuentran las opciones de “Guardar”, “Abrir”, Modificar Datos” y “Salir”. En la parte inferior ademas de los botones para cambiar de medida tenemos otro botón de guardar a modo de acceso directo y el boton para poder generar el informe en PDF.

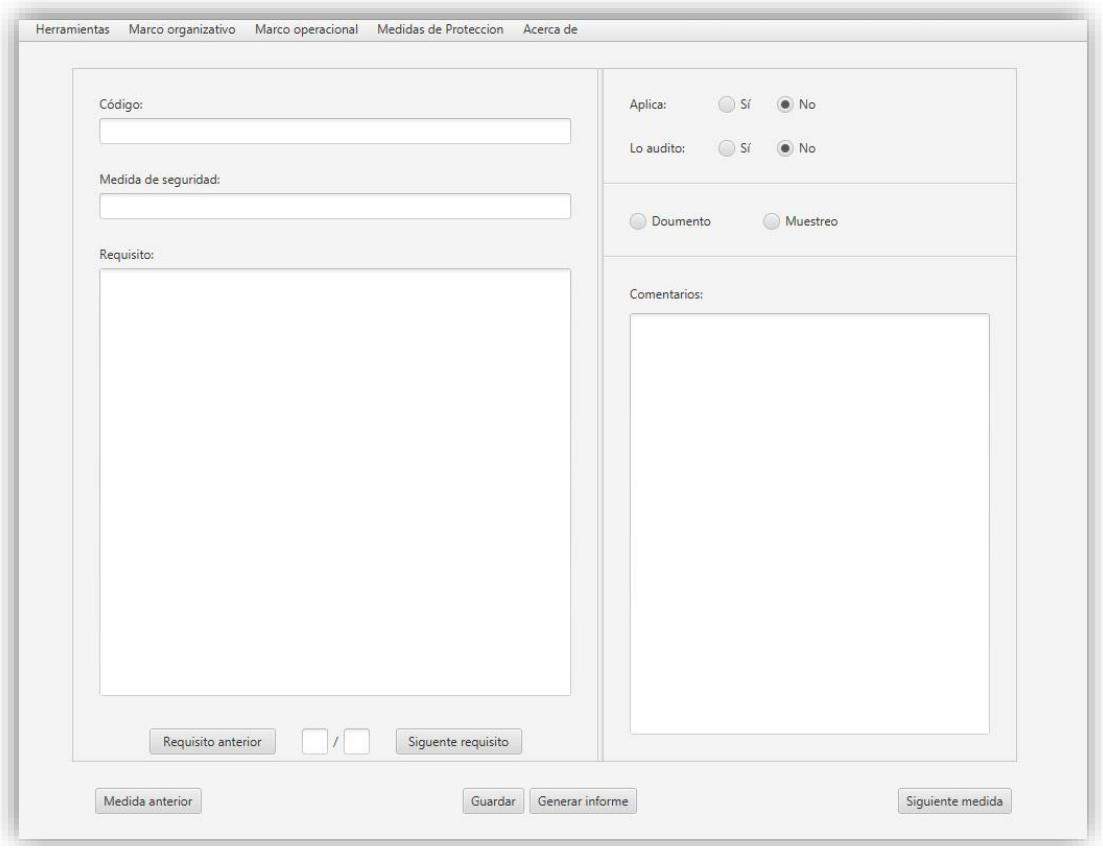

Ilustración 10: Ventana principal.

Las ventanas de datos, son usadas por los usuarios para incluir los datos ténicos que son necesarios para la auditoria en el informe. Se trata de dos ventanas, en la primera de ellas los usuarios introduciran datos como el nombre del organismo y del sistema el cual estan auditando, la fecha de inicio de la auditoria, la categoría del sistema o la localización o localizaciones en las que se encuentra el sistema.

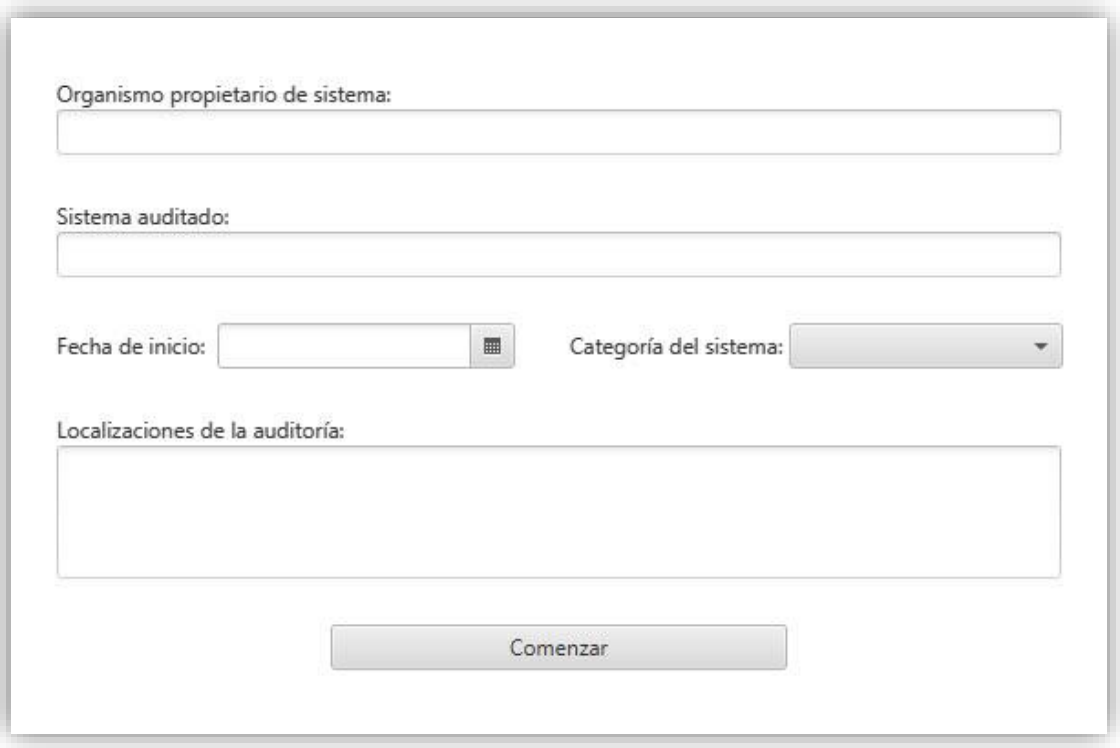

Ilustración 11: Ventana de datos 1

En la segunda ventana se introducen los datos del equipo auditor asi como, los nombres de los resposables del sistema y si fuera el caso el nombre de los expertos que han participado en la auditoria. Tambien se podran incluir en el infrome el criterio metodologico con el cual se ha llevado a acabo la auditoria y la legislacion adicional empleada si fuera necesario. Se debe seleccionar el tipo de auditoria mediante un selector de lista deplegable.

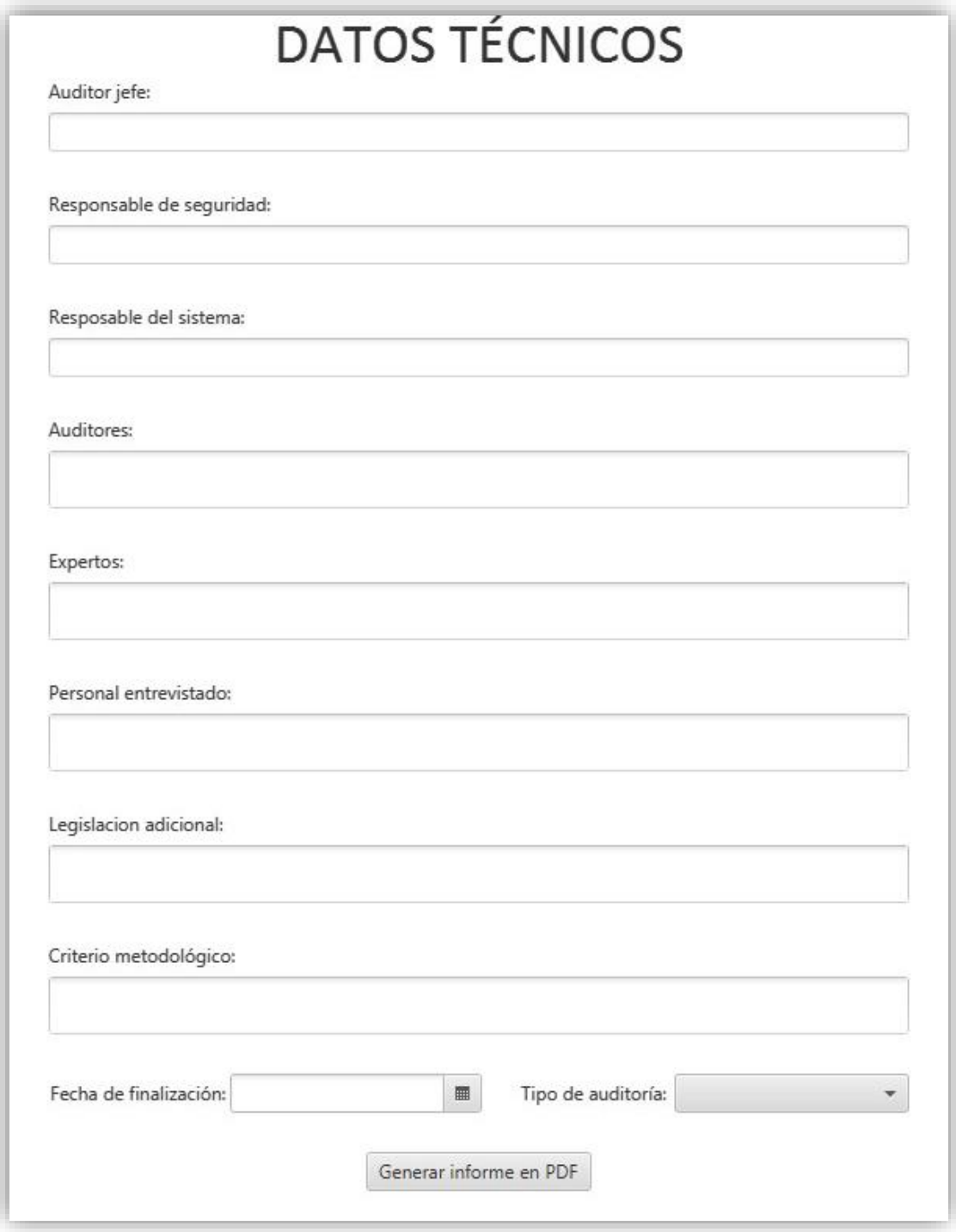

Ilustración 12: Ventana de datos 2

Por último tenemos la ventana que permite al usuario cambiar la base de datos que va a usar para la auditoria, el motivo de añadir esta opcion a la aplicación no es otro que asegurar que aunque cambie la normativa o los requisitos que se deben cumplir, la aplicación estara actualizada simplemente cambiando de base de datos, también

asegura que la aplaplicación pueda concetar a distintas bases de datos en distintas ubicaciones.

Ilustración 13: Ventana de ajuste de base de datos

5.3.2 Base de datos

El diseño de la base de datos es simple, pues no requiere una estructura compleja, tan solo necesitamos almacenar en una tabla las medidas de seguridad con su código correspondiente y en otra tabla los requisitos necesarios para cada medida. Por tanto, la tabla de medidas tendrá tres columnas, una para el código, otra para la medida y por último una que contendrá un número que establecerá el orden en el cual aparecen en la normativa. La tabla de requisitos contendrá para cada una de las medidas los requisitos que dicha medida debe cumplir, contará con una columna con el código de la medida, una columna con un identificador, una columna con un número que establece la posición u orden del requisito, y por último una comuna con los requisitos de dicha medida.

Esta base de datos es un modelo básico para el funcionamiento de la aplicación, para las pruebas se ha creado con la herramienta phpmyadmin localizada en el mismo

equipo que la aplicación, aunque de cara a un uso real de la aplicación debería conectarse a una base de datos central común para todos los usuarios. La base de datos proporciona la tolerancia a cambios en la normativa de la que hablábamos en los requisitos del sistema ya que en caso de un cambio en los requisitos tan solo se tendría que modificar la base de datos respetando el modelo.

5.4 Funcionalidad

A continuación, vamos a describir como se ha realizado la implementación de la funcionalidad básica de la aplicación. Para implementar la funcionalidad de la aplicación se ha utilizado el lenguaje java en la versión 8 y le herramienta eclipse en la versión neon.3.

Para la implementación del proyecto se ha optado por un diseño por capas. La estructura del proyecto java está dividida en 3 capas que corresponden a 3 paquetes dentro del proyecto llamados presentación, lógica y persistencia. Se ha optado por esta división de paquetes para facilitar la programación de la aplicación y la introducción de mejoras en un futuro.

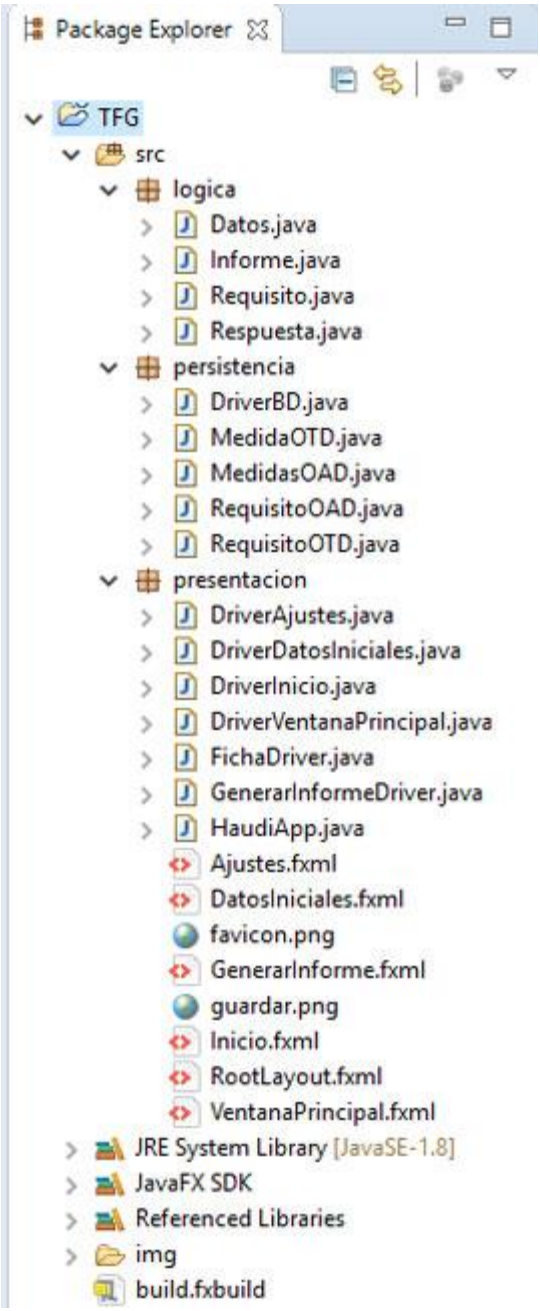

Ilustración 14: Arquitectura del proyecto

5.4.1 Presentación

En la parte visual encontramos las interfaces descritas en el apartado de diseño, Scene Builder las ha generado automáticamente mediante ficheros FXML. Junto con las interfaces tenemos los controladores que se encargan de otorgar la funcionalidad para la interacción de las interfaces con el usuario.

Estos controladores contienen todos los métodos necesarios para que la aplicación responda ante una acción del usuario, cada ventana FXML tiene asociada su controlador particular y especifico. Dentro de la clase del controlador se encuentra un

objeto por cada elemento que contiene la interfaz con un identificador único que nos servirá para implementar las acciones que realizará la aplicación. A continuación, expondremos como hemos implementado la funcionalidad de los elementos más importantes.

Primero vamos a explicar cómo hemos implementado la funcionalidad de los botones. Para que cuando el usuario haga clic en un botón, la aplicación realice un evento, lo primero fue definir el botón como un objeto de tipo Button de la siguiente forma:

```
@FXML
private Button nueva;
@FXML
private Button continuar;
@FXML
private Button salir;
```

Ilustración 15: Definición de un objeto de tipo Button

Después de definir el objeto hemos creado un método que contendrá las acciones que debe de realizar la aplicación cuando el usuario realice la acción. Un ejemplo de este método es el que hemos implementado para cuando el usuario desee continuar con una auditoria que dejo a mitad:

```
@FXML
void continuar(){
    informe=Informe.abrir();
    Parent root;
     FXMLLoader loader = new FXMLLoader(getClass().getResource("/visual/VentanaPrincipal.fxml"));
     try {
    root = (Parent) loader.load();
     Scene scene = new Scene(root, 1024,768);
     Stage stage = new Stage();
     stage.initModality(Modality.APPLICATION_MODAL);
     stage.setScene(scene);
     stage.setTitle("Ficha de auditoría");
     stage.setResizable(false);
     stage.show();


     } catch (IOException e) {
            // TODO Auto-generated catch block
            e.printStackTrace();
        }
}
```

Ilustración 16: Método continuar

El método actualiza el objeto informe llamando al método abrir() que explicaremos más adelante y posteriormente crea la ventana principal y la lanza permitiendo al usuario continuar con su auditoria.

Por último, solo hemos tenido que indicarle al código FXML que método debe ejecutar cuando el usuario haga seleccione el botón, podemos hacerlo desde Scene Builder, en

las propiedades del botón, o directamente desde el código FXML añadiendo la propiedad "*onAction*" con el nombre de nuestro método:

```
<Button fx:id="continuar" mnemonicParsing="false" onAction="#continuar" prefHeight="60.0" prefWidth="400.0" text="Continuar auditoría">
   <VBox.margin>
      <Insets bottom="10.0" />
   </VBox.margin>
   <font>
      <Font size="22.0" />
   </font>
</Button>
```

Ilustración 17: Llamada al método desde FXML

Otros elementos que componen nuestra interfaz son los RadioButton y Los TextField, estos elementos son los encargados de mostrar contenido a los usuarios y de recoger los datos que el usuario introduce. Para ello hemos definido los objetos de la misma forma que hemos hecho anteriormente con los botones, para mostrar los datos de la aplicación o para guardar los introducidos por el usuario nos hemos ayudado de los métodos setText() y getText() respectivamente para los TextField y de los métodos isSelected() y setSelected() para los RadioButton.

5.4.2 Lógica

La capa de lógica es en realidad el motor de nuestra aplicación, en ella se han implementado todos los métodos necesarios para que funcione correctamente. Los métodos de los controladores de la capa de presentación tan solo actúan como intermediarios, es decir llaman a otros métodos que están implementados en la capa de lógica.

Dentro de este paquete encontramos cuatro clases Informe, Datos, Requisitos y Respuesta. En la clase Informe es donde se encuentran los métodos más importantes de la aplicación que se definen a continuación.

El método para generar un informe llamado genInforme() que devuelve un HashMap que contiene como identificador la id de la medida a la que corresponderá un objeto de la clase Respuesta.

El método para guardar las auditorias en formato XML llamado guardarArchivo() este método genera un fichero con el formato establecido (Ver Anexo I) que guarda donde el usuario le indica mediante un objeto JFileChooser.

El método para abrir el archivo guardado con el método anterior llamado abrir() este método lee un fichero que selecciona el usuario y actualiza el objeto de tipo informe creado y los datos de la auditoria conforme a lo leído en el archivo XML.

Para valorar el grado de cumplimiento del sistema conforme al Esquema Nacional de Seguridad se han implementado dos métodos. El primero de ellos llamado grado() calcula el grado de cumplimiento con una sencilla formula que divide el número de medidas cumplidas entre el número total de medidas multiplicado por 100 para obtener un porcentaje. Cabe destacar que solo se consideran como medidas cumplidas las medidas que estén también auditadas. El segundo método llamado cumplimiento() indica si el cumplimiento es alto, medio o bajo en función del porcentaje obtenido en el primer método.

Por último, se ha implementado el método para generar los informes en pdf llamado informePdf() en este método se toman los datos introducidos por el usuario en la aplicación, con la ayuda de la librería IText se le da formato al archivo pdf, el formato es similar al propuesto por el CCN en el anexo II de la guía CCN-STIC-808 v1.0, una vez formateado la librería genera y guarda el archivo pdf.

El código de los métodos descritos anteriormente se adjunta en el anexo II del presente proyecto.

5.4.3 Persistencia

Para la conexión de la base de datos hemos implementado un driver con la ayuda de las clases Connection y DriverManager, el driver conecta nuestra aplicación con la base de datos introducida por el usuario en los ajustes, aunque la base de datos establecida por defecto se encuentra en localhost.

```
public static Connection conectar(){

    Connection conexion=null;
    try {
        Class.forName("com.mysql.jdbc.Driver");
        conexion =DriverManager.getConnection(url, usuario, contraseña );
    } catch (ClassNotFoundException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
    } catch (SQLException e) {
        Alert alert = new Alert(AlertType.ERROR);
        Stage stage = (Stage) alert.getDialogPane().getScene().getWindow();
        alert.setTitle("Error en la conexior");
        alert.setHeaderText("ERROR");
        alert.setContentText("No se pude conectar la base de datos."
                + "Comprueba que la ruta, nombre de usuario y contraseña son correctos");
        Optional<ButtonType> result = alert.showAndWait();
        if (result.get() == ButtonType.OK) {
            alert.close();
        } else {
            alert.close();
        }
        e.printStackTrace();
    }
    System.out.println("Base de datos conectada");
    return conexion;
}
```

Ilustración 18: Método para conectar la base de datos.

Para el intercambio de información con la base de datos hemos utilizado objetos de transferencia de datos, hemos creado dos clases MedidasOTD y RequisitosODT que crearan dichos objetos. Además, las clases DAO (Data Access Object) u Objetos de acceso a datos llamadas en nuestro proyecto MedidasOAD y RequisitosOAD contienen los métodos que se encargaran de realizar las consultas necesarias para extraer los datos de las bases de datos. A continuación, un ejemplo de un método que carga las medidas en el sistema:

```
public static HashMap<Integer,MedidaOTD> cargarMedidas(){
    HashMap<Integer,MedidaOTD> Medidas = new HashMap<Integer,MedidaOTD>();

    try {
        Connection conexion = DriverBD.conectar();
        String consulta="SELECT * FROM `medidas`";
        PreparedStatement sql = conexion.prepareStatement(consulta);
        ResultSet rs =sql.executeQuery();
        while(rs.next()){
            MedidaOTD pre = new MedidaOTD(
                    rs.getInt(1),
                    rs.getString(2).trim(),
                    rs.getString(3)
                    );
            Medidas.put(rs.getInt(1), pre);
        }
        System.out.println(Medidas);
        return Medidas;

    } catch (SQLException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
    }

    return null;
}
```

Ilustración 19: Método para cargar las medidas en la aplicación.

Como se observa en la ilustración el método utiliza el driver mencionado anteriormente para conectar con la base de datos, una vez conectado realiza la consulta en la base de datos utilizando una cadena de texto que contiene una sentencia SQL. Una vez la base de datos ejecuta la consulta devuelve los datos en un objeto de tipo ResultSet que el método lee y guarda los datos en un HashMap, se han elegido tablas hash para el almacenamiento de datos porque todas las medidas tienen un identificador único que se utiliza como clave, lo que facilita el acceso a los datos una vez ya cargados en la aplicación haciéndolo más rápido y eficiente.

5.5 Pruebas

Una vez terminada la fase de implementación de la funcionalidad se han realizado una serie de pruebas para comprobar que la aplicación cumple con los requisitos básicos y que su funcionalidad es correcta. Las pruebas llevadas a cabo han sido las siguientes:

- Arranque de la aplicación
- Comenzar nueva auditoria
    - Rellenar los datos iniciales del sistema
    - Realizar una auditoria simulada rellenando los campos de la ficha
    - Guardar auditoria
    - Rellenar los datos restantes
    - Generar informe en PDF y comprobar que corresponde con lo auditado.
- Continuar auditoria
    - Abrir una auditoria guardada previamente
    - Realizar cambios en los datos iniciales
    - Realizar cambios en los campos de la ficha
    - Guardar auditoria
    - Rellenar los datos restantes
    - Generar informe en PDF y comprobar que corresponde con lo auditado
- Ajustes
    - Introducir ruta de una base de datos creada y comprobar que conecta
    - Introducir datos erróneos y comprobar que no conecta

En todos los casos el resultado de las pruebas fue satisfactorio cumpliendo con lo mínimo exigido por los requisitos. Durante esta fase se han descubierto errores menores que se trataran de solucionar cuando se introduzcan mejoras en un futuro.

5.6 Futuras mejoras

Las mejoras pensadas para un futuro van orientadas al estilo y el tratamiento de errores, ya que la aplicación actualmente se puede considerar como un prototipo y en el caso de comercializarse sería conveniente mejorar ciertos aspectos para hacerla más atractiva a los usuarios y corregir algunos errores menores detectados en la fase de pruebas.

Para mejorar el aspecto visual de la aplicación podemos añadir un CSS a la interfaz que añada el estilo deseado a los elementos. Se pueden modificar los colores y las formas de

los botones e incluso añadirle iconos para que la aplicación se vuelva más intuitiva para el usuario. También se debería de mejorar la adaptabilidad a tabletas y móviles para que los usuarios que lo deseen puedan ejecutarla en sus dispositivos portátiles de una forma óptima.

Para solucionar los errores menores detectados en la fase de pruebas se deberá de añadir filtros en los campos de introducción de texto con alertas que indiquen al usuario si hay algún error en los datos que ha introducido y así guiarlo mejor en el uso correcto de la aplicación evitando errores en el informe final.

6. Conclusiones

Con este trabajo se ha conseguido elaborar una recopilación de normas que una infraestructura hospitalaria debería cumplir para adecuarse al Esquema Nacional de Seguridad, proporcionando un soporte en forma de aplicación de escritorio capaz de ayudar a los auditores a realizar mejor su trabajo.

Si queremos aprovechar al máximo los enormes beneficios que la tecnología aporta a la sociedad, más concretamente en el campo de la salud, debemos poner en marcha todas las medidas de prevención y protección necesarias para que dichas ventajas no nos provoquen problemas a corto y largo plazo. La actualización de los sistemas y de los métodos de seguridad debe de ser una prioridad, especialmente en un ámbito hospitalario, pues de su eficiencia depende la salud y la garantía de los derechos de las personas.

A su vez la legislación debe de evolucionar al mismo tiempo que lo hace la tecnología proporcionando un contexto jurídico actualizado y que prevenga cualquier tipo de perjuicio a la sociedad. La administración pública deberá proporcionar los medios y guías necesarios para que, tanto el personal que aplique las normas como el que verifica su correcto funcionamiento, puedan llevar a cabo su trabajo satisfactoriamente, pues de ellos depende la seguridad de la población.

A partir de este trabajo se debería de valorar la propuesta de otros que profundicen más en este tema. Uno de ellos debería de investigar las formas de aplicar la normativa recopilada en un hospital real, para poder valorar distintas formas de aplicar la normativa y evaluar que forma se adapta mejor o consigue mejores resultados. También debería de proponerse que, cogiendo la idea de la aplicación explicada en este trabajo, la mejore y la haga totalmente funcional y lista para ser utilizada por los

auditores, incluyendo las mejoras descritas anteriormente y otras que surjan con el fin de adaptarla al contexto jurídico de ese momento.

Para finalizar, y como valoración personal me gustaría resaltar que la recopilación de la información ha ocupado la mayor parte del proyecto, pues había que leer las normas completa o parcialmente para poderlas resumir e incluir en el trabajo. Algunas de ellas después de realizar el análisis, cambiaron o fueron sustituidas, lo que provocaba el hecho de tener que estar actualizado en materia normativa en todo momento. En cuanto a la idea de la aplicación la tuve en mente desde que mi tutor me dio las directrices del proyecto, pero lo difícil fue buscar diferentes formas de plasmarla y elegir, para mí, la más adecuada. Para mi este proyecto me ha producido una gran satisfacción personal y una gran forma de terminar mis estudios de grado.

7. Bibliografía

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Directrices para la elaboración de contratos entre responsables y encargados del tratamiento. [Consulta 25 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. El delegado de protección de datos en las administraciones públicas. [Consulta 27 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. El impacto del reglamento general de protección de datos sobre la actividad de las administraciones públicas [Consulta 26 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Impacto_RGPD_en_AAPP.pdf

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. El Reglamento de protección de datos en 12 preguntas. [Consulta 25 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Guía del reglamento general de protección de datos para responsables del tratamiento. [Consulta 26 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/guia_rgpd.pdf

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Guía para el cumplimiento del deber de informar. [Consulta 25 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Implicaciones prácticas del Reglamento General de Protección de Datos para entidades en el periodo de transición. [Consulta 25 mayo 2017] Disponible en: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_06_29_03-ides-idphp.php

AGENCIA ESPAÑOLA DE PROTECCION DE DATOS. Orientaciones y garantías en los procesos de anonimización de datos personales. [Consulta 25 mayo 2017] Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. *Informática sanitaria. Imagen digital y comunicación en medicina (DICOM) incluyendo el flujo de trabajo y la gestión de datos.*, UNE-EN ISO 12052, 2011.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. *Informática sanitaria. Modelo funcional de un sistema de historia clínica electrónica.*, UNE-EN ISO 10781, 2015.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. *Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos.*, UNE-ISO/IEC 27001, 2017.

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. *Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.*, UNE-ISO/IEC 27002, 2017.

CENTRO CRIPTOLÓGICO NACIONAL. CCN-STIC-802 Auditoría del ENS. [Consultado 24 enero 2017] Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/502-ccn-stic-802-auditoria-del-ens/file.html

CENTRO CRIPTOLÓGICO NACIONAL. CCN-STIC-804 ENS. Guía de implantación. [Consultado 24 enero 2017] Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/505-ccn-stic-804-medidas-de-implantancion-del-ens/file.html

CENTRO CRIPTOLÓGICO NACIONAL. CCN-STIC-808 Verificación del cumplimiento de las medidas en el ENS [Consultado 5 febrero 2017] Disponible en: https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/518-ccn-stic-808-verificacion-del-cumplimiento-de-las-medidas-en-el-ens-borrador/file.html

COMUNIDAD VALENCIANA. Ley 10/2014, de 29 de diciembre, de la Generalitat, de Salut de la Comunitat Valenciana. *Diari oficial de la Comunitat Valenciana*, de 29 de diciembre de 2014, núm. 7434, pp. 32201-32242.

ESPAÑA. Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. *Boletín oficial del Estado*, de 15 de noviembre de 2002, núm. 274 pp. 40126-40132.

ESPAÑA. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín oficial del Estado*, de 14 de diciembre de 1999, núm. 298, pp. 43088-43099.

ESPAÑA. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. *Boletín oficial del Estado*, de 29 de enero de 2010, núm. 25, pp. 8089-8138.

NOTICIAS JURÍDICAS. 2016. Contenido y novedades del Reglamento general de protección de datos de la UE (Reglamento UE 2016/679, de 27 de abril de 2016). [Consulta 25 mayo 2017] Disponible en: http://noticias.juridicas.com/actualidad/noticias/11050-contenido-y-novedades-del-reglamento-general-de-proteccion-de-datos-de-la-ue-reglamento-ue-2016-679-de-27-de-abril-de-2016/

PRIETO, Natividad et al. *Empezar a programar usando Java*. Valencia: Universidad Politécnica de Valencia. 2012. ISBN 978-84-8363-903-0

UNIÓN EUROPEA. Directiva 2011/24/UE del parlamento europeo y del consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. *Diario oficial de la Unión Europea,* de 4 de abril de 2011, núm. L 88, pp. 45-65.

UNIÓN EUROPEA. Directiva 95/46/CE del parlamento europeo y del consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. *Diario oficial de la Unión Europea*, de 23 de noviembre de 1995, núm. L 281, pp. 31-50.

UNIÓN EUROPEA. Recomendación 2008/594/CE de la comisión, de 2 de julio de 2008, sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos. *Diario oficial de la Unión Europea*, de 18 de julio de 2008, núm. L 190, pp. 37-43.

UNIÓN EUROPEA. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario oficial de la Unión Europea*, de 4 de mayo de 2016, núm. L 119, pp. 89-131.

UNIÓN EUROPEA. Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE. *Diario oficial de la Unión Europea*, de 28 de agosto de 2014, núm. L 257, pp. 73-114.

Anexo I

Ejemplo reducido del formato de una auditoria guardada mediante un archivo XML.

<auditoria>

<informe>

<org.1>

<audito>true</audito>

<aplica>true</aplica>

<documento>false</documento>

<muestreo>false</muestreo>

<comentario>correcto</comentario>

</org.1>

/*Repetido para cada medida de seguridad*/

<mp.s.9>

<audito>false</audito>

<aplica>false</aplica>

<documento>false</documento>

<muestreo>false</muestreo>

<comentario></comentario>

</mp.s.9>

</informe>

<datos>

<ajefe>Luis Martinez</ajefe>

<rseg>Pepe Arango</rseg>

<rsis>Javier Pérez</rsis>

<tipo>Ordinaria</tipo>

<sistema>Sistema informatico de atención a pacientes</sistema>

<propietario>Hospital la Fe de Valencia</propietario>

<idioma>Español</idioma>

<resumen></resumen>

<metodologia></metodologia>

<legislacion></legislacion>

<entrevistados></entrevistados>

<fechaf>20 6 2017</fechaf>

<fechai>20 6 2017</fechai>

<auditores></auditores>

<expertos></expertos>

<localidad>Valencia</localidad>

<rys></rys>

<categoria>Alta</categoria>

</datos>

</auditoria>

Anexo II

Código de los métodos de la clase Informe:

Método genInforme:

```
public static HashMap<String,Respuesta> genInforme(){
    int i=1;
    while(i<=medidas.size()){
    informe.put(medidas.get(i).getId(),new Respuesta(medidas.get(i).getId()));
        i++;
    }
    return informe;
}
```

Ilustración 20: Código del método genInforme.

Método guardarArchivo:

```
public static void guardarArchivo(HashMap<String,Respuesta> informe,HashMap<Integer, MedidaOTD> medidas){

    JFileChooser jF1= new JFileChooser();
    String ruta = "";
    if(jF1.showSaveDialog(null)==JFileChooser.APPROVE_OPTION){
    ruta = jF1.getSelectedFile().getAbsolutePath()+".xml"; }
    PrintWriter pw;
    try {
        pw = new PrintWriter(new File(ruta));

    int i=1;
    pw.println("<auditoria>");
    pw.println("<informe>");
    while(i<=informe.size()){
        System.out.println(medidas.get(i).getId()+">");
        pw.println("<"+informe.get(medidas.get(i).getId()).getMedida().trim()+">");
        pw.println("<audito>"+informe.get(medidas.get(i).getId()).isAudito()+"</audito>");
        pw.println("<aplica>"+informe.get(medidas.get(i).getId()).isAplica()+"</aplica>");
        pw.println("<documento>"+informe.get(medidas.get(i).getId()).isDocumento()+"</documento>");
        pw.println("<muestreo>"+informe.get(medidas.get(i).getId()).isMuestreo()+"</muestreo>");
        pw.println("<comentario>"+informe.get(medidas.get(i).getId()).getComentario()+"</comentario>");
        pw.println("</"+informe.get(medidas.get(i).getId()).getMedida().trim()+">");
        i++;
    }
    pw.println("</informe>");
    pw.println("<datos>");
    pw.println("<ajefe>"+Datos.getAuditorjefe()+"</ajefe>");
    pw.println("<rseg>"+Datos.getResponsableSeguridad()+"</rseg>");
    pw.println("<rsis>"+Datos.getResponsableSistema()+"</rsis>");
    pw.println("<tipo>"+Datos.getTipo()+"</tipo>");
    pw.println("<sistema>"+Datos.getSistema()+"</sistema>");
    pw.println("<propietario>"+Datos.getPropietario()+"</propietario>");
    pw.println("<idioma>"+Datos.getIdioma()+"</idioma>");
    pw.println("<resumen>"+Datos.getResumen()+"</resumen>");
    pw.println("<metodologia>"+Datos.getMetodologia()+"</metodologia>");
    pw.println("<legislacion>"+Datos.getLegislacion()+"</legislacion>");
    pw.println("<entrevistados>"+Datos.getEntrevistados()+"</entrevistados>");
    pw.println("<fechaf>"+Datos.getFechafin()+"</fechaf>");
    pw.println("<fechai>"+Datos.getFechaini()+"</fechai>");
    pw.println("<auditores>"+Datos.getAuditores()+"</auditores>");
    pw.println("<expertos>"+Datos.getExpertos()+"</expertos>");
    pw.println("<localidad>"+Datos.getLocalidad()+"</localidad>");
    pw.println("<rys>"+Datos.getRys()+"</rys>");
    pw.println("<categoria>"+Datos.getCategoria()+"</categoria>");
    pw.println("</datos>");
    pw.println("</auditoria>");
    pw.close();

    } catch (FileNotFoundException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
    }
}
```

Ilustración 21: Código del método guardarArchivo.

Método abrir:

```
public static HashMap<String,Respuesta> abrir()  {

    JFileChooser jF1= new JFileChooser();
    String ruta = "";
    if(jF1.showOpenDialog(null)==JFileChooser.APPROVE_OPTION){
    ruta = jF1.getSelectedFile().getAbsolutePath();}
    HashMap<String,Respuesta> inf = new HashMap<String,Respuesta>();
     try {
        Scanner s = new Scanner(new File(ruta));
        String info=s.nextLine();
        info=s.nextLine();
        while(s.hasNextLine()){
            String id=s.nextLine().replaceAll("<", "").replaceAll(">","").trim();
            System.out.println(id);
            if(id.equals("/informe")) break;
            boolean audito = false;
            String a =s.nextLine().replaceAll("<audito>", "").replaceAll("</audito>", "").trim();
            if(a.equals("true")) audito=true;
            System.out.println(audito);
            boolean aplico = false;
            String ap =s.nextLine().replaceAll("<aplica>", "").replaceAll("</aplica>", "").trim();
            if(ap.equals("true")) aplico=true;
            System.out.println(aplico);
            boolean documento = false;
            String d =s.nextLine().replaceAll("<documento>", "").replaceAll("</documento>", "").trim();
            if(d.equals("true")) documento=true;
            System.out.println(documento);
            boolean muestreo = false;
            String m =s.nextLine().replaceAll("<muestreo>", "").replaceAll("</muestreo>", "").trim();
            if(m.equals("true")) muestreo=true;
            System.out.println(muestreo);
            String comentario=s.nextLine().replaceAll("<comentario>", "").replaceAll("</comentario>", "");
            System.out.println(comentario);
            Respuesta r = new Respuesta(id, audito, aplico, documento, muestreo, comentario);
            System.out.println(r.getComentario());
            inf.put(id,r);
            System.out.println(inf.get(id).toString());
            id=s.nextLine();
        }
        Datos.setAuditorjefe(s.nextLine().replaceAll("<ajefe>", "").replaceAll("</ajefe>",""));
        Datos.setAuditorjefe(s.nextLine().replaceAll("<ajefe>", "").replaceAll("</ajefe>",""));
        Datos.setResponsableSeguridad(s.nextLine().replaceAll("<rseg>", "").replaceAll("</rseg>",""));
        Datos.setResponsableSistema(s.nextLine().replaceAll("<rsis>", "").replaceAll("</rsis>",""));
        Datos.setTipo(s.nextLine().replaceAll("<tipo>", "").replaceAll("</tipo>",""));
        Datos.setSistema(s.nextLine().replaceAll("<sistema>", "").replaceAll("</sistema>",""));
        Datos.setPropietario(s.nextLine().replaceAll("<propietario>", "").replaceAll("</propietario>",""));
        Datos.setIdioma(s.nextLine().replaceAll("<idioma>", "").replaceAll("</idioma>",""));
        Datos.setResumen(s.nextLine().replaceAll("<resumen>", "").replaceAll("</resumen>",""));
        Datos.setMetodologia(s.nextLine().replaceAll("<metodologia>", "").replaceAll("</metodologia>",""));
        Datos.setLegislacion(s.nextLine().replaceAll("<legislacion>", "").replaceAll("</legislacion>",""));
        Datos.setEntrevistados(s.nextLine().replaceAll("<entrevistados>", "").replaceAll("</entrevistados>",""));
        Datos.setFechafin(s.nextLine().replaceAll("<fechaf>", "").replaceAll("</fechaf>",""));
        Datos.setFechaini(s.nextLine().replaceAll("<fechai>", "").replaceAll("</fechai>",""));
        Datos.setAuditores(s.nextLine().replaceAll("<auditores>", "").replaceAll("</auditores>",""));
        Datos.setExpertos(s.nextLine().replaceAll("<expertos>", "").replaceAll("</expertos>",""));
        Datos.setLocalidad(s.nextLine().replaceAll("<localidad>", "").replaceAll("</localidad>",""));
        Datos.setRys(s.nextLine().replaceAll("<rys>", "").replaceAll("</rys>",""));
        Datos.setCategoria(s.nextLine().replaceAll("<categoria>", "").replaceAll("</categoria>",""));
        s.close();


    } catch (FileNotFoundException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();

    }return inf;


}
```

Ilustración 22: Código del método abrir.

Método grado:

```
public static double grado(HashMap<String,Respuesta> informe){

    int i=1;
    int x=0;
    double grado;

    while(i<=medidas.size()){

        boolean a =informe.get(medidas.get(i).getId()).isAudito();

        System.out.println(a);
        boolean b =informe.get(medidas.get(i).getId()).isAplica();

        System.out.println(b);
        if(a && b) x++;
        System.out.println(x);
        i++;
    }
    grado= (x*100)/medidas.size();
    System.out.println(medidas.size());
    System.out.println(grado);
    return grado;

    }
```

Ilustración 23: Código del método grado.

Método cumplimiento:

```
public static String cumplimiento(HashMap<String,Respuesta> informe){
    String c = "NULO";
    double grado = grado(informe);
    System.out.println(grado);
    if(grado==100) c ="COMPLETO";
    else if(grado >= 50)    c="ALTO";
    else if(grado>0) c="BAJO";
    return c;



}
```

Ilustración 24: Código del método cumplimiento.