Propuesta de un modelo de preservación digital para pequeñas y medianas instituciones sanitarias

Juan-José Boté Vericad

UNIVERSITAT DE BARCELONA

Doctorado en Sociedad e Información del Conocimiento

TESIS DOCTORAL

PROPUESTA DE UN MODELO DE PRESERVACIÓN DIGITAL PARA PEQUEÑAS Y MEDIANAS INSTITUCIONES SANITARIAS

Autor: Juan-José Boté Vericad

Director: Dr. Miquel Térmens Graells

Barcelona, 2012

A Christine

A Daniel

A Sara

„Wenn a für Erfolg steht, gilt die Formel a = x + y + z, x ist Arbeit, y ist Muße und z heißt Mundhalten…“

Albert Einstein

Resumen

La preservación digital es una disciplina emergente en la gestión de archivos. El presente trabajo de tesis propone el diseño de un modelo de preservación digital aplicable a una institución sanitaria. En el caso que nos ocupa, la conceptualización de dicho modelo está orientada a una organización que preserve historias clínicas electrónicas, escenario en el cual no existe un modelo. Su diseño está fundamentado en una modificación y adaptación del modelo Open Archival Information Systems (OAIS), ampliamente extendido en bibliotecas nacionales e instituciones internacionales.

A través de todo el proyecto de investigación se describe cómo se realiza el diseño conceptual mediante la articulación de procesos de auditorías reconocidas de seguridad informática, análisis de la preservación digital y análisis de riesgos en el contexto instituciones sanitarias.

El resultado del trabajo es un modelo conceptual que permite su aplicación directa en problemas relacionados con la gestión de archivos digitales en instituciones de custodia con escasez de medios, en un escenario realista.

Índice

Capítulo 1

INTRODUCCIÓN

1. Introducción

1.1 Presentación

La preservación digital forma parte de los procesos de conservación digital de aquellas entidades que custodian datos a largo plazo, adquiridos o depositados en ella, uniendo para ello técnicas y destrezas del campo de las ciencias de la información y de la informática. El objetivo de una organización que custodia datos es hacer que su material digital sea accesible informacionalmente en el tiempo gracias a la preservación digital. Este material digital disponible puede ser creado digitalmente desde su origen o generado a partir de material analógico. Obviamente, la preservación digital tiene un alto componente técnico. Ejemplos de unidades de información que requieran preservar material digital pueden ser el archivo de un ayuntamiento o de un hospital, una biblioteca, un museo o cualquier otra entidad que tenga la responsabilidad u obligación legal de custodiar datos digitales.

La preservación digital no sólo tiene implicaciones en las ciencias de la información sino que también las tiene de tipo social (Adam, 2010), histórico[1] (Hampshire y Johnson, 2009), económico (Walters y Skinner, 2010) y tecnológico.

Por lo que respecta a las implicaciones sociales, la preservación digital permite al conjunto de la población poder acceder a una documentación digital custodiada y que esté en condiciones de ser difundida públicamente. En un futuro, gracias a la preservación digital, se podrá consultar información de diferentes ámbitos como música electrónica, documentales de descubrimientos

[1] Por histórico se entiende el hecho de conservar a lo largo del tiempo, no en un período

arqueológicos o científicos, selecciones de lecturas en bibliotecas digitales o realizar visitas virtuales a exposiciones de museos.

Aún así, no todas las instituciones obligadas a conservar su información digital en el tiempo están en condiciones de liberar públicamente dicha información. Existen obligaciones de tipo legal, como la protección de datos personales o normativas de derechos de autor, que provocan que la información conservada digitalmente no sea accesible por el público en general. Aún siéndolo, puede estar limitada a un grupo reducido de población, por cuestiones de tipo científico o legal, como es el caso de los datos de este estudio.

De esta forma, por ejemplo, podría ser posible que se tuviera acceso a una determinada exposición virtual de pintura de un pintor aún desconocido, pero no tener acceso a una exposición de un pintor reconocido. Este ejemplo, trasladado a campos como el de la sanidad, ámbito de este estudio, podría revertir en la imposibilidad de investigar una determinada patología de un proceso asistencial mediante una estadística por cuestiones vinculadas a la protección de datos de carácter personal o a derechos de propiedad intelectual. En esta tesis se plantea la utilización de un modelo de preservación digital para la gestión de este tipo de situaciones, clasificando los derechos de uso de los datos gestionados mediante el modelo propuesto.

Por otra parte, las implicaciones de tipo histórico afectan a la herencia cultural, ya que, sin información digital que se custodie, no hay herencia ni cultura, pero sin tecnología que permita la preservación o recuperación de dicha información, tampoco. Si la información digital que se ha generado en los últimos años no se empieza a conservar digitalmente cuanto antes, es posible que se produzca un lapsus temporal en la historia donde no haya datos que analizar, comparar, explotar o investigar. En este sentido, esta tesis propone un

proceso a seguir para asegurar la continuidad de la preservación a lo largo del tiempo.

Asimismo y respecto a las implicaciones económicas, uno de los factores sobre los que se está investigando actualmente es la sostenibilidad financiera de la preservación digital y los diferentes modelos de costes de la misma (Oltmans, 2004). Un aspecto de interés es la consideración del coste de la pérdida de información, puesto que es muy elevado, a pesar de que precisar el valor de la pérdida es muy difícil, al depender éste del tipo de datos involucrados (BTRF, 2010). En cualquier caso, la pérdida de información digital en una unidad de custodia de información digital resulta difícil de amortizar. En muchas ocasiones, la regeneración de la información es imposible, especialmente si se trata de una entidad que conserva datos digitales antiguos, como por ejemplo, una unidad de custodia de información sanitaria que extravíe accidentalmente radiografías digitales o bases de datos con patologías específicas. No obstante, también hay otras implicaciones económicas que no están tan claras, como puede ser el coste de la conservación digital, que para cada organización dependerá de las actividades críticas que se hayan analizado y de su modelo de conservación (Kejser, Nielsen y Thirifays, 2009). En el modelo propuesto en esta tesis se han analizado algunos elementos referidos a la sostenibilidad económica incluyéndolos en el análisis de riesgos.

Finalmente, en el caso de las implicaciones tecnológicas, éstas tienen un impacto elevado en la preservación digital, afectando tanto a los diferentes procesos como al modelo de preservación de datos en una unidad de información. En una institución que realice procesos de preservación digital, si no se dispone de la tecnología adecuada que permita dar soporte a la conservación de datos, no se podrán ejecutar dichos procesos de preservación. En cualquier caso, no hay un modelo tecnológico establecido generalmente

aceptado, aunque sí se han creado estándares y criterios prácticos (LeFurgy, 2009). En el modelo descrito en esta tesis este aspecto se aborda mediante un mapeo entre diversas soluciones tecnológicas y las necesidades de las entidades sanitarias.

Estos lazos entre los aspectos sociales, históricos, económicos y tecnológicos hacen que la preservación digital haya sido reconocida recientemente como un campo importante de investigación, dentro de las ciencias de la información y de la informática, debido a las implicaciones informacionales y tecnológicas que existen. En el caso particular de los entornos sanitarios, existe un vacío que esta tesis pretende ayudar a cubrir.

1.2 Justificación e interés de la investigación

Son diversas las razones por las que una institución conserva una colección de objetos digitales. Razones, por ejemplo, de tipo legal; de legado histórico, incluso legado sentimental -si lo que se pretende conservar son documentos digitales personales (John, 2009)-; de investigación o memoria histórica además de aquellas que recuperan sitios web (Llueca, 2006). El objetivo final es que la información no se corrompa y sea accesible informacionalmente a lo largo del tiempo. En el caso de la sanidad, uno de los pilares de nuestra sociedad del bienestar, los datos que disponen las entidades sanitarias son digitales, en su mayoría, y cada vez más complejos. Por tanto, se requiere su gestión a fin de disponer de dichos datos preservados adecuadamente en un futuro.

Este trabajo de investigación se centra en las instituciones sanitarias que necesitan gestionar su propio archivo digital, sin necesidad de recurrir a un archivo público externo para su custodia. Esta gestión directa del archivo se justifica por los requisitos que obligan a que los datos clínicos o de

investigación sólo estén en poder de la misma institución que los ha creado. Estos requisitos son de tipo legal (como la protección de datos personales), de tipo contractual y de confidencialidad.

En el caso de la sanidad, existe un alto riesgo de pérdida de información, con el peligro que supone, para esta área de conocimiento a nivel de investigación, la pérdida de datos o la no conservación de registros clínicos. Uno de los aspectos primordiales en la preservación digital es la sostenibilidad financiera que supondrá mantener una infraestructura de este tipo, ya que ésta recae en los mismos hospitales que han generado esa información (Corn, 2009). La importancia de esta afirmación queda reflejada en las actuales propuestas al respecto. En abril de 2011 se realizó el primer Workshop on Long-term Preservation & Management of Electronic Health Record[2], donde se debatieron las problemáticas existentes alrededor de las historias clínicas electrónicas en términos de retos tecnológicos, desarrollo, estándares y estrategias a emplear como modelos (Stead, 2011).

Aquellas instituciones que actualmente realizan propuestas de preservación digital emplean sistemas grandes y dispendiosos. La gran mayoría de ellas aplica el modelo Open Archival Information System (OAIS) (CCSDS, 2002) para la conservación de sus datos digitales. Un aspecto relevante de esta investigación ha sido estudiar si el modelo actual de referencia OAIS es adaptable a cualquier institución en una forma simplificada. Desde la propia comunidad científica se ha planteado esta necesidad, es decir, la disposición de documentación complementaria para pequeñas instituciones bajo el nombre de OAIS-LITE (Allinson, 2006). También, en la revisión quinquenal del modelo OAIS, se recomienda una guía de implementación para gestores con listas de comprobación detalladas cuyo nombre sea OAIS-LITE (Higgins y Semple,

[2] http://ddpehr.nist.gov/home.php [consulta: 8 de marzo de 2012]

2006). Estas cuestiones son indicativas de la existencia de un vacío al respecto de la adaptación de este modelo, en entornos específicos, como, por ejemplo, el sanitario, objeto de estudio de esta tesis.

En una encuesta inicial, realizada a entidades sanitarias catalanas[4], se ha podido constatar que todas ellas cuentan con archivos de historiales médicos. Sin embargo, la realidad es que no están llevando a cabo un plan de preservación digital por cuestiones de diversa índole, como económicas o la ausencia de este objetivo en su plan estratégico. Existe, pues, la necesidad de que estas instituciones dispongan de un sistema de conservación y preservación digital de sus historias clínicas electrónicas y otros documentos electrónicos. Esto es, registros electrónicos de salud, imágenes radiográficas, documentos de investigación y documentos de formación, entre otros.

La aportación principal de esta tesis doctoral es la propuesta de una alternativa, a partir de la adaptación de la recomendación OAIS, mediante la cual una institución puede disponer de archivos digitales, conservados a largo plazo, sin tener que implementar una estrategia financieramente insostenible, ni plantear cambios inasumibles en su estructura. Esto no implica que los cambios sean hipotéticos o que no haya que realizar un proceso de formación del personal que se encargue de la custodia digital de los datos, entre otros.

En este estudio se realiza, por tanto, una exploración cualitativa entre diferentes instituciones sanitarias catalanas, a fin de poder analizar sus infraestructuras. Con los datos obtenidos se ha elaborado un mapa de las necesidades de conservación digital. A partir de esta exploración y de los datos analizados, se realiza una propuesta de preservación digital basada en una reducción del modelo de conservación OAIS. La propuesta de este modelo

[4] Ver Anexo II

permite disponer de un estándar adaptado y, quizás, menos estricto pero igualmente seguro, para organizaciones sanitarias que pretendan disponer de un archivo digital propio, cubriendo el vacío actual causado por la falta de modelos específicos para el entorno sanitario.

1.3 Objetivos de la investigación

El objetivo principal que se persigue en esta tesis es la propuesta de un modelo conceptual de preservación digital para entidades sanitarias.

Este objetivo parte de la convicción de que la gestión y preservación de datos complejos como los provenientes de un escenario sanitario, puede resolverse mediante la adaptación de los estándares de la preservación digital, en especial del modelo de conservación OAIS.

La investigación se ha estructurado a partir de la formulación de las siguientes preguntas:

1. ¿Qué características específicas tienen los datos a preservar en entornos sanitarios?
2. ¿Qué estrategias se están llevando a cabo actualmente para dicha tarea?
3. ¿Qué metodologías son válidas para evaluar una entidad sanitaria con respecto a la preservación digital de las historias clínicas?
4. ¿Qué modelos existen para la preservación digital de datos complejos?
5. ¿Qué elementos del entorno OAIS pueden adaptarse para dar respuesta a la preservación de datos en entidades sanitarias?

1.4 Delimitación del estudio

Este proyecto de tesis se circunscribe a aquellas entidades sanitarias privadas o concertadas en Catalunya, que participen en las auditorías previas de seguridad informática, auditoría de la preservación digital y análisis de riesgos diseñada con el objetivo de responder a la tercera pregunta de investigación.

Se entiende por entidad de gestión sanitaria una empresa titular de un hospital o responsable de varios hospitales, coordinando su gestión. Este tipo de entidad se caracteriza por dos cuestiones: la custodia de datos personales y el gran volumen de información manejada, en especial, historias clínicas electrónicas. La custodia de historias clínicas electrónicas por parte de las organizaciones sanitarias implica disponer de una gran cantidad de datos personales, con los retos que ello conlleva en seguridad e integridad de la información.

Para poder llevar a cabo el estudio, se han establecido acuerdos con una serie de entidades seleccionadas de entre todas las entidades de gestión de salud de Catalunya concertadas y privadas. La razón de ello es que muchas de las entidades que gestionan hospitales en Catalunya son entidades privadas que facilitan, mediante convenio de concertación, servicios a la red pública de sanidad. Por tanto, están obligadas a disponer de sus propios archivos, así como de su conservación. Además, en estas entidades, al ser privadas, no está claro que sus historiales médicos electrónicos, con el paso del tiempo, lleguen a formar parte de una biblioteca o archivo público, como es el caso de hospitales de titularidad pública. A este respecto, cuando se ha contactado con entidades sanitarias públicas (en Catalunya hay 8), o bien no han contestado o aquellas que lo han hecho han indicado que no estaban interesadas en el proyecto. Actualmente, la única entidad sanitaria catalana que deposita sus archivos en la

Biblioteca de Catalunya es el Archivo del Hospital de la Santa Creu y Sant Pau[6] (mediante un convenio de colaboración[7] desde el año 2006).

La selección de las entidades ha atendido a diferentes criterios: su situación actual respecto de la gestión de las historias clínicas, su voluntad de participar en el proyecto de investigación, y su representatividad estadística[8].

1.5 Metodología

Así pues, la ejecución del proyecto de tesis se ha basado en cinco bloques metodológicos diferenciados:

a) Revisión de la bibliografía y establecimiento de los marcos jurídicos, normativos y teóricos dando así respuesta a las preguntas primera y cuarta de investigación.

b) Selección de las entidades sanitarias a fin de analizarlas en los aspectos técnico y organizativo facilitando la respuesta a la segunda pregunta de investigación.

c) Adaptación de las metodologías de auditoría existentes al entorno sanitario, obteniendo la información necesaria para responder a la tercera pregunta de investigación.

d) Obtención de datos sobre la gestión de la seguridad de los datos digitales mediante herramientas cualitativas dando respuesta a la segunda pregunta de investigación.

[6] http://www.santpau.cat/patr_fitxa.asp [consulta: 7 marzo de 2012]
[7] http://www.bnc.cat/catalegs/fonsHSC/inici.php [consulta: 7 marzo de 2012]
[8] Cubriendo un 25,49% de los encuestados.

e) Diseño del modelo de conservación digital conceptualmente teórico y su propuesta final, tal y como se describe en el Capítulo 7. Este diseño nos permite dar respuesta a la quinta pregunta de investigación.

Es necesario aclarar que esta tesis doctoral no se plantea una validación del modelo propuesto mediante su implementación en alguna de las instituciones participantes en el estudio realizado, dado que esto conllevaría unos costes económicos y temporales que ninguna de las entidades participantes puede acometer actualmente, quedando por lo tanto, como una posible línea futura de trabajo en este campo.

1.5.1 Revisión bibliográfica y establecimiento de los marcos jurídicos, normativos y teóricos

Se ha realizado un vaciado de la bibliografía existente, así como de las normas jurídicas y técnicas. Los Capítulos 2, 3, 4 y 5 son un reflejo del estado de la cuestión existente en este aspecto. A este respecto, en la revisión bibliográfica se han enfatizado los puntos siguientes:

a) Revisión de la literatura en documentación médica y archivos.

b) Revisión de la legislación europea y española vigente respecto de las historias clínicas, así como legislación española en materia de seguridad, como es el Esquema Nacional de Seguridad (ENS).

c) Estudio de la metodología de análisis de la preservación, Trustworthy Repositories Audit Checklist (TRAC).

d) Verificación de las diferentes metodologías reconocidas de análisis de riesgos.

e) Examen de los diferentes modelos de preservación digital. Estos modelos están descritos en el Capítulo 2 y su estudio nos han permitido analizarlos y así poder contestar a la cuarta pregunta de investigación.

1.5.2 Selección de las entidades sanitarias y análisis técnico y organizativo

A fin de disponer de datos para el análisis, se ha procedido a una selección de entidades sanitarias de la forma siguiente:

a) Realización de una investigación preparatoria sobre la existencia de archivos digitales en entidades sanitarias catalanas[9]. El estudio preliminar se ha realizado mediante un cuestionario, enviado en marzo de 2010, con preguntas de elección múltiple, para tratar de conocer la situación actual de las entidades sanitarias y el corpus documental de que disponen.

b) A través del análisis de las respuestas obtenidas en el estudio preliminar se ha seleccionado una serie de entidades de entre todas las que respondieron. A las mismas se les presentó el proyecto y se solicitó su colaboración. Esta fase se realizó mediante entrevistas telefónicas o presenciales. Las razones más frecuentemente esgrimidas para la no participación en el estudio preliminar fueron la no disponibilidad de tiempo debido a prioridades internas de la organización, o bien que el proyecto no interesaba.

c) Una vez obtenida la colaboración de las organizaciones participantes, se procedió al estudio de auditoría de los procedimientos, formatos de objetos digitales e instrumentos de control de que disponen las

[9] Ver Anexo II

entidades sanitarias. Este apartado se realizó mediante la técnica de cuestionario con respuestas de alternativa múltiple así como preguntas de respuesta abierta. La encuesta fue enviada por correo postal junto con otra documentación afín al proyecto, como por ejemplo un compromiso de confidencialidad de los datos obtenidos.

d) Finalmente se realizaron nuevas entrevistas personales con las entidades participantes, con el objetivo de completar los datos obtenidos en las encuestas y lograr datos suficientes sobre sus estructuras técnicas de información, a fin de realizar un análisis de riesgos.

Respecto a la selección final de las entidades, hay que entender que todas las escogidas son entidades privadas concertadas y financiadas por el Departament de Salut de la Generalitat de Catalunya, excepto una entidad, que es totalmente privada. Las entidades, independientemente de su concierto de financiación, tienen que custodiar su información de forma autónoma. Es decir, no sólo deben ocuparse de la creación de sus propias historias clínicas, sino también de custodiarlas.

En este proyecto, tal y como se verá en el Capítulo 7, han participado las siguientes entidades que se enumeran en orden alfabético:

a) Consorci Sanitari del Maresme (CSdM)

b) Consorci Sanitari de Terrassa (CSdT)

c) Corporació Sanitària Maresme i la Selva (CSMiS)

d) Departament d'Obstetrícia, Ginecologia i Reproducció, Institut Dexeus[10]

e) Fundació Pere Mata

f) Grup Sagessa

g) Hospital Sant Joan de Déu

h) Mútua de Terrassa

Estas ocho entidades colaboradoras representan un 15,38% de las entidades privadas o concertadas existentes en Catalunya. Este porcentaje es suficientemente representativo del sector.

El análisis de las instituciones se ha realizado a nivel organizacional y técnico, a fin de detectar sus necesidades en la preservación digital de datos. Más en concreto, se ha llevado a cabo el estudio de aquellos servicios que corresponden a los sistemas de información que gestionan la explotación de las historias clínicas. Las unidades de información que habitualmente gestionan las historias clínicas son el departamento de tecnologías de la información y el archivo médico, siendo este último el servicio que todavía gestiona las historias clínicas analógicas remanentes.

1.5.3 Adaptación de las metodologías existentes al entorno sanitario

Con la finalidad de responder a la tercera pregunta de investigación, en este estudio aborda el análisis de las principales metodologías que pueden ser usadas para analizar una institución. Se han revisado, en un primer estadio, las diferentes metodologías de auditoría de la seguridad, las metodologías de

[10] Única entidad privada participante.

análisis de riesgos, así como aquellas metodologías que son un estándar (o estén en proceso de serlo) en el campo de la preservación digital. La selección final realizada, ha de permitir valorar las instituciones y, en base a los datos obtenidos, poder proponer un sistema de información fiable que facilite la preservación y conservación digital de las historias clínicas a largo plazo. En el caso de este estudio, se trabaja con tres metodologías de diferentes ámbitos, tal y cómo se describe a continuación.

La primera es MAGERIT, una metodología de análisis de riesgos (MAP, 2006). MAGERIT ha sido elaborada por el Consejo Superior de Administración Electrónica y se puede aplicar a través del programa PILAR, como se recoge en el Capítulo 6.

El empleo de MAGERIT así como de otras metodologías de análisis de riesgos se debe a que cumple con los requisitos para poder ser empleada junto con el ENS, que exige que para la realización de un análisis de riesgos en una institución esta ha de estar reconocida internacionamente como el es caso de MAGERIT. Otras metodologías de análisis de riesgos existentes no disponen de un software que ayuden en su aplicación o su documentación no era fácilmente accesible.

La segunda metodología es el Esquema Nacional de Seguridad (España, 2010), a modo de marco de seguridad de obligatorio cumplimiento en entidades que dependen de la Administración Pública española. El Esquema Nacional de Seguridad (ENS) es una metodología que permite evaluar una entidad y que ésta garantice la seguridad de sus sistemas. Se evalúa una organización desde el punto de vista de sus infraestructuras, el personal, la disponibilidad y la seguridad de los sistemas informáticos.

La tercera metodología es Trustworthy Repositories Audit & Certification (TRAC), empleada para el análisis de repositorios o sistemas de información enfocada a la preservación digital (CRL y OCLC, 2007). TRAC es una metodología elaborada y reconocida como norma ISO 16363:2012, fruto del consenso internacional. La metodología TRAC permite evaluar tres aspectos de una organización: la infraestructura de la organización, la gestión de sus objetos digitales y su seguridad.

Aunque el Esquema Nacional de Seguridad y TRAC son diferentes metodologías tanto en las formas como en su orientación, tienen puntos convergentes, como se muestra en el Capítulo 4. Mediante el análisis exhaustivo del Esquema Nacional de Seguridad y TRAC, a través de la combinación de sus respectivos indicadores, se ha podido disponer de un sistema fiable de auditoría siguiendo la metodología propuesta. El uso de ENS y TRAC en un mismo escenario es novedoso por lo que respecta a la literatura existente sobre estudios similares al propuesto.

La razón principal para analizar estas dos metodologías se debe a que el ENS es una normativa jurídica de reciente creación pero es de uso obligatorio para entidades pertenecientes a la administración pública. En este caso los hospitales encuestados tienen vínculos con la administración pública y por tanto obligatoriedad de emplearlo. En el caso de TRAC, si bien existen otras metodologías de análisis de la preservación digital, las alternativas existentes descritas en el Capítulo 4 o bien no cubrían todos los aspectos necesarios en la auditoría de la preservación digital o no gozaban del consenso internacional como es el caso de TRAC que es una norma ISO 16363:2012.

Una vez aplicadas las metodologías de análisis de riesgos y de seguridad, además de la información disponible, en diferentes grados en las entidades

participantes se ha podido conocer el mapa de las necesidades de preservación del sistema sanitario privado catalán. Finalmente, se ha podido elaborar una propuesta de un sistema de preservación digital a largo plazo con los resultados obtenidos en las diferentes metodologías de análisis anteriormente comentadas. Para ello, se han tenido en cuenta las diferentes propuestas de los modelos actuales de conservación digital (Muir, 2001), entre los cuales están el modelo OAIS y el modelo de ciclo de vida de la preservación digital.

El modelo OAIS está elaborado por el CCSDS, entidad vinculada a diferentes agencias espaciales internacionales, como la National Aeronautics and Space Administration (NASA) o la European Space Agency (ESA). El modelo de ciclo de vida de la preservación digital está propuesto por el Digital Curation Centre (DCC)[13]. El modelo OAIS ha sido ampliamente implementado por instituciones como la Biblioteca Británica (Woodyard, 2002), la Biblioteca Nacional de Nueva Zelanda (Knight, 2009) o la NASA (Sawyer, 2005). Actualmente el modelo de referencia de archivos OAIS, reconocido como ISO 14721:2003, permite a cualquier institución planificar la preservación a largo plazo de sus archivos digitales.

La adaptación de los archivos analógicos de pequeñas y medianas instituciones a un modelo de archivo digital implica, para éstas, una inversión en recursos muy elevada (National Archief, 2005). Esto es debido entre otros factores, a los procesos de digitalización, es decir, a la conversión de la información analógica en digital. La decisión de disponer de un archivo digital puede incrementar exponencialmente los costes de mantenimiento por encima de los correspondientes a los archivos analógicos, debido a los procesos de vigilancia tecnológica que hay que implementar y a la fragilidad de la información digital.

[13] http://www.dcc.ac.uk [consulta: 7 enero de 2012]

1.5.4 Obtención de los datos mediante herramientas cualitativas

La obtención de los datos para este estudio se ha realizado en tres fases diferenciadas:

a) Envío de una encuesta preliminar a 204 entidades sanitarias de Catalunya. Se pueden ver los resultados y su explotación en el Anexo II. Esta encuesta preliminar nos ha permitido averiguar las características específicas que tienen los datos a preservar en los entornos sanitarios obteniendo la respuesta a la primera pregunta de investigación. También nos ha permitido saber que estrategias se están llevando a cabo actualmente en Catalunya las entidades sanitarias consiguiendo los datos necesarios a la segunda respuesta de investigación.

b) Una segunda encuesta de auditoría con las 8 entidades que mostraron su interés en colaborar con el proyecto. La encuesta incorporaba parámetros de TRAC y del Esquema Nacional de Seguridad cómo se muestra en el apartado 6.2 del Capítulo 6, con el análisis de los resultados; el cuestionario completo se recoge en el Anexo III. La encuesta de auditoría estaba pensada para su realización en un tiempo máximo de veinticinco minutos si el receptor era la persona adecuada. De hecho, así lo eran todos, ya que eran responsables o bien del archivo médico o bien del departamento de informática. Aún así, los tiempos de retorno han oscilado entre tres días y seis meses, siendo variadas las causas de su retraso.

c) Una entrevista final, a fin de completar los datos para la investigación. Estas entrevistas se realizaron con todas las entidades participantes en la encuesta de auditoría y con las personas vinculadas al proyecto por parte

de las organizaciones. En total participaron dieciséis personas, ocho jefes de archivo y ocho directores de informática.

Los dos cuestionarios, el preliminar y el de auditoría, fueron examinados previamente por directores de informática y gestores de información de diferentes organizaciones, externas a la muestra, con la finalidad de añadir, corregir o eliminar en algunos casos preguntas que fueran superfluas o duplicadas o bien que pudieran no entenderse.

En referencia a la justificación de la recogida de datos, cabe recordar que en un proyecto de auditoría convencional, los datos recogidos pueden ser pruebas empíricas, es decir, demostrables, o bien datos recogidos mediante un test o reuniones de grupo. En el caso de este estudio, los datos fueron recogidos mediante una encuesta preliminar, una encuesta de auditoría, así como una entrevista final, como se muestra en el Capítulo 6. Estas entrevistas finales se realizaron mediante reuniones con los responsables de las unidades de información correspondientes. También se efectuó un contacto telefónico posterior para clarificar ciertos aspectos de la encuesta o de la reunión.

Todo este proceso se ha realizado de la forma más exhaustiva posible dentro de las limitaciones planteadas por las entidades. Los centros de gestión sanitaria participantes no estaban en condiciones de asignar personal al proyecto de investigación a fin de poder comprobar in situ, en sus instalaciones, los diferentes parámetros de sus sistemas de información. Por otro lado, legítimamente, el investigador tampoco podía estar sólo en las instalaciones sin que los responsables del centro supiesen exactamente que hacía, con riesgo para sus propios sistemas de información. Idealmente se tendría que haber revisado toda la configuración de los sistemas informáticos centrales. Aún teniendo permisos sobre la confidencialidad de los datos recolectados, la no pertenencia

a ninguna de las organizaciones ha provocado cierta dificultad en la obtención de los mismos, que aún así se han podido verificar mediante entrevistas.

Por tanto, la recogida de datos con las 8 organizaciones finalmente participantes se basa en un cuestionario de auditoría enviado por correo, postal a tres de las entidades y electrónico al resto. Posteriormente, se han realizado entrevistas finales a todas las personas de todas las entidades contactadas, a fin de completar los datos del estudio. Esto asegura una solidez y coherencia del proceso de recogida de datos.

En el Anexo IV se encuentran reflejados los datos obtenidos conjuntamente en la encuesta de auditoría. También se encuentran en tablas separadas, los datos correspondientes a TRAC y aquellos que pertenecen al Esquema Nacional de Seguridad. Estos datos se muestran de esta forma porque la encuesta de auditoría se envío cruzando los indicadores conjuntamente de TRAC y el Esquema Nacional de Seguridad. En el Capítulo 4 se muestra las semejanzas existentes entre la metodología TRAC y el Esquema Nacional de Seguridad.

1.6 Estructura del trabajo de tesis

El trabajo está estructurado en siete capítulos además del dedicado a las conclusiones, completándose con la bibliografía y los anexos.

Este Capítulo 1 explica la justificación del trabajo de tesis, la hipótesis y preguntas de investigación, así como la metodología empleada.

Los Capítulos 2, 3, 4 y 5 muestran, respectivamente, el estado de la cuestión explicando qué es la preservación digital y cuáles son el marco jurídico, el marco técnico y el modelo de referencia OAIS.

A través de los Capítulos 6 y 7 se describe la propuesta realizada en esta tesis. En el Capítulo 6 se realiza un análisis de las necesidades de preservación digital de las entidades colaboradoras, aplicando el marco teórico empleado en las metodologías del Esquema Nacional de Seguridad, Trustworthy Repositories Audit Criteria, mediante una encuesta de auditoría y el análisis de riesgos. En el Capítulo 7, por medio de dicho análisis, se presenta en forma de propuesta conceptual el modelo de conservación digital en un contexto sanitario.

Finalmente, en el Capítulo 8 se recogen las conclusiones finales, donde se se responde a las preguntas de investigación, se proponen aspectos clave para adoptar el modelo propuesto y, por último, se plantean posibles líneas de investigación para dar continuidad a este trabajo.

Capítulo 2

La preservación digital

2. La preservación digital

2.1 Concepto

Se puede afirmar que la preservación de la información ha existido desde siempre. La transformación de una comunicación a un formato para que este perdure en el tiempo, ha sido una característica antropológica del ser humano. Prueba de ello son, por ejemplo, las pinturas rupestres, que representan costumbres y, por tanto, el legado histórico de la época. Se puede afirmar pues que la preservación de información, del formato existente en cada época de la humanidad, ha existido siempre. Como consecuencia de ello, la preservación digital existe desde que el hombre es capaz de reproducir un elemento analógico en uno digital. Así, es posible convertir el texto de un periódico en un texto digital mediante un escáner. También lo es convertir una foto, una película en Super8 a un formato digital. Sin embargo, al convertir a formato digital una piedra, una montaña, una planta o un cubo perderá alguna de sus principales propiedades como la forma, o la dimensión espacial, a pesar de que ya empiezan a aparecer algunos ensayos sobre estructuras en 3D (Trinchão et al., 2011).

La preservación digital no se circunscribe únicamente a la informática o a las ciencias de la información, sino que abarca otros campos, al influir y afectar a todas las áreas del conocimiento. Se encuentran ejemplos en diversos ámbitos, como las ciencias de la tierra (Narock y Cragin, 2010), la astronomía (Gray y Woan, 2011), las ciencias de la salud (Bote y Termens, 2011), las matemáticas (Latecki, Conrad y Gross, 1998), la arquitectura (Kepczynska-Walczak, 2005), la ingeniería o la conservación de documentos personales (John, 2009). En todos estos campos, como en muchos otros, se hace necesaria una intervención y planificación de la preservación digital.

La preservación digital tiende a ser una disciplina globalizada más que localizada, tal y como queda patente en los múltiples proyectos internacionales e iniciativas que se realizan, disponibles muchos de ellos en páginas web. A modo de ejemplo se pueden citar los proyectos PLANETS[14] y CASPAR[15] y la red alemana NESTOR[16]. También el proyecto ENSURE[17], cuyo objetivo es llevar a la práctica el análisis de costes y su valor frente a diferentes soluciones cualitativas con datos heterogéneos. Este proyecto, en concreto, está orientado hacia entidades de gestión de salud, entidades financieras y ensayos clínicos.

La preservación digital se refiere a las técnicas o procesos, muchos de ellos provenientes conjuntamente del campo de la informática y de las ciencias de la información, que son necesarios para conservar en el tiempo objetos digitales en un sistema de información. Entre otros, se ocupa del almacenamiento de los datos así como de su integridad, para que estos se puedan recuperar en el tiempo, sin estar corruptos. Como resultado del almacenamiento y conservación, se obtiene una copia exacta de la información previamente introducida.

Previo a conocer los procesos existentes en la preservación digital, hay que conocer qué tipo de elementos participan en ella. El capital humano, los objetos a custodiar, los recursos técnicos y los recursos económicos que se dispongan, son algunos de los factores necesarios.

En función de los recursos que una unidad de información destine a esta materia, se podrá disponer de un bibliotecario, un archivero o un documentalista, es decir, personal especializado en gestión de la información,

[14] http://www.planets-project.eu/ [consulta: 8 de marzo de 2012]
[15] http://www.casparpreserves.eu/ [consulta: 8 de marzo de 2012]
[16] http://www.langzeitarchivierung.de/ [consulta: 8 de marzo de 2012]
[17] http://ensure-fp7-plone.fe.up.pt/site [consulta: 8 de marzo de 2012]

junto con personal de soporte, como puede ser un especialista en informática. Los recursos técnicos serán los establecidos sobre la base del presupuesto correspondiente. Los objetos a custodiar son la parte más importante, ya que son la materia prima con la que se va a trabajar. Se pueden distinguir dos tipos de objetos, los analógicos y los digitales, por lo cual es importante diferenciar entre los elementos analógicos y los objetos digitales. Ambos pueden estar presentes en un proceso de preservación digital pero requieren tratamientos diferentes.

Los objetos analógicos son el resultado de una técnica mediante la cual el elemento resultante no puede ser accedido digitalmente. Es posible hacer mención de diversos ejemplos, como un periódico, una partitura de música, una radiografía o una cinta de audio.

Los objetos digitales son la consecuencia de un proceso técnico mediante el cual el producto final es un elemento en formato digital. Ejemplos de objetos digitales pueden ser un documento electrónico creado con un procesador de textos, una pieza de música electrónica o una imagen realizada con una cámara digital.

Tanto los objetos digitales como los analógicos tienen, por ende, una serie de propiedades que hay que analizar en todo proceso de preservación digital: las propiedades significativas. Con el fin de poder aplicar el proceso más adecuado a un objeto, es necesario conocer las propiedades más importantes de éste mediante el soporte de técnicas informáticas, cada vez más imprescindibles en este campo.

Los primeros proyectos digitales documentados se desarrollaron de 1992 a 1997, cuando se empezaron a realizar los principales proyectos de digitalización

de imágenes en masa. Algunos proyectos pioneros fueron CLASS (Cornell University), Proyect Open Book (Yale University) y Making of America (Michigan University y Cornell University) (Seadle, 1997), que sentaron las primeras bases de proyectos de digitalización de fondos para bibliotecas. Hasta esas fechas, se había preservado la información existente en microfilm, pero la transformación de imágenes en un formato procesado por ordenador permitía la reducción de los costes de conservación, así como los de producción. Es por esto que se inició, posteriormente, la conversión de microfilm en bits, ya que este facilitaba tanto la duplicación, como mejor herramienta de conservación sin depender de agentes químicos, como una mejor calidad. Además, el hecho de poder digitalizar microfilms permitía también indexarlos de forma automática, con lo que se facilitaban las búsquedas y la recuperación de información (Conway, 1994).

A principios de la anterior década se empezó a elaborar el modelo OAIS, creado inicialmente para la industria aeroespacial. En sus formas iniciales, este modelo pretendía conservar los datos que se generaban en las exploraciones del espacio. El modelo OAIS se ha convertido en una norma estándar ISO 14723:2003 y ha sido adoptado no sólo por la industria aeroespacial, sino también por bibliotecas y archivos, generando a su alrededor una serie de estándares que han contribuido a mejorar lo que en sus inicios era un archivo de conservación de información sin una metodología definida.

2.1 Definición de preservación digital

Previo a realizar el análisis del concepto de preservación digital, es necesario aclarar dos términos que, a menudo, se encuentran en la literatura con un cierto carácter de sinónimos: la conservación digital y la preservación digital. La conservación digital es la acción de mantener objetos digitales a lo largo del

tiempo mediante su ciclo de vida (Muñoz, 2006). La preservación digital forma parte de los procesos de la conservación digital, incidiendo en metodologías y procesos tecnológicos, a fin de garantizar el acceso informacional a los objetos digitales custodiados.

Existen diversas acepciones y definiciones para la preservación digital, tópico de interés en investigación. A partir de ellas, y sin pretender citar la bibliografía existente al respecto se postula la siguiente definición: la preservación digital supone garantizar que la información digital del pasado y del presente sea accesible informacionalmente en el futuro por cualquier tipo de medio electrónico o analógico.

Con esta definición se pretende poner de manifiesto que para poder disponer de información digital en un futuro, de forma que se pueda entender, procesar y ser accesible informacionalmente, ésta se tiene que asegurar mediante los procesos técnicos, administrativos y de gestión necesarios. Si se aplica esta definición a una entidad de gestión sanitaria, la preservación digital sería el conjunto de técnicas a utilizar para poder conservar los datos que hay en las historias clínicas de los pacientes y que estos sean accesibles mediante algún tipo de dispositivo electrónico.

Si los diversos procesos que existen en la preservación digital se pudiesen medir mediante una ecuación matemática, quizás los procesos serían mucho más simples y elementales. Esto no es así, pero es posible aproximar la preservación digital a una definición que, aunque posiblemente sea inexacta, se acerque al modelo que se busca. Por ello, se introduce una fórmula teórica que pretende definir la preservación digital como el sumatorio del almacenamiento (a), complejidad de los fondos a conservar (θ), los costes derivados (C) multiplicado por la variable tiempo (t)

$$PD = \sum (a + \theta + C) * t$$

Los requisitos de almacenamiento (a) cada vez serán más grandes, ya que aumentan los volúmenes de la información.

La complejidad (θ) de los fondos a conservar dependerá de la unidad de custodia de información y del tipo de datos que se preserven. A modo de ejemplo, la custodia de datos médicos vinculados a historias clínicas, ensayos clínicos o datos de carácter personal es diferente a la custodia de música electrónica. En el caso de los datos médicos, se trata de documentos digitales, altamente complejos internamente, mientras que en el caso de la música electrónica, según la tecnología aplicada, los datos podrían ser menos complejos de custodiar, incidiendo esta menor complejidad en los costes. Asimismo, el tratamiento de la información que contengan los fondos, hará que la preservación sea más o menos compleja en función de las políticas de preservación digital que se apliquen. Hay que añadir, además, los problemas derivados de los derechos de autor y propiedad intelectual, así como aquellos derivados de la protección de datos de carácter personal.

Los costes (C) son un factor de influencia en la preservación digital, por ser una variable incremental a considerar a lo largo del tiempo, ya que a medida que se aceptan más fondos, aumentan también los diferentes costes implicados. Esta ecuación, aunque inexacta, puede ser considerada como una aproximación para el análisis de la viabilidad financiera de la preservación digital.

2.2 Las organizaciones de custodia

Cuando se habla de conservación digital y preservación digital, estos términos fácilmente se relacionan con entidades de conservación de legado histórico o

cultural. Las bibliotecas, los archivos o los museos, entre otros, formarían parte de este tipo de centros, pero también los centros de investigación, los centros de gestión médica, como los hospitales, y las entidades financieras tendrán, en un futuro inmediato, la necesidad o la obligación de preservar datos digitalmente. No se puede obviar que los datos digitales forman parte de su núcleo de negocio y, por tanto, su preservación será un requisito indispensable para su funcionamiento.

Toda organización que trabaje con datos digitales debería plantearse una serie de objetivos en lo referente al tratamiento de la información que procesa. Uno de los primeros propósitos que debería cuestionarse es el correcto funcionamiento de su sistema de información, tanto a nivel de almacenamiento como a nivel de manipulación de los datos. Esto es, la comprobación de la inexistencia de corrupción de la información y la seguridad de que la información que tiene almacenada pueda recuperarse siempre, independientemente del transcurso del tiempo. Ello implica asegurar que no sucedan anomalías de ningún tipo durante la manipulación y gestión de los datos. Una vez el sistema de información de trabajo está asegurado, hay que pensar en la información digital que hay que conservar a lo largo del tiempo, ya sea por motivos legales, estratégicos u organizacionales. En algunas organizaciones, esta información recibe el nombre de archivo digital, de sistema de información pasivo o de repositorio; en cualquier caso, la finalidad es la misma que en el sistema de información activo. Sin embargo, hay un matiz que lo diferencia del sistema de información activo: el archivo digital debe garantizar el acceso a la información a largo plazo.

El empleo del término largo plazo indica un periodo de custodia y conservación, establecido en años, a partir del cual el soporte que permite visualizar la información puede ser obsoleto, tanto a nivel de hardware como a

nivel de software. Este espacio temporal dependerá de la entidad que custodia los datos y de la naturaleza los mismos. En el caso de la sanidad, se considera largo plazo en las historias clínicas a partir de los cinco años de media, una vez finalizado el proceso asistencial de un paciente.

Sobre la información que se conserva en un archivo digital se ha de mantener un control estricto para evitar su corrupción, asegurar su integridad y evitar su posible pérdida. El sistema debe generar confianza y garantizar que los mismos datos que fueron depositados para su preservación digital en el tiempo, sean los mismos datos a los que se accede posteriormente, aunque no sea en las mismas circunstancias. A este tipo de sistemas se les llama archivos digitales de confianza (Trusted Digital Repository o TDR). Los archivos de confianza deben garantizar la inexistencia de corrupción, manipulación o pérdida de la información. Para ello, hay que aplicar, tanto en el archivo como en la unidad tecnológica y organizativa, técnicas y metodologías del ámbito de la preservación digital. En algunos casos, estas metodologías, como el análisis de riesgos o la auditoria del archivo, pueden ser considerados como estándares internacionales en la actualidad. Algunas de estas estrategias han sido aplicadas para la propuesta de un modelo conceptual de conservación digital de entidades de gestión sanitaria que se realiza en este estudio.

2.3 Aceptación de la información

Una organización que custodie datos y los conserve digitalmente puede recibir información para su conservación a largo plazo en diferentes formatos. La información puede estar representada de forma analógica o bien representada en forma de objeto digital. El soporte de representación de la información analógica puede ser información en papel, cintas de audio, video o papel fotográfico, entre otros formatos. Si el material es digital, puede estar

representado como un documento electrónico con texto, con material gráfico o con la combinación de ambos. Además, el material digital puede estar en diferentes tipos de soportes como CD o DVD, tarjetas de memoria o lápices ópticos. Estos soportes requerirán un tratamiento diferente en la unidad de custodia, en función de su naturaleza y forma de almacenamiento. En muchos casos existe una dependencia tanto del software propietario como del hardware, lo cual puede provocar que la información sea imposible de interpretar (Cerf, 2011).

2.4 Recepción de datos analógicos

El material analógico, una vez es aceptado por la institución de custodia, se convierte en digital mediante un proceso de digitalización. Si el material que se recibe es digital, este requiere de un tratamiento diferente, ya que ha sido creado digitalmente desde su origen (UNESCO, 2004). Posteriormente y una vez tratado, formará parte de un sistema que estará integrado en el propio archivo.

2.4.1 La digitalización

Es habitual escuchar el término digitalización en muchos tipos de entornos. En el caso de la preservación digital, la digitalización es la técnica por la cual un objeto analógico, independientemente de su forma, se transforma en digital. El elemento resultante es legible mediante un sistema de computación. Los procedimientos que podrían formar parte del proceso de digitalización son, entre otros, el fotografiado digital, el escaneado de documentos (Wentzel, 2006) o el uso de reconocimiento óptico de caracteres (ROC).

Distintos dispositivos, en muy diferentes formas, permiten la conversión de documentos en papel a formato digital. En este proceso, el objeto de entrada es un elemento analógico y el elemento de salida estará representado de forma digital. Esta representación de la forma digital es el formato, que permitirá decidir qué tipo de aplicación de software otorgará la visualización del objeto digitalizado.

Algunos de los diversos formatos de salida que se pueden obtener a través de un tratamiento de digitalización son Portable Document Format (PDF), una imagen gráfica en formato Tagged Image File Format (TIFF), Joint Photographic Experts Group (JPG) o Portable Network Graphic (PNG), un documento en formato Rich Text Format (RTF) o en formato Microsoft Word, si se emplean técnicas de ROC una vez manipulado computacionalmente el documento.

Es importante la elección del formato digital de salida, teniendo en cuenta cuál se adecua más a las necesidades de la unidad de información, institución u organización, de forma que se garantice la accesibilidad informacional futura, además de su sostenibilidad financiera en el tiempo (Arm y Fleischhauer, 2005).

La decisión sobre el formato elegido dependerá de la unidad de información que realice la digitalización y que posteriormente sea propietaria de la información resultante (Wentzel, 2006). Es importante pues disponer de documentación redactada sobre que formatos de salida se van a adoptar en un proceso de digitalización. Esta selección se debe apoyar en las guías y recomendaciones publicadas por parte de muchas y variadas instituciones (Lopatin, 2006; IFLA, 2005).

En la acepción del concepto material analógico ha de quedar claro que no sólo el papel se digitaliza. También se consideran material analógico susceptible

de digitalizar las fotografías en papel, diapositivas, posters, cintas de vídeo, cintas de audio, películas de cine de 8mm o de 35mm, entre otros (Wactlar y Christel, 2002).

Si el objetivo consiste en convertir audio, representado en forma de cinta o vídeo analógico, las técnicas son muy diferentes a las explicadas sobre el escaneado, ya que los instrumentos a emplear son otros. Esto exige que el proceso por el cual se digitalice sea distinto en cada momento y la tecnología a aplicar también.

Un ejemplo es el de las entidades sanitarias que convierten su archivo médico analógico en formato papel u otros formatos en digital. Pero la conversión no sólo afecta al archivo en formato analógico propiamente dicho, también es posible que se disponga de formatos digitales de representación antiguos: cintas de audio, videos en formato VHS o Beta, radiografías, grandes bases de datos con registros de voz en formatos obsoletos (Moen et al., 2004) u otros elementos que formen parte del archivo médico. Este proceso de integración suele ser costoso ya que la conversión previa valoración de datos digitales existentes a un sistema actualizado integrado puede suponer un problema de sostenibilidad financiera futura para la institución que lo lleve a cabo.

2.5 Recepción de datos digitales

El concepto nacido digital se aplica a aquellos objetos digitales que no tienen representación de origen analógico, es decir, el objeto ha sido creado de forma electrónica en origen. Otra cuestión distinta son las diferentes representaciones de los objetos nacidos digitales, que pueden ser en forma de documentos electrónicos gráficos o sonoros, entre otros. En este caso, en la recepción de los

datos digitales, se procederá a la aceptación o no de la información si resulta acorde con las líneas estratégicas de preservación de la unidad de información.

2.5.1 Que es un objeto nacido digital (born digital)

Como se ha mencionado previamente, se dispone de objetos analógicos y de objetos digitales. Estos últimos aparecen en la literatura como "born digital" o, dicho de otro modo, nacido digital[18].

Así podemos encontrar una definición (Ruan, J. y McDonough, J., 2009) donde se caracteriza un objeto de origen digital como *"The born-digital materials are those which are entirely computer generated and presented and that have no analog equivalent"*. Es decir, un objeto de origen digital no tiene ninguna representación analógica equivalente, lo que indica su fragilidad en el tiempo con respecto a otros materiales. La desaparición de objetos digitales debido a su tratamiento es mucho más rápida que la de los objetos analógicos. El concepto nacido digital es el que más problemas puede representar a una unidad de información que tenga que custodiar datos digitales en un futuro, si la planificación de la preservación digital no se realiza adecuadamente (Strodl et al., 2007). La elección de formatos para representar la información, soporte y ubicación puede determinar la accesibilidad a la información.

Los diversos conceptos técnicos que aparecen cuando se manipulan objetos nacidos digitales son obsolescencia (Cornell, 2006), migración (Mellor, Wheatley y Sergeant, 2002), emulación (Granger, 2000; Rothenberg, 1999) o análisis forense (John, 2008). Todos estos procesos, de forma individual o conjunta,

[18] Artículo 7 de la Carta de la Unesco sobre la Preservación del Patrimonio Digital (UNESCO, 2004)

pueden ser necesarios en el tratamiento de objetos digitales. A nivel legal surgen los conceptos de datos personales o los derechos de autor.

2.5.2 Obsolescencia

La obsolescencia tecnológica es un estado en el que se encuentra un soporte de información, que hace que no pueda ser leído ni su información extraída además de no poder representarse por ningún medio posible, aunque la información siga existiendo. El acceso a la información se puede realizar mediante una acción proactiva o una reactiva.

La reacción proactiva, a través procesos de vigilancia tecnológica, facilita que la información se pueda recuperar a lo largo del tiempo. Esto se consigue mediante técnicas, como la migración o la emulación, explicadas a continuación, u otros procesos que ayuden a recuperar la información, siempre dentro de un período en que el soporte o la representación de la información no estén caducos.

En contraste, existen las acciones reactivas, como el uso de técnicas de análisis forense, de forma que para acceder a la información se accede al objeto digital de forma intrusiva. En algunos casos es posible que una vez concluida la técnica de análisis forense digital, el objeto tratado de origen quede inutilizado.

2.5.3 Migración

La migración es una técnica que consiste en transformar un objeto digital en otro objeto digital en una versión tecnológicamente superior, de forma que la información contenida en éste, pueda ser accesible mediante un soporte diferente o con un sistema informático diferente. Así, se obtiene como resultado

una versión más moderna y avanzada. Este proceso puede conllevar pérdidas o cambios en las características de los documentos, la apariencia, llamada también el "look & feel" de la información. La modificación de determinadas características del objeto digital se conoce como modificación de las propiedades significativas de un documento.

Waters y Garrett (1996) proponen la siguiente definición de migración "*un conjunto de tareas diseñadas para alcanzar la transferencia periódica de materiales digitales de una configuración hardware/software a otra, o desde una generación tecnológica de ordenador a una generación subsiguiente*".

Para poder convertir un objeto digital en otro más actualizado tiene que existir el software que realizará la transformación y que tendrá que entender la información almacenada. Si esto lo traducimos en ejemplos podemos ver casos en los que es realmente sencillo y otros en los que no lo es tanto. Puede suceder que se modifique e incluso exista la pérdida de alguna propiedad significativa; en el caso de perderse, implicaría que habría características del objeto de los cuales no se podría disponer. Este sería el caso de una fotografía que se transforma de un formato como TIFF a JPG. En una transformación de este tipo se podría, a modo de ejemplo, perder resolución respecto a la imagen original.

Un ejemplo de migración puede ser la conversión de un documento de una hoja de cálculo en un archivo de texto donde los datos están separados por comas. Para poder realizar este proceso, existe en muchas ocasiones una opción para ello dentro del propio software que gestiona la hoja de cálculo. Actualmente la mayoría de las hojas de cálculo existentes contemplan esta opción. Un ejemplo un poco más complejo sería la conversión de una base de datos como Lotus 123 a un formato más actualizado como la base de datos Microsoft Access. El proceso que habría que realizar en este caso ya no es tan

simple. El tratamiento no sólo consiste en traspasar los datos de un tipo de base de datos a otra, sino también conservar la integridad referencial de los datos, ya que hay que transferir índices y relaciones para que estos se recuperen en la misma forma en que se crearon. Si la transmisión no se realiza de la forma adecuada, puede causar pérdidas de información o la ruptura de los índices y que cause un daño irreversible a la base de datos haciéndola inaccesible informacionalmente.

La técnica de la migración se podría aplicar mediante un modelo matemático pero todavía se necesitan sistemas de almacenamiento más rápidos y fiables (Luan et al., 2010).

2.5.4 Emulación

La emulación consiste en la utilización de un software que ha de funcionar en un software más actualizado para que la información a tratar pueda ser accesible. Se expone el siguiente ejemplo, donde se dispone de un documento realizado en una plataforma de 4 bits, que podría ser un documento electrónico realizado bajo un sistema operativo de la plataforma de juegos electrónica ATARI. Para poder acceder a la información de este documento en una plataforma de 32 o de 64 bits, como podría ser LINUX, hay que disponer de un software que, bajo un entorno LINUX, permita leer el documento. Este tipo de software no siempre está localizado ni es posible su ejecución (Bote, 2008).

Además, en el caso de la emulación, el software tiene que funcionar a la velocidad de proceso a la cual funcionaba el sistema operativo anteriormente. Esto implica que a la hora de elaborar el software, entre otros parámetros, hay que ralentizar los ciclos de reloj del ordenador. Este software se llama emulador. Otro ejemplo de emulador sería el software que emula el

funcionamiento de los videojuegos en una plataforma distinta para la que fueron creados (Guntembrunner et al., 2008).

2.5.5 El análisis forense digital

Una de las técnicas empleadas para poder disponer de objetos de origen digital son los métodos de análisis forense digital. Estos procedimientos son de muchísima utilidad, especialmente si se reciben en la unidad de información soportes digitales cuyo acceso es difícil o requiere que no tenga manipulación alguna. En cualquier objeto digital, al ser accedido por un ordenador, aunque sólo sea para su lectura, se deja un rastro del dispositivo que lo ha leído. Puede darse el caso que al recibir un soporte se necesite saber la última fecha en el que el objeto digital se creó. Las técnicas de análisis forense nos permiten identificar y traspasar datos tal y como se empleó por última vez el objeto digital. Como ejemplo, se podría citar el caso de un legado digital de un escritor a una biblioteca.

También las técnicas de análisis forense son útiles para saber sobre qué sistema se ha creado un objeto, y buscar los recursos adecuados para su tratamiento. Para emplear estos métodos existen programas de pago pero también hay opciones de software bajo licencia GNU (John, 2008).

El empleo de esta metodología con la utilización de software específico, implica disponer de personal adecuado en la unidad de información que se gestiona. Este hecho está provocando que los perfiles profesionales del personal de las bibliotecas y archivos estén cambiando.

2.5.6 Almacenamiento

El almacenamiento forma parte de la preservación digital, no sólo por las implicaciones que pueda tener en la corrupción de la información, sino en cómo se almacenan los datos a fin de recuperarlos después. La corrupción de la información es el resultado mediante el cual la información es alterada y se convierte en efímera o su comprensión semántica es otra a la que originalmente se creó. En ambos casos, la causa puede ser debida a un fallo mecánico del soporte donde está ubicada la información, obsolescencia del software o bien debido a la acción de un software malicioso, como un virus informático.

Si es un fallo mecánico, el hecho que un solo bit del soporte se convierta de 1 a 0 o viceversa, produce que la información quizás todavía se pueda recuperar e interpretar sin problemas. Si esto sucede con más bits, la cuestión ya no es tan clara. De hecho, aún realizando varias copias de seguridad y comprobando la suma de verificación del soporte de almacenamiento, no se garantiza la seguridad absoluta (Rosenthal, 2008). En el caso de un programa malicioso que altere la información, se puede disponer de una solución, como por ejemplo, un programa de antivirus. Una vez ejecutado el programa de antivirus, habrá que comprobar que la información que se haya podido corromper pueda ser informacionalmente accesible.

Uno de los grandes debates que existen es el lugar donde se almacenan los objetos digitales que se conservan y cómo. Así, los diferentes tipos de soportes de almacenamiento como el DVD, Blue-Ray o las diferentes soluciones con discos duros, son factores a tener en cuenta para grandes volúmenes de información, situación en la que se encontraría una entidad de gestión médica. El problema que se plantea es que si el producto tiene un error en un solo bit, qué efectos dañinos existirán sobre la información. Por tanto, cualquier

elemento físico de conservación de datos debe estar sometido a una monitorización constante, para poder evitar problemas posteriores en la recuperación de la información.

2.5.7 La integración digital

Una vez ya se dispone de los objetos digitalizados, surge la integración digital, es decir que los objetos digitales convivan en un mismo sistema de información. La integración digital es el proceso por el cual documentos digitalizados pasan a formar parte de un sistema de información donde hay otros documentos digitales, bien nacidos digitales u otros previamente digitalizados. Este proceso se produce en organizaciones en las cuáles se pretende que objetos, que habiendo pasado por un proceso de digitalización, pasen a formar parte de un sistema de información activo o pasivo, como puede ser el caso de las organizaciones de gestión sanitarias.

En este caso puede aparecer entre otros, el concepto de interoperabilidad, es decir, que el sistema digital existente pueda absorber documentos digitales de otras fuentes también digitales, sin que suponga una pérdida de información por cuestiones de inaccesibilidad, a la vez que entenderse digitalmente mediante los protocolos adecuados.

2.5.8 Las propiedades significativas de un objeto

Todo objeto que va a formar parte de un proceso de preservación digital tiene unas características intrínsecas que lo hacen único respecto del resto. Estas propiedades pueden definirse como:

> "*Las características de los objetos digitales que deben ser preservadas en el tiempo para asegurar su continua accesibilidad, usabilidad y significado de los objetos*" (Wilson, 2007).

Las propiedades significativas de un objeto digital pueden ser entre otras, el contenido, el contexto, la apariencia, la estructura, el comportamiento, las propiedades técnicas o de representación. En un proceso de migración, estas propiedades junto con otras, deben estar garantizadas de forma que en el objeto que haya sido reformateado, las propiedades resultantes sean equivalentes a las de la versión original del objeto, teniendo en cuenta un conjunto específico de características del mismo (Lynch, 1999). Este término también se puede encontrar en la literatura como esencia, características significativas, características esenciales y propiedades esenciales (Wilson, 2007).

El conocimiento de las propiedades significativas es necesario para saber si en un proceso de preservación digital estas van a verse alteradas o modificadas. Siempre que se realice una transformación de cualquier objeto analógico o digital en otro objeto digital, sus propiedades sufrirán consecuencias de algún tipo (Grace et al., 2008; Knight, 2008). Entender las propiedades significativas de un objeto digital implica saber, entre otros, qué propiedades tiene el objeto, cuáles son esenciales en su conservación y de cuáles puede prescindirse sin que afecte a su información. A modo de ejemplo, si se dispone de una colección con objetos analógicos de audio, cuestiones cómo la fidelidad, el volumen o la frecuencia de muestreo son propiedades que deben tenerse en cuenta cuando se realice la transferencia hacia un formato digital. Existen métodos formales para describir las propiedades significativas (Hedstrom y Lee, 2002).

2.6 Iniciativas en modelos de preservación digital

Existen diversas iniciativas de modelos de conservación digital. Todos los modelos tienen en su horizonte la preservación digital a largo plazo. El modelo de ciclo de vida de conservación, propuesto por el Digital Curation Centre (DCC), propone una conceptualización de todas las actividades necesarias en una unidad de custodia, a fin de obtener una concreción secuencial en todos los procesos de planificación y conservación digital.

El OAIS es otro de los modelos disponibles, siendo su característica principal la preservación a largo plazo de materiales digitales para una Comunidad Designada específicamente. Una Comunidad Designada es aquella que tiene alguna interrelación con el archivo OAIS en alguno de sus aspectos: la ingesta, la consumición de datos o la gestión. El modelo OAIS, en su propuesta de modelo de archivo de preservación digital, no hace referencia a ningún modelo de archivo organizativo en concreto, así como tampoco hace referencia alguna a un modelo tecnológico concreto, ni a un modelo informacional al respecto de la elección del tipo de datos a conservar. Sí menciona, sin embargo, una serie de procesos que una entidad debería seguir para preservar su información.

Existen iniciativas y proyectos internacionales compatibles con el modelo OAIS, como Networked European Deposit Library (NEDLIB), que hace énfasis en los requisitos de metadatos así cómo en las estrategias de preservación (Norona et al., 2001); CURL Exemplars in Digital Archives (CEDARS), un modelo de archivo digital distribuido (Jones, 2001); PANDORA[19], de la National Library of Australia (NLA), destinado a la preservación de recursos documentales australianos; o en la Harvard University Library el Digital

[19] http://pandora.nla.gov.au/ [consulta: 8 de marzo de 2012]

Repository Service (Harvard DRS)[20], cuyo objetivo principal es actuar como repositorio de preservación y como repositorio de acceso (Abrams et al., 2005).

2.7 Modelo de costes

Uno de los problemas pendientes en la preservación digital es disponer de un modelo de costes relativo a la custodia, tratamiento, almacenaje y otros procesos vinculados. A pesar de que existen diferentes estudios sobre modelos de costes, todavía no existe uno suficientemente aceptado. De entre todas las iniciativas realizadas a fin de obtener indicadores de costes, ninguna de ellas incide en un modelo concreto de preservación digital a largo plazo.

Es necesario indicar que todos los estudios existentes sobre modelos de costes se han basado en el modelo OAIS. En futuras investigaciones se debería incidir aún más en este modelo (Zeller; 2010). En la misma línea (Kejser et al, 2009) se propone un modelo basado en el modelo OAIS, señalando que hay determinadas funciones que deben ser analizadas con más detalle. Por otro lado, existe la propuesta de la realización de un modelo de costes basado en las seis entidades funcionales del modelo OAIS, que deberían ser parecidas en todas las instituciones, aunque existan diferencias entre países (Mageto, 2010).

[20] http://hul.harvard.edu/ois/systems/drs/ [consulta: 8 de marzo de 2012]

Capítulo 3

Marco jurídico

3 Marco jurídico y normativo

3.1 Estado de la cuestión

Para llevar a cabo los objetivos de este estudio, se ha procedido a analizar las recomendaciones de la Organización Mundial de la Salud (OMS) y la diferente legislación (europea, española y catalana) existente respecto a las historias clínicas. También se ha realizado un estudio exploratorio de los estándares internacionales vinculados a las historias médicas electrónicas. Finalmente, se han revisado los sistemas de auditoría, tanto informática como de preservación digital, así como diferente literatura científica al respecto. Una vez analizada la legislación existente sobre la historia clínica y su conservación se ha procedido a analizar la composición de la historia clínica y los estándares vinculados a ella.

Hay diferentes estándares utilizados en el sector sanitario. Respecto a los sistemas de información y a los datos médicos, los estándares son: HL7, de interoperabilidad entre sistemas de información sanitaria, y DICOM, para las imágenes médicas.

Una historia clínica dispone habitualmente de un formato HL7[21], el estándar de facto utilizado por todos los hospitales a nivel mundial. HL7 se emplea para la gestión de información en las historias clínicas electrónicas y está basado en el lenguaje de marcas EXtensible Markup Language (XML), que permite la interoperabilidad entre sistemas. Es decir, faculta que sistemas de información totalmente distintos puedan intercambiarse información. En el caso de España además, permite la interoperabilidad tanto entre hospitales como con el Ministerio de Sanidad, Servicios Sociales e Igualdad.

[21] http://www.hl7.org [consulta: 8 de marzo de 2012]

Una de las cuestiones que se plantea en la actualidad es cómo verificar la autenticidad de los registros médicos en el tiempo, más allá de la firma digital (Lekkas y Gritzalis, 2007). Se propone un mecanismo de monitorización del sistema para dar validez a los datos de aquellas historias clínicas firmadas digitalmente. Otra opción para contrastar la validez de los datos es el uso de sellos de tiempo ("time stamping") junto a las firmas digitales (Pirnejad, Bal y Berg, 2008). Es necesario tener en cuenta también que en el marco europeo, debido a la necesidad de guardar hasta treinta años, imágenes radiográficas, se complican especialmente estas tareas.

Se propone una línea conjunta con la OMS, gobiernos y asociaciones profesionales médicas a fin de poder reconstruir los contenidos de un registro médico. También se hace necesario plantear quién tendrá acceso a los datos de la historia clínica en un futuro y cómo se autorizará este acceso, reflexionando a la vez en la ética del uso de la información por parte de los profesionales de la medicina (Bakker, 2004)

3.2 La Organización Mundial de la Salud (OMS)

La OMS indica que los profesionales de la salud deberían emplear el formato electrónico de las historias clínicas, ya que mejoraría la calidad y precisión de los datos, la atención continua al paciente en el tiempo, la calidad de la atención ante la disposición inmediata de la información, la eficiencia de la gestión de las historias de salud, además de hacer la atención de la salud más sostenible. Sin embargo, indica que la durabilidad del soporte electrónico debe ser evaluada y documentada (WHO, 2006).

La OMS, además, considera crítico determinar el tiempo que los historiales médicos deberán conservarse y cuáles son los datos que deben conservarse.

3.3 Legislación comunitaria, española y catalana

En este trabajo se han tenido en cuenta las diferentes legislaciones existentes, como base para establecer cuestiones relativas a la seguridad, protección de datos personales y otros, en el ámbito jurídico vigente.

3.3.1 Directiva 95/46/CE

Esta es la Directiva del Parlamento Europeo (Europa, 1995) sobre el tratamiento de protección de datos. En el apartado 1 del artículo 8 se menciona lo siguiente:

> "*1. Los Estados miembros prohibirán el Tratamiento de datos personales que revelan 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.* "

Existe, sin embargo, una exención en el apartado 3:

> "*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 legislaciones nacionales o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.* "

3.3.2 Recomendación 2008/594/CE

En esta recomendación sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos (Europa, 2008) en el apartado de protección de datos personales, recomendaciones 10 a 15, indica que la aplicación de las salvaguardas necesarias deben ser realizadas por parte de los Estados Miembros en los historiales médicos así como, el establecimiento de un

período de conservación. Además, señala esta recomendación que, previo a la aplicación de cualquier sistema de historiales médicos, hay que realizar "*una evaluación de los riesgos en materia de seguridad de la información y de las repercusiones sobre la protección de datos personales*".

3.3.3 Directiva 2011/24/UE del Parlamento Europeo

En esta directiva relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza (Europa, 2011), se pone de manifiesto la necesidad, entre otros temas, de la interoperabilidad de datos asistenciales entre Estados Miembros, prestando especial atención a la protección de datos. En ella se indica que el derecho de las personas a acceder a los datos personales relativos a su salud, establecido por la directiva 95/46/CE de protección de datos personales, debe ser aplicado en el contexto de la asistencia sanitaria transfronteriza cubierta por la directiva 2011/24/CE. Sin embargo, no indica tiempo alguno para la conservación de los historiales médicos electrónicos.

3.3.4 España - Ley 15/99 (LOPD)

Ley Orgánica de Protección de Datos (BOE núm. 298, de 14.12.1999). Esta ley (España, 1999) regula en España la protección de datos de carácter personal. Dicha ley establece hasta tres niveles de seguridad en ficheros automatizados de datos personales y la obligación de notificación a la Agencia Española de Protección de Datos, mediante un documento sobre el tipo de datos que se disponen y qué nivel de seguridad se aplica.

Las entidades sanitarias aplican la Ley 15/99 en su nivel máximo. En este trabajo se tratará de comprobar también si estas instituciones están preparadas

para conservar a largo plazo las historias médicas electrónicas, como lo hacen en papel.

3.3.5 España - Ley 41/2002

La Ley 41/2002 de 14 de noviembre, es la ley básica reguladora de la autonomía del paciente y de Derechos y obligaciones en materia de información y Documentación Clínica (BOE núm. 274, de 11.15.2002). Esta ley (España, 2002) regula en España el contenido de la historia clínica como indica el artículo 14:

"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 ello, con objetivo de obtener la máxima Integración posible de la documentación clínica de cada paciente , por lo menos, en el ámbito de cada centro.*
>
> *2. Cada centro archivará las historias clínicas de suspensión pacientes, cualquiera que sea el soporte papel, audiovisual, informático o de otro tipo en el que constan, por lo que quedan garantizadas apoyo seguridad, apoyo 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 apoyo reproducción futura.*
>
> *4. Las Comunidades Autónomas aprobar las disposiciones de carácter necesarias para que los centros sanitarios puedan adoptar las medidas técnicas y organizativas adecuadas para archivar y proteger las historias clínicas y evitar apoyo destrucción o superior pérdida accidental. "*

Esta misma ley en su artículo 17 indica:

"Artículo 17. La conservación de la documentación clínica.

> *1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen apoyo correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuada a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial.* "

Tanto en el artículo 14 como en el 17 se puede comprobar que deben quedar garantizadas la seguridad de los historiales médicos, su conservación y recuperación de la información, así como el tiempo de custodia. Se determina un tiempo de conservación de cinco años. Como se puede observar en la Tabla 1, estos plazos varían en función de cada Comunidad Autónoma.

En este estudio de tesis se incide justamente en estos aspectos: la fiabilidad y seguridad de los historiales médicos, así como su preservación a largo plazo. Se evalúa si las entidades sanitarias catalanas están en condiciones de garantizar la conservación digital y se define un modelo de preservación de acuerdo con las características de estas entidades. Esta ley, junto con la versión adaptada del modelo OAIS propuesto en este estudio, permiten formalizar los aspectos derivados de los artículos 14 y 17, como se verá en el Capítulo 7.

3.3.6 España - Real Decreto 3 / 2010 de 8 de enero

El Real Decreto 3/2010 regula el Esquema Nacional de Seguridad (España, 2010) en el ámbito de la Administración Electrónica (BOE núm. 25 - 01/29/2010). Este Real Decreto persigue garantizar la confianza suficiente en los sistemas de información para que presten servicio sin interrupción. El Esquema Nacional de Seguridad (ENS) es de aplicación a los servicios que dan soporte a la administración electrónica dentro de las administraciones públicas. También corrobora que la información que se custodia ni se pierda ni llegue a terceros

sin el debido permiso. En definitiva, se trata de poder disponer de un sistema de información que sea de confianza. Los objetivos del ENS son:

- Crear las condiciones necesarias de confianza en el uso de medios electrónicos, tanto en los ciudadanos como en las administraciones públicas, para que ambas partes puedan ejercer sus derechos y sus obligaciones mediante los sistemas de información.

- Establecer una política de seguridad en la utilización de los medios electrónicos, con unos principios básicos y requisitos mínimos para una protección adecuada de la información.

- Disponer de elementos comunes de actuación en las administraciones públicas en materia de seguridad de tecnologías de la información y comunicación (TIC).

- Disponer de un lenguaje común entre las administraciones públicas y la industria en la comunicación de requisitos de seguridad.

Por cuestiones de coherencia, en este estudio también se utilizan como directrices de referencia aquellas que afectan a Catalunya, pero también se ha tenido en consideración las que corresponden a las otras comunidades mencionadas en la Tabla 1. Esto es debido a la disparidad de criterios entre las diferentes comunidades autónomas al respecto del tiempo de custodia de las historias clínicas.

3.3.7 Legislación en las Comunidades Autónomas

Una historia clínica (Catalunya, 2000) electrónica se compone de diferentes documentos de información clínica[22], como son: Informe Clínico de Alta, Informe Clínico de Consulta Externa, Informe Clínico de Urgencias, Informe Clínico de Atención Primaria, Informe de Cuidados de Enfermería, Informe de Resultados de pruebas de imagen, Informe de Resultados de pruebas de laboratorio, Informe de Resultados de otras pruebas diagnósticas e Historia Clínica Resumida.

Mediante el Informe Clínico de Alta, un hospital obtiene el Conjunto Mínimo Básico de Datos (CMBD). El CMBD son los campos mínimos que deben incluir los hospitales en sus historias clínicas en base al mencionado informe. El CMBD fue regulado por la Orden Ministerial de 6 de septiembre de 1984, BOE núm., 221 de 14 de septiembre, en su artículo 3. Al recibir la transferencia de competencias en materia de sanidad, todas las Comunidades Autónomas (CCAA) han acabado legislando el CMBD de acuerdo con sus necesidades, a fin de auditar la información.

Comunidad Autónoma	Nombre de la norma	Publicación	Artículo	Años de conservación
España	Ley autonomía básica del paciente	BOE - Ley 41/2002	Art. 17	5 años
Andalucía	Ley autonomía básica del paciente	BOE - Ley 41/2002	Art. 17	5 años
Aragón	Ley de Salud de Aragón	BOE - Ley 6/2002	Art. 18	-

Tabla 1. Marco legislativo.

[22] http://www.msc.es/profesionales/hcdsns/contenidoDoc/contenidos.htm [consulta: 8 de marzo de 2012]

Comunidad Autónoma	Nombre de la norma	Publicación	Artículo	Años de conservación
Canarias	Reglamento de Historia Clínica de Canarias	BOC - Decreto 178/2005	Art. 29	20 años
Cantabria	Ley de Sanidad de Cantabria	BOC - Ley 7/2002	Art. 71	15 años
Comunidad de Castilla y León	Decreto 101/2005	BOCYL-Decreto 101/2005		5 años y indefinido alguna documentación
Comunidad de Castilla-La Mancha	Circular 1/2009	DOCM-Resolución 27 de febrero de 2009	Art. 6.2	5 años
Catalunya	Llei d'Autonomia del Pacient i Drets d'informació i Documentació Clínica de Catalunya	DOGC - Llei 21/2000 y modificación del Parlament de Catalunya de 16/2010	Art. 12	15 años
Comunidad de Madrid	Recomendación 2/2004	BOCM-Recomendación 2/2004		5 años
Comunidad Foral de Navarra	Ley Foral de Derechos y deberes de las personas en materia de salud en Navarra	BOE- Ley Foral 17/2010	Art. 61.	5 años
Comunidad Valenciana	Ley de Derechos e Información al Paciente de la Comunidad Valenciana	DOGV- Ley 1/2003	Art. 8	n.a.
Extremadura	Ley de Información Sanitaria y Autonomía del Paciente de Extremadura	DOE - Ley 3/2005	Art. 34.	indefinidamente
Galicia	Ley de Sanidad de Galicia	DOG- Ley 8/2008	Art. 9.	n.a.
Illes Balears	Ley de Salud de las Islas Baleares	BOE - Ley 5/2003	Art. 14	n.a.
La Rioja	Ley de Salud de La Rioja	BOE- Ley 2/2002	Art. 11	n.a.
País Vasco	Decreto 45/1998	BOPV-Decreto 45/1998	Art. 9, 10 i 11	5 años
Principado de Asturias	Ley autonomía básica del paciente	BOE - Ley 41/2002	Art. 17	5 años
Región de Murcia	Ley de Derechos y Deberes de los Usuarios del Sistema Sanitario de Murcia	BO Región de Murcia- Ley 3/2009	Art. 54	20 años

Tabla 1 (cont.).

En el caso de Catalunya existe el CMDB es un órgano dependiente del Catsalut que es el encargado de recoger y analizar los CMDB (los datos), que los hospitales facilitan.

Respecto a las historias clínicas, si se realiza una comparativa a nivel nacional por Comunidades Autónomas (CCAA), se puede observar que existe diferente regulación respecto a la duración de su conservación. En la Tabla 1 se puede ver una comparativa de las leyes que se aplican a las diferentes Comunidades Autónomas sobre la historia clínica y el tiempo de conservación establecido. Se puede comprobar que dos Comunidades Autónomas, Andalucía y el Principado de Asturias no disponen de legislación al respecto. Es de suponer, pues, que prima la Ley 41/2002 (España, 2002) en estas comunidades y que el periodo de conservación de la historia clínica es lo que esta indica. Se ha descartado comparar los motivos por los que las CCAA establecen distintos plazos para la conservación de la historia clínica, aunque se pueden vislumbrar diferentes argumentos. En Catalunya, con la modificación de la norma (Catalunya, 2010), se establece que el período de conservación de la historia clínica es de quince años (15) a contar desde la fecha de alta de cada proceso asistencial. De otras Comunidades Autónomas establecen a modo de ejemplo cinco años (5) a partir del informe de alta. Lo que nos interesa, en cualquier caso, es el tiempo de conservación y su aplicación al modelo sanitario.

El modelo sanitario catalán (Catsalut, 2009) se basa, entre otros, en el concierto con entidades privadas mediante la Ley 15/1990 de Ordenación Sanitaria de Catalunya (LOSC) (Sanitat, 1999). Este hecho provoca que estas entidades tengan que disponer de un archivo digital propio, con las consecuencias a nivel organizativo o técnico que esto supone. Este archivo digital debe disponer de un sistema fiable y seguro para la conservación, entre otros elementos, de las historias clínicas electrónicas. No puede ser obviado

que, en la actualidad, hay un modelo híbrido donde conviven historias clínicas en papel e historias clínicas en digital. En el caso de las entidades estudiadas, estas están realizando una transición de la gestión de los archivos en papel a la gestión completamente digital.

3.3.8 Catalunya - Lley 16/2010

Ley 16/2010 de 3 de junio, modificación de la Ley 21/2000, de 29 de diciembre, sobre los derechos de información concerniente a la salud y la autonomía del paciente, y la documentación clínica. (DOGC núm. 5647, de 10.6.2010)

Uno de los objetivos de esta modificación de la ley 21/2000 (Catalunya, 2010) es "*la obligación de los centros sanitarios de conservar la historia clínica en las condiciones que garanticen la autenticidad, la integridad, la confidencialidad, la preservación y el mantenimiento correcto de la información asistencial registrada y que aseguren la reproducibilidad completa en el futuro, durante el tiempo en que sea obligatorio conservarla, independientemente del soporte en que se encuentre, que no debe ser necesariamente el soporte original.* " Así pues, en el artículo 12 de esta ley se indica lo siguiente:

> *"4. De la història clínica s'ha de conservar, juntament amb les dades d'identificació de cada pacient, com a mínim durant quinze anys des de la data d'alta de cada procés assistencial, la documentació següent:*
>
> *a) Els fulls de consentiment informat.*
>
> *b) Els informes d'alta.*
>
> *c) Els informes quirúrgics i el registre de part.*
>
> *d) Les dades relatives a l'anestèsia.*
>
> *e) Els informes d'exploracions complementàries.*
>
> *f) Els informes de necròpsia.*
>
> *g) Els informes d'anatomia patológica"*

3.4 Estándares Internacionales

3.4.1 ISO 12052 - DICOM

La normativa Health informatics — Digital Imaging and Communication in Medicine (DICOM) – ISO 12052 (AENOR, 2004) determina cómo deben ser las imágenes en medicina, fijando una serie de apartados para indicar su composición, así como la definición de los flujos de trabajo. Actualmente, esta norma es un estándar utilizado en todos los equipamientos médicos.

Este estándar en imagen digital médica es abierto y accesible mediante la National Electrical Manufacturers Association[23]. DICOM se empezó a emplear para que los pacientes se expusieran menos a las radiaciones cuando tenían que hacerse una radiografía. A este respecto, en el Reino Unido se estudió estadísticamente si se hacían más radiografías con el formato DICOM que con la radiografía analógica, concluyéndose que se hacían las mismas radiografías que con el sistema utilizado hasta la fecha (Weatheburn y Bryan, 1999). Así, en relación a la custodia de imágenes radiográficas, en el Reino Unido existe una recomendación para la custodia durante siete (7) años, poniéndose de manifiesto que el cálculo de costes de conservación es de difícil comprobación (Strickland, 2004). También en Canadá el tiempo de custodia de imágenes radiográficas es de siete (7) años (Scott, 2007). La cuestión está en determinar, respecto al volumen de radiografías, qué información es relevante guardar, pensando que una radiografía ocupa unos 10MB. También hay que indicar la existencia de DICOM Structured Reporting que es complementario al formato DICOM y cuya finalidad es estandarizar informes médicos y otros datos clínicos.

[23] ftp://medical.nema.org [consulta: 8 de marzo de 2012]

3.4.2 ISO 10781 - EHR

La norma ISO 10781 (ISO, 2006) establece cómo debe ser la funcionalidad de los registros electrónicos (HCE) en un sistema de información de salud. También indica cómo los historiales médicos electrónicos pueden ser interoperables e intercambiables con otros sistemas (RLG, 2002) a través del estándar conocido como HL7, estándar basado en el lenguaje de marcas XML.

3.5 Conclusiones respecto al marco jurídico y normativo

Del marco jurídico existente a nivel nacional se pueden plantear diversas reflexiones. El sector sanitario en España tiene una regulación jurídica que obliga a las instituciones sanitarias a conservar las historias clínicas electrónicas en sus propios archivos digitales. En muchos casos, se indica que la información debe conservarse independientemente de su soporte, aunque uno de esos soportes sea el digital. Cada Comunidad Autónoma tiene su propia legislación al respecto, siendo en algunas, como Catalunya, más restrictivas, lo que mejora aspectos como la seguridad e integridad de la información.

Por otro lado, existe el Esquema Nacional de Seguridad, que es de obligado cumplimiento en la Administración Pública. Esta norma jurídica provoca que las entidades sanitarias, como organizaciones que están vinculadas en mayor o menor grado a la Administración Pública, tengan que cumplir los requisitos que marca este Real Decreto.

Respecto al marco normativo, tanto los registros electrónicos de salud, los objetos digitales como las imágenes, son estándares en el sector médico. También el estándar de interoperabilidad entre registros facilita que varios sistemas con diferentes estructuras informáticas se puedan conectar entre sí. Estos estándares, en cierta forma, son una ventaja para construir un modelo de

conservación digital, ya que implica una homogeneidad respecto a los formatos que se conservarán.

Capítulo 4

Metodología de las auditorias

4. Metodología de las auditorias

4.1 Introducción a los sistemas de auditoria

Los mecanismos que permiten el análisis de una organización en aspectos como la seguridad informática, la valoración de riesgos, la auditoría de la información o la auditoría de la preservación, son cuestiones relevantes a la hora de establecer la planificación de la preservación digital en una institución.

Así, de forma descriptiva, se puede afirmar que la auditoría informática permite determinar el nivel tecnológico del sistema de información de una organización; la valoración de riesgos permite disponer de los criterios de evaluación necesarios para conocer las vulnerabilidades a las cuáles un sistema está sometido; la auditoría de la información estima la calidad de los datos que se procesan en una organización; y, finalmente, la auditoría de la preservación digital evalúa si una entidad está en condiciones de poder conservar su información digital en el tiempo.

Mediante los procedimientos de auditoría se obtienen una serie de variables a tener en cuenta con la finalidad de tomar medidas correctoras o preventivas. Sin esta información previa, difícilmente una entidad puede planificar todos los procesos correspondientes a la preservación digital.

En este capítulo se revisan las herramientas de auditoría más extendidas, algunas de las cuáles se han empleado finalmente en este proyecto.

4.2 Metodologías de auditoría Informática

4.2.1 COBIT

COBIT (IT Governance Institute, 2010) es un marco de trabajo que permite identificar aquella información que una empresa necesita para alcanzar sus objetivos, sus necesidades de inversión, así como la gestión y el control de los recursos TIC, utilizando para ello un conjunto de procesos que ayudan a garantizar la disposición de la información que se necesita.

COBIT se basa en los criterios de efectividad, eficiencia, confidencialidad, integridad, disponibilidad, desempeño y fiabilidad

Los recursos TIC que se pueden identificar en COBIT son aplicaciones, información, infraestructura y personal.

4.2.2 Microsoft Security Assessment Tool

La herramienta Microsoft Security Assessment Tool (Microsoft, 2009) está diseñada como método de autoevaluación para el análisis de riesgos, en materia de seguridad informática, de empresas que dispongan entre cincuenta (50) a quinientos (500) ordenadores. Esta herramienta es útil para el análisis de riesgos en entidades como las que estamos evaluando. La herramienta requiere de una información básica sobre la empresa para poder analizar la seguridad de las infraestructuras, de sus aplicaciones y operaciones, así como del personal, todo ello sin descuidar el entorno en el cual la organización interactúa.

La herramienta, por último, permite generar un informe abreviado o completo sobre el análisis de riesgos de una organización. El sistema de ayuda

nos indica claramente que la herramienta sirve como guía preliminar de análisis de riesgos y que no se debe sustituir por cualquier otra evaluación específica por equipos cualificados independientes. Aún así, esta herramienta no sigue ningún estándar en concreto, cuando menos no está reflejado en su documentación.

En cualquier caso, es una herramienta con poca difusión todavía, aunque empieza a emplearse en sistemas de aprendizaje de evaluación de riesgos (Bai, Summers y Bostworth, 2007).

4.2.3 MAGERIT

MAGERIT (MAP, 2006) es el acrónimo de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Esta metodología ha sido creada por el Consejo Superior de Administración Electrónica, organismo perteneciente al Ministerio de Política Territorial y Administración Pública. Permite evaluar los riesgos de un sistema de información dentro de la Administración. La metodología MAGERIT puede aplicarse mediante un software de nombre PILAR[24], actualmente en la versión 5.1.3, de fecha 13/07/2011. Esta es precisamente la metodología y versión empleada en este proyecto. El software PILAR facilita una serie de informes y gráficos indicando en qué situación se encuentran los activos de los sistemas. Además, actualmente esta herramienta permite ser implementada en el Esquema Nacional de Seguridad (ENS).

La metodología MAGERIT analiza el modelo de valor, evaluando los activos de los sistemas y el mapa de riesgos, para intentar determinar la relación de las posibles amenazas a las que los activos están expuestos. Además, permite llevar a cabo la evaluación de las salvaguardias, midiendo la seguridad de un sistema

[24] http://www.ar-tools.com [consulta: 8 de marzo de 2012]

de información y el estado del riesgo. Esta metodología también evalúa los activos de un sistema de información sobre la base de su riesgo residual. Y, por último, permite obtener el informe de suficiencias, mostrando las debilidades para mitigar los riesgos de un sistema, y el plan de seguridad, que facilita la realización de una correcta gestión de riesgos. Esta metodología es de carácter público, ya que pertenece al Ministerio de Política Territorial y Administración Pública. Para su utilización, no se necesita autorización previa.

4.3 Auditoria en conservación y preservación digital

4.3.1 Data Audit Framework

La herramienta DAF[25], creada en el año 2006, es una utilidad en línea que ayuda a planificar una estrategia de preservación y accesibilidad a largo plazo (Wilson et al. 2010). Fue elaborado para asegurar que los datos de investigación producidos por una institución de educación superior del Reino Unido estuviesen preservados y fuesen accesibles a largo plazo.

Esta metodología se compone de cuatro procesos: planificación de la auditoría; identificación y clasificación de los activos de datos; evaluación de la gestión de los datos; y realización del informe de evaluación con una propuesta de los posibles cambios a realizar en una organización. Estas cuatro fases son las que permiten evaluar los datos de investigación de un departamento con la finalidad de conservarlos a largo plazo (Martínez-Uribe, 2009).

[25] http://www.data-audit.eu [consulta: 8 de marzo de 2012]

4.3.2 Catalogue of Criteria for Trusted Digital Repositories

El Catalogue of Criteria for Trusted Digital Repositories está elaborado por el grupo de trabajo Working Group Trusted Repositories - Certification, dentro del proyecto Nestor[26]. El proyecto Nestor, es un programa de investigación en preservación y conservación digital financiado por el gobierno alemán. El grupo de trabajo ha creado este catálogo (Nestor, 2008) donde se exponen unos criterios para disponer de Repositorios Digitales de Confianza: Su primer borrador fue elaborado en 2006. El catálogo está fundamentado en estándares nacionales e internacionales, como DINI (DINI, 2007), el informe RLG-OCLC (RLG, 2002) y es la base de la metodología Trustworthy Repositories Audit & Certification: Criteria and Checklist (TRAC) (CRL y OCLC, 2007).

El documento es un catálogo de criterios orientados hacia la fiabilidad de un repositorio digital, identificando medidas de la organización a analizar, así como requerimientos técnicos. Los principios de este catálogo se basan en la aplicación de criterios de documentación, transparencia, adecuación y cuantificación de la medición. Emplea la terminología del modelo de referencia OAIS.

Este catálogo de criterios sobre repositorios de confianza, a pesar de estar pensado para Alemania, tiene un consenso importante dentro de la comunidad internacional.

Esta herramienta está siendo utilizada como base para la norma DIN[27] 31644, *Information und Dokumentation - Kriterienkatalog für vertrauenswürdige digitale Langzeitarchive*.

[26] http://www.langzeitarchivierung.de/ [consulta: 8 de marzo de 2012]
[27] http://www.din.de [consulta: 8 de marzo de 2012]

4.3.3 DINI

DINI[28] Certificate Document and Publication Services es una metodología editada en 2006, que se utiliza para evaluar la información contenida en un repositorio en línea. Permite determinar si un repositorio está en condiciones de conservar información a largo plazo.

4.3.4 DRAMBORA

DRAMBORA (DCC y DPE, 2007) es una herramienta de autoevaluación, de "autoauditoría" de análisis de riesgos para repositorios institucionales. Creada en 2007, ha sido elaborada por Digital Curation Centre (DCC) y el proyecto europeo Digital Preservation Europe (DPE)[29]. La herramienta puede ser utilizada tanto en línea como sin tener acceso a Internet, como herramienta de software, y ofrece a quien realice el análisis los siguientes apartados:

- Definir el alcance del repositorio
- Identificar las actividades del repositorio
- Identificar los riesgos y vulnerabilidades
- Calcular los riesgos
- Definir cuantitativamente los riesgos

DRAMBORA es una metodología orientada a la preservación digital que carece de un software automático de evaluación aunque sí dispone de plantillas, en forma de hoja de cálculo, con el objetivo de obtener resultados gráficos. Sin embargo, DRAMBORA es una metodología que no tiene en cuenta,

[28] http://www.dini.de [consulta: 8 de marzo de 2012]
[29] http://www.digitalpreservationeurope.eu [consulta: 8 de marzo de 2012]

de forma específica, la protección de datos personales, aunque sí la tiene sobre el entorno y la estructura técnica de los materiales a conservar.

4.3.5 IBM Long Term Digital Preservation Assessment

IBM elaboró en 2007, una herramienta de software, Long-Term Digital Preservation Assessment (LTDPA)[30], que permite evaluar, de acuerdo con TRAC, a una entidad que esté en proceso de tener un plan de preservación a largo plazo. La herramienta da como salida una información gráfica que indica el nivel de riesgos donde se encuentra la entidad, así como las carencias que tiene, y está orientada especialmente para empresas sanitarias. En el momento de elaboración de este proyecto de investigación, esta herramienta no estaba disponible.

4.3.6 Check-up: A Tool for Assessing Your Agency's Information and Records Management

En 2008, los Archivos Nacionales de Australia (NAA, 2008) publicaron esta guía basada en la Australian Standard for Records Management, la norma ISO 15489:2002 de gestión documental y en los estándares, políticas y guías de los Archivos Nacionales Australianos. Esta guía responde a las cuestiones sobre si una institución cumple los requisitos mínimos de estandarización que indican los Archivos Nacionales de Australia. También permite verificar si una institución puede mejorar la gestión de su información y archivos.

La guía se desglosa en procedimientos para: el análisis de riesgos vinculados a parte de la institución analizada; el análisis de las funciones y procesos que

[30] https://www.research.ibm.com/haifa/projects/storage/datastores/ltdp.html [consulta: 8 de marzo de 2012]

tienen un riesgo más elevado; la evaluación del alcance y, finalmente, la calificación del nivel de riesgos, en términos cuantitativos, en que se encuentra la institución analizada.

4.4 El Esquema Nacional de Seguridad

La aprobación en España, en enero de 2010, del Esquema Nacional de Seguridad (ENS), como desarrollo de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (BOE 23-6-2007), ha creado un marco para la realización de auditorías de seguridad informática en el sector público. El ENS es de obligada aplicación en los sistemas informáticos de entidades públicas españolas que soporten las actividades de administración electrónica, así como a la interoperabilidad en la prestación de servicios entre distintas administraciones públicas. La excepción en la aplicación de esta norma es el caso de aquellos sistemas que tratan información clasificada, regulada por la Ley 9/1968 de 5 de abril, de Secretos Oficiales y normas de desarrollo.

Por tanto, su aplicación al ámbito sanitario es plena, con especial relevancia en la gestión de la HCE. El ENS es una normativa basada en la auditoría de la seguridad. Examina la tecnología y su entorno, con sus salvaguardas correspondientes, permitiendo aplicar el nivel de seguridad que necesite la organización.

Al ser el ENS de reciente creación (España, 2010), no existe todavía literatura académica suficiente al respecto ni de su uso, ni de sus consecuencias, ni tampoco de experiencias en ningún tipo de entidad individual. Sin embargo, sí empieza a existir alguna experiencia en organizaciones como la Seguridad Social (Escudero, 2011).

El ENS tiene en su metodología los requisitos mínimos para una protección adecuada de la información de un sistema. Como ley, el ENS persigue que exista la confianza suficiente en los sistemas de información para que presten servicio ininterrumpidamente durante todo del año en la forma de 24 x 7. También corrobora que la información que se custodie no llegue a terceros sin la autorización debida, ni que se pierda. Se trata pues de una reglamentación que permite que un sistema de información sea fiable. Los objetivos de esta ley son:

- Crear las condiciones necesarias de confianza en el uso de medio electrónicos tanto en los ciudadanos, como en las administraciones públicas para que ambas partes puedan ejercer sus derechos y sus obligaciones mediante sistemas de información.

- Disponer de elementos comunes entre las administraciones públicas y la comunicación de requisitos de seguridad en la industria.

El ENS dispone de setenta y cinco indicadores (75) distribuidos en tres apartados: marco organizativo con seis indicadores (6), marco operacional con treinta y un indicadores (31) y medidas de protección con cuarenta indicadores (40).

4.5 Trustworthy Repositories Audit and Certification Criteria (TRAC)

Trusted Repositories Audit & Certification: Criteria & Checklist (TRAC) es una metodología orientada a la auditoria de repositorios digitales dedicados a la conservación digital a largo plazo. El *Trustworthy Repositories Audit & Certification* pretende en su versión 1.0 publicada en 2007, reunir las mejores

prácticas sobre los requerimientos necesarios para un repositorio digital de una institución sea fiable para conservar digitalmente documentos (ISO, 2012).

Este sistema de auditorías está creado por Research Library Group y el National Archives and Records Administration (RLG-NARA) e influenciado especialmente por dos organizaciones:

- The Center for Research Libraries (CRL) Auditing and Certification of Digital Archives Project.
- El grupo de trabajo de Nestor Network of Expertise in Long-Term Storage and Digital Resources con la publicación antes mencionada Catálogo of Criteria for Trusted Digital Repositories.

El sistema de auditoría establece una línea básica sobre la definición de un repositorio digital de confianza, mediante listas de comprobación.

TRAC dispone de tres apartados subdivididos en un total de ochenta y cuatro (84) indicadores. Según los apartados, Infraestructura de la Organización dispone de dieciséis indicadores (16), Gestión de los Objetos Digitales con cuarenta y cuatro indicadores (44) y Tecnologías, Infraestructura técnica y Seguridad con dieciséis indicadores (16). Estos indicadores se verifican mediante la comprobación y análisis de documentación o el análisis de evidencias que debe tener un repositorio. Una vez revisados los requisitos correspondientes a los indicadores, se dispone de información sobre el estado de certificación y auditoria del repositorio.

TRAC, además, dispone de una serie de indicadores de mínimo cumplimiento. De ellos, seis (6) pertenecen a Infraestructura de la Organización,

seis (6) a Gestión de los Objetos Digitales y siete (7) a Tecnologías, Infraestructura Técnica y Seguridad.

En la revisión de la literatura realizado, no se han encontrado referencias a la incidencia directa de TRAC con OAIS, si bien es cierto que están relacionados entre sí (Dobratz, 2007). TRAC emplea vocabulario del modelo de referencia Open Archival Information System (OAIS), ISO 14721:2003 (Bote y Termens, 2011) para tener referencias y similitudes con este modelo, así como evitar precisamente confusiones en la terminología.

La aplicabilidad de sus criterios también se basa en la nomenclatura tanto del grupo de trabajo de Nestor como del DCC: *documentación, transparencia, adecuación y cuantificación de la medición*.

Actualmente este sistema de auditoría es una norma ISO 16363:2012, publicada el 14/02/2012.

4.5.1 Experiencias con TRAC

Si bien es cierto que se han elaborado y hechos público pocos informes de aplicación de TRAC a un centro determinado, el Centre for Research Libraries tiene publicados dos informes realizados (CRL, 2010 y CRL, 2011) donde se analizan dos entidades, Portico y HathiTrust. También se dispone de auditorías sobre Lots of Copies Keep Stuff Safe (LOCKSS) y Interuniversity Consortium for Political and Social Research (ICPSR)[31], realizadas con versiones preliminares de la metodología TRAC.

[31] http://www.crl.edu/archiving-preservation/digital-archives/digital-archive-reports [consulta: 8 de marzo de 2012]

Portico[32] es un proveedor de servicios dedicado a preservar digitalmente documentos de la comunidad académica como revistas o libros. HathiTrust[33] es un consorcio dedicado a la conservación de patrimonio cultural digital, básicamente formado por bibliotecas universitarias. Ambos informes evalúan positivamente a las dos organizaciones pero, aún así, les invitan a una posterior revisión a fin de mejorar sus evaluaciones. En los dos informes se hace una evaluación con puntuaciones de 1 a 5, siendo 1 la peor puntuación y 5 la mejor. Es importante recalcar que en los dos informes se hace alusión a TRAC pero también a otras métricas complementarias y desarrolladas por el CRL, aunque no se precisa qué otras métricas emplean en ninguno de los dos informes.

Por otro lado (Steinhart y Dietrich, 2009) realizan el análisis de un repositorio en línea que no está dedicado a la preservación directamente y por tanto descarta algunos puntos de TRAC que no le resultan de utilidad. Es decir, se aplica TRAC a un repositorio, con el objetivo que sea de confianza pero no con la finalidad de preservar información digitalmente.

En el presente estudio se han empleado todos los indicadores de TRAC, aunque se ha incidido especialmente en los indicadores mínimos necesarios señalados en la propia normativa TRAC. Esto se debe a que ninguna entidad de gestión sanitaria tiene todavía desarrollado un mecanismo de conservación de historias clínicas electrónicas y, por tanto, hay determinados indicadores que no se han podido evaluar.

[32] http://www.portico.org/digital-preservation/ [consulta: 8 de marzo de 2012]
[33] http://www.hathitrust.org/ [consulta: 8 de marzo de 2012]

4.5.2 Tendencias en TRAC

TRAC, como se ha mencionado anteriormente, es un modelo de auditoría que irá evolucionando, estando en este momento en proceso la creación de un cuerpo de auditores internacionales[34]. De esta forma no sólo será un estándar, sino que dispondrá de auditores, que permitirán garantizar que las instituciones sean evaluadas con determinadas garantías.

4.6 Mapeado de TRAC y el Esquema Nacional de Seguridad

4.6.1 Auditoria de la seguridad

La consolidación de la historia clínica electrónica (HCE) así como de otros procesos de la gestión sanitaria exige que la documentación que estos generan sea gestionada en óptimas condiciones informáticas que garanticen su seguridad a nivel de disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad. Estas dimensiones de la seguridad informática normalmente se establecen dentro de los objetivos de los sistemas de aseguramiento de la calidad (siguiendo la norma ISO 27000 o similares), con una visión de prestación del servicio a corto plazo. Una de las principales ventajas que llevan a la generalización de la HCE es la consulta y la reutilización de los datos clínicos a medio y largo plazo, pero, para que ello sea posible, es imprescindible asegurar la preservación digital a largo plazo de estos datos.

[34] http://wiki.digitalrepositoryauditandcertification.org/bin/view [consulta: 8 de marzo de 2012]

4.6.2 Metodología aplicada a los indicadores

Se ha realizado una permuta de los indicadores del ENS y TRAC, reflejada en la Figura 1, y viceversa, reflejada en la Figura 2. Esta permuta se ha realizado comparando los requisitos y definiciones conceptuales de cada indicador de TRAC junto con los del ENS. Existen redundancias o duplicaciones en algunos indicadores que se han eliminado de las imágenes para facilitar su lectura.

Debido a que en el ENS existe una granularidad en sus indicadores originadas en los diferentes niveles de seguridad a aplicar, se han ejecutado las permutas en un primer nivel descriptivos de los indicadores.

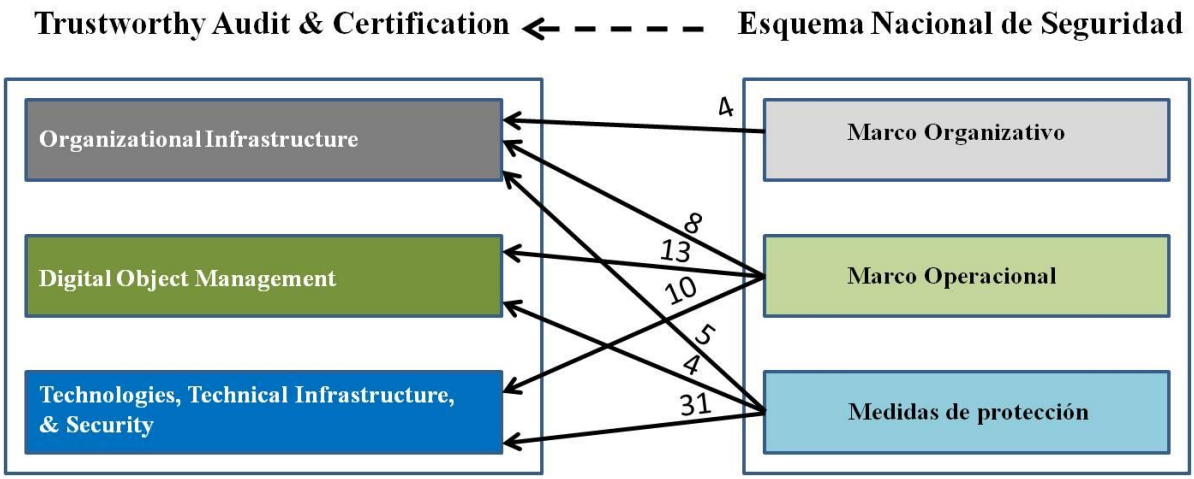

Figura 1. Permuta de indicadores entre el ENS y TRAC.

En el intercambio de indicadores de ENS con TRAC, como se muestra en la Figura 1, dieciséis (16) indicadores pertenecientes al apartado del marco operacional coinciden con los objetivos mínimos de TRAC. Estos están distribuidos entre los subapartados de planificación con cinco (5), control de acceso con cuatro (4), explotación con cinco (5) y monitorización del sistema con dos (2) indicadores. Esto también se puede observar en el apartado de medidas de protección, donde un total de ocho (8) indicadores también coinciden con algunos objetivos mínimos de TRAC. Estos se reparten entre los subapartados

de protección de las instalaciones con cuatro (4), gestión de personal con uno (1), protección de los equipos con uno (1), protección de las comunicaciones con uno (1) y protección de la información con uno (1).

Uno de los aspectos más importantes ha sido la protección de datos, ya que ambas metodologías se aplican en entornos muy diferentes. En este caso, el ENS complementa a TRAC.

A nivel específico, no se produce ningún cruce del ENS con TRAC en los apartados de TRAC relativos a la sostenibilidad financiera, ingesta de datos en el repositorio, ingesta de paquetes AIP, planificación de la preservación y almacenamiento de los archivos.

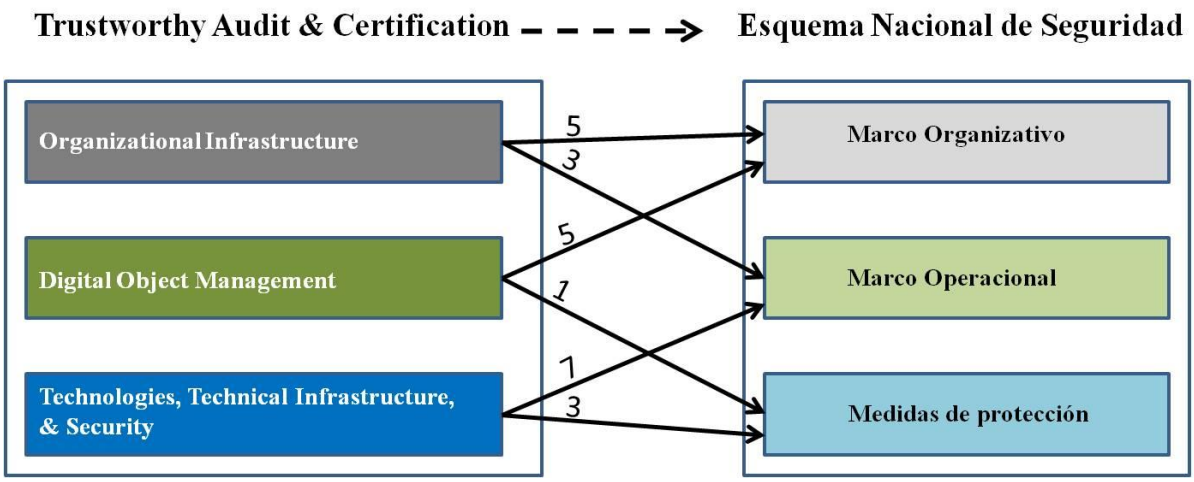

Figura 2. Permuta de indicadores entre TRAC y el ENS.

A nivel específico, en el ENS, en su apartado de medidas de protección, coincide en las permutas, en un 90% de sus indicadores, con el apartado de Seguridad de TRAC. Esto indica que las medidas de seguridad adoptadas en TRAC contemplan una protección más global de equipos, personal, información, soportes de la información y de los servicios que proporciona el servicio auditado. Así como TRAC define unos apartados mínimos a cumplir

para que un repositorio sea de confianza, esto no está claro en el ENS, a pesar de que hay indicada una serie de requisitos mínimos en el artículo 11, pero que no está reflejada en los indicadores del ENS.

Sin embargo, en sentido inverso pocos de los indicadores de TRAC tienen algún indicador en común con el ENS, como se puede observar en la Figura 2. Esto quiere decir que TRAC dispone de todos los elementos del ENS por ser TRAC una normativa más genérica y orientada a la preservación digital. Respecto a los veintisiete indicadores (27) de cumplimiento mínimo que TRAC dispone, sólo diez (10) se han podido combinar con indicadores del ENS.

4.6.3 Agrupación de indicadores de ambas metodologías

En este apartado se indica la agrupación de elementos del ENS y Trustworthy Repository Audit and Certification Criteria. Puesto que el ENS no contempla todas las opciones de TRAC, sólo se indicarán aquellas que se pueden agrupar de forma conjunta. A fin de facilitar la lectura se han separado los apartados en colores y se ha introducido un título en cada uno de ellos, siguiendo el orden de lectura del ENS.

Para facilitar la comprensión del cruce de indicadores, se han organizado los mismos siguiendo el ENS. En la Tabla 2, se indican cómo se han organizado.

Marco organizativo	No dispone de subapartados
Marco Operacional	Planificación Control de acceso Explotación Servicios Externos Continuidad del servicio Monitorización del sistema
Medidas de protección	Protección de las infraestructuras Gestión de personal Protección de los equipos Protección de las comunicaciones Protección de la información Protección de las aplicaciones informáticas Protección de la información

Tabla 2. Distribución de los indicadores.

Marco Organizativo

ENS	**TRAC**
Marco Organizativo	*Criterio*
Política de seguridad [org. 1]	A1.1 Declaración de la misión del repositorio. A1.1 Marco legal o legislativo; necesidades regulatorias. A2.2 Definiciones de roles y responsabilidades. A2.2 Diagramas organizativos. A2.2 Documentación con la descripción de estrategias de salida y planes de contingencia.

ENS	**TRAC**
Marco Organizativo	*Criterio*
Normativa de seguridad [org. 2]	A2.1 Planes de desarrollo y definición de competencias. A2.2 Definiciones de roles y responsabilidades.
Nota: La descripción del uso correcto de los equipos debe formar parte de la definición de competencias del personal. Si se contrata personal inadecuado la probabilidad de uso incorrecto será elevada, por lo tanto se considera que este apartado debe tener relación con la estructura organizativa y personal de TRAC.	

ENS	**TRAC**
Marco Organizativo	*Criterio*
Procedimientos de seguridad [org. 3]	A2.1 Descripción del puesto de trabajo. A2.1 Definición de competencias. C1.5 Informes de errores y análisis de amenazas.

ENS	**TRAC**
Marco Organizativo	*Criterio*
Proceso de autorización [org. 4]	C3.1 Documentación con la descripción del análisis de sistemas, personal y necesidades de Seguridad.
Nota: Todos estos apartados implican realizar un análisis de riesgos antes de entrar en producción. Es por ello que se ha agrupado en el apartado 3.1 de TRAC "*Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs*" C3.1 está marcado en gris porque es un requisito mínimo en TRAC.	

Marco Operacional

Organización de los indicadores en el marco operacional

Marco Operacional	Planificación Control de acceso Explotación Servicios Externos Continuidad del servicio Monitorización del sistema

Tabla 3. Distribución de los indicadores en el marco operacional

Planificación

ENS	**TRAC**
Marco Operacional	*Criterio*
Planificación	
Análisis de riesgos [op.pl. 1]	C3.1 Evaluación regular de riesgos.
Nota: Todos estos apartados implican realizar un análisis de riesgos antes de entrar en funcionamiento. Es por ello que se ha agrupado en el apartado 3.1 de TRAC. "*Repository maintains a systematic analysis of such factors as data, systems, personnel, physical plant, and security needs*" Por otra parte, ya que se evaluará un entorno médico aplicará la categoría ALTA. C3.1 está marcado en gris porque es un requisito mínimo en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Planificación	
Arquitectura de seguridad [op.pl. 2]	C2.1 Inventario de hardware. C2.2 Inventario de software. C3.3 Documentación de autorización del sistema. C1.9 Procedimientos de evaluación documentados. C2.1 Vigilancia tecnológica.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Planificación	
Adquisición de nuevos componentes [op.pl. 3]	C3.1 Evaluación regular de riesgos.
	C3.2 El repositorio ha implementado controles para controlar adecuadamente cada una de las necesidades de seguridad definidas.
	A2.3 Plan de formación y desarrollo de personal A4.4 Documentos de inversión financiera.
Los elementos marcados en gris son indicadores mínimos en TRAC. Nota: El apartado c) contiene dos indicadores de TRAC ya que en TRAC son dos indicadores diferenciados	

ENS	**TRAC**
Marco Operacional	*Criterio*
Planificación	
Dimensionamiento / gestión de capacidades [op.pl. 4]	C1.1 El repositorio funciona en sistemas operativos adecuados y en otros núcleos de software de infraestructuras. Inventario software, documentación del sistema.
	A2.1 El repositorio tiene identificados y establecidos deber que necesita para mejora y dispone de personal con las habilidades adecuadas y la experiencia para cubrir estas obligaciones.
	C2.1 Documentación de procedimientos, vigilancia tecnológica, evaluación de las necesidades de los usuarios.
Los elementos marcados en gris son indicadores mínimos en TRAC. Nota: El apartado C de TRAC está indicado para los requisitos generales de infraestructuras (General system infrastructure requirements). Es por ello que se ha escogido esta opción en los apartados a, b, d.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Planificación	
Componentes certificados [op.pl. 5]	C2.1 Tecnologías apropiadas; documentación de procedimientos, vigilancia tecnológica, evaluación de las necesidades de los usuarios.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

Control de Acceso

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Identificación [op.acc. 1]	B6.5 Matrices de autenticación
	B6.6 Gestión de errores e incidentes
Nota: En este indicador tienen cabida tanto el indicador 6.5 Matrices de autenticación y 6.6 Gestión de errores e incidentes.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Requisitos de acceso [op.acc. 2]	B6.3 Mecanismos de acceso al sistema que prevengan acciones no autorizadas.

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Segregación de funciones y tareas [op.acc. 3]	B6.6 Registros de acceso.

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Proceso de gestión de derechos de acceso [op.acc. 4]	B6.3 Políticas de acceso, registros de acceso a los usuarios y denegaciones a los usuarios.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Mecanismo de autenticación [op.acc. 5]	B6.4 Mecanismos de validación de acceso dentro del sistema: documentación de la autenticación y procedimientos de validación.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Acceso local [op.acc. 6]	B6.4 Mecanismos de validación de acceso dentro del sistema: documentación de la autenticación y procedimientos de validación.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Control de acceso	
Acceso remoto [op.acc. 7]	B6.4 Mecanismos de validación de acceso dentro del sistema: documentación de la autenticación y procedimientos de validación.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

Explotación

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Inventario de activos [op.exp. 1]	C2.1 Inventario de hardware.
Los elementos marcados en gris son indicadores mínimos en TRAC. Nota: También podría agruparse dentro de este apartado tanto A2.1 como A2.2 que son relativos a la descripción de trabajo y los roles y responsabilidades.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Configuración de la seguridad [op.exp. 2]	C3.2 El repositorio ha implementado controles de acuerdo a les necesidades de seguridad definidas.

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Gestión de la configuración [op.exp. 3]	C1.10 Documentación relativa a la actualización de las instalaciones.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Mantenimiento [op.exp. 4]	C1.7 Documentación del fabricante de hardware.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Gestión de cambios [op.exp. 5]	C1.8 El repositorio dispone de procesos de gestión de cambios documentadas que identifican los cambios en los procesos críticos que potencialmente afectan a la capacidad del repositorio de cumplir con sus responsabilidades legales.
Los elementos marcados en gris son indicadores mínimos en TRAC	

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Protección frente código dañino [op.exp. 6]	C3.2 El repositorio ha implementado controles para coordinar adecuadamente cada una de las necesidades de seguridad definidas.

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Gestión de incidencias [op.exp. 7]	C3.2 El repositorio ha implementado controles para coordinar adecuadamente cada una de las necesidades de seguridad definidas.
Los elementos marcados en gris son indicadores mínimos en TRAC	

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Registro de la actividad de los usuarios [op.exp. 8]	B6.5 Matrices de autenticación.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Registro de la gestión de incidencias [op.exp. 9]	B6.6 Registros de acceso.

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Protección de los registros de actividad [op.exp. 10]	B6.6 Registros de acceso.

ENS	**TRAC**
Marco Operacional	*Criterio*
Explotación	
Protección de claves criptográficas [op.exp. 11]	B6.6 Registros de acceso.

Servicios externos

ENS	**TRAC**
Marco Operacional	*Criterio*
Servicios externos	
Contratación y acuerdos de nivel de servicio [op.ext.1]	A5.3 El repositorio tienes especificadas todas las propiedades con terceras partes.

ENS	**TRAC**
Marco Operacional	*Criterio*
Servicios externos	
Gestión diaria [op.ext.2]	A5.3 El repositorio tiene especificadas todas las propiedades con terceras partes.

ENS	**TRAC**
Marco Operacional	*Criterio*
Servicios externos	
Medios alternativos [op.ext.9]	A5.3 El repositorio tiene especificadas todas las propiedades con terceras partes.

Continuidad del servicio

ENS	**TRAC**
Marco Operacional	*Criterio*
Continuidad del servicio	
Análisis de impacto [op.cont.1]	A3.2 Documentación detallada para revisión, actualización y mecanismos de desarrollo.

ENS	**TRAC**
Marco Operacional	*Criterio*
Continuidad del servicio	
Plan de continuidad [op.cont.2]	A3.2 Documentación detallada para revisión, actualización y mecanismos de desarrollo

ENS	**TRAC**
Marco Operacional	*Criterio*
Continuidad del servicio	
Pruebas periódicas [op.cont.3]	A3.4 El repositorio se someterá formalmente a revisiones periódicas y evaluación.

Monitorización del sistema

ENS	**TRAC**
Marco Operacional	*Criterio*
Monitorización del sistema	
Detección de intrusión [op.mon.1]	B6.2 Políticas de acceso. C3.2 Análisis de amenazas.
Ambos indicadores pueden ser válidos ya que implica disponer de políticas de acceso al repositorio monitorizando otro implica que la política esté implementada.	

ENS	**TRAC**
Marco Operacional	*Criterio*
Monitorización del sistema	
Sistema de métricas [op.mon.2]	C3.2 Análisis de amenazas.
En este caso implica que el plan de métricas esté desarrollado.	

Medidas de protección

Medidas de protección	Protección de las infraestructuras Gestión de personal Protección de los equipos Protección de las comunicaciones Protección de la información Protección de las aplicaciones informáticas Protección de la información

Tabla 4.Distribución de los indicadores en Medidas de Protección

Protección de las infraestructuras

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las infraestructuras	
Áreas separadas y con control de acceso [mp.if.1]	C3.2 El repositorio tiene implementado controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las infraestructuras	
Identificación de las personas [mp.if.2]	C3.2 El repositorio tiene implementado controles para las necesidades de seguridad definidas.
Aparte de ser una necesidad de seguridad como indica 3.2 también forma parte de la agrupación B6.5 donde se implementan las políticas de acceso.	

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de les infraestructuras	
Acondicionamiento de los locales [mp.if.3]	C3.2 El repositorio tiene implementado controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las infraestructuras	
Energía eléctrica [mp.if.4]	C3.4 Plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Medidas de protección	*Criterio*
Protecció de les infraestructuras	
Protección frente a incendios [mp.if.5]	C3.4 Plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las infraestructuras	
Protección frente a inundaciones[mp.if.6]	C3.4 Plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las infraestructuras	
Registro de entrada y salida de equipamiento [mp.if.7]	C3.4 Plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC. A pesar de ser una medida de Seguridad, también se podría agrupar con los indicadores C2.1 documentación de procedimientos o el indicador C1.7 documentación de procesos; mantenimiento y sustitución.	

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de les infraestructuras	
Instalaciones alternativas [mp.if.9]	C3.4 Plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

Gestión de personal

ENS	**TRAC**
Medidas de protección	*Criterio*
Gestión del personal	
Caracterización del lugar de trabajo [mp.per.1]	A2.1 y A22 Definiciones de la descripción del lugar de trabajo y roles y responsabilidades.

ENS	**TRAC**
Medidas de protección	*Criterio*
Gestión del personal	
Deberes y obligaciones [mp.per.2]	A2.2 Roles y responsabilidades.

ENS	**TRAC**
Medidas de protección	
Gestión del personal	Indicador
Concienciación [mp.per.3]	A2.2 Roles y responsabilidades.

ENS	**TRAC**
Medidas de protección	*Criterio*
Gestión del personal	
Formación [mp.per.4]	A2.3 Plan de formación continua y desarrollo profesional.

ENS	**TRAC**
Medidas de protección	*Criterio*
Gestión del personal	
Personal alternativo [mp.per.9]	C3.4 Plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

Protección de los equipos

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los equipos	
Puesto de trabajo despejado [mp.eq.1]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los equipos	
Bloqueo de puesto de trabajo [mp.eq.2]	C3.1 Evaluación regular de riesgos.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los equipos	Indicador
Protección de equipos portátiles [mp.eq.3]	C3.1 Evaluación regular de riesgos.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los equipos	
Medios alternativos [mp.eq.9]	C3.4 Plan de contingencia o plan de servicio continuado.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

Protección de las comunicaciones

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las comunicaciones	Indicador
Perímetro seguro [mp.com.1]	C3.2 El repositorio tiene implementado controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las comunicaciones	
Protección de la confidencialidad [mp.com.2]	C3.1 Evaluación regular de riesgos.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las comunicaciones	
Protección de la autenticidad y de la integridad [mp.com.3]	C3.1 Evaluación regular de riesgos.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las comunicaciones	
Segregación de redes [mp.com.4] Medios alternativos [mp.com.9]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

Protección de los soportes de información

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los soportes de información	
Etiquetado [mp.si.1]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los soportes de información	
Criptografia [mp.si.2]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los soportes de información	
Custodia [mp.si.3]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los soportes de información	
Transporte [mp.si.4]	C3.2 El repositorio tiene implementado controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los soportes de información	
Borrado y destrucción [mp.si.5]	C3.2 El repositorio tiene implementado controles para las necesidades de seguridad definidas.

Protección de las aplicaciones informáticas

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las aplicaciones informáticas	
Desarrollo de aplicaciones [mp.sw.1]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de las aplicaciones informáticas	
Aceptación y puesta en servicio [mp.sw.2]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

Protección de la información

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de la información	
Datos de carácter personal [mp.info.1] Calificación de la información [mp.info.2] Cifrado de la información [mp.info.3] Firma electrónica [mp.info.4] Sellos de tiempo [mp.info.5] Limpieza de documentos [mp.info.6]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas.

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de la información	
Copias de seguridad (backup) [mp.info.9]	C3.4 Planes de contingencia.
Los elementos marcados en gris son indicadores mínimos en TRAC.	

ENS	**TRAC**
Medidas de protección	*Criterio*
Protección de los servicios	
Protección del correo electrónico [mp.s.1] Protección de servicios y aplicaciones web [mp.s.2] Protección frente a la denegación de servicio [mp.s.8] Medios alternativos [mp.s.9]	C3.2 El repositorio tiene implementados controles para las necesidades de seguridad definidas. Añadidura de controles basados en la detección de riesgos continúa.

Capítulo 5

Marco teórico del modelo OAIS

5 Marco teórico del modelo OAIS

5.1 El modelo de preservación. El archivo OAIS

El modelo OAIS (CCSDS, 2002), ISO 14721:2003, creado por el Consultative Committe for Space Data Systems (CCSDS), es un modelo de referencia utilizado para la conservación y preservación de archivos digitales. . El CCSDS engloba a las agencias espaciales de Brasil, Canadá, China, Unión Europea, Francia, Alemania, Italia, Japón, Rusia, Reino Unido y Estados Unidos (la NASA). Este organismo define el OAIS de la siguiente manera: "*An OAIS is an archive, consisting of an organization of people and systems, that has accepted the responsibility to preserve information and make it available for a Designated Community.*"(CCSDS, 2002).

El modelo OAIS fue diseñado inicialmente para su uso dentro de la comunidad científica del espacio, teniendo como objetivo conservar digitalmente los datos provenientes de las misiones espaciales. Sin embargo, ha sido adoptado ampliamente por las bibliotecas, especialmente las de aquellos países que han participado en su elaboración (Woodyard, 2002), como la Biblioteca del Congreso de Estados Unidos, la Biblioteca Británica, la Biblioteca Nacional Alemana o la Biblioteca Nacional de Nueva Zelanda, que fue la pionera en implantarlo (Knight, 2009). Es por esto que el modelo OAIS tiene una amplia aplicabilidad para la preservación a largo plazo en cualquier contexto, incluido el sanitario.

Evidentemente, para poder implantar el modelo OAIS a una institución donde los recursos son limitados, se debe recurrir a su adaptación, para facilitar su aplicabilidad y su sostenibilidad financiera. Por ello, es imprescindible averiguar, en otras, las características del entorno, la formación de su personal o

la seguridad de sus datos. El principal objetivo de este estudio es precisamente este, plantear la adaptación de un modelo OAIS que se pueda aplicar a las entidades de gestión sanitaria para la conservación de sus historias clínicas electrónicas. En España, de acuerdo con la Ley de Autonomía Básica del Paciente (España, 2002), las historias clínicas deben ser accesibles durante un período de 5 años. El modelo OAIS, aplicado a las entidades sanitarias, permite cumplir este requerimiento legal.

El modelo OAIS incorpora la vigilancia tecnológica, la conservación digital y todos aquellos procesos que requieren que los documentos digitales existentes en un centro de datos no puedan ser sometidos a alteraciones, modificaciones o pérdidas. En el modelo OAIS se definen los actores dentro de un archivo, así como los flujos de información. Los actores que intervienen en un modelo OAIS son Productor (Producer), Gestor (Management) y Consumidor (Consumer).

Como se ha mencionado previamente, el modelo OAIS, es un modelo de conservación de objetos digitales que establece una serie de flujos de datos que determinan las obligaciones de un sistema de conservación a largo plazo para archivar y gestionar de los objetos digitales. Este modelo, hasta ahora, se ha considerado como un modelo válido de preservación digital, como queda patente en su extendida aplicación en la industria aeroespacial y en las bibliotecas digitales (McGray y Gallager, 2001). No se ha planteado todavía el hecho de que el modelo OAIS tenga que ser el único modelo de preservación digital, aunque sí hay autores que han indicado la posibilidad de una reducción o simplificación del mismo debido a la complejidad de su puesta en funcionamiento (Allinson, 2006; Spence, 2006).

No es objeto de este trabajo la descripción de cómo se ha llegado a ese modelo, ya que otros autores ya lo han hecho previamente (Lee, 2005). Pero si

es importante destacar que es un estándar que se somete a revisión cada cinco años y que, aunque exista una revisión en curso (conocida como versión Magenta), la versión actualmente oficial es la versión de 2002.

5.1.1 Productor, Consumidor y Gestor. Tres roles

OAIS como se han indicado anteriormente, define tres roles que interactúan con el archivo OAIS: Producer (Productor), Consumer (Consumidor) y Management (Gestor), además del propio archivo OAIS como se puede observar en la Figura 3.

El Productor es el encargado de enviar objetos digitales para su conservación a largo plazo. El Consumidor es el encargado de entender y acceder a la información que se va a acceder. El Gestor se encarga de las políticas de conservación, ingesta y acceso dentro de un archivo OAIS.

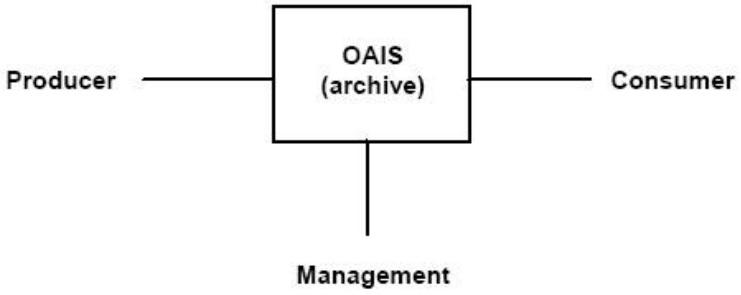

Figura 3. Entorno del modelo OAIS.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

En el caso de las entidades sanitarias, pueden surgir cambios a este entorno, ya que Productor y Consumidor y la entidad que representa al Gestor pueden pertenecer a la misma Comunidad Designada, es decir las personas o instituciones de una organización que se encargarán de las políticas de

conservación digital de los archivos médicos. En este caso, la Comunidad Designada es la constituida principalmente por el personal sanitario perteneciente a una organización sanitaria, hospital, centro de atención de día u otro tipo de centro y que genere información o acceda a ella. El Productor será el profesional o grupo de profesionales sanitarios que introducirán datos en las HCE a preservar y, en muchas ocasiones, serán ellos mismos los que recuperarán la información que han decidido conservar. Así, en este caso, tanto Productor, Consumidor y Gestor pueden coincidir. Es por esto que si se simplifica el modelo del archivo OAIS es posible que obtengamos un escenario parecido a la imagen de la Figura 4.

El Productor envía la información al archivo OAIS en paquetes llamados Paquetes de Información (Information Packages), es decir, información encapsulada en dos bloques diferenciados: el Contenido de la información (Objeto de Datos + Representación de la Información) (Content Information (Data Object + Representation Information)) y la Información de la Descripción de la Preservación (IDP) (Preservation Description Information (PDI)).

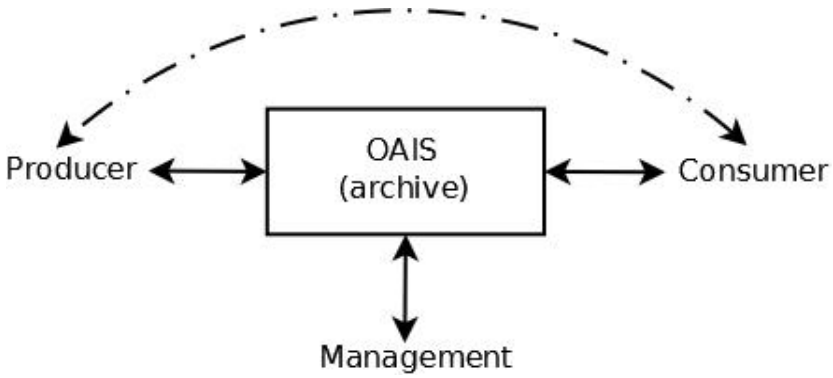

Figura 4. Posible entorno OAIS en una organización de gestión sanitaria.

El Productor es el actor encargado de realizar la ingesta de Paquetes de Información (Information Packages) al archivo OAIS. La Información de la Descripción de la Preservación (Preservation Description Information - PDI)

está formada por las identificaciones que indican la fuente de información, el contexto bajo en cual está hecha la información y un identificador único que identifica el Paquete de Información.

Por tanto, el PDI ofrece datos sobre el entorno en el cuál se ha creado la información, permitiendo asimismo proteger el contenido de la información para que permanezca inalterable. Como ejemplo tendríamos una HCE que pertenece al archivo pasivo. Esta HCE, en función de los datos que facilite un paciente, tendrá información en formato PDF o imágenes adjuntas. Así pues, las HCE que se quieran conservar a largo plazo tendrán que disponer de PDI para que su contenido se pueda mantener inalterable.

Los tres actores mencionados anteriormente, Productor, Consumidor y Gestor, no tienen porqué ser individuos. Pueden ser una institución, un ordenador o un individuo.

Si reflejamos la estructura de la Figura 4 trasladada a un archivo donde se custodian HCE y los tres actores fueran personas, el Productor se correspondería con el personal sanitario, el documentalista médico o el archivero encargado de introducir información en el archivo. En el caso del Consumidor, que es quién solicita la información, también sería personal sanitario, que incluso podría ser el mismo productor, dependiendo del proceso asistencial y del tiempo de custodia. En el caso del Gestor, el personal es distinto, al corresponder la gestión del archivo a una persona especializada que debe coordinar todas las políticas de preservación digital. Hay que tener en cuenta que, según las circunstancias bajo las cuales se ha generado información en una historia clínica, el consumidor y el productor pueden llegar a ser la misma persona. Esto se debe a que en un hospital se considera una historia clínica como pasiva (información no activa, por tanto archivada), una vez que

han pasado entre tres y cinco años de la finalización del proceso asistencial del paciente.

5.1.2 El modelo de información

El modelo OAIS se basa en la definición del modelo de información, para poder custodiarla posteriormente, con una serie de elementos funcionales que permiten conservar un archivo digitalmente, sin contemplar una tecnología concreta para su aplicación.

De acuerdo con la definición del modelo OAIS, hay dos conceptos importantes que hay que tener en cuenta. Estos son el Modelo de Información (Information Model) y la Comunidad Designada (Designated Community).

Para que un archivo OAIS pueda conservar información a largo plazo, ésta tiene que estar definida y representada de una forma clara. Esto quiere decir que la información ha de tener una transparencia técnica a todos los niveles, para que siempre se puedan tomar medidas adecuadas en caso de existir barreras tecnológicas o inaccesibilidad a los datos.

Un archivo OAIS representa todo el conjunto de información mediante dos elementos, el Objeto de los Datos (Data Object) y su Representación de la Información (Representation Information).

El Objeto de los Datos es la información a conservar a largo plazo, es decir, el contenido. La Representación de la Información es la forma en cómo será accedido ese objeto con información, el continente. Ambos representan la Base de Conocimiento (Knowledge Base).

Una Base de Conocimiento en un archivo OAIS permite que la información que se va a conservar a largo plazo se pueda entender y procesar. La Base de Conocimiento permite al archivo OAIS entender la información que se conserva a largo plazo. Por ejemplo, en una historia clínica electrónica (HCE), podemos encontrar una imagen de diagnóstico DICOM. La imagen es el conjunto de bits que compone esa imagen y su Representación de la Información es la forma de expresión del significado de esa imagen, su formato, la fecha en que se hizo, además de otros elementos descriptivos.

Para poder tener un archivo compatible con el modelo OAIS en un sistema de información de salud es necesario, de acuerdo con la documentación de OAIS, que el punto 1.4 "Conformance", el punto 2.2 "OAIS Information" y el apartado 3 "Responsibility" se cumplan. En un modelo OAIS reducido, los apartados necesarios son también los puntos antes mencionados: 1.4, 2.2 y 3 (CCSDS, 2002).

5.1.3 La Comunidad Designada

Una de las principales características del modelo OAIS es la definición de a quién va dirigido el archivo que conserva los materiales digitales a largo plazo, es decir, su público objetivo, denominada Comunidad Designada. Esta es una comunidad generadora y receptora de información, tal y como se menciona en la definición del modelo OAIS. El término Comunidad Designada puede ser definido como aquel conjunto de entidades personales o corporativas que serán capaces de entender el contenido de la información preservada digitalmente a largo plazo.

Así pues, una de las obligaciones que tendrá un archivo OAIS específico será la definición de la Comunidad Designada, que podrá interactuar con el archivo

OAIS y entender la información que se está preservando a largo plazo. Esto quiere decir que no sólo tienen que poder recibir la información que se ha conservado sino que han de tener la capacidad de entender esa información cuando sean los receptores de la misma. La capacidad de entender se extiende tanto a habilidades sintácticas, gramaticales y visuales, como a la competencia digital para poder acceder a ella. En cualquier caso, la Comunidad Designada debería poder entender la información conservada sin necesidad de soporte técnico.

Este hecho aporta, como valor añadido, que exista una uniformidad de criterios en el tratamiento de los objetos digitales que se espera sean homogéneos frente a la unidad de información que los trata, aunque los objetos digitales a conservar pueden ser heterogéneos entre sí. También permite definir una granularidad y especificidad a la hora de conservar documentos digitales.

En el caso de los archivos de las historias de salud electrónicas, la Comunidad Designada podrá ser principalmente el personal sanitario que pertenece a la propia institución y que necesita consultar las Historias Clínicas Electrónicas (HCE). El personal sanitario puede responder a diferentes perfiles profesionales, como médicos, investigadores y otros profesionales que trabajen en la entidad.

Respecto a los profesionales sanitarios y su pertenencia a la Comunidad Designada, es relevante el hecho de que en muchos casos serán esos mismos actores los generadores o productores de información. Incluso en algunos casos podría ocurrir que también el mismo profesional fuese Productor y Consumidor de la información custodiada en el archivo OAIS, tal como se indica en la Figura 4. Así pues, será determinante definir en las políticas de

acceso al archivo, la definición del nivel de información al cual puede acceder, así como el tipo de profesionales que puedan acceder.

Sin embargo, también hay que tener en cuenta a los pacientes que han sido atendidos en el centro. Si existe cierto grado de dependencia, los familiares de los pacientes también formarán parte de la Comunidad Designada ya que, en función de las normas y la legislación vigente de cada país, el paciente tiene derecho a acceder a sus datos a lo largo de su vida. A pesar de que los pacientes pueden pedir los datos de sus HCE a un hospital, no accederán de forma directa al archivo OAIS, que será gestionado por una entidad sanitaria o un tercero, pero si serán receptores de sus propios datos. Formarán parte de la Comunidad Designada, pero sólo como receptores finales. Otra cuestión a abordar es como se presenta a los pacientes esta información para que sea informacionalmente accesible.

También, en el caso de la sanidad, la Comunidad Designada aportará cierta simplificación en el OAIS Reference Model, al disponer de un lenguaje común para interpretar la información, ya que será la misma Comunidad la que produzca y consuma la información que ha generado. Asimismo, el acceso a la información por parte de toda esta Comunidad Designada se hará bajo la misma regulación legal.

5.1.4 Las entidades funcionales de un archivo OAIS

Una vez revisados los participantes en el modelo OAIS así como una parte de la definición del modelo de información, se hace necesario profundizar en el funcionamiento interno del modelo, empezando con las entidades funcionales. Un archivo OAIS puede ser una entidad única pero también puede comunicarse con otros archivos OAIS en el caso de archivos federados.

El modelo OAIS, se desglosa en un conjunto de seis entidades funcionales, que son Ingesta (Ingest), Almacenamiento de Archivo (Archival Storage), Gestión de Datos (Data Management), Administración (Administration), Planificación de la Preservación (Preservation Planning) y Acceso (Access), según se muestra en la Figura 5. Estas entidades funcionales son las que permiten preservar la información de acuerdo con el modelo de información definido. Dicho modelo de información especifica cómo hay que gestionar la información y cómo se transporta desde la entidad funcional de Ingesta de datos hasta la entidad funcional Acceso correspondiente. Además, existen un pequeño conjunto de responsabilidades obligatorias dentro de las entidades funcionales que son necesarias para disponer de la conformidad de un archivo OAIS, de acuerdo al modelo de información elegido.

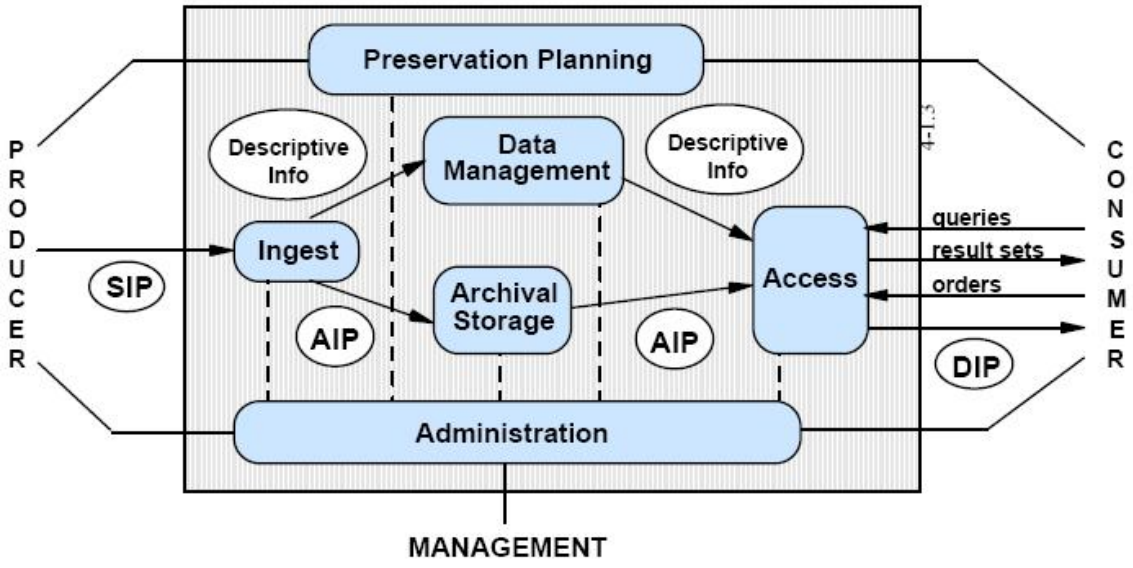

Figura 5. Entidades funcionales de OAIS.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

A continuación se explican los puntos más relevantes de cada entidad funcional, aunque su detalle se puede encontrar en la norma publicada por el CCSDS. En las imágenes que se adjuntan a cada entidad se muestran todos los detalles, no solo los relevantes, pues ello será necesario para la comprensión del modelo propuesto en el Capítulo 7.

5.1.5 Ingesta

Ingesta es una entidad que acepta la información de los Productores (Figura 6). El proceso de ingesta puede rechazar información del Productor si esta no está definida según el modelo de información de OAIS. En este proceso, interviene el Paquete de Información de la Submisión (Submission Information Package) (SIP), con los datos que proceden del Productor. El proceso ingesta genera un Paquete de Información de Archivo (Archival Information Package) (AIP) donde la información se prepara para ser archivada.

El funcionamiento del proceso de Ingesta se resume a continuación:

El Productor envía información al archivo en forma de Paquete de Información de la Submisión (SIP). Este es recibido por la función Recepción de la Submisión (Receive Submission), para después enviarlo al bloque de Verificación de la Calidad (Assurance Quality), con la misión de comprobar que coincide con el modelo de información y validar la entrada.

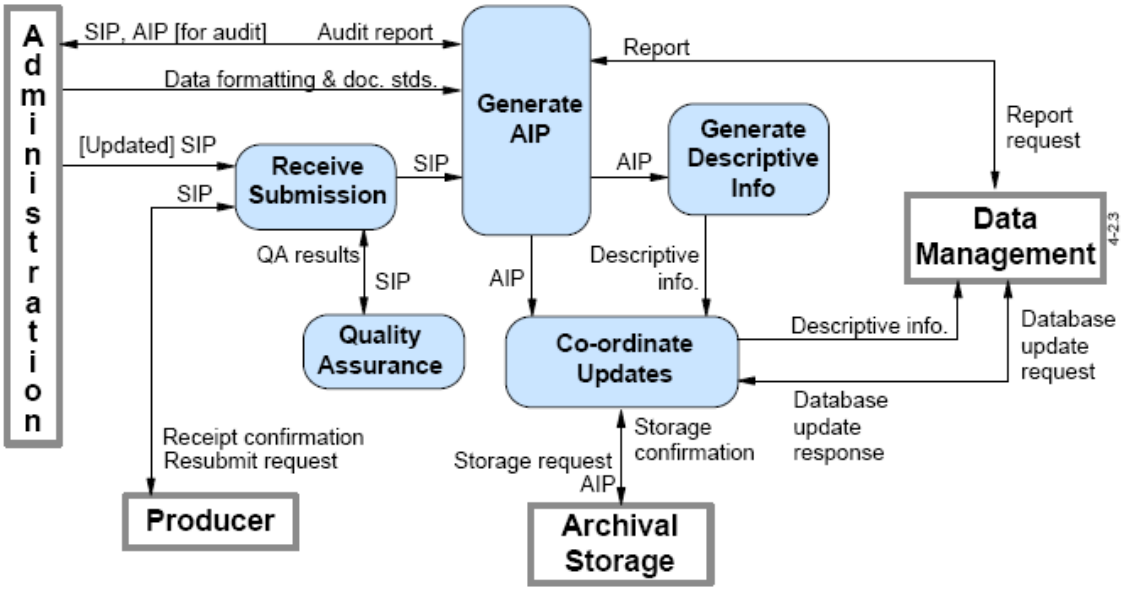

Figura 6. Función Ingesta.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

Una vez validado el SIP se traslada a la función Generar AIP (Generate AIP) donde se generan los datos correspondientes mediante la función Generar Información Descriptiva (Generate Descriptive Info). Estas dos últimas funciones son coordinadas por la función Coordinar las Actualizaciones (Co-ordinate Updates), que facilita que la información que haya sido enviada sea archivable y que el Paquete de Información se almacene en Almacenamiento de Archivo (Archival Storage). A su vez actualiza la base de datos de información mediante la función Gestión de Datos (Data Management).

5.1.6 Almacenamiento de Archivo

El Almacenamiento de Archivo es la entidad que recibe el Paquete de Información de Archivo (Archival Information Package) (AIP) y lo almacena en la base de datos del archivo OAIS.

La función Almacenamiento de Archivo, como puede apreciarse en la Figura 7, se encarga de recibir el AIP en la función Recibir Datos (Receive Data) y enviar una señal de Confirmación de Almacenamiento (Storage Confirmation) al bloque Ingesta.

A su vez, desde la entidad funcional Administración (Administration), se gestionan las políticas de acceso a través de las funciones Gestión de la Jerarquia de Almacenamiento (Manage Storage Hierarchy) y Substitución de Medios (Replace Media), que sirve para cambiar el soporte donde está la información y que esta no se pierda. Las funciones Comprobación de Error (Error Checking) y Recuperación frente a Desastres (Disaster Recovery) realizan actividades de notificación de errores y recuperación de copias del archivo, en caso de haber corrupción en los datos o en el soporte donde estos se alojan.

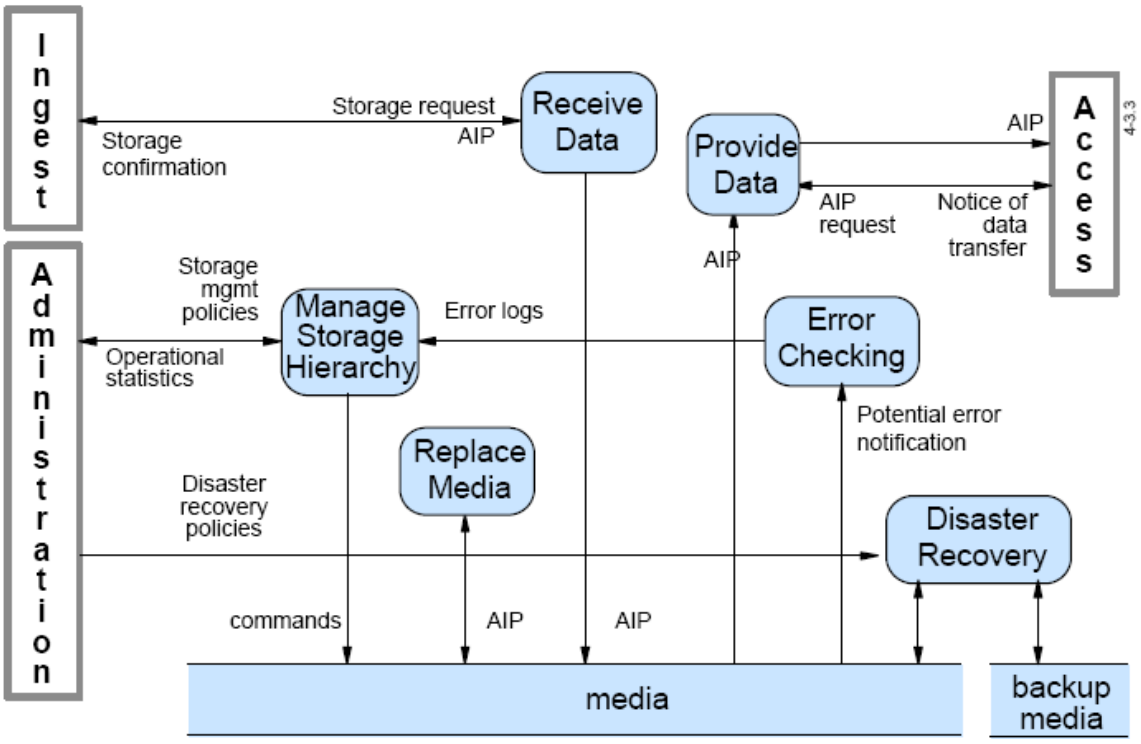

Figura 7. Función de Almacenamiento de Archivo.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

5.1.7 Gestión de Datos

La entidad funcional Gestión de Datos se encarga de actualizar la base de datos (Database) del archivo OAIS, así como de mejorar el acceso a la Información Descriptiva (Descriptive Information).

La función más relevante es Administrador de la Base de Datos (Administer Database), responsable de mantener la integridad de los datos, creando tablas o esquemas que soporten las funciones de Gestión de Datos (Data Management). También tiene un bloque denominado Recepción de la actualización de la Base de Datos (Receive Database Updates), implicado en la notificación de la actualización de la base de datos a las entidades funcionales Ingesta y Administración.

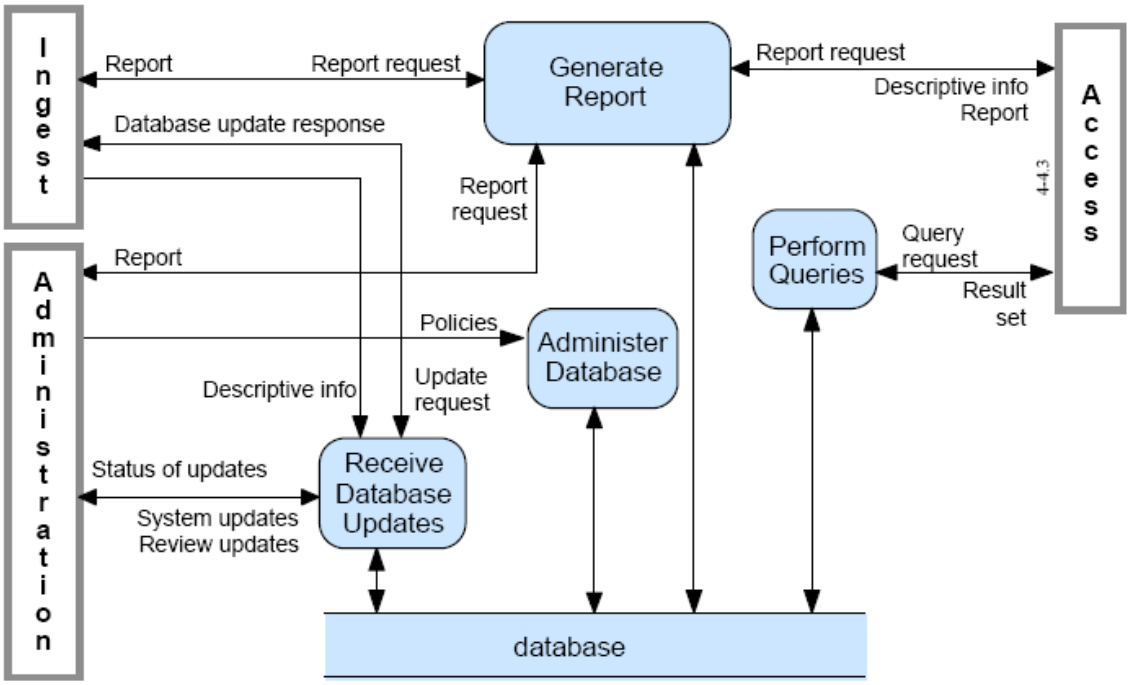

Figura 8. Función Gestión de Datos.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

Dispone también de la función Realización de Peticiones (Perform Queries), que ofrece resultados de recuperación de información a la entidad funcional Access. La función Genera Informe (Generate Report) es la encargada de realizar todo tipo de informes sobre los datos o estadísticas a las entidades funcionales Ingesta, Administración y Acceso como se puede ver en la Figura 8.

5.1.8 Administración

Administración es una entidad que se encarga de realizar todo el mantenimiento del archivo OAIS. Esto es, la ejecución de las operaciones de archivo o la migración/actualización de los datos archivados. Este proceso se ilustra en la Figura 9.

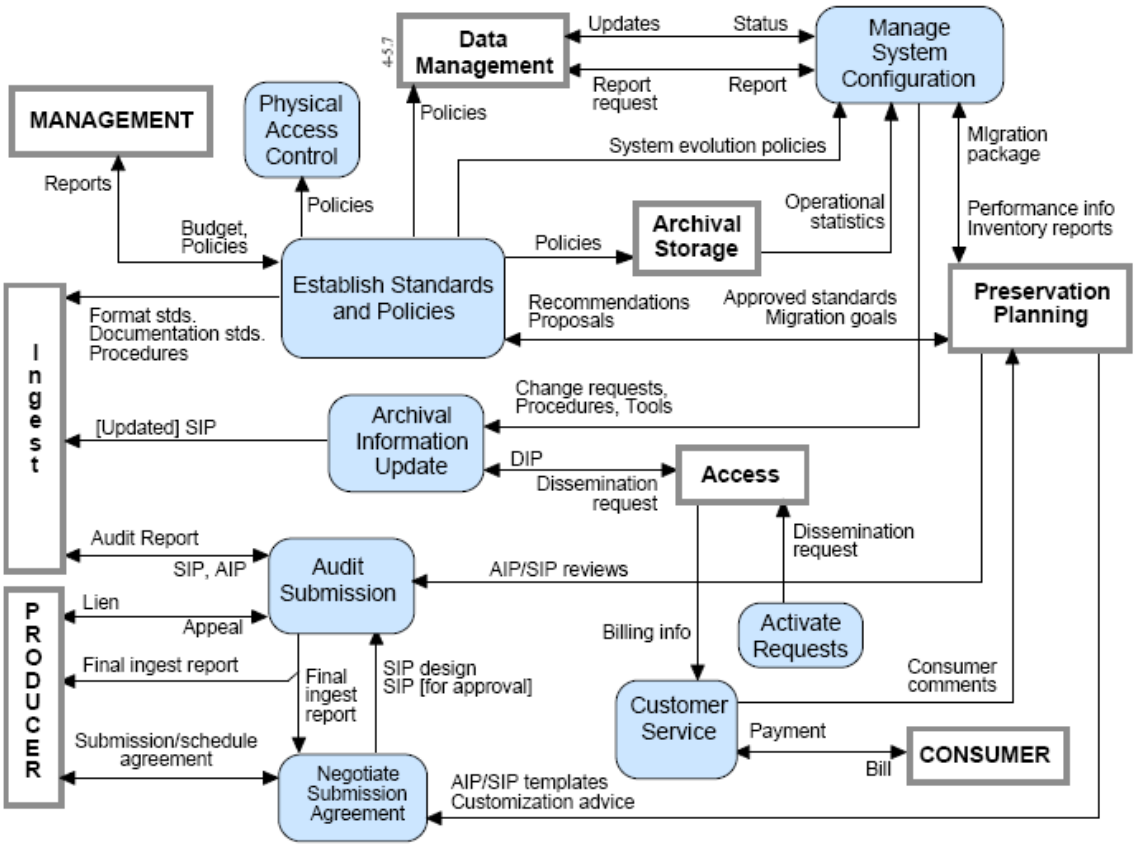

Figura 9. Función de Administración.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

En esta entidad funcional están involucrados todos los actores del modelo OAIS ya que Administración se encarga de la gestión de todos los flujos de políticas de los datos que se van a archivar. Así, es responsable de mantener la integridad y la trazabilidad de la configuración durante las fases del ciclo de vida de los documentos. También permite gestionar tanto los procesos de auditoría, para verificar la calidad de los archivos, como las políticas de archivos y verificación de estándares.

5.1.9 Planificación de la preservación

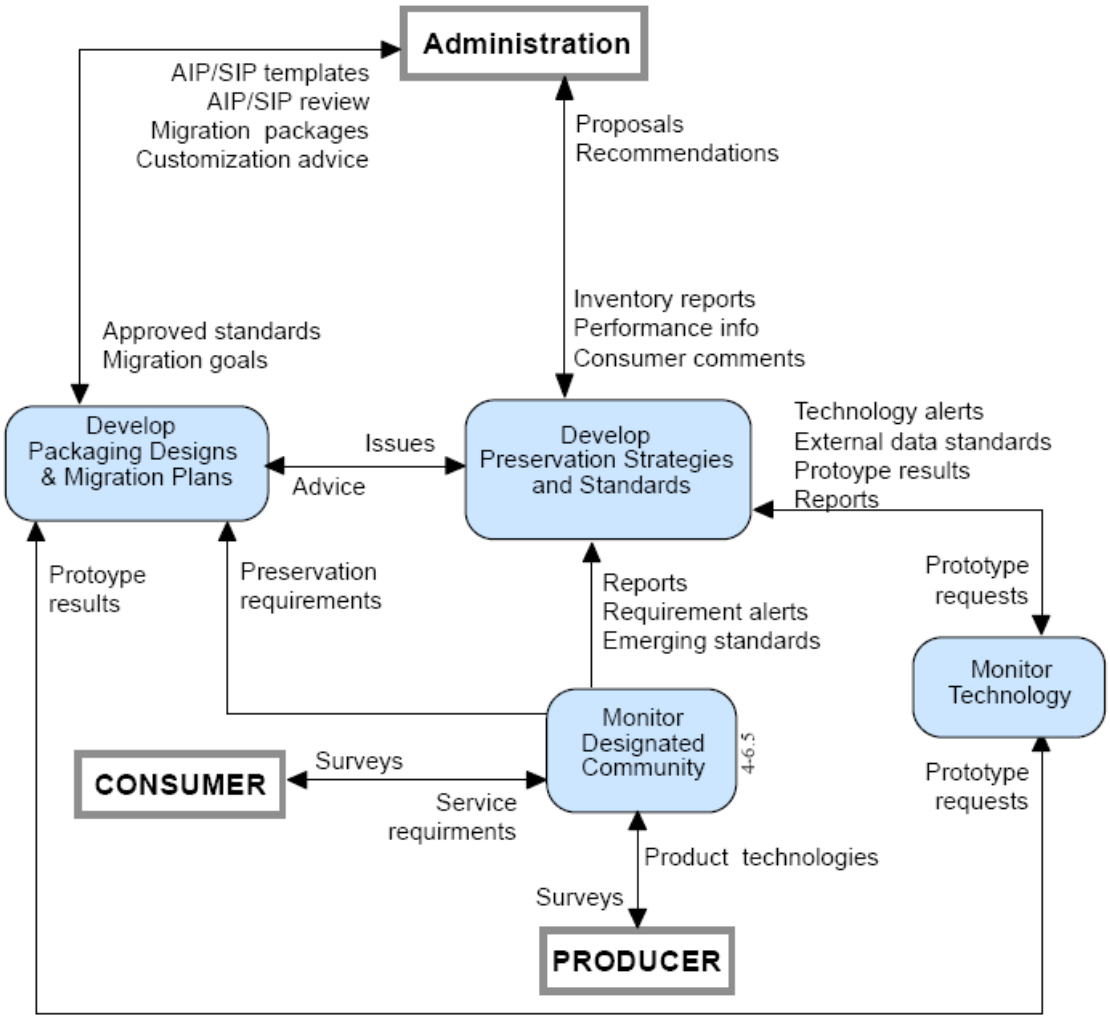

Figura 10. Función de Preservation Planning.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

La Planificación de la Preservación (Preservation Planning) es la entidad que monitoriza los servicios del archivo OAIS como asegurar que la información sea accesible, a largo plazo para la Comunidad Designada. También se encarga de realizar recomendaciones de mejora del archivo y permite la monitorización de los nuevos avances en la tecnología, para poder aplicar después nuevas políticas de preservación y estándares. Todo este proceso se ilustra en la Figura 10.

5.1.10 Acceso

Acceso (Access) es la entidad funcional que facilita servicios a los Consumidores para que puedan recibir y entender la información que solicitan.

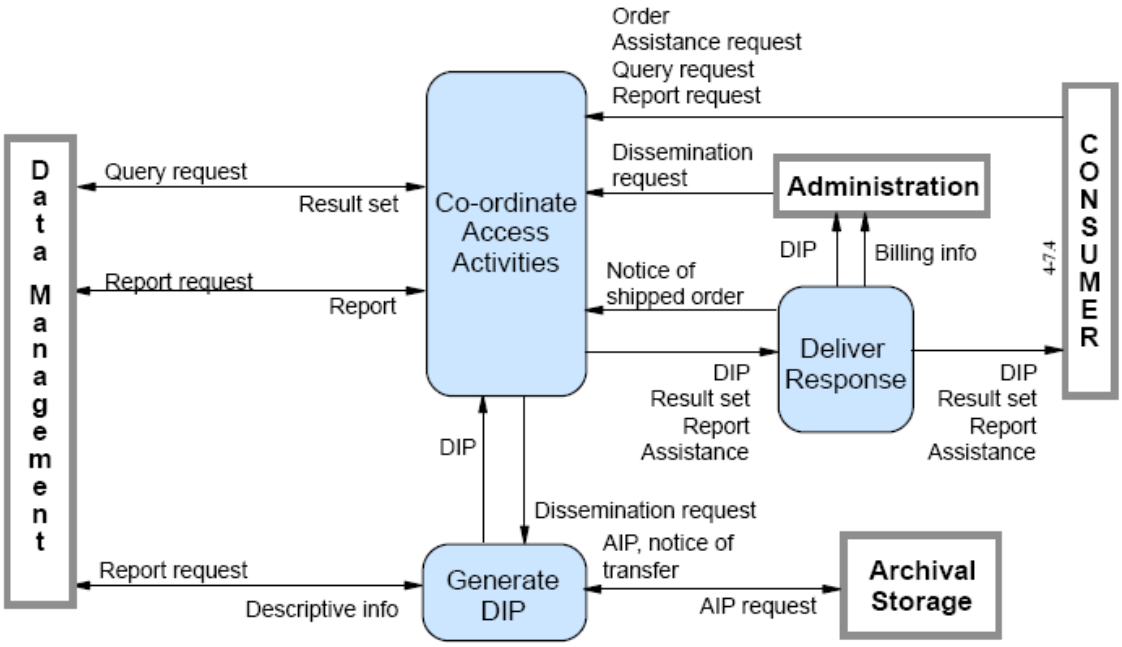

Figura 11. Función de Acceso.

Reimpreso con permiso del Consultative Committee for Space Data Systems.

Esta última función coordina las actividades de acceso de información, recuperando y generando un Paquete de Información, el Paquete de

Información de Diseminación (Disseminated Information Package) (DIP), para que el Consumidor pueda disponer de la información que requiere, tal y como se ilustra en la Figura 11. Los datos que recibirá el Consumidor serán una copia exacta de la información introducida en el archivo OAIS, pero es posible que esta información pueda estar representada en un formato diferente al original.

5.1.11 Iniciativas y retos en el diseño e implantación de archivos OAIS

El modelo OAIS, como se ha mencionado previamente, tiene un uso muy extendido en la industria aeroespacial y en las bibliotecas digitales, pero existen iniciativas en diferentes ámbitos como la astronomía, las matemáticas, la aeronáutica, los archivos digitales o incluso en la nube.

En el campo de la astronomía (Gray, 2011) se cuestiona el término largo plazo en relación a la definición existente en el modelo OAIS. Esta cuestión se pone de relevancia especialmente en proyectos científicos con un gran volumen de datos.

En el campo de las matemáticas, en el proyecto MathArc (Cornell University, 2004), se propone la preservación de elementos de las ciencias matemáticas creando metadatos especializados para ello. A su vez, se están desarrollando representaciones digitales centradas en la geometría, para conservar datos creados digitalmente en trabajos de ingeniería como el CAD (Regli et al., 2009).

En el campo de la aeronáutica, se plantea un modelo de conservación a largo plazo de datos geoespaciales, a escala nacional, en los Estados Unidos (Jan'ee, 2008). El modelo presenta una aproximación mínima y está basado en las influencias del modelo OAIS. En este caso, la diversidad de datos que suponen los formatos de datos digitales de los objetos geoespaciales, plantean muchos retos a nivel de capacidad, gestión de los formatos, usabilidad y límites en el

ancho de banda en la transferencia de datos en el caso de datos muy voluminosos (como el material gráfico con sonido, fotografía o su representación en forma de video). Con el fin de optimizar el tiempo de ingesta, se ha creado un software tipo "crawler", que rastrea unidades enteras de disco, identificando y empaquetando el material para su posterior envío y preservación.

También en los archivos digitales se aplica OAIS, como es el caso de los archivos nacionales holandeses, que han creado el e-Depot, con el núcleo del sistema planteado por IBM, llamado Digital Information Archiving System (DIAS) (Oltmans, 2004). Este repositorio sirve, entre otras finalidades, para preservar publicaciones digitales de diferentes grupos editoriales.

Para finalizar, también se aplica el modelo OAIS en la nube (Askhoj, 2011). Se ha planteado un modelo en Japón para la compartición de datos entre unidades de archivos en la nube, que permitirá transferir datos entre agencias del gobierno de Japón y los archivos nacionales. Los datos transferidos por las diferentes unidades estatales tienen que ser transformados al modelo único de información del archivo. Esto se debe a la disparidad tanto de sistemas informáticos como de los modelos de información que tienen las agencias gubernamentales japonesas. Este modelo en la nube puede ser válido para determinado tipo de documentos, pero de difícil aplicación en un entorno médico donde los datos personales han de estar altamente protegidos.

El modelo de referencia OAIS se ha probado también en proyectos para uso personal, mediante la utilización de software de uso habitual. Una base de datos estándar (DBMS), podría soportar una amplia gama de formatos a fin de organizar un archivo OAIS en un entorno integrado y de forma homogénea (Rödig et al., 2003).

En otro contexto, la conservación de datos de vídeos digitales plantea la creación de un modelo de información dentro del modelo OAIS para la preservación de este tipo de materiales (Lee et al., 2006).

Como se ha visto hasta ahora, cada proyecto tiene que abordar varias problemáticas respecto a sus objetos digitales, especialmente cuando se trata de introducir datos en el sistema de información que va a procesar, posteriormente, los datos.

5.1.12 Tecnología empleada en el modelo OAIS

Uno de los aspectos relevantes en el diseño de un archivo OAIS es el uso de la tecnología que, en un archivo OAIS, ha de servir tanto para los sistemas de almacenamiento como para la manipulación de los objetos digitales que conviven en el archivo. En este punto, hay que tener en cuenta que la tecnología empleada se ha dirigido hacia proyectos orientados a bibliotecas o archivos digitales, la industria aeroespacial o la astronomía.

En el campo de la astronomía, el proyecto SI2tools[35], desarrollado por el Centre national d'études spatiales (CNES), permite crear directamente un archivo OAIS y posteriormente federar el desarrollo de la herramienta para que laboratorios científicos tengan su propio modelo. La herramienta se soporta en tecnología JAVA.

En el campo de los archivos podemos encontrar los proyectos RODA y CRIB (Ramalho et al., 2008), aplicados en el Archivo Nacional de Portugal, un sistema de preservación digital para imágenes en formato JPG, documentos electrónicos en Word y en PDF. El repositorio está basado en el software Fedora con la base de datos PostgreSQL.

[35] http://sourceforge.net/projects/sitools2/ [consulta: 8 de marzo de 2012]

Otro modelo tecnológico basado en OAIS es el proyecto realizado por la National Library of New Zealand (Knight, 2010), donde se elabora un modelo propio y se adopta un sistema de software desarrollado en tecnología JAVA y un esquema propio de metadatos, comercializado posteriormente por la empresa Ex Libris.

Respecto a los metadatos, se ha de indicar que se han desarrollado esquemas de metadatos para preservación digital. Una de las razones por la que se han creado diversos modelos de metadatos es porque el modelo OAIS no define una tecnología en concreto, así que para cada modelo de datos es posible encontrar diferentes iniciativas. Entre éstas, se puede mencionar Metadata Encoding and Transmission Standard (METS), mantenido por la Library of Congress y que se utilizan en la transmisión de datos; XML Formatted Data Unit (XFDU), standard[36] desarrollado por el CCSDS y que se acerca al modelo de información del OAIS; MPEG-21 que sirve para empaquetar datos multimedia; y PREMIS [37], un diccionario de datos para registrar los metadatos de preservación.

Respecto a los sistemas de gestión del almacenamiento, también se ha desarrollado software como DSpace[38] o Fedora (Tansley et al., 2003). DSpace es un sistema de almacenamiento desarrollado por MIT Libraries y Hewlett-Packard Laboratories. DSpace utiliza los metadatos METS. Fedora[39] inicialmente fue diseñado para el almacenamiento de objetos digitales multimedia. Tiene sus propios sistemas de metadatos, aunque permite la inclusión de metadatos MPEG-21 y METS. Estas dos iniciativas, DSpace y Fedora disponen de software que se puede personalizar según las necesidades,

[36] http://sindbad.gsfc.nasa.gov/xfdu [consulta: 8 de marzo de 2012]
[37] http://www.loc.gov/standards/premis/ [consulta: 8 de marzo de 2012]
[38] http://www.dspace.org [consulta: 8 de marzo de 2012]
[39] http://www.fedora-commons.org [consulta: 8 de marzo de 2012]

pero la modificación de este software requiere de personal cualificado, ya que no es inmediata.

Se puede ver pues, que a pesar de que OAIS no recomienda ninguna tecnología en concreto, existen diversas aplicaciones al respecto, con soluciones tecnológicas distintas.

5.2 La gestión de riesgos

La gestión de riesgos es una forma metodológica de prever errores de diversa índole en una organización. De esta manera, se pueden prever sucesos que pueden ocurrir de una forma u otra y se puede reaccionar antes de que los hechos sucedan. La gestión de riesgos es un proceso continuo dentro de una organización que permite identificar y analizar los riesgos así como su impacto, aceptando después el mismo, mitigándolo o limitándolo. En definitiva, la gestión de riesgos permite disponer de los elementos de juicio y de las herramientas necesarias, de forma cuantitativa o cualitativa, para evitar incidentes que perjudiquen a la organización.

En una organización, los incidentes pueden ser múltiples, por lo cual es necesario conocer de antemano que puede ocurrir bajo determinadas circunstancias y cómo reaccionar ante las mismas. A modo de ejemplo, se indica el estudio de las causas y circunstancias que pueden suceder si hay un incendio en una instalación, a qué afectará y qué medidas preventivas o reactivas se podrán tomar. En el proceso de gestión de riesgos habrá que valorar, por ejemplo, qué causas pueden provocar un incendio (riesgo), analizar ese riesgo (impacto o evaluación) y planificarlo (mitigación, aceptación o limitación del riesgo).

En el ámbito de la gestión de riesgos hay que diferenciar los pasos a realizar. Así, la identificación, el análisis, la planificación, la monitorización y el control de riesgos, permitirán su gestión en conjunto dentro de una organización.

Es posible evaluar los riesgos en una organización de diferentes formas, pudiendo ser a nivel de producto, proceso, sistema de información o a nivel estratégico. Existen diversos modelos de gestión de riesgos que diferencian estos distintos niveles. Así, tenemos métodos de evaluación de riesgos cualitativos, cuantitativos (Greenfield, 2000) o la combinación de ambos.

El propósito de este apartado es conocer qué es la gestión de riesgos en los sistemas de información, los estándares y metodologías más utilizados. Se realizará una breve mención de algunas de ellas, ya que existen muchas y variadas. Se incidirá en aquellas metodologías que pueden orientarse a la preservación digital. Se pondrá de manifiesto el software existente que ayude a la evaluación de riesgos. Finalmente se expondrá una evaluación de riesgos que se ha realizado a las ocho entidades que han colaborado en el estudio. El objetivo de dicha evaluación de riesgos es disponer de argumentos que ayuden posteriormente a la creación de la propuesta del archivo OAIS adaptado a las entidades de gestión sanitaria y, en concreto, a sus hospitales.

5.2.1 Diferentes definiciones vinculadas a la gestión de riesgos

La primera norma que se creó para la gestión de riesgos fue la norma AS/NZS 4360:1995, que posteriormente ha evolucionado a la norma AS/NZS 4360:2004 para convertirse finalmente en la norma ISO 31000:2009. En esta última documentación se puede encontrar la definición de riesgo:

"efecto de la incertidumbre en los objetivos"

El efecto puede ser positivo o negativo y los objetivos pueden tener diferentes aspectos como salud, finanzas, seguridad o preservación digital, pudiéndose aplicar en diferentes niveles como el estratégico, técnico o a un proceso determinado. Así pues, el riesgo se asocia a la probabilidad de que este suceda.

Según el diccionario de la Real Academia de la Lengua Española el riesgo es "*Contingencia o proximidad de un daño*". Esta definición supone un enfoque diferente, más abierto, ya que si bien existe el concepto de daño, este no está claro sobre que incide.

De acuerdo con la Metodología MAGERIT la definición de riesgo es

> "*estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización*".

Así pues, disponiendo de varias definiciones sobre el riesgo, donde se sabe que es un grado de exposición o incertidumbre sobre un objetivo o activo de una organización y que puede causar deterioros en la misma, se puede pensar que el riesgo hay que analizarlo y posteriormente gestionarlo. De esta forma, se observa el análisis de riesgos como forma de evaluación de posibles peligros en una organización o sistema información y la gestión de riesgos, para actuar frente a los posibles peligros analizados previamente.

5.2.2 Formas de gestionar el riesgo

En la revisión de la literatura se han encontrado diferentes formas de ver el riesgo, según el tipo de organización y los objetivos a analizar. Debido a la naturaleza de este estudio, se centra la revisión en los análisis de riesgos vinculados a bibliotecas, sistemas de información y entidades sanitarias,

cubriendo diferentes aspectos, como la seguridad o los riesgos derivados en la información a organizaciones en su conjunto.

Centrándonos en los sistemas de información, podemos encontrar los riesgos aplicados a un entorno web, donde se exponen las limitaciones respecto a la evaluación de riesgos de seguridad, definiendo para cada apartado de seguridad, sin que sean excluyentes, los riesgos que pueden existir (Boja y Doinea, 2010). Otros autores proponen una aproximación del patrón de activos a proteger de un entorno web mediante el patrón de Simon, donde comparando las metodologías de análisis de riesgos MAGERIT y EBIOS, se propone que en un patrón de análisis de riesgos en un entorno web sea lo más simple posible (Romero et al., 2008), aplicando diferentes metodologías que ayuden a la valoración del riesgo. En otro ámbito, se expone la gestión de riesgos en los procesos de negocios de una universidad (Roşca, Năstase y Mihai, 2010), donde se índice en el modelo económico.

Por otro lado, en el diseño de los sistemas de información, se discuten los niveles de riesgo que se experimentan en una organización a la hora de diseñar un sistema de información, a la vez que se propone un marco de análisis de riesgos relacionando el contexto de la organización, así como los aspectos que influyen en los sistemas de IT y los beneficios que puede suponer dicho análisis (Willcocks y Margetts, 1994).

En el ámbito de las bibliotecas, en la British Library se aplicó el estándar AS/NZS 4360:2004 al repositorio digital, a fin de poder entender mejor los posibles problemas con los soportes de los objetos digitales. De esta forma, se pudo exponer un plan y sus estrategias para mitigar los riesgos en las colecciones digitales. El estudio se completó combinando los resultados obtenidos con las tablas de riesgo expuestas por la metodología Digital

Repository Audit Method based on the Risk Assessment (DRAMBORA) (McLeod, 2008).

De esta forma también se propone un proceso de evaluación del riesgo del ciclo de vida de la información (Bernard, 2007), para afrontar los riesgos que existen no sólo en la información electrónica, sino en aquella que no lo es, pero que es crítica en una organización.

En el ámbito de los sistemas de información de la salud, se dispone un marco de evaluación de análisis de riesgos (Sicotte et al., 2006) en el que se propone cinco dimensiones. Se identifica una relación de calidad entre la gestión del riesgo y el nivel de beneficios en un proyecto de creación de un sistema de información clínica. En otro caso, se facilitan una serie de dimensiones con sus riesgos asociados, que afectan al desarrollo de software de los sistemas de información clínica (Paré et al, 2008).

También se propone un sistema cuantitativo de métricas de valoración del riesgo en sistemas de información de salud centrados en el paciente, es decir, sistemas de información que gestionen las historias clínicas personales (Huang et al., 2008). Esto facilita el desarrollo de los procesos de valoración del riesgo para sistemas de salud centrados en el paciente.

Respecto a la comparación de las diferentes metodologías de gestión de riesgos, se puede encontrar una comparación de las metodologías Mehari, MAGERIT, NIST800-30 y Microsoft's Security Management Guide (Syalim, Hori y Sakurai, 2009), llevando a cabo una revisión de los pasos realizados por las metodologías. En tres de ellas, Mehari, MAGERIT y Microsoft's Security Management Guide, se echan en falta una serie de elementos, como recomendaciones de control, así como una guía de valoración del riesgo. También se realiza una comparación sobre la metodología de programación

Metricav3 y MAGERIT, identificando similitudes en la valoración de riesgos entre ambas, vistas además como complementarias (Sierra et al., 1999).

Capítulo 6

Análisis de las necesidades de preservación digital de las entidades sanitarias

6 Análisis de las necesidades de preservación digital de las entidades sanitarias

6.1 Presentación inicial de las instituciones

En este capítulo se expondrán los diferentes resultados obtenidos a través de las distintas fuentes de información utilizadas: cuestionario preliminar como primera aproximación (Anexo II), cuestionario de auditoría sobre las necesidades de preservación digital basado en el Esquema Nacional de Seguridad y TRAC (Anexo III), así cómo posteriores entrevistas realizadas a las entidades que han colaborado en este proyecto de investigación. Los resultados se presentan en forma de tabla, exponiendo primero los obtenidos en la encuesta facilitada a los centros hospitalarios y la valoración de los mismos.

A lo largo de este proyecto de tesis han participado una serie de instituciones que han colaborado activamente en la recopilación de datos para la propuesta del modelo teórico. Las ocho entidades que han participado, en orden alfabético, son:

- Consorci Sanitari del Maresme
- Consorci Sanitari de Terrassa
- Corporació Sanitària Maresme i la Selva
- Departament d' Obstetrícia, Ginecologia i Reproducció, Institut Dexeus
- Fundació Pere Mata
- Grup Sagessa

- Hospital Sant Joan de Déu
- Mútua de Terrassa

Previo al análisis sobre las necesidades de preservación de las instituciones de gestión sanitaria, se expone la tipología de centro hospitalario en Catalunya y la primera aproximación a estos mediante la encuesta preliminar. Posteriormente, se facilitan datos sobre su estructura como hospitales, centros sociosanitarios o centros de atención primaria; también la cobertura en población de todas las entidades y el margen de territorio que abarcan, así como y números de camas disponibles en el caso de los hospitales.

6.2 Tipología de las entidades sanitarias en Catalunya

En este estudio, se expone un marco de referencia en preservación digital para entidades sanitarias catalanas de tipo mediano o pequeño. Para establecer la definición de entidad pequeña-mediana pasaremos a describir qué tipo de clasificación podemos disponer en España y en Catalunya.

El Ministerio de Sanidad, Servicios Sociales e Igualdad establece una clasificación de los hospitales españoles por número de camas por hospital, sin atender a su especialización ni a recursos asistenciales. Por otra parte, en Catalunya, se dispone además de otra clasificación en función de la atención a los ciudadanos y de los recursos con que cuenta el hospital (Catsalut, 2009), independientemente de su titularidad.

Se puede encontrar en la literatura como está distribuido el sistema sanitario catalán y, en concreto, los hospitales (Safina, 2003). Así, se puede observar que se dispone de hospitales generales básicos, hospitales de referencia y hospitales de alta tecnología, como se refleja más adelante en la Figura 12. Existen dos

subdivisiones adicionales: los hospitales aislados geográficamente o que pertenecen a una red de salud complementaria, además de los hospitales ligeros -denominación ésta de nueva creación-. En el momento de realizar este proyecto sólo existe un hospital del denominado ligero en la población de Cambrils (Tarragona). Las tipologías de centros mencionadas se caracterizan por los siguientes rasgos:

Hospital general básico: hospital que atiende a las cuatro quintas partes de una población de referencia.

Hospital de referencia: hospital destinado prácticamente a resolver la totalidad de los problemas de salud de curación y mejora, fuera de aquellos que requieren recursos tecnológicos de alto nivel o una práctica altamente especializada. Tiene que haber uno por cada población de referencia de cuatrocientos mil habitantes.

Hospital de alta tecnología: es aquel que dispone de superespecialidades y de nuevas tecnologías diagnóstico-terapéuticas. Atiende a los pacientes que no se pueden tratar en los hospitales de referencia. Hay un hospital de alta tecnología por cada millón y medio de habitantes.

Hospital ligero: centro de salud que acerca la atención especializada y urgente a la población en un proyecto basado en la accesibilidad y la resolución. Potencia la integración con la atención primaria de la salud. Como hospital, permite una mayor resolución de la atención primaria, disponiendo de procesos más ágiles. Son hospitales cuya organización se basa en la innovación tecnológica y organizativa.

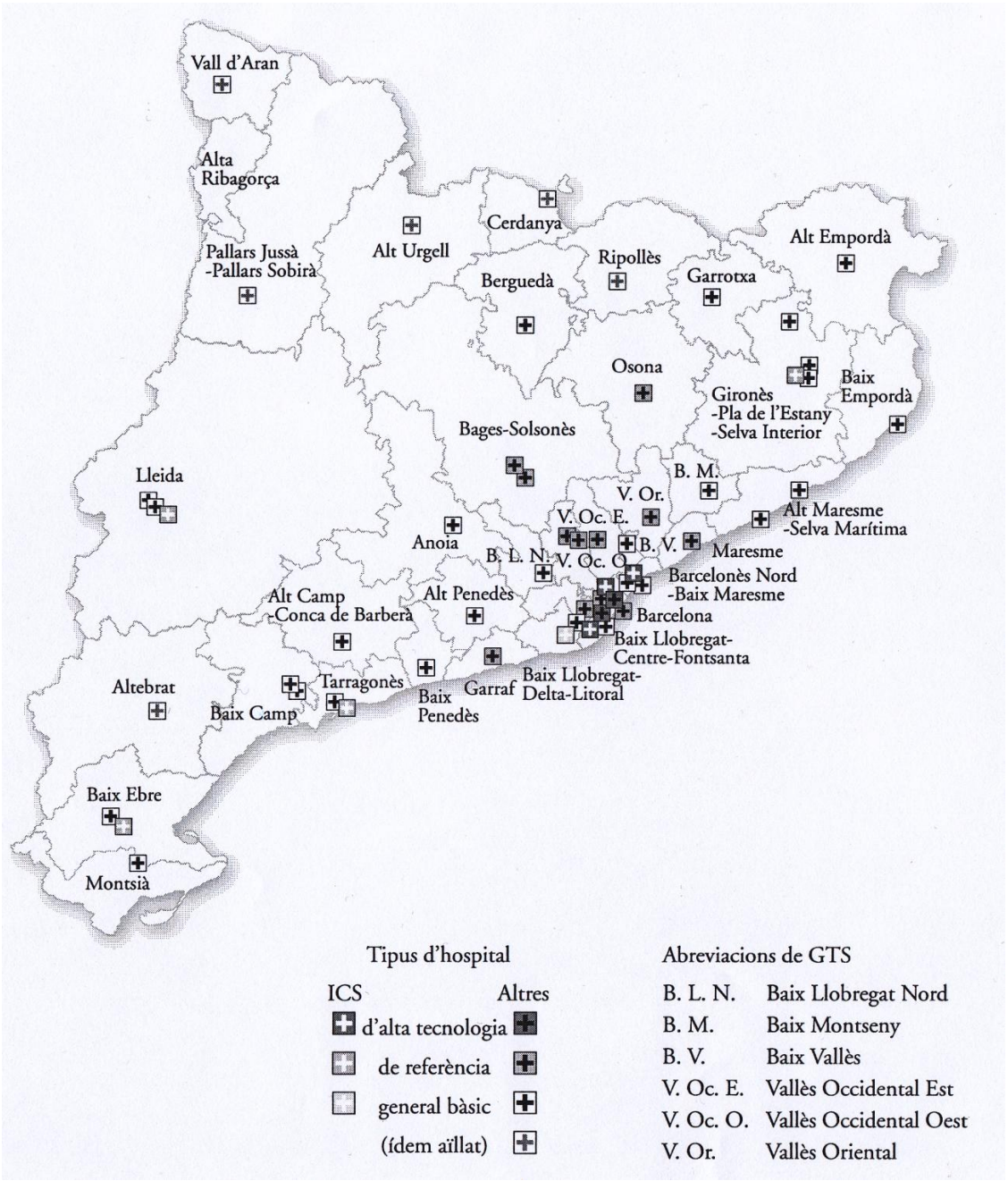

Figura 12. Mapa de distribución de los hospitales de Catalunya por nivel y titularidad.

Imagen extraída del libro "Els sistemes de pagament de la sanitat pública a Catalunya, 1981-2009: evolució històrica i perspectives de futur". *Reimpreso con permiso del Departament de Salut de la Generalitat de Catalunya.*

6.3 Primera aproximación

En la primera aproximación se realizó una encuesta preliminar a doscientas cuatro entidades de Catalunya, con las que se obtuvieron los resultados que se comentan a continuación. Todos los datos recogidos correspondientes a esta primera aproximación se encuentran en el Anexo II, tanto las preguntas como la explotación de los resultados.

Dadas las circunstancias y el entorno de trabajo así como los tipos de datos, se puede afirmar que las entidades encuestadas disponen de un modelo de gestión de información digital para la creación de historiales médicos electrónicos así como de otros documentos[40]. También se ha podido verificar que existe conciencia sobre el volumen de datos que manejan. Además, se denota cierta preocupación por los archivos médicos y su contenido, bien en forma de historias clínicas u otros documentos, como informes de investigación y pruebas médicas.

De forma generalizada, se desconocen los estándares existentes en la conservación digital. Esta afirmación está soportada por la respuesta a la pregunta 3 (Anexo II), donde el 40,38% de los encuestados indica que aplica como normativa de custodia o normativa de almacenamiento la Ley Orgánica de Protección de Datos (LOPD).

Respecto a quién elabora las respuestas, está el personal vinculado la Dirección con un 15,4% y la Administración con un 3,8%, pensando que son los gestores económicos de los centros sanitarios y, por tanto, con cierta preocupación por sus datos, ya que son su núcleo de negocio. Por otro lado, los sistemas de información, informática o el departamento de sistemas con un 29,8%, que son los encargados de la custodia de los archivos digitales.

[40] Ver Anexo II

Respecto al personal que realiza la custodia de los datos clínicos, un 38,46% de las entidades disponen de más de dos personas para custodiar o almacenar los objetos digitales en los archivos sin que se especifique su perfil profesional ni el departamento con el que están vinculados a este respecto.

Por lo que se refiere al corpus documental, destaca el uso de bases de datos para la gestión de las HCE, con un 67,31%, así como la alta disponibilidad de imágenes radiográficas en el formato DICOM, con un 61,54% el empleo de documentos en formato Word, con un 51,92%, y Excel con un 36,54%. Destaca especialmente la baja utilización de documentos en formato PDF, con un 19,22%. Esta cuestión es relevante, teniendo en cuenta que un documento en formato PDF aporta más seguridad inicial que un documento Word, ya que los datos contenidos no pueden ser manipulados fácilmente.

6.4 Presentación del proyecto a las entidades sanitarias

La presentación del proyecto a las entidades sanitarias fue acogida inicialmente de forma muy positiva, pues en general tenían presente su obligación de custodiar sus historias clínicas, esfuerzo que recae siempre sobre el departamento de informática. Esta dependencia se explica por el hecho de que las HCE se generan gracias al departamento de informática, mediante el uso de diferentes tipos de herramientas de software, y, por tanto, al final es este mismo departamento el que las gestiona. En el futuro habrá que ver la evolución de esta situación y las funciones asumidas tanto por los responsables de archivo médico, que tendrán que gestionar el archivo digital, como por el departamento de informática. En cualquier caso, durante la elaboración de este proyecto, han participado tanto personas responsables de archivo médico como directores de informática, algunos con conocimientos en preservación digital y otros no.

Durante todo el proyecto ha existido la participación de las personas responsables de archivo médico y directores de informática, algunos con conocimientos en preservación digital y otros no.

A la especialidad de responsable de archivo médico se llega después de los estudios de medicina y estudios posteriores de postgrado en archivo médico o por otras vías. Por tanto no se puede asegurar que las personas encargadas de los archivos, tengan conocimientos técnicos. Es importante recalcar que para la aplicación de estrategias de preservación digital en las instituciones sanitarias, tendrá que realizarse un gran esfuerzo en formación tanto del personal de los departamentos de informática, como de los responsables de archivo médico, debido a todas las implicaciones que se han observado en este proyecto.

Durante todo el proyecto se ha puesto de manifiesto, especialmente en las entrevistas finales, la interlocución de diferentes perfiles. Los responsables del archivo médico y el responsable del departamento de informática han sido las personas con las que se ha contactado y las que han participado de forma más generalizada, aunque dependiendo de qué entidad haya sido, también ha participado personal de otros departamentos, como el de protección de datos. Uno de los documentos demandados por todas las entidades ha sido el de confidencialidad de la información (Anexo I) y un documento descriptivo sobre el proyecto de investigación que se iba a realizar.

La comunicación con todos los interlocutores ha sido siempre muy fluida, sabiendo que su colaboración era totalmente desinteresada. Esta comunicación ha sido bien presencial, telefónica o vía correo electrónico, como ya se indicó en el Capítulo 1.

Una vez presentado el proyecto se envió un cuestionario de auditoría de 25 preguntas con respuestas cerradas de elección múltiple (Anexo III). Una vez

recibidas las repuestas del cuestionario se procedió a realizar una entrevista final, con preguntas abiertas, a fin de complementar los datos obtenidos. La entrevista se centraba en preguntas generales respecto a la encuesta y otras respecto a la estructura informática disponible. De esta forma, con los datos obtenidos sobre sus sistemas informáticos, se ha podido realizar posteriormente un análisis de riesgos de las entidades.

Por otro lado, no ha sido necesario realizar una auditoría de la información del sistema de información electrónica de las entidades sanitarias estudiadas. Cada año, los hospitales de Catalunya facilitan datos del conjunto mínimo básico de datos, al organismo con el mismo nombre Conjunt Mínim Bàsic de Dades (CMBD)[41] que es el encargado de realizar la auditoría. Este órgano depende del Servei Català de la Salut de la Generalitat de Catalunya.

6.4.1 Consorci Sanitari del Maresme

El Consorci Sanitari del Maresme es una entidad jurídica pública de carácter asociativo con personalidad jurídica plena. Se constituyó en 1998 por el Servei Català de la Salut (CatSalut), el Consell Comarcal del Maresme y el Ayuntamiento de Mataró. El consorcio cubre los servicios de procesos asistenciales dentro del ámbito comarcal del Maresme. Está compuesto por el Hospital de Mataró, tres centros de Asistencia Básica de la Salut y cinco consultorios locales en diferentes localidades. Su ámbito de cobertura es de un total de quince poblaciones del Maresme, como se muestra en la Tabla *5*.

[41] http://www10.gencat.cat/catsalut/cat/prov_cmbd.htm [consulta: 8 de marzo de 2012]

Ámbito de cobertura	
Arenys de Mar	Orrius
Arenys de Munt	Premià de Dalt
Argentona	Premià de Mar
Cabrera de Mar	Sant Andreu de Llavaneres
Cabrils	Sant Vicenç de Montalt
Caldes d'Estrac	Vilassar de Dalt
Dosrius	Vilassar de Mar
Mataró	

Tabla 5. Ámbito de cobertura del Consorci Sanitari del Maresme.

Hospital	**Estructura**
Hospital de Mataró	300 plazas Población de cobertura 251.110 personas en la atención hospitalaria de agudos
Centros sociosanitarios	**Estructura**
Antic Hospital de Sant Jaume i Santa Magdalena Residència Sant Josep Programa d'Atenció Domiciliària Equip de Suport (PADES)	127 plazas 62 plazas Población de cobertura 112.518
Centros de atenció primaria	**Localidad de referencia**
ABS Mataró Centre ABS Cirera-Molins ABS Argentona - Consultorio local de El Cros - Consultorio local de Dosrius - Consultorio local de Can Massuet - Consultorio local de Canyamars - Consultorio local d'Òrrius	Mataró Mataró Argentona Argentona Dosrius Dosrius Canyamars Òrrius
Centros de Salud Mental y Adicciones	**Localidad de referencia**
Hospital de Dia d'Adults Hospital de Dia Infantojuvenil Centre de Salut Mental d'Adults Centre de Salut Mental Infantojuvenil Centre d'Atenció a les Drogodependències	Son centros especializados que no cubren un área del Maresme en concreto.
Datos extraídos de la Memoria Anual de 2009 disponible en http://www.csdm.es	

Tabla 6. Estructura logística del Consorci Sanitari del Maresme.

Además de la atención hospitalaria que se realiza en el Hospital de Mataró, su área de trabajo cubre atención primaria, atención sociosanitaria, salud mental y adicciones y dependencias.

6.4.2 Consorci Sanitari de Terrassa

El Consorci Sanitari de Terrassa (CSdT) es una entidad pública formada por la Generalitat de Catalunya, el Ayuntamiento de Terrassa y la Fundació Sant Llàtzer, creado en el año 1998. El CSdT comprende la población de la comarca del Vallès Occidental. Dispone de tres hospitales: el Hospital de Terrassa, el Hospital Penitenciario y el Hospital de Sant Llàtzer. Asimismo dispone de siete centros de atención primaria, como se muestra en la Tabla 7.

Hospitales	**Estructura**
Hospital de Terrassa	342 camas de agudos 73 camas sociosanitario
Hospital Penitenciari	35 camas
Hospital de Sant Llàtzer	100 camas 36 plazas de hospital de dia
Llar tutelada de Rubí	12 plazas
Centro de Alto Rendimiento de Sant Cugat	216 plazas internas
Centros de atención primaria	**Localidad de referencia**
A.B.S. Sant Llàtzer	Terrassa
A.B.S. Terrassa Nord	Terrassa
A.B.S. Est	Terrassa
A.B.S. Anton de Borja	Rubí
A.B.S. Sant Genís	Rubí
A.B.S. Sant Quirze	Sant Quirze del Vallès
A.B.S. Can Rull	Sabadell
Datos extraídos de la memoría anual de 2009 disponible en http://www.cst.cat	

Tabla 7. Estructura logística del Consorci Sanitari de Terrassa.

6.4.3 Corporació Sanitària Maresme i la Selva

La Corporació Sanitària Maresme i la Selva(CSMS) es una entidad pública participada por el Departament de Sanitat i Seguretat Social, el Servei Català de la Salut, las corporaciones locales, a través de los ayuntamientos de Calella, Blanes y Lloret de Mar, así como el Consorcio Hospitalario de Catalunya. La CSMS cubre también un amplio abanico de población, centros y especialidades. Así, dispone de siete centros de atención primaria, tres centros sociosanitarios y dos hospitales, además de dos centros de rehabilitación, como se puede observar en la Tabla 8.

Hospitales	**Estructura**
Hospital Comarcal Sant Jaume de Calella	160 camas de atención a pacientes agudos 10 plazas de cirugia sin ingreso 7 places d'hospital de dia
Hospital Comarcal de Blanes	100 camas de atención a pacientes agudos 6 plazas de cirugía sin ingreso 6 plazas de hospital de día
Centros sociosanitarios	**Estructura**
Hospital Sociosanitari Sant Jaume de Blanes	81 camas de residencia asistida 23 camas de larga estancia
Hospital Sociosanitari Sant Jaume de Calella	33 camas de larga estancia 29 camas de convalecencia 10 plazas de hospital de día
Hospital Sociosanitari de Lloret de Mar	63 plazas sociosanitaria 24 plazas de residencia asistida 15 plazas de hospital de día
Centros de Atención Primaria	**Localidad de referencia**
CAP Calella CAP Lloret de Mar CAP Tossa de Mar CAP Malgrat de Mar CAP Palafolls CAP Fenals CAP Dr. F. Benito - Rieral	Calella Lloret de Mar Tossa de Mar Malgrat de Mar Palafolls Fenals Lloret de Mar
Centros de rehabilitación	
Centre de Rehabilitació de Tordera Centre Can Xaubet	Son centros especializados que no cubren un área del Maresme y la Selva en concreto.
Datos extraídos de la memoria anual de 2009 disponible en http://www.salutms.cat	

Tabla 8. Estructura logística de la Corporació Sanitària Maresme i la Selva.

6.4.4 Departament d'Obstetrícia, Ginecologia i Reproducció, Institut Dexeus

El Consultori Dexeus, S.A. (Departament d'Obstetrícia, Ginecologia i Reproducció d'USP – Institut Universitari Dexeus) pertenece a la organización de la empresa USP Hospitales. USP Hospitales es una empresa privada de atención médica que cubre multitud de especialidades.

Provincia	Centros
Alicante	Hospital USP San Jaime (Torrevieja) Centro Médico USP Virgen del Socorro (Torrevieja)
Baleares	Clínica USP Palmaplanas (Palma de Mallorca) Centro Médico USP Sa Pobla (Palma de Mallorca) Hospital de Día USP Playa de Muro (Palma de Mallorca)
Barcelona	Instituto Universitario USP Dexeus USP Oftalmológico de Barcelona (Barcelona) USP Oftalmológico de Barcelona (Badalona) USP Oftalmológico de Barcelona (Girona)
Tenerife	Hospital USP La Colina (Santa Cruz de Tenerife) Hospital USP Costa Adeje (Adeje - Tenerife)
Coruña	Hospital USP Santa Teresa Centro de Especialidades Médicas USP Santa Teresa Centro Médico USP Ferrol Hospital Oftalmológico USP Santa Teresa
Madrid	Hospital USP San Camilo (Madrid) Hospital USP San José (Madrid)
Málaga	Hospital USP Marbella (Marbella)
Murcia	Hospital USP San Carlos (Murcia) Centro Médico USP Juan Carlos I (Lorca - Murcia)
Sevilla	Clínica USP Sagrado Corazón (Sevilla) Centro Médico USP Nervión (Sevilla) Centro Médico de Consultas y Diagnóstico USP Aljarafe (Sevilla) Centro Médico USP Sevilla Este (Sevilla) USP Centro Médico de La Mujer (Sevilla) Centro de Consultas y Diagnóstico USP La Palmera (Sevilla) Centro de Cirugía Mayor Ambulatoria USP Ave María (Sevilla) Instituto Hispalense de Pediatría (Sevilla) Instituto de Especialidades Neurológicas, IENSA (Sevilla)
Vitoria	Clínica USP La Esperanza (Vitoria) USP Araba Sport Clinic (Vitoria) USP Mediplan Sport (Vitoria)
Datos extraidos de http://www.dexeus.com	

Tabla 9. Estructura organizacional grupo USP Hospitales.

Dispone de 12 hospitales en toda España y 23 centros de consultas, de diagnóstico y de cirugía de día, como se recoge en la Tabla 9. El Consultori Dexeus es un centro especializado en Ginecología, Obstetricia y Medicina de la Reproducción.

6.4.5 Fundació Pere Mata

La Fundació Pere Mata es una entidad proveedora del CatSalut, especializada en la atención de pacientes de salud mental. Esto representa una diferenciación respecto a las otras entidades colaboradoras, ya que implica que sus pacientes son de larga duración. Dispone de diversos centros de atención, como el Institut Pere Mata de Reus, y otros centros y residencias, tal y como se muestra en la Tabla 10.

Centros	Estructura
Institut Pere Mata Centros de Salud Mental de Adultos (CSMA)	 CSMA de Reus CSMA Tarragona Nord CSMA Tarragona Sud CSMA El Vendrell CSMA Valls
Centre de Salut Mental Infantil i juvenil (CSMIJ)	CSMIJ Reus CSMIJ Tarragona CSMIJ El Vendrell CSMIJ Antena Valls
Centre Villablanca –Atenció en discapacitat intel·lectual	366 plazas de residencia 47 plazas de centro de dia
Institut Paulo Freire Residència Bellisens Residència Garbí Residència Mestral Residència Bellvitge – Discapacidad Intelectual	 50 plazas 50 plazas 28 plazas de residencia 12 plazas de centro de día
Fundació Villablanca Residència Marinada Centre de Dia d'Atenció Especialitzada CAE Marinada Unitat de Recerca en Discapacitat Intel·lectual i Trastorns del Desenvolupament (UNIVIDD)	 74 plazas 15 plazas
Datos extraídos de la memoria anual de 2009 disponible en http://www.grupperemata.cat	

Tabla 10. Estructura logística de la Fundació Pere Mata.

6.4.6 Mútua de Terrassa

La Mútua de Terrassa es una entidad aseguradora que está presente en nueve comarcas de Catalunya, en los ámbitos asistenciales, aseguradores y sociosanitarios. Las comarcas que abarca son Anoia, Bages, Baix Camp, Baix Llobregat, Barcelonès, La Selva, Vallès Occidental, Vallès Oriental y Ribera d'Ebre. Sus servicios se encuentran fundamentalmente en el municipio de Terrassa y en la comarca del Vallès. Atiende diversas especialidades como Neurocirurgia, Cirurgia Toràcica, Hematologia y Hemodinàmia cardíaca. Además, su área de influencia abarca una población de 1.000.000 de habitantes, como se muestra en la Tabla 11.

Centros	**Estructura**
Hospital Universitara Mútua de Terrassa	469 plazas
Clínica MútuaTerrassa	
Hospital de Martorell	130 plazas
Atención a la dependencia	**Estructura**
Casa Marquès	24 plazas y 10 de centro de día
Residencial Vallparadís	114 plazas y 30 de centro de día
Sociosanitari Vallparadís	81 plazas y 30 de centro de día
Triginta	30 plazas residentes
Residència i centre de dia L'Ametlla	88 plazas residentes
Centre de dia Can Anglada	30 plazas residentes
Residència i centre de dia Baix Camp	52 plazas residenciales y 15 de centro de día
Residència i centre de dia La Pineda	42 plazas y 18 de centro de día
Residència i centre de dia Parc Serentill	56 plazas residenciales y 25 de centro de día
Residència i centre de dia Falguera	81 plazas residenciales y 16 de centro de día
Residència i centre de dia Poblenou	90 plazas residenciales y 30 de centro de día
Residència i centre de dia Porta	88 plazas residenciales y 30 de centro de día
Residència i centre de dia Mora	30 plazas residenciales y 20 de centro de día
Centre de dia Les Arenes	30 plazas residenciales
Centre de dia Rubí	22 plazas residenciales
Residència i Centre de dia Tursia	35 plazas residenciales y 10 de centro de día
Residència i Centre de dia Borja	25 plazas residenciales
Residència i Centre de dia El Tamariu	48 plazas residenciales y 10 de centro de día
Residència i Centre de dia Montserrat Betriu	
Atención Primaria	**Atención Primaria**
CAP RAMBLA I i II	CAP Valldoreix
CAP Rubí	CAP Can Trias-Ernest Lluch
CAP Sant Cugat	CONSULTORI Ullastrell
CAP Oest	CONSULTORI de La Floresta
CAP Terrassa Sud	CONSULTORI de les Planes
CAP Olesa de Montsserrat	CONSULTORI Viladecavalls
Datos extraídos de la memoria anual de 2010 disponibles en http://www.mutuaterrassa.cat/	

Tabla 11. Estructura organizativa de Mútua de Terrassa.

6.4.7 Grup Sagessa

El Grup Sagessa (Grupo de Assistència Sanitària i Social) es una entidad de titularidad pública. Su ámbito geográfico de trabajo son las comarcas del Sur de Catalunya y dispone de cinco hospitales. Sus centros asistenciales cubren atención primaria, atención de agudos y atención sociosanitaria, además de la gestión sanitaria. También el grupo dispone de centros escolares especializados en preescolar y educación especial. Todos sus centros se pueden ver reflejados en la Tabla 12.

Centros	Estructura
Area Salud	
Centre MQ Reus	Centro medicoquirurgico
Hospital Comarcal d'Amposta	40 plazas atención agudos
Hospital Comarcal de Móra d'Ebre	66 plazas atención agudos
Hospital Universitari Sant Joan de Reus	
Hospital de la Santa Creu de Jesús-Tortosa	335 plazas
Hospital Lleuger de Cambrils	Sin plazas – atención primaria i urgencias
Àrea Bàsica de Salut de la Selva del Camp	
Àrea Bàsica de Salut de Riudoms	
Àrea Bàsica de Salut de Vandellòs-l'Hospitalet	
Àrea Bàsica de Salut Reus V	
Area Social	
Residència d'Avis d'Amposta	80 plazas y 20 plazas centro de día
Residència d'Avis d'Ascó	80 plazas y 10 plazas centro de día
Residència d'Avis de Gandesa	54 plazas y 16 plazas centro de día
Residència d'Avis de la Sénia	28 plazas y 5 plazas centro de día
Residència d'Avis de la Selva del Camp	55 plazas y 20 plazas de centro de día
Centre de Dia de Batea	15 plazas
Centre de Dia de Benissanet	10 plazas
Servei d'Ajuda a Domicili	
Centres Residencials d'Acció Educativa	
Area Educativa	
Escola bressol municipal "el Margalló"	
Escola bressol municipal "el Marfull"	
Escola bressol municipal "els Musterets"	
Escola bressol municipal "l'Auberge"	
Escola bressol municipal "la Ginesta"	
Escola bressol municipal "l'Olivera"	
Escola bressol municipal "la Morera"	
Escola bressol municipal "Montsant"	
Escola bressol municipal "el Lligabosc"	
Aules "Ralet, ralet...", Mas Abelló	
Datos extraídos de http://www.grupsagessa.com	

Tabla 12. Estructura organizativa del Grup Sagessa.

6.4.8 Hospital Sant Joan de Déu

El Hospital Sant Joan de Déu (HSJD) es un hospital privado de alta tecnología, dedicado fundamentalmente a la pediatría. Forma parte de una entidad religiosa, la Orden Hospitalaria de Sant Joan de Déu y está ubicado en Esplugues de Llobregat (Barcelona). La Orden Hospitalaria de Sant Joan de Déu está presente en 50 países de los cinco continentes. La estructura del hospital, emplazado en Esplugues de Llobregat, se recoge en la Tabla 13.

Centro	**Estructura**
Hospital Sant Joan de Déu	362 camas 12 quirófanos
Ámbito de trabajo	
Barcelonès Baix Llobregat	
Datos extraídos de http://www.hsjdbcn.org	

Tabla 13. Estructura logística del Hospital Sant Joan de Déu de Esplugues de Llobregat.

6.5 Análisis de los resultados obtenidos en las auditorias de seguridad y de preservación

En este apartado se presenta un análisis pormenorizado de los resultados obtenidos en la encuesta expuestos en la sección anterior. Cabe destacar que si bien las entidades sanitarias todavía tienen una falta de requisitos generales para disponer de una planificación de la preservación digital, así como de un archivo basado en el modelo OAIS, todas ellas muestran un alto grado de seguridad en sus sistemas de información.

Pregunta 1 – Marco organizativo

Disponen de un comité de gestión de la seguridad de la información?

SI NO

Indique qué marco legislativo afecta al sistema de información en el archivo digital (Marque las opciones que corresponda)

LO 15/1999, de Protección de Datos de Carácter Personal	
Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica	
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.	
RD 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica	
RD 21/2000, sobre los derechos de información concerniente a la salud y a la autonomía del paciente y a la documentación clínica.	
Ley 16/2010, modificación de la ley 21/2000, del 29 de diciembre, sobre los derechos de información concerniente a la salud y a la autonomía del paciente y a la documentación clínica.	

Todas las entidades disponen de un comité de gestión de la seguridad de la información. De hecho, todas las personas de las entidades sanitarias que han participado en el estudio pertenecen a él, hecho lógico teniendo en cuenta que son responsables de la custodia y gestión de datos pertenecientes a pacientes y, por tanto, datos sensibles.

Sin embargo, no tienen tan claro en qué forma afecta la legislación a su sistema de información, dado que sólo dos de las entidades reconocen que el Esquema Nacional de Seguridad les atañe. En realidad, el Esquema Nacional de Seguridad, excepto a una entidad que es totalmente privada, afecta al resto de las entidades, ya que reciben fondos públicos de una forma u otra.

Las instituciones son conscientes de encontrarse bajo el alcance de la ley de protección de datos LO 15/1999. Sorprende que en cuatro casos se haya marcado la Ley 34/2002, referida al comercio electrónico, cuando ésta no es pertinente, pues ninguna de las webs de estas instituciones realiza actividades de comercio electrónico ni tienen, como se verá más adelante, conectados sus sistemas de historias clínicas a internet.

Pregunta 2 – Normativa de seguridad

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Directrices documentadas donde se indica la estructuración de la documentación de seguridad del sistema, gestión y acceso	
Directrices que indique que es lo que se considera uso indebido del equipamiento o la información	
Documentación que indique la responsabilidad del personal respecto al cumplimiento y violación de normas de seguridad de acuerdo con la legislación vigente	
Documento explicativo sobre los deberes y obligaciones en materia de seguridad de de información	
Plan de contingencias documentado para casos de quiebra de su sistema	
Documento explicativo sobre la calidad de los registros del Sistema de Información	

Es una pregunta contestada mayoritariamente de forma positiva, donde se aprecia una gran concienciación respecto a la materia en seguridad y al uso indebido de la información.

Tres entidades han indicado que no disponen de un plan de contingencias en caso de fallo del sistema. Esta respuesta hace pensar en un riesgo muy elevado en caso de pérdida de información.

Pregunta 3 – Arquitectura de seguridad

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Inventario de hardware	
Procesos de actualización de hardware	
Inventario de software	
Documentación que indique las líneas de defensa	
Documentación que indique la identificación y autentificación de los usuarios	
Controles técnicos internos	
Procesos documentados sobre vigilancia tecnológica	

Con esta pregunta se pretendía averiguar la posible documentación sobre el material encargado de la gestión de los datos, tanto de software como de hardware. Si bien todas las entidades disponen de ambos inventarios, se detecta una falta de documentación respecto a las líneas de defensa en caso de ataques al sistema. Esta circunstancia está justificada en algunos casos, ya que el sistema es cerrado, sin acceso a internet ni acceso remoto, pero en otros casos no es así.

Todas las entidades identifican y autentifican a los usuarios, de forma que existe un control sobre quién entra y sale del sistema de información.

Lo que no queda ya tan de manifiesto es la vigilancia tecnológica, ni que se entiende por este proceso, hecho que se volvió a plantear en las entrevistas mantenidas con diferentes responsables. En algunos casos se entendía que era la comprobación de que el hardware y el software estaban actualizados y en otros casos el concepto en sí no estaba claro.

Pregunta 4 – Procedimientos de seguridad y autorización

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Como se llevarán a cabo las tareas habituales en el lugar de trabajo	
Quién debe llevar a cabo las tareas en el lugar de trabajo	
Procesos, procedimientos o documentación de comportamientos anómalos en el sistema (creación de informes de errores, análisis de amenazas, etc.)	
Utilización de instalaciones habituales y alternativas	
Entrada de equipos en producción	
Entrada de aplicaciones en producción	
Establecimientos de enlaces de comunicaciones con otros sistemas	
Utilización de medios de comunicación habituales y alternativos	
Utilización de soportes de información	
Utilización de equipos móviles	
Análisis de sistemas	
Descripción de personal	
Necesidades de seguridad	

Esta pregunta se ha planteado para saber si se disponía de instalaciones alternativas y de los mecanismos de entrada en producción de los diferentes elementos que componen el sistema de información de una entidad sanitaria.

a, b.– En general, las entidades tienen documentación escrita sobre las funciones a llevar a cabo en la organización.

c.- Salvo dos, todas las entidades tienen un registro de comportamientos anómalos del sistema. Esto tiene su explicación si el sistema es cerrado, pero no lo es tanto si desde un terminal se accede a las HCE y en este terminal, como se verá en el análisis de riesgos, disponen de puertos USB, necesarios por otra parte para conexión de dispositivos de firma electrónica de recetas.

d.- Sólo dos entidades tienen la posibilidad de disponer de instalaciones alternativas a su lugar de trabajo habitual.

e y f.- En estas dos entradas se puede apreciar que, si bien hay entidades que disponen de la documentación de entrada tanto de equipos como de aplicaciones en producción, son mayoría las que documentan la entrada de aplicaciones en producción, ya que supone un riesgo más elevado para el sistema que un equipo.

g.- Aún teniendo diferentes sistemas intercomunicados entre sí, todas las entidades tienen este proceso documentado.

i.- Cinco entidades, disponen de procesos de medios de comunicación habitual, pero también de medios alternativos. Es decir, en caso de fallos en el sistema de comunicación, estas entidades disponen de medios alternativos.

j.- Sólo dos entidades disponen de procesos con equipos móviles. Esto tiene sentido si disponen de accesos remoto desde alguna instalación. De todas formas, tampoco parece ser un escenario común el uso de equipos móviles en las entidades de gestión sanitaria.

k.- En general, se realiza análisis de sistemas. Sólo dos entidades han indicado que no lo realizan.

l.- Seis entidades disponen de documentación respecto a la descripción de personal en tanto en cuanto la descripción se refiere a las capacidades que se necesitan para desempeñar el puesto de trabajo.

m.- Cuatro entidades, la mitad de las encuestadas, tienen documentadas sus necesidades de seguridad. Esta respuesta puede tener sentido, ya que algunas de ellas tienen sus sistemas totalmente cerrados y por tanto, al no tener conexiones externas, no parece que sea imprescindible disponer de documentación al respecto.

Pregunta 5 – Sobre el análisis de riesgos

Utilizan alguna de las metodología de evaluación de riesgos citadas a continuación?

MAGERIT		ISAMM		DRAMBORA	
OCTAVE		IT-Grundschutz			
CRAMM		ISO 31000:2009			
MARION				CAP	

Si utilizan **otra** diferente la podrían indicar?

Si la respuesta es **otra**, podría indicar cuál de estas medidas se contemplan en la evaluación de riesgos?

Identificación cualitativa de los activos de más valor	□
Cuantificación de las amenazas	□
Identificación de les vulnerabilidades de les amenazas	□
Identificación de les salvaguardas	□
Identificación del valor residual del riesgo	□

Esta pregunta se refiere a los análisis de riesgos. Sorprende que sólo una entidad realice análisis de riesgos de sus sistemas. El análisis de riesgos es una herramienta que no sólo permite ver en qué estado está el sistema, tanto activo como pasivo, sino que también permite, a través del análisis de datos, optimizar los posibles costes en inversión, tanto de maquinaria como de software.

Al menos una entidad dispone de un análisis de riesgos que cuantifica sus amenazas, identifica las vulnerabilidades de las mismas e identifica las salvaguardas.

Debido a la ausencia de documentación por parte de todas las entidades, se ha decidido realizar un análisis de riesgos de la forma más simple posible. La metodología que se ha empleado es MAGERIT, que es una metodología reconocida internacionalmente, empleando el programa PILAR.

Pregunta 6 – Certificación de componentes

Disponen de componentes/equipos certificado por los fabricantes con normativas internacionales o europeas?	
SI	NO

En esta respuesta, todas las entidades indican que disponen de equipos certificados con normativas europeas.

Pregunta 7 – Adquisición de nuevos componentes

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Controles para controlar las necesidades de seguridad	
Plan de formación y desarrollo del personal de sistemas de información o archivo	
Documentos de información financiera respecto de su unidad	
Procedimientos en la adquisición de nuevos componentes del sistema	

La adquisición de nuevos componentes se recoge en esta pregunta.

a.- Cuatro entidades disponen de procesos para controlar las necesidades de seguridad. Son, de hecho, las mismas entidades que en la pregunta 4 tenían documentación sobre las necesidades de seguridad.

b.- Cuatro entidades disponen de un plan de formación en ICT o archivos. El matiz reside en que, según las entrevistas realizadas, estos planes de formación se realizan según las necesidades existentes en ese momento. Sólo en un caso, esta formación es resultado de una decisión clara y planificada, según se deduce de las entrevistas mantenidas.

c.- Cuatro entidades indican que disponen de información financiera de su unidad, pero, en las entrevistas posteriores, se ha aclarado que esta información se refiere a la evaluación de las auditorías que realiza el hospital. Por tanto, la información financiera disponible lo es respecto a toda la entidad sanitaria.

d.- Cinco entidades disponen de procesos para adquirir nuevos componentes del sistema. Este parámetro indica que no sólo se compra a medida que el sistema va creciendo, sino que el crecimiento del sistema está planificado y que, por tanto, existe una reglamentación interna al respecto.

Pregunta 8 – Gestión de capacidades

El personal dispone de perfiles laborales adecuados a la unidad donde trabajan
(1 Totalmente en desacuerdo, 5 Totalmente de acuerdo):

1 2 3 4 5

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Necesidades de procesamiento del sistema	
Necesidades de software)	
Procedimiento sobre vigilancia tecnológica	
Procedimientos sobre les necesidades de los usuarios	

En esta pregunta se pretendía evaluar el op.pl.4 del Esquena Nacional de Seguridad, es decir, decidir si los perfiles laborales son los adecuados para la unidad. Todas las entidades han respondido que están satisfechas y hasta muy satisfechas. Ninguna ha mostrado un desacuerdo con los perfiles laborales que hay en la unidad. Por tanto, tienen personal adecuado a las necesidades de su servicio.

a.- Tres entidades indican que tienen documentadas las necesidades de proceso del sistema. Esto quiere decir que disponen del tipo de ordenadores necesarios para procesar el tipo de información que necesitan.

b.- Cinco entidades tienen documentados las necesidades de software en su unidad. Hay que decir que todas las entidades producen software propio, como se indica más adelante, y, por tanto, se gestionan las necesidades a medida que van surgiendo o que aumenta el volumen de información.

c.- En la pregunta 4 se mencionaban los procesos de vigilancia tecnológica, pero era respecto a sus necesidades. En esta pregunta se incide directamente en si estos están documentados. Como resultado, sólo dos entidades tienen los procesos de vigilancia tecnológica documentados.

d.- Al preguntar sobre las necesidades de los usuarios, evidentemente se hace referencia a los usuarios internos, puesto que el público en general no tiene acceso al sistema de información activo, ni pasivo. Así pues, cinco entidades tienen documentados los requerimientos sobre las necesidades de los usuarios.

e.- En este apartado se preguntaba por las necesidades de los usuarios, evidentemente hablamos de los usuarios internos, puesto que el público en general no tiene acceso al sistema de información activo, ni pasivo. Así pues cinco entidades tienen documentados los requerimientos sobre las necesidades de los usuarios.

Pregunta 9 – Control de acceso

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

El sistema de información, identifica los usuarios de forma única	
El sistema de información tiene mecanismos de acceso de prevención de acciones no autorizadas	
Existen **personas** responsables que pueden decidir los derechos de acceso a recursos por parte de los usuarios del sistema	
Existe control de accesos a los registros de configuración del sistema	
Un sistema de auditoría o supervisión de cualquier función en el sistema	
Un sistema de control concurrente para la denegación o autorización de tareas críticas	
Políticas de derechos de acceso de los usuarios	

En esta pregunta se evaluaba las condiciones de acceso de los usuarios al sistema, tanto a nivel de identificación, registro, y auditoria del sistema.

a.- Todas las entidades han respondido que los usuarios se identifican de forma única. Es decir, no tienen dobles códigos los empleados, ni privilegios que no les corresponden, ya que, aumentaría el riesgo de errores o ataques al sistema.

b.- Cinco entidades tienen mecanismos de prevención de acciones no autorizadas. Estos mecanismos son procesos realizados a través del propio software del sistema.

c.- Todas las entidades tienen personas responsables que pueden decidir sobre los accesos a los recursos de los usuarios del sistema. Dicho de otro modo, todas tienen un administrador o más de uno en el sistema que otorga o deniega recursos a los usuarios.

d.- Todas las entidades tienen un control de acceso a los registros del sistema. Esto implica que las acciones de los usuarios no sólo se registran sino que además existe un mecanismo que permite controlar el acceso a registros de los ordenadores para evitar acciones maliciosas en el sistema.

e.- Seis entidades indican que disponen de un sistema de auditoría de cualquier función del sistema. Es decir, las funciones que tiene el sistema son comprobadas para evitar comportamientos anómalos.

f.- Cuatro entidades tienen un sistema de control concurrente para la denegación de tareas críticas.

g.- Todas las entidades, a su vez, tienen políticas de derecho de acceso a los usuarios documentadas. Esto implica que ni todos los usuarios tienen los mismos derechos, ni todos los usuarios tienen los mismos perfiles ni acceso a los recursos.

Pregunta 10 - Autentificación

¿Disponen de procedimientos de validación de acceso dentro del sistema?
Ex: -Suspensión del autentificador después de un periodo de no utilización, No utilización de Claves concertadas, dispositivos físicos personalizados o biométricos

SI NO

En esta pregunta se trataba de averiguar si existía control por inactividad dentro del sistema, mediante algún tipo de control, cómo biométrico o suspensión del autentificador. Siete entidades han respondido que sí disponían de controles dentro del sistema.

Pregunta 11 – Acceso local

¿Disponen de documentación sobre les políticas de acceso (reglas de autorización, requerimientos de autentificación)?		
	SI	NO
¿Las tienen implementadas?		
	SI	NO

En la pregunta once se pretendía poner de relieve si las políticas de acceso al sistema están documentadas e implementadas. De las entidades analizadas, siete entidades han respondido que las tienen documentadas e implementadas, siendo únicamente una entidad la que las tiene implementadas y no documentadas.

Pregunta 12 – Acceso remoto

Disponen de documentación escrita sobre las políticas de acceso remoto?

SI NO

¿Las tienen implementadas?

SI NO

En esta pregunta se plantean las condiciones bajo las cuáles las entidades tienen acceso remoto. Hay que indicar que no todas disponen de acceso remoto porque el sistema es cerrado. Las entidades que disponen de documentación son cuatro, siete las tienen implementadas y una no dispone de documentación ni las tiene implementadas, simplemente porque no hay acceso remoto a la unidad. Es importante recordar que el acceso remoto es exclusivo de la entidad y no hay acceso a internet ni desde el exterior ni a través de él.

Pregunta 13 - Explotación

Los equipos están configurados de forma que:	
Se retiran las cuentas y contraseñas estándares	□
Se les aplica la regla de mínima funcionalidad	□
Se les aplica la regla <<seguridad por defecto>>	□

Para conocer cómo están configurados los equipos que hay en las entidades de gestión sanitaria se plantea esta pregunta. Los resultados en los tres apartados son muy dispares y merecen un comentario.

a.- Seis entidades de ocho retiran cuentas estándares. Esto quiere decir que antes de poner un equipo en producción, es decir, disponible al personal que trabaja en la entidad, los usuarios que vienen estándares con el software, como "Invitado", "Administrador" o "Usuario" se eliminan. Esto provoca una disminución de riesgos en los equipos para no ejecutar software malintencionado que posteriormente entre con derechos superiores a los que dispone un usuario. Sólo dos entidades no realizan esta acción.

b.- La aplicación de la regla de funcionalidad mínima quiere decir que no disponen de más software del que se necesita para trabajar, ni conexiones a dispositivos externos, cómo impresoras, más que las necesarias. En este apartado, siete entidades han contestado que aplican esta regla.

c.- Cinco entidades indican que aplican la seguridad por defecto. Esto quiere decir que la seguridad que se aplica en la empresa sigue sus propios criterios. Tres empresas, en cambio, no aplican el concepto de seguridad por defecto. Esto no quiere decir que no tenga medidas ni planificación de la seguridad. Quiere decir, que no configuran los equipos de esta forma, sino que emplean la seguridad que tiene el software con el que viene el ordenador de fábrica.

Pregunta 14 – Instalaciones, configuraciones

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Procesos reactivos ante la posibilidad de actualizaciones de software de seguridad basada en una evaluación beneficio-riesgo	
Documentación para atender las especificaciones de los fabricantes	
Procesos para un seguimiento continuo ante cambios por defecto	
Procesos de gestión del cambio documentados que identifiquen los cambios en los procesos críticos	
Mecanismos de prevención y reacción ante código maligno	
Proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema	
Procesos de registros de la actividad de los usuarios (logs de usuario, traza de operaciones)	
Disponen de registros de gestión de incidencias (Aclaración: errores de gestión, incidentes inapropiados por parte del personal)	
Protección sobre los registres de acceso	
Disponen de equipos con claves criptográficas protegidas durante todo el ciclo de vida	

En esta pregunta se pretendía averiguar qué tipo de control se hace a los usuarios sobre sus actividades en el sistema. También que actitudes reactivas o proactivas se eligen con los equipos, usuarios y software.

a.- Dos entidades de las ocho organizaciones evaluadas indican que actualizan el software de seguridad evaluando beneficio-riesgo, es decir, que otras implicaciones tendrá la actualización de determinado software de seguridad con respecto al software que funciona en la empresa.

b.- Sólo tres entidades de ocho indican que disponen de documentación para atender las especificaciones de los fabricantes. A pesar de tener los equipos certificados, como respondieron ocho en la pregunta seis, sólo tres conservan información para atender requerimientos.

c.- Dos entidades han indicado que tienen procesos de seguimiento ante cambios en el sistema. Esto puede indicar una falta de recursos en la empresa para disponer de personal que realice esta función.

d.- Sólo una entidad ha respondido que dispone de documentación sobre los requerimientos o necesidades en los procesos críticos. Sin embargo, un proceso crítico implica una serie de riesgos en el sistema que habría que documentar, precisamente para minimizar los riesgos.

e.- Cinco entidades han respondido que tienen mecanismos documentados para responder a un código maligno. Pensando en que tienen sistemas cerrados, es coherente que la respuesta sea así, sin alcanzar a la totalidad de entidades.

f.- Dos empresas disponen de procesos para hacer frente a incidentes con impacto en la seguridad. Es decir, que en caso de necesidad, por vulneración de la seguridad, sólo estas dos entidades tendrían capacidad para seguir actuando según procedimientos.

g.- Seis de las ocho empresas indican que disponen de registros de la actividad de sus usuarios. El registro de la actividad de los usuarios suele tener un componente de seguridad agregado, para que se sepa en todo momento las acciones que hacen los usuarios, y, en determinados casos, puede llegar a tener implicaciones legales, por ejemplo por mal uso del sistema.

h.- Siete de las ocho entidades han respondido que disponen de registros sobre la gestión de incidencias. Es decir, las incidencias que suceden en el sistema de información con respecto a las historias clínicas, se gestionan, y se dispone de un histórico de cómo se han solucionado.

i.- Seis de las ocho entidades disponen de protección sobre los registros de acceso al sistema. Esto quiere decir que, para evitar que los usuarios manipulen registros de sistema en el ordenador de trabajo, estos se protegen.

j.- Una entidad ha respondido positivamente sobre la disposición de equipos con claves criptográficas en el ciclo de vida de los equipos. Es una alta medida de seguridad que permite minimizar los riesgos de los equipos así como el acceso indebido a la información.

Pregunta 15 – Servicios con terceras partes

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Especificación de acuerdos con terceras partes	
Documentación que especifique los acuerdos y tareas de coordinación con terceras partes (Ex: externalización de algún servicio vinculado a TIC)	
Acuerdos con terceros sobre la provisión del servicio por medios alternativos en caso de indisponibilidad del servicio	

En esta pregunta se pretendía determinar cómo era el acuerdo con terceras partes en materia contractual.

a.- Todas las entidades disponen de documentación con terceras partes en forma de contratos de colaboración y confidencialidad.

b.- Todas las entidades, además, disponen de acuerdos con terceras partes así cómo tareas de coordinación.

c.- Sin embargo, sólo cinco de las ocho entidades disponen de acuerdos con terceras partes para ofrecer un servicio alternativo. Esto indica que, en caso de necesidad, tres entidades no podrán ofrecer servicio alguno alternativo.

Pregunta 16 – Continuidad del servicio

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Documentación que indique análisis de impacto ante el crecimiento del sistema	
Plan de continuidad del sistema	
Calendario de autoevaluación de revisiones periódicas del sistema	

¿Cuál es el tiempo de parada asumible de todo el servicio?

En esta pregunta se pretendía analizar el impacto y plan de continuidad del sistema.

a.- Sólo una entidad ha indicado que dispone de análisis de impacto sobre el crecimiento del sistema. Es decir, qué implicaciones le supondrá a nivel técnico, humano y económico el crecimiento de su sistema.

b.- Dos entidades han respondido que disponen de un plan de continuidad del sistema.

c.- Dos entidades han indicado que disponen de un calendario de autoevaluación de revisiones periódicas. Es decir, comprobar el correcto funcionamiento del sistema periódicamente.

d.- Con respecto al tiempo de parada asumible en el sistema, tres entidades no han indicado nada, pero en las entrevistas mantenidas se aclaró que simplemente los equipos no pueden parar.

Respecto al tiempo de paradas asumible, tres entidades indican que disponen de menos de 24 horas para poner otra vez en marcha el servicio, una indica que 0 horas y una última que sólo está permitido el tiempo de parada de 2 a 4 horas y por las noches. Todas estas respuestas tienen su lógica si pensamos que del

funcionamiento del sistema depende todo un hospital, desde la entrada en admisión, hasta el alta. Por tanto, este es un punto crítico a tener en cuenta.

Pregunta 17 – Monitorización del sistema

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Mecanismos para a la detección de intrusiones	
Sistema de métricas que midan los desarrollos reales en materia de seguridad ante posibles amenazas	

Con esta pregunta se trataría de analizar los mecanismos de detección de intrusiones. Seis de ocho entidades disponen de mecanismos para la detección de intrusiones y dos de ellas no. Por otro lado, sólo dos de las ocho entidades disponen de documentación sobre métricas que midan el nivel de seguridad ante posibles amenazas.

Pregunta 18 – Gestión de personal

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Directivas que indiquen los planes de desarrollo, definición de competencias del personal que trabaja	
Documentación sobre los roles y responsabilidades del personal y descripción de su lugar de trabajo	
Documentación sobre los deberes y obligaciones del personal	
Disponen de un plan de formación continuada para formar el personal en a) Configuración de sistemas b) Detección y reacción ante incidencias c) Gestión de la información en cualquier soporte que se encuentre.	
Es dispone de un plan de servicio continuado con personal alternativo con las mismas garantías que el personal habitual	

En esta pregunta se planteaban cuestiones respecto a los planes de desarrollo y el empleo del personal del servicio.

a.- Seis de las ocho entidades disponen de documentación de directrices que indiquen los planes de desarrollo y competencias.

b.- Seis de las ocho entidades disponen de la descripción del lugar del trabajo, como de los roles y responsabilidad del personal.

c.- Cuatro de las ocho entidades disponen de documentación sobre los deberes y obligaciones del personal. Cuatro de ellas, sin embargo, indican que no disponen de documentación alguna.

d.- Sólo tres entidades indican que disponen de planes de formación en configuración de sistemas. Cinco indican que no tienen planes de formación al respecto.

e.- Cuatro de las ocho entidades indican que disponen de documentación sobre formación en detección y reacción ante incidentes. Esto puede indicar que o se dispone en las otras cuatro de personal muy especializado o no se disponen de recursos suficientes.

f.- Sólo tres entidades de las ocho indican que disponen de planes de formación en gestión de la información en cualquier soporte. De las otras cinco que no han contestado, se puede presuponer que, al tener sistemas centralizados y basados en grandes sistemas de almacenamiento, es posible que no los necesiten.

g.- Una entidad ha indicado que dispone de un plan de servicio con personal alternativo. Es decir, en caso de substituir un empleo por baja, enfermedad o porque se va de la empresa, se dispone de plan alternativo para continuar disponiendo del mismo personal en las mismas condiciones técnicas que el anterior.

Pregunta 19 – Medidas de protección

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Los equipos están separados según su función específica	
El acceso a los equipo disponen de controles a sus áreas	
Les áreas de los equipos están vigiladas	
Las personas que acceden a las áreas donde el equipo forma parte del sistema de información se identifican	
Se registran las entradas y salidas de personas	
Se disponen de controles sobre condiciones de temperatura y humedad	
Se disponen de protecciones frente a amenaces identificadas en el análisis de riesgos	
Es disponen de protecciones de cableado frente incidentes fortuitos o deliberados	
Se dispone de un plan de servicio continuado que garantice el suministro eléctrico y el funcionamiento de las luces de energía	
Se dispone de un plan de servicio continuado que garantice la protección frente a incendios	
Se dispone de un plan de servicio continuado que garantice la protección frente a inundaciones	
Se dispone de un plan de servicio continuado que registra toda entrada y salida de material así como la identificación de la personal que autoriza el movimiento	
Disponen de un plan de servicio continuado que garantice la disponibilidad de instalaciones alternativas en las mismas condiciones de seguridad en caso de que las instalaciones habituales no estén disponibles.	

a.- Cinco entidades indican que los equipos están separados según su función específica, respuesta que pueda deberse a que disponen de más recursos. Los que han contestado negativamente a esta cuestión disponen de menos recursos y, por tanto, deben destinar equipos compartidos para otros fines.

b.- Siete de las ocho entidades responden que el acceso a los equipos dispone de controles en sus áreas. Esta respuesta no es necesariamente indicativa de que para acceder a un equipo hay un control sino que puede ser que el control esté dentro del propio equipo.

c.- Cuatro de las ocho entidades han contestado que las áreas de los equipos están vigiladas, mientras que cuatro han contestado que no lo están. Esto puede deberse al hecho de que para acceder a los equipos se necesita un alto nivel de seguridad o bien que no se dispone de recursos suficientes para que las áreas estén vigiladas.

d.- Siete entidades han contestado que las personas que acceden a los equipos se identifican y sólo una que no.

e.- Seis de las ocho entidades han contestado que se registran las entradas y salidas de personal, es decir, que el acceso a las instalaciones dentro de la entidad requiere una identificación. Dos entidades han contestado que no disponen de este registro, lo cual, además de ser un riesgo añadido, puede ser debido a la estructura de sus instalaciones que hace que no sea necesario.

f.- Todas las entidades disponen de controles de temperatura y humedad, lo que indica que los equipos trabajan, o se procura que trabajen, en condiciones óptimas y no en condiciones extremas.

g.- Cinco entidades han respondido que disponen de protección frente a amenazas identificadas en el análisis de riesgos. Esta respuesta sorprende ya que sólo una ha contestado que realiza análisis de riesgos, a la vista de las respuestas a la cuestión siete. Esto quiere decir que o no se realizan análisis de riesgos, o se presupone que determinadas acciones son un riesgo, quizás sin haberlas analizado previamente, realizándose la protección correspondiente.

h.- Cinco entidades de las ocho han contestado que disponen de protecciones de cables frente a accidentes fortuitos y tres entidades han contestado que no disponen de dichas protecciones.

i, j .- Todas las entidades disponen de un plan de protección documentado frente a incendios y la garantía de un plan continúo de luz y energía. Estas respuestas son coherentes con lo respondido en la pregunta dieciséis.,

k.- Tres de las ocho organizaciones disponen de protección frente a inundaciones.

l.- Sólo dos de las ocho entidades realizan un registro de entrada y salida de material. Teniendo en cuenta el tipo de entidades que son, es un riesgo muy elevado el hecho de que no se realicen registros de material tanto de entrada como de salida.

m.- Ninguna entidad dispone de instalaciones alternativas en caso de necesidad.

Pregunta 20 – Protección de los equipos

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Sus necesidades de seguridad incluyen que el lugar de trabajo esté despejado sin más material que el requerido para la actividad que se esté realizando en cada momento	
Los lugares de trabajo se bloquean pasado un tiempo prudencial de inactividad	
Los equipos portátiles están protegidos	
Plan de contingencia con la posibilidad de emplear medios alternativos para garantizar la continuidad del servicio	

Esta pregunta aborda el tema de la protección de los equipos.

a.- Tres de las ocho entidades indican que en el lugar de trabajo sólo hay el material requerido. Cinco entidades, en cambio, indican que en el lugar de trabajo hay más material del necesario. Esta respuesta puede deberse a la disposición de poco espacio para trabajar.

b.- Siete entidades indican que los lugares de trabajo se bloquean, pasado un tiempo de inactividad. En esta acción, normalmente, se pretende minimizar el riesgo bajo el cual otra persona no autorizada, ajena a la unidad de servicio o la entidad, acceda a los derechos de uso del sistema informático que goza el usuario que ha dejado su lugar de trabajo inactivo. También se trata de impedir que se introduzca o gestione información que no corresponda.

c.- Todas las entidades indican que los equipos portátiles de las que disponen están protegidos. En las entrevistas posteriores, el concepto de equipo portátil se entendía como aquel equipo que podía acceder al sistema o a las historias clínicas, sin que necesariamente fuese un ordenador portátil.

d.- La mitad de las entidades disponen de un plan de contingencia documentado para emplear medios alternativos. Esta es una cuestión relevante,

ya que si bien ninguna entidad en la pregunta diecinueve disponía de la garantía de estar en posesión de instalaciones alternativas, se ve como, en algunos casos, si pueden disponer de medios alternativos para facilitar el servicio.

Pregunta 21 - Backups

El sistema de seguridad realiza la copia de (marque la opción indicada):

a) La información de trabajo de la organización
b) Las aplicaciones en explotación incluidos los sistemas operativos
c) Datos de configuración, servicios, aplicaciones, equipos u otra naturaleza
d) Claves para preservar la confidencialidad de la información

En esta pregunta se trataba de analizar cómo se realizaban las copias de seguridad de la información dentro de la organización

a.- Siete de las ocho entidades han respondido que su sistema realiza copias de la información de trabajo.

b.- También siete entidades indican que su sistema de seguridad realiza copias de las aplicaciones en explotación, incluidos los sistemas operativos.

c.- En seis de ellas el sistema de seguridad realiza copias de los datos de configuración, aplicaciones y equipos.

d.- Siete de las ocho organizaciones indican que su sistema de seguridad realiza copia de claves para preservar la confidencialidad de la información.

e.- Seis de las ocho organizaciones indican que disponen de un sistema de backup redundante.

Pregunta 22 – Protección de las comunicaciones

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Controles de flujos de información que separe la red interna de la exterior	
Sistemas redundantes	
Controles para la protección de la confidencialidad de las comunicaciones	
Controles para la protección de la autenticidad e integridad de la información	
Redes segregadas	

a.- Siete entidades de las ocho encuestadas indican que tienen separada su red interna de su red externa. Es decir, que las comunicaciones de red con el exterior están diferenciadas técnicamente de las de interior

b.- Seis entidades indican que disponen de sistemas redundantes, es decir, sistemas que comparten ciertos tipos de ficheros. Esto quiere decir que ahorran espacio de cuotas de almacenamiento.

c.- Siete de las ocho organizaciones indican que disponen de controles para la protección de la confidencialidad de las comunicaciones.

d.- Cinco entidades responden que disponen de mecanismos de protección de la autenticidad e integración de la información. Esto implica que existe un mecanismo que asegure la integridad de los datos. Tres de ellas no disponen de este sistema.

e.- Seis de las ocho organizaciones indican que disponen de redes segregadas. Las otras dos organizaciones indican que no tienen su sistema configurado de esta forma, pudiendo ser debido a que no lo necesitan en su organización.

Pregunta 23 – Protección de los soportes de información

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Los soportes externos donde se guardar información, están etiquetados de forma que sin revelar su contenido se indique el nivel de seguridad de la información contenida	
Los usuarios están capacitados para entender el significado de les etiquetas	
Mecanismos criptográficos en dispositivos removibles con tal de garantizar la confidencialidad y la integridad de la información	
Mecanismos de custodia en los soportes de información de forma que se garantice su acceso y se respeten las exigencias del fabricante	
Controles de entrada y salida cuando la información se tiene que desplazar a un lugar externo	
Borrado de la información cuando se reutilizan soportes de información	

a.- Cuatro entidades indican que sus soportes externos están etiquetados, sin desvelar el nivel de seguridad de la información. Las otras cuatro entidades indican que no lo están. La no utilización de soportes etiquetados para identificar el nivel de información puede explicarse porque los datos están en unidades de almacenamiento centralizado.

b.- En consonancia con la anterior respuesta, solo cuatro entidades indican que los usuarios entienden el significado de las etiquetas.

c.- Sólo una entidad dispone de mecanismos criptográficos para garantizar la confidencialidad de la información. Las otras siete restantes indican que no disponen de ese mecanismo. Esta ausencia de respuesta general puede ser debido a que, con las autenticaciones de los usuarios en el sistema, sea suficiente y no necesiten mecanismos criptográficos para hacerlo.

d.- Respecto a los mecanismos de custodia, sólo cuatro entidades indican que disponen de estos mecanismos, respetando las exigencias del fabricante. Las otras cuatro indican que no disponen de ellos.

e.- Respecto a los registro de entrada y salida de información, seis entidades indican que disponen de registros de entrada y salida de información cuando se desplaza a un lugar externo. Dos de ellas no disponen de este registro, pudiendo indicar con ello que no lo necesiten porque la información se envíe por un conducto de comunicación electrónica interno.

f.- Cinco organizaciones de las ocho señalan que realizan borrado de información cuando se reutilizan soportes. Tres indican que no borran la información. Esta cuestión pone de manifiesto que, o no reutilizan soportes y por tanto se desechan con las medidas de seguridad pertinentes, o no se realiza la operación de borrado.

Pregunta 24 – Protección del software

Desarrollan aplicaciones de software propias ?	SI	NO
En caso afirmativo,		
¿Se realiza sobre un sistema diferente al de producción?	SI	NO
¿Aplican metodologías reconocidas en su desarrollo?	SI	NO
Las pruebas anteriores a la implantación no se realizan no datos reales	SI	NO
¿Se comprueba que se cumplen los criterios de aceptación en materia de seguridad?	SI	NO
Al poner en marcha el software nuevo, se comprueba que no se deteriora la seguridad de otros componentes?	SI	NO
Las pruebas de aceptación no se realizan con datos reales	SI	NO

Esta pregunta analiza el desarrollo y explotación del software, así como a su puesta en producción.

a.- Todas las organizaciones indican que disponen de desarrollo propio de aplicaciones. Esto pone de manifiesto que disponen de personal especializado para ello.

b.- Siete entidades señalan que el desarrollo de aplicaciones lo realizan en un sistema diferente al de producción.

c.- Seis de las ocho organizaciones indican que aplican metodologías de programación reconocidas en su desarrollo. Es decir, emplean técnicas de programación estandarizadas para el desarrollo de sus aplicaciones.

d.- Dos entidades manifiestan que las pruebas previas a la implantación de una aplicación no se realizan con datos reales. Las otras seis entidades indican que las pruebas las realizan con datos reales.

e.- De las ocho organizaciones, siete constatan que se comprueba que sus aplicaciones cumplen criterios de aceptación en materia de seguridad. Sólo una entidad indica que no se realiza esta comprobación.

f.- Todas las entidades indican que realizan la comprobación de que no se deteriora la seguridad de otros componentes de software. Esto es, no se ralentiza el sistema y las otras aplicaciones no muestran pérdida de datos. También indica que la aplicación de otras medidas de seguridad que realicen las organizaciones tampoco deteriora la seguridad.

g.- Cinco entidades manifiestan que las pruebas de aceptación de la aplicación no se realizan con datos reales. Sin embargo, las pruebas de aceptación del software sí las realizan con datos reales.

Pregunta 25 – Protección de la información

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Procedimientos para cualificar la información	
Procedimientos de cifrados de la información	
Procedimientos que empleen la firma electrónica	
Procedimientos de mecanismos de sellado de tiempo (time stamping)	
Procedimientos de limpieza de documentos que garanticen la confidencialidad de la información	

En esta pregunta se trata de analizar las medidas de protección de la información.

a.- Dos entidades han respondido que disponen de mecanismos para cualificar la información.

b.- Cinco de ellas indican que disponen de procedimientos de cifrado de la información. Tres manifiestan que no disponen de métodos de cifrado de información.

c.- Cinco de las ocho entidades argumentan que disponen de procedimientos que emplean firma electrónica. Tres constatan que no disponen de ese procedimiento.

d.- Una entidad señala que dispone de mecanismos de sellado de tiempo. Es decir, la validación de un documento electrónico a través del tiempo.

e.- Dos entidades han manifestado que disponen de procedimientos de limpieza de documentos para garantizar la información.

6.6 Análisis de Riesgos en las entidades sanitarias

La norma ISO 31000:2009 de gestión de riesgos propone un proceso de gestión de riesgos. Así se describen cinco pasos generales

- Comunicación y consulta
- Establecimiento del contexto
- Evaluación del riesgo (se subdivide en 3 apartados)
    - Identificación del riesgo
    - Análisis del riesgo
    - Evaluación del riesgo
- Tratamiento del riesgo
- Monitorización y revisión

En el estudio realizado a las entidades sobre las que se trabaja, no se han abordado las dos últimas etapas el tratamiento del riesgo y su monitorización. La realización y ejecución de estos dos pasos correspondería directamente a las entidades de gestión sanitaria. Así pues, lo que se ha realizado es una propuesta de evaluación de riesgos contextualizada dentro del ámbito de las historias clínicas y de la preservación digital.

En los siguientes apartados se expondrán todos los procesos marcados por la norma ISO 31000:2009.

6.6.1 Comunicación y consulta

El primer paso, comunicación y consulta, se ha realizado como consecuencia de que en las encuestas enviadas a las entidades de gestión sanitaria, sólo una de las entidades indicaba que había realizado análisis de riesgos de sus sistemas de información. Esto se ha podido comprobar posteriormente en las entrevistas realizadas.

El no empleo del análisis de riesgos se debe a la falta de suficiente presupuesto para ello. Por otro lado, realizar la evaluación de una normativa ISO no es de obligatorio cumplimiento. La acreditación de una norma ISO indica la forma en que trabaja una determinada organización, siendo a la vez un crédito para la misma. Evidentemente, la acreditación de una normativa ISO es costosa, tanto en recursos humanos como técnicos. Por ello, difícilmente se encontrará una organización que disponga de todo su proceso de trabajo acreditado con normativas ISO.

En nuestro caso se ha decidido pues, evaluar el riesgo analizando como estaba configurado el sistema de información de las organizaciones sanitarias, que tipos de conexiones había con el exterior y los permisos de los usuarios.

6.6.2 Establecimiento del contexto

En el establecimiento del contexto se pone de manifiesto que el tratamiento de las historias clínicas electrónicas exige que no haya fugas de datos dentro de la propia organización, ni peligros de que la información contenida se corrompa. El objetivo del contexto se puede aplicar después a un repositorio digital que contenga las historias clínicas. Se persigue saber, especialmente, qué amenazas tienen las historias clínicas electrónicas, así como la forma de poder mitigar estas amenazas.

6.6.3 Evaluación del riesgo

Una vez se han recibido las encuestas de las entidades sanitarias y analizado el cuestionario para detectar sus necesidades en la preservación digital, se ha observado que no realizan de forma generalizada un análisis de riesgos en su sistema de información. Tan sólo una organización indicaba que había realizado una certificación de gestión de riesgos.

6.6.3.1 Identificación del riesgo

A fin de identificar los riesgos y de una forma muy básica, se procedió a enviar, junto con las entrevistas finales del cuestionario de auditoría, un cuestionario sobre estructuras informáticas, a fin de obtener información para proceder al análisis de riesgos, tal y como se indicó en el Capítulo 1.

Todas las preguntas se han hecho de forma general, teniendo en cuenta las respuestas de los centros en las encuestas de auditoría. Es importante recordar que es una evaluación de riesgos de aquellos elementos o personas que afectan a las historias clínicas digitales. Por tanto, estamos refiriéndonos a la gestión de riesgos del sistema de información de la entidad y no de otros procesos, como podrían ser flujos económicos o laborales. El cuestionario aplicado es el siguiente:

Infraestructura informática

- ¿Cuántos servidores tienen?
- ¿Bajo qué sistema operativo funcionan?
- Describa la base de datos donde se encuentran las historias clínicas aunque esta sea de desarrollo propio.

- ¿Cuántos terminales se conectan al servidor? ¿Bajo qué sistema operativo?
- Si todos los terminales tienen la misma configuración la respuesta es 1. Si hay diferentes configuraciones sumaremos 1.
- ¿Tienen los puertos USB-Infrarrojos-Bluetooth habilitados o deshabilitados?
- ¿Cuántas impresoras están conectadas a los terminales?
- ¿Cuántos usuarios tienen? ¿Los tienen estratificados?
- ¿Cuántos equipos médicos están integrados en alguno de los servidores?
- Si tienen el acceso remoto, describa como es (ej: VPN, https, ssh)

Las respuestas se resumen en la Tabla 14, donde la última columna de la derecha muestra una entidad modelo (ESn), basada en las respuestas de las anteriores. Esta entidad modelo se ha empleado después para realizar análisis de riesgos. De esta forma, se puede mantener el anonimato de todas las entidades y no se repite un análisis de riesgos por cada entidad, que nos daría resultados muy similares entre todas ellas.

Infraestructura técnica	**ES1**	**ES2**	**ES3**	**ES4**	**ES5**	**ES6**	**ES7**	**ES8**	**ESn**
Núm servidores	7	20	3	3	2	3	15	2	1
Sist. Operativo	Windows 2003	Solaris 10, Win 2003	UNIX	LINUX	W2003	Windows Server 2005	W2003	LINUX	WIN,LIN,UNIX
Base de datos	CACHE	Universe, Microsoft SQL Server	INFORMIX	CACHE	CACHE	CACHE	HNET	HCIS	CACHE
Núm. de Terminales	1000 (Win XP)	1300 (Win XP)	700 (Win XP)	150 (Win XP)	80 (Win XP)	500 (Win XP)	700 (Win XP)	1200 (Win Xp)	1 (WinXp)
USB-Bluetooth	Habilitado	Deshabilitado	Habilitado	Habilitado	Habilitado	Habilitado	Habilitado	Habilitado	Habilitado
Impresoras	500	250	300	150	300	90	700	600	1
Usuarios	2000	2460	1400	150	300	250	2000	2500	1
Estratificación	4 grupos	4 grupos	4 grupos	5 grupos	4 grupos	5 grupos	4 grupos	5 grupos	4
Equipos médicos integrados	10	48	4	1	10 -	15	20	50	1
Acceso remoto	Fibra Óptica Punto a Punto	VPN, http con ssh	Sistema cerrado	VPN	No hay	VPN, pero no se accede a las HCE	Terminal Server	VPN, CITRIX	VPN

Tabla 14. Estructuras técnicas de las entidades sanitarias.

6.6.3.2 *Análisis del riesgo*

En este apartado de análisis del riesgo se ha empleado el software PILAR, programa de análisis de riesgos interactivo que permite analizar una organización identificando los activos y sus amenazas, calculando posteriormente los riesgos y su impacto en una organización.

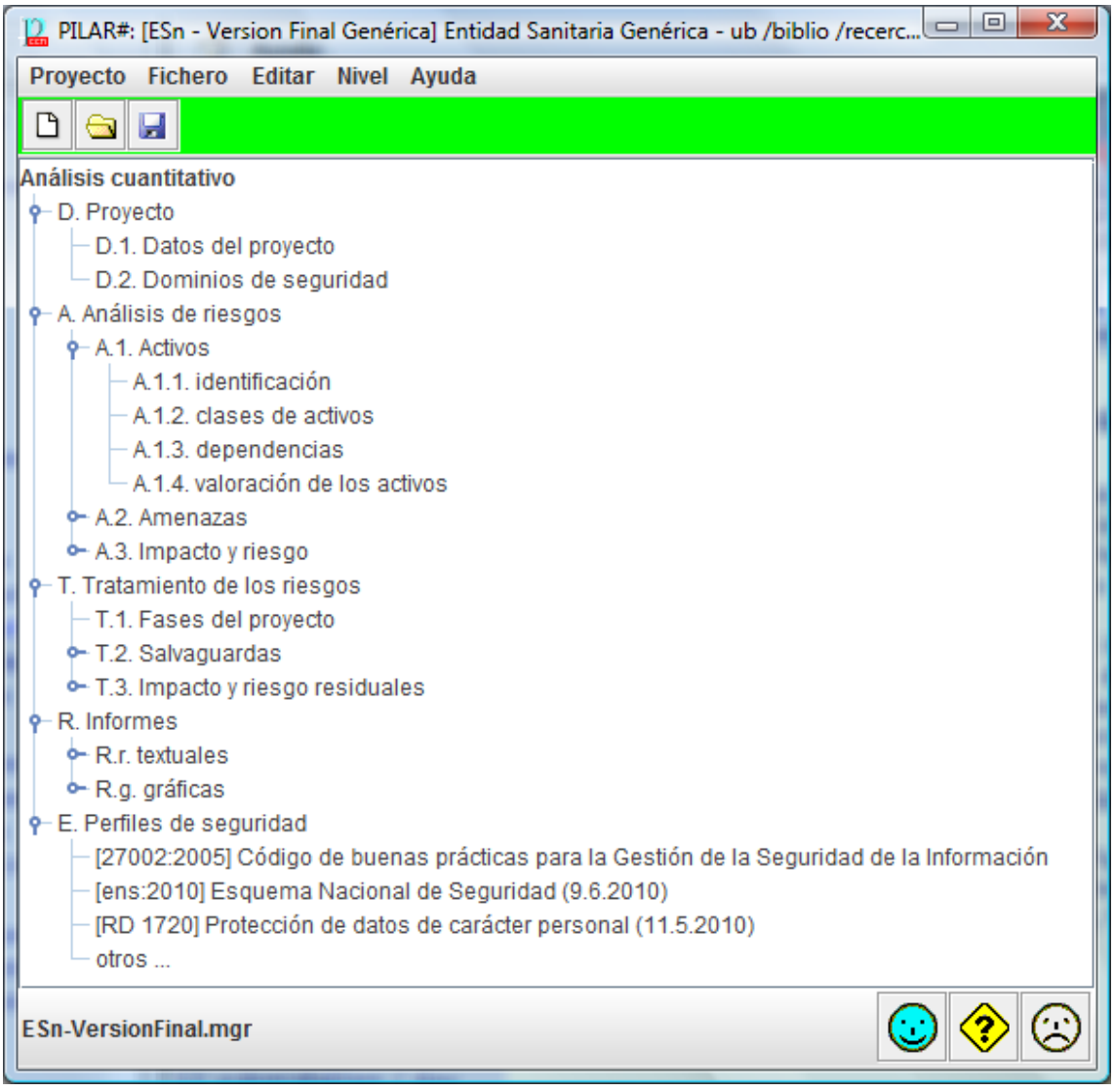

Figura 13. Programa PILAR.

PILAR permite realizar análisis de riesgos de forma cuantitativa y cualitativa, siguiendo la Metodología de Análisis y Gestión de Riesgos de los

Sistemas de Información (MAGERIT). Esta metodología está publicada por el Ministerio de Administraciones Públicas. En el caso de este estudio, se ha trabajado de forma cuantitativa. En la Figura 13 se muestra el aspecto de la interficie del programa PILAR.

El programa PILAR permite trabajar en tres modos: Básico, Medio y Experto. La diferencia existente entre los tres niveles es la mejora de los análisis de los activos, así como la muestra de más informes, tanto de impacto como de amenazas. El objetivo de su utilización en este estudio se debe a que las entidades sanitarias que han colaborado en el estudio, han indicado que no se han realizado análisis de riesgos alguno en sus departamentos de IT.

Uno de los aspectos en los que incide tanto la metodología TRAC como PILAR, es en la realización de análisis de riesgos. De esta forma, se pueden ver las lagunas existentes en la unidad de información, y aplicar métodos de corrección necesarios. En nuestro estudio se ha empleado el modo Básico de PILAR, ya que es un análisis de riesgos genérico aplicable a otras entidades. Además, el hecho de no disponer de información más profunda sobre los sistemas de información de las organizaciones de gestión sanitaria, hace que emplear el modo Básico sea el más adecuado para este estudio.

6.6.3.3 Evaluación de riesgos de una entidad genérica

A fin de poder realizar un análisis de riesgos objetivo, se ha procedido a generar una Entidad Sanitaria n, genérica. (ESn). Como se puede observar en la Tabla 14, todas las entidades sanitarias disponen de organizaciones a nivel de IT similares. Se pueden encontrar cambios en los sistemas operativos o en el tipo de gestor de bases de datos, pero la configuración ante los usuarios de que disponen las entidades y su estratificación, hace que sean similares, a grandes rasgos. Debido a esto, y teniendo en cuenta que lo que las diferencia son el

tratamiento de la información, que es propio a cada institución, se ha creado una entidad que disponga una configuración similar a las de las otras entidades. De esta forma, se evita la duplicidad de datos y permite disponer de datos más objetivos. Además, se evita relevar datos que puedan afectar a la seguridad y confidencialidad de las propias empresas.

La entidad sanitaria genérica dispone de una configuración similar a las participantes en el estudio, como se ha indicado anteriormente. Es decir, se trataría de una entidad que dispondrá de un servidor, bajo un sistema operativo que pueda ser LINUX, WINDOWS o UNIX, con un terminal que funciona bajo un sistema operativo Windows XP, además de disponer de un equipo médico integrado PAC, cuatro grupos de usuarios estratificados, terminales USB habilitados, acceso remoto tipo VPN. Finalmente, dispondrá de un tipo de gestor de base de datos CACHE y una impresora. Esta configuración queda resumida en la Tabla 15.

Infraestructura técnica	**ESn**
Núm servidores	1
Sist. Operativo	WIN,LIN,UNIX
Base de datos	CACHE
Núm. de Terminales	1 (WinXp)
USB-Bluetooth	Habilitado
Impresoras	1
Usuarios	1
Estratificación personal	4
Equipos médicos integrados	1
Acceso remoto	VPN

Tabla 15. Descripción de una entidad genérica.

En el análisis de riesgos con el programa PILAR, se ha realizado una definición de activos, simplificando la estructura al mínimo, a fin de evitar duplicidades dentro del programa. Así, si un equipo es igual que otro teniendo la misma configuración, el equipo que está en riesgo es uno aunque se

dispongan de mil (1000) terminales, como el caso de algunas entidades. El riesgo será el mismo para uno (1) que para mil (1000).

Todas las entidades que han participado en el estudio tienen equipos médicos integrados, normalmente equipos radiológicos, cuya información va directamente al servidor y a la historia clínica electrónica del paciente, dentro de su proceso asistencial. Es por este motivo que en la definición de activos en el programa PILAR, se ha creado además un equipo informático integrado, PACS (Picture Archiving Communication System), ya que todas las entidades sanitarias disponen de varios conectados con las historias clínicas. En este caso se le ha dado el nombre de PAC y engloba aparatos genéricos que bien podrían ser dispositivos radiográficos, ecógrafos u otro dispositivo, que permitan extraer datos de un paciente en un proceso asistencial e incorporarlos a su historia médica de forma electrónica.

A pesar de que algunas entidades tienen un acceso cerrado a sus historias clínicas, se ha procedido a definir una conexión VPN para acceder desde otro centro sanitario.

En el Anexo VI se puede observar la definición de los activos definidos en el programa PILAR.

6.6.3.4 Informe gráfico de riesgo

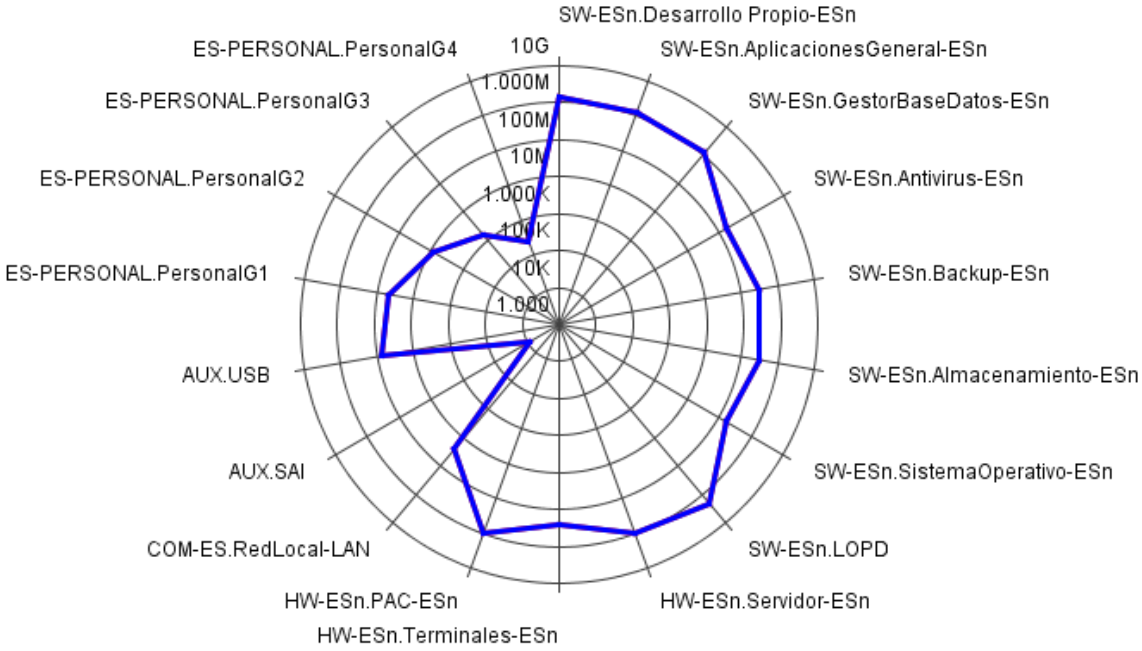

Figura 14. Diagrama de análisis de riesgos.

En la Figura 14 se puede ver por cada activo la situación de riesgo de cada activo declarado. Así, se puede observar que aquellos activos que están declarados como SW (Software) tienen mucho más riesgos que otros. Si se observa el concepto de personal, aquellos que están definidos en Personal G1, estos tienen mucho más riesgo respecto a los que están declarados en Personal G4. Esto es debido a que se generaron cuatro grupos de personal, con diferentes prioridades de riesgo. Así, G1 tenía más prioridad sobre el sistema, por tanto más riesgo y más posibilidad de hacer daño al sistema que el personal de G4. No se puede diferenciar una clasificación de qué personal correspondería a G1, G2, G3, o G4. Eso dependerá de cada organización y los accesos que se faciliten a los grupos.

También se puede ver que los elementos de HW (Hardware) son elementos que tienen un alto nivel de riesgo, ya que son vulnerables. Esto es válido tanto para el servidor como para los terminales.

Corresponderá a la institución las medidas a tomar en función de los riesgos que tienen estos dispositivos.

6.6.4 Conclusiones al análisis de riesgos en las entidades sanitarias

La medición y evaluación de riesgos puede ser asociada a muchas disciplinas, como la informática o la medicina. Aún así, empiezan a existir iniciativas de medición para la evaluación de riesgos en la preservación digital. El uso de una metodología permite evaluar los riesgos en los repositorios de forma cuantitativa.

Para poder llevar a cabo una metodología, se requiere de medidas de análisis concretas siguiendo los estándares actuales. Debido a la complejidad del análisis, es recomendable que se emplee software que ayude a la evaluación de riesgos. Este permite definir tanto los activos como los riesgos y su impacto dentro de una organización. Es evidente que el análisis de riesgos siempre es subjetivo respecto a una organización, pero mejor tener mediciones subjetivas que no tener ningún parámetro del que se pueda disponer. Una laguna importante que se puede encontrar en el análisis de riesgos realizado es aquellos riesgos que explícitamente corresponderían a la preservación digital. Así, elementos como la obsolescencia o el riesgo de realizar la migración, no se pueden medir concretamente con este software, si bien cubre la mayor parte de las necesidades de una institución.

Capítulo 7

Modelo de preservación digital aplicando el modelo OAIS

7 Modelo de preservación digital aplicando el modelo OAIS

7.1 Presentación general de la propuesta

Una vez analizado el cuestionario de auditoría sobre las necesidades de preservación digital, así como los datos obtenidos en las entrevistas finales, que han permitido realizar el análisis de riesgos, se propone un modelo de preservación digital basado en la simplificación del modelo OAI, tomando estos datos como punto de partida.

Es importante tener en cuenta que se está trabajando en entornos cerrados, es decir, ninguna entidad tiene sus sistemas relativos a las HCE conectados a internet. Aún así, como se ha podido comprobar en el análisis de riesgos, existen indicadores con valores elevados que señalan las precauciones a tomar a este respecto.

Un archivo OAIS, como se ve en la Figura 5, dispone, como se ha indicado en el Capítulo 5, de seis funcionalidades, que son las siguientes: Ingesta (Ingest), Administración (Administration), Planificación de la Preservación (Preservation Planning), Gestión de los Datos (Data Management), Archivo de Almacenamiento (Archival Storage) y Acceso (Access). Se expondrá sucintamente una recapitulación de las seis funcionalidades.

- Ingesta (Ingest) es el proceso que se encarga de recibir los paquetes de información y de añadir los metadatos correspondientes para convertir el objeto en archivable. Estos metadatos como se ha especificado en el Capítulo 5, formarán parte del Paquete de Información Archivable (AIP).

- Administración (Administration) facilita las funciones para la gestión del archivo completo.

- Planificación de la Preservación (Preservation Planning) facilita recomendaciones para asegurar que la información almacenada en un archivo OAIS es accesible a la Comunidad Designada, incluso si el entorno se vuelve obsoleto.

- Gestión de los Datos (Data Management) facilita los servicios y funciones para mantener la Información Descriptiva (Descriptive Information) y los datos administrativos para la gestión de los datos.

- Archivo de Almacenamiento (Archival Storage) gestiona el almacenamiento de los datos, y facilita la capacidad de recuperación de los mismos.

- Acceso (Access) permite realizar funciones de recuperación de la información a los consumidores, incluida la denegación de acceso.

De acuerdo con los resultados obtenidos en el análisis de las respuestas de las encuestas de auditoría así como en las entrevistas finales realizadas, se propone una reducción de las entidades funcionales del modelo OAIS como se puede observar en la Figura 15.

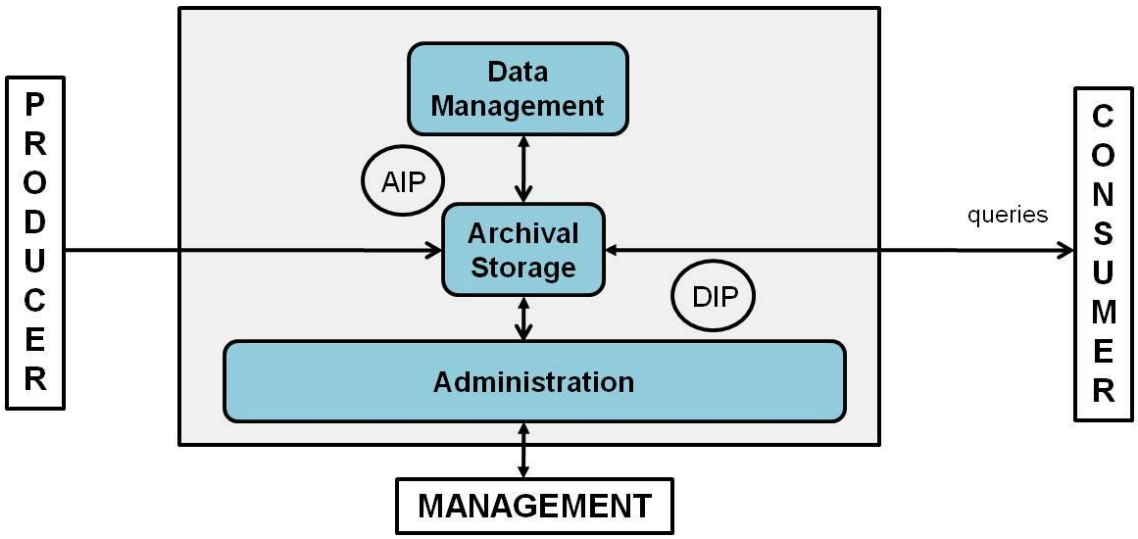

Figura 15. Propuesta de modelo de archivo OAIS simplificado para instituciones sanitarias.

Si se compara esta figura con la Figura 5, se puede observar que se propone la simplificación de las funcionalidades Ingesta (Ingest), Planificación de la Preservación (Preservation Planning) y Acceso (Access).

Ingesta (Ingest) se simplifica por las razones que se exponen a continuación. El contenido de las Historias Clínicas Electrónicas (HCE) es información que se introduce en el sistema a medida que el paciente está siendo atendido, es decir, durante el proceso asistencial. Cuando este proceso ha finalizado, la información no se extrae, ni se elimina, simplemente reside en el sistema, almacenada, ocupando espacio de almacenamiento. Por tanto, no existirá un paquete de información que sea introducido, como se indica en el archivo OAIS, sino que la información ya estará introducida y auditada. El único parámetro que necesitarán añadir las HCE será un nivel de metadatos, mediante una estructura como PREMIS, que contribuya a generar el Paquete de Información Archivable (AIP), es decir, que la historia clínica electrónica sea un objeto archivable a largo plazo.

Hay que tener en cuenta que la HCE sólo se recupera cuando el paciente vuelve al cabo de un tiempo para un proceso asistencial o en casos de necesidad a efectos de investigación. Esto puede suceder una vez cerrado el proceso asistencial inicial o unos cuántos años después, si se diese el caso. Si el tiempo es superior a tres años, que es la media que han indicado todas las entidades colaboradoras en el proyecto de investigación, la historia clínica electrónica ya ha pasado a ser un objeto pasivo que ocupa su espacio de almacenamiento. En consecuencia, pasado este tiempo será un objeto archivable AIP.

La entidad funcional Planificación de la Preservación (Preservation Planning) también se simplifica. Todo el estudio presentado en las páginas anteriores forma parte de la Planificación de la Preservación. Esta planificación se ha llevado a cabo mediante dos procesos. El primero se realizó con la utilización de la metodología TRAC y del Esquema Nacional de Seguridad, y la realización de encuestas y posteriores entrevistas. El segundo proceso consistió en la realización de un análisis de riesgos, empleando la metodología MAGERIT aplicada con el software PILAR (5.1.3-13/07/2011), con la que se evaluaron tanto el sistema como los formatos existentes.

La entidad funcional Acceso (Access) se simplifica por razones similares a Ingesta (Ingest). El Consumidor demanda una historia clínica a través de una consulta (queries) a la entidad funcional Archivo de Almacenamiento (Archival Storage). Esta historia clínica vendrá representada por un Paquete de Diseminación de la Información (Dissemination Information Package, DIP), que será el objeto que el Consumidor recibirá. Para que el Consumidor reciba de forma adecuada el DIP, será necesario extraer la información con los metadatos incluidos y presentar la información en el soporte más adecuado para el Consumidor.

7.2 Simplificación de la entidad funcional Ingesta

De esta entidad se simplifican las siguientes funciones:

Recepción de la Sumisión (Receive Submission): de acuerdo con su descripción en el modelo OAIS, se encarga de facilitar la apropiada capacidad de almacenamiento desde el Productor o desde el Administrador. De acuerdo con los datos obtenidos a través del análisis de las entrevistas finales realizadas y con la encuesta de auditoría, las historias clínicas ya están introducidas y, por tanto, una vez finalizado el proceso asistencial residen en el sistema y no es necesario un envío de paquetes de información.

Aseguramiento de la calidad (Quality Assurance): es un mecanismo encargado de que la transferencia de datos sea correcta mediante Comprobaciones de Redundancia Cíclica (CRC). En el caso de las historias clínicas, no hay transferencia sino que se introducen a medida que se realizan. Además, la información es auditada anualmente por el CMDB, del Departament de Salut de la Generalitat de Catalunya, con las implicaciones que esto conlleva atendiendo a la integridad de los datos.

Generar AIP (Generate AIP): es una función que se encarga de convertir SIP en AIP para formatear la información de forma estándar, acorde con el archivo. En este caso, al estar ya introducidas las historias clínicas, todas cumplen con el estándar de acceso la interoperabilidad, el estándar HL7. Por tanto, esta función no es necesaria.

Generación de Información Descriptiva (Generate Descriptive Information): esta función es la encargada de extraer información de los AIP, que en este caso serán la historia clínica en su conjunto, para enviarla a la entidad funcional Gestión de Datos (Data Management). La función permite después recuperar el

objeto archivado a largo plazo, mediante el uso de metadatos. A su vez, esta información descriptiva permite controlar los formatos de ficheros que contiene el AIP, a fin de poder aplicar posteriormente correcciones en la Planificación de la Preservación. Esta función no se simplifica, ya que es la encargada de la extracción/generación de metadatos para después poder recuperar la información. La propuesta es generar metadatos PREMIS sobre las historias clínicas. Sin embargo, y puesto que se simplifica la entidad funcional de INGEST, este módulo se incluirá en la entidad de Almacenamiento de Archivos (Archival Storage).

Coordinación de las Actualizaciones (Coordinate Updates): esta función, como se ha comentado previamente, permite coordinar el envío de AIPs al Archivo de Almacenamiento (Archival Storage) y la Información Descriptiva (Descriptive Information) a Gestión de Datos (Data Management). En el caso de las HCE, la información ya está almacenada y sólo habría que enviar la Información Descriptiva (Descriptive Information) a la entidad funcional Gestión de Datos (Data Management).

7.3 Simplificación de la entidad funcional Almacenamiento de Archivo

La entidad funcional Almacenamiento de Archivo, es quizás una de las funciones más relevantes de un archivo OAIS, ya que es la encargada de almacenar la información en el medio físico. Aún así, se propone simplificar esta entidad de la siguiente forma:

Recepción de Datos (Receive Data): esta función, que antes existía como se refleja en la Figura 7, ahora se simplifica dado que no existe recepción de datos. Como se puede observar en la Figura 16, es el Productor el que ya ha

introducido los datos, y por tanto, la información ya está en el sistema con su información descriptiva.

Generación de Información Descriptiva (Generate descriptive Info): esta función, que antes se encontraba en Ingesta (Ingest), ahora se emplaza a esta entidad funcional. Esto se debe a que esta función es necesaria para generar los metadatos para la conservación digital, o sea convertir las HCE en AIP.

Substitución de Medios (Replace Media): reproduce AIPS en el tiempo. Sirve para hacer las migraciones o desplazamientos en el sistema. Esta función es necesaria si hay que realizar copias hacia un sistema de almacenamiento nuevo. Durante su ejecución, el Contenido de la Información (Content Information) y Preservación de la Descripción de la Información (Preservation Description Information, PDI) no se deben alterar.

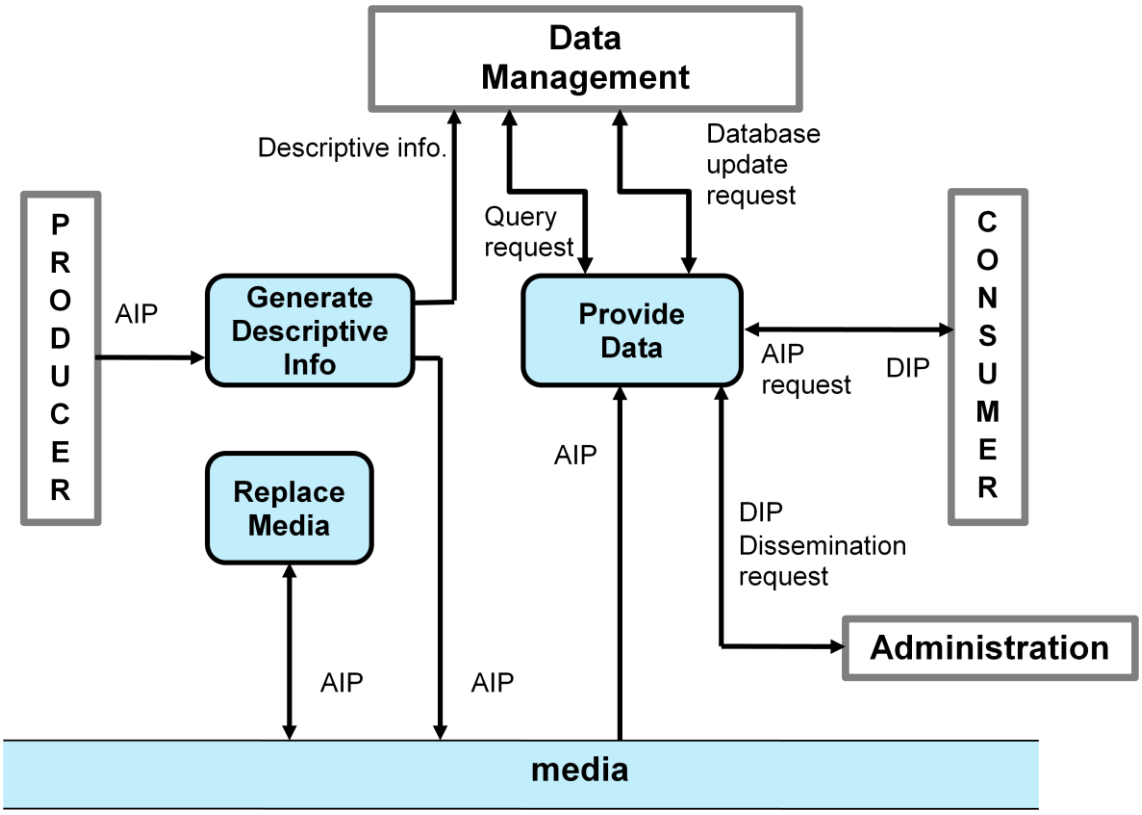

Figura 16. Entidad funcional Almacenamiento de Archivos (Archival Storage) simplificada.

Jerarquía de Gestión del Almacenamiento (Manage Storage Hierarchy): esta función permite situar los AIPS en el medio de almacenamiento adecuado, añadiendo si es necesario políticas correctas de seguridad. Esta función se puede simplificar porque el AIP o la historia clínica siempre van al mismo sitio y no vienen transferidas por la entidad funcional Ingesta, sino por el Productor. Asimismo, la función Comprobación de Errores (Error Checking), complementaria a la función anterior, también se puede simplificar. De acuerdo con las encuestas realizadas, esta función actualmente ya está siendo implementada debido a la auditoria de los datos y, por lo tanto, se ha de evitar su duplicidad.

Recuperación frente a Desastres (Disaster Recovery): esta función permite copiar todo el contenido de la información digital y duplicarlo en un volumen de información separado. Esta función también se puede simplificar ya que todas las entidades realizan copias de respaldo redundantes, es decir, ya existe el mecanismo adecuado para las copias de seguridad.

Facilitador de Datos (Provide Data): esta función se encarga de realizar copias de los AIPS para tener el acceso a la información. En nuestro caso, esta función crearía una copia exacta, generando el DIP de la historia clínica desde el momento en que se finalizó el proceso asistencial, teniendo en cuenta los formatos técnicos asociados a la historia clínica electrónica.

7.4 Simplificación de la entidad funcional Gestión de Datos

Como se ha indicado previamente, la entidad funcional Gestión de Datos (Data Management), facilita los servicios y funciones para mantener la Información Descriptiva (Descriptive Information) que identifica y documenta los datos necesarios para gestionar el archivo. Esta función es necesaria en su totalidad,

ya que sin esta entidad funcional no se podría disponer de los elementos necesarios para detectar obsolescencia de formatos digitales almacenados.

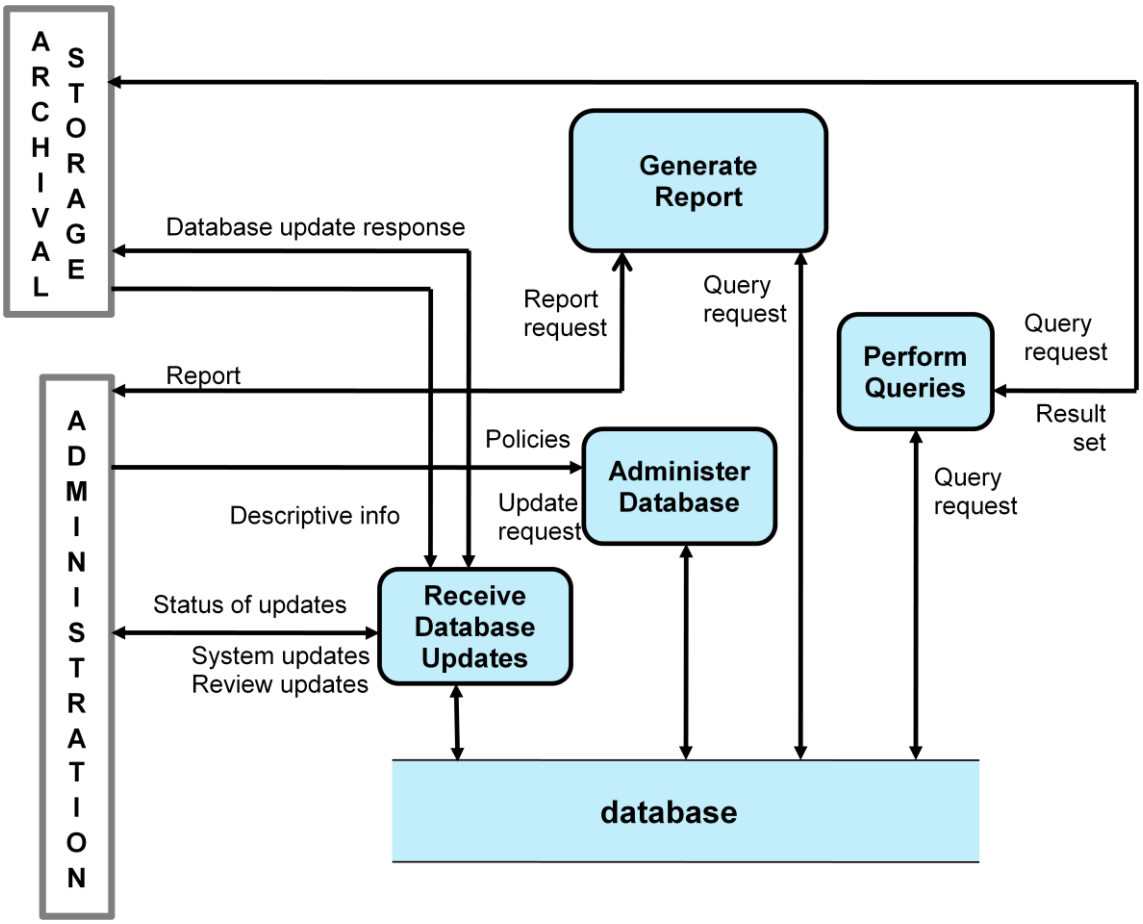

Figura 17. Simplificación de la entidad funcional Gestión de Datos (Data Management).

En la Figura 17 se puede observar que la función Ingesta (Ingest) es la encargada de pedir un informe estadístico, de actualizar la base de datos con nuevos AIP o de realizar la modificación de los mismos. Debido a la simplificación de la función Ingesta (Ingest), se produce un cambio desde la función Almacenamiento de Archivos (Archival Storage) que a través de la función Receive Database Updates genera la Información Descriptiva (Descriptive Information), y actualizará la información relativa al AIP, como se puede ver en la Figura 17.

Generación de Informe (Generate Report): esta función se generará por la entidad Administración (Administration), ya que Acceso (Access), que será generado por el profesional que requiere los datos, necesitará un AIP y no una estadística sobre el archivo en sí. Esta función sólo deberá ser ejecutada por la entidad Administración, vía Gestión (Management) del archivo, quién necesitará los informes a efectos de mantenimiento del archivo OAIS.

7.5 Simplificación de la entidad funcional Administración

Esta entidad funcional es la más compleja de todas, como se puede observar en la Figura 9, puesto que es la encargada de la gestión de todo el archivo OAIS. Es por esto que, habiendo simplificado otras entidades funcionales como Ingesta (Ingest) o Planificación de la Preservación (Preservation Planning), también sufrirá algunos cambios.

Como se ve en la Figura 18 y comparando respecto a la Figura 9, todas las funciones vinculadas a Ingesta (Ingest), Planificación de la Preservación (Preservation Planning) y Productor (Producer), se reducen, puesto que son funciones simplificadas.

Acuerdos de la Negociación de la Sumisión (Negotiate Submission Agreement): esta función se reduce, porque al desaparecer la ingesta de datos no hay acuerdos de sumisión en el archivo. Estos acuerdos no existirán en una entidad médica, porque se recuperará o guardará información que ya ha sido previamente introducida y auditada.

Auditoría de la Sumisión (Audit Submission): esta función ha de comprobar que los SIP y los AIP cumplen las especificaciones del archivo. En el caso de este estudio, la información es homogénea, es decir siempre será el mismo tipo de información la que se archivará y no habrá terceras partes. Será la propia

entidad sanitaria la que genere y recupere los datos que, a su vez, serán auditados para verificar su calidad.

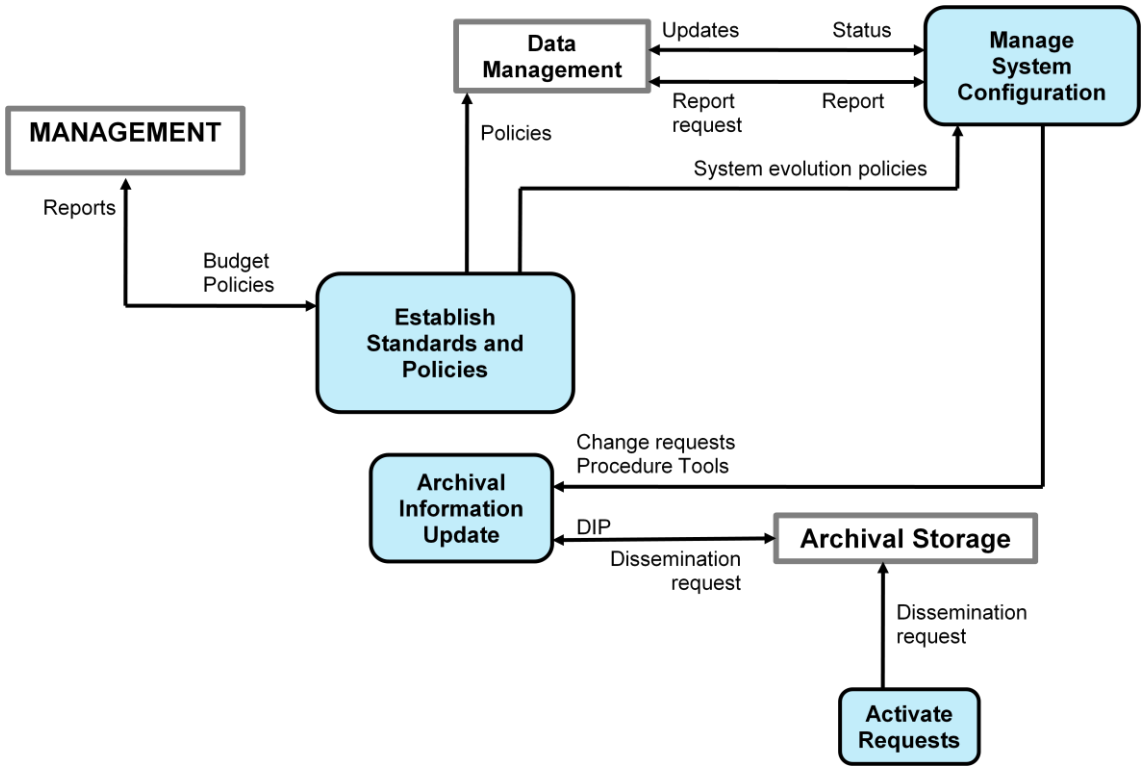

Figura 18. Reducción de la entidad funcional Administración (Administration).

Activación de la Petición (Activate Request): esta función se hace necesaria ya que permite crear peticiones de difusión de la información.

Control de Acceso Físico (Physical Access Control): esta función es la encargada de disponer de mecanismos para restringir el acceso a elementos del archivo. Como se puede observar en las encuestas realizadas, esta función existe en todas las entidades consultadas actualmente, por lo cual se realiza su simplificación.

Actualización de la Información del Archivo (Archival Information Update): facilita mecanismos para actualizar los contenidos del archivo OAIS. En este caso, esta función es imprescindible.

Establecimiento de Estándares y Políticas (Establish Standards and Policies): es una función encargada de mantener las políticas y estándares del archivo OAIS. Esta función es imprescindible, ya que es posible que más adelante se deban añadir más estándares, lo que obliga a la existencia de esta función.

Sistema de Gestión de la Configuración (Manage Configuration System): es una función que monitoriza constantemente el archivo a nivel tecnológico. Depende de la anterior y ayuda a mantener el archivo OAIS.

Servicio al Cliente (Customer Service): esta función es la encargada de mantener las cuentas de los consumidores, además de generar la información de facturación. Se considera que no tiene utilidad tal y como está planteada, ya que no se realizan funciones de facturación por petición de información. Actualmente, en las entidades de gestión hospitalaria, esta función no existe. Por otro lado, las cuentas de los consumidores se generan dentro del sistema de IT general y será otra función, fuera del archivo OAIS, la que permitirá la manipulación de las cuentas de la Comunidad Designada.

7.6 Simplificación de la entidad funcional Planificación de la Preservación

Como se ha explicado anteriormente y se representa en la Figura 10, la función Planificación de la Preservación (Preservation Planning) se simplifica totalmente en el modelo de archivo OAIS que se propone.

Monitorización de la Comunidad Designada (Monitor Designated Community): esta función se encarga de interactuar con los Consumidores y Productores, a fin de registrar sus requerimientos de servicio. De acuerdo con el modelo OAIS (CCSDS, 2002), está función se puede implementar como un

servicio solicitando retroalimentación a la Comunidad Designada. La encuesta de auditoría, que disponía de 25 preguntas, formaría parte de este servicio.

Monitorización de la Tecnología (Monitor Technology): esta función se encarga de monitorizar las tecnologías que pueden causar obsolescencia en el entorno informatizado del archivo. Esta función se puede eliminar ya que los nuevos sistemas que pueden aparecer de gestión de historias clínicas electrónicas serán compatibles con el protocolo HL7, a fin de facilitar su interconexión con otros sistemas previos.

Desarrollo de Estrategias de Preservación y Estándares (Develop Preservation Strategies and Standards): es una función encargada de recomendar estrategias y nuevos estándares de conservación para anticiparse a los cambios.

Desarrollo de Diseño de Empaquetamiento y Planes de Migración (Develop Packaging Design and Migration Plans): esta función es la encargada de llevar a cabo las políticas de migración y los prototipos para implementar las políticas de Administración. Actualmente, esta función no tiene sentido alguno, ya que todos los hospitales que han participado en el estudio están en un estado inicial donde toda su información está bajo un solo estándar de intercomunicación de datos, el formato HL7.

7.7 Simplificación de la entidad funcional Acceso

Esta función se simplifica en su totalidad excepto en la función Generación de DIP (Generate DIP), ya que si bien en el proceso de Ingesta (Ingest) los datos estaban en el sistema y por tanto sólo se necesita de una capa de metadatos como PREMIS, en esta ocasión se prepara el paquete de información para su difusión generando un DIP.

Generación de DIP (Generate DIP): es una función que acepta una petición de diseminación (dissemination request), recupera el AIP de la entidad funcional Almacenamiento de Archivos (Archival Storage) y realiza una copia de los datos para ser procesada. Hay que recordar que la finalidad de un archivo OAIS es entregar una copia de un objeto digital en las mismas condiciones en las que se creó.

Esta función estará enmarcada dentro de la funcionalidad Almacenamiento de Archivo (Archival Storage), como se ve en la Figura 16.

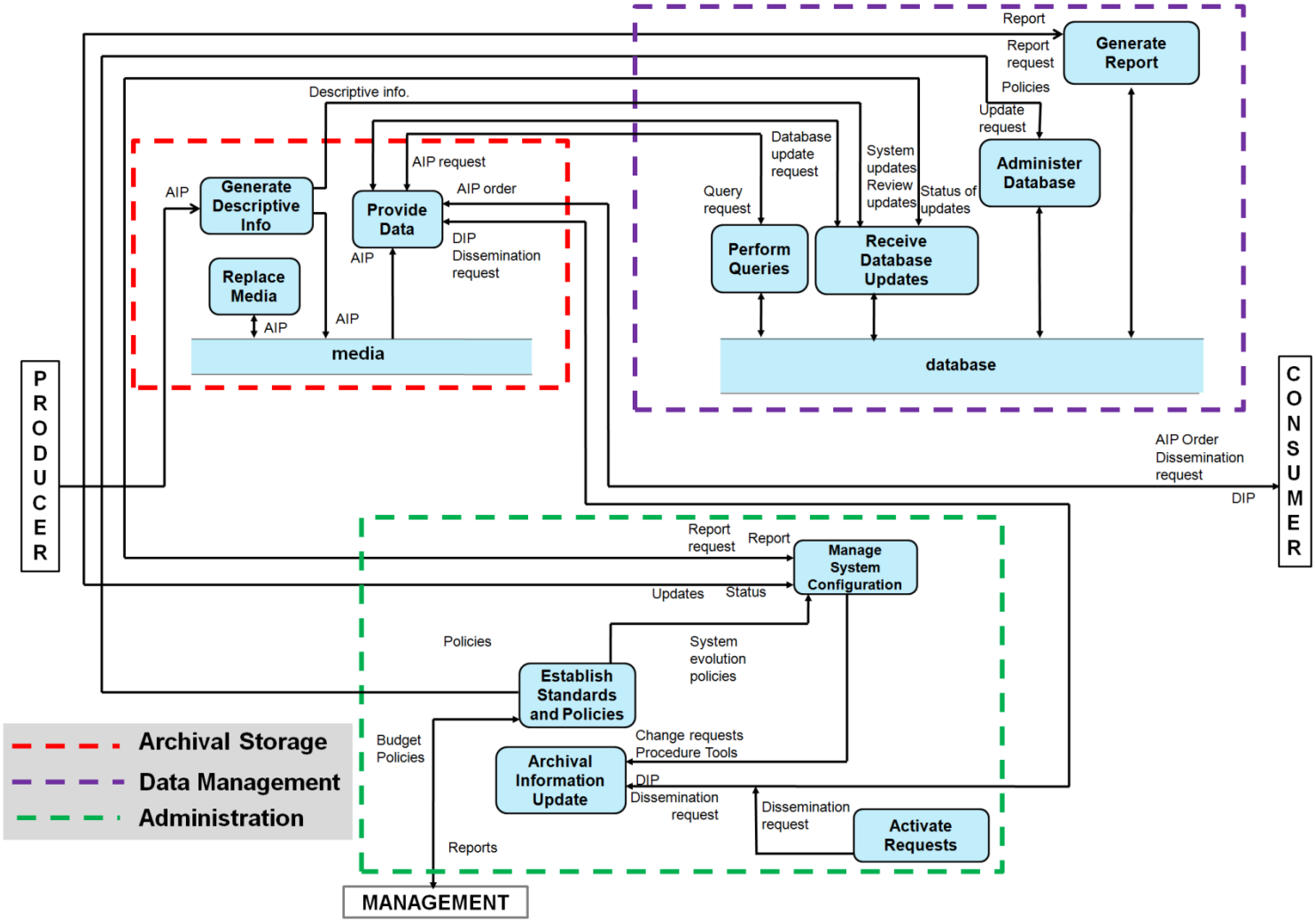

Figura 19. Modelo OAIS reducido para entidades sanitarias.

Capítulo 8

Conclusiones

8 Conclusiones

8.1 Revisión de la propuesta

En los entornos sanitarios la preservación digital de la información es un tipo de proceso que todavía no se lleva a cabo. La complejidad de los datos que manejan las entidades sanitarias condiciona el desarrollo de sus necesidades de preservación. La preservación de datos complejos requiere de un análisis previo de medidas de seguridad, vigilancia tecnológica y del diseño de modelos de conservación digital, pero en la actualidad cada entidad sanitaria adopta su propio modelo de custodia de información sin seguir ningún tipo de política o estándar con las dificultades que ello conlleva respecto a su sostenibilidad tecnológica y económica.

La adopción de estándares es una de las posibles soluciones, como se ha propuesto en esta tesis, ya que un estándar influye en la sostenibilidad del propio modelo, factor muy a tener en cuenta. En este caso, la adaptación de un modelo como OAIS contribuye a la solución del problema de preservación digital de la información sanitaria sin tener que plantear un diseño totalmente nuevo, que requeriría de mayores esfuerzos.

A lo largo de esta tesis se ha elaborado un mapa de las necesidades de preservación digital de diversas entidades sanitarias que han colaborado voluntariamente, finalizando con el diseño de un modelo de preservación digital adaptado a las necesidades de dichas entidades. Para ello se ha realizado un estudio cualitativo con las diferentes metodologías.

La interpretación de los datos de las encuestas de auditoría realizadas se podía haber llevado a cabo de formas diversas. En este caso, se ha considerado

que, dada la muestra de sólo ocho entidades de gestión sanitaria, no era adecuado emplear técnicas estadísticas, habiéndose optado por una aproximación más cualitativa, dado que era un grupo reducido y se podían extraer detalles concretos de los datos facilitados. No por ello los datos de estas ocho instituciones dejan de ser una muestra significativa con respecto a la totalidad de la muestra de entidades de gestión sanitaria en Catalunya, tal y como se indicaba en el Capítulo 1.

El proceso de análisis se inició con una encuesta preliminar, a fin de obtener información sobre los datos digitales que dichas entidades manejan. Posteriormente, y previo estudio de diferentes metodologías, se realizó una encuesta de auditoría que permitió ejecutar un análisis de la seguridad y un análisis de la preservación digital, empleando conjuntamente indicadores del Esquema Nacional de Seguridad y Trustworthy Repositories Audit Criteria (TRAC) descritos en el Capítulo 4. Una vez realizada la encuesta de auditoría, mediante una entrevista final a fin de completar la recogida de datos, se ha podido realizar un análisis de riesgos. En su conjunto, todos los datos han permitido diseñar un modelo de preservación digital simplificado, basado en el modelo OAIS.

Por otro lado, en la encuesta de auditoría, al tratarse de preguntas cerradas, la extracción de datos ha permitido conocer en detalle si las entidades cumplían determinados indicadores tanto de Trustworthy Repository Audit Criteria como del Esquema Nacional de Seguridad.

La aportación más significativa de este proyecto, por tanto, no ha sido el conocimiento que genera el proceso de auditoría, sino la propuesta de adaptación de un modelo de preservación digital estándar como OAIS a un entorno como el de los centros sanitarios, donde, aún siendo los datos

complejos, estos tienen un cierto grado de homogeneidad. Por lo tanto, el modelo propuesto basado en el estándar OAIS permite resolver las necesidades de gestión y preservación de datos complejos de un escenario sanitario.

A continuación se muestran las aportaciones del trabajo de investigación de forma detallada, los aspectos clave para adoptar de forma práctica el modelo propuesto en esta tesis y, finalmente, se exponen las líneas de investigación futuras que ésta puede abrir.

8.2 Aportaciones de la investigación

Respecto al objetivo principal de la investigación se pueden extraer las reflexiones siguientes:

a) El modelo OAIS es aplicable a instituciones sanitarias teniendo en cuenta que es un modelo inicialmente creado para industria aeronáutica y ampliamente extendido en el entorno de las bibliotecas y entidades de herencia cultural.

b) El modelo OAIS permite su reducción sin que se pierdan funcionalidades originales, flujos de datos o flujos de información ni nomenclatura.

c) El modelo OAIS permite adaptarse a un entorno menos complejo del creado inicialmente como el sector aeronaútico.

d) Se tendría que verificar la adaptación de OAIS a otros entornos con flujos de información controlado en especial aquellos que no tengan necesidades de control de ingesta de datos como el sanitario.

e) Otro factor que facilita la simplificación de OAIS, es poder disponer de un marco jurídico que facilite en este caso la historia clínica electrónica (HCE) tanto a nivel nacional (España, 2002), autonómico (Catalunya, 2010) como también a nivel internacional por organismos como la UNESCO (UNESCO, 2004) o la Organización Mundial de la Salud (WHO, 2006).

En la introducción, además, se formularon inicialmente cinco preguntas de investigación que se responden a continuación:

- En respuesta a la primera pregunta de investigación, los datos a preservar en las entidades sanitarias tienen características específicas, siendo las historias clínicas electrónicas un objeto digital complejo compuesto de diferentes componentes (como por ejemplo documentos PDF, imágenes en formato DICOM, registros de audio, etc.) pero no siendo éstos los únicos aspectos que constituyen una historia clínica electrónica, sino que hay que tener en cuenta otros, como la secuencia temporal, los procesos operacionales o las cuestiones legales.

  Las medidas de seguridad tecnológicas en un entorno sanitario son más estrictas que en otro tipo de entornos, ya que en ellas no sólo influye la tipología de los objetos digitales, como por ejemplo imágenes de vídeo o registros auditivos, sino que también tiene influencia la legislación relativa a la protección de datos personales, tal y como se ha descrito en el Capítulo 3 correspondiente al marco jurídico en el cual se lleva a cabo la actividad. Estos condicionantes tienen como consecuencia facilitar la preservación de los datos al exigir un grado superior de integridad de la información.

- Con el fin de responder a la segunda pregunta de investigación, tal y como se ha podido observar a través del análisis realizado en este trabajo, las entidades sanitarias no están actualmente realizando ninguna acción en cuanto a la preservación digital, a pesar de estar obligadas legalmente a ello, como se indica en el Capítulo 3. Esta falta de políticas de preservación pone en riesgo todo el proceso de gestión de datos a largo plazo.

- Como se puede observar en el Capítulo 4 y en referencia a la tercera pregunta de investigación, las metodologías aplicadas validas son el ENS, TRAC y la metodología de análisis de riesgos MAGERIT. Estas metodologías tienen su validez ya que el ENS es de obligado cumplimiento en España, TRAC es una normativa estándar con el consenso de la comunidad internacional y MAGERIT a través del programa PILAR permite realizar un análisis computacional, en comparación con otras metodologías internacionalmente en las que esto no es posible.

  La falta de conocimiento de modelos de preservación digital y en algunos casos la escasez de recursos provoca que no se realice una planificación de la preservación digital en las entidades sanitarias desde su inicio, es decir, desde el proceso inicial de digitalización de las historias clínicas hasta el proceso final de integración en el sistema de información de la entidad. La planificación de la preservación digital mediante un modelo como el propuesto en esta tesis doctoral facilitaría acciones proactivas al respecto, como la elección de formatos o tecnología que faciliten dicha preservación digital. Por ejemplo, el uso de tecnología no dependiente de un solo fabricante.

- Respondiendo a la cuarta pregunta de investigación el modelo más extendido actualmente de preservación digital es el modelo OAIS. Como se ha visto en el Capítulo 5, hay otros modelos estos pero no cubren todas las necesidades que una organización puede requerir. El modelo OAIS está además consensuado por la comunidad internacional.

- Por lo que respecta a la adaptación del modelo OAIS y en respuesta a la quinta pregunta de investigación, tal y como se ha visto en el Capítulo 7, se han podido minimizar tres de las entidades funcionales del modelo OAIS, como son la Ingesta (Ingest), Planificación de la Preservación (Preservation Planning) y Acceso (Access). La simplificación de estos elementos se debe a que son procesos que ya están realizándose en los hospitales como parte de la gestión de su información diaria, por lo que el modelo propuesto no debe ser más complejo de lo estrictamente necesario, potenciando su aplicación práctica.

  Finalmente, para mantener la compatibilidad del modelo propuesto, es necesario conservar la nomenclatura existente y evitar en lo posible crear procedimientos funcionales nuevos con respecto al modelo OAIS original, con el objetivo de no alterar el modelo de información original.

Como resultado colateral de esta investigación, se ha constatado de forma sorprendente que las metodologías de análisis de riesgos no se están aplicando a los sistemas información, tecnología y comunicación de las entidades sanitarias. Hay que indicar que una auditoría como TRAC incide especialmente en la ejecución del análisis de riesgos. El análisis de riesgos aplicado a la información digital es una herramienta útil para prevenir errores, fallos y

peligros innecesarios en un sistema de información. Tradicionalmente, el análisis de riesgos se ha empleado en el desarrollo de herramientas de software pero también es aplicable a la información que gestiona un sistema. Prueba de ello son las múltiples métricas existentes y reconocidas internacionalmente como MAGERIT, que se ha aplicado mediante el uso del programa PILAR, tal y como se ha descrito en el Capítulo 6.

El objetivo principal de este proyecto de tesis ha sido obtener un modelo reducido del modelo OAIS. El inconveniente que esto planteaba era que únicamente un autor ha analizado previamente un modelo reducido (Spencer, 2006) aplicado en el contexto de la Biblioteca Nacional de Gales. Por su parte otro autor (Allinson, 2006) abogaba por reducir el modelo o plantear la existencia de un lista de indicadores de comprobación para gestores, denominando a esta versión OAIS-LITE. Este proyecto de tesis cubre por lo tanto este vacío.

Las particularidades que pueden llevar a la simplificación del modelo OAIS en un entorno sanitario con respecto al expuesto por los autores que tradicionalmente emplean este modelo, se refieren a la homogeneidad en la información (tanto la entrante como la saliente). El hecho de que la información ya esté ingresada, que es el caso de los sistemas de información sanitarios, favorece que no sea necesario elaborar un completo proceso de Ingesta (Ingest), tal y como se exige en el modelo OAIS descrito en el Capítulo 5. Es necesario, no obstante, un proceso complementario para poder disponer de las propiedades significativas. Es por esto que se propone realizar dicho proceso en la función Almacenamiento de Archivo (Archival Storage), lo cual resulta novedoso y es un resultado secundario pero relevante de este trabajo.

También facilita la reducción del modelo el disponer de una Comunidad Designada (Designated Community) con vocabulario y conocimientos homogéneos. Nos referimos a los profesionales sanitarios que, debido a su formación, comparten un lenguaje común.

Finalmente, se ha demostrado que, a pesar de ser un modelo abstracto, el modelo OAIS puede simplificarse y adaptarse para un tipo de organización en concreto, pero bajo determinadas condiciones. Estas condiciones, como se ha visto en este proyecto de tesis, son entornos cerrados que cumplen requisitos de seguridad en la información, como garantía de integridad de los datos. En el entorno sanitario la integridad es relevante porque sin ella no se puede realizar la prestación asistencial. La simplificación del modelo OAIS variará según se aplique a casos en los que previamente no existe un sistema de información o, por el contrario, se aplique a estructuras informacionales existentes a las cuales habrá que adaptar el modelo OAIS. En esta tesis se propone una forma de implementar esta segunda aplicación mediante el proceso de encuesta de auditoría, entrevistas finales y análisis de riesgos, descritos en los Capítulos 6 y 7.

8.3 Aspectos clave en la implementación práctica

Para la implementación del modelo de preservación propuesto en una institución sanitaria, se recomienda la participación de una representación de aquellas personas que forman parte de la Comunidad Designada como médicos, personal de archivo, personal administrativo o personal del departamento de informática.

Es relevante que para la implementación se hace necesario en el uso de TRAC y ENS como modelo de auditoría la participación de un número

representativo de la Comunidad Designada sin olvidar personal de las escalas ejecutivas o de gestión. La razón de ello, es que es importante entender que las operaciones de conservación digital tienen un coste y éste ha de ser sostenible para la propia institución. Si determinadas acciones posteriormente no se pueden ejecutar por falta de financiación se corre el riesgo de pérdidas de información, en algunos casos irreparables.

Una vez obtenidos los resultados de la auditoría es recomendable realizar un estudio en profundidad de la tecnología a emplear si es que hay que establecer cambios en ella o modificaciones, ya que en algunas ocasiones diferentes tecnologías tienen que convivir conjuntamente con los riesgos que supone para su funcionamiento. Es por esto que la implantación de un archivo OAIS reducido no supondría una gran dificultad técnica para las entidades si previamente se ha realizado la evaluación de la tecnología a emplear así como los distintos aspectos que influyen en ella.

En la implantación de todo el proceso, el establecimiento de un calendario adecuado facilitará una implantación eficaz del sistema. En la misma habrá que tener en cuenta habrá que tener en cuenta no sólo los aspectos mencionados anteriormente, sino también la necesidad de formación del personal, pues la implementación del modelo OAIS en forma reducida representará un entorno y conceptos nuevos para aquellas personas implicadas en su gestión diaria.

8.4 Líneas futuras de trabajo

A través del desarrollo de esta tesis se han observado posibles líneas futuras de investigación como las que se describen a continuación:

- Implementación y validación del modelo propuesto. Como se ha descrito en el Capítulo 1, en esta tesis se realiza la propuesta de un modelo de

conservación. La implementación y validación de este modelo propuesto podría dar lugar al establecimiento concreto de un modelo de preservación sanitario compartido entre varias entidades.

- Análisis de las diferentes tecnologías a adoptar en la simplificación propuesta del modelo OAIS. Como se ha comentado, una de las cuestiones a abordar es la dependencia de un solo fabricante por parte de una institución sanitaria para la gestión de historias clínicas. El estudio de las diferentes tecnologías permitiría discutir qué tecnología sería la adecuada en un entorno sanitario teniendo en cuenta las particularidades del mismo, así como de las historias clínicas.

- Movilidad en las historias clínicas en dispositivos móviles. Con el paso del tiempo, las historias clínicas además de estar en un entorno seguro es posible que se requiera que estén disponibles en dispositivos móviles. El uso de estos dispositivos requerirá no sólo del estudio de la preservación, sino también de aspectos como la usabilidad, la capacidad de los dispositivos para la visualización de la información o la seguridad e integridad de los datos.

- Estudio de la complejidad de las historias clínicas en la nube. Una solución de almacenamiento externo para entidades sanitarias, como por ejemplo en el caso de una organización que disponga de varios centros geográficamente dispersos, implica ciertos riesgos a la vez que retos a asumir por una entidad sanitaria que deben ser evaluados.

- Realización de un análisis de las necesidades de preservación en otras entidades sanitarias de otras comunidades autónomas, con el objetivo de crear un mapa nacional que dé lugar al establecimiento de un marco de políticas nacionales de preservación digital de las historias clínicas.

9

Referencias bibliográficas

9 Referencias bibliográficas

ABRAMS, S. ET AL. (2005). Harvard's perspective on the archive ingest and handling test. *D-Lib Magazine*, *11*(12). [en línea] <http://dlib.org/dlib/december01/12inbrief.html> [consulta: 8 de enero de 2012]

ADAM, S. (2010). Preserving authenticity in the digital age. *Library Hi Tech, 28*(4), 595-604. doi:10.1108/07378831011096259

ALLINSON, J. (2006). *An introduction to OAIS reference models for repositories.* [en línea] <http://www.slideshare.net/j.allinson/oais-as-a-reference-model-for-repositories>. [consulta: 8 de abril de 2010]

ALLINSON, J. (2006). *OAIS as a reference model for repositories: An evaluation*. Manuscrito no publicado. [en línea] <http://www.ukoln.ac.uk/repositories/publications/oais-evaluation-200607/Drs-OAIS-evaluation-0.5.pdf> [consulta: 06 de junio de 2011]

ARM, C., FLEISCHHAUER, C. (2005). Digital Formats: Factors for Sustainability, Functionality, and Quality. Ponencia presentada en *Proceedings of Archiving 2005,* Washington, DC, USA

ASKHOJ, J., NAGAMORI, M., & SUGIMOTO, S. (2011). Archiving as a service: A model for the provision of shared archiving services using cloud computing. Ponencia presentada *en Proceedings of the 2011 iConference,* Seattle, Washington. 151-158. doi:doi.acm.org/10.1145/1940761.1940782

ASOCIACIÓN ESPAÑOLA DE NORMALIZACIÓN Y CERTIFICACIÓN. (2004). En AENOR (Ed.), *Informática sanitaria. Imagen Digital. Comunicación, flujo de trabajo y gestión de datos: UNE-EN 12052*

BAI, Y., SUMMERS, W. & BOSWORTH, E. (2007). Teaching network risk assessment to online graduate students. Ponencia presentada en *Proceedings of the 4th annual conference on Information security curriculum development* (InfoSecCD '07). ACM, New York, NY, USA. http://doi.acm.org/10.1145/1409908.1409917

BAKKER, AB. (2004). Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences. *International Journal of Medical Informatics*, *73*(3), 267-270. doi:10.1016/j.ijmedinf.2003.11.008

BERNARD, R. (2007). Information Lifecycle Security Risk Assessment: A tool for closing security gaps. *Computers & Security, 26*(1), 26-30. doi:10.1016/j.cose.2006.12.005

BLUE TASK RIBBON FORCE. (2010). Sustainable Economics for a digital planet: ensuring long-term to digital information. [en línea] <http://brtf.sdsc.edu/biblio/BRTF_Final_Report.pdf> [consulta: 29 de abril de 2011]

BOJA, C., DOINEA, M. (2010). Security Assessment of Web Based Distributed Applications. *Informatica Economică, 14*(1), 152-162. [en línea] <http://revistaie.ase.ro/content/53/16%20Boja,%20Doinea.pdf> [consulta: 14 de abril de 2011]

BOTE, J. (2008). Second digital preservation challenge. [en línea] <http://www.digitalpreservationeurope.eu/publications/challenge_reports/vericad.pdf> [consulta: 9 de septiembre de 2011]

BOTE, J., TERMENS, M. (2011). Trac y ens en la auditoría de preservación digital de los archivos sanitarios. Ponencia presentada en *Actas del XIV Congreso nacional de informática de la salud 2011*, Madrid. 155-159

CATALUNYA. GENERALITAT DE CATALUNYA. DEPARTAMENT DE SANITAT I SEGURETAT SOCIAL (1999). *Legislació sobre ordenació sanitària a Catalunya. Col·lecció Quaderns de Legislació, 23*. [en línea] <http://www10.gencat.cat/catsalut/archivos/ql23_LOSC.pdf> [consulta: 14 de junio de 2010]. ISBN: 84-393-4857-6

CATALUNYA. GENERALITAT. CATSALUT (2009). *Els sistemes de pagament de la sanitat pública a Catalunya, 1981-2009: evolució històrica i perspectives de futur.* 1a ed. Barcelona: Servei Català de la Salut (Catsalut). ISBN: 978-84-393-8192-1

CENTER FOR RESEARCH LIBRARIES, ONLINE COMPUTER LIBRARY CENTER, INC. (2007). *Trustworthy Repositories Audit & Certification: Criteria & Checklist*, Version 1.0. [en línea] <http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf> [consulta: 20 de mayo de 2010]

CENTER FOR RESEARCH LIBRARIES. (2010). *Report on Portico Audit Findings*. [en línea] <http://www.crl.edu/archiving-presentation/digital-archives/certification-and-assessment-digital-repositories/portico> [consulta: 20 de junio de 2010]

CENTER FOR RESEARCH LIBRARIES. (2011). *Report on HathiTrust Digital Repository*. [en línea] <http://www.crl.edu/archiving-presentation/digital-archives/certification-and-assessment-digital-repositories/hathi> [consulta: 20 de mayo de 2011]

CERF, V. (2011). Avoiding "Bit Rot"·: Long-Term Preservation of Digital Information. *Proceedings of the IEEE*, *99*(6), 915-916. doi:10.1109/JPROC.2011.2124190

CONSULTATIVE COMITEE FOR SPACE DATA SYSTEMS (2002) *Reference Model for an Open Archival Information System (OAIS).* [en línea] <http://public.ccsds.org/publications/archive/650x0b1.pdf> [Consulta: 20 de mayo de 2010]

CONWAY, P. (1994). Digitizing preservation. *Library Journal, 119*(2), 42-45.

CORN, M. (2009). Archiving the phenome: Clinical records deserve long-term preservation. *Journal of the American Medical Informatics Association*, *16*(1), 1-6. doi:10.1197/jamia.M2925

CORNELL UNIVERSITY LIBRARY AND GÖTTINGEN STATE AND UNIVERSITY LIBRARY. (2004). *Ensuring Access to Mathematics Over Time: Cooperative Management of Distributed Digital Archives*. [en línea] <http://www.library.cornell.edu/dlit/MathArc/web/index.html> [consulta: 20 de mayo de 2011]

CORNELL UNIVERSITY. (2006). *Digital Preservation Management: Implementing Short-Term Strategies for Long-Term Problems*. [en línea] <http://www.icpsr.umich.edu/dpm/dpm-eng/eng_index.html> [consulta: 20 de mayo de 2011]

DEUTSCHE INITIATIVE FÜR NETZWERKINFOMATION EV (2007) *DINI-certificate Document and Publication Services.* [en línea] <http://edoc.hu-berlin.de/series/dini-schriften/2006-3-en/PDF/3-en.pdf> [consulta: 15 de febrero de 2010]

DIGITAL CURATION CENTRE AND DIGITALPRESERVATIONEUROPE, (2007), *DCC and DPE Digital Repository Audit Method Based on Risk Assessment,* v1.0., [en línea] < http://www.repositoryaudit.eu/download> [consulta: 2 de octubre de 2009]

DOBRATZ, S., SCHOGER, A. (2007). Trustworthy digital long-term repositories: The nestor approach in the context of international developments. En L. Kovács, N. Fuhr & C. Meghini (Eds.), *Research and advanced technology for digital libraries* (pp. 210-222) Springer Berlin / Heidelberg. doi:10.1007/978-3-540-74851-9_18

ESCUDERO, C. (2011). *El nuevo esquema nacional de seguridad. La experiencia en la Seguridad Social*. [en línea] <http://www.socinfo.es/contenido/seminarios/seguridaden/giss.pdf> [consulta: 2 julio de 2011].

ESPAÑA. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado* (14 diciembre 1999), núm. 298, p. 43.088.

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* (15 noviembre 2002), núm. 274, p. 40.126.

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* (29 enero 2010), núm. 25, p. 8.089.

ESPAÑA. CATALUNYA. Llei 21/2000, de 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica. *Diari Oficial de la Generalitat de Catalunya* (11 gener 2001), núm 3.303 i rectificació a *Diari Oficial de la Generalitat de Catalunya* (22 març 2001), núm 3.353.

ESPAÑA. CATALUNYA. Llei 16/2010, del 3 de juny, de modificació de la llei 21/2000, del 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica. *Diari Oficial de la Generalitat de Catalunya*, (10 juny 2010), núm. 5.647.

EUROPA**.** 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 (23 noviembre 1995), nº L 281, p. 0031 – 0050.*

EUROPA. Recomendación de la comisión de 2 de julio de 2008 sobre la interoperabilidad transfronteriza de los sistemas de historiales médicos electrónicos. 2008/594/CE. *Diario Oficial de la Unión Europea* (18 julio 2008), nº L. 190, p. 0037 – 0043.

EUROPA. Directiva 2011/24/UE del parlamento europeo y del consejo relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. *Diario Oficial de la Unión Europea* (4 abril 2011), nº L 88/45, p. 0045 – 0065.

GRANGER, S. (2000). Emulation as a Digital Preservation Strategy. *D-Lib Magazine, 6*(10). [en línea] <http://www.dlib.org/dlib/october00/granger/10granger.html> [consulta: 20 de abril de 2010]

GRACE, S., GRINDLEY, N. & YOUNG, G. (2008). Significant properties and their role in digital preservation. Ponencia presentada en *Proceedings of Archiving 2008,* Bern, Switzerland.

GRAY, N., WOAN, G. (2011). Digital Preservation and Astronomy: Lessons for funders and the funded. Ponencia presentada en *Proceedings of the 20th Annual Astronomical Data Analysis Software and Systems XX*. Boston, MA. 13-16.

GREENFIELD, M. (2000). *Risk Management Tools*. [en línea] <http://www.fmea-fmeca.com/nasa-risk-management.pdf> [consulta: 10 julio de 2011]

GUTEMMBRUNNER, M., BECKER, C., RAUBER, A. & KEHRBERG, C. (2008). Evaluating strategies for preservation of console video games. Ponencia presentada en *Proceedings of the Fifth International Conference on Preservation of Digital Objects,* London, UK. 115-121. [en línea] <http://www.bl.uk/ipres2008/presentations_day1/18_Guttenbrunner.pdf> [consulta: 5 de septiembre de 2010]

HAMPSHIRE, E., JOHNSON, V. (2009). The digital world and the future of historical research. *Twentieth Century British History, 20*(3), 396-414. doi:10.1093/tcbh/hwp036

HEDSTROM, M., LEE, C. (2002). Significant properties of digital objects: definitions, applications, implications. Ponencia presentada en *Proceedings of the DLM-Forum 2002, Barcelona, 6-8 May 2002*, 218-227. Luxembourg: Office for Official Publications of the European Communities, 2002. [en línea] <http://www.ils.unc.edu/callee/sigprops_dlm2002.pdf> [consulta: 8 de abril de 2011]

HIGGINS, S., SEMPLE, N. (2006). *OAIS Five-year review Recommendations for update*. [en línea] <http://www.era.lib.ed.ac.uk/bitstream/1842/3352/1/Higgins%20OAIS_5-Year_Review.pdf> [consulta: 8 de abril de 2010].

Huang, L., Bai, X. & Nair, S. (2008). Developing a SSE-CMM-based Security Risk Assessment Process for Patient-Centered Healthcare Systems. *Ponencia presentada en las actas de 6th Workshop on Software Quality*, Leipzig, Germany. doi:10.1145/1370099.1370103

IFLA, CONSEJO INTERNACIONAL DE ARCHIVOS, & UNESCO. (2005). *Directrices para proyectos de digitalización de colecciones y fondos de dominio público, en particular para aquellos custodiados en bibliotecas y archivos*. Madrid: Ministerio de Cultura. Secretaría General Técnica.

INTERNATIONAL STANDARD ORGANIZATION. (2006). *Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management. ISO 12052*. Genève.

INTERNATIONAL STANDARD ORGANIZATION. (2006). *Health informatics — HL7 version 3 — Reference information model — Release 1. ISO/HL7 21731*. Genève.

INTERNATIONAL STANDARD ORGANIZATION. (2012). *Space data and information transfer systems -- Audit and certification of trustworthy digital repositories. ISO 16363:2012*. Genève.

ISACA. IT GOVERNANCE INSTITUTE. *COBIT* v. 4.1 [en línea] <http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1spanish.pdf> [consulta: 5 de junio de 2010]

JAN'EE, G., MATHENA, J. & FREW, J. (2008). A data model and architecture for long-term preservation. Ponencia presentada en *Proccedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries*, Pittsburgh PA, USA. 134-144. doi:doi.acm.org/10.1145/1378889.1378912

JOHN, J. L. (2008). Adapting existing technologies for the digital archiving of personal lives. *Ponencia presentada en las actas de Fifth International Conference on Preservation of Digital Objects,* London, UK. 48-55. [en línea] <http://www.bl.uk/ipres2008/presentations_day1/09_John.pdf> [consulta: 8 de febrero de 2011]

JOHN, J. L. (2009). The future of saving our past. *Nature, 459*(7248), 775-776. doi:10.1038/459775a

JONES, M. (2001). The CEDARS Project Website. *D-Lib Magazine*, *7*(12). [en línea] <http://dlib.org/dlib/december01/12inbrief.html> [consulta: 8 de enero de 2012]

KEJSER, U.; NIELSEN, A. & THIRIFAYS, A.; (2009). Cost Model for Digital Curation: Cost of Digital Migration. Ponencia presentada en *Proccedings of the Sixth International Conference on Preservation of Digital Objects*, San Francisco, California, USA. 98-104. [en línea] <http://escholarship.org/uc/item/4d09c0bb> [consulta: 8 de febrero de 2011]

KEPCZYNSKA-WALCZAK, A. (2005). A method proposed for adoption of digital technology in architectural heritage documentation. Ponencia presentada en *Proceedings of the 11th International Conference on Computer Aided Architectural Design Futures,* Viena, Austria. 73-82. doi:10.1007/1-4020-3698-1_6

KNIGHT, G., PENNOCK, M. (2008). *Data without meaning: establishing the Significant Properties of Digital Research*. Ponencia presentada en *Proccedings of the Fifth International Conference on Preservation of Digital Objects,* London, UK. 99-106. [en línea] <http://www.bl.uk/ipres2008/presentations_day1/16_Knight.pdf> [consulta: 8 de febrero de 2011]

KNIGHT, S. (2009). From OAIS to DPS to NDHA. Ponencia presentada en *Proceedings of Archiving 2009*, Arlington, USA. 1-3.

KNIGHT, S. (2010). Early learnings from the national library of New Zealand's national digital heritage archive project. *Program-electronic library and information systems, 44*(2), 85-97. doi:10.1108/00330331011039151

LATECKI, L.; CONRAD, C. & GROSS, A. (1998). Preserving Topology by a Digitization Process. *Journal of Mathematical Imaging and Vision*, *8*(2), 131-159. doi:10.1023/A:1008273227913

LEFURGY, W. (2009). NDIIPP partner perspectives on economic sustainability. *Library Trends, 57*(3), 413-426.

LEE, C. A. (2005). *Defining digital preservation work: A case study of the development of the reference model for an open archival information system*. (Tesis doctoral). University of Michigan. Disponible en la base de datos ProQuest Dissertations and Theses. http://search.proquest.com/docview/305424285?accountid=15299

LEE, C. A., TIBBO, H. R., HOWARD, D., SONG, Y., RUSSELL, T. & JONES, P. (2006). Keeping the context: An investigation in preserving collections of digital video. *Ponencia presentada en las actas de 6th ACM/IEEE-CS Joint Conference on Digital Libraries*, Chapel Hill, NC, USA. 363-363. doi: doi.acm.org/10.1145/1141753.1141858

LEKKAS, D., GRITZALIS, D. (2007). Long-term verifiability of the electronic healthcare records authenticity. *International Journal of Medical Informatics*, 76(5), 442-448. doi:10.1016/j.ijmedinf.2006.09.010

LLUECA, C. (2006). Archivando la Web, el proyecto Padicat (Patrimonio Digital de Cataluña). *El Profesional de la Información, 15*(6). 473-478. [en línea] <http://hdl.handle.net/10760/8399> [consulta: 9 de enero de 2010]

LOPATIN, L. (2006). Library digitization projects, issues and guidelines. *Library Hi Tech, 24*(2), 273-289, doi:10.1108/07378830610669637

LUAN, F., NYGAR, M. & MESTL, T. (2010). A Mathematical Framework for Modelling and Analyzing Migration Time. *Ponencia presentada en las actas de Joint Conference of Digital Libraries*, Queensland, Australia. 323-332. doi:doi.acm.org/10.1145/1816123.1816172

LYNCH, C. (1999). Canonicalization: A Fundamental Tool to Facilitate Preservation and Management of Digital Information. *D-Lib Magazine, 5*(9). [en línea] <http://www.dlib.org/dlib/september99/09lynch.html> [consulta: 9 de enero de 2010]

MAGETO, D. (2010). Determining Cost Factors in Digital Preservation using OAIS Model. Ponencia presentada en *Proceedings of the 8th European Conference of Digital Archiving*, Bern, Switzerland.

MARTINEZ-URIBE, L. (2009). Using the Data Audit Framework: an Oxford Case Study. [en línea] < http://www.disc-uk.org/docs/DAF-Oxford.pdf> [consulta: 2 de junio de 2011]

MCCRAY, A., GALLAGHER, M. (2001). Principles for digital library development. *Commun.ACM, 44*(5), 48-54. doi:10.1145/374308.374339

MCLEOD, R. (2008). Risk Assessment; using a risk based approach to prioritise handheld digital information. Ponencia presentada en *Proccedings of the Fifth International Conference on Preservation of Digital Objects*, London, UK. [en línea] < http://www.bl.uk/ipres2008/presentations_day1/20_McLeod.pdf > [consulta: 8 de febrero de 2010]

MELLOR, P., WHEATLEY, P. & SERGEANT, D. (2002). Migration on request, a practical technique for preservation. Ponencia presentada en *Proccedings of the 6th European Conference on Research and Advanced Technology for Digital Libraries*. doi:10.1007/3-540-45747-X_38

MICROSOFT CORPORATION, INC. *Microsoft Assesment Tool* v4. 0 [en línea] <https://partner.microsoft.com/40081388> [consulta: 28 de mayo de 2010].

MINISTERIO DE ADMINISTRACIONES PÚBLICAS. (2006). *MAGERIT - Versión 2: Metodología de análisis y gestión de riesgos de los sistemas de información* 1ª ed. Madrid [en línea] < http://www.csi.map.es/csi/pg5m20.htm> [consulta: 8 de mayo de 2010].

MOEN, I., GRAM SIMONSEN, H. & LINDSTAD, A. M. (2004). An electronic database of norwegian speech sounds: Clinical aspects. *Journal of Multilingual Communication Disorders*, *2*(1), 43-49. doi:10.1080/14769670310001616624

MUIR, A. (2001). Legal deposit and preservation of digital publications: a review of research and development activity. *Journal of Documentation*, *57*(5), 652-682. doi:10.1108/EUM0000000007097

MUÑOZ, B. (2006). La gestión de riesgos orientada a la conservación de información en soporte digital. *Documentación de las Ciencias de la Información, 29*, 125-140. [en línea] <http://revistas.ucm.es/index.php/DCIN/article/view/DCIN0606110125A/19112 > [consulta: 17 de abril de 2010]

Narock, T., Cragin, M. (2010). Earth and space science informatics infrastructure. *Earth Science Information*, *3*(1), 1-3. doi:10.1007/s12145-009-0041-8

NATIONAL ARCHIEEF. (2005) *The Cost of Digital Perserving*, Version 1.0 [en línea] http://www.digitaleduurzaamheid.nl/bibliotheek/docs/CoDPv1.pdf [consulta: 1 de febrero de 2010].

NATIONAL ARCHIVES OF AUSTRALIA. (2008). *CHECK-UP: A tool for assessing your agency's information and records management*. [en línea]< http://www.naa.gov.au/Images/Check-up%20text%20version_tcm2-12664.pdf> [consulta: 28 de febrero de 2010].

NESTOR WORKING GROUPTRUSTED REPOSITIORIES CERTIFICATION. (2008). *Catalogue of Criteria for Trusted Digital Repositories*, Version 2.0 [en línea] <http://files.d-nb.de/nestor/materialien/nestor_mat_08-eng.pdf> [consulta: 20 de mayo de 2010].

NORONHA, N., CAMPOS, J., GOMES, D., SILVA, M. & BORBINHA, J. (2001). En Constantopoulos P., Sølvberg I.(Eds.). *A deposit for digital collections* Springer Berlin / Heidelberg. doi:10.1007/3-540-44796-2_18

OLTMANS, E. (2004). Cost models in digital archiving: An overview of life cycle management at the National Library of the Netherlands. *Liber Quarterly*, *14*(3/4). [en línea] <http://liber.library.uu.nl/publish/issues/2004-3_4/index.html?000103> [consulta: 30 de marzo de 2010]

OLTMANS, E., VAN DIESSEN, R. & VAN WIJNGAARDEN, H. (2004). Preservation functionality in a digital archive. Ponencia presentada en *Proccedings of the 4th ACM/IEEE-CS Joint Conference on Digital Libraries*, Tuscon, AZ, USA. 279-286. doi:doi.acm.org/10.1145/996350.996416

PARÉ, G., SICOTTE, C., JAANA & M., GIROUARD, D. (2008). Prioritizing Clinical Information System Project Risk Factors: A Delphi Study. *Methods of Information in Medicine, 47(3)*, 251-259. doi:10.3414/ME0512

PIRNEJAD, H., BAL, R. & BERG, M. (2008). Building an inter-organizational communication network and challenges for preserving interoperability. *International journal of medical informatics, 77*(12), 818-827. doi:10.1016/j.ijmedinf.2008.05.001

RAMALHO, J., FERREIRA, M. ET AL. (2008). RODA and Crib. A Service-Oriented Digital Repository. Ponencia presentada en *Proccedings of the Fifth International Conference on Preservation of Digital Objects*, London, UK.

REGLI, W. C., GRAUER, M. & KOPENA, J. B. (2009). A framework for preservable geometry-centric artifacts. Ponencia presentada en *Proccedings of 2009 SIAM/ACM Joint Conference on Geometric and Physical Modeling,* San Francisco, California. 67-78. doi:doi.acm.org/10.1145/1629255.1629265

RESEARCH LIBRARIES GROUP. (2002) *Trusted Digital Repositories: Attributes and Responsibilities* [en línea] <http://www.oclc.org/research/activities/past/rlg/trustedrep/repositories.pdf> [consulta: 3 de abril de 2010].

RÖDIG, P., BORGHOFF, U. M., SCHEFFCZYK, J. & SCHMITZ, L. (2003). Preservation of digital publications: An OAIS extension and implementation. Ponencia presentada en *Proceedings of 2003 ACM Symposium on Document Engineering*, Grenoble, France. 131-139. doi:doi.acm.org/10.1145/958220.958245

ROMERO, B.; VILLEGAS, M. AND MEZA, M. (2008) Simon's Intelligence Phase for Security Risk Assessment in Web Applications. Ponencia presentada en *Proccedings of the Fifth International Conference on Information Technology: New Generations*, Las Vegas, Nevada, USA. 622-627. doi:10.1109/ITNG.2008.163

ROŞCA, I., NĂSTASE, P. & MIHAI, F. (2010). Information Systems Audit for University Governance in Bucharest Academy of Economic Studies. *Informatica Economică, 14*(1), 21-31. [en línea] <http://revistaie.ase.ro/content/53/02%20Rosca,%20Nastase.pdf> [consulta: 12 de junio de 2011]

ROSENTHAL, D. (2008). Bit Preservation: A Solved Problem?. *Ponencia presentada en las actas de Fifth International Conference on Preservation of Digital Objects*, London, UK. [en línea] <http://www.bl.uk/ipres2008/presentations_day2/43_Rosenthal.pdf> [consulta: 9 de septiembre de 2010]

ROTHENBERG, J. (1999). *Avoiding technological quicksand : finding a viable technical foundation for digital preservation*. Washington DC, Council on Library and Information Resources, 1999. [en línea] <http://www.clir.org/pubs/reports/rothenberg/pub77.pdf> [consulta: 2 de febrero de 2010]

RUAN J., MCDONOUGH, J. P. (2009). En Liu H., Zheng X. G. (Eds.), *Preserving born-digital cultural heritage in virtual world*. NEW YORK; 345 E 47TH ST, NEW YORK, NY 10017 USA: IEEE. doi:10.1109/ITIME.2009.5236324

SAFINA, S. (2003). *Vulnerabilidad sísmica de edificaciones esenciales. Análisis de su contribución al riesgo sísmico.* (Tesis doctoral, Universitat Politècnica de Catalunya). [en línea] <http://www.tesisenxarxa.net/TESIS_UPC/AVAILABLE/TDX-0225103-164824/> [consulta: 2 de febrero de 2010]

SAWYER, D. (2005). *OAIS Reference Model Standard:Motivation, Applicability, Follow-on Efforts.* [en línea] <http://edge.cs.drexel.edu/LTKR/sawyer.pdf> [consulta: 10 de septiembre de 2011]

SCOTT, E. (2007). e-Records in health—Preserving our future. *International Journal of Medical Informatics, 76*(5), 427-431. doi:10.1016/jj.ijmedinf.2006.09.007

SEADLE, M. (1997). Digitization for the masses. *Reference Services Review, 25*(3/4), 119-130. doi:10.1108/00907329710307255

SICOTTE, C.; PARÉ, G.; MOREAULT, M. & PACCIONI, A. (2006). A Risk Assessment of Two Interorganizational Clinical Information Systems. *Journal of the American Medical Informatics Association, 13*(5). doi:10.1197/jamia.M2012

SIERRA, J.; RIBARGORDA, A. & MUÑOZ, A. (1999). Security interface between Métrica and Magerit. Development of secure information systems. Ponencia presentada en *IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology*. Madrid, Spain.

SPENCE, J. (2006). Preserving the cultural heritage: An investigation into the feasibility of the OAIS model for application in small organisations. Ponencia presentada en *Aslib Proceedings, 58*(6) 513-524. doi:10.1108/00012530610713597

STEAD, W. (2011). *Emerging Computational Approaches to Interoperability – the Key to Long Term Preservation of EHR Data*. [en línea] <http://ddpehr.nist.gov/pdf/Stead-_NLM_4-5-11_v10.pdf> [consulta: 10 de septiembre de 2011]

STEINHART, G., DIETRICH, D. (2009). Establishing Trust in a Chain of Preservation. The TRAC Checklist Applied to a Data Staging Repository (DataStaR) *D-Lib Magazine, 15*(9/10). [en línea] < http://www.dlib.org/dlib/september09/steinhart/09steinhart.html> [consulta: 9 de enero de 2010]

STRICKLAND, N. (2004) Multidetector CT: what do we do with all the images generated? *The British Journal of Radiology 77,* S14-S19. doi:10.1259/bjr/95034282

STRODL, S., BECKER, C., NEUMAYER, R., & RAUBER, A. (2007). How to choose a digital preservation strategy: Evaluating a preservation planning procedure. Ponencia presentada en *Proceedings of the 7th ACM/IEEE-CS Joint Conference on Digital Libraries*, Vancouver, BC, Canada. 29-38. doi:doi.acm.org/10.1145/1255175.1255181

SYALIM, A.; HORI, Y. & SAKURAI, K. (2009) Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. *Ponencia presentada en International Conference on Availability, Reliability and Security*, Fukuoka, Japan. doi:10.1109/ARES.2009.75

TANSLEY, R., BASS, M., STUVE, D., BRANSCHOFSKY, M., CHUDNOV, D., MCCLELLAN, G. & SMITH, M. (2003). The DSpace institutional digital repository system: Current functionality. Ponencia presentada en *Proceedings of the 3rd ACM/IEEE-CS Joint Conference on Digital Libraries,* Houston, Texas. 87-97.

Trinchão, B., Mazetto, C., Oliveira, J., Regina, O. & Silva, L. (2011). 3D preserving xviii century barroque masterpiece: Challenges and results on the digitalnext termprevious termpreservationnext term of Aleijadinho's sculpture of the Prophet Joel. *Journal of Cultural Heritage,* (0) doi:dx.doi.org/10.1016/j.culher.2011.05.003

UNESCO (2004). *Carta sobre la preservación del patrimonio digital*. Actas de la Conferencia General. Paris, Francia, 79-82.

WACTLAR, H., CHRISTEL, M. (2002). Digital video archives: Managing through metadata. En *Building a national strategy for digital preservation: Issues in digital media archiving* (pp. 84)

WALTERS, T., SKINNER, K. (2010). Economics, sustainability, and the cooperative model in digital preservation. *Library Hi Tech, 28*(2), 259-272. doi:10.1108/07378831011047668

WATERS, D., GARRETT, J. (1996). *Preserving Digital Information. Report of the Task Force on Archiving of Digital Information*. [en línea]< http://www.clir.org/pubs/reports/pub63watersgarrett.pdf> [consulta: 1 de julio de 2011]

WEATHEBURN, G., BRYAN, S. (1999) The effect of picture archiving and communications system (PACS) on patient radiation doses for examination of the lateral lumbar spine. *The Bristish Journal of Radiology*, *72*(858), 534-545.

WENTZEL, L. (2006). Scanning for digitization projects. *Library Hi Tech News Incorporating Online and CD Notes*, *23*(4), 11-13. doi:10.1108/07419050610674712

WILLCOCKS L., MARGETTS H. (1994). Risk assessment and information systems. *European Journal of Information Systems*, *3*, 127–138. doi:10.1057/ejis.1994.13

WILSON, A. (2007). *Significant propierties report*. [en línea] <http://www.significantproperties.org.uk/wp22_significant_properties.pdf > [consulta: 18 de mayo de 2011]

WOODYARD, D. (2002). *The OAIS experience at the British Library*. ERPANET OAIS Training Seminar, [en línea] <http://www.erpanet.org> [consulta: 2 de septiembre de 2011]

WORLD HEALTH ORGANIZATION (2006) *Electronic Health Records: Manual for Developing Countries* [en línea] < http://www.wpro.who.int/NR/rdonlyres/5753F8CF-8A78-4639-BEFC-F0EE9B3CBA0A/0/EHRmanual.pdf > [consulta: 18 de mayo de 2010]. ISBN: 92-906-1217-7

ZELLER, J. (2010). Cost of digital archiving: Is there an universal model? Ponencia presentada en *Proceedings of the 8th European Conference of Digital Archiving*, Bern, Switzerland.

10

Abreviaciones y Acrónimos

10 Abreviaciones y acrónimos

A fin de evitar problemas de compresión o confusión en los acrónimos, se ha mantenido en todo el texto la nomenclatura original si ésta es en inglés.

10.1 Acrónimos

ABS	Área básica de Salud.
AIP	Archival Information Package.
AS/NZ 4360	Australian and New Zealand Standard on Risk Management 4360.
CCAA	Comunidades Autónomas
CCSDS	Consultative Committee for Space Data Systems.
CCTA	Central Computer and Telecommunications Agency.
CNES	Centre national d'études spatiales.
CRAMM	CCTA Risk Analysis and Management Method.
DIP	Dissemination Information Package.
DRAMBORA	Digital Repository Method Based on Risk Assessment.
EHR	Electronic Health Record.
ENS	Esquema Nacional de Seguridad.
ESA	European Space Agency.
HCE	Historia clínica electrónica.

IEC	International Electrotechnical Commission.
ISO	International Organization for Standardization.
IT	Information and Technology.
ITC	Information Technology and Communication.
JPG	Joint Photographic Experts Group.
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
NASA	National Aeronautics and Space Administration.
OAIS	Open Archival Information System.
OCTAVE	Operationally Critical Threat, Asset, and Vulnerability Evaluation.
OMS	Organización Mundial de la Salud.
PDF	Portable Document Format.
PDI	Preservation Description Information.
PILAR	Programa de Análisis y Gestión de Riesgos.
SIP	Submission Information Package.
TDR	Trustworthy Digital Repository.
TIFF	Tagged Image File Format.
TRAC	Trustworthy Repositories Audit & Certification.
UML	Unified Modeling Language.

UNESCO	Organización de las Naciones Unidas, para la Educación la Ciencia y la Cultura.
XML	Extensible Markup Language.

10.2 Glosario

En este apartado se introduce a la terminología existente en la preservación digital. Sin ánimos de ser extenso, se facilita la terminología empleada, no sólo en todo el estudio, sino terminología que también se encuentra en la literatura a fin de que sea más sencillo entender los términos.

Activo	Elemento que pertenece a una entidad que se analiza a fin de calcular el riesgo del ser dañado. Ej: Un terminal de ordenador
Análisis forense	Técnica de análisis informático que permite extraer información de un soporte digital total o parcialmente.
Archivo Activo	Lugar donde se almacenan historias clínicas que todavía no han finalizado su proceso asistencial.
Archivo Pasivo	Lugar donde se almacenan historias clínicas que ya han finalizado su proceso asistencial. Normalmente una historia clínica pasa al archivo pasivo al cabo de 3 años de finalizar el proceso asistencial.
Conservación digital	Conjunto de procesos que se ejecutan en una entidad de conservación de datos digitales y que contempla todo el ciclo de vida de un objeto digital.
Coste	Relacionado con la preservación digital, precio valorado en unidades monetarias que hay pagar para preservar datos digitalmente.

Emulación	Técnica informática que permite mediante un software generar otro que imite uno anterior.
Estándar	Conjunto de reglas que sirve como tipo, modelo, norma, patrón o referencia.
Exitus	Relacionado con los archivos médicos. Un caso de exitus es relativo a aquellas historias clínicas cuyos pacientes han fallecido.
Largo Plazo	Unidad de tiempo que se considera en un archivo digital para conservar digitalmente objetos. Se consideran largo plazo períodos superiores a 10 años. Este tiempo es suficientemente largo para ser conscientes de los impactos de los cambios tecnológicos, incluyendo soporte para nuevos medios y formatos de datos además de los cambios en una comunidad de usuarios sobre la información que está siendo retenida por un repositorio.
Migración	Técnica informática mediante la cuál un objeto digital se convierte en otro de forma que permita ser accedido por un software más moderno. En el proceso de migración puede haber pérdidas de forma.
Preservación digital	Conjunto de técnicas que permite acceder a la información de objetos digitales tecnológicamente obsoletos.

Proceso Asistencial	Período del tiempo por el cual un paciente es atendido. Durante este tiempo su historia clínica permanece activa.
Riesgo	Probabilidad de que un objeto resulte dañado.
Salvaguarda	Mecanismo informático o de otro tipo que permite evitar daños a un activo.

Anexo I

11 Anexo I

11.1 Cartas del estudio del caso dirigidas a los hospitales

Sr.,

Me presento: soy el Dr.. Miguel Térmens Graells, profesor del Departamento de Biblioteconomía y Documentación de la Universidad de Barcelona.

Me dirijo a usted como director de la tesis doctoral que está preparando el señor Juan José Boté Vericad. En esta tesis se quieren analizar los requerimientos de seguridad necesarios para asegurar la preservación a medio y largo plazo de la documentación digital generada por las instituciones hospitalarias. Dentro de la fase de recogida de información, hemos seleccionado su institución como una de las que creemos representativas del sector y que nos puede aportar unas informaciones que, una vez analizadas junto con las de otras instituciones, nos permitan conocer cuál es la realidad de este tema en nuestro país.

Por ello, pido que colaboren en la recogida de datos que está haciendo el señor Juan José Boté Vericad. Esta colaboración se concreta en:

- El señor Juan José Boté Vericad no necesita tener acceso a datos médicos, administrativas o económicas. Sí necesita saber cómo están organizadas estos datos a nivel informático, en especial en cuanto a su almacenamiento. También necesita poder entrevistarse con el personal que sea responsable del mantenimiento y almacenamiento de estos datos a nivel informático (no en cuanto a su explotación). Los temas principales de interés son: formato de los ficheros, hardware en el que se almacenan, política de copias de seguridad, estándares que se siguen, política de digitalización de documentación impresa, distribución funcional de responsabilidades respecto a la documentación digital, y sistemas de auditoría o de control de calidad aplicados al ámbito informático.
- Pedimos que cumplimente una encuesta relativa a la gestión informática de estos datos. Después deseamos comentar o ampliar los resultados en una entrevista, en horario a convenir.
- No se hablará con pacientes.
- No se hablará con personal médico o administrativo del centro, a no ser que esto haya sido autorizado de forma expresa.
- Las informaciones obtenidas no serán utilizadas para discutir la política en informática o en gestión administrativa de este centro.

- No es necesario decir, que el señor Juan José Boté Vericad mantendrá la confidencialidad de las informaciones a las que pueda tener acceso y que, si es necesario, firmará una declaración de confidencialidad.

Agradezco de antemano su atención y quedo a su disposición para cualquier aclaración.

Cordialmente,

Dr. Miquel Térmens Graells

Barcelona, 8 de febrero de 2011

Anexo II

12 Anexo II

En este anexo se reflejará una encuesta inicial que se hizo en los centros sanitarios de Catalunya.

El objetivo de la encuesta era averiguar si los centros sanitarios disponían de información digital en sus archivos y qué normas seguían por conservarlos.

Datos de la encuesta:

Fuente de los datos:	Ministerio de Sanidad y Política Social
Población:	204 hospitales
Muestra:	204 hospitales
Número de preguntas:	5

Fecha de realización de la encuesta: 5 de febrero de 2010

Fecha límite de recepción de las respuestas: 1 de marzo de 2010

Formato de la encuesta:	preguntas de elección múltiple, cerrada y semiabierta
Formato de envío:	correo postal
Formato de la respuesta:	correo postal

Todas las instituciones encuestadas se encuentran en Catalunya. Los datos postales para el envío de la encuesta, han sido extraídos de la web del Ministerio de Sanidad y Política Social[42] que disponía del Catálogo Nacional de Hospitales 2009. Los datos para su descarga estaban disponibles en formato PDF o en formato de base de datos Access. Esta Base de Datos está actualizada al año en curso.

Se decide escoger Centros Sanitarios pertenecientes a la Red Hospitalaria de Utilización Pública (XHUP), que son las entidades que tienen convenio con la Generalitat de Catalunya y que están en la bases de datos del Ministerio de Salud y Política Social facilitada.

[42] http://www.msc.es/ciudadanos/prestaciones/centrosServiciosSNS/hospitales/home.htm

12.1 Encuesta inicial

1.-Disponen de un archivo digital?

SI NO

2.-Si es así, ¿en qué tipo de soporte guardan la información?

CD □

DVD □

BLUE-RAY □

DISC EXTERNO □

CINTA □

ORDENADOR CENTRAL □

SE ENCARGA UNA EMPRESA EXTERNA □

3.-Siguen algún tipo de normativa local, nacional o internacional para guardar la información en el archivo digital?

SI La podrían especificar?: _____

NO

4.-¿Cuántas personas se encargan de la custodia del archivo digital?

1 □

2 □

más de 2 □

5.- ¿De qué tipos de documentos disponen?

Microsoft Word □

Power Point □

Excel □

Bases de Datos □

Imágenes (JPG, TIFF, PNG, etc) □

Video	AVI	MOV	MPEG	OTRO	□
Audio	MP3	WAV		OTRO	□

Otro:

Especifíquelo, por favor:

12.2 Centros sanitarios que han respondido

El 10 de marzo de 2010 se disponía de 52 (25,49% de los encuestados) respuestas per parte de los hospitales.

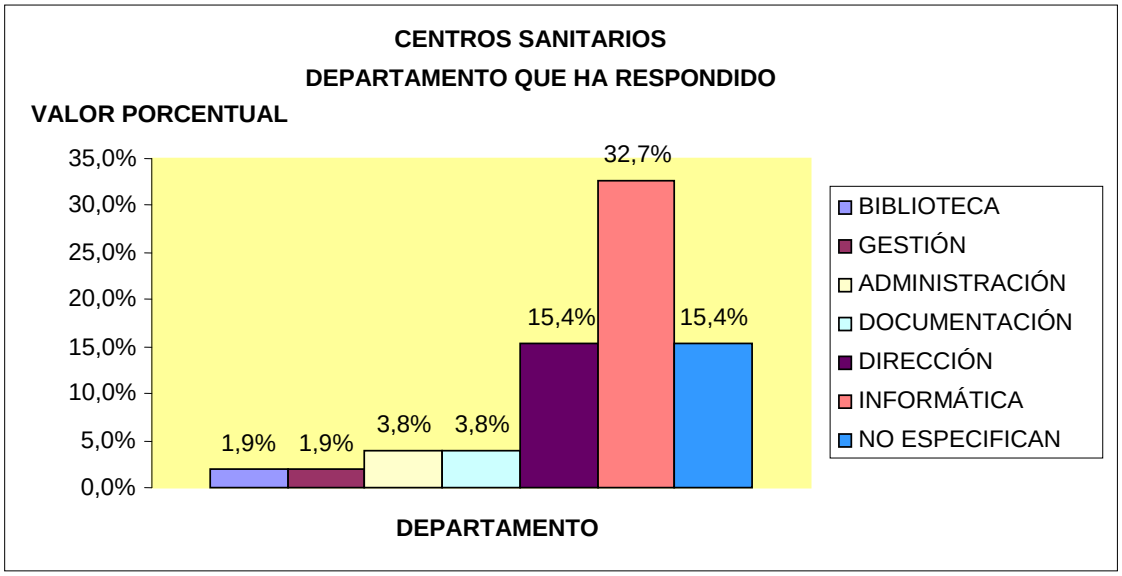

Figura 20. Centros que han respondido

En Figura 20 se puede comprobar que un 32,7% de los centros sanitarios que han respondido, lo ha hecho el departamento de sistemas, informática o IT y por tanto quien está encargado de llevar esta tarea. Después ha respondido en segundo puesto porcentual la dirección. No se han unido Gestión, Dirección y Administración bajo el mismo valor ya que Gestión corresponde a unidades de gestión que responden la encuesta y que muchas veces forman parte del esquema de la organización por debajo de otros estamentos directivos. En el caso de Administración está claro que conceptualmente no es lo mismo. Las áreas de Documentación o Biblioteca prácticamente no ocupan un valor significativo entre los que han respondido. De estos valores se puede sacar la conclusión de que Biblioteca o Documentación no disponen de recursos suficientes, humanos, técnicos o económicos dentro de sus organizaciones para gestionar un archivo digital.

12.3 Análisis de las respuestas

12.3.1 Pregunta 1. Existencia de un archivo digital

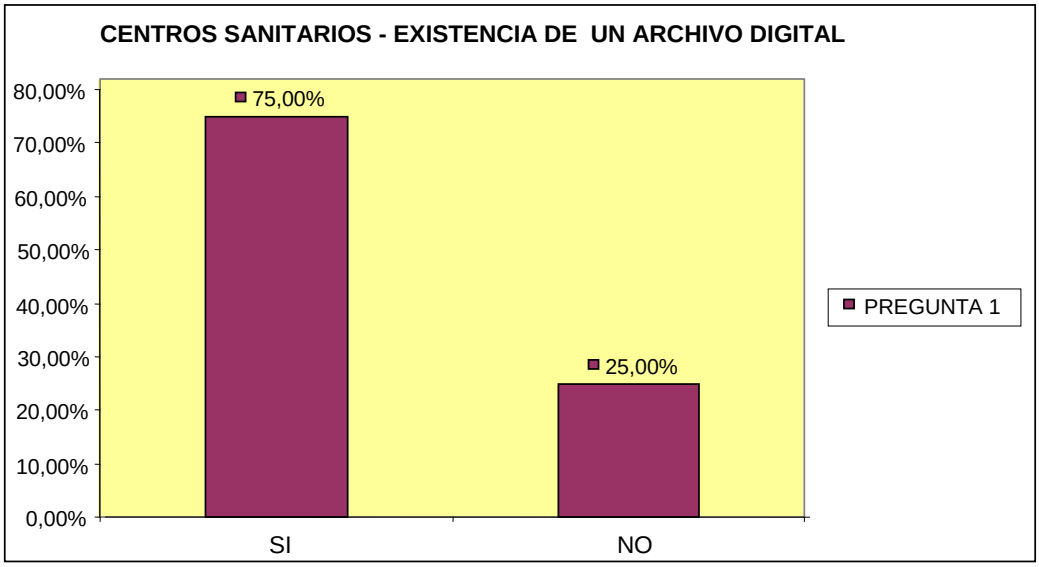

Figura 21. Existencia de un archivo digital

Tal y como se puede observar en la Figura 21, un 75,00% de las entidades sanitarias catalanas que han respondido indican que disponen de un archivo digital y un 25,00% que no disponen de un archivo digital.

12.3.2 Pregunta 2. Soportes de almacenamiento

Esta pregunta admitía varias respuestas y de hecho varios hospitales han seleccionado más de una opción. Lo que sí se puede extraer es que los hospitales que han respondido un 59,62% disponen de una estructura centralizada en sus sistemas de información como se refleja en la Figura 22.

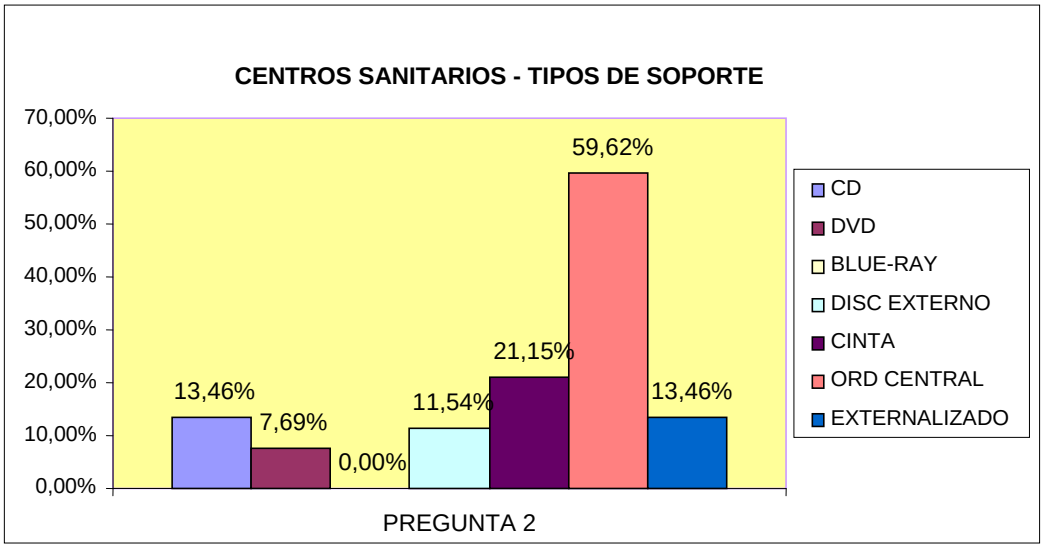

Figura 22. Tipos de soporte

12.3.3 Pregunta 3. Seguimiento de normativas de custodia

En la Figura 23, un 57,69% de los encuestados que han respondido indica que tienen conocimiento de alguna normativa de custodia y un 17,31% que no. Si esto se traslada ahora a cuáles son las normativas que conocen y que aplican en sus centros, se puede ver que en la Figura 24, la LOPD es la norma mayoritaria (40,38%) como normativa de conservación, custodia y almacenamiento.

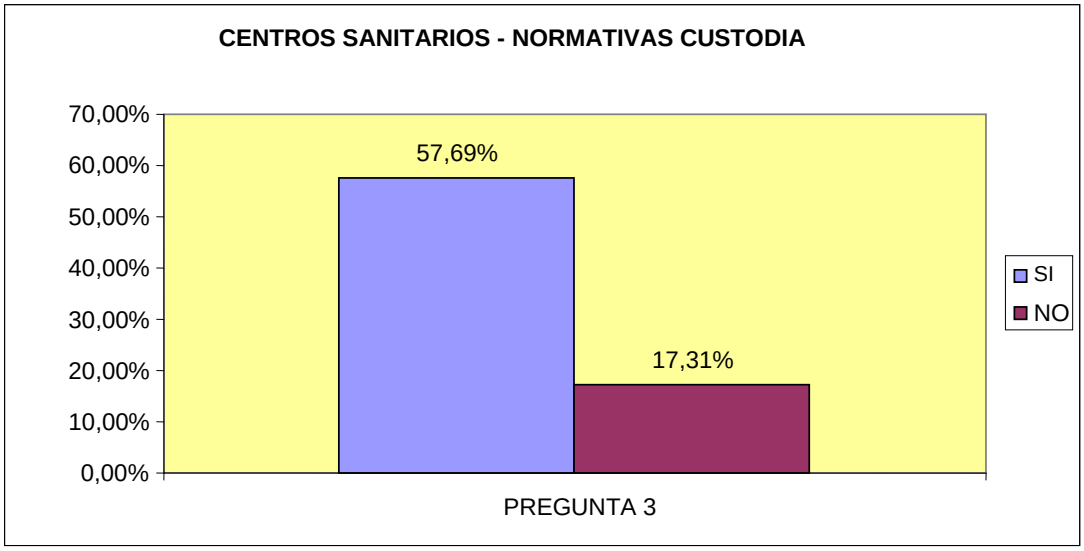

Figura 23. Normativas de custodia

Se puede también observar que algunos manifiestan tener una normativa propia, que la normativa de custodias son las copias de seguridad y finalmente consideran el formato DICOM como una normativa de conservación.

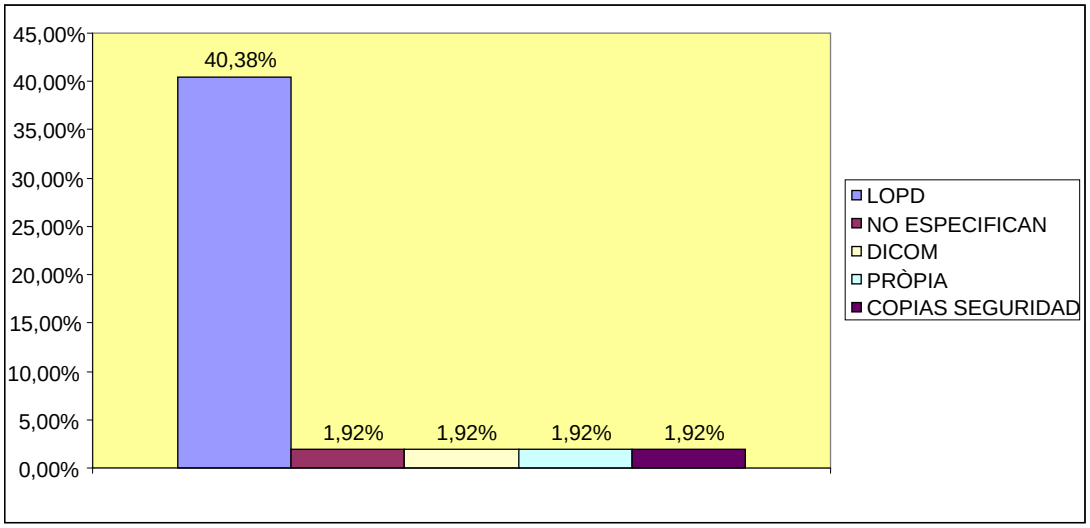

Figura 24. Normativas de custodia (II)

12.3.4 Pregunta 4. Recursos humanos encargados de la custodia

En esta pregunta donde se representan gráficamente las respuestas en la Figura 25, se puede ver que en un 38,46% de las entidades tienen más de dos personas encargadas de la custodia de archivos. Adicionalmente se encuentran relativas a las personas que custodian un archivo médico entre una persona con un 19,23% y dos personas con un 13,46%.

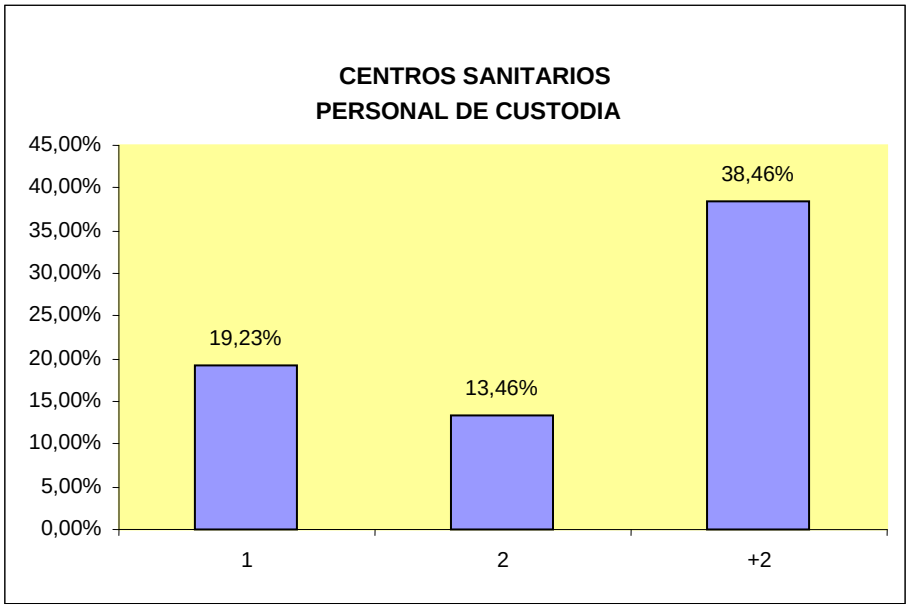

Figura 25. Personal de custodia

12.3.5 Pregunta 5. Tipología documental

En esta pregunta, la respuesta ha sido bastante variada como se puede observar en la Figura 26. Debido a su magnitud en la gestión, las bases de datos (BD) y las imágenes captan mayoritariamente las respuestas, siendo el formato Word con un 51,92% el tercer formato más existente. Es necesario aclarar que en los centros sanitarios las imágenes diagnósticas son en formato DICOM y, por tanto, todos los equipos médicos que generan alguna salida de datos gráfica lo hacen en este formato, para poder integrarla después en el historial médico.

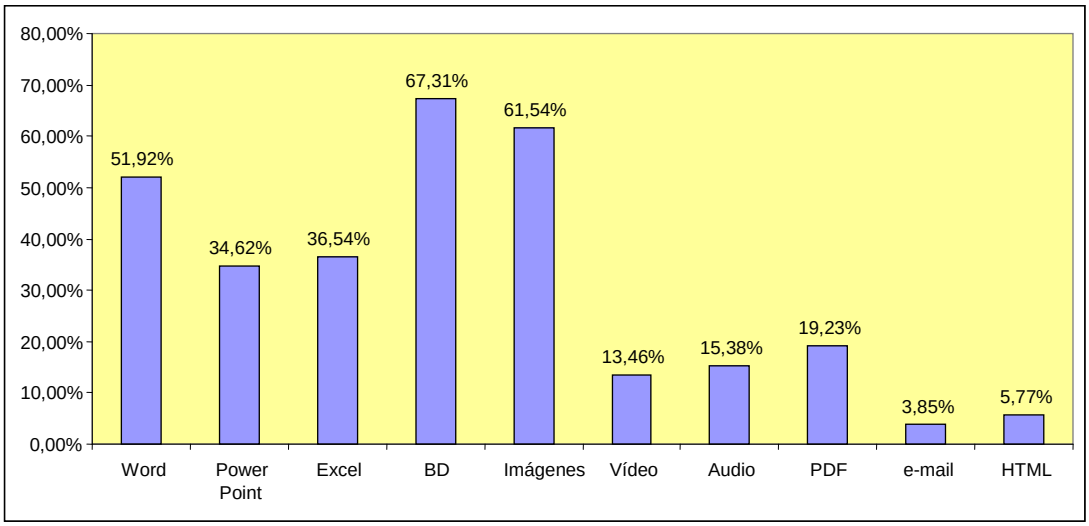

Figura 26. Tipología documental

Anexo III

13 Anexo III

13.1 Cuestionario sobre la conservación digital y seguridad

Pregunta 1 – Marco Organizativo

Disponen de un comité de gestión de la seguridad de la información?

SI NO

Indique qué marco legislativo afecta al sistema de información en el archivo digital (Marque las opciones que corresponda)

LO 15/1999, de Protección de Datos de Carácter Personal	
Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica	
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.	
RD 3/2010, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica	
RD 21/2000, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica	
Llei 16/2010, modificació de la llei 21/2000, del 29 de desembre, sobre els drets d'informació concernent la salut i l'autonomia del pacient, i la documentació clínica	

Pregunta 2 – Normativa de seguridad

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Directrices documentadas donde se indica la estructuración de la documentación de seguridad del sistema, gestión y acceso	
Directrices que indique que es lo que se considera uso indebido del equipamiento o la información	
Documentación que indique la responsabilidad del personal respecto al cumplimiento y violación de normas de seguridad de acuerdo con la legislación vigente	
Documento explicativo sobre los deberes y obligaciones en materia de seguridad de de información	
Plan de contingencias documentado para casos de quiebra de su sistema	
Documento explicativo sobre la calidad de los registros del Sistema de Información	

Pregunta 3 – Arquitectura de la seguridad

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Inventario de hardware	
Procesos de actualización de hardware	
Inventario de software	
Documentación que indique las líneas de defensa	
Documentación que indique la identificación y autenticación de los usuarios	
Controles técnicos internos	
Procesos documentados sobre vigilancia tecnológica	

Pregunta 4 – Procedimientos de seguridad y autorización

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Como se llevarán a cabo las tareas habituales en el lugar de trabajo	
Quién debe llevar a cabo las tareas en el lugar de trabajo	
Procesos, procedimientos o documentación de comportamientos anómalos en el sistema (creación de informes de errores, análisis de amenazas, etc.)	
Utilización de instalaciones habituales y alternativas	
Entrada de equipos en producción	
Entrada de aplicaciones en producción	
Establecimientos de enlaces de comunicaciones con otros sistemas	
Utilización de medios de comunicación habituales y alternativos	
Utilización de soportes de información	
Utilización de equipos móviles	
Análisis de sistemas	
Descripción de personal	
Necesidades de seguridad	

Pregunta 5 – Sobre el análisis de riesgos

Utilizan alguna de las metodología de evaluación de riesgos citadas a continuación?

MAGERIT		MARION		DRAMBORA	
OCTAVE		ISAMM			
CRAMM		IT-Grundschutz			
MARION		ISO 31000:2009		CAP	

Si utilizan **otra** diferente la podrían indicar?

Si la respuesta es **otra**, podría indicar cuál de estas medidas se contemplan en la evaluación de riesgos?

Identificación cualitativa de los activos de más valor □
Cuantificación de las amenazas □
Identificación de les vulnerabilidades de les amenazas □
Identificación de les salvaguardas □
Identificación del valor residual del riesgo □

Pregunta 6 – Certificación de componentes

Disponen de componentes/equipos certificado por los fabricantes con normativas internacionales o europeas?

SI NO

Pregunta 7 – Adquisición de nuevos componentes

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Controles para controlar las necesidades de seguridad	
Plan de formación i desarrollo del personal de sistemas de información o archivo	
Documentos de información financiera respecto de su unidad	
Procedimientos en la adquisición de nuevos componentes del sistema	

Pregunta 8 – Gestión de les capacidades

El personal dispone de perfiles laborales adecuados a la unidad donde trabajan
(1 Totalmente en desacuerdo, 5 Totalmente de acuerdo):

1 2 3 4 5

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Necesidades de procesamiento del sistema	
Necesidades de software)	
Procedimiento sobre vigilancia tecnológica	
Procedimientos sobre les necesidades de los usuarios	

Pregunta 9 – Control de acceso

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

El sistema de información, identifica los usuarios de forma única	
El sistema de información tiene mecanismos de acceso de prevención de acciones no autorizadas	
Existen **personas** responsables que pueden decidir los derechos de acceso a recursos por parte de los usuarios del sistema	
Existe control de accesos a los registros de configuración del sistema	
Un sistema de auditoría o supervisión de cualquier función en el sistema	
Un sistema de control concurrente para la denegación o autorización de tareas críticas	
Políticas de derechos de acceso de los usuarios	

Pregunta 10 - Autentificación

¿Disponen de procedimientos de validación de acceso dentro del sistema?
Ex: -Suspensión del autentificador después de un periodo de no utilización, No utilización de Claves concertadas, dispositivos físicos personalizados o biométricos

SI NO

Pregunta 11 – Acceso local

¿Disponen de documentación sobre les políticas de acceso (reglas de autorización, requerimientos de autentificación)?

SI NO

¿Las tienen implementadas?

SI NO

Pregunta 12 – Acceso remoto

Disponen de documentación escrita sobre las políticas d acceso remoto?

SI NO

¿Las tienen implementadas?

SI NO

Pregunta 13 - Explotación

Los equipos están configurados de forma que:

Se retiran las cuentas y contraseñas estándares ☐
Se les aplica la regla de mínima funcionalidad ☐
Se les aplica la regla <<seguridad por defecto>> ☐

Pregunta 14 – Instalaciones, configuraciones

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Procesos reactivos ante la posibilidad de actualizaciones de software de seguridad basada en una evaluación beneficio-riesgo	
Documentación para atender las especificaciones de los fabricantes	
Procesos para un seguimiento continuo ante cambios por defecto	
Procesos de gestión del cambio documentados que identifiquen los cambios en los procesos críticos	
Mecanismos de prevención y reacción ante código maligno	
Proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema	
Procesos de registros de la actividad de los usuarios (logs de usuario, traza de operaciones)	
Disponen de registros de gestión de incidencias (Aclaración: errores de gestión, incidentes inapropiados por parte del personal)	
Protección sobre los registres de acceso	
Disponen de equipos con claves criptográficas protegidas durante todo el ciclo de vida	

Pregunta 15 – Servicios con terceras partes

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Especificación de acuerdos con terceras partes	
Documentación que especifique los acuerdos y tareas de coordinación con terceras partes (Ex: externalización de algun servicio vinculado a TIC)	
Acuerdos con terceros sobre la provisión del servicio por medios alternativos en caso de indisponiblidad del servicio	

Pregunta 16 – Continuidad del servicio

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Documentación que indique análisis de impacto ante el crecimiento del sistema	
Plan de continuidad del sistema	
Calendario de autoevaluación de revisiones periódicas del sistema	

¿Cuál es el tiempo de parada asumible de todo el servicio?

Pregunta 17 – Monitorización del sistema

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Mecanismos para a la detección de intrusiones	
Sistema de métricas que midan los desarrollos reales en materia de seguridad ante posibles amenazas	

Pregunta 18 – Gestión de personal

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Directivas que indiquen los planes de desarrollo, definición de competencias del personal que trabaja	
Documentación sobre los roles y responsabilidades del personal y descripción de su lugar de trabajo	
Documentación sobre los deberes y obligaciones del personal	
Disponen de un plan de formación continuada para formar el personal en d) Configuración de sistemas e) Detección y reacción ante incidencias f) Gestión de la información en cualquier soporte que se encuentre.	
Es dispone de un plan de servicio continuado con personal alternativo con las mismas garantías que el personal habitual	

Pregunta 19 – Medidas de protección

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Los equipos están separados según su función específica	
El acceso a los equipo disponen de controles a sus áreas	
Les áreas de los equipos están vigiladas	
Las personas que acceden a las áreas donde el equipo forma parte del sistema de información se identifican	
Se registran las entradas y salidas de personas	
Se disponen de controles sobre condiciones de temperatura y humedad	
Se disponen de protecciones frente a amenaces identificadas en el análisis de riesgos	
Es disponen de protecciones de cableado frente incidentes fortuitos o deliberados	
Se dispone de un plan de servicio continuado que garantice el suministro eléctrico y el funcionamiento de las luces de energía	
Se dispone de un plan de servicio continuado que garantice la protección frente a incendios	
Se dispone de un plan de servicio continuado que garantice la protección frente a inundaciones	
Se dispone de un plan de servicio continuado que registra toda entrada y salida de material así como la identificación de la personal que autoriza el movimiento	
Disponen de un plan de servicio continuado que garantice la disponibilidad de instalaciones alternativas en las mismas condiciones de seguridad en caso de que las instalciones habituales no estén disponibles.	

Pregunta 20 – Protección de los equipos

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Sus necesidades de seguridad incluyen que el lugar de trabajo esté despejado sin más material que el requerido para la actividad que se esté realizando en cada momento	
Los lugares de trabajo se bloquean pasado un tiempo prudencial de inactividad	
Los equipos portátiles están protegidos	
Plan de contingencia con la posibilidad de emplear medios alternativos para garantizar la continuidad del servicio	

Pregunta 21 - Backups

El sistema de seguridad realiza la copia de (marque la opción indicada):

e) La información de trabajo de la organización
f) Las aplicaciones en explotación incluidos los sistemas operativos
g) Datos de configuración, servicios, aplicaciones, equipos u otra naturaleza
h) Claves para preservar la confidencialidad de la información

Pregunta 22 – Protección de las comunicaciones

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Controles de flujos de información que separe la red interna de la exterior	
Sistemas redundantes	
Controles para la protección de la confidencialidad de las comunicaciones	
Controles para la protección de la autenticidad e integridad de la información	
Redes segregadas	

Pregunta 23 – Protección de los soportes de información

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Los soportes externos donde se guardar información, están etiquetados de forma que sin revelar su contenido se indique el nivel de seguridad de la información contenida	
Los usuarios están capacitados para entender el significado de les etiquetas	
Mecanismos criptográficos en dispositivos removibles con tal de garantizar la confidencialidad y la integridad de la información	
Mecanismos de custodia en los soportes de información de forma que se garantice su acceso y se respeten las exigencias del fabricante	
Controles de entrada y salida cuando la información se tiene que desplazar a un lugar externo	
Borrado de la información cuando se reutilizan soportes de información	

Pregunta 24 – Protección del software

Desarrollan aplicaciones de software propias ? SI NO

En caso afirmativo,

- ¿Se realiza sobre un sistema diferente al de producción? SI NO
- ¿Aplican metodologías reconocidas en su desarrollo? SI NO
- Las pruebas anteriores a la implantación no se realizan no datos reales SI NO
- ¿Se comprueba que se cumplen los criterios de aceptación en materia de seguridad? SI NO

Al poner en marcha el software nuevo, se comprueba que no se deteriora la seguridad de otros componentes? SI NO

Las pruebas de aceptación no se realizan con datos reales SI NO

Pregunta 25 – Protección de la información

Indique si dispone de los procesos, documentación escrita o mecanismos siguientes: (Marque la opción que corresponda)

Procedimientos para cualificar la información	
Procedimientos de cifrados de la información	
Procedimientos que empleen la firma electrónica	
Procedimientos de mecanismos de sellado de tiempo (time stamping)	
Procedimientos de limpieza de documentos que garanticen la confidencialidad de la información	

13.2 Cuestionario de ampliación y entrevista

Historias Clínicas

- ¿La introducción de datos en la historia clínica es introducida por el profesional a medida que hace las visitas?
- ¿Se puede acceder desde todos los centros mediante acceso remoto o de otra forma a las historias clínicas?
- ¿Disponen de archivo activo y pasivo digital?
- Si disponen de las historias clínicas divididas en activo y pasivo, ¿cuánto tiempo consideran que una historias digitales pasa al pasivo? Si este proceso no existe indique cuando pasan las de formato papel
- ¿Generan algún tipo de metadatos?
- ¿Cómo se localiza la historia de los pacientes? (ej: número de historia, DNI, etc)
- Si los pacientes les piden acceso a su historia clínica, ¿pueden hacerlo? ¿Siguen un protocolo?
- Indique quien tienen acceso a las historias clínicas electrónicas (que perfiles laborales genéricos)
- ¿Tienen constancia de cuanto ocupa en bytes una historia clínica media con datos anexos (PDF, imágenes radiológicas, etc)?

Anexo IV

14 Anexo IV

Como se ha mencionado en la introducción, en las páginas siguientes se exponen las tablas de resultados correspondientes primero a los resultados obtenidos en la auditoría de TRAC, a continuación los resultados obtenidos en la auditoría del Esquema Nacional de Seguridad y finalmente los datos obtenidos en la encuesta, donde se cruzan los parámetros del Esquema Nacional de Seguridad y de TRAC. Al finalizar, se presenta un análisis pormenorizado de los resultados de la encuesta. Las tablas disponen de tres valores en sus casillas: x indica que se cumple el requisito, n.a. no aplica y si en la casilla no hay datos es que ese valor se cumple por la entidad correspondiente. Los valores correspondientes a los hospitales no se corresponden con la lista facilitada en orden alfabético; esto se hace así, a fin de garantizar su anonimato.

14.1 Exposición del cuestionario completo

En este apartado se encuentran todas las respuestas al cuestionario completo, que está reproducido en el Anexo II. A continuación se encuentra un análisis pormenorizado de todas las respuestas. En cada pregunta se indica entre paréntesis cuantos indicadores hay, que indicadores de TRAC y del Esquema Nacional de Seguridad están vinculados, así como los datos contestados pertenecientes a cada entidad. El orden de las entidades está cambiado respecto a la lista indicada en orden alfabético. Esto se realiza a fin de mantener la confidencialidad de los datos.

		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 1 (7)	Disponen de un comité de gestión de la seguridad de la información										
1 a	SI / NO	[org. 1]	A1.1	X	X	X	X	X	X	X	X
1 b	LO 15/199		A2.2	X	X	X	X	X		X	X
1 c	L 41/2002			X	X	X		X		X	X
1 d	RD 34/2002			X				X		X	X
1 e	RD 3/2010				X					X	
1 f	RD 21 /2000			X	X	X		X		X	X
1 g	L 16/2010			X	X	X		X		X	X
Pregunta 2 (6)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
2 a	Estructuración de la documentación de seguridad del sistema gestión y acceso	[org. 2]	A2.2	X	X	X	X	X		X	X
2 b	Directrices sobre la consideración de uso indebido de información	[org. 2]	A2.1	X	X	X	X			X	X
2 c	Responsabilidad del personal frente violación de la seguridad	[org. 2]	A2.2	X	X	X	X	X		X	X
2 d	Deberes y obligaciones en materia de seguridad de información	[mp.per.3]	A1.1	X	X	X	X	X	X	X	X
2 e	Plan de contingencias en caso de fallo del sistema	[mp.per.3]			X			X	X	X	X
2 f	Explicación sobre la calidad de información de los registros del SI	[mp.per.3]									
Pregunta 3 (7)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
3 a	Inventario de hardware	[op.exp.1]	C2.1	X	X	X	X	X	X	X	X
3 b	Procesos de actualización de hardware	[op.exp.2]	C2.1	X		X	X	X	X	X	
3 c	Inventario de software	[op.exp.1]	C3.3	X	X	X	X	X	X	X	X
3 d	Documentación que indique las líneas de defensa		C3.3	X				X			X
3 e	Indicaciones sobre la identificación y autenticación de usuarios		C3.3	X	X	X	X	X	X	X	X
3 f	Controles técnicos internos		C1.9	X	X	X	X			X	
3 g	Procesos documentados sobre vigilancia tecnológica		C2.1		X		X		X		

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 4 (13)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
4 a	Forma de llevar a cabo las tareas habituales en el lugar de trabajo	[org. 4]	C3.1	X	X		X	X	X	X	
4 b	Que tiene que llevar a cabo las tareas en el lugar de trabajo		C3.1	X	X		X	X		X	
4 c	Registro de comportamientos anomálos en el sistema		C3.1	X	X		X	X	X	X	
4 d	Utilización de instalaciones habituales y alternativas		C3.1	X			X				
4 e	Entrada de equipos en producción		C3.1	X	X		X		X		X
4 f	Entrada de aplicaciones en producción		C3.1	X	X	X	X		X	X	
4 g	Establecimientos de enlaces de comunicaciones con otros sistemas		C3.1	X	X		X	X	X	X	X
4 h	Utilización de medios de comunicación habituales y alternativos		C3.1	X	X	X	X			X	
4 i	Utilización de soportes de información		C3.1	X	X		X		X		
4 j	Utilización de equipos móviles		C3.1	X	X						
4 k	Análisis de sistemas		C3.1	X	X		X	X	X	X	
4 l	Descripción de personal		C3.1	X	X		X		X	X	X
4 m	Necesidades de seguridad		C3.1	X	X		X			X	
Pregunta 5 (14)	Utilizan alguna metodología de análisis de riesgos?										
5 a	MAGERIT	[op. pl. 1]	C3.1								
5 b	OCTAVE										
5 c	CRAMM										
5 d	MARION										
5 e	DRAMBORA										
5 f	ISAMM										
5 g	IT-Grundschutz										
5 h	ISO 31000:2009									X	
5 i	NINGUNA			X	X	X	X				X
5 j	OTRA										
5 k	Identificación cualitativa de los activos de más valor en el sistema			X	X						
5 l	Cuantificación de las amenazas				X						
5 m	Identificación de las vulnerabilidades de las amenazas				X						
5 n	Identificación de las salvaguardas				X						
5 o	Identificación del valor residual del riesgo										

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 6	Disponen de componentes/equipos certificados con normativas internacionales o europeas										
6 a	SI	[op.pl.5]		X	X	X	X	X	X	X	X
Pregunta 7 (4)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
7 a	Controles para controlar las necesidades de seguridad	[op.pl.3]	A2.3	X	X		X			X	
7 b	Plan de formación para el personal de ITC o archivo		C3.1	X	X				X	X	
7 c	Documentos de información financiera de su unidad		C3.2	X	X		X		X	X	
7 d	Procedimientos para adquirir nuevos componentes del sistema		A4.4	X	X		X		X	X	
Pregunta 8 (9)	El personal dispone de perfiles laborales adecuados a la unidad donde trabajan										
8 a	1 (en desacuerdo)	[op.pl.4]	A2.1								
8 b	2										
8 c	3			X		X			X		
8 d	4				X			X			
8 e	5 (totalmente de acuerdo)						X			X	
	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
8 f	Necesidades de proceso del sistema		C1.1	X	X				X		
8 g	Necesidades de software		C1.1	X	X		X	X	X		
8 h	Procedimientos de vigilancia tecnológica		C2.1		X				X		
8 i	Procedimientos sobre las necesidades de los usuarios		C2.1	X	X		X		X		X
Pregunta 9 (7)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
9 a	Identificación a los usuarios de forma única	[op.acc.1]	B6.5	X	X	X	X	X	X	X	X
9 b	Mecanismos de acceso de prevención de acciones no autorizadas	[op.acc.2]	B6.3	X	X	X	X	X			
9 c	Existen personas responsables que pueden decidir sus derechos de acceso de recursos por parte de usuarios del sistema	[op.acc.2]	B6.3	X	X	X	X	X	X	X	X
9 d	Control de acceso a los registros de configuración del sistema	[op.acc.2]	B6.3	X	X	X	X	X	X	X	X
9 e	Un sistema de auditoría de cualquier función en el sistema	[op.acc.3]	B6.6	X	X		X		X	X	X
9 f	Un sistema de control concurrente para la denegación o autorización de tareas críticas	[op.acc.3]	B6.6	X	X				X	X	
9 g	Políticas de derechos de acceso a los usuarios	[op.acc.4]	B6.3	X	X	X	X	X	X	X	X

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 10 (1)	Disponen de procedimientos de validación de acceso dentro del sistema										
10 a	SI	[op.acc.5]	B6.4	X	X		X	X	X	X	X
Pregunta 11 (2)	Disponen de documentación sobre las políticas de acceso										
11 a	SI	[op.acc.6]	B6.4	X	X	X	X		X	X	X
	¿Las tienen implementadas?										
11 b	SI	[op.acc.6]	B6.4	X	X	X	X	X	X	X	X
Pregunta 12 (2)											
12 a	¿Documentación sobre las políticas de acceso remoto?	[op.acc.7]	B6.4	X	X				X	X	
12 b	¿Las tienen implementadas?	[op.acc.7]	B6.4	X	X	X		X	X	X	X
Pregunta 13 (3)	Los equipos están configurados de forma que										
13 a	Se retiran las cuentas y contraseñas estándares	[op.exp.2]	C3.2	X	X			X	X	X	X
13 b	Se les aplica la regla de mínima funcionalidad	[op.exp.2]	C3.2	X	X	X		X	X	X	X
13 c	Se les aplica la regla de "seguridad por defecto"	[op.exp.2]	C3.2		X	X	X		X	X	
Pregunta 14 (10)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
14 a	Actualización de SW de seguridad con beneficio-riesgo	[op.exp.3]	C1.10		X			X			
14 b	Atención a las especificaciones de los fabricantes	[op.exp.4]	C1.7	X	X		X				
14 c	Seguimiento continuo ante cambios por defecto	[op.exp.4]	C1.7	X	X						
14 d	Cambios en los procesos críticos	[op.exp.5]	C1.8		X						
14 e	Prevención y reacción ante código maligno	[op.exp.6]	C3.2	X	X		X	X	X		
14 f	Hacer frente a incidentes con impacto en la seguridad	[op.exp.7]	C3.2		X		X				
14 g	Registros de la actividad de los usuarios	[op.exp.8]	B6.5	X	X		X	X	X		X
14 h	Procesos de registros de gestión de incidencias	[op.exp.9]	B6.6	X	X	X	X	X	X		X
14 i	Protección sobre los registros de acceso	[op.exp.10]	B6.6	X	X		X	X	X		X
14 j	Equipos con claves criptográficas en el ciclo de vida	[op.exp.11]	B6.6	X							
Pregunta 15 (3)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
15 a	Especificación de acuerdos con terceras partes	[op.ext.1]	A5.3	X	X	X	X	X	X	X	X
15 b	Acuerdos y tareas de coordinación con terceras partes	[op.ext.2]	A5.3	X	X	X	X	X	X	X	X
15 c	Acuerdos con terceros de servicio alternativo	[op.ext.9]	A5.3	X	X			X	X	X	

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 16 (3)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
16 a	Análisis de impacto ante el crecimiento del sistema	[op.cont.1]	A3.2		X						
16 b	Plan de continuidad del sistema	[op.cont.2]	A3.2	X	X						
16 c	Calendario de autoevaluación de revisiones periódicas	[op.cont.3]	A3.2	X				X			
16 d	¿Cuál es el tiempo de parada de todo el servicio asumible?	[op.cont.2]	A3.2			< 24h	< 24h	0 h	< 24h		2-4h noches
Pregunta 17 (2)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
17 a	Mecanismos para la detección de intrusiones	[op.mon.1]	B6.2	X	X	X	X		X	X	
17 b	Métricas que midan la seguridad ante posibles amenazas	[op.mon.2]	C3.2		X		X				
Pregunta 18 (7)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
18 a	Directrices que indiquen los planes de desarrollo, definición de competencias del personal que trabaja	[mp.per.2]	A2.2	X	X		X		X	X	X
18 b	Roles y responsabilidades del personal y descripción de su lugar de trabajo	[mp.per.3]	A2.2	X	X		X	X	X	X	
18 c	Documentación sobre los deberes y obligaciones del personal	[mp.per.2]	A2.2				X	X	X	X	
18 d	Plan de formación en configuración de sistemas	[mp.per.4]	A2.2	X					X	X	
18 e	Plan de formación en detección y reacción ante incidentes	[mp.per.4]	A2.2	X	X			X		X	
18 f	Plan de formación en gestión de la información en cualquier soporte	[mp.per.4]	A2.3	X				X		X	
18 g	Plan de servicio con personal alternativo	[mp.per.9]	C3.4							X	

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 19 (13)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
19 a	Los equipos están separados según su función específica	[mp.if.1]	C3.2	X			X	X	X		X
19 b	El acceso a los equipos dispone de controles en sus áreas	[mp.if.1]	C3.2	X		X	X	X	X	X	X
19 c	Las áreas de los equipos están vigiladas	[mp.if.1]	C3.2	X	X			X		X	X
19 d	Las personas que acceden al área de los equipos se identifican	[mp.if.2]	C3.2	X		X	X	X	X	X	X
19 e	Se registran las entradas y salidas de personal	[mp.if.2]	C3.2	X			X	X	X	X	X
19 f	Se disponen de controles de condiciones de temperatura y humedad	[mp.if.3]	C3.2	X	X	X	X	X	X	X	X
19 g	Protecciones frente a amenazas identificadas en el análisis de riesgos	[mp.if.3]	C3.2	X			X	X		X	X
19 h	Se dispone de protecciones de cableados frente incidentes fortuitos	[mp.if.3]	C3.2	X			X	X		X	X
19 i	Plan de servicio continuo que garantice luz y luces de energía	[mp.if.4]	C3.4	X	X	X	X	X	X	X	X
19 j	Garantía de protección frente a incendios	[mp.if.5]	C3.4	X	X	X	X	X	X	X	X
19 k	Garantía de protección frente a inundaciones	[mp.if.6]	C3.4	X					X	X	
19 l	Registro de entrada y salida de material	[mp.if.7]	C3.4	X	X						
19 m	Garantía de disponibilidad de instalaciones alternativas	[mp.if.9]	C3.4								
Pregunta 20 (4)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
20 a	En el lugar de trabajo sólo hay el material requerido	[mp.eq.1]	C3.2	X				X		X	
20 b	Los lugares de trabajo se bloquean pasado un tiempo de inactividad	[mp.eq.2]	C3.1	X	X		X	X	X	X	X
20 c	Los equipos portátiles están protegidos	[mp.eq.3]	C3.1	X	X	X	X	X	X	X	X
20 d	Plan de contingencia para emplear medios alternativos	[mp.eq.9]	C3.4		X		X			X	X

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 21 (5)	El sistema de seguridad realiza la copia de										
21 a	La información de trabajo de la organización	[mp.info.9]	C3.4	X	X		X	X	X	X	X
21 b	Las aplicaciones en explotación incluidos los sistemas operativos	[mp.info.9]	C3.4	X	X		X	X	X	X	X
21 c	Datos de configuración, servicio, aplicaciones, equipos, etc	[mp.info.9]	C3.4	X	X		X	X		X	X
21 d	Claves para preservar la confidencialidad de la información	[mp.info.9]	C3.4	X	X		X	X	X	X	X
21 e	Disponen de un sistema de backup reduntante	[mp.info.9]	C3.4		X	X	X	X	X	X	
Pregunta 22 (5)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
22 a	Separación de la red interna de la externa	[mp.com.1]	C3.2	X	X	X	X	X		X	X
22 b	Sistemas redundantes	[mp.com.1]	C3.2	X	X		X	X		X	X
22 c	Controles de protección de la confidencialidad de la comunicaciones	[mp.com.2]	C3.2	X	X		X	X	X	X	X
22 d	Protección de la autenticidad e integridad de la información	[mp.com.3]	C3.2	X	X		X	X	X		
22 e	Redes segregadas	[mp.com.4]	C3.2	X	X	X		X		X	X
Pregunta 23 (6)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
23 a	Los soportes externos están etiquetados sin desvelar el nivel de seguridad de la información	[mp.si.1]	C3.2				X	X		X	X
23 b	Los usuarios entienden el significado de las etiquetas	[mp.si.1]	C3.2	X			X		X	X	
23 c	Mecanismos criptográficos para garantizar la confidencialidad de la información	[mp.si.1]	C3.2							X	
23 d	Mecanismos de custodia respetando las exigencias del fabricante	[mp.si.1]	C3.2				X	X	X	X	
23 e	Controles de entrada y salida cuando la información se desplaza a un lugar externo	[mp.si.1]	C3.2	X			X	X	X	X	X
23 f	Borrado de la información cuando se reutilizan soportes	[mp.si.1]	C3.2				X	X	X	X	X

Preguntas		ENS	TRAC	ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
Pregunta 24 (7)											
24 a	¿Desarrollan aplicaciones propias?	[mp.sw.1]	C3.2	X	X	X	X	X	X	X	X
24 b	¿Se realizan sobre un sistema diferente al de producción?	[mp.sw.1]	C3.2	X	X	X		X	X	X	X
24 c	¿Aplican metodologías reconocidas en su desarrollo?	[mp.sw.1]	C3.2	X	X		X	X		X	X
24 d	¿Las pruebas anteriores a la implantación no se realizan con datos reales?	[mp.sw.1]	C3.2	X			X				
24 e	¿Comprueban que se cumplen criterios de aceptación en materia de seguridad	[mp.sw.2]	C3.2	X	X		X	X	X	X	X
24 f	¿Se comprueba que no se deteriora la seguridad de otros componentes en la puesta en marcha del software?	[mp.sw.2]	C3.2	X	X	X	X	X	X	X	X
24 g	Las pruebas de aceptación no se realizan con datos reales	[mp.sw.2]	C3.2	X		X	X		X	X	
Pregunta 25 (5)	Indique si dispone de los procesos, documentación escrita o mecanismos siguientes										
25 a	Procedimientos para cualificar la información	[mp.info.2]	C3.2		X			X			
25 b	Procedimientos de cifrados de la información	[mp.info.3]	C3.2	X			X	X		X	X
25 c	Procedimientos que empleen la firma electrónica	[mp.info.4]	C3.2	X	X			X	X		X
25 d	Procedimientos de mecanismos de sellado de tiempo	[mp.info.5]	C3.2					X			
25 e	Procedimientos de limpieza de documentos que garanticen la confidencialidad de la información	[mp.info.6]	C3.2					X			X

14.2 Exposición de resultados en TRAC

Sección	Infraestructura organizacional								
Aspecto	A1 . Governanza y Viabilidad organizacional								
Criterio		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
A1.1.	El repositorio cuenta con una declaración donde el propósito es la retención, gestión y acceso a la información digital a largo plazo	x	x	x	x	x	x	x	x
A1.2	El repositorio tiene un plan adecuado, plan formal de continuidad, los planes de contingencia, y / o depósitos de custodia en el sitio, en caso de que el repositorio deje de funcionar o la gestión o institución que lo financie cambie sus objetivos.								
	A2. Estructura organizacional y personal								
A2.1	El repositorio tiene identificadas y establecidas las obligaciones que necesita llevar a cabo y tiene deber que necesita para mejora y con personal determinado con las destrezas adecuadas y la experiencia para cubrir estas obligaciones.	x	x	x	x			x	x
A2.2	El repositorio cuenta con un apropiado número de personal para llevar a cabo todas las funciones y servicios	x	x	x	x	x		x	x
A2.3	El repositorio dispone de un programa profesional de desarrollo activo que facilita al personal con habilidades y experiencia oportunidades de desarrollo	x				x		x	
Aspecto	A3. Procedimientos contables y marco de políticas								
A3.1	El repositorio tiene definida su comunidad designada así como su base de conocimiento y tiene públicas y accesible definiciones y políticas en el sitio para disponer como se llevarán a cabo los requisitio del servicio de preservación.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A3.2	El repositorio dispone de procedimientos y políticas en plaza, y mecanismos para su revisión, actualización, y desarrollo tanto si el repositorio crece y si la tecnología y las prácticas de la comunidad evolucionan.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A3.3	El repositorio mantiene escritas políticas que especifiquen la naturaleza de cualquier permiso legal necesarias para preservar contenido digital con el paso del tiempo, y el repositorio puede demostrar que estas permisos han sido adquiridos cuando se han necesitado.	x	x	x	x	x	x	x	x
A3.4	El repositorio está comprometido a revisiones periódicas y evaluaciones formales para asegurar la responsabilidad de los desarrollos tecnológicos y la evolución de los requisitos	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a

Sección	Infraestructura organizacional (cont.)								
Aspecto	A3. Procedimientos contables y marco de políticas (cont.)								
Criterio		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
A3.5	El repositorio tiene políticas y procedimientos para garantizar que la información proveniente de los productores y los usuarios se retroalimenta sistemáticamente a lo largo del tiempo.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A3.6	El repositorio cuenta con un historial de cambios documentado en sus operaciones, procedimientos, software y hardware de forma que cuando es necesario está enlazado a estrategias de preservación relevantes y describe los efectos potenciales de preservar contenido digital.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A3.7	El repositorio se compromete a la transparencia y responsabilidad en todas las acciones soportadas en las operaciones y gestión del repositorio especialmente aquellas que afectan a la preservación del contenido digital en el tiempo.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A3.8	El repositorio se compromete a definir, reunir, trazar y facilitar a la demanda sus métricas de integración de información	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A3.9	El repositorio se compromete en una agenda regular de auto-evaluación y certificación y si está certificado, se compromete a notificar a las entidades certificadoras de los cambios operacionales que cambien o anulen su estatus de certificación.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
Aspecto	A4. Sosteniblidad financiera								
A4.1	El repositorio dispone de procesos de planificación de negocio a corto y largo plazo en el lugar para sostener financieramente el repositorio a lo largo del tiempo	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A4.2	El repositorio dispone de procesos para revisar y ajustar los planes de negocio por lo menos anualmente	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A4.3	Las prácticas financieras y procedimientos del repositorio son transparentes, de acuerdo con los estándares relevantes de contabilidad y prácticas, y auditado por terceras partes de acuerdo con los requisitos territoriales y legales.	x	x	x	x	x	x	x	x
A4.4	El repositorio tiene un compromiso continuo para analizar y elaborar informes de riesgo, beneficios, inversiones y costes (incluyendo activos, pasivos y licencias)	x	x		x		x	x	
A4.5	El repositorio se compromete a supervisar y cerrar las brechas en la financiación.	x	x	x	x	x	x	x	x

Sección	Infraestructura organizacional (cont.)								
Aspecto	A5 . Contratos, licencias y pasivos								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
A5.1	Si el repositorio gestiona, preserva y / o facilita el acceso a materiales digitales en nombre de otra organización, tiene y mantiene contratos o acuerdos apropiados de depósito.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A5.2	Los contratos del repositorio o los acuerdos de disposiciones deben especificar y transferir todos los derechos necesarios de preservación y aquellos que ya estén transferidos deben estar documentados.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
A5.3	El repositorio tiene especificados todos los aspectos pertinentes de la adquisición, mantenimiento, acceso, y la retirada de los acuerdos por escrito con los depositantes y demás partes interesadas.	x	x	x	x	x	x	x	x
A5.4	El repositorio registra y gestiona los derechos de propiedad intelectual y las restricciones sobre el uso de contenido del repositorio como es requerido por contrato de depósito, contrato o licencia.	x	x	x	x	x	x	x	x
A5.5	Existen políticas de responsabilidad sobre derechos de autor y propiedad intelectual, en caso de que el repositorio tenga contenidos digitales con propiedades y/o derechos dudosos.	x	x	x	x	x	x	x	x

Sección	Gestión de Objetos Digitales								
Aspecto	B1. Ingesta: adquisición de contenido								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
B1.1	El repositorio identifica las propiedades que preservará de los objetos digitales.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.2	El repositorio especifica claramente la información que debe estar asociada con el material digital en el momento de su depósito (p.e.: SIP).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.3	El repositorio dispone de mecanismos para la autenticación de la fuente de los materiales	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.4	El proceso de ingesta del repositorio verifica cada objeto ingesta (ej. SIP) por su integridad y exactitud especificadas en el punto B1.2.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.5	El repositorio dispone de suficiente control físico sobre los objetos digitales para preservarlos.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.6	El repositorio facilita las repuestas adecuadas durante el proceso de ingesta al productor / depositor	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.7	El repositorio puede demostrar cuando la responsabilidad de la preservación está formalmente aceptada para los contenidos de los objetos de datos entregados (ie, SIP).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B1.8	El repositorio tiene registros actualizados de acciones y procesos de administración que son relevantes para la preservación (Ingesta: adquisición de contenidos)	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
Aspecto	B2. Ingesta: creación del paquete de archivo								
B2.1	El repositorio cuenta con una definición escrita identificable para cada AIP o clase de información preservada por el repositorio.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.2	El repositorio tiene una definición para cada AIP (o clase) que es adecuada para acomodarla dentro de las necesidades de la preservación a largo plazo.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.3	El repositorio cuenta con una descripción de cómo se construye cada AIP desde un SIP.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.4	El repositorio puede demostrar que todos los objetos entregados (ej.: SIP) son o bien aceptados como un todo o como parte de un objeto archivable eventual (ej. AIP) o cedidos de forma de forma grabada.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.5	El repositorio dispone y utiliza convenciones de nombres que generan identificadores únicos, persistentes y visibles para todos los objetos archivados (ej., AIPS)	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.6	Si los identificadores únicos están asociados con los SIP antes de la ingesta, el repositorio preserva los identificadores de forma que mantiene una asociación persistente con el objeto archivado resultante (ej., AIP)	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a

Sección	Gestión de Objetos Digitales (cont.)								
Aspecto	B2. Ingesta: creación del paquete de archivo (cont.)								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
B2.7	El repositorio demuestra que tiene acceso a herramientas y recursos necesarios para establecer el contexto de autoridad semántica o técnica de los objetos digitales que contiene (es decir, el acceso a la información adecuada representación internacional y los registros de formato).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.8	El repositorio registra / graba la Representación de la Información depositada (incluyendo formatos).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.9	El repositorio adquiere metadatos de preservación (ej. PDI) para sus contenidos de información asociados.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.10	Repositorio tiene un proceso documentado para las pruebas de comprensión de los contenidos de información y con lo que el contenido de la información hasta el nivel acordado de comprensibilidad.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.11	El repositorio verifica cada AIP para su integridad y exactitud en el punto en que se ha generado.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.12	El repositorio facilita un mecanismo independiente para auditar la integridad del contenido del repositorio.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B2.13	El repositorio tiene registros contemporáneos de las acciones y procesos de administración que son relevantes para la conservación (AIP creación).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
Aspecto	B3. Planificación de la preservación								
B3.1	El repositorio tiene documentadas las estrategias de preservación	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B3.2	El repositorio tiene mecanismos en plaza para notificar y monitorizar cuando la Representación de la Información (incluyendo los formatos) empieza a ser obsoleta o no está disponible nunca más.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B3.3	El repositorio tiene mecanismos para cambiar sus planes de preservación como resultado de sus actividades de monitorización.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B3.4	El repositorio puede facilitar evidencias de la efectividad de sus planes de preservación.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a

Sección	Gestión de Objetos Digitales (cont.)								
Aspecto	B4. Almacenamiento del archivo y preservación/mantenimiento de AIPs								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
B4.1	El repositorio emplea estrategias de preservación documentadas.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B4.2	El repositorio implementa/responde a estrategias para el almacenamiento de objetos archivables y migración.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B4.3	El repositorio preserva el Contenido de la Información (Content Information) de los objetos archivables (ej.: AIPs).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B4.4	El repositorio monitoriza activamente la integridad de los objetos de archivo (ej.; AIPs).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B4.5	El repositorio tiene registros actualizados de procesos y acciones de administración que son relevantes para la preservación (Almacenamiento de archivos).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
Aspecto	B5. Gestión de la información								
B5.1	El repositorio articula los requerimientos de metadatos mínimos para habilitar a la comunidad/es designada/s a descubrir e identificar material de interés.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B5.2	El repositorio captura o crea el mínimo de metadatos descriptivos y asegura que está asociado con los objetos archivados (ej.; AIPs).	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B5.3	El repositorio puede demostrar que la integridad referencial se ha creado entre todos los objetos archivados (ej.: AIPs) y la información descriptiva asociada	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B5.4	El repositorio puede demostrar que la integridad referencial se mantiene entre todos los objetos archivados (ej.: AIPs) y la información descriptiva asociada.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a

Sección	Gestión de Objetos Digitales (cont.)								
Aspecto	B6. Gestión del acceso								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
B6.1	El repositorio documenta y comunica a su comunidad/es designada/s que las opciones de acceso y entrega están disponibles.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B6.2	El repositorio tiene implementada una política para registrar todas las acciones de acceso (incluidas peticiones, pedidos, etc) que se encuentran en los requerimientos del repositorio y la información de los productores / depositores.	x	x	x	x	x	x	x	x
B6.3	El repositorio asegura que los acuerdos aplicables a las condiciones de acceso están adheridos.	x	x	x	x	x	x	x	x
B6.4	El repositorio tiene documentadas e implementadas políticas de acceso (normas de autorización, requisitos de autenticación) consistente con acuerdos de depósito para objetos almacenados.	x	x	x	x	x	x	x	x
B6.5	El repositorio accede al sistema de gestión que implementa completamente las políticas de acceso.	x	x	x	x	x	x	x	x
B6.6	El repositorio registra todos los accesos erróneos de gestión y el personal revisa los incidentes inapropiados "denial access".	x	x		x	x	x	x	
B6.7	El repositorio puede demostrar que el proceso que genera la petición de objetos digitales (ej., DIP) es completo en relación a la petición.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B6.8	El repositorio puede demostrar que el proceso que genera la petición de objeto digital (ej., DIP) es correcto en relación a la petición.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B6.9	El repositorio demuestra que todas las peticiones de acceso resultan en respuesta a la aceptación o rechazo.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
B6.10	El repositorio habilita la diseminación de copias de los objetos originales guardados.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a

Sección	C. Tecnologías, infraestructura técnica y seguridad								
Aspecto	C1. Sistema de infraestructuras								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
C1.1	El repositorio funciona en sistemas operativos bien soportados y otros núcleos de software de infraestructuras.	x	x				x		
C1.2	El repositorio se asegura de que tiene el hardware adecuado y soporte de software para la funcionalidad de copia de seguridad suficiente para los servicios del repositorio y de los datos que posee, por ejemplo, los metadatos asociados a los controles de acceso, el contenido del repositorio principal.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
C1.3	El repositorio gestiona el número y localización de copias de todos los objetos digitales.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
C1.4	El repositorio dispone de un mecanismo en plaza para asegurar que alguna / múltiples copias de objetos digitales están sincronizadas.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
C1.5	El repositorio dispone de mecanismos efectivos para detectar pérdidas o corrupción de bit.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
C1.6	El repositorio informa a su administración de todos los incidentes de corrupción de datos o pérdidas y los pasos que se deben tomar para reparar / reemplazar los datos corrompidos o perdidos.	n.a	n.a	n.a	n.a	n.a	n.a	n.a	n.a
C1.7	El repositorio ha definido procesos debido al cambio de medios de almacenamiento y / o hardware (ej. Refresco, migración).	x	x						
C1.8	El repositorio cuenta con un proceso de gestión de cambio documentado que identifica los cambios en los procesos críticos que potencialmente afectan la habilidad del repositorio para cumplir con sus responsabilidades obligatorias.		x						
C1.9	El repositorio cuenta con un proceso para evaluación de los efectos de los cambios críticos en el sistema.	x	x	x	x			x	
C1.10	El repositorio dispone de un proceso para reaccionar a la disponibilidad de una actualización de seguridad en el software basada en una evaluación riesgo-beneficio.		x			x			

Sección	C. Tecnologías, infraestructura técnica y seguridad (cont.)								
Aspecto	C2. Tecnologías apropiadas								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
C2.1	El repositorio dispone de tecnologías de hardware apropiadas a los servicios que facilita a su comunidad designada y dispone de procedimientos en plaza para recibir y monitorizar notificaciones, y evaluar cuando se necesita un cambio en la tecnología del hardware.	x	x	x	x	x	x	x	
C2.2	El repositorio dispone de tecnologías de software apropiadas a los servicios que facilita a su comunidad elegida y dispone de procedimientos en plaza para recibir y monitorizar notificaciones, y evaluar cuando se necesita un cambio en la tecnología del software.	x	x	x	x	x	x	x	x
Aspecto	C3. Seguridad								
C3.1	El repositorio mantiene un análisis sistemático de factores como datos, sistemas, personal, planta de ubicación física y necesidades de seguridad.	x	x		x		x	x	
C3.2	El repositorio ha implementado controles para controlar adecuadamente cada una de las necesidades de seguridad definidas.	x	x	x	x	x	x	x	x
C3.3	El personal del repositorio ha delimitado funciones, responsabilidades y autorizaciones relativas a los cambios de implementación dentro del sistema.	x				x			x
C3.4	El repositorio dispone un plan(es) escrito apropiado de recuperación y estado de preparación, incluyendo al menos una copia de seguridad fuera del lugar habitual (en otro edificio) de toda la información preservada junta con una copia del plan(es) de recuperación.	x	x	x	x	x	x	x	x

14.3 Exposición de resultados del Esquema Nacional de Seguridad

Uno de los aspectos a recalcar del análisis según el Esquema Nacional de Seguridad es respecto a la dimensión que se ha analizado. El Esquema Nacional de Seguridad establece las dimensiones Básica, Media y Alta. En el cuestionario se ha aplicado una dimensión básica. El análisis en las dimensiones Media y Alta hubiera exigido el uso de herramientas informáticas para el análisis y evaluación del sistema y que no formaban parte de su utilización en el estudio.

Aspecto	Marco Organizativo								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
org. 1	Política de seguridad	x	x	x	x	x	x	x	x
org. 2	Normativa de seguridad	x	x	x	x	x		x	x
org. 3	Procedimientos de seguridad		x			x	x	x	x
org. 4	Proceso de autorización	x	x		x	x	x	x	
aspecto	Marco Operacional								
op.pl	Planificación								
op.pl. 1	Análisis de riesgos							x	
op.pl. 2	Arquitectura de seguridad	x			x	x		x	x
op.pl. 3	Adquisición de nuevos componentes	x	x		x			x	
op.pl. 4	Dimensionamiento / Gestión de capacidades	x	x	x	x	x	x	x	x
op.pl. 5	Componentes certificados	x	x	x	x	x	x	x	x
op.acc	Control de acceso								
op.acc. 1	Identificación	x	x	x	x	x	x	x	x
op.acc. 2	Requisitos de acceso	x	x	x	x	x			
op.acc. 3	Segregación de funciones y tareas	x	x				x	x	
op.acc. 4	Proceso de gestión de derechos de acceso	x	x	x	x	x	x	x	x
op.acc. 5	Mecanismo de autenticación	x	x		x	x	x	x	x
op.acc. 6	Acceso local (local logon)	x	x	x	x		x	x	x
op.acc. 7	Acceso remoto (remote login)	x	x				x	x	

Aspecto	Marco Operacional								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
op.exp	Explotación								
op.exp. 1	Inventario de activos	x	x	x	x	x	x	x	x
op.exp. 2	Configuración de seguridad		x	x			x	x	
op.exp. 3	Gestión de la configuración		x			x			
op.exp. 4	Mantenimiento	x	x						
op.exp. 5	Gestión de cambios		x						
op.exp. 6	Protección frente a código dañino	x	x		x	x	x		
op.exp. 7	Gestión de incidencias		x		x				
op.exp. 8	Registro de la actividad de los usuarios	x	x		x	x	x		x
op.exp.9	Registros de la gestión de incidencias	x	x	x	x	x	x		x
op.exp. 10	Protección de los registros de actividad	x	x		x	x	x		x
op.exp. 11	Protección de claves criptográficas	x							
op.ext	Servicios externos								
op.ext. 1	Contratación y acuerdos de nivel de servicio	x	x	x	x	x	x	x	x
op.ext. 2	Gestión diaria	x	x	x	x	x	x	x	x
op.ext. 9	Medios alternativos	x	x			x	x	x	
op.cont	Continuidad del servicio								
op.cont. 1	Análisis de impacto		x						
op.cont. 2	Plan de continuidad	x	x						
op.cont. 3	Pruebas periódicas	x				x			
op.cont	Monitorización del sistema								
op.mon. 1	Detección de intrusión	x	x	x	x		x	x	
op.mon. 2	Sistema de métricas		x		x				

Aspecto	Medidas de protección								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
mp.if	Protección de las instalaciones e infraestructuras								
mp.if. 1	Áreas separadas y con control de acceso	x				x			x
mp.if. 2	Identificación de las personas	x			x	x	x	x	x
mp.if. 3	Acondicionamiento de los locales	x			x	x		x	x
mp.if. 4	Energía eléctrica	x	x	x	x	x	x	x	x
mp.if. 5	Protección frente a incendios	x	x	x	x	x	x	x	x
mp.if. 6	Protección frente a inundaciones	x					x	x	
mp.if. 7	Registro de entrada y salida de equipamiento	x	x						
mp.if. 9	Instalaciones alternativas								
mp.per	Gestión de personal								
mp.per. 1	Caracterización del puesto de trabajo							x	
mp.per. 2	Deberes y obligaciones	x	x		x		x	x	x
mp.per. 3	Concienciación	x	x	x	x	x	x	x	x
mp.per. 4	Formación	x						x	
mp.per. 9	Personal alternativo							x	
mp.eq	Protección de los equipos								
mp.eq. 1	Puesto de trabajo despejado	x				x		x	
mp.eq. 2	Bloqueo del puesto de trabajo	x	x		x	x	x	x	x
mp.eq. 3	Protección de los equipos portátiles	x	x	x	x	x	x	x	x
mp.eq. 9	Medios alternativos		x		x			x	x
mp.com	Protección de las comunicaciones								
mp.com. 1	Perímetro seguro	x	x		x	x		x	x
mp.com. 2	Protección de la confidencialidad	x	x		x	x	x	x	x
mp.com. 3	Protección de la autenticidad y de la integridad	x	x		x	x	x		
mp.com. 4	Segregación de redes	x	x	x		x		x	x
mp.com. 9	Medios alternativos	x	x	x	x			x	

Aspecto	Medidas de protección								
		ES1	ES2	ES3	ES4	ES5	ES6	ES7	ES8
mp.si	Protección de los soportes de información								
mp.si. 1	Etiquetado				x			x	
mp.si. 2	Criptografía							x	
mp.si. 3	Custodia				x	x	x	x	
mp.si. 4	Transporte	x			x	x	x	x	x
mp.si. 5	Borrado y destrucción				x	x	x	x	x
mp.sw	Protección de las aplicaciones informáticas								
mp.sw. 1	Desarrollo	x			x				
mp.sw. 2	Aceptación y puesta en servicio	x			x		x	x	
mp.info	Protección de la información								
mp.info. 1	Datos de carácter personal	x	x	x	x	x	x	x	x
mp.info. 2	Calificación de la información		x			x			
mp.info. 3	Cifrado	x			x	x		x	x
mp.info. 4	Firma electrónica	x	x			x	x		x
mp.info. 5	Sellos de tiempo					x			
mp.info. 6	Limpieza de documentos					x			x
mp.info. 9	Copias de seguridad (backup)	x	x		x	x	x	x	x
mp.s	Protección de los servicios								
mp.s. 1	Protección del correo electrónico								
mp.s. 2	Protección de servicios y aplicaciones web								
mp.s. 8	Protección frente a la denegación de servicio								
mp.s. 9	Medios alternativos								

Anexo V

Análisis de Riesgos versión larga

15 Anexo V

15.1 Análisis de riesgo versión larga

Modelo de valor

proyecto: [ESn - Version Final Genérica] Entidad Sanitaria Genérica

1. Datos del proyecto

ESn - Version Final Genérica	Entidad Sanitaria Genérica
Autor	Juan-José Boté
Versión	1
Fecha	11 de agosto de 2011
biblioteca	[std] Biblioteca INFOSEC (23.3.2011)

Descripción

Tesis doctoral

Licencia

ub /biblio /recerca
Facultat de Biblioteconomia i Documentació
Universitat de Barcelona
[... 31.12.2011]

2. Dimensiones

- [D] disponibilidad
- [I] integridad de los datos
- [C] confidencialidad de los datos
- [A] autenticidad de los usuarios y de la información
- [T] trazabilidad del servicio y de los datos

3. Dominios de seguridad

- [base] Base

4. Activos

4.1. Capa - [B] Capa de negocio

4.2. Capa - [IS] Servicios internos

4.3. Capa - [E] Equipamiento

[SW-ESn] Aplicaciones
[Desarrollo Propio-ESn] DP-ESn
[AplicacionesGeneral-ESn] AplicacionesGeneralESn
[GestorBaseDatos-ESn] GestorBaseDatos
[Antivirus-ESn] Antivirus
[Backup-ESn] Backup
[Almacenamiento-ESn] Almacenamiento
[SistemaOperativo-ESn] SistemaOperativo
[LOPD] LOPD-Alto
[HW-ESn] Equipos
[Servidor-ESn] ES-Servidor
[Terminales-ESn] ESn-Terminales
[PAC-ESn] PAC
[COM-ES] Comunicaciones
[RedLocal-LAN] RedLocal
[VPN] VPN /no existe /invisible
[AUX] Elementos auxiliares
[SAI] SistemasAlimentacionIninterrumpida-SAI
[USB] ConexionUSB
4.4. Capa - [SS] Servicios subcontratados

4.5. Capa - [L] Instalaciones

4.6. Capa - [P] Personal

[ES-PERSONAL] Personal
[PersonalG1] PersonalGrupo1
[PersonalG2] PersonalGrupo2
[PersonalG3] PersonalGrupo3
[PersonalG4] PersonalGrupo4
4.7. Resumen de valoración

[E] Equipamiento

activo	[D]	[I]	[C]	[A]	[T]
[SW-ESn.Desarrollo Propio-ESn] DP-ESn	220K(1)	2,2M(2)	2,2M(3)	2,2M(4)	470K(5)
[SW-ESn.AplicacionesGeneral-ESn] AplicacionesGeneralESn	4,7K(6)	4,7K(7)	2,2K(8)	4,7K(9)	1.000(10)
[SW-ESn.GestorBaseDatos-ESn] GestorBaseDatos	2,2M(11)	2,2M(12)	2,2M(13)	2,2M(14)	470K(15)
[SW-ESn.Antivirus-ESn] Antivirus	4,7K(16)	4,7K(17)	4,7K(18)	220K(19)	4,7K(20)
[SW-ESn.Backup-ESn] Backup	2,2M(21)	2,2M(22)	2,2M(23)	2,2M(24)	2,2M(25)
[SW-ESn.Almacenamiento-ESn] Almacenamiento	2,2M(26)	2,2M(27)	2,2M(28)	2,2M(29)	470K(30)

[SW-ESn.SistemaOperativo-ESn] SistemaOperativo	220K(31)	22K(32)	22K(33)	47K(34)	22K(35)
[SW-ESn.LOPD] LOPD-Alto	2,2M(36)	2,2M(37)	2,2M(38)	2,2M(39)	2,2M(40)
[HW-ESn.Servidor-ESn] ES-Servidor	2,2M(41)	2,2M(42)	2,2M(43)	2,2M(44)	2,2M(45)
[HW-ESn.Terminales-ESn] ESn-Terminales	220K(46)	470K(47)	2,2M(48)	2,2M(49)	220K(50)
[HW-ESn.PAC-ESn] PAC	4,7K(51)	470K(52)	470K(53)	470K(54)	470K(55)
[COM-ES.RedLocal-LAN] RedLocal	220K(56)	220K(57)	220K(58)	220K(59)	220K(60)
[AUX.SAI] SistemasAlimentacionIninterrumpida-SAI	1.000(61)	1.000(62)	1.000(63)	1.000(64)	1.000(65)
[AUX.USB] ConexionUSB	4,7K(66)	470K(67)	470K(68)	470K(69)	470K(70)

(1) [M-] Nivel medio-
[I.d.a.4] porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[I.d.m.rto] cuando el RTO se sitúa entre 4 horas y un día
[M] Medio (disponibilidad del servicio)
[S.d.m.rto] cuando el RTO se sitúa entre 4 horas y un día

(2) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[I.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

(3) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...

(4) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría

pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(5) [A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
[I.t.a.3] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave
[S.t.a.3] porque la incapacidad para rastrear un acceso al servicio o dificultaría notablemente la capacidad para perseguir delitos

(6) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(7) [B+] Nivel bajo+
[I.i.b.2] porque su manipulación o modificación no autorizada causaría algún perjuicio
[S.i.b.2] porque la manipulación o modificación no autorizada de la información que maneja causaría algún perjuicio

(8) [I.c.b.3] porque su revelación causaría algún perjuicio
[S.c.b.3] porque su revelación causaría algún perjuicio

(9) [B+] Nivel bajo+
[I.a.b.2] porque la falsedad en su origen o en su destinatario causaría algún perjuicio
[S.a.b.2] porque la falsedad en su origen o en su destinatario causaría algún perjuicio

(10) [I.t.n.1] cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
[I.t.n.2] cuando no se pueden perpetrar delitos relevante, o su investigación es fácilmente realizable por otros medios
[S.t.n.1] cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
[S.t.n.2] cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios

(11) [10] Nivel 10
[A-] Nivel alto-
[I.d.a.1] por imposición administrativa: ley, decreto, orden, reglamento, …
[I.d.a.2] porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible recuperación
[I.d.a.3] porque la indisponibilidad de la información supondría el incumplimiento grave de una norma

[I.d.a.4] porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[I.d.a.rto, 7.rto] cuando el RTO es inferior a 4 horas
[S.d.a.1] por imposición administrativa: ley, decreto, orden, reglamento, …
[S.d.a.2] porque la detención del servicio causaría un grave daño, de difícil o imposible recuperación
[S.d.a.3] porque la detención del servicio supondría el incumplimiento grave de una norma
[S.d.a.4] porque la detención del servicio causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.d.a.rto] cuando el RTO es inferior a 4 horas

(12) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[I.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

(13) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.c.a.4] porque su revelación supondría el incumplimiento grave de una norma
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.4] porque la revelación de la información que maneja supondría el incumplimiento grave de una norma

(14) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación

[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(15) [A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
[I.t.a.3] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave
[S.t.a.3] porque la incapacidad para rastrear un acceso al servicio o dificultaría notablemente la capacidad para perseguir delitos

(16) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(17) [B+] Nivel bajo+
[I.i.b.2] porque su manipulación o modificación no autorizada causaría algún perjuicio
[I.i.b.3] porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[S.i.b.2] porque la manipulación o modificación no autorizada de la información que maneja causaría algún perjuicio
[S.i.b.3] porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones

(18) [B+] Nivel bajo+
[I.c.b.3] porque su revelación causaría algún perjuicio
[S.c.b.3] porque su revelación causaría algún perjuicio

(19) [I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación

(20) [B+] Nivel bajo+
[I.t.b.2] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[S.t.b.2] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

(21) [10] Nivel 10
[A+] Nivel alto+
[I.d.a.2] porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible recuperación
[I.d.a.3] porque la indisponibilidad de la información supondría el incumplimiento grave de una norma
[S.d.a.2] porque la detención del servicio causaría un grave daño, de difícil o imposible recuperación
[S.d.a.3] porque la detención del servicio supondría el incumplimiento

grave de una norma

(22) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas

(23) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.c.a.3] porque su revelación causaría un grave daño, de difícil o imposible recuperación
[I.c.a.4] porque su revelación supondría el incumplimiento grave de una norma
[I.c.a.5] porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.3] porque la revelación de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.c.a.4] porque la revelación de la información que maneja supondría el incumplimiento grave de una norma
[S.c.a.5] porque la revelación de la información que maneja causaría pérdidas económicas elevadas o alteraciones financieras significativas

(24) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(25) [10] Nivel 10
[A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error

grave
[I.t.a.3] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave
[S.t.a.3] porque la incapacidad para rastrear un acceso al servicio o dificultaría notablemente la capacidad para perseguir delitos

(26) [10] Nivel 10
[A+] Nivel alto+

(27) [10] Nivel 10
[A+] Nivel alto+

(28) [10] Nivel 10
[A+] Nivel alto+

(29) [10] Nivel 10
[A+] Nivel alto+

(30) [A+] Nivel alto+

(31) [A-] Nivel alto-
[I.d.a.rto, 7.rto] cuando el RTO es inferior a 4 horas
[S.d.a.rto] cuando el RTO es inferior a 4 horas

(32) [M-] Nivel medio-
[I.i.m.2] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
[S.i.m.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un daño importante aunque subsanable

(33) [M-] Nivel medio-
[I.c.m.3] porque su revelación causaría un daño importante aunque subsanable
[S.c.m.3] porque la revelación de la información que maneja causaría un daño importante aunque subsanable

(34) [M+] Nivel medio+
[I.a.m.2] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[S.a.m.2] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable

(35) [I.t.m.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error importante
[S.t.m.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante
[I.t.b.2] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[S.t.b.2] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

(36) [10] Nivel 10
[A+] Nivel alto+

(37) [10] Nivel 10

[A+] Nivel alto+

(38) [10] Nivel 10
[A+] Nivel alto+

(39) [10] Nivel 10
[A+] Nivel alto+

(40) [10] Nivel 10
[A+] Nivel alto+

(41) [10] Nivel 10
[I.d.a.4] porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[I.d.a.5] porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración seria del orden público)
[S.d.a.4] porque la detención del servicio causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.d.a.5] porque la detención del servicio podría desembocar en protestas masivas (alteración seria del orden público)

(42) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas

(43) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.c.a.4] porque su revelación supondría el incumplimiento grave de una norma
[I.c.a.5] porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.3] porque la revelación de la información que maneja causaría un grave daño, de difícil o imposible recuperación

(44) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.1] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

[S.a.a.1] por imposición administrativa: ley, decreto, orden, reglamento, …
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(45) [10] Nivel 10
[A+] Nivel alto+

(46) [B+] Nivel bajo+
[I.d.a.rto, 7.rto] cuando el RTO es inferior a 4 horas
[S.d.a.rto] cuando el RTO es inferior a 4 horas

(47) [A+] Nivel alto+
[A] Alto (integridad de la información)
[A] Alto (integridad de [la información que maneja] el servicio)

(48) [10] Nivel 10
[A+] Nivel alto+
[A] Alto (confidencialidad de la información)
[A] Alto (confidencialidad de [la información que maneja] el servicio)

(49) [10] Nivel 10
[A+] Nivel alto+
[A] Alto (autenticidad de la información)
[A] Alto (autenticidad del servicio)

(50) [A-] Nivel alto-
[A] Alto (trazabilidad de la información)
[A] Alto (trazabilidad del servicio)

(51) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(52) [A+] Nivel alto+

(53) [A+] Nivel alto+

(54) [A+] Nivel alto+

(55) [A+] Nivel alto+

(56) [A] Alto (disponibilidad de la información)
[A] Alto (disponibilidad del servicio)

(57) [A] Alto (integridad de la información)
[A] Alto (integridad de [la información que maneja] el servicio)

(58) [A] Alto (confidencialidad de la información)
[A] Alto (confidencialidad de [la información que maneja] el servicio)

(59) [A] Alto (autenticidad de la información)
[A] Alto (autenticidad del servicio)

(60) [A] Alto (trazabilidad de la información)
[A] Alto (trazabilidad del servicio)

(61) [S] Sin valorar (disponibilidad de la información)
[S] Sin valorar (disponibilidad del servicio)

(62) [S] Sin valorar (integridad de la información)
[S] Sin valorar (integridad de [la información que maneja] el servicio)

(63) [S] Sin valorar (confidencialidad de la información)
[S] Sin valorar (confidencialidad de [la información que maneja] el servicio)
(64) [S] Sin valorar (autenticidad de la información)
[S] Sin valorar (autenticidad del servicio)
(65) [S] Sin valorar (trazabilidad de la información)
[S] Sin valorar (trazabilidad del servicio)
(66) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio
(67) [A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
(68) [A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
(69) [A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
(70) [A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave

[P] Personal

activo	[D]	[I]	[C]	[A]	[T]
[ES-PERSONAL.PersonalG1] PersonalGrupo1	220K(1)	220K(2)	470K(3)	470K(4)	470K(5)
[ES-PERSONAL.PersonalG2]	22K(6)	22K(7)	100K(8)	47K(9)	470K(10)

PersonalGrupo2					
[ES-PERSONAL.PersonalG3] PersonalGrupo3	2,2K(11)	2,2K(12)	22K(13)	10K(14)	470K(15)
[ES-PERSONAL.PersonalG4] PersonalGrupo4	2,2K(16)	1.000(17)	2,2K(18)	4,7K(19)	470K(20)

(1) [I.d.a.2] porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible recuperación
[I.d.a.3] porque la indisponibilidad de la información supondría el incumplimiento grave de una norma
[S.d.a.2] porque la detención del servicio causaría un grave daño, de difícil o imposible recuperación
[S.d.a.3] porque la detención del servicio supondría el incumplimiento grave de una norma

(2) [I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación

(3) [A+] Nivel alto+
[A] Alto (confidencialidad de la información)

(4) [A+] Nivel alto+

(5) [A+] Nivel alto+

(6) [I.d.m.2] porque la indisponibilidad de la información causaría un daño importante aunque subsanable
[I.d.m.3] porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma
[S.d.m.2] porque la detención del servicio causaría un daño importante aunque subsanable
[S.d.m.3] porque la detención del servicio supondría el incumplimiento material o formal de una norma

(7) [I.i.m.2] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
[I.i.m.3] porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma
[S.i.m.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un daño importante aunque subsanable
[S.i.m.3] porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma

(8) [A-] Nivel alto-

(9) [M+] Nivel medio+

(10) [A+] Nivel alto+

(11) [I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[I.d.b.3] porque la indisponibilidad de la información supondría el

incumplimiento leve de una norma
[S.d.b.2] porque la detención del servicio causaría algún perjuicio
[S.d.b.3] porque la detención del servicio supondría el incumplimiento leve de una norma

(12) [I.i.b.2] porque su manipulación o modificación no autorizada causaría algún perjuicio
[I.i.b.3] porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[S.i.b.2] porque la manipulación o modificación no autorizada de la información que maneja causaría algún perjuicio
[S.i.b.3] porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones

(13) [M] Medio (confidencialidad de la información)
[M] Medio (confidencialidad de [la información que maneja] el servicio)

(14) [M-] Nivel medio-

(15) [A+] Nivel alto+

(16) [I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[I.d.b.3] porque la indisponibilidad de la información supondría el incumplimiento leve de una norma
[S.d.b.2] porque la detención del servicio causaría algún perjuicio
[S.d.b.3] porque la detención del servicio supondría el incumplimiento leve de una norma

(17) [I.i.n.1] cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables
[S.i.n.1] cuando los errores en la información que maneja carecen de consecuencias o son fácil y rápidamente reparables

(18) [B] Bajo (confidencialidad de la información)
[B] Bajo (confidencialidad de [la información que maneja] el servicio)

(19) [B+] Nivel bajo+

(20) [A+] Nivel alto+

5. Activos

5.1. [SW-ESn.Desarrollo Propio-ESn] DP-ESn

- [D] Datos / Información
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [HW] Equipamiento informático (hardware)

Dominio de seguridad

- [base] Base

Datos

responsable	yo

Superiores (activos que dependen de este)

- [SW-ESn.Antivirus-ESn] Antivirus
- [HW-ESn.Terminales-ESn] ESn-Terminales (C:100%)

Inferiores (activos de los que depende este)

- [SW-ESn.LOPD] LOPD-Alto

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	220K(1)	7,3M
[I] integridad de los datos	2,2M(2)	9,1M
[C] confidencialidad de los datos	2,2M(3)	11,6M
[A] autenticidad de los usuarios y de la información	2,2M(4)	9,6M
[T] trazabilidad del servicio y de los datos	470K(5)	7,3M

(1) [M-] Nivel medio-
[I.d.a.4] porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[I.d.m.rto] cuando el RTO se sitúa entre 4 horas y un día
[M] Medio (disponibilidad del servicio)
[S.d.m.rto] cuando el RTO se sitúa entre 4 horas y un día

(2) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[I.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

(3) [10] Nivel 10
[A+] Nivel alto+

[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...

(4) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(5) [A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
[I.t.a.3] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave
[S.t.a.3] porque la incapacidad para rastrear un acceso al servicio o dificultaría notablemente la capacidad para perseguir delitos

5.2. [SW-ESn.AplicacionesGeneral-ESn] AplicacionesGeneralESn

- [D] Datos / Información
- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.browser] navegador web
- [SW.std.file] servidor de ficheros
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.av] anti virus
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows
- [SW.std.os.linux] linux
- [SW.std.backup] aplicación de backup
- [HW] Equipamiento informático (hardware)

Dominio de seguridad

- [base] Base

Datos

responsable	yo

Superiores (activos que dependen de este)

- [SW-ESn.Antivirus-ESn] Antivirus
- [HW-ESn.Terminales-ESn] ESn-Terminales

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	4,7K(1)	7,3M
[I] integridad de los datos	4,7K(2)	7,4M
[C] confidencialidad de los datos	2,2K(3)	9,4M
[A] autenticidad de los usuarios y de la información	4,7K(4)	9,6M
[T] trazabilidad del servicio y de los datos	1.000(5)	7,1M

(1) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(2) [B+] Nivel bajo+
[I.i.b.2] porque su manipulación o modificación no autorizada causaría algún perjuicio
[S.i.b.2] porque la manipulación o modificación no autorizada de la información que maneja causaría algún perjuicio

(3) [I.c.b.3] porque su revelación causaría algún perjuicio
[S.c.b.3] porque su revelación causaría algún perjuicio

(4) [B+] Nivel bajo+
[I.a.b.2] porque la falsedad en su origen o en su destinatario causaría algún perjuicio
[S.a.b.2] porque la falsedad en su origen o en su destinatario causaría algún perjuicio

(5) [I.t.n.1] cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
[I.t.n.2] cuando no se pueden perpetrar delitos relevante, o su investigación es fácilmente realizable por otros medios
[S.t.n.1] cuando no se pueden producir errores de importancia, o son fácilmente reparables por otros medios
[S.t.n.2] cuando no se pueden perpetrar delitos relevantes, o su investigación es fácilmente realizable por otros medios

5.3. [SW-ESn.GestorBaseDatos-ESn] GestorBaseDatos

- [D] Datos / Información
- [D.biz] datos de interés para el negocio
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto

- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] Base

Datos

responsable	Director IT

Superiores (activos que dependen de este)

- [SW-ESn.Antivirus-ESn] Antivirus

Inferiores (activos de los que depende este)

- [SW-ESn.LOPD] LOPD-Alto

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	2,2M(1)	9,3M
[I] integridad de los datos	2,2M(2)	9,1M
[C] confidencialidad de los datos	2,2M(3)	9,4M
[A] autenticidad de los usuarios y de la información	2,2M(4)	9,6M
[T] trazabilidad del servicio y de los datos	470K(5)	7,3M

(1) [10] Nivel 10
[A-] Nivel alto-
[I.d.a.1] por imposición administrativa: ley, decreto, orden, reglamento, …
[I.d.a.2] porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible recuperación
[I.d.a.3] porque la indisponibilidad de la información supondría el incumplimiento grave de una norma
[I.d.a.4] porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[I.d.a.rto, 7.rto] cuando el RTO es inferior a 4 horas
[S.d.a.1] por imposición administrativa: ley, decreto, orden, reglamento, …
[S.d.a.2] porque la detención del servicio causaría un grave daño, de difícil o imposible recuperación
[S.d.a.3] porque la detención del servicio supondría el incumplimiento grave de una norma
[S.d.a.4] porque la detención del servicio causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

[S.d.a.rto] cuando el RTO es inferior a 4 horas

(2) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[I.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.4] porque su manipulación o alteración no autorizada causaría un daño reputacional grave con los ciudadanos o con otras organizaciones

(3) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.c.a.4] porque su revelación supondría el incumplimiento grave de una norma
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.4] porque la revelación de la información que maneja supondría el incumplimiento grave de una norma

(4) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(5) [A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
[I.t.a.3] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave

[S.t.a.3] porque la incapacidad para rastrear un acceso al servicio o dificultaría notablemente la capacidad para perseguir delitos

5.4. [SW-ESn.Antivirus-ESn] Antivirus

- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.av] anti virus
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] Base

Datos

responsable	Director IT

Superiores (activos que dependen de este)

- [SW-ESn.SistemaOperativo-ESn] SistemaOperativo

Inferiores (activos de los que depende este)

- [SW-ESn.Desarrollo Propio-ESn] DP-ESn
- [SW-ESn.AplicacionesGeneral-ESn] AplicacionesGeneralESn
- [SW-ESn.GestorBaseDatos-ESn] GestorBaseDatos

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	4,7K(1)	7,1M
[I] integridad de los datos	4,7K(2)	6,9M
[C] confidencialidad de los datos	4,7K(3)	7,3M
[A] autenticidad de los usuarios y de la información	220K(4)	7,5M
[T] trazabilidad del servicio y de los datos	4,7K(5)	6,9M

(1) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(2) [B+] Nivel bajo+
[I.i.b.2] porque su manipulación o modificación no autorizada causaría algún perjuicio
[I.i.b.3] porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[S.i.b.2] porque la manipulación o modificación no autorizada de la

información que maneja causaría algún perjuicio
[S.i.b.3] porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones

(3) [B+] Nivel bajo+
[I.c.b.3] porque su revelación causaría algún perjuicio
[S.c.b.3] porque su revelación causaría algún perjuicio

(4) [I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación

(5) [B+] Nivel bajo+
[I.t.b.2] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[S.t.b.2] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

5.5. [SW-ESn.Backup-ESn] Backup

- [D] Datos / Información
- [D.vr] datos vitales (registros de la organización)
- [D.password] credenciales (ej. contraseñas)
- [D.auth] datos de validación de credenciales
- [D.acl] datos de control de acceso
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [S] Servicios
- [S.backup] servicio de copias de respaldo (backup)
- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] Base

Datos

responsable	Director IT

Inferiores (activos de los que depende este)

- [SW-ESn.SistemaOperativo-ESn] SistemaOperativo

Valor

dimensión	***valor***	***valores acumulados***

[D] disponibilidad	2,2M(1)	2,2M
[I] integridad de los datos	2,2M(2)	2,2M
[C] confidencialidad de los datos	2,2M(3)	2,2M
[A] autenticidad de los usuarios y de la información	2,2M(4)	2,2M
[T] trazabilidad del servicio y de los datos	2,2M(5)	2,2M

(1) [10] Nivel 10
[A+] Nivel alto+
[I.d.a.2] porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible recuperación
[I.d.a.3] porque la indisponibilidad de la información supondría el incumplimiento grave de una norma
[S.d.a.2] porque la detención del servicio causaría un grave daño, de difícil o imposible recuperación
[S.d.a.3] porque la detención del servicio supondría el incumplimiento grave de una norma

(2) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas

(3) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.c.a.3] porque su revelación causaría un grave daño, de difícil o imposible recuperación
[I.c.a.4] porque su revelación supondría el incumplimiento grave de una norma
[I.c.a.5] porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.3] porque la revelación de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.c.a.4] porque la revelación de la información que maneja supondría el incumplimiento grave de una norma

[S.c.a.5] porque la revelación de la información que maneja causaría pérdidas económicas elevadas o alteraciones financieras significativas

(4) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(5) [10] Nivel 10
[A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave
[I.t.a.3] porque la incapacidad para rastrear un acceso a la información dificultaría notablemente la capacidad para perseguir delitos
[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave
[S.t.a.3] porque la incapacidad para rastrear un acceso al servicio o dificultaría notablemente la capacidad para perseguir delitos

5.6. [SW-ESn.Almacenamiento-ESn] Almacenamiento

- [D] Datos / Información
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [S] Servicios
- [S.file] almacenamiento de ficheros
- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] Base

Datos

responsable	Director IT

Inferiores (activos de los que depende este)

- [SW-ESn.SistemaOperativo-ESn] SistemaOperativo

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	2,2M(1)	2,2M
[I] integridad de los datos	2,2M(2)	2,2M
[C] confidencialidad de los datos	2,2M(3)	2,2M
[A] autenticidad de los usuarios y de la información	2,2M(4)	2,2M
[T] trazabilidad del servicio y de los datos	470K(5)	470K

(1) [10] Nivel 10
[A+] Nivel alto+
(2) [10] Nivel 10
[A+] Nivel alto+
(3) [10] Nivel 10
[A+] Nivel alto+
(4) [10] Nivel 10
[A+] Nivel alto+
(5) [A+] Nivel alto+

5.7. [SW-ESn.SistemaOperativo-ESn] SistemaOperativo

- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] Base

Datos

responsable	DirectorIT

Superiores (activos que dependen de este)

- [SW-ESn.Backup-ESn] Backup
- [SW-ESn.Almacenamiento-ESn] Almacenamiento
- [HW-ESn.Servidor-ESn] ES-Servidor

Inferiores (activos de los que depende este)

- [SW-ESn.Antivirus-ESn] Antivirus

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	220K(1)	7,1M

[I] integridad de los datos	22K(2)	6,9M
[C] confidencialidad de los datos	22K(3)	7,3M
[A] autenticidad de los usuarios y de la información	47K(4)	7,2M
[T] trazabilidad del servicio y de los datos	22K(5)	6,9M

(1) [A-] Nivel alto-
[I.d.a.rto, 7.rto] cuando el RTO es inferior a 4 horas
[S.d.a.rto] cuando el RTO es inferior a 4 horas

(2) [M-] Nivel medio-
[I.i.m.2] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
[S.i.m.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un daño importante aunque subsanable

(3) [M-] Nivel medio-
[I.c.m.3] porque su revelación causaría un daño importante aunque subsanable
[S.c.m.3] porque la revelación de la información que maneja causaría un daño importante aunque subsanable

(4) [M+] Nivel medio+
[I.a.m.2] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable
[S.a.m.2] porque la falsedad en su origen o en su destinatario causaría un daño importante aunque subsanable

(5) [I.t.m.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error importante
[S.t.m.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error importante
[I.t.b.2] porque la incapacidad para rastrear un acceso a la información dificultaría la capacidad de subsanar errores
[S.t.b.2] porque la incapacidad para rastrear un acceso al servicio dificultaría la capacidad de subsanar errores

5.8. [SW-ESn.LOPD] LOPD-Alto

- [D] Datos / Información
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [SW] Aplicaciones (software)
- [SW.prp] desarrollo propio (in house)
- [SW.std] estándar (off the shelf)
- [SW.std.dbms] sistema de gestión de bases de datos
- [SW.std.os] sistema operativo
- [SW.std.os.windows] windows

Dominio de seguridad

- [base] Base

Superiores (activos que dependen de este)

- [SW-ESn.Desarrollo Propio-ESn] DP-ESn
- [SW-ESn.GestorBaseDatos-ESn] GestorBaseDatos
- [AUX.USB] ConexionUSB

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	2,2M(1)	11,9M
[I] integridad de los datos	2,2M(2)	14,3M
[C] confidencialidad de los datos	2,2M(3)	16,3M
[A] autenticidad de los usuarios y de la información	2,2M(4)	16,5M
[T] trazabilidad del servicio y de los datos	2,2M(5)	10,6M

(1) [10] Nivel 10
[A+] Nivel alto+
(2) [10] Nivel 10
[A+] Nivel alto+
(3) [10] Nivel 10
[A+] Nivel alto+
(4) [10] Nivel 10
[A+] Nivel alto+
(5) [10] Nivel 10
[A+] Nivel alto+

5.9. [HW-ESn.Servidor-ESn] ES-Servidor

- [essential] Activos esenciales
- [D] Datos / Información
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [S] Servicios
- [S.file] almacenamiento de ficheros
- [S.ftp] transferencia de ficheros
- [SW] Aplicaciones (software)
- [HW] Equipamiento informático (hardware)
- [HW.host] grandes equipos (host)
- [HW.mid] equipos medios
- [HW.pc] informática personal
- [HW.vhost] equipos virtuales
- [HW.cluster] cluster
- [HW.data] que almacena datos
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión

- [COM] Redes de comunicaciones
- [COM.LAN] red local
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Base

Datos

responsable	yo
cantidad	7

Superiores (activos que dependen de este)

- [COM-ES.RedLocal-LAN] RedLocal
- [AUX.SAI] SistemasAlimentacionIninterrumpida-SAI
- [ES-PERSONAL.PersonalG1] PersonalGrupo1
- [ES-PERSONAL.PersonalG2] PersonalGrupo2
- [ES-PERSONAL.PersonalG3] PersonalGrupo3
- [ES-PERSONAL.PersonalG4] PersonalGrupo4

Inferiores (activos de los que depende este)

- [SW-ESn.SistemaOperativo-ESn] SistemaOperativo
- [HW-ESn.Terminales-ESn] ESn-Terminales
- [HW-ESn.PAC-ESn] PAC

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	2,2M(1)	2,6M
[I] integridad de los datos	2,2M(2)	2,6M
[C] confidencialidad de los datos	2,2M(3)	3M
[A] autenticidad de los usuarios y de la información	2,2M(4)	2,9M
[T] trazabilidad del servicio y de los datos	2,2M(5)	4,2M

(1) [10] Nivel 10
[I.d.a.4] porque la indisponibilidad de la información causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[I.d.a.5] porque la indisponibilidad de la información podría desembocar en protestas masivas (alteración seria del orden público)
[S.d.a.4] porque la detención del servicio causaría un daño reputacional grave con los ciudadanos o con otras organizaciones
[S.d.a.5] porque la detención del servicio podría desembocar en protestas masivas (alteración seria del orden público)

(2) [10] Nivel 10
[A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un

grave daño, de difícil o imposible recuperación
[I.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación
[S.i.a.3] porque su manipulación o alteración no autorizada causaría pérdidas económicas elevadas o alteraciones financieras significativas

(3) [10] Nivel 10
[A+] Nivel alto+
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.c.a.4] porque su revelación supondría el incumplimiento grave de una norma
[I.c.a.5] porque su revelación causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.3] porque la revelación de la información que maneja causaría un grave daño, de difícil o imposible recuperación

(4) [10] Nivel 10
[A+] Nivel alto+
[I.a.a.1] por imposición administrativa: ley, decreto, orden, reglamento, ...
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.1] por imposición administrativa: ley, decreto, orden, reglamento, …
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(5) [10] Nivel 10
[A+] Nivel alto+

5.10. [HW-ESn.Terminales-ESn] ESn-Terminales

- [essential] Activos esenciales
- [SW] Aplicaciones (software)
- [HW] Equipamiento informático (hardware)
- [HW.host] grandes equipos (host)
- [HW.mid] equipos medios
- [HW.pc] informática personal
- [HW.vhost] equipos virtuales
- [HW.cluster] cluster
- [HW.backup] equipamiento de respaldo

- [HW.data] que almacena datos
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión
- [COM] Redes de comunicaciones
- [COM.LAN] red local
- [COM.vpn] red privada virtual

Dominio de seguridad

- [base] Base

Datos

cantidad	700

Superiores (activos que dependen de este)

- [HW-ESn.Servidor-ESn] ES-Servidor
- [ES-PERSONAL.PersonalG1] PersonalGrupo1
- [ES-PERSONAL.PersonalG2] PersonalGrupo2
- [ES-PERSONAL.PersonalG3] PersonalGrupo3
- [ES-PERSONAL.PersonalG4] PersonalGrupo4

Inferiores (activos de los que depende este)

- [SW-ESn.Desarrollo Propio-ESn] DP-ESn (C:100%)
- [SW-ESn.AplicacionesGeneral-ESn] AplicacionesGeneralESn
- [AUX.USB] ConexionUSB

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	220K(1)	2,8M
[I] integridad de los datos	470K(2)	3,1M
[C] confidencialidad de los datos	2,2M(3)	5,1M
[A] autenticidad de los usuarios y de la información	2,2M(4)	5M
[T] trazabilidad del servicio y de los datos	220K(5)	4,4M

(1) [B+] Nivel bajo+
[I.d.a.rto, 7.rto] cuando el RTO es inferior a 4 horas
[S.d.a.rto] cuando el RTO es inferior a 4 horas

(2) [A+] Nivel alto+
[A] Alto (integridad de la información)
[A] Alto (integridad de [la información que maneja] el servicio)

(3) [10] Nivel 10
[A+] Nivel alto+
[A] Alto (confidencialidad de la información)
[A] Alto (confidencialidad de [la información que maneja] el servicio)

(4) [10] Nivel 10

[A+] Nivel alto+
[A] Alto (autenticidad de la información)
[A] Alto (autenticidad del servicio)

(5) [A-] Nivel alto-
[A] Alto (trazabilidad de la información)
[A] Alto (trazabilidad del servicio)

5.11. [HW-ESn.PAC-ESn] PAC

- [D] Datos / Información
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [HW] Equipamiento informático (hardware)
- [HW.host] grandes equipos (host)
- [HW.mid] equipos medios
- [HW.pc] informática personal
- [HW.vhost] equipos virtuales
- [HW.cluster] cluster
- [HW.data] que almacena datos
- [HW.peripheral] periféricos
- [HW.peripheral.print] medios de impresión

Dominio de seguridad

- [base] Base

Superiores (activos que dependen de este)

- [HW-ESn.Servidor-ESn] ES-Servidor

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	4,7K(1)	2,6M
[I] integridad de los datos	470K(2)	3,1M
[C] confidencialidad de los datos	470K(3)	3,4M
[A] autenticidad de los usuarios y de la información	470K(4)	3,4M
[T] trazabilidad del servicio y de los datos	470K(5)	4,7M

(1) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(2) [A+] Nivel alto+

(3) [A+] Nivel alto+

(4) [A+] Nivel alto+

(5) [A+] Nivel alto+

5.12. [COM-ES.RedLocal-LAN] RedLocal

- [D] Datos / Información
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [COM] Redes de comunicaciones
- [COM.ADSL] ADSL
- [COM.wifi] WiFi
- [COM.LAN] red local
- [COM.vpn] red privada virtual
- [COM.backup] comunicaciones de respaldo

Dominio de seguridad

- [base] Base

Inferiores (activos de los que depende este)

- [HW-ESn.Servidor-ESn] ES-Servidor

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	220K(1)	220K
[I] integridad de los datos	220K(2)	220K
[C] confidencialidad de los datos	220K(3)	220K
[A] autenticidad de los usuarios y de la información	220K(4)	220K
[T] trazabilidad del servicio y de los datos	220K(5)	220K

(1) [A] Alto (disponibilidad de la información)
[A] Alto (disponibilidad del servicio)
(2) [A] Alto (integridad de la información)
[A] Alto (integridad de [la información que maneja] el servicio)
(3) [A] Alto (confidencialidad de la información)
[A] Alto (confidencialidad de [la información que maneja] el servicio)
(4) [A] Alto (autenticidad de la información)
[A] Alto (autenticidad del servicio)
(5) [A] Alto (trazabilidad de la información)
[A] Alto (trazabilidad del servicio)

5.13. [AUX.SAI] SistemasAlimentacionIninterrumpida-SAI

- [AUX] Equipamiento auxiliar
- [AUX.power] fuentes de alimentación
- [AUX.ups] sai - sistemas de alimentación ininterrumpida
- [AUX.supply] suministros esenciales

Dominio de seguridad

- [base] Base

Datos

responsable	YO
cantidad	1

Inferiores (activos de los que depende este)

- [HW-ESn.Servidor-ESn] ES-Servidor

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	1.000(1)	1.000
[I] integridad de los datos	1.000(2)	1.000
[C] confidencialidad de los datos	1.000(3)	1.000
[A] autenticidad de los usuarios y de la información	1.000(4)	1.000
[T] trazabilidad del servicio y de los datos	1.000(5)	1.000

(1) [S] Sin valorar (disponibilidad de la información)
[S] Sin valorar (disponibilidad del servicio)
(2) [S] Sin valorar (integridad de la información)
[S] Sin valorar (integridad de [la información que maneja] el servicio)
(3) [S] Sin valorar (confidencialidad de la información)
[S] Sin valorar (confidencialidad de [la información que maneja] el servicio)
(4) [S] Sin valorar (autenticidad de la información)
[S] Sin valorar (autenticidad del servicio)
(5) [S] Sin valorar (trazabilidad de la información)
[S] Sin valorar (trazabilidad del servicio)

5.14. [AUX.USB] ConexionUSB

- [Media] Soportes de información
- [Media.electronic] electrónicos
- [Media.electronic.usb] memorias USB
- [AUX] Equipamiento auxiliar
- [AUX.power] fuentes de alimentación
- [AUX.ups] sai - sistemas de alimentación ininterrumpida
- [AUX.supply] suministros esenciales

Dominio de seguridad

- [base] Base

Superiores (activos que dependen de este)

- [HW-ESn.Terminales-ESn] ESn-Terminales
- [ES-PERSONAL.PersonalG1] PersonalGrupo1

- [ES-PERSONAL.PersonalG2] PersonalGrupo2
- [ES-PERSONAL.PersonalG3] PersonalGrupo3
- [ES-PERSONAL.PersonalG4] PersonalGrupo4

Inferiores (activos de los que depende este)

- [SW-ESn.LOPD] LOPD-Alto

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	4,7K(1)	2,8M
[I] integridad de los datos	470K(2)	3,5M
[C] confidencialidad de los datos	470K(3)	5,6M
[A] autenticidad de los usuarios y de la información	470K(4)	5,5M
[T] trazabilidad del servicio y de los datos	470K(5)	4,9M

(1) [B+] Nivel bajo+
[I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[S.d.b.2] porque la detención del servicio causaría algún perjuicio

(2) [A+] Nivel alto+
[I.i.a.2] porque su manipulación o modificación no autorizada causaría un grave daño, de difícil o imposible recuperación
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación

(3) [A+] Nivel alto+
[I.c.a.1] porque la información deben conocerla un número muy reducido de personas
[I.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...
[S.c.a.1] porque la información que maneja deben conocerla un número muy reducido de personas
[S.c.a.2] por imposición administrativa: ley, decreto, orden, reglamento, ...

(4) [A+] Nivel alto+
[I.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[I.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas
[S.a.a.2] porque la falsedad en su origen o en su destinatario causaría un grave daño, de difícil o imposible recuperación
[S.a.a.3] porque la falsedad en su origen o en su destinatario causaría pérdidas económicas elevadas o alteraciones financieras significativas

(5) [A+] Nivel alto+
[I.t.a.2] porque la incapacidad para rastrear un acceso a la información impediría o dificultaría notablemente la capacidad de subsanar un error grave

[S.t.a.2] porque la incapacidad para rastrear un acceso al servicio impediría o dificultaría notablemente la capacidad de subsanar un error grave

5.15. [ES-PERSONAL.PersonalG1] PersonalGrupo1

- [essential] Activos esenciales
- [D] Datos / Información
- [D.biz] datos de interés para el negocio
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [P] Personal
- [P.ui] usuarios internos
- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.des] desarrolladores / programadores

Dominio de seguridad

- [base] Base

Datos

responsable	DirectorIT

Inferiores (activos de los que depende este)

- [HW-ESn.Servidor-ESn] ES-Servidor
- [HW-ESn.Terminales-ESn] ESn-Terminales
- [AUX.USB] ConexionUSB

Valor

dimensión	***valor***	***valores acumulados***
[D] disponibilidad	220K(1)	220K
[I] integridad de los datos	220K(2)	220K
[C] confidencialidad de los datos	470K(3)	470K
[A] autenticidad de los usuarios y de la información	470K(4)	470K
[T] trazabilidad del servicio y de los datos	470K(5)	470K

(1) [I.d.a.2] porque la indisponibilidad de la información causaría un grave daño, de difícil o imposible recuperación
[I.d.a.3] porque la indisponibilidad de la información supondría el incumplimiento grave de una norma
[S.d.a.2] porque la detención del servicio causaría un grave daño, de difícil o imposible recuperación
[S.d.a.3] porque la detención del servicio supondría el incumplimiento grave de una norma

(2) [I.i.a.2] porque su manipulación o modificación no autorizada causaría un

grave daño, de difícil o imposible recuperación
[S.i.a.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un grave daño, de difícil o imposible recuperación

(3) [A+] Nivel alto+
[A] Alto (confidencialidad de la información)

(4) [A+] Nivel alto+

(5) [A+] Nivel alto+

5.16. [ES-PERSONAL.PersonalG2] PersonalGrupo2

- [essential] Activos esenciales
- [D] Datos / Información
- [D.biz] datos de interés para el negocio
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [P] Personal
- [P.ui] usuarios internos
- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.des] desarrolladores / programadores

Dominio de seguridad

- [base] Base

Datos

Inferiores (activos de los que depende este)

- [HW-ESn.Servidor-ESn] ES-Servidor
- [HW-ESn.Terminales-ESn] ESn-Terminales
- [AUX.USB] ConexionUSB

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	22K(1)	22K
[I] integridad de los datos	22K(2)	22K
[C] confidencialidad de los datos	100K(3)	100K
[A] autenticidad de los usuarios y de la información	47K(4)	47K
[T] trazabilidad del servicio y de los datos	470K(5)	470K

(1) [I.d.m.2] porque la indisponibilidad de la información causaría un daño importante aunque subsanable
[I.d.m.3] porque la indisponibilidad de la información supondría el incumplimiento material o formal de una norma

[S.d.m.2] porque la detención del servicio causaría un daño importante aunque subsanable
[S.d.m.3] porque la detención del servicio supondría el incumplimiento material o formal de una norma

(2) [I.i.m.2] porque su manipulación o modificación no autorizada causaría un daño importante aunque subsanable
[I.i.m.3] porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma
[S.i.m.2] porque la manipulación o modificación no autorizada de la información que maneja causaría un daño importante aunque subsanable
[S.i.m.3] porque su manipulación o modificación no autorizada supondría el incumplimiento material o formal de una norma

(3) [A-] Nivel alto-

(4) [M+] Nivel medio+

(5) [A+] Nivel alto+

5.17. [ES-PERSONAL.PersonalG3] PersonalGrupo3

- [essential] Activos esenciales
- [D] Datos / Información
- [D.biz] datos de interés para el negocio
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [P] Personal
- [P.ui] usuarios internos
- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.des] desarrolladores / programadores

Dominio de seguridad

- [base] Base

Inferiores (activos de los que depende este)

- [HW-ESn.Servidor-ESn] ES-Servidor
- [HW-ESn.Terminales-ESn] ESn-Terminales
- [AUX.USB] ConexionUSB

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	2,2K(1)	2,2K
[I] integridad de los datos	2,2K(2)	2,2K
[C] confidencialidad de los datos	22K(3)	22K
[A] autenticidad de los usuarios y de la información	10K(4)	10K
[T] trazabilidad del servicio y de los datos	470K(5)	470K

(1) [I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[I.d.b.3] porque la indisponibilidad de la información supondría el incumplimiento leve de una norma
[S.d.b.2] porque la detención del servicio causaría algún perjuicio
[S.d.b.3] porque la detención del servicio supondría el incumplimiento leve de una norma
(2) [I.i.b.2] porque su manipulación o modificación no autorizada causaría algún perjuicio
[I.i.b.3] porque su manipulación o modificación no autorizada causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
[S.i.b.2] porque la manipulación o modificación no autorizada de la información que maneja causaría algún perjuicio
[S.i.b.3] porque la falsedad en su origen o en su destinatario causaría un daño reputacional apreciable con los ciudadanos o con otras organizaciones
(3) [M] Medio (confidencialidad de la información)
[M] Medio (confidencialidad de [la información que maneja] el servicio)
(4) [M-] Nivel medio-
(5) [A+] Nivel alto+

5.18. [ES-PERSONAL.PersonalG4] PersonalGrupo4

- [essential] Activos esenciales
- [D] Datos / Información
- [D.biz] datos de interés para el negocio
- [D.per] datos de carácter personal
- [D.per.A] de nivel alto
- [P] Personal
- [P.ui] usuarios internos
- [P.adm] administradores de sistemas
- [P.com] administradores de comunicaciones
- [P.dba] administradores de BBDD
- [P.des] desarrolladores / programadores

Dominio de seguridad

- [base] Base

Inferiores (activos de los que depende este)

- [HW-ESn.Servidor-ESn] ES-Servidor
- [HW-ESn.Terminales-ESn] ESn-Terminales
- [AUX.USB] ConexionUSB

Valor

dimensión	*valor*	*valores acumulados*
[D] disponibilidad	2,2K(1)	2,2K

[I] integridad de los datos	1.000(2)	1.000
[C] confidencialidad de los datos	2,2K(3)	2,2K
[A] autenticidad de los usuarios y de la información	4,7K(4)	4,7K
[T] trazabilidad del servicio y de los datos	470K(5)	470K

(1) [I.d.b.2] porque la indisponibilidad de la información causaría algún perjuicio
[I.d.b.3] porque la indisponibilidad de la información supondría el incumplimiento leve de una norma
[S.d.b.2] porque la detención del servicio causaría algún perjuicio
[S.d.b.3] porque la detención del servicio supondría el incumplimiento leve de una norma

(2) [I.i.n.1] cuando los errores en su contenido carecen de consecuencias o son fácil y rápidamente reparables
[S.i.n.1] cuando los errores en la información que maneja carecen de consecuencias o son fácil y rápidamente reparables

(3) [B] Bajo (confidencialidad de la información)
[B] Bajo (confidencialidad de [la información que maneja] el servicio)

(4) [B+] Nivel bajo+

(5) [A+] Nivel alto+

Anexo VI

Índice de tablas y figuras

16 Anexo VI

16.1 Índice de tablas

16.2 Índice de gráficos

Agradecimientos

17 Agradecimientos

Este estudio no hubiera sido posible sin los consejos, ayuda o recomendaciones de muchas personas que trabajan para diferentes instituciones. Me gustaría no olvidarme de ninguna de ellas

Al Dr. Tèrmens por sus consejos y recomendaciones en todo el estudio.

Entidades y personas que han colaborado en el estudio

Sr. Doménec Cardona, Cap d'Informàtica, Hospital Sant Joan de Déu

Gemma Gelabert, Cap d'Arxiu, l'Hospital Sant Joan de Déu

Lidia Garcia, Cap d'Arxiu, Consorci Sanitari de Terrassa

Manuel Martínez Motos, Cap d'Informàtica de Mútua de Terrassa

Sr. Bru, gerencia, Grup SAGESSA

Montse Aluja, Cap d'Arxiu, l'Hopital Sant Joan de Déu de Reus del Grup SAGESSA

Guillem Palauzie, Cap d'Arxiu, Corporació de Salut Maresme i la Selva

Imma Bosch, Cap d'Informàtica, Consorci Sanitari del Maresme

Robert Roger, gerent, Fundació Pere Mata

Carlos Cabello, Cap d'Informàtica, Fundació Pere Mata

Ricard Bernat Martinez-Hidalgo, Director de Sistemes d'Informació, Departament d' Obstetrícia, Ginecologia i Reproducció, Institut Universitari Dexeus

Xavier Salvador del Conjunt Mínim Bàsic de Dades, Departament de Salut de la Generalitat de Catalunya

Mr. John Garrett, CCSDS Data Archive Ingest Working Group Chair

Mr. Donald Sawyer, CCSDS

Dr. David Giaretta, Director of the Alliance for Permanent Access

Mr. John Jeremy Leighton, Digital Manuscript of the British Library

Frau Sabine Schmidt, Deutsche National Bibliotek.

Jordi, Anna, Marisa, Alex y Maite por las incansables horas que hemos estado juntos.

Belén, Silvia, Julià y Elena, gracias por vuestra ayuda

Al Dr. Juan R. Vericad, por sus innumerables consejos.

Finalmente agradecer a mi familia, Christine mi mujer, Daniel y Sara, mis hijos su infinita paciencia y sus ánimos constantes.